**ΠΑΝΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΟΙΝΩΝΙΚΩΝ ΚΑΙ ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ**
ΣΧΟΛΗ ΔΙΕΘΝΩΝ ΣΠΟΥΔΩΝ, ΕΠΙΚΟΙΝΩΝΙΑΣ & ΠΟΛΙΤΙΣΜΟΥ
ΤΜΗΜΑ ΔΙΕΘΝΩΝ, ΕΥΡΩΠΑΪΚΩΝ ΚΑΙ ΠΕΡΙΦΕΡΕΙΑΚΩΝ ΣΠΟΥΔΩΝ
**ΠΜΣ ΔΙΕΘΝΩΝ ΟΙΚΟΝΟΜΙΚΩΝ ΣΧΕΣΕΩΝ**

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ ΜΕ ΤΙΤΛΟ:

# ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΑ: Η ΠΕΡΙΠΤΩΣΗ ΤΟΥ BITCOIN

Φοιτήτρια: **ΒΟΥΛΓΑΡΗ ΑΓΓΕΛΙΚΑ ΑΣΤΡΙΝΤ**

ΑΜ: 1214M092

Επιβλέπων καθηγητής: **ΜΑΣΤΡΟΓΙΑΝΝΗΣ ΑΝΑΣΤΑΣΙΟΣ**

Ακαδημαϊκό έτος εκπόνησης εργασίας: 2014-2015

## ΠΕΡΙΛΗΨΗ

Στόχος της παρούσας εργασίας είναι η παρουσίαση των κρυπτονομισμάτων και συγκεκριμένα του Bitcoin. Τα κρυπτονομίσματα αποτελούν μέσα πληρωμής που χρησιμοποιούν την κρυπτογραφία για να εξασφαλίσουν τις συναλλαγές και για τον έλεγχο της δημιουργίας νέων μονάδων. Το Bitcoin έγινε το πρώτο αποκεντρωμένο κρυπτονόμισμα το 2009 ενώ από τότε έχουν δημιουργηθεί πολλά εναλλακτικά αυτού, αποκαλούμενα συνολικά ως altcoins (alternative coins). Η εργασία έπειτα από μία αναδρομή στην δημιουργία του χρήματος και στα παγκόσμια νομίσματα, προχωράει στην περιγραφή του τρόπου λειτουργίας του εξεταζόμενου κρυπτονομίσματος και των συνθετικών στοιχείων του. Εν συνεχεία παρουσιάζει τα ενδεχόμενα κίνητρα της δημιουργίας του, το υπάρχον νομοθετικό πλαίσιο αλλά και τις δυνητικές και πραγματικές επιπτώσεις και προκλήσεις που συνεπάγονται αυτού. Ακόμα, αποτυπώνει την κατάσταση και την χρήση του κρυπτονομίσματος στην Ελλάδα εν μέσω capital controls ενώ τέλος, ολοκληρώνει με την διασύνδεση της τιμής του με γεγονότα που την έχουν επηρεάσει και επίλογο.

## ΛΕΞΕΙΣ - ΚΛΕΙΔΙΑ

Κρυπτονομίσματα, Bitcoin, εικονικά χρήματα, ψηφιακό νόμισμα, αποκεντρωμένο νόμισμα, επαναπροσδιορισμός χρήματος

# Περιεχόμενα

# ΕΙΣΑΓΩΓΗ

Οι τεχνολογικές εξελίξεις μεταβάλλουν και διαμορφώνουν καθημερινώς κι αδιαλείπτως τις ζωές μας. Μία από τις πιο πρόσφατες απ' αυτές τις εξελίξεις, το Bitcoin. Πρόκειται για ένα ψηφιακό κρυπτονόμισμα που δημιουργήθηκε το 2009 από τον Satoshi Nakamoto ως μία εναλλακτική στα παραδοσιακά νομίσματα. Σκοπός του είναι να επιτρέπει συναλλαγές μεταξύ των χρηστών μέσω του διαδικτύου χωρίς την ανάμειξη τράπεζας ή άλλου τρίτου μέρους. Χρησιμοποιεί μία καινοτόμο κι ενδιαφέρουσα τεχνική που απαλλάσσει τους χρήστες από την ανάγκη ύπαρξης εμπιστοσύνης μεταξύ τους και προσφέρει πλεονεκτήματα όπως ταχύτητα, μείωση κόστους συναλλαγών και ψευδωνυμία. Η τεχνολογία του κρυπτονομίσματος έχει αγκαλιαστεί από την διαδικτυακή και τεχνολογική κοινότητα ενώ πολλές εταιρείες όπως η Microsoft και η Dell[1] αποδέχονται το bitcoin ως μέσο πληρωμής.

Η εργασία χωρίζεται σε 3 μέρη. Στο 1ο μέρος κρίνεται σκόπιμη μία ιστορική αναδρομή στην ιστορία του χρήματος ούτως ώστε να αναγνωριστούν οι λόγοι που οδήγησαν τους ανθρώπους στην υιοθέτησή του και αποδοχή του παρά την μηδαμινή εγγενή αξία του. Άλλωστε, για να κατανοήσει κάποιος το Bitcoin, θα πρέπει πρώτα να κατανοήσει το χρήμα. Έπειτα, καθώς το Bitcoin φιλοδοξεί να επαναπροσδιορίσει την ταυτότητα του χρήματος και να καταστεί ενδεχομένως ένα παγκόσμιο νόμισμα, γίνεται μία σύντομη ανάλυση των παγκόσμιων νομισμάτων τόσο σε πραγματικό όσο και σε ιδεατό επίπεδο.

Το 2ο μέρος εστιάζει σχεδόν εξολοκλήρου στο Bitcoin. Περιγράφεται λεπτομερώς με όσο το δυνατόν απλούστερο τρόπο η λειτουργία καθώς και τα συνθετικά του χαρακτηριστικά, που αποτελεί και τον βασικό σκοπό της εργασίας. Για την ακρίβεια γίνεται αναφορά σε ένα από τα βασικά σημεία προώθησης του κρυπτονομίσματος, την ψευδωνυμία/ημιανωνυμία. Εν συνεχεία, περιγράφονται ο τρόπος πρόσβασης και αποθήκευσης των Bitcoin νομισμάτων, ο ρόλος των miners και του mining καθώς και πώς αυτό διενεργείται, το όριο που υπάρχει στην ποσότητα των νομισμάτων που μπορούν να κυκλοφορήσουν και οι συνεπαγόμενες επιπτώσεις αυτού. Ακόμα, αναλύεται η έννοια των χαμένων νομισμάτων και η ήδη υπάρχουσα διαιρετότητα ενώ διερευνάται το ενδεχόμενο διεύρυνσής της. Τέλος, περιγράφονται τα Altcoins και παράλληλα επισημαίνεται η χρησιμότητά τους για το κρυπτοσύστημα του Bitcoin αλλά και τον ευρύτερο κλάδο.

Στο 3ο μέρος επιχειρείται η ανάλυση των κινήτρων του δημιουργού του Bitcoin ενώ εκτιμάται και ο βαθμός της επικινδυνότητας του για το κρυπτονόμισμα και την κοινότητά του. Έπειτα, περιγράφεται το ρυθμιστικό πλαίσιο ανά τον κόσμο και οι επιπτώσεις -είτε αρνητικές είτε θετικές- που το Bitcoin μπορεί να έχει καθώς και οι προκλήσεις που αυτό θέτει. Το μέρος αυτό ολοκληρώνει με την αποτύπωση της κατάστασης του κρυπτονομίσματος στην Ελλάδας εν μέσω capital controls και την διασύνδεση των αυξομειώσεων της τιμής του με σημαντικά για αυτό γεγονότα.

[1] http://www.coindesk.com/information/what-can-you-buy-with-bitcoins/ και http://www.bitcoinvalues.net/who-accepts-bitcoins-payment-companies-stores-take-bitcoins.html

Ακολουθεί επίλογος ενώ στο παράρτημα δίδεται λεξικό βασικών όρων.

# 1ο ΜΕΡΟΣ

## 1.1 Η δημιουργία του χρήματος.

Για να κατανοήσει κάποιος το Bitcoin, θα πρέπει πρώτα να κατανοήσει το χρήμα. Γιατί το χρησιμοποιούμε; Πώς το εφήυραμε; Πώς έφτασε να είναι στην παρούσα του μορφή; Από ποιά στάδια πέρασε;

Η ιστορία του χρήματος έχει ως αφετηρία την μετεξέλιξη των κυνηγών-τροφοσυλλεκτών σε αγρότες και τον μετέπειτα καταμερισμό εργασίας. Αυτό συνέβη διότι οι κυνηγοί-τροφοσυλλέκτες δεν συναλλάσσονταν και δεν αποθήκευαν την τροφή τους κι επομένως εξέλειπε γι' αυτούς η ανάγκη χρήσης χρημάτων.[2] Κατά τον Adam Smith[3], απ' την στιγμή που υπήρξε επαρκής καταμερισμός εργασίας και εξειδίκευση των εργατών, τα άτομα δύνατο να εξυπηρετήσουν ολοένα μειούμενο μέρος των αναγκών τους και συνεπώς προέκυψε σε μεγαλύτερο βαθμό η ανάγκη για ανταλλαγές. Το σύστημα Barter όπως είναι γνωστό, ήτοι ο αντιπραγματισμός ή ανταλλακτική οικονομία ή ανταλλακτικό εμπόριο, εντοπίζεται στις προκαπιταλιστικές οικονομίες, οι οποίες στηρίζονταν στην ανταλλαγή αγαθών.

Όπως είναι λογικό, το προσφερόμενο από κάποιον προς ανταλλαγή αγαθό μπορεί να μην ήταν επιθυμητό από τον κάτοχο του αγαθού που επιθυμούσε ο πρώτος. Αυτό, οδήγησε τα άτομα να αναζητήσουν αγαθά τα οποία θα γίνονταν αποδεκτά από όλους και θα μπορούσαν να χρησιμεύσουν είτε ως ιδία κατανάλωση ή χρήση είτε για την αγορά κάποιου άλλου αγαθού. Έτσι, στην πρώτη μορφή του χρήματος, έχουμε αγαθά ως χρήματα. Ιστορικά, τα αγαθά που έχουν επιτελέσει αυτόν τον ρόλο είναι μεταξύ άλλων τα βόδια, το αλάτι, τα κοχύλια, τα αποξηραμένα ψάρια, η ζάχαρη, τα δέρματα ακόμα και τα καρφιά.[4]

Η χρήση όμως αγαθών για την αγορά άλλων αγαθών βρίσκει πολλά κωλύματα με τα κύρια να εντοπίζονται στην ανισοσκελή αξία μεταξύ των αγαθών, στην φθαρτότητα των ιδίων των αγαθών καθώς και στην αδιαιρετότητά τους. Εάν παραδείγματος χάρη, ως κτηνοτρόφος κάποιος έχει βόδια κι επιθυμεί να αγοράσει ψωμί, θα πρέπει να αγοράσει ψωμί ίσης αξίας με ένα βόδι, ανεξαρτήτως της ποσότητας που επιθυμεί στην πραγματικότητα να αγοράσει, επειδή το βόδι δεν διαιρείται σε μικρότερα μέρη. Ακόμα, η αγορασμένη ποσότητα ψωμιού θα έχει σύντομη ημερομηνία λήξης, καθιστώντας τον κτηνοτρόφο υποχρεωμένο είτε να το καταναλώσει, είτε να το μεταπωλήσει, ή να υποστεί την απώλεια. Καθώς εξειδικεύονταν τα οικονομικά υποκείμενα κι αυξάνονταν οι εμπορικές συναλλαγές, η μέθοδος των ανταλλαγών δεν επαρκούσε. Ένα καθολικά αποδεκτό μέσο ανταλλαγής ήταν απαραίτητο.

Το νέο μέσο ανταλλαγής βέβαια, θα έπρεπε παράλληλα να παρουσιάζει ορισμένα ποιοτικά χαρακτηριστικά που θα το καθιστούσαν ευέλικτο, διαιρετό και το κατά δύναμιν άφθαρτο. Την απάντηση ήρθαν να δώσουν τα μέταλλα που πέραν των προαναφερθέντων χαρακτηριστικών, παρουσιάζουν επιπλέον και την δυνατότητα επανένωσης τους μέσω της τήξης. Το είδος των μετάλλων επιλεγόταν με βάση την αφθονία

[2] Ferguson, Niall, *Η εξέλιξη του χρήματος: Μία οικονομική ιστορία του κόσμου*, Εκδόσεις Αλεξάνδρεια, 2011, μεταφρασμένο
[3] Smith, Adam, *Έρευνα για τη φύση και τις αιτίες του πλούτου των εθνών*, Εκδόσεις Ελληνικά Γράμματα, 2010, μεταφρασμένο
[4] Ferguson, Niall, *Η εξέλιξη του χρήματος: Μία οικονομική ιστορία του κόσμου*, Εκδόσεις Αλεξάνδρεια, 2011, μεταφρασμένο

στην οποία υπήρχαν στην περιοχή ενδιαφέροντος. Σίδηρος, χαλκός, άργυρος και χρυσός ήταν τα πιο συνηθισμένα. Σε μία πρώτη μορφή, τα μέταλλα χρησιμοποιούνταν σε ράβδους αλλά καθώς αυτό δημιουργούσε προβλήματα ως προς την καθαρότητα κάθε φορά της ράβδου αλλά και της ζύγισης που έπρεπε να γίνεται και που συνεπακολούθως χρειαζόταν ακριβή εργαλεία ζύγισης, εφευρέθηκαν τα νομίσματα. Τα νομισματοκοπεία άνηκαν συνήθως στον ηγεμόνα της κάθε περιοχής και έκοπταν νομίσματα που είχαν δημόσια σφραγίδα για την πιστοποίηση της γνησιότητας. Η σφράγιση που γινόταν εγγυόταν υποτίθεται την ομοιόμορφη ποιότητα των νομισμάτων που βρίσκονταν σε κυκλοφορία. Εάν ήταν σφραγισμένη μονάχα η μία πλευρά του νομίσματος, ήταν εγγυημένη η καθαρότητά του, αλλά αυτό θα έπρεπε να ζυγιστεί καθώς δεν ήταν απόλυτα ομοιόμορφη η ποσότητα πολύτιμου μετάλλου στο κάθε νόμισμα. Η σφράγιση και των δύο πλευρών εγγυόταν και την ποσότητα κι έτσι τα νομίσματα αθροίζονταν αριθμητικά πλέον και δεν ζυγίζονταν.

Το μέταλλα ήταν πια μία λογιστική μονάδα, αποθηκευτής αξίας και φορητής ισχύος.[5]

Αρχικά οι ονομασίες των νομισμάτων εξέφραζαν την αξία, το βάρος ή την ποσότητα μετάλλου που περιείχαν. Ελλείψεις όμως στα πολύτιμα αυτά μέταλλα, οδήγησαν τους ευρωπαίους ηγεμόνες να προχωρήσουν σε κατακτητικούς πολέμους και λεηλασίες για την κάλυψη της έλλειψης. Ανάμεσα σε αυτούς τους πολέμους ήταν και οι Σταυροφορίες προς ανατολάς και η προς δυσμάς κατάκτηση του "Νέου Κόσμου" από τους ισπανούς κονκισταδόρες.

Οι μεγάλες αυτοκρατορίες όπως η Ρωμαϊκή, η Βρετανική και η Κινεζική εγκαθιστούσαν ενιαίους νομισματικούς κανόνες στις περιοχές που κυριαρχούσαν. Αξιοσημείωτη είναι όμως η κατάκτηση των Ίνκας με τα υπερμεγέθη αποθέματα ασημιού από τους ισπανούς, με την κατάσταση του ισπανικού ρεαλιού ως παγκόσμιο νόμισμα αφού χρησιμοποιήθηκε τόσο για την χρηματοδότηση περαιτέρω πολέμων όσον και για τις εμπορικές συναλλαγές με την Ασία. Ακολουθώντας όμως με τους νόμους της προσφοράς και της ζήτησης, η υπερπροσφορά ασημιού προκάλεσε θεαματική πτώση στην αξία του ίδιου του μετάλλου και συνεπώς στην αγοραστική του δύναμη. Η αξία ενός νομίσματος είναι λοιπόν σχετική κι όχι απόλυτη καθόσον ένα νόμισμα αξίζει μονάχα όσα διατίθεται ο άλλος να σου πληρώσει γι' αυτό.

Όσο πλήθαιναν οι εμπορικές συναλλαγές όμως, τόσο αυξανόταν η ανάγκη για νέα νομίσματα. Αρχικά, ο καθένας πήγαινε τον χρυσό του στο νομισματοκοπείο για να του κόψει νομίσματα ενώ το κέρδος των νομισματοκοπείων προέκυπτε συνήθως από την παρακράτηση ενός μικρού ποσοστού των νομισμάτων. Αργότερα, ο τρόπος με τον οποίο τα νομισματοκοπεία αποκτούσαν τα απαραίτητα πολύτιμα μέταλλα, ήταν μέσω της αγοράς της πρώτης ύλης από "παραγωγούς". Οι λεπτές ισορροπίες όμως ανάμεσα στην τιμή του μετάλλου και στην τιμή του νομίσματος φτιαγμένο από το ίδιο μέταλλο, εάν αναλογιστούμε και το κόστος παραγωγής, αφού τα μέταλλα υπόκεινται στις ίδιες επιδράσεις της προσφοράς και της ζήτησης όπως οποιοδήποτε άλλο αγαθό, οδήγησε σιγά σιγά τους ηγεμόνες στους οποίους άνηκαν τα νομισματοκοπεία να

[5] Ferguson, Niall, *Η εξέλιξη του χρήματος: Μία οικονομική ιστορία του κόσμου*, Εκδόσεις Αλεξάνδρεια, 2011, μεταφρασμένο

αναζητούν εναλλακτικές οδούς για την αποφυγή των προβλημάτων που προέκυπταν και που πήγαζαν από αυτήν την διαφορά στις τιμές του αγαθού στα διαφορετικά στάδιά του. Η λύση ήλθε όταν παρατηρήθηκε κι αναγνωρίστηκε πως τα άτομα χρησιμοποιούσαν ψευδονομίσματα πολύ μεγαλύτερης αξίας από το μέταλλο απ' το οποίο ήσαν κατασκευασμένα και καθώς οι ηγεμόνες δεν μπορούσαν να βρουν τα απαραίτητα πολύτιμα μέταλλα για να διατηρήσουν την αναλογία βάρους - ποσότητας μετάλλου - αξίας, προχώρησαν είτε στην νοθεία των νομισμάτων, είτε στην κατασκευή τους από μέταλλα χαμηλότερης αξίας.

Η αποδοχή νομισμάτων με την αξία των συστατικών του να είναι πολύ χαμηλότερη έως μηδαμινή συναντάται και στα χαρτονομίσματα. Η ιστορία των υποσχετικών ξεκινάει από την αρχαία Μεσοποταμία πριν από 5000 χρόνια όπου οι άνθρωποι κατέγραφαν σε μικρούς πήλινους δίσκους εμπορικές δοσοληψίες, όπου δηλωνόταν ότι ο κομιστής θα ελάμβανε συγκεκριμένη ποσότητα κάποιου συγκεκριμένου αγαθού σε μία συγκεκριμένη χρονική στιγμή. Είναι σημαντικό το γεγονός ότι δεν διευκρινιζόταν το πρόσωπο κι αυτό διότι σήμαινε ότι μπορούσαν να μεταβιβαστούν σε κάποιο άλλο άτομο ως πληρωμή κι αυτό το άτομο να εξαργυρώσει έπειτα τον πήλινο δίσκο. Τα σύγχρονα χαρτονομίσματα, που έχουν τις ρίζες τους στην Κίνα του έβδομου αιώνα, είναι απλά κομμάτια χαρτιού με καμία εγγενή αξία. Οι πρώτοι τραπεζίτες τα έδιναν για να βεβαιώσουν τους καταθέτες τους ότι μπορούν ανά πάσα στιγμή να επιστρέψουν τα χαρτιά και να λάβουν ποσό νομισμάτων ίσο με το αναγραφόμενο. Όσο η υποσχετική δύνατο να εξαργυρωθεί από οποιονδήποτε, οποτεδήποτε, δεν υπήρχε λόγος να μην μεταβιβάζεται σε κάποιο άλλο άτομο για την πληρωμή μεγαλυτέρων ποσών καθώς ήταν βολικότερο. Η σημασία της αρχικής ανάγκης για δυνατότητα εξαργύρωσης και μετατρεψιμότητας σε νόμισμα, αντικαταστάθηκε από την ζωτικής για κάθε νόμισμα σημασίας ευρείας αποδοχής (acceptability)[6]. Η κυκλοφορία όλο και περισσότερων χαρτονομισμάτων απαιτούσε πλέον μονάχα την αποδοχή τους από όλα τα εμπορικοοικονομικά υποκείμενα.

Όπως σωστά αναρωτιέται ο Ferguson[7], "πότε έπαψε το χρήμα να είναι μεταλλικό και μεταλλάχθηκε σε χαρτί προτού γίνει εντελώς αόρατο;". Η σημασία της αποδοχής έχει προχωρήσει τόσο ώστε πλέον αποδεχόμαστε χρήμα ακόμα και στην άυλη μορφή του με την χρήση πιστωτικών και χρεωστικών καρτών ή με ακόμα πιο ακραία αϋλότητα ως απλά νούμερα στην οθόνη ενός υπολογιστή. Όπως σωστά παρατηρούν οι Cowan και Jonard[8], "ήδη από τον Schumpeter, οι οικονομολόγοι έχουν αναγνωρίσει ότι η καινοτομία συνίσταται σε μεγάλο βαθμό στην ανασύσταση υπάρχουσας γνώσης". Κάπως έτσι φτάνουμε στη ιδιόμορφη περίπτωση των κρυπτονομισμάτων που στηρίζονται ίσως περισσότερο από τα παραδοσιακά νομίσματα -με την ευρεία έννοια ακόμα και στην άυλή τους μορφή- στην πίστη, στην αποδοχή (acceptability), μην έχοντας τίποτα το υλικό που να πιστοποιεί την ύπαρξή τους και την κυριότητά τους και χωρίς να υποστηρίζονται από κάποια κεντρική τράπεζα ή από κάποια κυβέρνηση.

[6] Cannan, Edwin, Collected Works. *Money: Its connection with rising and falling prices - Modern Currency and the regulation of its value - Economic scares*, Volume VII, Routledge/Thoemmes Press, eighth edition, 1997
[7] Ferguson, Niall, *Η εξέλιξη του χρήματος: Μία οικονομική ιστορία του κόσμου*, Εκδόσεις Αλεξάνδρεια, 2011, μεταφρασμένο
[8] Soete, Luc & ter Well, Bas, (editors), *The economics of the digital society*, Edward Elgar Publishing, Cheltenham, UK - Northampton, MA, USA, 2005

## 1.2 Παγκόσμια νομίσματα: Πραγματικά και Ιδεατά

Πώς θα ήταν το χρήμα εάν το εφευρίσκαμε σήμερα; Είναι πολύ πιθανό να μην είχε την ίδια μορφή που όλοι γνωρίζουμε καλά. Καθ' ότι βρισκόμαστε πλέον σε μία εποχή με κυρίαρχες τις ηλεκτρονικές συσκευές, την εποχή της πληροφορικής, όπου ο ψηφιακός κόσμος συναγωνίζεται και ενίοτε ξεπερνάει τον πραγματικό, τον υλικό, θα ήταν ασφαλές να υποθέσουμε πως το μόλις εφευρεμένο χρήμα, εάν δηλαδή το είχαμε εφεύρει σήμερα, θα ήταν σε ψηφιακή μορφή. Τα χαρακτηριστικά που θα προσλάμβανε θα ήταν τέτοια ώστε να ταιριάζουν στον σύγχρονο τρόπο ζωής.

Εάν λοιπόν εφευρίσκαμε το χρήμα σήμερα θα θέλαμε να είναι ψηφιακό αντί για χάρτινο ή μεταλλικό καθώς αυτά τα δύο μπορούν εύκολα είτε να καταστραφούν είτε να χαθούν. Θα επιλέγαμε πιθανώς να είναι αποκεντρωμένο αντί να ελέγχεται από κάποια οντότητα που θα σήμαινε ότι θα μειωνόταν ο κίνδυνος να χειραγωγείτο. Ακόμα, θα μας διευκόλυνε εξαιρετικά να είναι παγκόσμιο, κάνοντας δυνατή την χρήση του σε οποιοδήποτε και κάθε μέρος του πλανήτη χωρίς να υπάρχει η ανάγκη μετατροπής από ένα νόμισμα σε κάποιο άλλο.

Η ιδέα ενός παγκόσμιου νομίσματος δεν είναι φυσικά κάτι καινούργιο. Μία ανασκόπηση[9] στην νομισματική ιστορία θα δείξει πως υπήρξαν πολλές προσπάθειες για την καθιέρωση ενός ενιαίου νομίσματος. Η επιθυμία για απόπειρα και μεταστροφή προς ένα ενιαίο νόμισμα έχει υπάρξει συνεχής. Κάθε φορά που η οικονομική και πολιτική σταθερότητα επέτρεπαν την επέκταση του διεθνούς εμπορίου, γίνονταν προσπάθειες για την εισαγωγή ενός παγκόσμιου, καθολικού νομίσματος που να ικανοποιούσε τις απαιτήσεις του διεξαγόμενου εμπορίου.

Λόγω των πολιτικών οφελών που επέρχονται μετά την καθιέρωση ενός παγκόσμιου, καθολικού νομίσματος, η επέκταση της πολιτικής ισχύος συνήθως συνοδεύεται από έναν ενιαίο νομισματικό κανόνα. Αντιστρόφως, ένα ενιαίο νόμισμα απαιτεί συνήθως μία κοινή κοινωνική, πολιτική ή/και οικονομική κουλτούρα, μία ενιαία κυβερνητική αρχή και μία ευρεία περιοχή διεξαγωγής εμπορίου, που να μπορούν να επωφεληθούν από την χρήση ενός κοινού νομίσματος. Ιστορικά, τα ενιαία νομίσματα έπρεπε να αναμένουν την δημιουργία μεγάλων (πολιτικών) αυτοκρατοριών πριν να μπορέσουν να εισαχθούν. Τόσο η Ρωμαϊκή Αυτοκρατορία όσο και η Κινέζικη και η Βρετανική, ίδρυσαν όλες έναν ενιαίο νομισματικό κανόνα για τις περιοχές στις οποίες ήσαν κυρίαρχες. Παρά όμως το γεγονός ότι πίσω από την ύπαρξη ενός παγκόσμιου νομίσματος κρύβονται οικονομικοί λόγοι, η ιστορία μας δείχνει ότι η πολιτική και όχι η οικονομία είναι αυτή που αποτελεί τον καθοριστικό παράγοντα στον σχηματισμό νομισματικών ζωνών στο παρελθόν αλλά και σήμερα. Στο παρελθόν, πάντως, όσο ενέμεναν η οικονομική και πολιτική σταθερότητα, νομισματικώς ενοποιημένες περιοχές αποσκοπούσαν στην εξυπηρέτηση των αναγκών του εμπορίου. Μονάχα όταν παράπαιε η οικονομική ή -πιο συχνά- η πολιτική σταθερότητα, εισάγονταν νέα, εναλλακτικά προς το υπάρχον, νομίσματα.

[9] Taylor Bryan, A History of Universal Currencies, Global Financial Data, [doc] http://www.singleglobalcurrency.org/documents/ArticlebyBryanTaylorAHistoryofUnivesalCurrencies.doc

Υπάρχουν από τα αρχαία χρόνια περιπτώσεις κερμάτων, καλής ποιότητας, που γίνονταν αποδεκτά από όλον τον αρχαίο κόσμο, όπως το αθηναϊκό τετράδραχμο με την γλαύκα. Η πραγματική εμφάνιση όμως ενός παγκόσμιου, καθολικού νομίσματος, έπρεπε να περιμένει την ίδρυση της Ρωμαϊκής Αυτοκρατορίας στην περιοχή της Μεσογείου καθώς και τις Qin kai Han δυναστείες στην Κίνα. Οι νομισματικώς ενοποιημένες περιοχές της Ρώμης και της Κίνας, διατηρήθηκαν για όσο καιρό ενέμεναν η οικονομική και πολιτική σταθερότητα. Όταν επερχόταν αστάθεια σε αυτούς τους δύο ζωτικούς τομείς, τα ενιαία νομίσματα αποτύγχαναν.

Η Διεθνής Νομισματική Διάσκεψη του 1867 επιχείρησε να δημιουργήσει έναν ενιαίο νομισματικό κανόνα για όλη την Ευρώπη. Μία από τις ιδέες που συζητήθηκαν στην συνδιάσκεψη, πρότεινε την κοπή ενός νομίσματος που να ισούτο με 25 γαλλικά φράγκα, 5 αμερικανικά δολάρια ή 1 λίρα Βρετανίας οπότε και θα περιείχε ίση ποσότητα χρυσού και θα μπορούσε να χρησιμοποιηθεί σε ολόκληρη την Ευρώπη και τις ΗΠΑ. Η ιδέα, φυσικά, δεν είχε ευρεία αποδοχή και καμία νομισματική αλλαγή δεν επήλθε της διασκέψεως. Το 1878, οι ΗΠΑ συγκάλεσαν νέα Διεθνή Νομισματική Διάσκεψη με την ελπίδα να θεσπιστεί ένας διμεταλλικός χρυσός και ασημένιος κανόνας, η οποία επίσης απέτυχε.

Μετά από μία σειρά οικονομικών αλλαγών, φτάνουμε στον Χρυσό Κανόνα, σύμφωνα με τον οποίο "κάθε χώρα έθετε μία σταθερή τιμή χρυσού σε όρους του νομίσματός της, στην οποία ήταν έτοιμη να αγοράσει ή να πουλήσει."[10] Συνεπώς, το νόμισμα της κάθε χώρας ήταν άμεσα ανταλλάξιμο σε χρυσό ανά πάσα στιγμή. Χωρίς μία ενιαία ευρωπαϊκή κυβέρνηση, μία κοινώς αποδεκτή υπερεθνική αρχή ή μία διεθνή νομισματική συμφωνία, ο χρυσός κανόνας ήταν ότι πιο κοντινό σε ένα παγκόσμιο νόμισμα που μπορούσε να υπάρχει. Οι ισοτιμίες των νομισμάτων λοιπόν καθορίστηκαν ως προς τον χρυσό και μέσω αυτού, ο χρυσός έδενε τις συναλλαγματικές ισοτιμίες μεταξύ τους. Αν το νόμισμα μίας χώρας υπερτιμάτο, ο χρυσός έρεε εκτός των συνόρων αυτής προς άλλες χώρες, αποκαθιστώντας με αυτόν τον τρόπο την συναλλαγματική ισοτιμία στα φυσιολογικά της επίπεδα. Το αποτέλεσμα ήταν σχεδόν η πλήρης κατάργηση των διακυμάνσεων των συναλλαγματικών ισοτιμιών μεταξύ των σημαντικότερων νομισμάτων παγκοσμίως.

Μέχρι το 1914, την αρχή του Α' Παγκοσμίου Πολέμου και το τέλος του Χρυσού Κανόνα, η βρετανική λίρα ήταν το κυρίαρχο διεθνές νόμισμα. Ουσιαστικά, η Τράπεζα της Αγγλίας λειτουργούσε ως παγκόσμια κεντρική τράπεζα, διαχειριζόμενη τον Χρυσό Κανόνα μέσω των επιτοκίων. Η έλευση όμως του Παγκοσμίου Πολέμου το 1914, ανάγκασε τις χώρες να αναστείλουν σταδιακά την μετατρεψιμότητα των νομισμάτων τους και συνεπακολούθως τον Χρυσό Κανόνα που μέχρι τον Αύγουστο εκείνου του έτους είχε λειτουργήσει ομαλά.

Παρά τις πολυάριθμες προσπάθειες για να σταθεροποιηθεί το διεθνές χρηματοπιστωτικό σύστημα μετά το τέλος του Α' Παγκοσμίου Πολέμου, κάθε προσπάθεια διακρινόταν μόνο από προσωρινή επιτυχία. Χωρίς

[10] McAleese, Dermot, "Οικονομική για επιχειρησιακές σπουδές: Ανταγωνισμός, Μακροσταθερότητα και Παγκοσμιοποίηση", Εκδόσεις Τυπωθήτω, 2005, μεταφρασμένο.

την απαραίτητη πολιτική και οικονομική σταθερότητα, οποιαδήποτε προσπάθεια εισαγωγής κάποιου ενιαίου νομίσματος ήταν καταδικασμένη να αποτύχει. Η περίοδος του Μεσοπολέμου διακρινόταν από διεθνή οικονομική αστάθεια με υπερπληθωρισμό κι ανταγωνιστικές υποτιμήσεις. Η Βρετανία ήταν πολύ αδύναμη οικονομικά για να επιτελέσει στο παγκόσμιο χρηματοπιστωτικό σύστημα ρόλο παρόμοιο με αυτόν που είχε κατά την περίοδο του Χρυσού Κανόνα, ενώ οι πιεστικές τάσεις απομονωτισμού των ΗΠΑ τις έκαναν απρόθυμες να αναλάβουν την θέση της Βρετανίας στο παγκόσμιο χρηματοοικονομικό στερέωμα.

Τον Ιούλιο του 1944, έπειτα από την λήξη του Β' Παγκοσμίου Πολέμου, οι εκπρόσωποι 44 χωρών συναντήθηκαν στο Bretton Woods.[11] Η διάσκεψη αυτή, είχε ως στόχο την εκ νέου καθιέρωση ενός βιώσιμου νομισματικού συστήματος και την διασφάλιση ότι τα οικονομικά προβλήματα που ακολούθησαν τον Α' Παγκόσμιο Πόλεμο κατά την περίοδο του Μεσοπολέμου δεν θα εμφανίζονταν και πάλι μετά την λήξη του Β'. Το Bretton Woods καθιέρωσε έναν κανόνα δολαρίου, αντικαθιστώντας τον κανόνα του χρυσού. Η τιμή του δολαρίου θα ήταν σταθερή ως προς τον χρυσό στα 35 $ ανά ουγκιά και τα άλλα νομίσματα θα ήταν κλειδωμένα προς το δολάριο. Οι συναλλαγματικές ισοτιμίες ήταν προκαθορισμένες βραχυπρόθεσμα αλλά άφηναν ανοιχτό το ενδεχόμενο αναπροσδιορισμού τους μακροπρόθεσμα. Ενώ την δεκαετία του 1950, το χαμηλό επίπεδο διεθνών ροών κεφαλαίου και διεθνούς εμπορίου καθιστούσε σχετικά εύκολη την διαχείριση από το σύστημα του Bretton Woods, μέχρι τις αρχές του 1970, ο κόσμος είχε αλλάξει δραματικά και το σύστημα άρχισε να σπάει υπό την πίεση. Το διεθνές εμπόριο αυξήθηκε και οι χώρες ξεκίνησαν να διαφοροποιούν τις νομισματικές τους πολιτικές. Οι επιρροές του κεϋνσιασμού ως προς την δημοσιονομική πολιτική ωθούσαν πολλές κυβερνήσεις να επιθυμούν τον περιορισμό του υφεσιακού κομματιού των οικονομικών κύκλων και δημιουργούσαν αιτήματα για αύξηση των κρατικών δαπανών συνδυαζόμενα με καθυπόταξη της νομισματικής πολιτικής στην δημοσιονομική. Οι πληθωριστικές πιέσεις που ακολούθησαν ήταν σταδιακές αλλά επίμονες. Το σύστημα του Bretton Woods κατέρρευσε οριστικώς το 1973 και οι σταθερές συναλλαγματικές ισοτιμίες αντικαταστάθηκαν από κυμαινόμενες. Στο καινούργιο Μη-Σύστημα, το δολάριο εξακολουθεί παρόλα αυτά να απολαμβάνει κεντρικό και ηγεμονικό ρόλο ως κορυφαίο συναλλαγματικό και αποθεματικό νόμισμα.

Στην σφαίρα του ιδεατού, λόγω της σύνδεσης των παγκόσμιων ανισορροπιών με τις συναλλαγματικές ισοτιμίες, η αντιμετώπιση αυτών έχει πολλές φορές εκφραστεί μέσω της ανάπτυξης ιδεών περί ρύθμισης των νομισματικών πολιτικών των κρατών συνήθως με την δημιουργία κάποιου παγκόσμιου νομίσματος. Εκκινώντας με τον Keynes[12] που στις αρχές της δεκαετίας του 1940 πρότεινε ένα διεθνές τραπεζικό χρήμα, το bancor, του οποίου η αξία θα ήταν σταθερή αλλά όχι αμετάβλητη προς τον χρυσό και θα γινόταν αποδεκτό από την Βρετανική Κοινοπολιτεία, τις ΗΠΑ καθώς κι όλα τα μέλη της Διεθνούς Ένωσης Εκκαθαρίσεως που θα είχε ιδρυθεί. Ο Graham, το 1944 προτείνει ένα παγκόσμιο εμπορευματικό

[11] McAleese, Dermot, "Οικονομική για επιχειρησιακές σπουδές: Ανταγωνισμός, Μακροσταθερότητα και Παγκοσμιοποίηση", Εκδόσεις Τυπωθήτω, 2005, μεταφρασμένο.

[12] http://www.econ.jku.at/members%5CLandesmann%5Cfiles%5CWS08%5C239339%5CDiplomarbeit_Klaffenboeck_zentrale_kapitel.pdf

αποθεματικό νόμισμα, αποτελούμενο από ένα καλάθι 23 εμπορευμάτων συχνής χρήσης, αφότου είχε παρατηρήσει ότι κατά την διάρκεια της κρίσης 1920-1921 η τιμή του χρυσού είχε διατηρηθεί σταθερή.[13] Στηριζόμενος σε αυτήν την πρόταση, ο Kaldor μαζί με τους Hart και Tinbergen, το 1964 πρότειναν κι αυτοί στην Διάσκεψη των Ηνωμένων Εθνών για το Εμπόριο και την Ανάπτυξη (UNCTAD) ένα εμπορευματικό αποθεματικό νόμισμα. Έπειτα κι από την πρόταση του Triffin που είχε διατυπωθεί το 1960 για μία νέα μονάδα αποθεματικού που θα ήταν ανεξάρτητη από άλλα νομίσματα ή τον χρυσό[14], υιοθετήθηκε τελικά το 1968 από το ΔΝΤ μία ενδιάμεση λύση με τα Ειδικά Τραβηκτικά Δικαιώματα (Special Drawing Rights ή SDR). Όμως, αυτά απέτυχαν να αντικαταστήσουν το δολάριο και τον χρυσό ως παγκόσμια αποθεματικά[15] ενώ δεν αποτελούν παρά αξίωση σε νομίσματα μελών του ΔΝΤ[16].

[13] http://www.bloombergview.com/articles/2013-02-28/benjamin-graham-s-clever-idea-for-averting-currency-wars
[14] https://www.imf.org/external/np/exr/center/mm/eng/mm_sc_03.htm
[15] http://www.qc-econ-bba.org/seminarpapers/leanne_figss.pdf
[16] http://www.bengrahaminvesting.ca/outreach/articles/commodities_as_a_global_currency.pdf

# 2ο ΜΕΡΟΣ

## 2.1 Το Bitcoin

Την Πέμπτη 8 Ιανουαρίου του 2009 ώρα 14:27:40 EST, ένας άνθρωπος ή μία ομάδα ανθρώπων υπό το ψευδώνυμο Satoshi Nakamoto[17] ανακοίνωνε/ανακοίνωναν "the first release of Bitcoin, a new electronic cash system that uses a peer-to-peer network to prevent double-spending. It's completely decentralized with no server or central authority."[18] Δύο μήνες νωρίτερα, είχε/είχαν δημοσιοποιήσει στο διαδίκτυο μία εργασία με τίτλο "Bitcoin: A Peer-to-Peer Electronic Cash System"[19].

Το Bitcoin είναι το πρώτο αποκεντρωμένο ψηφιακό κρυπτονόμισμα. Πρόκειται για ένα αποκεντρωμένο σύστημα ψηφιακών μετρητών που χρησιμοποιεί μία peer-to-peer (P2P)[20] δικτύωση μαζί με ηλεκτρονικές υπογραφές και κρυπτογράφηση για να παράγει το νόμισμα. Λειτουργεί με ένα δημόσιο βιβλίο ισολογισμού όπου καταγράφονται όλες οι συναλλαγές που διεξάγονται στο οικοσύστημα του νομίσματος.

Η μετάβαση από την χρήση μετάλλων με εγγενή αξία στην χρήση παραστατικού χρήματος ή χρήματος αναγκαστικής κυκλοφορίας (fiat money) όπως είναι τα χαρτονομίσματα[21] σηματοδότησε την αφετηρία της ψηφιοποίησης των χρημάτων. Δεν έχουμε πια να κάνουμε με μέταλλα αλλά με αριθμούς. Έτσι τα χρήματα γίνονται ευκολότερα στην μέτρηση, στην διαχείριση και στην μεταφορά. Στον σύγχρονο κόσμο των ηλεκτρονικών υπολογιστών, η ψηφιοποίηση έχει προχωρήσει ένα βήμα παραπέρα καθώς η συντριπτική πλειοψηφία των χρημάτων την σήμερον ημέρα, υπάρχει μονάχα ως αριθμός σε κάποια οθόνη. Τον ρόλο επιτηρητή και διαχειριστή αυτού του συστήματος ώστε να λειτουργούν όλα ορθά κι ομαλά στις συναλλαγές μεταξύ των ατόμων επιτελούν οι τράπεζες. Οι τράπεζες ως τα έμπιστα τρίτα μέλη, κρατούν αρχεία, βιβλία ισολογισμού, όπου καταγράφουν ποιος έχει τί στον λογαριασμό του. Όποιος επιθυμεί να κάνει χρήση αυτού του συστήματος διατηρεί απλά έναν λογαριασμό σε κάποια τράπεζα. Έτσι, εμείς εμπιστευόμαστε τις τράπεζες να γνωρίζουν, να πιστοποιούν και να αποδέχονται την κυριότητα των όσων μας ανήκουν κι αυτές με την σειρά τους εμπιστεύονται τους υπολογιστές τους με κεντρικά ελεγχόμενα βιβλία ισολογισμών.

Το 2008, ο Satoshi Nakamoto παρουσίασε στον κόσμο έναν τρόπο να λυθεί το πρόβλημα του double spending[22] που εμφανιζόταν στις ηλεκτρονικές συναλλαγές συνήθως εκτός του πλαισίου κάποιας τράπεζας με ένα αποκεντρωμένο, δημόσιο βιβλίο ισολογισμού που παρέκαμπτε την ανάγκη ύπαρξης κάποιου έμπιστου τρίτου μέλους, ήτοι τις τράπεζες. Ίσως το πιο γνωστό παγκοσμίως σύστημα που λειτουργεί χωρίς

[17] Η ταυτότητα του ατόμου ή των ατόμων που κρύβονται πίσω από το Bitcoin παραμένει μέχρι και σήμερα άγνωστη. Για ευκολία, πολλές φορές θα γίνεται λόγος για τον Satoshi ή τον Satoshi Nakamoto ώσαν να είναι ένα άτομο γένος αρσενικού με τοιαύτο το όνομα. Δεν πρέπει να λησμονείται πως ούτε το γένος ούτε ο αριθμός κι ούτε φυσικά το πραγματικό όνομα του ή των ατόμων είναι γνωστά.

[18] http://www.metzdowd.com/pipermail/cryptography/2009-January/014994.html

[19] https://bitcoin.org/bitcoin.pdf

[20] Το peer-to-peer αναφέρεται σε υπολογιστικά συστήματα ή συστήματα δικτύου που έχουν μία αρχιτεκτονική κατανεμημένων εφαρμογών που επιτρέπουν στο κάθε ισόκυρο και ισοδύναμο συμμετέχοντα να αλληλεπιδρά οργανωμένα και συλλογικά με άλλους.

[21] http://users.uom.gr/~esartz/teaching/macro/Kef27.pdf

[22] Πρόβλημα που παρουσιάζεται στις ηλεκτρονικές συναλλαγές παντός τύπου και αφορά την πίστωση των ίδιων νομισματικών μονάδων σε δύο ξεχωριστούς παραλήπτες/χρήστες ταυτόχρονα.

κεντρικό έλεγχο είναι το internet. Το internet δεν ανήκει σε κανέναν. Είναι το πιο μεγάλο και ισχυρό δίκτυο που έχει δημιουργήσει ποτέ ο άνθρωπος, αλλά δεν ανήκει σε καμία εταιρεία ή κυβέρνηση. Η υποδομή όμως, για να λειτουργεί, είναι κατασκευασμένη και συντηρείται από ανθρώπους κι επιχειρήσεις, πέραν συνόρων, ιδεολογιών και εταιρικών αντιπαλοτήτων. Φυσικά, αυτά γίνονται χάριν κέρδους και οικονομικών συμφερόντων. Τα κίνητρα λοιπόν που παρέχει το internet είναι κι αυτά που συντηρούν την λειτουργία του.

Είναι εξαιρετικά πιθανό ο Satoshi να είχε το internet στο μυαλό του καθώς σχεδίαζε το Bitcoin. Κατ' αρχάς λειτουργεί αποκεντρωμένα, χωρίς να ελέγχεται από κάποια κεντρική ή μη τράπεζα ή κάποια κυβέρνηση. Έχει στην βάση του ένα κρυπτογραφικό πρωτόκολλο, ένα σύστημα στο οποίο κανείς δεν μπορεί να επέμβει κι ένα αλγόριθμο που θέτει τους κανόνες της παραγωγής των νέων νομισμάτων. Κατά δεύτερον, το βιβλίο ισολογισμού είναι δημόσιο, κοινόχρηστο και συντηρούμενο από το κοινό. Ο καθένας, όπως έχουν ήδη κάνει χιλιάδες, μπορεί να κατεβάσει και να διατηρεί ένα αντίγραφο του βιβλίου αυτού στον ηλεκτρονικό του υπολογιστή και φυσικά να το επαληθεύει. Το βιβλίο ισολογισμού ονομάζεται blockchain και είναι μία συνεχώς μεγεθυνόμενη βάση δεδομένων με λογιστική μονάδα το bitcoin, όπου αποθηκεύονται όλες οι επαληθευμένες συναλλαγές. Κατά τρίτον, ένας από τους ζωτικούς παράγοντες λειτουργίας του κρυπτονομίσματος είναι οι miners. Αυτοί αποτελούν τους ρυθμιστές του οικοσυστήματος του Bitcoin, καθώς είναι αυτοί που επικυρώνουν τις συναλλαγές που γίνονται εντός του πλαισίου του. Ως κίνητρο για την παροχή των υπηρεσιών τους, λαμβάνουν ως αμοιβή τα νέα νομίσματα που παράγονται. Οι συναλλαγές διενεργούνται μεταξύ διευθύνσεων αντί μεταξύ λογαριασμών. Σε κεφάλαια που θα ακολουθήσουν, θα γίνει προσπάθεια αναλυτικότερης περιγραφής των στοιχείων που συνθέτουν το εξεταζόμενο κρυπτονόμισμα.

## 2.2 Ψευδωνυμία και Ημιανωνυμία στο κρυπτοσύστημα

Το Bitcoin λειτουργεί στην βάση της ψευδωνυμίας. Οι χρήστες, δεν είναι υποχρεωτικό να δηλώνουν κάπου το όνομά τους ή τα πλήρη στοιχεία τους. Ο κάθε χρήστης, δημιουργώντας έναν λογαριασμό, αποκτά μία διεύθυνση στην οποία αντιστοιχούν ένα ιδιωτικό κι ένα δημόσιο κλειδί. Το ιδιωτικό κλειδί κρατείται κρυφό από τον χρήστη καθώς αυτό του δίνει την δυνατότητα να έχει πρόσβαση στο πορτοφόλι του και να παράγει μία ψηφιακή υπογραφή (digital signature) με την οποία πιστοποιεί την συναλλαγή την οποία επιθυμεί να κάνει. Το δημόσιο κλειδί του είναι αυτό που γίνεται γνωστό στο δεύτερο μέλος της συναλλαγής. Δεν υπάρχει περιορισμός στον αριθμό δημοσίων και ιδιωτικών κλειδιών που μπορεί να έχει ο καθένας. Η ψευδωνυμία προκύπτει από το γεγονός ότι ο χρήστης χρησιμοποιεί το δημόσιο κλειδί του και όχι το όνομα του. Συνεπώς, τα άτομα με τα οποία συναλλάσσεται δεν μπορούν να γνωρίζουν την ταυτότητα του ιδίου.

Θα μπορούσε ακόμα, να γίνει λόγος όχι περί πλήρους ανωνυμίας αλλά περί ημιανωνυμίας. Αυτό σχετίζεται άμεσα με τον τρόπο λειτουργίας των συναλλαγών στο σύστημα του Bitcoin. Όλες οι συναλλαγές εντός του οικοσυστήματος του κρυπτονομίσματος, αποτελούν μία αλυσίδα, την Transaction Blockchain. Κάθε συναλλαγή πρέπει να παραπέμπει σε μία προηγούμενη ώστε να πιστοποιείται ότι όντως υπάρχουν τα bitcoin

που επιθυμούνται να ξοδευτούν. Δηλαδή εάν κάποιος κατέχει 10 bitcoin, έχοντας λάβει 5 bitcoin από την συναλλαγή Α και 5 από την συναλλαγή Β και εν συνεχεία επιθυμεί να αποστείλει σε κάποιον άλλον χρήστη 10 bitcoin, θα πρέπει στην συναλλαγή να χαρακτηρίζει ως inputs τις συναλλαγές Α και Β. Εάν βρεθεί κατά τον έλεγχο της συναλλαγής ότι τα inputs δεν έχουν χρησιμοποιηθεί κάπου αλλού, η συναλλαγή εγκρίνεται. Εάν όμως υποθέσουμε ότι από την συναλλαγή Α είχε πάρει 7 bitcoin αντί για 5, τότε στην συναλλαγή Γ θα πρέπει να συμπεριλάβει κι ένα υπόλοιπο 2 bitcoin τα οποία θα του επιστρέφονται, εξαιτίας του γεγονότος ότι στα inputs μπορεί κανείς να χρησιμοποιήσει μονάχα προηγούμενες συναλλαγές στην πληρότητά τους κι όχι μόνο ένα μέρος τους.

Το γεγονός της ημιανωνυμία του κρυπτονομίσματος συνδέεται άμεσα με τα ψηφιακά αποτυπώματα και ίχνη που αφήνει ο κάθε χρήστης στο διαδίκτυο. Όπως αποδεικνύεται άλλωστε κι από την πραγματικότητα (περίπτωση Silk Road και pirate@40 - ponzi scheme)[23], δεν παρέχεται πλήρη ανωνυμία στους χρήστες έναντι στις διωκτικές αρχές παρά το γεγονός ότι ο σχεδιασμός του συστήματος δεν τις διευκολύνει στο έργο τους.

Ένα ακόμα σημείο που αξίζει να αναφερθεί είναι πως αν και ο κάθε χρήστης μπορεί να έχει όσα ιδιωτικά και δημόσια κλειδιά θέλει, η αλληλοσύνδεση και παραπομπή των συναλλαγών στην αλυσίδα μπορεί τελικά να συνδέσει κλειδιά μεταξύ τους κι έτσι να αποκαλύπτει εμμέσως την ταυτοπροσωπία του κατόχου διαφόρων κατά τα άλλα ανεξάρτητων μεταξύ τους λογαριασμών.

## 2.3 Bitcoin Πορτοφόλι.

Το Bitcoin πορτοφόλι υπεραπλουστευμένα θεωρείται ως ο χώρος στον οποίο αποθηκεύονται τα bitcoin του κάθε χρήστη. Για την ακρίβεια όμως, είναι ο χώρος όπου αποθηκεύονται οι πληροφορίες με τις οποίες ο κάθε χρήστης μπορεί να ξεκλειδώσει και να χρησιμοποιήσει τα bitcoin του. Το πορτοφόλι επιτρέπει δηλαδή στον χρήστη να δέχεται και να αποστέλλει bitcoin και θα μπορούσε να είναι κάποιο λογισμικό, μια ιστοσελίδα, ένα χάρτινο πορτοφόλι, ένα κινητό τηλέφωνο, ένα usb stick ή ένας εξωτερικός σκληρός δίσκος ή ακόμα και υλικά νομίσματα. Στον κάθε χρήστη αντιστοιχούν ένα ιδιωτικό κλειδί (private key) κι ένα δημόσιο (public key) κι αυτές ακριβώς είναι οι πληροφορίες που περιέχονται στο πορτοφόλι. [24]

Ας παρομοιάσουμε το πορτοφόλι με μία διεύθυνση ηλεκτρονικού ταχυδρομείου. Κατ' αρχάς για να λειτουργήσουν όλα χρειαζόμαστε ένα πρόγραμμα να μας εξυπηρετήσει. Στα e-mail αυτό μπορεί να είναι λ.χ. το outlook, το gmail ή κάτι παρόμοιο. Για το σύστημα του Bitcoin αυτό θα είναι ένα Bitcoin client[25].

---

[23] http://www.forbes.com/sites/andygreenberg/2013/10/25/fbi-says-its-seized-20-million-in-bitcoins-from-ross-ulbricht-alleged-owner-of-silk-road/ και https://www.cryptocoinsnews.com/pirate40-arrested-bitcoin-ponzi-scam/

[24] Beigel Ofil, What is a Bitcoin Wallet, 29/01/2014, 99Bitcoins, https://99bitcoins.com/what-is-a-bitcoin-wallet/

[25] "**Εξυπηρετητής** ή **διακομιστής** (αγγλ.: **server**) είναι υλικό ή / και λογισμικό που αναλαμβάνει την παροχή διάφορων υπηρεσιών, «εξυπηρετώντας» αιτήσεις άλλων προγραμμάτων, γνωστούς ως **πελάτες** (clients) που μπορούν να τρέχουν στον ίδιο υπολογιστή ή σε σύνδεση μέσω δικτύου. Όταν ένας υπολογιστής εκτελεί κυρίως τέτοια προγράμματα εξυπηρετητές συνεχόμενα, 24 ώρες την ημέρα, τότε μπορούμε να αναφερθούμε σε όλον τον υπολογιστή ως *εξυπηρετητή*, αφού αυτή είναι η κύρια λειτουργία

Για να δεχτούμε ένα e-mail πρέπει να έχουμε μία διεύθυνση την οποία μπορούν να δουν όλοι. Έτσι και στο Bitcoin, το δημόσιο κλειδί εκτελεί χρέη διεύθυνσης. Το συγκεκριμένο κλειδί μπορούν να το δουν όλοι και αυτό είναι το στοιχείο που δηλώνεται όταν κάποιος πρόκειται να μας στείλει bitcoin. Για να έχουμε πρόσβαση όμως να διαβάσουμε αυτό το e-mail χρειάζεται να γνωρίζουμε τον απαραίτητο κωδικό, το password. Στο Bitcoin, κωδικός μας είναι το ιδιωτικό κλειδί. Αυτό, μας επιτρέπει αφ' ενός να κάνουμε log-in στο πορτοφόλι κι αφετέρου να παράγουμε την ψηφιακή υπογραφή μας. Η ψηφιακή ή κρυπτογραφική υπογραφή αποτελεί ένα μαθηματικό μηχανισμό που με την χρήση του ιδιωτικού κλειδιού επιτρέπει την απόδειξη της κυριότητας των bitcoin.

Τα πορτοφόλια χωρίζονται σε δύο κατηγορίες, τα hot και τα cold, ανάλογα με την πρόσβαση ή όχι που έχουν στο internet. Τα hot έχουν άμεση και πιθανόν συνεχή πρόσβαση ενώ τα cold είτε δεν έχουν καμία απολύτως πρόσβαση στο διαδίκτυο είτε μπορούν ενδεχομένως να συνδεθούν έμμεσα, κατ' επιλογή του χρήστη. Στην πρώτη κατηγορία περιλαμβάνονται ο ηλεκτρονικός υπολογιστής στον οποίο ο χρήστης μπορεί να τρέχει κάποιο λογισμικό, ένας ειδικός διαδικτυακός τόπος (dedicated wallet), το κινητό τηλέφωνο εφ' όσον έχει πρόσβαση στο διαδίκτυο και οι αγορές συναλλάγματος ή αλλιώς χρηματιστήρια. Οι ειδικοί διαδικτυακοί τόποι και τα χρηματιστήρια συγκεκριμένα, διατηρούν το 20% των κεφαλαίων τους σε hot wallets χάριν ρευστότητας.

Στην δεύτερη κατηγορία, τα cold wallets, συμπεριλαμβάνονται ο ηλεκτρονικός υπολογιστής εφ' όσον είτε δεν είναι συνδεδεμένος στο διαδίκτυο ή ο χρήστης έχει ένα κρυπτογραφημένο αρχείο πολυμέσων δηλαδή κρατάει το κλειδί κρυπτογράφησης offline, οπότε ακόμα κι εάν κάποιος έχει πρόσβαση στο ιδιωτικό κλειδί, δεν θα μπορεί να το αποκρυπτογραφήσει. Εν συνεχεία, μπορεί να είναι ένα usb stick ή ένας εξωτερικός σκληρός δίσκος, υλικά νομίσματα ή και χάρτινο πορτοφόλι. Όσον αφορά το χάρτινο πορτοφόλι, πρέπει να πούμε πως πρόκειται για ένα απλό κομμάτι χαρτί όπου υπάρχουν εκτυπωμένα το δημόσιο και το ιδιωτικό κλειδί, ακόμα και με την μορφή QR code, όπως φαίνεται στην παρακάτω εικόνα.


του. Παρομοίως, ως ***πελάτη*** μπορούμε να θεωρήσουμε είτε κάποιο λογισμικό που επικοινωνεί και υποβάλει αιτήματα στον εξυπηρετητή, είτε σε όλο τον υπολογιστή όταν ο εξυπηρετητής είναι άλλος υπολογιστής και οι 2 υπολογιστές είναι συνδεδεμένοι σε ένα δίκτυο." https://el.wikipedia.org/wiki/%CE%95%CE%BE%CF%85%CF%80%CE%B7%CF%81%CE%B5%CF%84%CE%B7%CF%84%CE%AE%CF%82

Αξίζει ακόμα να αναφέρουμε πως όταν γίνεται λόγος για υλικά νομίσματα, δεν πρέπει να τα μπερδεύουμε με τα συμβατικά νομίσματα. Τα ψηφιακά νομίσματα δεν έχουν υλική μορφή. Τα υλικά bitcoin είναι εξαιρετικά σπάνια και είναι δημιουργήματα κάποιων οργανισμών, οι οποίοι εκτυπώνοντας ένα ιδιωτικό κλειδί Bitcoin πάνω σε μάρκες, τις έχουν κάνει να είναι εξαργυρώσιμες προς bitcoin. Έτσι, θα πρέπει να αποβάλλουμε από το μυαλό μας εικόνες όπως η παρακάτω καθώς είναι ως επί το πλείστον παραπλανητικές.

Όπως είναι φυσικό, κάθε κατηγορία πορτοφολιών έχει πλεονεκτήματα και μειονεκτήματα. Στα πλεονεκτήματα της πρώτης κατηγορίας, τα hot wallets, εντοπίζουμε την εξ αποστάσεως πρόσβαση. Ο χρήστης μπορεί από οποιοδήποτε σημείο της γης να έχει πρόσβαση άμεσα στα bitcoin του. Στα μειονεκτήματα βρίσκουμε τους κινδύνους hack και απάτης. Ναι μεν το Bitcoin ως σύστημα είναι σε αρκετά μεγάλο βαθμό προστατευμένο από αυτά τα δύο αλλά το ίδιο δεν ισχύει για τα κλειδιά των χρηστών. Όσον αφορά τα cold wallets είναι πιο προστατευμένα από αυτές τις απειλές καθώς για να τους γίνει hacking, ο hacker θα πρέπει πρώτα να έχει πρόσβαση στο cold storage, που εάν πρόκειται για deep cold storage είναι ακόμα πιο δύσκολο καθώς αυτός ο όρος αναφέρεται στην αποθήκευση του cold sotrage εντός χρηματοκιβωτίου. Βέβαια, αυτού του είδους τα πορτοφόλια δεν παρέχουν τις ανέσεις της εξ αποστάσεως πρόσβασης ενώ ακόμα υπάρχει ο κίνδυνος να χαθούν ή να καταστραφούν. Επιπλέον, συγκεκριμένα ως προς το χάρτινο πορτοφόλι, αυτό έχει το μειονέκτημα να μπορεί να χρησιμοποιείται μονάχα μία φορά οπότε εάν ο χρήστης δεν ξοδέψει ολόκληρο το ποσό, θα πρέπει να καταθέσει το υπόλοιπο σε ένα νέο χάρτινο πορτοφόλι.

Έτσι λοιπόν συνιστάται στους χρήστες να ζυγίζουν τα αρνητικά και τα θετικά της κάθε κατηγορίας. Όταν επιλέγουν online wallets θα πρέπει να είναι εξαιρετικά προσεκτικοί καθώς έχουν συμβεί hacks κι έχουν παρατηρηθεί ζητήματα ασφαλείας. Θα πρέπει να διαβάζονται οι αξιολογήσεις των υπηρεσιών και να επιλέγεται η ασφαλέστερη. Ακόμα και η ασφαλέστερη όμως δεν θα είναι ποτέ 100% αδιάτρητη. Εάν επιλεγεί η οδός των cold wallets, πρέπει να τηρούνται αντίγραφα ασφαλείας έτσι ώστε σε περίπτωση απώλειας, καταστροφής ή αποτυχίας του συστήματος, να μην χαθούν τα bitcoin. Ο ασφαλέστερος τρόπος είναι να τηρούνται πολλά διαφορετικά πορτοφόλια για την ελαχιστοποίηση των ρίσκων και να γίνεται χρήση πορτοφολιών κι από τις δύο κατηγορίες, ένα hot wallet για να υπάρχει η απαραίτητη ρευστότητα κι ένα cold για την φύλαξη των υπολοίπων bitcoin. Μια χρήσιμη συμβουλή όσον αφορά τα cold wallets είναι να αποθηκεύονται ασφαλώς, αλλά να διατηρείται εύκολα προσβάσιμη η διεύθυνση, δηλαδή το δημόσιο κλειδί, ώστε να είναι δυνατή η αποδοχή bitcoin ακόμα κι εάν ο χρήστης δεν μπορεί να τα χρησιμοποιήσει. Τέλος, για τους προχωρημένους χρήστες, υπάρχει η επιλογή της πιστοποίησης δύο παραγόντων (two factor authentication) που αφορά ένα επιπλέον μέτρο ασφαλείας. Σε αυτήν την επιλογή, για να πιστοποιηθεί η ταυτότητα του χρήστη και για να υπάρχει η βεβαιότητα ότι αυτός που επιχειρεί να κάνει log-in είναι όντως ο νόμιμος δικαιούχος του πορτοφολιού, απαιτείται αφ' ενός ένας κωδικός που ήδη γνωρίζει ο χρήστης κι αφ' ετέρου ένας δεύτερος κωδικός που μπορεί π.χ. να αποσταλεί στον χρήστη μέσω ενός γραπτού μηνύματος στο κινητό του τηλέφωνο.[26]

## 2.4 Miners και Mining

Οι miners είναι ένα από τα βασικά κομμάτια του παζλ του Bitcoin χωρίς τους οποίους το σύστημα δεν θα λειτουργούσε. Δεν θεωρούνται άδικα οι ρυθμιστές του οικοσυστήματος αφού επιτελούν διπλό ρόλο καθώς αφ' ενός επεξεργάζονται και καταχωρούν τις συναλλαγές στο δημόσιο βιβλίο ισολογισμού κι αφ' ετέρου "εξορύσσουν" τα νέα νομίσματα που θα τεθούν σε κυκλοφορία.

Τα Bitcoin δεν εκτυπώνονται από κάποια Κεντρική Τράπεζα ή αρχή όπως τα παραδοσιακά χρήματα. Αντ' αυτού, εξορύσσονται μέσα από το σύστημα από τους miners με την χρήση ενός ηλεκτρονικού υπολογιστή που τρέχει ένα συγκεκριμένο πρόγραμμα. Όπως κάθε άλλος φυσικός πόρος, υπάρχει περιορισμένος αριθμός Bitcoin μονάδων, ενώ όπως ακριβώς συμβαίνει στον πραγματικό κόσμο σε ένα ορυχείο, πρέπει να ξοδευτεί ενέργεια για να εξαχθούν τα νομίσματα εξού και ο τίτλος των miners.

Συνοπτικά, μπορούμε να πούμε ότι ο ηλεκτρονικός υπολογιστής του miner καλείται να επιλύσει μία σειρά από σύνθετα μαθηματικά προβλήματα. Όταν επιτύχει, τα λοιπά nodes[27] επιβεβαιώνουν την ορθότητα της λύσης, το νέο block επικυρώνεται και στον miner πιστώνονται τα μόλις εξορυχθέντα νομίσματα ως αμοιβή.

[26] http://www.theguardian.com/technology/2013/oct/07/fbi-bitcoin-silk-road-ross-ulbricht

[27] Αποτελούν ενεργές ηλεκτρονικές συσκευές συνδεδεμένες στο δίκτυο και ικανές να δημιουργήσουν, να λάβουν ή/και να διαβιβάσουν πληροφορίες διαμέσου ενός διαύλου επικοινωνίας.

Η πραγματικότητα είναι λίγο πιο περίπλοκη. Όταν δημιουργείται ένα block[28] με συναλλαγές, οι miners το περνάνε από μία διαδικασία. Ανακτούν τις πληροφορίες που εμπεριέχονται σε αυτό και εφαρμόζοντάς τους μία μαθηματική φόρμουλα, τις μετατρέπουν σε κάτι το διαφορετικό. Τις μετατρέπουν σε μία κατά πολύ μικρότερη, φαινομενικά τυχαία, σειρά αριθμών και γραμμάτων, γνωστή ως hash.[29] Οι πληροφορίες αποτελούν το input και το hash το output. Το hash αυτό, με την σειρά του, αποθηκεύεται μαζί με το block στο -εκείνης της χρονικής στιγμής- τέλος της blockchain.

Καθώς το block μονάχα ενός miner μπορεί να μπει κάθε φορά στην blockchain, γίνεται ένας αγώνας δρόμου μεταξύ των miners για το ποιος θα παράξει πρώτος το hash. Ο ευκολότερος τρόπος να περιγράψουμε αυτόν τον αγώνα δρόμου είναι εάν τον παρομοιάσουμε με έναν γρίφο που δεν μπορεί να λυθεί βάσει λογικής όπως για παράδειγμα μία κλειδαριά με συνδυασμό. Για να εισαχθεί λοιπόν το block στην αλυσίδα, θα πρέπει να παραχθεί το hash του, δηλαδή κάποιος να μαντέψει τον κατάλληλο συνδυασμό. Όποιος τον μαντέψει πρώτος, παίρνει και την αμοιβή. Το hash πρέπει να παρουσιάζει κάθε φορά μία συγκεκριμένη μορφή που ορίζεται από το σύστημα. Μπορεί π.χ. να ζητείται ένας συγκεκριμένος αριθμός μηδενικών και συγκεκριμένος αριθμός συνολικών χαρακτήρων. Επειδή, όπως θα δούμε παρακάτω, η παραγωγή των block πρέπει να γίνεται ανά συγκεκριμένο χρονικό διάστημα, ο βαθμός δυσκολίας του γρίφου αναβαθμονομείται ανάλογα με την ταχύτητα λύσης ανά 2016 blocks προς την επιθυμητή κατεύθυνση.

Η προαναφερθείσα μαθηματική φόρμουλα της οποίας γίνεται χρήση για την εξόρυξη των bitcoin είναι συνήθως η επονομαζόμενη SHA-256[30], στης οποίας και το όνομα θα αρκεστούμε για τους σκοπούς αυτής της εργασίας. Όταν γίνεται αναφορά στο hash rate, αναφερόμαστε στην ουσία στην ταχύτητα με την οποία μαντεύονται οι συνδυασμοί. Αυτήν την στιγμή το παγκόσμιο hash rate κινείται γύρω από τις 4,5e+17 μαντεψιές ανά δευτερόλεπτο.[31]

Τα hash παρουσιάζουν μερικές ενδιαφέρουσες ιδιότητες. Η παραγωγή ενός hash από μία συλλογή δεδομένων όπως ένα Bitcoin block, θεωρείται σε γενικές γραμμές μία σχετικά απλή διαδικασία, αν εξαιρέσει κανείς το γεγονός της αύξησης της δυσκολίας από το ίδιο το σύστημα. Είναι όμως σχεδόν αδύνατο να καταλάβει κάποιος τί ή ποιά ήταν αυτά τα δεδομένα απλώς και μόνο κοιτώντας το hash. Ακόμα,

[28] Η κάθε καταγραφή στην blockchain. Περιλαμβάνει τις ανεπιβεβαίωτες συναλλαγές και τις καταχωρεί στην blockchain.

[29] Το hash παράγεται βάσει της συνάρτησης κατατεμαχισμού ή κατακερματισμού. Για περισσότερες πληροφορίες βλ. https://el.wikipedia.org/wiki/%CE%A3%CF%85%CE%BD%CE%AC%CF%81%CF%84%CE%B7%CF%83%CE%B7_%CE%BA%CE%B1%CF%84%CE%B1%CF%84%CE%B5%CE%BC%CE%B1%CF%87%CE%B9%CF%83%CE%BC%CE%BF%CF%8D

[30] Από τα αρχικά Secure Hash Algorithm. Για περισσότερες πληροφορίες σχετικά με το SHA-256 βλ. https://en.wikipedia.org/wiki/SHA-2

[31] Το παρόν hashrate κυμαίνεται στα 450,000,000 GH/s σύμφωνα με το https://blockchain.info/charts/hash-rate . Οι πολλαπλάσιες μονάδες του hash rate εμφανίζονται ως εξής:
1 kH/s = 1,000 (χίλια) hashes ανά δευτερόλεπτο.
1 MH/s = 1,000,000 (ένα εκατομμύριο) hashes ανά δευτερόλεπτο.
1 GH/s = 1,000,000,000 (ένα δισεκατομμύριο) hashes ανά δευτερόλεπτο.
1 TH/s = 1,000,000,000,000 (ένα τρισεκατομμύριο) hashes ανά δευτερόλεπτο.
1 PH/s = 1,000,000,000,000,000 (ένα τετράκις εκατομμύριο) hashes ανά δευτερόλεπτο.
1 EH/s = 1,000,000,000,000,000,000 (ένα πεντάκις εκατομμύριο) hashes ανά δευτερόλεπτο. http://bitcoin.stackexchange.com/questions/9219/what-is-the-difference-between-kh-s-mh-s-and-gh-s

παρότι είναι πολύ εύκολη η διαδικασία παραγωγή ενός hash από μία ικανή ποσότητα δεδομένων, το κάθε hash είναι μοναδικό. Συνεπώς, η αλλαγή ακόμα κι ενός συνθετικού χαρακτήρα, γράμματος ή αριθμού, σε ένα bitcoin block, θα διαφοροποιούσε το hash εντελώς.

Βέβαια, οι miners δεν χρησιμοποιούν μονάχα τις πληροφορίες των συναλλαγών ενός block για να παράγουν ένα hash, αλλά και μία σειρά από άλλα δεδομένα. Ένα από αυτά τα δεδομένα, που τους δίνει και την δυνατότητα να καταλήγουν στον κατάλληλο συνδυασμό για να παραχθεί το αναζητούμενο hash, μέσα από αμέτρητες διαφορετικές εναλλακτικές, είναι το αποκαλούμενο nonce. Το nonce αποτελείται από ένα τυχαίο κομμάτι τυχαίων δεδομένων. Είναι επίσης το μόνο κομμάτι που δύναται να αλλαχθεί κάθε φορά στο block έως ότου καταλήξουν στο hash που θα ταιριάζει στην απαιτούμενη μορφή. Εάν θα θέλαμε λοιπόν να συνδέσουμε το nonce με το παράδειγμα των συνδυασμών που αναφέρθηκε παραπάνω, το nonce θα ήταν οι χαρακτήρες της κλειδαριάς που θα άλλαζαν μέχρι να βρεθεί ο κατάλληλος συνδυασμός. Άλλο δεδομένο αποτελεί και το hash του αμέσως προηγούμενου block που υπάρχει στην blockchain. Έτσι, αφού το hash του κάθε block έχει παραχθεί χρησιμοποιώντας το hash του αμέσως προηγούμενου block, το hash αποτελεί στην ουσία το ψηφιακό αντίστοιχο μίας σφραγίδας ασφαλείας. Επιβεβαιώνει ότι τόσο αυτό, όσο και κάθε επόμενο block είναι γνήσιο καθώς και μέρος της ίδιας αλυσίδας. Εάν κάποιο αλλοιωνόταν, όλοι θα το γνώριζαν.

Στην περίπτωση που κάποιος θα προσπαθούσε να πλαστοποιήσει μία συναλλαγή αλλάζοντας ένα block που ήδη υπάρχει στην blockchain, θα άλλαζε το hash αυτού του block. Όταν μετά κάποιο άλλο άτομο θα ήλεγχε την γνησιότητα του εν λόγω block, εκτελώντας την hash function ή αλλιώς συνάρτηση κατακερματισμού σε αυτό, προσπαθώντας δηλαδή να επαναλάβει την διαδικασία παραγωγής του, θα ανακάλυπτε ότι το hash είναι διαφορετικό από αυτό που ήδη είναι αποθηκευμένο σε παλαιότερα blocks της αλυσίδας. Άρα, το αλλοιωμένο block θα αναγνωριζόταν αμέσως ως πλαστό. Επειδή το hash του κάθε block χρησιμοποιείται στην παραγωγή του επόμενου block στην αλυσίδα, η αλλοίωση κάποιου block θα καθιστούσε και τα μετέπειτα block λανθασμένα. Αυτό θα επηρέαζε ολόκληρη την πορεία της αλυσίδας.

Όλες οι συναλλαγές που διενεργούνται, μπαίνουν αυτόματα σε ένα pool ανεπιβεβαίωτων συναλλαγών. Όταν κάποιος miner ξεκινήσει την διαδικασία επίλυσης ενός hash, το πρώτο πράγμα που θα πρέπει να κάνει είναι να φτιάξει το block που προτείνει να είναι το επόμενο στην blockchain. Θα πρέπει λοιπόν να επιλέξει συναλλαγές οι οποίες θα συμπεριληφθούν στο block που ετοιμάζει. Η επιλογή μπορεί να είναι τυχαία. Ας υποθέσουμε πως παράλληλα με τον miner A, το ίδιο κάνει και ο miner B. Ας υποθέσουμε και πως καταφέρνουν να επιλύσουν ταυτόχρονα το hash του κάθε block τους. Τότε θα υπάρχουν δύο νέα block που ετοιμάστηκαν την ίδια στιγμή και άρα θα πρέπει να μπουν και τα δύο στην αλυσίδα. Καθώς αυτό δεν είναι δυνατό, θα δημιουργηθούν τότε δύο παρακλάδια της ίδιας αλυσίδας. Τα υπόλοιπα nodes θα επικυρώσουν την ορθότητα του πρώτου νέου block που θα λάβουν, και θα το δεχτούν ως τον τελευταίο κρίκο της αλυσίδας, ως το σημείο από το οποίο θα συνεχίσουν να την επιμηκύνουν. Η λύση στο πρόβλημα της

"ισοπαλίας", θα έρθει όταν λυθεί το επόμενο block. Τότε, σύμφωνα με τον γενικό κανόνα, τα nodes θα μεταπηδήσουν αυτόματα στην αλυσίδα που είναι μακρύτερη. Είναι πάντως σπάνιο να λύνονται ταυτόχρονα 2 block κι ακόμα σπανιότερο αυτό να συμβαίνει πολλαπλές φορές στην σειρά. Όταν όμως τυχαίνει, η blockchain σταθεροποιείται σχετικά σύντομα κι όλα τα nodes καταλήγουν να συμφωνούν ως προς την σειρά των block σε αυτήν.

Αυτό που μόλις περιγράψαμε όμως, επαναφέρει το πρόβλημα του double spending ή διπλοξοδέματος. Παρότι το Bitcoin είναι ένα σύστημα σχεδιασμένο για την αποφυγή αυτού του προβλήματος, επαληθεύοντας την κάθε συναλλαγή που προστίθεται στην blockchain για να εξασφαλίσει ότι τα ποσά που χαρακτηρίστηκαν ως inputs δεν είχαν προηγουμένως δαπανηθεί σε άλλη συναλλαγή, το πρόβλημα έχει πιθανότητες να προκύψει. Εάν ο κακόβουλος χρήστης Α κάνει δύο συναλλαγές, την ~Χ~ όπου αποστέλλει bitcoin στον χρήστη Β βάσει κάποιας συμφωνίας κι έπειτα την ~Υ~ όπου αποστέλλει τα ίδια bitcoin, χρησιμοποιώντας δηλαδή τα ίδια inputs, σε κάποια άλλη διεύθυνση, και οι δύο συναλλαγές θα βρεθούν στο pool των ανεπιβεβαίωτων συναλλαγών. Τώρα, υπάρχουν δύο περιπτώσεις. Στην πρώτη, η συναλλαγή ~Υ~ καταλήγει πριν από την ~Χ~ στο block που μπαίνει στην αλυσίδα κι έτσι όταν φτάνει η σειρά της ~Χ~, τα nodes την απορρίπτουν καθώς τα inputs της έχουν ήδη χρησιμοποιηθεί σε συναλλαγή προηγούμενου block και συνεπώς είναι άκυρη. Στην δεύτερη περίπτωση, η συναλλαγή ~Χ~ μπαίνει όντως πρώτη σε block της blockchain αλλά ο χρήστης Α καταφέρνει να παράγει ένα εναλλακτικό παρακλάδι της blockchain[32] που θα πρέπει να είναι και μακροσκελέστερο του άλλου, κι έτσι, όπως αναφέραμε παραπάνω, τα nodes θα μεταπηδήσουν στην αλυσίδα με τα περισσότερα blocks. Έτσι, η συναλλαγή ~Χ~ θα βρεθεί εκ νέου στο pool των ανεπιβεβαίωτων συναλλαγών και θα απορριφθεί και πάλι χαρακτηριζόμενη άκυρη.

Οι συνέπειες των περισσότερων ειδών των double spend επιθέσεων, μπορούν να αποφευχθούν με την απλή αναμονή επιβεβαίωσης, δηλαδή παραγωγής κάποιων block πριν να θεωρηθεί από τους χρήστες ότι η συναλλαγή τους όντως πραγματοποιήθηκε. Όσο πιο πίσω στην blockchain βρίσκεται η συναλλαγή τους, τόσο πιο ασφαλής είναι καθώς ο επιτιθέμενος χρήστης θα έπρεπε να ξεπερνάει είτε σε ταχύτητα είτε σε τύχη ολόκληρο το δίκτυο για μεγαλύτερο χρονικό διάστημα. Μην ξεχνάμε ότι η λύση του hash για παραγωγή των blocks είναι ένας αγώνας δρόμου κι ο επιτιθέμενος θα ανταγωνίζεται ολόκληρο το δίκτυο.

Τα πράγματα αλλάζουν όταν πρόκειται για ">50% επίθεση" ή "51% επίθεση" γνωστή και ως "επίθεση της πλειοψηφίας". Σε αυτήν την περίπτωση, ο επιτιθέμενος ελέγχει παραπάνω από το ήμισυ του hashrate του δικτύου και γι' αυτό θεωρείται πως η επίθεσή του έχει πιθανότητα 100% να επιτύχει. Κι αυτό διότι, δεδομένου του ότι ο επιτιθέμενος δύναται να παράγει blocks γρηγορότερα απ' ότι το υπόλοιπο δίκτυο, μπορεί απλά να επιμείνει στο δικό του παρακλάδι της αλυσίδας έως ότου αυτό γίνει μακροσκελέστερο από αυτό που παράγεται από το έντιμο, καλόβουλο δίκτυο. Κανένας αριθμός επιβεβαιώσεων (αναμονής block) δεν μπορεί να αποτρέψει αυτήν την επίθεση. Ωστόσο, η αναμονή επιβεβαίωσης αυξάνει αθροιστικά το

[32] Το παρακλάδι της αλυσίδας δεν είναι δυνατόν να παραχθεί εκ προοιμίου.

κόστος των πόρων απαραίτητων για την εξαπόλυση της επιθέσεως κι έτσι μπορεί να την καταστήσει ασύμφορη ή να την καθυστερήσει αρκετά έως ότου αλλάξουν οι συνθήκες ή οι μέθοδοι συγχρονισμού βραδύτερης δράσεως να καταφέρουν να τεθούν σε λειτουργία. Πάντως, εάν κάποιος έχει τον έλεγχο άνω του 50% του hashrate στο συνολικό δίκτυο, αφ' ενός μεν τα οφέλη από τις αμοιβές του mining μπορούν ενδεχομένως να ξεπεράσουν τα οφέλη κάποιας μικρού σκέλους double spend επίθεσης κι αφ' ετέρου, το σύστημα μάλλον θα κατέρρεε υπό τον φόβο υπερσυγκέντρωσης ελέγχου, όπως παραλίγο να συμβεί τον Ιούνιο του 2014 όταν ένα mining pool λίγο έλλειψε να αγγίξει αυτό το όριο πριν κάποιοι από τους miners να αναζητήσουν εναλλακτικά pools.[33],[34]

Θεωρητικά ο οποιοσδήποτε θα μπορούσε να κάνει mining από το σπίτι του με τον απλό προσωπικό του υπολογιστή όμως το πλήθος των miners ανά την υφήλιο καθώς και η πρόοδος της τεχνολογίας έχουν σχεδόν εκμηδενίσει τις πιθανότητες επιτυχίας με αυτού του είδους το mining. Γι' αυτό πολλοί επιλέγουν να συμμετάσχουν σε mining pools. Ως mining pools εννοούμε ουσιαστικά ομάδες στις οποίες συμμετέχει ένας αριθμός από miners που εργάζονται συλλογικά για την παραγωγή block και μοιράζονται τις αμοιβές. Θα μπορούσαμε να παρομοιάσουμε αυτές τις ομάδες σαν μία ομάδα ανθρώπων οι οποίοι για να αυξήσουν τις πιθανότητες τους να κερδίσουν το λαχείο, συνεργάζονται με άλλους ανθρώπους για την αγορά πολλών λαχείων μοιραζόμενοι το κόστος. Έτσι, όσοι συμμετέχουν σε mining pools αντί να εργάζονται μόνοι τους, αυξάνουν τις πιθανότητες λύσης κάποιου block αλλά μοιράζονται την αμοιβή που αυτό προσφέρει. Ο τρόπος διαμοιρασμού των αμοιβών διαφέρει από pool σε pool αλλά συνήθως συνδέεται με τα shares, την συνεισφορά δηλαδή του καθενός στην λειτουργία της ομάδας και στην λύση των block. Η συμμετοχή σε μία τέτοια ομάδα, μπορεί να δημιουργήσει ένα σταθερό εισόδημα παρότι αυτό θα είναι κατά πολύ μικρότερο σε σχέση με την πλήρη ανταμοιβή που παρέχει το κάθε block.

Η εξέλιξη του mining από την χρήση απλών ηλεκτρονικών υπολογιστών, από χρήση επεξεργαστών (CPU) σε χρήση καρτών γραφικών (GPU), σε κυκλώματα ειδικής κατασκευής με χρήση τεχνολογίας FPGA (Field Programmable Gate Array) και σήμερα σε κυκλώματα ASIC (Application Specific Integrated Circuits)[35], έχει μεν αυξήσει κατακόρυφα την αποδοτικότητα των μηχανημάτων ειδικά σε σχέση με την κατανάλωση ρεύματος αλλά έχει αυξήσει και το κόστος αγοράς τους. Αυτός είναι κι ο λόγος που οι περισσότεροι χρήστες συμμετέχουν σε τέτοιες ομάδες. Η επένδυση σε κατάλληλα για mining μηχανήματα για να λειτουργήσει κάποιος αυτόνομα εκτός πλαισίου κάποιου mining pool μαζί με το κόστος λειτουργίας και ψύξης των μηχανημάτων έχει γίνει ασύμφορη ειδικά εάν αναλογιστούμε τις μικρές πιθανότητες που έχει να λύσει κάποιος ένα block μόνος του. Ρόλο παίζει φυσικά και η ισοτιμία στην οποία κυμαίνεται το bitcoin,

[33] http://www.economist.com/news/business/21638124-minting-digital-currency-has-become-big-ruthlessly-competitive-business-magic?fsrc=scn/fb/te/pe/ed/magicofmining και http://www.coindesk.com/bitcoin-miners-ditch-ghash-io-pool-51-attack/ Παρούσα διανομή hashrate: https://blockchain.info/pools

[34] Για περισσότερες πληροφορίες για το πρόβλημα του doublespending βλ. https://en.bitcoin.it/wiki/Double-spending

[35] Για περισσότερες πληροφορίες σχετικά με τα τεχνολογικής φύσεως αναφερόμενα βλ. http://www.pcsteps.gr/13927-bitcoin-mining/

καθώς πρόκειται για μία ευμετάβλητη αγορά, κι έτσι συνιστάται ιδιαίτερη προσοχή στους δυνητικούς επενδυτές.

Μία ακόμα πτυχή του mining που φαίνεται να διαφεύγει της προσοχής αρκετών είναι αυτή του περιβαλλοντικού κόστους. Όπως αναφέραμε, όπως ακριβώς συμβαίνει στον πραγματικό κόσμο σε ένα ορυχείο, έτσι και στο Bitcoin πρέπει να ξοδευτεί ενέργεια για να εξορυχθούν τα νομίσματα. Μπορεί μεν να έχει αυξηθεί κατακόρυφα η αποδοτικότητα των μηχανημάτων που κάνουν χρήση της νέας τεχνολογίας, παρ' όλα αυτά η κατανάλωση ενέργειας για την λειτουργία αλλά πολύ σημαντικότερα για την ψύξη των μηχανημάτων παραμένει σε σημαντικά επίπεδα. Ακόμα κι εάν η ενέργεια προέρχεται από ανανεώσιμες πηγές κι εάν γίνεται χρήση σύγχρονων εγκαταστάσεων σε εκ φύσεως ψυχρά κλίματα για την μείωση αναγκών ψύξης, η ποσότητα κατανάλωσης ρεύματος δεν είναι αμελητέα.[36] Φυσικά αυτό είναι ένα πρόβλημα που δεν αφορά μόνο το mining αλλά όλους εμάς, την τεχνολογική και ιδιαίτερα την διαδικτυακή κοινότητα, είτε από πλευράς ιδιωτών είτε από πλευράς επιχειρήσεων καθώς η ολοένα αυξανόμενη χρήση των ηλεκτρονικών μέσων στην καθημερινή μας ζωή αντικατοπτρίζεται από εξίσου αυξημένες ενεργειακές ανάγκες.

## 2.5 Το όριο.

Το Bitcoin έχει ένα εγγενές αποπληθωριστικό χαρακτηριστικό. Σύμφωνα με το πρωτόκολλό του, ο μέγιστος αριθμός νομισμάτων που μπορούν να "εξορυχθούν" είναι 21,000,000 μονάδες. Αυτό σημαίνει πως ο μέγιστος αριθμός bitcoin νομισμάτων που μπορεί να κυκλοφορήσει δεν δύναται να ξεπερνάει αυτό το όριο ούτε κατά ένα bit[37]. Όπως ακριβώς ένα ορυχείο πολύτιμων μετάλλων έχει συγκεκριμένη ποσότητα μεταλλεύματος που μπορεί να εξορυχθεί, έτσι λοιπόν και το Bitcoin έχει συγκεκριμένο αριθμό νομισμάτων που μπορούν να κυκλοφορήσουν. Η εξόρυξη των νομισμάτων από το σύστημα είναι σαν την εξόρυξη πολύτιμων μετάλλων από κάποιο μαθηματικό ορυχείο. Όπως κι ένα απλό ορυχείο έχει μια μέγιστη περιεκτικότητα μεταλλεύματος, έτσι και το ηλεκτρονικό μαθηματικό ορυχείο του Bitcoin έχει έναν μέγιστο αριθμό κρυπτονομισμάτων. Γίνεται, λοιπόν, αναπόφευκτο κάποια στιγμή να εξορυχθούν όλα τα νομίσματα. Συνεπακολούθως, αναπόφευκτη γίνεται και η έκλειψη της ανταποδοτικότητας που παρέχει αυτήν την στιγμή το σύστημα στους miners, με την πληρωμή τους σε νέα bitcoin για την εργασία τους. Γι' αυτόν τον λόγο, μελλοντικά υπάρχει η ελπίδα και προσδοκάται τα τέλη των συναλλαγών να παίζουν μεγαλύτερο ρόλο, ώστε οι miners να συνεχίσουν να έχουν κίνητρο να επιτελούν τον ρυθμιστικό ρόλο που έχουν στο σύστημα του κρυπτονομίσματος. Ενώ τώρα οι συναλλαγές που περιέχονται στα block επιλέγονται τυχαία, μελλοντικά οι συναλλαγές που δεν συμπεριλαμβάνουν κάποιο τέλος, θα αφήνονται εκτός. Εικάζεται λοιπόν, ότι ο όγκος

[36] http://www.economist.com/news/business/21638124-minting-digital-currency-has-become-big-ruthlessly-competitive-business-magic?fsrc=scn/fb/te/pe/ed/magicofmining
[37] Αποτελεί υποδιαίρεση του bitcoin. Το 1 bitcoin ισούται με 1,000,000 bit

των συναλλαγών θα είναι αρκετά υψηλός, ώστε όταν οι αμοιβές προερχόμενες από τα τέλη συναλλαγών αθροίζονται, να επαρκούν ώστε να μπορούν να επισκιάσουν οποιαδήποτε ανταμοιβή εξόρυξης.

Οι απόψεις βέβαια ως προς την ημέρα της κρίσης, διίστανται. Σύμφωνα με τον ρυθμό εξόρυξης η ημέρα που θα εξορυχθεί το τελευταίο Bitcoin θα είναι το έτος 2140. Κάποιοι θεωρούν όμως πως δεν θα περιμένουμε μέχρι να εξορυχθούν όλα τα αποθέματα αλλά αντ' αυτού η ημέρα αυτή θα έρθει συντομότερα. Όπως και να έχει στις παραμέτρους υπολογισμού θα πρέπει σίγουρα να συμπεριληφθούν η πρόοδος στην τεχνολογία και η δημοτικότητα του νομίσματος.

Στο σύστημα του εν λόγω κρυπτονομίσματος, η αμοιβή των miners μειώνεται με τον χρόνο. Για κάθε 210.000 νέα block που παράγονται, η αμοιβή μειώνεται κατά το ήμισυ. Τον Ιανουάριο του 2009 η αμοιβή παραγωγής των miners βρισκόταν στα 50 bitcoin ανά block. Η τρέχουσα αμοιβή βρίσκεται στα 25 BTC[38] ενώ προβλέπεται πως το ποσό αυτό θα μειωθεί στα 12,5 BTC κάποια στιγμή προς το τέλος του επόμενου έτους. Για να παραχθούν 210.000 block υπολογίζεται ότι απαιτούνται περίπου 4 χρόνια καθώς θεωρείται πως το ιδανικό χρονικό διάστημα παραγωγής 2016 blocks είναι οι 14 ημέρες. Προς αυτό, κάθε φορά που παράγονται 2016 blocks, υπολογίζεται ο χρόνος που χρειάστηκε κι αναλόγως αναβαθμονομείται η δυσκολία επίλυσης των hash. Εάν χρειάστηκαν πάνω από δύο βδομάδες, η επίλυση γίνεται ευκολότερη ενώ εάν η λύση προέκυψε συντομότερα, ο βαθμός δυσκολίας αυξάνεται. Σε γενικές γραμμές πάντως, το σύνηθες είναι να παράγεται ένα καινούργιο block στην blockchain κάθε δέκα λεπτά, 6 κάθε ώρα, 144 κάθε ημέρα, κ.ο.κ...[39]

Κάθε block περιέχει ακριβώς μία coinbase συναλλαγή, δηλαδή μία συναλλαγή που ενώ δεν έχει πραγματικά inputs, αποτυπώνει outputs που δεν είναι άλλα από την αμοιβή εξόρυξης σε νέα νομίσματα. Με την αμοιβή σε καινούργια bitcoin να βρίσκεται στα 25 BTC και την δημιουργία ενός block ανά δέκα λεπτά, μπορούμε να υπολογίσουμε πως κάθε έτος επιτρέπεται να δημιουργηθούν περίπου 1,314,900 νέα νομίσματα αφού 25 bitcoins * 6 blocks/ώρα * 24 ώρες/ημέρα * 365,25 ημέρες/έτος = 1,314,900 BTC. Αφού όπως αναφέραμε, κάθε 210,000 blocks η εν λόγω αμοιβή μειώνεται κατά το ήμισυ, σύντομα θα παράγονται 657,450 νέα bitcoin κάθε χρόνο, μετά από 4 χρόνια και για 4 χρόνια 328,725, έπειτα 164,362.5 κ.ο.κ έως ότου, καθώς υπάρχει ο περιορισμός των 8 δεκαδικών ψηφίων, το ποσό πέσει στο 0.00000001. Τέσσερα χρόνια μετά από αυτήν την στιγμή, τα νομίσματα θα έχουν εξαντληθεί.[40]

Λόγω αυτού, σημαντικό είναι να καταλάβουμε ότι εφ' όσον η αμοιβή μειώνεται κατά το ήμισυ ανά τέσσερα περίπου έτη, από ένα σημείο κι έπειτα, το ποσό της αμοιβής θα είναι απειροελάχιστο. Αυτός είναι και ο λόγος που θα χρειαστούν τόσα χρόνια ώστε να εξαντληθούν τα αποθέματα. Όμως, η επισκίαση της αμοιβής από τα τέλη συναλλαγών είναι κάτι που θα πρέπει να συμβεί πριν από εκείνο το σημείο και σίγουρα πολύ νωρίτερα από την εξάντληση των αποθεμάτων, καθώς η παραγωγή των block δεν μπορεί να παύσει όσο

[38] **BTC**: συντομογραφία της λογιστικής μονάδας του bitcoin.
[39] https://www.youtube.com/watch?v=Y-w7SnQWwVA&list=PL7gCWi6YZxUNzChLFZipomPfAUudj4cVy
[40] How many bitcoins are mined per day?, Bitcoin Forum, 17/12/2013, https://bitcointalk.org/index.php?topic=373844.0

συνεχίζουν να γίνονται συναλλαγές. Η εργασία που επιτελούν οι miners είναι απαραίτητη προκειμένου να συνεχίσουν να επικυρώνονται οι συναλλαγές και τόσο αρκετά χρόνια πριν όσο και μετά την εξάντληση των τελευταίων νομισμάτων, η αμοιβή εξόρυξης σε νέα νομίσματα θα αποτελείται από μερικά μόνο Satoshis[41]. Εξαρτώμενη βεβαίως από την πορεία της αξίας του εν λόγω κρυπτονομίσματος, η χρηματοδότηση από τα τέλη συναλλαγής θα πρέπει όμως να καλύπτει τουλάχιστον τα λειτουργικά έξοδα. Υπενθυμίζουμε πως για την εξόρυξη, απαραίτητος είναι ένας ισχυρός ηλεκτρονικός υπολογιστής με όσα παρελκόμενα χρειάζεται αυτός για να λειτουργήσει.

## 2.6 Χαμένα Νομίσματα.

Ένα από τα προβλήματα που θα επηρεάσουν στο μέλλον το Bitcoin, ειδικά όταν στερεύσουν τα αποθέματα νέων νομισμάτων, είναι τα "χαμένα νομίσματα"[42]. Πρόκειται για νομίσματα στα οποία δεν έχει πλέον κανείς πρόσβαση. Η απώλεια πρόσβασης μπορεί να οφείλεται σε μία σειρά από αιτίες, όπως οι αμετάκλητοι και πλέον ξεχασμένοι κωδικοί πρόσβασης, ξεχασμένα ηλεκτρονικά πορτοφόλια από τις αρχές του νομίσματος όταν ακόμα αυτό είχε μικρή αξία, βλάβες του hardware ή ακόμα και θάνατο του κατόχου. Ακόμα, υπάρχει και η πιθανότητα της "καύσης" των bitcoin που μπορεί να γίνει απλά στήνοντας ένα ηλεκτρονικό πορτοφόλι χωρίς να είναι γνωστό το ιδιωτικό κλειδί του. Έτσι, αυτό παραμένει ορατό διαδικτυακά, μαζί με κάθε συναλλαγή, αλλά το περιεχόμενό του είναι πολύ πιθανό να μην μπορεί να ανακτηθεί ποτέ. Παράδειγμα τέτοιου είδους αποτελεί το πορτοφόλι "Bitcoin Eater" που δημιουργήθηκε χωρίς καμία λογική ή τουλάχιστον φανερή αιτία και στο οποίο μπορεί ο οποιοσδήποτε να αποστείλει τα ψηφιακά νομίσματα. Είναι εξαιρετικά απίθανο και πρακτικά αδύνατο όμως να ανακτηθούν τα χαμένα νομίσματα, λόγω των παραμέτρων ασφαλείας που ενυπάρχουν στο πρωτόκολλο του κρυπτονομίσματος.

Ένα ακόμα ενδιαφέρον σημείο αποτελεί το γεγονός ότι ο δημιουργός ή η ομάδα δημιουργών, "Satoshi Nakamoto", κατέχει πάνω από 1 εκατομμύριο νομίσματα που εξορύχθηκαν κατά τα πρώτα χρόνια δημιουργίας του Bitcoin.[43] Τα νομίσματα αυτά ουδέποτε έχουν ξοδευτεί ή μετακινηθεί και παραμένει αδιευκρίνιστος ο σκοπός που εξυπηρετούν κι εάν η παραγωγή και η αχρηστία στην οποία έχουν υποπέσει γίνεται εσκεμμένα ή όχι. Πάντως, μετά από τόσα χρόνια αδράνειας μπορεί σχετικά ασφαλώς να υποτεθεί ότι πρόκειται για χαμένα νομίσματα.

Όσον αφορά το βαθμό στον οποίο επηρεάζουν τα χαμένα νομίσματα το σύστημα του Bitcoin, θα μπορούσαμε να πούμε ότι είναι ουσιαστικά αμελητέος. Προφανώς τα άτομα που χάνουν τα νομίσματά τους επηρεάζονται αρνητικώς αλλά για την υπόλοιπη κοινότητα θεωρητικά θα μπορούσε να λειτουργήσει θετικά. Κι αυτό διότι δεδομένης της αναπόφευκτης εξάντλησης των αποθεμάτων και έτσι την τελμάτωση της

[41] Η μικρότερη δυνατή λογιστική μονάδα. Ισούται με 0.00000001 BTC.
[42] http://www.coinbuzz.com/2015/03/31/23-bitcoins-mined-13-may-lost/
[43] Lerner Sergio Demian, The well deserved fortune of Satoshi Nakamoto, Bitcoin creator, visionary and genius, Bitsblog, 17/04/2013, https://bitslog.wordpress.com/2013/04/17/the-well-deserved-fortune-of-satoshi-nakamoto/

προσφοράς του νομίσματος, θα μπορούσε αυτό να οδηγήσει σε άνοδο της τιμής τους. Πάντως, καθώς η αξία των νομισμάτων έχει αυξηθεί θεαματικά σε σχέση με τον πρώτο καιρό δημιουργίας του, η αμελής μεταχείριση από τους κατόχους έχει ελαττωθεί. Αναπόδραστα όμως, νομίσματα σίγουρα θα συνεχίσουν να χάνονται αν και όχι στον ίδιο βαθμό και στην ίδια ποσότητα.

## 2.7 Διαιρετότητα.

Ίσως ένα από τα σημαντικότερα χαρακτηριστικά του συγκεκριμένου νομίσματος είναι η διαιρετότητά του. Το σύστημα επιτρέπει κλασματικά κέρματα με την μικρότερη δυνατή μονάδα σε Bitcoin να είναι 0,00000001, ή αλλιώς γνωστό και ως ένα Satoshi. Η υποδιαίρεση αυτή, που αποτελεί ένα εκατοστό εκατομμυριοστό ενός bitcoin, ονομάστηκε έτσι συλλογικά από την κοινότητα ως φόρος τιμής στον δημιουργό ή την ομάδα δημιουργών του κρυπτονομίσματος. Όλα τα ποσά της blockchain είναι εκφρασμένα σε Satoshi πριν μετατραπούν για την ευκολότερη ανάγνωσή τους κατά της προβολή τους στην οθόνη. Ο πηγαίος κώδικας χρησιμοποιεί επίσης Satoshi όταν ορίζεται ένα ποσό Bitcoin. Τέλος, κατά την προβολή μιας εξαιρετικά μικρής υποδιαίρεσης, όπως ισχύει για σύγχρονα faucets[44], το ποσό εμφανίζεται σε Satoshi για να διευκολύνεται η αναγνωσιμότητα.

Δεν αποκλείεται σε μελλοντικές εκδόσεις του πρωτοκόλλου να εισαχθούν υποδιαιρέσεις μικρότερες του ενός Satoshi, εφ' όσον κριθεί απαραίτητο από την κοινότητα. Αν και το σενάριο να παρουσιαστεί η αναγκαιότητα για δόμηση στήριξης μικρότερων υποδιαιρέσεων στην βάση κώδικα του Bitcoin κρίνεται μάλλον απίθανο, εάν υπήρχε έκρηξη του όγκου συναλλαγών και το κρυπτονόμισμα υιοθετείτο για μικροσυναλλαγές, με παράλληλη επαρκή άνοδο στην αξία του, τότε φυσικά θα προέκυπτε η ανάγκη μεγαλύτερης διαιρετότητάς του.

Αναλυτικότερα[45], ακόμα κι εάν η αξία του Bitcoin έφτανε μελλοντικά το 1.000.000 δολάρια, τότε το 1 Satoshi θα ήταν ίσο με 1 cent δολαρίου (0,01$) καθώς σε κάθε bitcoin αντιστοιχούν 100.000.000 Satoshis. Έτσι, το Satoshi θα εξακολουθούσε να αντιπροσωπεύει ένα ελάχιστο μικροποσό που δεν θα ξεπερνούσε τα 0,01 δολάρια. Η ανάγκη περαιτέρω διαιρετότητάς του σε υπομονάδες μικρότερης αξίας από το 1 Satoshi, θα προέκυπτε από το γεγονός ότι αυτό θα ήταν και το μικρότερο δυνατό τέλος συναλλαγών το οποίο θα μπορούσε κάποιος να αποδώσει. Έτσι, θα γινόταν απαγορευτικά ακριβό για οποιαδήποτε επιχείρηση βασίζεται σε μικροπληρωμές, όπως βασιζόμενα σε Bitcoins paywalls[46] περιεχομένου, άμεσες πληρωμές κινήσεως διαδικτύου σε Παρόχους Υπηρεσιών Διαδικτύου (ISPs), ή άλλα συστήματα λειτουργούντα με

[44] Πρόκειται για ιστοσελίδες που δίνουν "δωρεάν" bitcoins ως αντάλλαγμα για μία απλή διαδικασία/εργασία όπως το κλικάρισμα μίας διαφήμισης, η επίλυση μίας CAPTCHA ή ακόμα και την προβολή μίας ιστοσελίδας για ένα ορισμένο χρονικό διάστημα. Τα ποσά συνήθως είναι εξαιρετικά μικρά και το μέγεθός τους κυμαίνεται ανάλογα με την τρέχουσα αξία του Bitcoin. https://en.wikipedia.org/wiki/Bitcoin_faucet

[45] http://bitcoin.stackexchange.com/questions/122/will-we-ever-need-smaller-amounts-of-bitcoin-than-a-satoshi

[46] Το paywall είναι ένα σύστημα που απαγορεύει στους χρήστες του διαδικτύου την πρόσβαση στο περιεχόμενο μιας ιστοσελίδας χωρίς πληρωμένη συνδρομή. https://en.wikipedia.org/wiki/Paywall

αυτοματοποιημένες μικροπληρωμές. Λόγου χάρη, η πληρωμή 0,05 $ για την πρόσβαση σε κάποιο άρθρο θα σήμαινε ένα τέλος συναλλαγής ίσο με το 20% της αξίας της ίδιας της συναλλαγής.

Φυσικά οι υπηρεσίες αυτές θα μπορούσαν να κινηθούν εκτός του πλαισίου του blockchain, όπου θα υπήρχε η δυνατότητα να προστίθετο μεγαλύτερη ακρίβεια. Όμως, οι χρήστες θα έπρεπε να δημιουργούν νέους λογαριασμούς για κάθε μία από αυτές τις υπηρεσίες και να δεσμεύουν πόρους άνευ λόγου ενώ παράλληλα θα επανεμφανιζόταν ο κίνδυνος αντισυμβαλλομένου (thirdparty/counterparty), κάτι που ουσιαστικά θα αντέστρεφε κάποια από τα βασικά σημεία προώθησης του Bitcoin.

Ακολουθεί πίνακας πολλαπλασίων και υποδιαιρέσεων του Bitcoin:[47]

| Unit | Abbreviation | Decimal (BTC) | Alternate names | Info |
|---|---|---|---|---|
| Algorithmic maximum | | 20,999,999.9769 | | Calculation |
| tam-bitcoin | | 2,814,749.76710656 | | 1,0000,0000 tonal |
| mega-bitcoin | MBTC | 1,000,000 | | Rare in context |
| kilo-bitcoin | kBTC | 1,000 | | Rare in context |
| hecto-bitcoin | hBTC | 100 | | Rare |
| Initial block subsidy | | 50 | | Until block 210000 |
| bong-bitcoin | $^{b}$TBC | 4.294.967.296 | | 1,0000 tonal |
| Current block subsidy | | 25 | block | As of block 210000 |
| deca-bitcoin | daBTC | 10 | | Rare |
| mill-bitcoin | $^{m}$TBC | 268.435.456 | | 1000 tonal |
| bitcoin | BTC | 1 | coin | SI base unit |
| san-bitcoin | $^{s}$TBC | 0.16777216 | | 100 tonal |
| deci-bitcoin | dBTC | 0.1 | | Rare |
| ton-bitcoin | $^{t}$TBC | 0.01048576 | | 10 tonal |
| centi-bitcoin | cBTC | 0.01 | bitcent | Formerly frequent |

[47] https://en.bitcoin.it/wiki/Units

| | | | | |
|---|---|---|---|---|
| milli-bitcoin | mBTC | 0.001 | millibit, millie | Occasional |
| bitcoin | TBC | 0.00065536 | | Tonal base unit |
| bitcoin-ton | $TBC^{t}$ | 0.00004096 | | 0.1 tonal |
| bitcoin-san | $TBC^{s}$ | 0.00000256 | | 0.01 tonal |
| micro-bitcoin | μBTC | 0.000001 | bit | Frequent |
| bitcoin-mill | $TBC^{m}$ | 0.00000016 | | 0.001 tonal |
| | | 0.0000001 | finney | |
| bitcoin-bong | $TBC^{b}$ | 0.00000001 | | 0.0001 tonal |
| | sat. | 0.00000001 | satoshi | Blockchain value |

## 2.8 Altcoins

Τα Altcoins, που είναι συντομογραφία για το alternative coins, είναι κι αυτά κρυπτονομίσματα. Όπως δηλώνει και το όνομά τους, αποτελούν εναλλακτικά του Bitcoin νομίσματα και για αυτόν τον λόγο, με τον όρο Altcoin, περιγράφουμε κάθε κρυπτονόμισμα που δεν είναι το Bitcoin. Καθότι το πρωτόκολλο, ο κώδικας του Bitcoin είναι εξολοκλήρου διαθέσιμος στο κοινό, τα Altcoins δημιουργούνται βάσει αυτού του κώδικα. Τα περισσότερα εξ αυτών δεν είναι παρά ελαφρώς βελτιωμένοι κλώνοι του Bitcoin, παρουσιάζοντας αμελητέες διαφοροποιήσεις, αλλάζοντας μόνο ήσσονος σημασίας χαρακτηριστικά όπως την ταχύτητα των συναλλαγών, την μέθοδο διανομής ή τον hashing αλγόριθμο. Η πλειοψηφία από τα Altcoins ευελπιστεί να μιμηθεί την επιτυχία του πρωτόπλαστου Bitcoin και, τουλάχιστον σε έναν βαθμό, είτε να το αντικαταστήσει είτε να βελτιώσει κάποιο από τα χαρακτηριστικά του. Κάποια, επιχειρούν επίσης να αντιμετωπίσουν διαφαινόμενες αδυναμίες του πρωτότυπου και να παράσχουν ανταγωνιστικά πλεονεκτήματα. Υπάρχουν 612[48] Altcoins και περισσότερα εμφανίζονται κάθε ημέρα. Λίγα, όμως, καταφέρνουν να επιβιώσουν.

Παρότι τα Altcoins δεν αναγνωρίζονται από πολλούς ως το κάτι χρήσιμο, επιτελούν σημαντικό ρόλο. Γενικά, συνεισφέρουν στην περαιτέρω αποκέντρωση της κρυπτονομισματικής κοινότητας, που είναι κι ένας από τους σημαντικότερους στόχους του Bitcoin. Επιπλέον, μερικά από αυτά καινοτομούν δοκιμάζοντας χρήσιμες λειτουργίες τις οποίες δεν προσφέρει το Bitcoin κι επιτρέπουν στους προγραμματιστές να

[48] Στις 4/11/2015, σύμφωνα με το CoinMarketCap (http://coinmarketcap.com/currencies/views/all/).

πειραματίζονται με μοναδικά χαρακτηριστικά. Αν και τα χαρακτηριστικά αυτά μπορούν εύκολα να αντιγραφούν από το Bitcoin σε περίπτωση που υπάρξει αυτή η επιθυμία από τους προγραμματιστές ή την κοινότητά του, ένα πλήρως λειτουργικό Altcoin αποτελεί προσφορότερο κρυπτονομισματικό εργαστήριο από το σύστημα του ίδιου του Bitcoin. Τέλος, τα Altcoins παρέχουν στο Bitcoin, υγιή ανταγωνισμό. Αποτελούν εναλλακτικές επιλογές στους χρήστες κρυπτονομισμάτων και αναγκάζουν τους προγραμματιστές του Bitcoin να παραμένουν ενεργοί και να συνεχίσουν να καινοτομούν και να βελτιώνουν το σύστημά τους. Στην περίπτωση που οι ψηφιακές επιθυμίες των χρηστών δεν ικανοποιούνται πλέον από το Bitcoin, μπορούν να το εγκαταλείψουν εις υιοθέτισην ενός εναλλακτικού κρυπτονομίσματος. Εάν επαρκής αριθμός χρηστών Bitcoin το εγκατέλειπε για ένα συγκεκριμένο Altcoin, τότε οι προγραμματιστές του πρώτου θα αναγκάζονταν να υιοθετήσουν τα χαρακτηριστικά του ανταγωνιστικού νομίσματος που θα αποζητούσε η κοινότητα, αλλιώς θα κινδύνευε να χάσει την θέση του ως το υπερέχον κρυπτονόμισμα.

Καθώς τα κρυπτονομίσματα αποτελούν μία νέα εφεύρεση και το τοπίο συνεχώς μεταβάλλεται, οι επενδύσεις σε αυτά θεωρούνται υψηλού ρίσκου.[49] Ακόμα και το Bitcoin, που είναι μακράν το σταθερότερο, παρουσιάζει μεγάλη μεταβλητότητα στην τιμή του. Συγκριτικά όμως, τα Altcoins είναι καταφανώς πιο ασταθή κι ευμετάβλητα. Λόγω της χαμηλής κεφαλαιοποίησής τους στην αγορά παρουσιάζονται ιδιαίτερα επιρρεπή σε χειραγωγήσεις τιμών. Πολλές φορές, εύποροι επενδυτές, συχνά αποκαλούμενοι ως "φάλαινες", τοποθετούν σημαντικά ποσά σε κρυπτονομίσματα με χαμηλή τιμή ώστε να αυξήσουν την δημοτικότητά τους και να οδηγήσουν την τιμή τους στα ύψη. Μόλις η τιμή αυξηθεί σημαντικά και είναι ικανοποιημένοι, πωλούν τα νομίσματά τους στα χρηματιστήρια με τεράστιο κέρδος. Αυτό έχει φυσικά ως αποτέλεσμα την άμεση, γρήγορη κι απότομη πτώση της τιμής του κρυπτονομίσματος και την χασούρα των αφελών επενδυτών που είχαν σπεύσει να επενδύσουν τα χρήματά τους στο αναδυόμενο κρυπτονόμισμα "θαύμα". Η μέθοδος αυτή, που είναι γνωστή ως "pump and dump"[50], δεν είναι βλαβερή μόνο για τους αφελείς και ίσως άπληστους επενδυτές που βγαίνουν χαμένοι αλλά τις περισσότερες φορές αποδεικνύεται και τοξική για το Altcoin που λίγο μετά αφήνει την τελευταία του πνοή. Σημαντικά χαρακτηριστικά ενός υγιούς Altcoin πάντως, είναι μία ισχυρή κοινότητα, η υψηλή ρευστότητα και η συνεχής βελτίωση του πηγαίου κώδικα του νομίσματος από τους προγραμματιστές του.

Δεδομένου ότι το Bitcoin είναι ήδη το κυρίαρχο peer-to-peer νόμισμα και δεδομένης της υποστήριξης που έχει από του περισσότερους επενδυτές και την διαδικτυακή κοινότητα, θεωρείται δύσκολο για κάποιο Altcoin να το ξεπεράσει.[51] Βέβαια, το ίδιο δύσκολο εάν όχι αδύνατο φαινόταν πριν από μερικά έτη να λειτουργήσει και να επιτύχει σε οποιοδήποτε βαθμό οποιοδήποτε peer-to-peer κρυπτονόμισμα. Μπορεί βέβαια το Bitcoin τελικά να αποτύχει. Ως η πρώτη προσπάθεια δημιουργίας ενός παγκοσμίας χρήσης κρυπτονομίσματος, μπορεί τελικά να αποδεικτεί ότι πρόκειται για ένα ελαττωματικό σύστημα. Εάν είναι

[49] Wilmoth Josiah, What is an Altcoin, 19/09/2014, https://www.cryptocoinsnews.com/altcoin/
[50] https://www.cryptocoinsnews.com/pump-dump-know-signs-trading-altcoins/
[51] https://99bitcoins.com/altcoins/

έτσι, ένας μετέπειτα διάδοχος του πρωτόπλαστου κρυπτονομίσματος μπορεί πράγματι να αναδυθεί ως καλύτερη εναλλακτική λύση. Μέχρι στιγμής όμως, κανένα από τα Altcoins δεν φαίνεται να βρίσκεται σε θέση να το κάνει αυτό. Ο όποιος διάδοχος θα πρέπει να αντιμετωπίσει τις θεμελιώδεις αδυναμίες του Bitcoin, αν και, έως τώρα, καμία από αυτές δεν έχει αποδειχθεί μοιραία.

Ενδεικτικά, στα γνωστότερα Altcoins συγκαταλέγονται τα: Namecoin, Litecoin, Dogecoin, Feathercoin, Peercoin, Darkcoin, Ripple, Ethereum και Dash[52]. Ιδιαίτερο ενδιαφέρον παρουσιάζει το Namecoin, το πρώτο από τα Altcoins, που δημιουργήθηκε το 2011. Αν και λειτουργεί και ως νόμισμα, πρωταρχικός σκοπός του Namecoin είναι η αποκέντρωση του domain name registration[53], που θα καθιστούσε την λογοκρισία στο διαδίκτυο δυσκολότερη. Το Namecoin έχει παραμείνει ένα από τα πιο επιτυχημένα εναλλακτικά κρυπτονομίσματα καθόλη την διάρκεια της μέχρι τώρα σύντομης ζωής του και θεωρείται πως είναι το μόνο που θα μπορούσε να συνυπάρξει μη ανταγωνιστικά με το Bitcoin, λόγω του ρόλου που επιδιώκει να επιτελεί.[54]

[52] http://coinmarketcap.com/

[53] Για περισσότερες πληροφορίες σχετικά με το domain name registration βλ. https://en.wikipedia.org/wiki/Domain_Name_System#Domain_name_registration

[54] Beigel Ofil, What are Altcoins, 30/01/2014, 99Bitcoins, https://99bitcoins.com/altcoins/

# 3ο ΜΕΡΟΣ

## 3.1 Τα κίνητρα και η επικινδυνότητα του Satoshi Nakamoto[55]

Ο μυστηριώδης άνθρωπος ή ομάδα "Satoshi Nakamoto"[56] που κρύβεται πίσω από την δημιουργία του κρυπτονομίσματος Bitcoin, έχει, όπως αναφέραμε σε παραπάνω κεφάλαιο, όχι αμελητέα ποσότητα νομισμάτων που παραμένουν μέχρι σήμερα αδαπάνητα και αδρανή. Ποίος είναι όμως ο σκοπός που εξυπηρετούν, ποιό το μέλλον τους και πώς αυτό θα επηρεάσει το οικοσύστημα και την κοινότητα του Bitcoin;

Υπάρχει η ανησυχία, κι όχι αναίτια, πως έχει δοθεί υπερβολική δύναμη σε έναν και μόνο άνθρωπο ενώ παράλληλα έχει δημιουργηθεί η απορία πώς είναι δυνατό να του δίνεται τόση εμπιστοσύνη, ειδικά αναλογιζόμενοι την δυνατότητα επιρροής και πλούτου που του παρέχει το απόθεμα που έχει συγκεντρώσει. Το απόθεμα αυτό υπολογίζεται στο 1 εκατομμύριο bitcoin και αποκτήθηκε στις απαρχές της εξόρυξης του κρυπτονομίσματος που έκανε ο ίδιος για να εκκινήσει το σύστημα. Τα νομίσματα αυτά παραμένουν σε αδράνεια και ουδέποτε έχουν μετακινηθεί ή χρησιμοποιηθεί. Οι μόνες εξαιρέσεις στην αδράνεια των εξορυγμένων από τον Satoshi νομισμάτων, εντοπίζονται σε μερικές δοκιμαστικές συναλλαγές κατά τις πρώτες δέκα ημέρες λειτουργίας του συστήματος δηλαδή από την στιγμή που εξορύχθηκε το γενετήσιο block, ήτοι το πρώτο block στην blockchain.

Η προσωπική περιουσία λοιπόν του Satoshi υπολογίζεται ότι ανέρχεται σε περίπου 330 εκατομμύρια δολάρια[57]. Με το 1 εκατομμύριο κατέχει το 6,76% του παρόντος Bitcoin αποθέματος που βρίσκεται σε κυκλοφορία καθόσον έχουν εξορυχθεί 14,800,000 μονάδες[58] από τις συνολικά 21,000,000. Αυτό σημαίνει πρακτικά το 1/15 σε ένα ψηφιακό νόμισμα με κεφαλαιοποίηση στην αγορά που αγγίζει τα 5 δισεκατομμύρια δολάρια[59]. Κι αυτό χωρίς να συνυπολογίζονται οι δυνατότητες που παρέχονται από την ταχέως αναπτυσσόμενη ψηφιακή οικονομία που δομείται πάνω του.

Όπως είναι φυσικό, η φημολογία περί του μέλλοντος των νομισμάτων είναι έντονη κι έχουν σχηματιστεί αρκετά σενάρια.[60] Ο Satoshi θα μπορούσε λ.χ. να τα θέσει όλα άμεσα και μονομιάς σε κυκλοφορία. Ακόμα, θα μπορούσε να τα πωλεί σε μικρές δόσεις. Μία άλλη εναλλακτική θα ήταν να τα έκαιγε ενώ τέλος θα μπορούσε να συνδυάσει στοιχεία των προαναφερθέντων σεναρίων.

Πιο αναλυτικά, κατά το πρώτο σενάριο όπου ο δημιουργός θα τα έθετε όλα σε κυκλοφορία, αυτό θα ασκούσε εξαιρετικά μεγάλη πίεση στην αγορά του Bitcoin και θα οδηγούσε άμεσα σε μεγάλη πτώση της

[55] http://www.coindesk.com/dangerous-satoshi-nakamoto/
[56] Για ευκολία και μόνο, χωρίς να λησμονείται η διευκρίνιση της άγνοιας ως προς την πραγματική ταυτότητα του ή των δημιουργών, θα γίνεται λόγος για ένα πρόσωπο με το όνομα Satoshi Nakamoto.
[57] Με βάση τον δείκτη BPI του CoinDesk που αφορά τις Bitcoin τιμές, κατά την στιγμή της συγγραφής. http://www.coindesk.com/price/
[58] 4,76% στο σύνολο των 21 εκατομμυρίων.
[59] Σύμφωνα με το http://coinmarketcap.com/ και κατά την στιγμή της συγγραφής, 17/11/2015.
[60] http://www.coindesk.com/dangerous-satoshi-nakamoto/

αξίας του κρυπτονομίσματος καθώς μία τόσο μεγάλη αύξηση στην προσφορά θα μείωνε την τιμή του. Οι συνέπειες θα μπορούσαν να είναι καταστροφικές εάν κρίνουμε από το "BearWhale" περιστατικό, όπου η απελευθέρωση 26,000 BTC στο BitStamp[61] την 6η Οκτώβρη του 2014 προκάλεσε μείωση της αξίας κατά 10%.[62] Μεγαλύτερο όμως πρόβλημα από την πτώση στην αξία του νομίσματος, θα αποτελούσε η επίδραση της απώλειας της εμπιστοσύνης. Από την στιγμή που ο δημιουργός θα έπαυε να έχει εμπιστοσύνη στο ίδιο του το δημιούργημα, η εμπιστοσύνη θα εξέλειπε και σε όλους τους χρήστες. Οι εταιρείες που πραγματεύονται το Bitcoin, θα καθίσταντο αφερέγγυες και η αγορά του θα χρειαζόταν μεγάλο διάστημα για να ανακάμψει εάν τελικά ανέκαμπτε.

Σε ένα καλύτερο σενάριο, ο Satoshi θα πωλούσε τα νομίσματά του με υπευθυνότητα. Στην ήπια αυτή περίπτωση, μπορούμε να υποθέσουμε πως ο Satoshi θα ξεκινούσε πουλώντας ή ξοδεύοντας 1 satoshi στο block N, έπειτα δύο satoshis στο block N+1, τρία στο block N+2 κ.ο.κ. Οι πωλήσεις θα γίνονταν από διαφορετικές διευθύνσεις που όμως θα ήταν γνωστό ότι ανήκουν σε αυτόν ώστε να αποδεικνύεται ότι ο ίδιος έχει τον έλεγχο τους και την δυνατότητα να κινήσει αυτά τα νομίσματα. Εν συνεχεία, θα ενημέρωνε την κοινότητα περί των σχεδίων του να δαπανήσει τα νομίσματα που έχει στην κατοχή του αλλά παράλληλα θα την διαβεβαίωνε ότι σκόπευε να το κάνει αργά και σταδιακά. Σε μία πρώτη φάση, μία αρχική αντίδραση της αγοράς θα μπορούσε να οδηγήσει σε πτώση της τιμής λόγω του φόβου που θα δημιουργείτο από την κίνηση των νομισμάτων από τις διευθύνσεις του Satoshi, αλλά έπειτα θα επανέκαμπτε. Ακόμα, το όλο ενδεχόμενο της επανεμφάνισης του δημιουργού στην ενεργό δράση εντός της κοινότητας ίσως και να λειτουργούσε θετικά, αυξάνοντας την εμπιστοσύνη και οδηγώντας ανοδικά την τιμή του κρυπτονομίσματος με την πάροδο του χρόνου.

Σε προηγούμενο κεφάλαιο όπου αναφέρθηκε το πρόβλημα των "χαμένων" νομισμάτων, αναφερθήκαμε και στην δυνατότητα "καύσης" τους. Ένα από τα σενάρια που κυκλοφορούν στο διαδίκτυο, κάνουν λόγο για "καύση" των νομισμάτων που έχει στην κατοχή του ο Satoshi. Ο Satoshi, με μία απλή αποστολή των νομισμάτων σε μία από αυτές τις χωρίς δυνατότητα ξοδέματος διευθύνσεις, θα μπορούσε να εξαλείψει το απόθεμά του από την αγορά του Bitcoin. Αυτό, αυτομάτως, θα αύξανε την τιμή. Σε περίπτωση "καύσης" ενός εκατομμυρίου bitcoin, η αγορά θα αντιδρούσε με θεαματικά αποτελέσματα, αφού λιγότερα διαθέσιμα bitcoin θα σήμαινε ότι αυτά που απομένουν θεωρούνται πιο πολύτιμα.

Εναλλακτικά προς τα προηγούμενα σενάρια, πιστεύεται πως ο Satoshi θα μπορούσε να συνδυάσει στοιχεία από τις προαναφερθείσες προσεγγίσεις, δίνοντάς του την δυνατότητα τόσο να παραμείνει ανώνυμος αλλά και να έχει κάποιο κέρδος εξαργυρώνοντας μερίδιο των νομισμάτων του. Θα μπορούσε λοιπόν να αγοράσει bitcoin σε τρέχουσες τιμές αγοράς από κάποιο χρηματιστήριο και στην συνέχεια να "κάψει" νομίσματα από το απόθεμά του, πράγμα που θα οδηγήσει όπως είπαμε σε αύξηση των τιμών. Υποθέτοντας πως η τιμή όντως θα αυξηθεί, θα μπορούσε τότε να πουλήσει τα νομίσματα που είχε αγοράσει και να καρπωθεί το

[61] Εταιρεία αγοραπωλησίας Bitcoin. https://www.bitstamp.net/
[62] http://www.coindesk.com/market-weekly-bitcoin-bulls-return-wake-bearwhale-slaying/

κέρδος. Το σενάριο αυτό όμως παρουσιάζει τα εξής προβλήματα. Για να επωφεληθεί πλήρως και να πάρει την πλήρη αγοραία αξία των νομισμάτων που θα "κάψει", θα πρέπει όχι μόνο να πάρει πίσω τα χρήματα που έδωσε για την αγορά των νομισμάτων στο χρηματιστήριο, αλλά και ένα ίσο ποσό σε καθαρό κέρδος. Αυτό σημαίνει πως η αύξηση της τιμής στο κρυπτονόμισμα θα πρέπει να είναι της τάξεως του 100%. Για να το επιτύχει αυτό, θα πρέπει να "κάψει" σεβαστό μέρος των αποθεμάτων του και ενδεχομένως να προκαλέσει αποσταθεροποίηση της αγοράς, κάνοντας την μέθοδο αυτή εξαιρετικά ριψοκίνδυνη και μη βιώσιμη, ειδικά όταν πρόκειται για τόσο μεγάλο αριθμό νομισμάτων.

Το να μαντέψει κανείς τις προθέσεις του Satoshi δεν είναι εύκολο έργο. Όχι μόνο ως προς τα νομίσματα που έχει συσσωρεύσει αλλά και ως προς το Bitcoin στο σύνολό του. Έχει τελικώς κάποιον απώτερο σκοπό; Έγιναν όλα χάριν περισσότερης ελευθερίας και υπό την ιδεολογία της ισότητας, όπως φαίνεται να υποστηρίζει σε κάποιες από τις πρώτες του δημοσιεύσεις; Κάποιοι υποστηρίζουν πως ναι και ειδικότερα όσον αφορά την συσσώρευση του αποθέματος, επιχειρηματολογούν ότι κάποιος έπρεπε να δώσει το έναυσμα στο δίκτυο του Bitcoin και να το "φορτώσει" με νομίσματα όταν ακόμη λίγοι του έδιναν σημασία. Άλλωστε, με την προσπάθεια που έχει καταβληθεί για την προστασία της ανωνυμίας του, κανείς δεν μπορεί να υποστηρίξει ότι το κάνει για την δόξα.

Για την υποστήριξη του προαναφερθέντος επιχειρήματος, ενδιαφέρον έχει το γεγονός ότι ο Satoshi αποσύρθηκε σταδιακά από την διαδικασία της εξόρυξης, επιτρέποντας στους miners να αναλαμβάνουν όλο και μεγαλύτερο ποσοστό του hashrate. Η απόσυρση έγινε σε πολλαπλά στάδια, το κάθε στάδιο με δύο φάσεις. Αρχικά, ελάττωνε τον ρυθμό hashing στα μηχανήματά του. Έπειτα, αποσυνέδεε ένα και μοναδικό από αυτά και στη συνέχεια αύξανε τον ρυθμό hash στα εναπομείναντα για αντιστάθμιση της απώλειας. Αφ' ενός μεν δινόταν η δυνατότητα στον δημιουργό να ελέγξει την ανταπόκριση του συστήματος στην αποσύνδεση μίας μηχανής, αφ' ετέρου όμως, η μέθοδος αυτή μας επιτρέπει να εκλάβουμε τις ενέργειές του ως ηθελημένες κι όχι ως απλή δυσλειτουργία. Έτσι, ενισχύεται η υπόθεση ότι σκοπός του δεν ήταν το κέρδος αλλά η παραχώρηση των ανταμοιβών εξορύξεως σε άλλους. [63]

Σε μία από τις τελευταίες πάντως γνωστές επικοινωνίες του Satoshi τον Απρίλιο του 2011, ειπώθηκε πως έχει "προχωρήσει σε άλλα πράγματα". Η εξαφάνισή του όχι μόνο εγγυήθηκε δημοσιότητα στο θέμα αλλά προσέδωσε ένα πέπλο μυστηρίου στο Bitcoin και μία μυθική διάσταση στις συνθήκες γέννησής του. Άλλωστε, μοιάζει ταιριαστό σε ένα αποκεντρωμένο κρυπτονομισματικό σύστημα να απουσιάζει ένας αρχηγός.[64] Υποστηρικτές του εμφανίζονται καθησυχαστικοί, υποστηρίζοντας πως ένας εξολοκλήρου προσβάσιμος στο κοινό πηγαίος κώδικας ακυρώνει την ανάγκη γνωστοποίησης του δημιουργού καθώς είναι

[63] http://www.coindesk.com/dangerous-satoshi-nakamoto/

[64] http://www.economist.com/blogs/economist-explains/2015/11/economist-explains-1?fsrc=scn/fb/wl/ee/st/whoissatoshinakamoto

αδύνατο να κρύβονται μυστικά από πίσω.[65] Επίσης, η χρήση ψευδωνύμου ανάγκασε τους ανθρώπους να εστιάσουν στην τεχνολογία αντί στον δημιουργό.[66]

Για όσους εξακολουθούν να έχουν αμφιβολίες ως προς τα κίνητρα του δημιουργού-πατέρα του εξεταζόμενου κρυπτονομίσματος, πιθανώς καταφεύγουν σε συνομωσιολογικές θεωρίες ή εν γένει ανησυχούν για το μέλλον του νομίσματος, η απλούστερη λύση είναι η διαφοροποίηση του χαρτοφυλακίου τους σε περίπτωση που σκοπεύουν να επενδύσουν. Κανείς δεν μπορεί να αρνηθεί ότι το Bitcoin αποτελεί μία υψηλού ρίσκου επένδυση και γι' αυτό θα πρέπει να χειρίζεται ως τέτοια. Ελαφρώς καθησυχαστικά θα έπρεπε να λειτουργούν πάντως το γεγονός ότι ο κώδικας του κρυπτοσυστήματος έχει ξαναγραφτεί σχεδόν εξολοκλήρου, αφήνοντας λίγο χώρο για κερκόπορτες και ότι η θέση του Satoshi αποδυναμώνεται κατά 25 BTC ανά δεκάλεπτο. Τέλος, το Bitcoin δεν έχει φτάσει ακόμα στο σημείο να μπορεί να επιφέρει παραπάνω από ισχνούς κυματισμούς στην παγκόσμια οικονομία οπότε η προσοχή ίσως θα έπρεπε να είναι στραμμένη αλλού[67]..

## 3.2 Νομοθετικό πλαίσιο του Bitcoin

Το Bitcoin σχεδιάστηκε ως ένα κρυπτονομισματικό σύστημα που θα λειτουργούσε εκτός ελέγχου κυβερνητικών θεσμών χωρίς να μπορεί να λογοκριθεί ή να ρυθμιστεί, δίνοντας στους χρήστες του την δυνατότητα ιδιωτικών, ασφαλών και ανώνυμων ψηφιακών συναλλαγών. Στα σχεδόν 7 χρόνια ζωής του, το κρυπτονόμισμα συνεχίζει να αποδεικνύεται ένα άκρως αμφιλεγόμενο ζήτημα για τις ρυθμιστικές αρχές, τόσο τις φορολογικές όσο και τις νομικές αλλά και τους φορείς επιβολής του νόμου που εξακολουθούν να παλεύουν όχι μόνο να το εντάξουν στα ήδη υπάρχοντα ρυθμιστικά πλαίσια αλλά ακόμα και να κατανοήσουν την λειτουργία του καθώς και τις επιπτώσεις που αυτό προκαλεί.

Πολλά από τα πρωτοφανή χαρακτηριστικά της τεχνολογίας του Bitcoin, τού δίνουν την δυνατότητα να διαταράξει ένα ευρύ φάσμα θεσμών και υπηρεσιών που μέχρι πρότινος υπάγονταν στις ρυθμίσεις των κρατών. Μεταξύ τους, η δυνατότητα να αποσταλούν χρήματα από οποιονδήποτε οπουδήποτε στον κόσμο μέσα σε λίγα λεπτά, η peer-to-peer αποκεντρωμένη φύση της μεταβίβασης αξίας και η ύπαρξή του εξολοκλήρου στο ψηφιακό φάσμα. Οι κύριοι όμως λόγοι ανησυχίας που σχετίζονται με το κρυπτονόμισμα, πηγάζουν από τον αποκεντρωμένο χαρακτήρα του συστήματος και είναι ως επί το πλείστον σχετικοί με παράνομες δραστηριότητες. Το κρυπτονόμισμα αποτελεί δυνητικό εργαλείο ξεπλύματος μαύρου χρήματος, αγοράς παράνομων προϊόντων όπως είναι τα ναρκωτικά αλλά και τα όπλα. Οι ανησυχίες αυτές δεν περιορίζονται στο ιδεατό περιβάλλον χωρίς καμία ανταπόκριση στην πραγματικότητα αλλά επαληθεύονται συχνά. Μία από τις πιο γνωστές περιπτώσεις αποτελεί η περίπτωση του επονομαζόμενου "Silk Road", μίας ανώνυμης διαδικτυακής αγοράς που είχε το Bitcoin ως την μοναδική αποδεκτή μορφή νομίσματος. Έκλεισε

[65] http://www.coindesk.com/dangerous-satoshi-nakamoto/
[66] http://www.coindesk.com/information/who-is-satoshi-nakamoto/
[67] http://www.economist.com/news/schoolsbrief/21584534-effects-financial-crisis-are-still-being-felt-five-years-article

τον Οκτώβρη του 2013 μετά από επέμβαση του FBI. Ακόμα, το Bitcoin γίνεται όλο και πιο δημοφιλές σε απαγωγείς, οι οποίοι ζητούν τα λύτρα να πληρώνονται με αυτό[68] ενώ μέχρι και η τρομοκρατική ισλαμική οργάνωση ISIS είναι γνωστό πως το μεταχειρίζεται για τις συναλλαγές της[69]. Απ' την άλλη πλευρά όμως, τα οφέλη κάθε νέας τεχνολογίας δύνανται να εκμεταλλευθούν αρνητικώς καθώς η απόλαυση των διευκολύνσεων δεν περιορίζεται πότε στους ενάρετους χρήστες. Επιπροσθέτως, ελλείψει δυνατότητας χρήσης bitcoin, τα μετρητά αποτελούν πάντα εναλλακτική λύση για πληρωμές και συναλλαγές που διαφεύγουν του ελέγχου τραπεζών και κυβερνητικών αρχών.

Η αποτελεσματική ρύθμιση των ψηφιακών νομισμάτων έχει αποδειχθεί ένα δύσκολο έργο για τις κυβερνήσεις ενώ ακόμα και η χάραξη συγκεκριμένης πολιτικής και η επικαιροποίηση της νομοθεσίας σχετικά με αυτά βρίσκεται σε πρώιμο (εάν όχι μηδενικό) στάδιο. Η ρύθμιση του ζητήματος έχει γίνει ένα από τα πιο αμφιλεγόμενα και πολυσυζητημένα θέματα του κλάδου των ψηφιακών νομισμάτων. Υπάρχουν θέματα και απόψεις που θα πρέπει να εξεταστούν κι από τις δύο πλευρές για να καταλήξει η διαδικασία λήψης αποφάσεων σε ένα εύλογο ρυθμιστικό πλαίσιο. Όλα αυτά φυσικά καθιστούν την ήδη δύσκολη κι εύθραυστη διαδικασία ακόμα πιο περίπλοκη.

Όσον αφορά την στάση που τηρούν τα κράτη απέναντι στο Bitcoin, κυμαίνονται από την πλήρη αποδοχή του νομίσματος κι ένταξή του στο υπάρχον κανονιστικό πλαίσιο, έως αδιαφορία ή τήρηση στάσης αναμονής με ενδεχόμενη διατύπωση επιφυλάξεων ή προειδοποιήσεων αναφορικά με την χρήση των κρυπτονομισμάτων ενώ υπάρχουν και περιπτώσεις όπου έχουμε πλήρη απαγόρευσή του. Ο φορέας ρύθμισης του θέματος ποικίλλει αναλόγως με την χώρα αλλά συνήθως θεωρείται ως θέμα που αφορά πρωτίστως τις εθνικές χρηματοπιστωτικές ρυθμιστικές αρχές. Σε κάποιες μάλιστα, το θέμα ρυθμίζεται και σε ομοσπονδιακό ή περιφερειακό επίπεδο, είτε πρόκειται για τις πολιτείες των ΗΠΑ, είτε για την ΕΕ. [70]

Οι ΗΠΑ έχουν το πιο εξελιγμένο ρυθμιστικό πλαίσιο. Κατ' αρχήν το Υπουργείο Οικονομικών της χώρας, έχει εκδώσει κατευθυντήριες γραμμές, κατηγοριοποιώντας τους χρήστες του σε επιχειρήσεις υπηρεσιών χρήματος (γνωστές και ως επιχειρήσεις μεταβίβασης χρημάτων ή Money Transmitting Businesses (MTBs)) και μη. Όσοι εντάσσονται στην κατηγορία των MTBs είναι υποχρεωμένοι να εφαρμόζουν μέτρα Anti-Money Laundering (AML) και Know Your Client (KYC). Στην πράξη αυτό σημαίνει ότι απλοί χρήστες που απλά αγοράζουν υπηρεσίες και προϊόντα κάνοντας χρήση του νομίσματος, δεν εντάσσονται σε αυτήν την κατηγορία. Το ίδιο ισχύει και για τους miners που εξορύσσουν το νόμισμα για προσωπική τους χρήση όπως και για τις εταιρείες που αγοράζουν και πωλούν το ψηφιακό νόμισμα αποκλειστικώς ως επένδυση.[71]

[68] https://www.cryptocoinsnews.com/bitcoin-ransoms-becoming-popular-kidnappings/
[69] http://www.kathimerini.gr/831795/article/oikonomia/die8nhs-oikonomia/bitcoin-xrhsimopoiei-to-islamiko-kratos
[70] Is Bitcoin Legal?, CoinDesk, 19/08/2014, http://www.coindesk.com/information/is-bitcoin-legal/
[71] Rizzo Pete, FinCen declares Bitcoin miners, investors aren't money transmitters, CoinDesk, 31/01/2014, http://www.coindesk.com/fincen-bitcoin-miners-investors-money-transmitters/

Αντιθέτως, εάν κάποιος πωλεί το ψηφιακό νόμισμα με αντάλλαγμα πραγματικό νόμισμα, τότε θεωρείται MTB. Φυσικά, σε αυτήν την κατηγορία εμπίπτουν και τα χρηματιστήρια κρυπτονομισμάτων.

Συνεχίζοντας, δύο άλλες υπηρεσίες, η Commodity Futures Trading Commission (CTFC) υπεύθυνη για χρηματοπιστωτικά παράγωγα και η Securities and Exchange Commision (SEC), διατηρούν επιφυλάξεις για μελλοντική ρύθμιση του ζητήματος ενώ έχουν εκδώσει προειδοποιήσεις προς τους υποψήφιους επενδυτές. Καθώς η κάθε πολιτεία έχει δικές της χρηματοοικονομικές ρυθμιστικές αρχές αλλά και νόμους, το νομοθετικό τοπίο ως σύνολο εξακολουθεί να παραμένει θολό. Κάθε πολιτεία προσεγγίζει το κρυπτονόμισμα διαφορετικά. Στην πολιτεία του Texas, το bitcoin θεωρείται χρήμα έπειτα από δικαστική απόφαση το 2013. Η πολιτεία της Νέας Υόρκης είναι η μοναδική πολιτεία που έχει καταλήξει σε κάποια τελική ρύθμιση του. Πρόκειται για το "Bitlicense", το πρώτο καθεστώς χορήγησης αδειών ειδικά για ψηφιακά νομίσματα. Έπειτα υπάρχει και το IRS (Internal Revenue Service δηλαδή η αμερικάνικη εφορία), που επιθυμεί να προχωρήσει σε συμπερίληψη του bitcoin στα φορολογητέα εισοδήματα[72], θεωρώντας ότι εφόσον οι φορολογούμενοι αποκτούν εισοδήματα σε κάποιο ψηφιακό νόμισμα θα πρέπει να τα δηλώνουν μαζί με τα λοιπά φορολογητέα εισοδήματα. Η δήλωση αυτή όμως στηρίζεται στο ήδη υπάρχουν κανονιστικό πλαίσιο που ισχύει για τα εισοδήματα από τυχερά παιχνίδια, την ανταλλαγή εμπορευμάτων ή κάποιο χόμπυ.

Ο κλάδος των κρυπτονομισμάτων, απ' την άλλη, έχει αντιδράσει στις αυξανόμενες ανησυχίες και στην προσπάθεια ρύθμισης του τομέα στις ΗΠΑ ποικιλοτρόπως. Έχει υπάρξει σοβαρή προσπάθεια να ανοίξει ο διάλογος και να συμπεριληφθούν οι ιδιώτες φορείς στην συνομιλία ώστε να αναπτυχθούν εύλογες κατευθυντήριες γραμμές και ρυθμίσεις. Τα χρηματιστήρια έχουν επιδιώξει να αποκτήσουν άδειες ως MTBs τόσο σε πολιτειακό όσο και ομοσπονδιακό επίπεδο ενώ κάποιοι αποφεύγουν όποια επιχειρηματική δραστηριότητα αφορά αμερικανούς πελάτες έως ότου ξεκαθαρίσει το τοπίο.

Όσον αφορά την Ευρωπαϊκή Ένωση, το 2012 σε μία δημοσίευση[73] της ΕΚΤ αναφορικά με τα συστήματα εικονικών νομισμάτων, δηλωνόταν πως το Bitcoin δεν μπορεί να συμπεριληφθεί στις παραδοσιακές ρυθμίσεις του χρηματοπιστωτικού τομέα καθώς δεν αφορά παραδοσιακούς χρηματοπιστωτικούς παράγοντες. Στην ίδια δημοσίευση το εν λόγω κρυπτονόμισμα ταξινομήθηκε ως μετατρέψιμο αποκεντρωμένο εικονικό νόμισμα (convertible decentralized virtual currency). Το 2013 όπως και το 2014, η Ευρωπαϊκή Αρχή Τραπεζών (EBA), εξέδωσε προειδοποίηση[74] για επενδυτικό κίνδυνο, απάτη, φοροδιαφυγή και άλλα εγκλήματα που μπορούν πιθανόν να συνδέονται με το κρυπτονόμισμα και γνωμοδότησε συμβουλεύοντας τις ευρωπαϊκές τράπεζες να απέχουν από τα εικονικά νομίσματα όπως το Bitcoin έως ότου αναπτυχθεί ένα κανονιστικό πλαίσιο. Η σημαντικότερη μέχρι στιγμής απόφαση που έχει ληφθεί εντός της ΕΕ αφορά την πρόσφατη απόφαση του Δικαστηρίου των Ευρωπαϊκών Κοινοτήτων που απαλλάσσει τις

[72] Rizzo Pete, IRS to tax digital currencies as property, not currency, CoinDesk, 25/03/2014, http://www.coindesk.com/internal-revenue-service-treat-digital-currencies-property/

[73] http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

[74] European Banking Authority, EBA Opinion on 'virtual currencies', 4/7/2014, [pdf] http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf

συναλλαγές πραγματικού νομίσματος με ψηφιακό από φόρους προστιθέμενης αξίας. Η απόφαση αυτή ήρθε ως απάντηση σε αίτημα από τις σουηδικές φορολογικές αρχές και η γενική ιδέα είναι πως το bitcoin πρέπει να αντιμετωπίζεται ως μέσο πληρωμής, όπως δηλαδή τα παραδοσιακά νομίσματα και ως εκ τούτου προστατεύεται από την ευρωπαϊκή οδηγία που απαλλάσσει τις συναλλαγές νομισμάτων από φόρους προστιθέμενης αξίας. Τα κράτη-μέλη της ΕΕ, έχουν ως επί το πλείστον περιοριστεί στην έκδοση προειδοποιήσεων για τους κινδύνους του νομίσματος στους ιδιώτες χωρίς να προχωρήσουν σε ρυθμίσεις.

Στην Ρωσία το τοπίο σχετικά με την νομιμότητα ή μη του bitcoin παραμένει θολό.[75] Αρχικά τον Φεβρουάριο του 2014, η Κεντρική Τράπεζα της Ρωσίας εξέδωσε ανακοίνωση όπου χαρακτήριζε την χρήση οποιουδήποτε άλλου νομισματικού μέσου ή υποκατάστατου απαγορευμένη καθώς το επίσημο ρωσικό νόμισμα είναι το ρούβλι. Τον Μάρτη του ίδιου έτους σε ερώτηση που απήυθυνε ιδιώτης όμως, η ΚΤ απάντησε πως σε συνάντηση των κορυφαίων ρωσικών χρηματοοικονομικών αρχών το bitcoin δεν απαγορεύτηκε. Η απάντηση, συνεχίζοντας, χαρακτήριζε την συνάντηση ως αφιερωμένη στην καταπολέμηση των εγκλημάτων σχετικών με την χρήση ανώνυμων συστημάτων πληρωμής και κρυπτονομισμάτων στο έδαφος της Ρωσίας ενώ εξέφραζε και την διάθεση ανάπτυξης ενιαίας προσέγγισης για τον καθορισμό του νομισματικού καθεστώτος των κρυπτονομισμάτων.[76] Το 2014, το Υπουργείο Οικονομικών της χώρας ανακοίνωσε πρόταση απαγόρευσης του Bitcoin καθώς και όλων των ειδών δραστηριοτήτων που σχετίζονται με αυτό, περιλαμβανομένων της εμπορίας, της εξόρυξης και των συναλλαγών.[77] Δεν ισχύει λοιπόν ακόμα κάποια επίσημη απαγόρευση αλλά η χρήση του αποδοκιμάζεται από την κυβέρνηση και τις λοιπές ρυθμιστικές αρχές.

Στην Κίνα από κρατικής πλευράς επικρατεί μία έντονα αρνητική εικόνα έναντι του bitcoin και των ομοίων του ενώ έχουν εκδοθεί πολλάκις προειδοποιήσεις και συχνά προβάλλονται ντοκυμαντέρ που ενημερώνουν τους πολίτες για τους κινδύνους που διατρέχει όποιος το χρησιμοποιεί. Δεν ισχύει κάποια απαγόρευση σε ιδιώτες, οι οποίοι μπορούν ελεύθερα τόσο να το κατέχουν όσο και να το χρησιμοποιούν. Σε χρηματοπιστωτικά ιδρύματα απαγορεύεται να έχουν οποιαδήποτε σχέση με το εν λόγω κρυπτονόμισμα. Η αγορά του Bitcoin βρίσκεται όμως σε άνθιση στην χώρα αυτή, μερικώς λόγω των capital controls που βρίσκονται σε ισχύ.

Στις χώρες που έχουν απαγορεύσει το Bitcoin[78] συγκαταλέγονται η Βολιβία και το Κιργιστάν ενώ στο Μπαγκλαντές η χρήση του νομίσματος αποτελεί αξιόποινη πράξη με ποινή φυλάκισης έως και 12 ετών. Το Εκουαδόρ έχει απαγορεύσει το bitcoin και άλλα κρυπτονομίσματα με τον λόγο να πιθανολογείται ότι

[75] Tessier Benoit, 'You can play with your bitcoins but you can't pay with them':Russia may ban cryptocurrencies by 2015, RT, 12/09/2014, https://www.rt.com/business/187440-bitcoin-ban-russia-cryptocurrency/

[76] Perez Yessi Bello, Russia's central bank meets with finance reps for Bitcoin talks, CoinDesk, 12/06/2015, http://www.coindesk.com/russias-central-bank-meets-with-finance-reps-for-bitcoin-talks/

[77] Yashu Gola, Russia planning to criminalize bitcoin activities, NEWSBTC, 24/09/2015, http://www.newsbtc.com/2015/09/24/russia-planning-to-criminalize-bitcoin-activities/

[78] Smart Evander, Top 10 countries in which Bitcoin is banned, 27/05/2015, CryptoCoinsNews, https://www.cryptocoinsnews.com/top-10-countries-bitcoin-banned/

αποτελεί το γεγονός ότι σχεδιάζει την δημιουργία δικού του κρυπτονομίσματος στο μέλλον. Στην Ισλανδία, η οποία ασκεί αυστηρούς ελέγχους στην κίνηση κεφαλαίων επιδιώκοντας προστασία από εκροή του ισλανδικού νομίσματος από την χώρα, η ανταλλαγή ξένου συναλλάγματος προς bitcoin απαγορεύεται καθώς θεωρείται πως το κρυπτονόμισμα δεν είναι συμβατό με τον νόμο περί συναλλάγματος που υπάρχει. Στην Ταϊλάνδη, το τοπίο είναι θολό καθώς το Bitcoin θεωρείται παράνομο λόγω έλλειψης υπαρχόντων κανόνων που να το ρυθμίζουν. Από τεχνικής άποψης λοιπόν υπάρχει απαγόρευση η οποία όμως δεν είναι σε ισχύ στην πραγματικότητα. Στο Βιετνάμ, η χρήση του Bitcoin είναι παράνομη για χρηματοπιστωτικά ιδρύματα αλλά όχι για ιδιώτες, αν και αποθαρρύνεται εντόνως. Στην Ταϊβάν, το Bitcoin πρόσφατα χαρακτηρίστηκε ως παράνομο ύστερα από μία απαγωγή επιχειρηματία, τα λύτρα για τον οποίο ζητήθηκαν σε bitcoin.[79] Τέλος, στην Ινδία, παρότι το Bitcoin δεν χαρακτηρίζεται παράνομο, το Bitcoin χρηματιστήριο της χώρας έκλεισε τον Μάιο του 2015 λόγω του ότι η τράπεζα με την οποία συνεργαζόταν δεν επιτρέπει πλέον την λειτουργία του ενώ αδυνατεί να βρει κάποια άλλη τράπεζα μέσω της οποίας θα μπορούσε να επαναλειτουργήσει καθώς "όπως φαίνεται αυτή είναι η γενικότερη πολιτική που ισχύει στην Ινδία" πλέον.[80]

Στα έξι και πλέον χρόνια ζωής του κρυπτονομίσματος, τα κράτη και οι ρυθμιστικές αρχές τους ακόμα δεν έχουν αναπτύξει σαφή κανονιστικά πλαίσια που είτε να περιορίζουν είτε να ρυθμίζουν είτε να απαγορεύουν πλήρως την λειτουργία και την χρήση του. Πολλές χώρες εξακολουθούν να αναζητούν τον καλύτερο τρόπο για να ρυθμιστεί εύλογα το ζήτημα, επιτρέποντας την νόμιμη χρήση του και προλαμβάνοντας παράλληλα τις εγκληματικές πράξεις που συνδέονται με αυτό. Η αποκεντρωμένη και ανώνυμη φύση του, δεν συνεισφέρουν ουδόλως στην διαδικασία. Το Bitcoin παραμένει εντός μία γκρίζας ζώνης καθώς το τεχνολογικό άλμα που αδιαμφισβήτητα αποτελεί η τεχνολογία των κρυπτονομισμάτων έχει αφήσει πίσω νομοθέτες και ρυθμιστές.

## 3.3 Επιπτώσεις και Προκλήσεις

Οι επιπτώσεις του κρυπτοσυστήματος του Bitcoin, ενδεχόμενες και πραγματικές, επεκτείνονται πολύ πέραν των επιπτώσεων που έχει το νόμισμά του. Το Bitcoin είναι πολύ περισσότερα από ένα νόμισμα, αν και το νόμισμα είναι η πρώτη του εφαρμογή και συνεπώς η πιο γνωστή. Η τεχνολογική καινοτομία, όμως, που βρίσκεται πίσω από το Bitcoin μπορεί να επιφέρει στην καθημερινότητά μας αλλαγές ανάλογων αυτών που επέφερε το διαδίκτυο.[81] Λεχθέντων τούτων, κρίνεται σκόπιμος ο διαχωρισμός των αντικτύπων και συνεπειών του κρυπτονομίσματος από αυτά του κρυπτοσυστήματος εν γένει ως τεχνολογίας, δηλαδή της τεχνολογίας της blockchain.

[79] Das Samburaj, Bitcoin declared illegal in Taiwan, 02/11/2015, https://www.cryptocoinsnews.com/bitcoin-declared-illegal-in-taiwan/
[80] https://www.cryptocoinsnews.com/indian-bank-shuts-bitcoin-exchange-btcxindia/
[81] http://www.thestreet.com/story/13319579/1/bitcoin-may-change-our-world-in-ways-as-profound-as-the-internet.html

### 3.3.1 Του Κρυπτονομίσματος

Όσον αφορά το Bitcoin ως νόμισμα, όπως έχει προλεχθεί, δημιουργεί σίγουρα προκλήσεις στις κυβερνητικές αρχές οι οποίες αδυνατούν να ανταπεξέλθουν με την κατάρτιση ενός εύλογου ρυθμιστικού πλαισίου. Το κρυπτονόμισμα κατ' αρχήν μπορεί να αποτελέσει πρόσφορο εργαλείο για την διεξαγωγή και χρηματοδότηση παράνομων δραστηριοτήτων, όπως το ξέπλυμα μαύρου χρήματος, η αγορά παράνομων προϊόντων, ενώ έχουν υπάρξει και περιπτώσεις απαγωγών όπου τα λύτρα ζητούνται από τους απαγωγείς να καταβληθούν σε bitcoin. Ακόμα, η ψευδωνυμία που προσφέρει, η οποία αποτελεί και βασικό χαρακτηριστικό γνώρισμα αλλά και σημείο προώθησής του, προκαλεί δυσκολίες στην φορολογική πολιτική των κρατών καθώς διευκολύνει την φοροδιαφυγή. Έχει επίσης αντίκτυπο στην νομισματική πολιτική των κρατών καθώς μπορεί να εξυπηρετήσει θαυμάσια όσους επιθυμούν να φυγαδεύσουν κεφάλαια στο εξωτερικό εν μέσω λ.χ. capital controls.

Από την πλευρά των ίδιων των εθνικών νομισμάτων, το Bitcoin δεν φαντάζει τουλάχιστον ακόμα να μπορεί να τα απειλήσει. Αφ' ενός μεν δεν είναι ακόμα αρκετά ευρέως διαδεδομένο κι αφ' ετέρου η εξαιρετικά ευμετάβλητη τιμή του το κάνει μία ριψοκίνδυνη επένδυση. Αν και μπορεί να υποστηριχθεί ότι η καινοτομία του κρυπτονομίσματος είναι αντίστοιχη αυτής του διαδικτύου κι ως εκ τούτου αργά αλλά σταθερά αυτό θα αρχίσει να υπερφαλαγγίζει τα πεπαλαιωμένα νομίσματα, όπως το διαδίκτυο αντικατέστησε "αρχαίες" μεθόδους επικοινωνίας. Η σημασία λοιπόν δεν θα πρέπει να δίνεται στο Bitcoin αυτό καθεαυτό αλλά στις έμφυτες επαναστατικές δυνατότητες της τεχνολογικής καινοτομίας του.[82] Πάντως, προς το παρόν, μόνο πεπειραμένοι χρήστες φαίνεται να μπορούν να παρακάμψουν τυχόν απαγορεύσεις που επιβάλλονται σε αυτό εκ των κρατικών ρυθμιστικών αρχών.

Όσον αφορά τους ίδιους τους χρήστες, το bitcoin μπορεί να αποτελέσει μία πιο αποδοτική μέθοδο πληρωμής ως προς το κόστος συναλλαγών σε σύγκριση με τις παραδοσιακές μεθόδους. Παρακάμπτοντας τις παραδοσιακές χρηματοπιστωτικές υποδομές, χρησιμοποιώντας πολλαπλούς διαύλους λόγω της αποκεντρωμένης φύσης του, παρουσιάζει πλεονεκτήματα στην ροή πραγματοποίησης των πληρωμών καθώς αυτή γίνεται ανθεκτική σε τυχόν κινδύνους να τεθεί κάποιο από τα συστήματα επεξεργασίας των πληρωμών εκτός λειτουργίας.[83] Αναφορικά με την ασφάλεια των καταναλωτών/χρηστών πάσχει πάντως καθώς ελλείψει κάποιας κεντρικής αρχής και της μη αναστρεψιμότητας των συναλλαγών λόγω του τρόπου βάσει του οποίου λειτουργεί η blockchain, τυχόν απώλεια bitcoin από κλοπή, απάτη ή οποιουδήποτε άλλου λόγου δεν δύναται να αντιστραφεί κι έτσι δεν μπορεί να υπάρχει αποκατάσταση του χρήστη. Ακόμα, λόγω της πληθώρας των κρυπτονομισμάτων αλλά και χρηματιστηρίων, η προσοχή που πρέπει να καταβάλλει ο καθείς πριν την επιλογή του κατάλληλου, πρέπει να είναι αυξημένη. Τέλος, λίγες είναι οι επιχειρήσεις που αποδέχονται πληρωμές σε κρυπτονόμισμα, απομειώνοντας πρακτικά την χρησιμότητά τους στις καθημερινές συναλλαγές.

[82] http://cointelegraph.com/news/115555/why-the-exploding-bitcoin-price-really-doesnt-matter
[83] http://www.riksbank.se/Documents/Rapporter/POV/2014/2014_2/rap_pov_artikel_4_1400918_sve.pdf

Μία ακόμα πτυχή του κρυπτονομίσματος που δεν μπορεί να παραβλεφθεί, είναι οι δυνατότητες που μπορεί να παρέχει σε κατοίκους των αναπτυσσόμενων χωρών. 2,5 δισεκατομμύρια άνθρωποι παγκοσμίως χωρίς κάποιον τραπεζικό λογαριασμό, εν μέρει λόγω έλλειψης πρόσβασης σε κάποια τράπεζα ή λόγω της σαθρής φύσης του εγχώριου τραπεζικού τους συστήματος, θα μπορούσαν να συνδεθούν μέσω του κρυπτονομίσματος στο επίσημο χρηματοπιστωτικό σύστημα και να απολαύσουν τα όποια οφέλη αυτό θα τους παρέχει.[84] Προϋπόθεση βέβαια αποτελεί η πρόσβαση στο διαδίκτυο.

Πολλοί ανησυχούν για τις δυνητικές επιπτώσεις των κρυπτονομισμάτων στην ομαλή λειτουργία και συνέχεια των χρηματοπιστωτικών ιδρυμάτων λόγω της φύσης των πρώτων που επιτρέπει την εξολοκλήρου παράκαμψη των δεύτερων. Απέχουμε πολύ από την ημέρα που τα κρυπτονομίσματα θα καταφέρουν να αποτελέσουν απειλή για τις τράπεζες. Εκ των πραγμάτων, ακόμα και τα χρηματιστήρια των κρυπτονομισμάτων αναζητούν τις υπηρεσίες των τραπεζών, κυρίως για την διατήρηση καταθέσεων αλλά και διευκόλυνση της ρευστότητας. Βέβαια, λίγες είναι οι τράπεζες που αποδέχονται να συνεργαστούν με τέτοιου είδους επιχειρήσεις[85], ενώ σε ορισμένες χώρες αυτό απαγορεύεται δια νόμου. Διάλογο επιδέχεται το ζήτημα εάν και κατά πόσο θα πρέπει να έχουν σχέση τα χρηματοπιστωτικά ιδρύματα με κρυπτονομίσματα. Η επικρατούσα άποψη πιστεύει πως δεν πρέπει να σχετίζονται οι δύο τομείς λόγω της ευμετάβλητης τιμής και της ριψοκινδυνότητας της επένδυσης που μπορεί να έχει σοβαρές επιπτώσεις στο χαρτοφυλάκιο των τραπεζών και συνεπαγομένως στην ασφάλεια των καταθετών. Σε δήλωσή της πάντως, η Christine Lagarde, πρόεδρος του ΔΝΤ και πρώην υπουργός οικονομικών της Γαλλίας, εξέφρασε την άποψη πως το υπάρχον χρηματοπιστωτικό σύστημα δεν έχει κανέναν λόγο να φοβάται τις τεχνολογίες αυτού του είδους για όσο καιρό ακόμα οι τεχνολογίες αυτές εκμεταλλεύονται το χαρακτηριστικό της ανωνυμίας.[86] Τέλος, θα πρέπει να αναφέρουμε και το γεγονός ότι οι συναλλαγές στο Bitcoin δεν εκτελούνται σε πραγματικό χρόνο, εν αντιθέσει με τις συναλλαγές με πιστωτικές κάρτες για τις οποίες απαιτούνται μονάχα κάποια δευτερόλεπτα.

### 3.3.2 Της Τεχνολογίας του

Λέγοντας blockchain αναφερόμαστε σε ένα κοινό, αξιόπιστο, δημόσιο βιβλίο ισολογισμού, το οποίο ο καθένας μπορεί να επιθεωρεί και να πιστοποιεί την εγκυρότητά του χωρίς όμως αυτό να βρίσκεται υπό τον έλεγχο κανενός χρήστη. Το βιβλίο κρατείται ενημερωμένο συλλογικά από τους συμμετέχοντες ενώ αυτό μπορεί να τροποποιηθεί μόνο σύμφωνα με αυστηρούς κανόνες κι έπειτα από γενική συμφωνία. Η επαναστατική νέα τεχνολογία της blockchain απαλλάσσει τους συναλλασσόμενους από την ανάγκη ύπαρξης εμπιστοσύνης μεταξύ τους παρακάμπτοντας παράλληλα την ανάγκη τρίτου έμπιστου μέρους. Μάλιστα το περιοδικό The Economist, την έχει χαρακτηρίσει "μηχανή (παραγωγής) εμπιστοσύνης".[87] Μονάχα πρόσφατα όμως, η δημοσιότητα έχει μετατοπιστεί από το κρυπτονόμισμα στην τεχνολογία που

[84] http://www.economist.com/news/business-books-quarterly/21638093-rise-and-fall-crypto-currency-good-news-authors-least-much

[85] http://www.wsj.com/news/articles/SB10001424052702304202204579252850121034702

[86] http://www.coindesk.com/imf-chief-banks-bitcoin-blockchain/

[87] http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine?fsrc=scn/fb/te/pe/ed/thetrustmachine

βρίσκεται στην βάση του. Οι καταπληκτικές δυνατότητές της αγνοούνται καθώς πολλοί αδυνατούν να παραβλέψουν την κακή φήμη που εξακολουθεί να έχει το Bitcoin[88].

Οι δυνατότητες αυτές μπορούν να εκτείνονται σε όλο το φάσμα του "κλάδου της εμπιστοσύνης". Εκεί φυσικά εντάσσουμε οποιαδήποτε κυβερνητική αρχή ή επιχείρηση στηρίζεται στην αξιοπιστία για την διεκπεραίωση συναλλαγών και άλλων δραστηριοτήτων. Ανάμεσά τους, τα χρηματοπιστωτικά ιδρύματα, εταιρείες εκκαθάρισης και κρατικές υπηρεσίες. Οι εξελίξεις δεν είναι απαραίτητο να είναι αρνητικές για τον προαναφερθέντα κλάδο, καθώς τα ιδρύματα, οι επιχειρήσεις και οι υπηρεσίες θα μπορούν να υιοθετήσουν και ενδεχομένως να προσαρμόσουν τις τεχνολογικές εξελίξεις στις ανάγκες τους. Άλλωστε, σε μία εποχή αμφισβήτησης της αξιοπιστίας τους, η απαλλαγή από την ανάγκη ύπαρξης εμπιστοσύνης και η αύξηση της διαφάνειας δεν σημαίνει απαραιτήτως κάτι το κακό. Παραδείγματος χάριν, τα χρηματοπιστωτικά ιδρύματα μπορούν να ωφεληθούν από την τήρηση μίας μονάχα blockchain αντί μίας σειράς εσωτερικών ισολογιστικών βιβλίων. Η δημιουργία απαραβίαστων δημοσίων βάσεων δεδομένων είναι κάτι που όχι μόνο μπορεί να αντιμετωπίσει την κρατική διαφθορά αλλά μπορεί να μειώσει θεαματικά το κόστος τήρησής τους και να αυξήσει την αποδοτικότητα[89] όπως και την διαφάνεια.

Η διαπίστωση ότι αποκεντρωμένα συστήματα τήρησης μητρώων μπορούν να είναι εξίσου αξιόπιστα με κεντρικά διαχειριζόμενα, μπορεί να επιφέρει ριζικές αλλαγές. Ένας κόσμος με μαθηματικώς ανοσοποιημένη σε πράξεις χειραγώγησης τήρηση αρχείων θα έχει πολλαπλά οφέλη. Ο τρόπος με τον οποίο συνεργάζονται άνθρωποι κι επιχειρήσεις μπορεί να μεταβληθεί ριζικά. Οι δυνατότητες είναι μεγάλες και αναλογιζόμενοι το νεαρό της ηλικίας της τεχνολογίας, είναι αρκετά πιθανό να χρειαστούν αρκετά χρόνια ακόμα πριν καταστεί σαφής η πλήρης δυναμική της. Η επανάστασή της δεν θα έρθει εν μία νυκτί.[90]

## 3.4 Το Bitcoin στην Ελλάδα των capital controls

Τα bitcoin, όπως έχουμε αναφέρει, μεταφέρονται από άτομο σε άτομο μέσω του διαδικτύου χωρίς να μεσολαβεί κάποια τράπεζα ή άλλος διαμεσολαβητής. Έτσι, μπορούν να χρησιμοποιηθούν παντού στον κόσμο δίχως να υπάρχει η δυνατότητα επιβολής περιορισμών ενώ ο λογαριασμός του χρήστη είναι αδύνατον να "παγώσει". Η αποκεντρωμένη φύση του νομίσματος με την αδυναμία επιβολής ελέγχων από οποιαδήποτε κεντρική τράπεζα ή άλλη αρχή και η ψευδωνυμία βάσει της οποίας λειτουργεί, του προσδίδει εξαιρετικά χαρακτηριστικά εναλλακτικής οδού εν μέσω κεφαλαιακών ελέγχων με την παράλληλη δυνατότητα αποφυγής νομικών αντιποίνων για τα άτομα που το χρησιμοποιούν.

Η επιβολή κεφαλαιακών ελέγχων στην Ελλάδα της κρίσης τον Ιούλιο του 2015 αποτέλεσε ευκαιρία για την ενημέρωση του ελληνικού κοινού για την ύπαρξη και τις δυνατότητες εναλλακτικών ή/και παράλληλων

[88] πχ http://krugman.blogs.nytimes.com/2013/12/28/bitcoin-is-evil/?_r=0
[89] http://www.coindesk.com/can-blockchain-technology-stem-government-corruption/
[90] Much more than digital cash, The Economist, 8/01/2015, http://www.economist.com/news/business-books-quarterly/21638093-rise-and-fall-crypto-currency-good-news-authors-least-much

νομισμάτων, όπως το Bitcoin. Από την παροχή δυνατότητας πληρωμής με το εν λόγω κρυπτονόμισμα σε εστιατόρια[91] έως την εμφάνιση ιστοσελίδων, εταιρειών αλλά και ATM[92], και διεξαγωγή εκδηλώσεων με κεντρικό θέμα το ίδιο,[93] οι εγχώριες εξελίξεις στον χώρο του Bitcoin έχουν υπάρξει πρωτοφανώς καταιγιστικές. Μάλιστα φημολογείται η εγκατάσταση 1,000 Bitcoin ATM.[94]

Η χρήση του νομίσματος έχει διευκολύνει αρκετές επιχειρήσεις στις συναλλαγές τους με το εξωτερικό, για αγορά π.χ. πρώτων υλών κι άλλων εισαγόμενων ειδών, δίνοντας τους την δυνατότητα να παρακάμπτουν τους κεφαλαιακούς ελέγχους που επέβαλε η ελληνική κυβέρνηση. Παρ' όλα αυτά, κάποιοι περιορισμοί παραμένουν καθώς οι επιχειρήσεις που προσφέρουν τις υπηρεσίες συναλλαγών σε bitcoin, θέτουν όρια στις συναλλαγές με τους πελάτες τους σε μία προσπάθεια να ελέγξουν την ζήτηση καθώς αφ' ενός μεν φοβούνται κούρεμα των ιδίων τους καταθέσεων κι αφ' ετέρου δεν επιθυμούν να υπερεκτεθούν οι ίδιοι στο bitcoin. Ρυθμιστικά λειτουργεί και η προμήθεια που επιβάλλεται σε κάθε κατάθεση.

Μαζί με τις διευκολύνσεις όμως που παρέχονται στις επιχειρήσεις από τις δυνατότητες χρήσης του εναλλακτικού αυτού μέσου πληρωμής, παρουσιάζονται και προβλήματα τόσο για το κράτος όσο και για τις τράπεζες. Η αβεβαιότητα που κυριαρχεί ως προς την ασφάλεια των καταθέσεων, μπορεί εύκολα να οδηγήσει σε μεταφορά αποταμιεύσεων από τις τράπεζες σε κάποιο Bitcoin πορτοφόλι, εξασθενώντας τις ακόμα περισσότερο κι εάν το Bitcoin γινόταν ευρέως αποδεκτό, θα κλονίζονταν περαιτέρω. Ακόμα, η απουσία οποιουδήποτε επώνυμου μητρώου καταθέσεων ή συναλλαγών ανοίγει τον δρόμο και διευκολύνει την φοροδιαφυγή και την φυγάδευση κεφαλαίων στο εξωτερικό. Μία ενδεχόμενη απαίτηση όμως από την ελληνική κυβέρνηση δημιουργίας τέτοιου είδους μητρώου θα καθιστούσε ένα από τα βασικά στοιχεία προώθησής του -την ημιανωνυμία/ψευδωνυμία-, άκυρο και θα οδηγούσε τους χρήστες του σε αναζήτηση άλλων λύσεων.[95] Αξίζει πάντως να αναφερθεί πως τα χρηματιστήρια δεν χρειάζονται άδεια λειτουργίας από την Τράπεζα της Ελλάδος, καθώς καμία διάσταση του ψηφιακού νομίσματος δεν ρυθμίζεται από τις αρχές της χώρας.[96] Τέλος, μία ακόμα προβληματική πτυχή του ζητήματος, αφορά τις εγχώριες πληρωμές των επιχειρήσεων καθώς το κρυπτονόμισμα δεν τροφοδοτεί με ρευστότητα το εσωτερικό της ελληνικής αγοράς.[97]

---

[91] http://www.kathimerini.gr/824573/article/epikairothta/ellada/gardoympakia-kai-mpiftekia-me-bitcoins

[92] http://www.kathimerini.gr/822812/article/oikonomia/ellhnikh-oikonomia/ay3hsh-synallagwn-me-bitcoin-eferan-ta-capital-controls

[93] http://gr.pcmag.com/chainthon/18701/news/chainthon-to-1o-blockchain-bitcoin-hackathon-sten και http://insidebitcoins.com/news/october-17-the-first-blockchain-hackathon-in-greece/35347

[94] http://cointelegraph.com/news/115143/greece-to-receive-1000-bitcoin-atms-as-trust-in-banks-long-gone και http://www.businessinsider.com/greece-to-install-1000-bitcoin-atms-2015-8 και http://www.cnbc.com/2015/08/19/greece-could-soon-get-1000-bitcoin-atms.html

[95] "Greece's Bitcoin Debacle: Lying, Cheating, and Corruption", Dent Research Team of Analysts/ Dent Research, on FXSTREET The Forex Market, δημοσιεύτηκε στις 20/10/2015, 22:29. Ανακτήθηκε στις 1/11/2015 http://www.fxstreet.com/analysis/how-to-survive-prosper-through-economic-trends/2015/10/20/02/

[96] http://www.kathimerini.gr/822812/article/oikonomia/ellhnikh-oikonomia/ay3hsh-synallagwn-me-bitcoin-eferan-ta-capital-controls

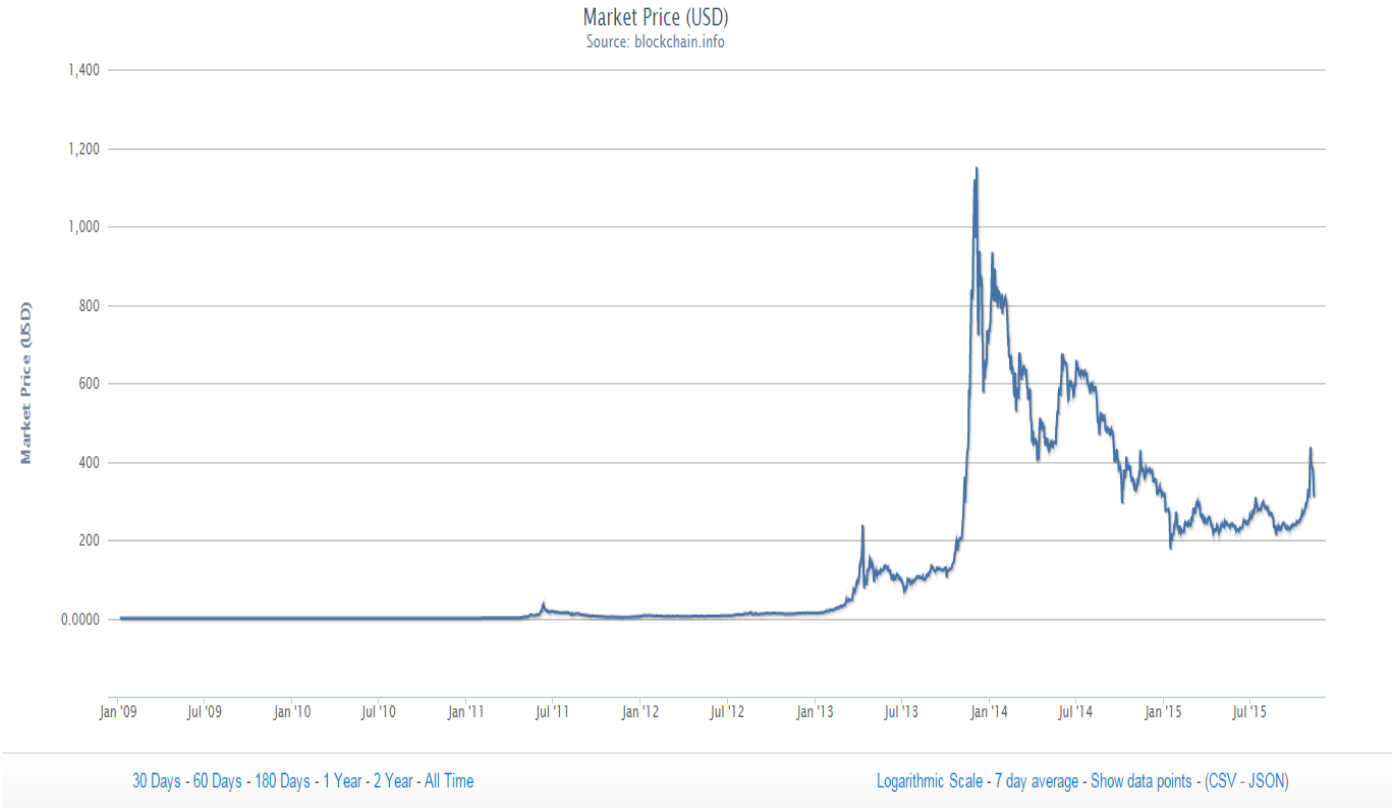
[97] http://www.newsbeast.gr/financial/arthro/1989979/oli-i-alithia-gia-ta-bitcoins

Ενδιαφέρον παρουσιάζει η σύνδεση από πολλούς μιας αυξομείωσης της τιμής του Bitcoin με την επιβολή capital controls και την συμφωνία που επετεύχθη με τους ευρωπαίους εταίρους και η ανάδυση θεωριών που θέλουν το Bitcoin ως ένα ασφαλές καταφύγιο περιουσιακών στοιχείων σε περιόδους οικονομικής αναταραχής,. Τον Ιούλιο του 2015, τα κέρδη του Bitcoin επιταχύνθηκαν, ιδιαίτερα κατά τις τελευταίες ημέρες διαπραγμάτευσης μεταξύ της Ελλάδας και της ευρωζώνης όπου η έξοδος της πρώτης από το ευρώ διαφαινόταν σχεδόν βέβαιη, ενώ η τιμή του κατέρρευσε με την επίτευξη της συμφωνίας.[98] Η διασύνδεση των δύο γεγονότων δεν μπορεί να γίνει εκ του ασφαλούς, καθώς κοινές σχέσεις είχαν εντοπιστεί και κατά την χρηματοπιστωτική κρίση στην Κύπρο το 2013, όταν η τιμή του Bitcoin είχε φτάσει στο αποκορύφωμά της. Τότε, βέβαια, είχε συντρέξει και μία εξαιρετικά μεγάλη εισροή κεφαλαίων από το Silicon Valley των ΗΠΑ.[99] Επίσης, λόγος έγινε για θεαματική αύξηση στους έλληνες χρήστες του Bitcoin όμως όποιο ποσοστό αύξησης και να παρατηρήθηκε, μικρή σημασία έχει εάν ο αριθμός χρηστών ήταν αρχικώς πολύ χαμηλός. Επιπλέον, η αύξηση της τιμής του μπορεί να αποδοθεί σε επιχειρήσεις όπως η Coinbase, που σε μία προσπάθεια να ενθαρρύνουν τις αγορές bitcoin, μηδένισαν τα τέλη συναλλαγών τους. Το Bitcoin εξακολουθεί να παραμένει ένα ιδιαίτερα ευμετάβλητο ψηφιακό νόμισμα που πυροδοτεί, γοητεύει κι αιχμαλωτίζει την προσοχή τόσο σκεπτικιστών όσο και λατρών του.[100]

## 3.5 Διασύνδεση τιμής και γεγονότων[101]

Η τιμή του Bitcoin, παρότι εμφανίζεται ως η σταθερότερη μεταξύ των κρυπτονομισμάτων, παραμένει ευμετάβλητη. Τα περιορισμένα έτη ζωής των κρυπτονομισμάτων και το συνεχώς μεταβαλλόμενο τεχνολογικό και μη τοπίο διατηρούν τον χαρακτήρα της επένδυσης σε ένα υψηλού ρίσκου επίπεδο. Πολλοί παράγοντες είναι αυτοί που μπορούν να επηρεάσουν την αξία του ψηφιακού νομίσματος. Μεταξύ τους συγκαταλέγονται το (αβέβαιο) νομικό καθεστώς του, οι περιορισμοί των ελέγχων κεφαλαίου, η δημοτικότητά του στα μέσα ενημέρωσης και στο διαδίκτυο και η συσχέτισή του με εγκληματικές/παράνομες πράξεις/ενέργειες.

[98] http://www.financemagnates.com/cryptocurrency/trading/bitcoin-price-returns-to-300/
[99] http://www.theguardian.com/technology/2015/jun/29/bitcoin-fans-eye-potential-in-greek-crisis
[100] http://www.coindesk.com/bitcoin-price-surpasses-300-drops-after-greek-bailout/
[101] https://bitcoinhelp.net/know/more/price-chart-history




Παραπάνω απεικονίζεται η πορεία της τιμής του Bitcoin από την ημέρα δημιουργίας του έως τις 11/11/2015. Στις απαρχές του εν λόγω κρυπτονομίσματος, από την γένεση του πρώτου block της blockchain με την καταγραφή της πρώτης συναλλαγής σε bitcoin, η τιμή του βρισκόταν σε απειροελάχιστα χαμηλά επίπεδα, αξίζοντας τα 0,00076 δολάρια. Ύστερα από μία σειρά γεγονότων, όπως η δημοσίευση της πρώτης συναλλαγματικής ισοτιμίας στις 05/10/2009, η πρώτη συναλλαγή του έναντι πραγματικών χρημάτων αναγκαστικής κυκλοφορίας (fiat) στις 12/10/2009, η πρώτη αγορά προϊόντος στις 11/07/2011, φτάνουμε στο πρώτο spike στην τιμή του Bitcoin, στα 31 δολάρια, έπειτα από την δημοσίευση άρθρου αναφορικά με το Silk Road στις 01/06/2011 και την διαπίστωση από το κοινό της χρησιμότητας του απολύτως μοναδικά ξεχωριστού χαρακτηριστικού που ενέχει το κρυπτονόμισμα, της ανωνυμίας. Η τιμή του έπειτα φάνηκε να σταθεροποιείται στα 17 περίπου δολάρια έως ότου υπήρξε επίθεση hacking σε ένα από τα πρώτα και μεγαλύτερα χρηματιστήρια του νομίσματος. Η διαπραγμάτευση στο συγκεκριμένο χρηματιστήριο διακόπηκε για 7 ημέρες για την επανασφάλιση των συστημάτων του ενώ την ίδια τακτική υπό τον φόβο νέας επίθεσης ακολούθησαν ακόμα δύο μεγάλα χρηματιστήρια. Η τιμή του έπεσε κάτω από τα 5 δολάρια και παρέμεινε εκεί για σχεδόν ένα έτος.

Έπειτα, το bitcoin μπήκε σε μία δυναμικά ανοδική πορεία, ξεπερνώντας αρνητικά γεγονότα όπως το ponzi scheme του pirate40, την ημέρα της πρώτης μείωσης κατά το ήμισυ της αμοιβής των miners, ένα bug που αντιμετωπίστηκε μέσω της ταχείας κι συντονισμένης αντίδρασης των προγραμματιστών, των miner και των μελών της κοινότητας και φτάνοντας να αγγίζει τα $260 εν μέσω της Κυπριακής χρηματοπιστωτικής κρίσης. Όπως αναφέρεται όμως και στο κεφάλαιο περί του Bitcoin στην Ελλάδα των capital controls, η

διασύνδεση της χρηματοπιστωτικής κρίσης της Κύπρου με την θεαματική άνοδο της τιμής δεν μπορεί να γίνει εκ τους ασφαλούς καθώς είχε συντρέξει μία εξαιρετική μεγάλη εισροή κεφαλαίων από την Silicon Valley των ΗΠΑ.

Η τιμή φάνηκε να σταθεροποιείται στα $130 από τον Μάρτιο έως τον Οκτώβριο του 2013, με μία μικρή εξαίρεση τον Απρίλιο όπου η αυξημένη εισροή επιχειρήσεων στα χρηματιστήρια του Bitcoin οδήγησε την τιμή στα $180 μέχρι που υπερφορτώθηκαν οι servers του μεγαλύτερου χρηματιστηρίου δημιουργώντας προβλήματα στην ολοκλήρωση των συναλλαγών και πανικοβάλλοντας χρήστες και επενδυτές και ρίχνοντας ξανά την τιμή στα περίπου $125. Έπειτα από την σύλληψη του "Dread Pirate Rob" ή κατά κόσμον Ross Ulbricht από το FBI[102], του φερόμενου ως ιδρυτή και διαχειριστή του Silk Road, της ανώνυμης διαδικτυακής αγοράς παράνομων προϊόντων που είχε το bitcoin ως την μοναδική αποδεκτή μορφή νομίσματος, το κρυπτονόμισμα μπήκε σε τροχιά εκτίναξης της τιμής του, φτάνοντας τα $685,75 πριν η συζήτηση μίας ειδικής κυβερνητικής επιτροπής των ΗΠΑ καταλήγοντας στο συμπέρασμα πως το Bitcoin είναι πολλά υποσχόμενο και πως η καινοτομία του δεν πρέπει να παρεμποδιστεί εκτοξεύσει την τιμή του πάνω από τα $1,000. Σε αυτό συνέβαλλε φυσικά και η δήλωση της Κεντρικής Τράπεζας της Κίνας ότι δεν υπάρχει θέμα όσον αφορά την ελευθερία συμμετοχής στην αγορά του Bitcoin και ότι θα υιοθετείτο μία μακροπρόθεσμη σκοπιά αναφορικά με το νόμισμα, αφού στην χώρα επικρατούν περιορισμοί ελέγχου κεφαλαίων.

Μετά το peak της τιμής στα $1,242, η φούσκα ξεκίνησε να σκάει. Στις 05/12/2013, η κινεζική κυβέρνηση απαγορεύει την χρήση του Bitcoin από τα χρηματοπιστωτική ιδρύματα. Στις 07/02/2014 τρία από τα μεγαλύτερα χρηματιστήρια του κρυπτονομίσματος χτυπώνται από DDoS[103] επιθέσεις. Στις 24/02/2014 το πρώτο χρηματιστήριο που είχε ανοίξει, τερματίζει απότομα την λειτουργία του λόγω κακοδιαχείρισης έπειτα από φημολογούμενη απώλεια 744,000 BTC. Συνεχίζοντας τα αλλεπάλληλα χτυπήματα που δέχθηκε το κρυπτονόμισμα, στις 26/03/2014 η αμερικάνικη εφορία χαρακτηρίζει το bitcoin ιδιοκτησία κι όχι νόμισμα, φτάνοντας την τιμή του στα $453,05 ενώ οι πιέσεις της ΚΤ της Κίνας οδηγεί 15 ημέρες αργότερα κινεζικές τράπεζες να εκδώσουν προθεσμία κλεισίματος λογαριασμών χρηματιστηρίων bitcoin, φτάνοντας την τιμή του Bitcoin στα $408. Η εύρεση εμφανών νομοθετικών κενών στο ρυθμιστικό πλαίσιο όμως, οδηγεί σύντομα στην υιοθέτησή τους από τα κινεζικά χρηματιστήρια επαναφέροντας την τιμή στα $500.

Έχοντας -η τιμή του Bitcoin- μέχρι τον Ιούνιο του 2014 φτάσει τα 600 σχεδόν δολάρια, και μένοντας ουσιαστικά ανεπηρέαστη από την μίνι κρίση όταν ένα mining pool λίγο έλλειψε να αγγίξει το όριο του 51% πριν κάποιοι από τους miners αναζητήσουν εναλλακτικά pools, το επόμενο σημαντικό γεγονός που την

[102] http://www.theguardian.com/technology/2015/may/29/silk-road-ross-ulbricht-sentenced

[103] Distributed Denial-of-Service: "tying both willing and unwilling (via trojan virus) computers into giant “botnets” that launch rapid-fire connection requests against a targeted web server. Because websites can accommodate only so many visitors at once, this leads to service interruption and can occasionally cause physical damage to server equipment." http://foreignpolicy.com/2015/11/13/anonymous-hackers-islamic-state-isis-chan-online-war/?utm_content=buffer07f11&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer

επηρέασε ήταν η δημοπράτηση 29,656 νομισμάτων από την US Marshals Υπηρεσία που τα είχε κατασχέσει από το Silk Road. Η τιμή άγγιξε τα $662 πριν ξεκινήσει να πέφτει και πάλι με τον σημαντικότερο αναγνωρισμένο λόγο να αποτελεί η ανακοίνωση του νέου καθεστώτος χορήγησης αδειών "BitLicense" της πολιτείας της Νέας Υόρκης.

Η καθοδική πορεία συνεχίστηκε μέχρι τις αρχές του 2015 οπότε κι έγινε επίθεση hacking στο ηλεκτρονικό πορτοφόλι του BitStamp, οδηγώντας σε κατάρρευση της τιμής στα $198,59. Από το τέλος του Ιανουαρίου έως και τον Ιούνιο του 2015, η τιμή διατηρείτο σταθερή στο 225-240 δολάρια. Κατόπιν, επήλθε σχετικά απότομη αυξομείωση, αγγίζοντας τα $291,66 έπειτα από ομολογία ενοχής δύο ομοσπονδιακών πρακτόρων του FBI για κλοπή Bitcoin για προσωπικό κέρδος κατά την διάρκεια της έρευνας για το Silk Road και πέφτοντας στα $214,30 μετά την κυκλοφορία του Bitcoin XT από δύο από τους βασικούς προγραμματιστές του κρυπτονομίσματος. Το Bitcoin XT αποτελεί ένα εναλλακτικό προς το Bitcoin client λογισμικό που διαφέρει προς το πρωτότυπο ως προς το μέγεθος των block, προτείνοντας ένα αυξητικά μεταβαλλόμενο σε προβλέψιμο ρυθμό ανώτατο όριο μεγέθους block σε αντιδιαστολή προς το υπάρχον σταθερό ανώτατο όριο του ενός megabyte. Το Bitcoin XT αποτέλεσε το αποκορύφωμα της διένεξης μεταξύ των βασικών προγραμματιστών επί του θέματος ενώ η κοινότητα φοβάται πως εφόσον δεν υπάρξει συναίνεση σχετικά με το ζήτημα, η δημιουργία εναλλακτικής blockchain μπορεί να καταλήξει σε δύο εντελώς ξεχωριστές εκδόσεις στο παγκόσμιο δημόσιο βιβλίο ισολογισμού του Bitcoin.

Στο τέλος του Ιουλίου του 2015, όταν ακόμα διαφαινόταν πιθανή μία έξοδος της Ελλάδας από το ευρώ, η τιμή του κινήθηκε ανοδικά αλλά με την επίτευξη της συμφωνίας η τιμή έπεσε εκ νέου. Στις 22/10/2015, το Δικαστήριο των Ευρωπαϊκών Κοινοτήτων εξέδωσε απόφαση που απαλλάσσει τις συναλλαγές πραγματικού νομίσματος με ψηφιακό από φόρους προστιθέμενης αξίας, επηρεάζοντας θετικά την τιμή του Bitcoin, η οποία έφτασε τα $318,43. Η εμφάνισή του στο πρωτοσέλιδο του περιοδικού The Economist στις 31/10/2015 οδήγησε σε νέα άνοδο ενώ την πρώτη εβδομάδα του Νοεμβρίου ξεπέρασε τα $450[104] για πρώτη φορά ύστερα από ένα σχεδόν έτος. Η ευφορία φυσικά δεν διήρκεσε πολύ με την τιμή να έχει επανέλθει στα 330 περίπου δολάρια την ώρα συγγραφής.[105] Ενδιαφέρον παρουσιάζει πάντως το γεγονός πως πολλοί αναμένουν ότι η τιμή θα ξεπεράσει τα $500 έως το 2016.[106]

[104] http://www.coindesk.com/bitcoin-hits-450-for-the-first-in-2015/
[105] 17/11/2015, σύμφωνα με το http://www.coindesk.com/price/
[106] http://www.coindesk.com/poll-48-percet-bitcoin-price-500-2016/

## ΕΠΙΛΟΓΟΣ

Περιγράψαμε λοιπόν με τον κατά δύναμιν απλούστερο τρόπο την λειτουργία του Bitcoin. Παρουσιάσαμε τα στοιχεία που το συνθέτουν, τις δυνατότητές του, τις επιπτώσεις που μπορεί να έχει και τις προκλήσεις που μπορεί να θέσει. Η δυναμική και η αξία του Bitcoin είναι αδιαμφισβήτητες. Τόσο το κρυπτονόμισμα το ίδιο αλλά πολύ περισσότερο η τεχνολογία της blockchain που κρύβει από πίσω του, παρουσιάζουν τρομακτικά μεγάλες δυνατότητες. Η τεχνολογία, όπως έχει δείξει πολλές φορές στο παρελθόν, έχει την δύναμη να αλλάξει ριζικά την ζωή μας. Κανείς δεν μπορεί να είναι βέβαιος για το πού θα οδηγηθούμε στο μέλλον, ούτε καν σε βραχυπρόθεσμο ορίζοντα. Εάν αυτό θα είναι σε μία ελαφρώς βελτιωμένη εκδοχή της σύγχρονης ζωής μας όπως την γνωρίζουμε ή εάν θα βρεθούμε ξαφνικά σε ένα εντελώς νέο τοπίο εκμεταλλευόμενοι τις καινοτόμες ιδέες στην πλήρη τους δυνατότητα. Ο τρόπος με τον οποίο θα διαχειριστούν οι ρυθμιστικές αρχές το ζήτημα χρειάζεται μεγάλη προσοχή, καθώς η υπερρύθμισή του μπορεί να έχει αρνητικά αποτελέσματα για την πρόοδο και περαιτέρω ανάπτυξη της καινοτόμου αυτής τεχνολογίας.

Όσον αφορά το ίδιο το Bitcoin, αυτό μπορεί να αποτελέσει βασικό ρόλο στο μέλλον, μπορεί και όχι. Μπορεί να παραμεριστεί από κάποιο Altcoin που θα προσφέρει δυνατότητες που αυτό δεν προσφέρει. Οι τόσο ραγδαίες εξελίξεις και το ευμετάβλητο του τοπίο, δεν αφήνουν χώρο για βεβαιότητες. Το μόνο σίγουρο είναι ότι "όποιος και να είναι κι όπου κι εάν βρίσκεται ο κύριος Nakamoto, μπορεί να είναι υπερήφανος για την εξαπόλυση ενός κύματος χρηματοπιστωτικής καινοτομίας και την ίδρυση ενός -απ' ότι φαίνεται- σημαντικού νέου κλάδου στην παγκόσμια βιομηχανία της τεχνολογίας της πληροφορίας."[107]

Κλείνοντας, μία φράση του Leon C. Megginson: "It is not the strongest of the species that survives, nor the most intelligent that survives. It is the one that is most adaptable to change."[108]

[107] http://www.economist.com/news/business/21638124-minting-digital-currency-has-become-big-ruthlessly-competitive-business-magic

[108] http://quoteinvestigator.com/2014/05/04/adapt/#more-8823

# ΒΙΒΛΙΟΓΡΑΦΙΑ

## Βιβλία


Cannan, Edwin, Collected Works. *Money: Its connection with rising and falling prices - Modern Currency and the regulation of its value - Economic scares*, Volume VII, Routledge/Thoemmes Press, eighth edition, 1997

Ferguson, Niall, *Η εξέλιξη του χρήματος: Μία οικονομική ιστορία του κόσμου*, Εκδόσεις Αλεξάνδρεια, 2011, μεταφρασμένο

McAleese, Dermot, "Οικονομική για επιχειρησιακές σπουδές: Ανταγωνισμός, Μακροσταθερότητα και Παγκοσμιοποίηση", Εκδόσεις Τυπωθήτω, 2005, μεταφρασμένο.

Smith, Adam, *Έρευνα για τη φύση και τις αιτίες του πλούτου των εθνών*, Εκδόσεις Ελληνικά Γράμματα, 2010, μεταφρασμένο

Soete, Luc & ter Well, Bas, (editors), *The economics of the digital society*, Edward Elgar Publishing, Cheltenham, UK - Northampton, MA, USA, 2005


## Διαδικτυακές πηγές


Andersson, Mattias, *Beskattning av digitala valutor: Bitcoin och liknande företeelser*, Uppsala Universitet, 2014, [pdf] https://www.diva-portal.org/smash/get/diva2:699860/FULLTEXT01.pdf

Azotic, ELI5: bitcoin mining (xpost in ELI5), *Reddit r/bitcoin*, 18/02/2013, https://www.reddit.com/r/Bitcoin/comments/18q2jx/eli5_bitcoin_mining_xpost_in_eli5/

Bajpai Prableen, Countries where Bitcoin is legal and illegal, 06/05/2015, *Investopedia*, http://www.investopedia.com/articles/forex/041515/countries-where-bitcoin-legal-illegal.asp

Barnato Katy, Greece could soon get 1000 bitcoin ATMs, 19/08/2015, *CNBC*, http://www.cnbc.com/2015/08/19/greece-could-soon-get-1000-bitcoin-atms.html

Bartunek Robert-Jan, Bitcoin currency exchange not liable for VAT taxes: top EU court, *Reuters*, 22/10/2015, http://www.reuters.com/article/2015/10/22/us-bitcoin-tax-eu-idUSKCN0SG0X920151022

Basiladze George, Bitcoin's twisty trek toward adoption in Russia, 27/09/2015, *Finance Magnates*, http://www.financemagnates.com/cryptocurrency/bloggers/bitcoins-twisty-trek-toward-adoption-in-russia/

Beigel Ofil, Accessing the Darknet in under 2 minutes - Beginner's guide, 12/10/2015, *99Bitcoins*, https://99bitcoins.com/accessing-dark-net-under-minutes-beginners-guide/

Beigel Ofil, How to generate bitcoins from your home computer, 28/05/2015, *99Bitcoins*, https://99bitcoins.com/how-to-generate-bitcoins-from-your-home-computer/

Beigel Ofil, What are Altcoins, 30/01/2014, *99Bitcoins*, https://99bitcoins.com/altcoins/

Beigel Ofil, What is a Bitcoin Wallet, 29/01/2014, *99Bitcoins*, https://99bitcoins.com/what-is-a-bitcoin-wallet/

Beigel Ofil, What is Bitcoin, 21/01/2014, *99Bitcoins*, https://99bitcoins.com/what-is-bitcoin-for-dummies/

Beigel Ofil, What is Feathercoin, 27/01/2014, *99Bitcoins*, https://99bitcoins.com/feathercoin/

Beigel Ofir, Bitcoin Explained in 3:30 minutes, 10/11/2013, *99Bitcoins*, https://99bitcoins.com/bitcoin-explained-in-330-minutes/

Beigel Ofir, Explain a Bitcoin hash to me like I'm five, 15/11/2014, *99Bitcoins*, https://99bitcoins.com/what-is-bitcoin-hash/

Beigel Ofir, Is Bitcoin actually anonymous?, 22/10/2014, *99Bitcoins*, https://99bitcoins.com/bitcoin-actually-anonymous/

Beigel Ofir, Is Bitcoin Safe? Yes. It's you I'm not so sure about, 4/12/2014, *99Bitcoins*, https://99bitcoins.com/is-bitcoin-safe/

Beigel Ofir, What Bitcoin is for grandmas, 7/10/2014, *99Bitcoins*, https://99bitcoins.com/bitcoin-grandmas/

Beigel Ofir, What is Bitcoin mining, 3/02/2014, *99Bitcoins*, https://99bitcoins.com/what-is-bitcoin-mining/

Bie Nanok, Bitcoin-guide: så gör du, *SVTNyheter*, 27/11/2013, http://www.svt.se/nyheter/inrikes/bitcoin-guide-sa-gor-du

Bitcoin Regulation Report, *CoinDesk*, 3/3/2015, http://www.coindesk.com/research/regulation-report/

Bitcoin χρησιμοποιεί το "Ισλαμικό Κράτος", *Η Καθημερινή*, 22/09/2015, http://www.kathimerini.gr/831795/article/oikonomia/die8nhs-oikonomia/bitcoin-xrhsimopoiei-to-islamiko-kratos

Bodoni Stephanie & Thomson Amy, EU's top court rules that Bitcoin Exchange is tax-free, 22/10/2015, Bloomberg, http://www.bloomberg.com/news/articles/2015-10-22/bitcoin-virtual-currency-exchange-is-tax-free-eu-court-says-ig21wzcd

Booker Brian, Bitcoin as a commodity: License to tax?, 28/11/2015, 99Bitcoins, https://99bitcoins.com/bitcoin-as-a-commodity-license-to-tax/

Bradbury Danny, How dangerous is Satoshi Nakamoto?, 23/11/2014, CoinDesk, http://www.coindesk.com/dangerous-satoshi-nakamoto/

Brett Scott, The visions of a techno-leviathan: The politics of the Bitcoin Blockchain, 01/06/2014, E-International Relations, http://www.e-ir.info/2014/06/01/visions-of-a-techno-leviathan-the-politics-of-the-bitcoin-blockchain/

Carney Michael, With $130M of bitcoin wealth and plans to sell, the FBI could create the virtual currency cage, Pando, 2/01/2014, https://pando.com/2014/01/02/with-130m-of-bitcoin-wealth-and-plans-to-sell-the-fbi-could-rattle-the-virtual-currency-cage/

Cawrey Daniel, FBI proves seizing bitcoins isn't the same as owning them, CoinDesk, 30/10/2013, http://www.coindesk.com/fbi-proves-seizing-bitcoins-isnt-owning/

Cawrey Daniel, What are Bitcoin nodes and why do we need them?, 9/5/2014, CoinDesk, http://www.coindesk.com/bitcoin-nodes-need/

Chokun Jonas, Who accepts bitcoins as payment? List of companies, stores, shops, BitcoinValues.net, 19/02/2014, http://www.bitcoinvalues.net/who-accepts-bitcoins-payment-companies-stores-take-bitcoins.html

Crash course, The Economist, 07/09/2013, http://www.economist.com/news/schoolsbrief/21584534-effects-financial-crisis-are-still-being-felt-five-years-article

Cuthbertson Anthony, Greece is planning to install 1000 bitcoin ATMs, 19/08/2015, Business Insider, http://www.businessinsider.com/greece-to-install-1000-bitcoin-atms-2015-8

Darwish Muhammad, Greece's cash crisis is Bitcoin's boost, 8/07/2015, *BloombergBusiness*, http://www.bloomberg.com/news/articles/2015-07-08/greece-s-cash-crisis-is-bitcoin-s-boost-ibuhh68t

Das Samburaj, Bitcoin declared illegal in Taiwan, 02/11/2015, https://www.cryptocoinsnews.com/bitcoin-declared-illegal-in-taiwan/

De Geer Christoffer, Bitcoin may change our world in ways as profound as the internet, 21/10/2015, The Street, http://www.thestreet.com/story/13319579/1/bitcoin-may-change-our-world-in-ways-as-profound-as-the-internet.html

Dent Research Team of Analysts, Greece's Bitcoin Debacle: Lying, Cheating, and Corruption, 20/10/2015, FXStreet, http://www.fxstreet.com/analysis/how-to-survive-prosper-through-economic-trends/2015/10/20/02/

Driscoll Scott, How Bitcoin works under the hood, *Imponderable Things* (blog), 14/07/2013, http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html#more

Driscoll Scott, The essence of how Bitcoin works, Imponderable Things (blog), 6/11/2014, http://webcache.googleusercontent.com/search?q=cache:http://www.imponderablethings.com/&gws_rd=cr&ei=7uISVsexIMSyaZTwjpAP

Duivestein Sander & Savalle Patrick, Bitcoin: It's the platform, not the currency, stupid!, TNWNews, 14/02/2014, http://thenextweb.com/insider/2014/02/15/bitcoin-platform-currency/

DuPont Quinn, The politics of cryptography: Bitcoin and the ordering machines, The Journal of Peer Production, http://peerproduction.net/issues/issue-4-value-and-currency/peer-reviewed-articles/the-politics-of-cryptography-bitcoin-and-the-ordering-machines/

European Banking Authority, EBA Opinion on 'virtual currencies', 4/7/2014, [pdf] http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf

European Central Bank, Virtual Currency Schemes, 10/2012, [pdf] http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

FBI is global stakeholder in cryptocurrency, currently owns largest bitcoin wallet, *RT*, 19/12/2013, https://www.rt.com/usa/fbi-owns-largest-bitcoin-wallet-458/

Forking Hell: A spat exposes unwieldy governance at the digital currency, 22/08/2015, *The Economist*, http://www.economist.com/news/business-and-finance/21661404-spat-between-developers-may-split-digital-currency-forking-hell?fsrc=scn%2Ffb%2Fte%2Fpe%2Fed%2Faspatbewteendevelopersmaysplit

Graydon Carter, Pump and dump: Know the signs when trading Altcoins, 09/07/2014, https://www.cryptocoinsnews.com/pump-dump-know-signs-trading-altcoins/

Graydon Carter, What is Bitcoin?, 10/09/2014, https://www.cryptocoinsnews.com/bitcoin/

Graydon Carter, What is cryptocurrency?, 16/09/2014, https://www.cryptocoinsnews.com/cryptocurrency/

Greenberg Andy, FBI says it's seized $28.5 millin in bitcoins from Ross Ulbricht alleged owner of Silk Road, 25/10/2013, *Forbes*, http://www.forbes.com/sites/andygreenberg/2013/10/25/fbi-says-its-seized-20-million-in-bitcoins-from-ross-ulbricht-alleged-owner-of-silk-road/

Gupta Nikhil, How will 2017's block reward halving affect Bitcoin price?, *NEWSBTC*, 13/03/2015, http://www.newsbtc.com/2015/03/13/how-will-2017s-block-reward-halving-affect-bitcoin-price/

Hajdarbegovic Nermin, Bitcoin Miners ditch Ghash.io pool over fears of 51% attack, CoinDesk, 9/1/2014, http://www.coindesk.com/bitcoin-miners-ditch-ghash-io-pool-51-attack/

Hajdarbegovic Nermin, EU banking regulator issues warning on virtual currencies, *CoinDesk*, 13/12/2013, http://www.coindesk.com/eu-banking-regulator-warning-virtual-currencies/

Hern Alex, Bitcoin fans eye potential in Greek crisis, 29/06/2015, The Guardian, http://www.theguardian.com/technology/2015/jun/29/bitcoin-fans-eye-potential-in-greek-crisis

Hern Alex, FBI struggles to seize 600000 bitcoins from alleged Silk Road founder, 7/10/2013, The Guardian, http://www.theguardian.com/technology/2013/oct/07/fbi-bitcoin-silk-road-ross-ulbricht

Higgins Stan, IMF Chief: Banks shouldn't fear Bitcoin or the Blockchain, CoinDesk, 05/11/2015, http://www.coindesk.com/imf-chief-banks-bitcoin-blockchain/

Higgins Stan, No, Satoshi Nakamoto hasn't moved a thing, CoinDesk, 05/08/2015, http://www.coindesk.com/no-satoshi-nakamoto-hasnt-moved-a-thing/

Horwitz Ariel, Bitcoin Whiteboard Tuesday - What is Bitcoin?, 99Bitcoins, 19/10/2015, https://99bitcoins.com/bitcoin-whiteboard-tuesday-what-is-bitcoin/

How Bitcoin mining works, *CoinDesk*, 22/12/2014, http://www.coindesk.com/information/how-bitcoin-mining-works/

How does cloud mining bitcoin work?, Coindesk, http://www.coindesk.com/information/cloud-mining-bitcoin-guide/

How many bitcoins are mined per day?, Bitcoin Forum, 17/12/2013, https://bitcointalk.org/index.php?topic=373844.0

How to calculate mining profitability, CoinDesk, http://www.coindesk.com/information/mining-profitability/

How to set up a Bitcoin miner, 26/11/2013, CoinDesk, http://www.coindesk.com/information/how-to-set-up-a-miner/

Hughes Eric, A cyperphunk's manifesto, 9/03/1993, Satoshi Nakamoto Institute, http://nakamotoinstitute.org/cypherpunk-manifesto/

Inman Phillip, Bitcoin could pose threat to financial stability of UK, warns Bank of England, 11/11/2014, The Guardian, http://www.theguardian.com/technology/2014/sep/11/bitcoin-threat-financial-stability-uk-bank-of-england

Is Bitcoin Legal?, CoinDesk, 19/08/2014, http://www.coindesk.com/information/is-bitcoin-legal/

Keynes John M., Proposal for an International Currency Union, [pdf] http://www.econ.jku.at/members%5CLandesmann%5Cfiles%5CWS08%5C239339%5CDiplomarbeit_Klaffenboeck_zentrale_kapitel.pdf

Krugman Paul, Bitcoin is Evil, *The New York Times*, 28/12/2013, http://krugman.blogs.nytimes.com/2013/12/28/bitcoin-is-evil/?_r=0

Larsen Jacob, 2/3 of all bitcoins have been mined, 1/3 may be lost, 03/2015, CoinBuzz, http://www.coinbuzz.com/2015/03/31/23-bitcoins-mined-13-may-lost/

Lerner Sergio Demian, The well deserved fortune of Satoshi Nakamoto, Bitcoin creator, visionary and genius, Bitsblog, 17/04/2013, https://bitslog.wordpress.com/2013/04/17/the-well-deserved-fortune-of-satoshi-nakamoto/

Maras Elliot, Indian Bank shuts down bitcoin exchange BTCIndia, 08/05/2015, https://www.cryptocoinsnews.com/indian-bank-shuts-bitcoin-exchange-btcxindia/

McMillan Robert, Who owns the world's biggest Bitcoin wallet? The FBI, Wired, 18/12/2013, http://www.wired.com/2013/12/fbi_wallet/

Miedema Douwe, Regulator mulls setting rules for digital currency Bitcoin, Reuters, 6/5/2013, http://www.reuters.com/article/2013/05/06/net-us-bitcoin-regulation-idUSBRE9450Y520130506

Much more than digital cash, The Economist, 8/01/2015, http://www.economist.com/news/business-books-quarterly/21638093-rise-and-fall-crypto-currency-good-news-authors-least-much

Murphy Edward V., Murphy M. Maureen, Seitzinger Michael V., *Bitcoin: Questions, Answers, and Analysis of Legal Issues,* Congressional Research Services, 2015, [pdf] https://www.fas.org/sgp/crs/misc/R43339.pdf

Nakamoto Satoshi, Bitcoin: A peer-to-peer electronic cash system, 31/10/2008, Satoshi Nakamoto Institute, http://nakamotoinstitute.org/bitcoin/

Niloy Mainul Alam, History of Bitcoin: The journey of a virtual currency, 1/11/2015, 99Bitcoins, https://99bitcoins.com/history-of-bitcoin-the-journey-of-a-virtual-currency/

Oconell Justin, Bitcoin ransoms are becoming popular in kidnappings, 29/10/2015, https://www.cryptocoinsnews.com/bitcoin-ransoms-becoming-popular-kidnappings/

Oconell Justin, Bitcoin surges as US marshalls prepare for final Silk Road Bitcoin auction, 3/11/2015, https://www.cryptocoinsnews.com/bitcoin-surges-us-marshalls-hold-final-silk-road-auction/

Parthum Jason, Khan Academy - Bitcoin Course, 26/06/2014, Youtube, https://www.youtube.com/playlist?list=PL73q2zDIiGK_O5OYdK5vxcezzC0zu_3OS

Perez Bello Yessi, Jamie Dimon: Bitcoin will not survive, CoinDesk, 5/11/2015, http://www.coindesk.com/jamie-dimon-bitcoin-will-not-survive/

Perez Yessi Bello, Bitcoin exempt from VAT, rules European Court of Justice, CoinDesk, 22/10/2015, http://www.coindesk.com/bitcoin-is-exempt-from-vat-says-european-court-of-justice/

Perez Yessi Bello, *Bitcoin Price Breaks $400 Amid 12% Surge*, 3/11/2015, CoinDesk, http://www.coindesk.com/bitcoin-price-breaks-400/

Perez Yessi Bello, Bitcoin price hits $450 for the first time in 2015, CoinDesk, 4/11/2015, http://www.coindesk.com/bitcoin-hits-450-for-the-first-in-2015/

Perez Yessi Bello, Bitcoin price surpasses $300, drops after greek bailout, CoinDesk, 13/07/2015, http://www.coindesk.com/bitcoin-price-surpasses-300-drops-after-greek-bailout/

Perez Yessi Bello, How payment giants are embracing Bitcoin and blockchain tech, CoinDesk, 29/10/2015, http://www.coindesk.com/how-payment-giants-are-embracing-bitcoin-and-blockchain/

Perez Yessi Bello, Poll: 48% believe Bitcoin will be worth over $500 by 2016, CoinDesk, 9/11/2015, http://www.coindesk.com/poll-48-percet-bitcoin-price-500-2016/

Perez Yessi Bello, Russia's central bank meets with finance reps for Bitcoin talks, CoinDesk, 12/06/2015, http://www.coindesk.com/russias-central-bank-meets-with-finance-reps-for-bitcoin-talks/

Prisco Giulio, "Pirate@40" arrested for Bitcoin ponzi scam, 07/11/2014, https://www.cryptocoinsnews.com/pirate40-arrested-bitcoin-ponzi-scam/

Prosser Marc, Can blockchain technology stem government corruption?, CoinDesk, 25/10/2015, http://www.coindesk.com/can-blockchain-technology-stem-government-corruption/

Rizzo Pete, Bank of Greece breaks silence on Bitcoin, CoinDesk, 13/02/2014, http://www.coindesk.com/bank-of-greece-breaks-silence-bitcoin/

Rizzo Pete, Bank of Montreal open to rekindling partnerships with Bitcoin businesses, CoinDesk, 2/04/2014, http://www.coindesk.com/bank-montreal-open-rekindling-partnerships-bitcoin-businesses/

Rizzo Pete, Bidder turnout tier all-time low in final Silk Road Bitcoin auction, CoinDesk, 5/11/2015, http://www.coindesk.com/bidder-turnout-low-silk-road-bitcoin-auction/

Rizzo Pete, Bitcoin and Blockchain square off at Money 20/20, CoinDesk, 29/10/2015, http://www.coindesk.com/bitcoin-and-blockchain-square-off-at-money2020/

Rizzo Pete, Bitcoin in the headlines: Blockchain scores Economist cover, CoinDesk, 30/10/2015, http://www.coindesk.com/bitcoin-in-the-headlines-blockchain-scores-economist-cover/

Rizzo Pete, Capital One survey finds blockchain interest growing at Money 20/20, CoinDesk, 29/10/2015, http://www.coindesk.com/capital-one-blockchain-impact-financial-services/

Rizzo Pete, FinCen declares Bitcoin miners, investors aren't money transmitters, CoinDesk, 31/01/2014, http://www.coindesk.com/fincen-bitcoin-miners-investors-money-transmitters/

Rizzo Pete, Genesis trading, binary financial to bid in final Silk Road Bitcoin auction, CoinDesk, 3/11/2015, http://www.coindesk.com/genesis-trading-binary-to-bid-in-final-silk-road-bitcoin-auction/

Rizzo Pete, IRS to tax digital currencies as property, not currency, CoinDesk, 25/03/2014, http://www.coindesk.com/internal-revenue-service-treat-digital-currencies-property/

Rushe Dominic, *Bitcoin to be treated as property instead of currency by IRS*, 25/3/2014, The Guardian http://www.theguardian.com/technology/2014/mar/25/bitcoin-property-currency-irs-rules

Santos Maria, Do you love Bitcoin? Then you must know what a 51 percent attack is, 15/05/2013, 99Bitcoins, https://99bitcoins.com/do-you-love-bitcoins-then-you-must-know-what-a-51-percent-attack-is/

Santos Maria, How does a Bitcoin transaction work?, 19/05/2013, 99Bitcoins, https://99bitcoins.com/how-does-a-bitcoin-transaction-work/

Santos Maria, What's a DDoS attack?, 25/05/2013, 99Bitcoins, https://99bitcoins.com/whats-a-ddos-attack/

Satoshi Nakamoto, Bitcoin v0.1 released, (mail), 8/1/2009, http://www.metzdowd.com/pipermail/cryptography/2009-January/014994.html

Segendorf Björn, *Vad är Bitcoin?,* Sveriges Riksbank, 2014, [pdf] http://www.riksbank.se/Documents/Rapporter/POV/2014/2014_2/rap_pov_artikel_4_1400918_sve.pdf

Skatteverket, Virtuella valutor, https://www.skatteverket.se/privat/skatter/vardepapper/andratillgangar/virtuellavalutor.4.15532c7b1442f256bae11b60.html?q=bitcoin

Smart Evander, Top 10 countries in which Bitcoin is banned, 27/05/2015, CryptoCoinsNews, https://www.cryptocoinsnews.com/top-10-countries-bitcoin-banned/

Smart Evander, Why Bitcoin value vs. the Dollar doesn't matter (and never will), CryptoCoinsNews, 28/09/2014, https://www.cryptocoinsnews.com/why-bitcoin-value-doesnt-matter/

Southurst Jon, FinCen: Bitcoin miners need not register as money transmitters, CoinDesk, 29/12/2013, http://www.coindesk.com/fincen-bitcoin-miners-need-not-register-money-transmitters/

Southurst Jon, Vault of Satoshi gets full money services license for Canada, CoinDesk, 26/03/2014, http://www.coindesk.com/vault-of-satoshi-gets-full-money-services-license-canada/

Spaven Emily, US judge rules bitcoin 'is a currency or form of money', CoinDesk, 7/8/2013, http://www.coindesk.com/us-judge-rules-bitcoin-is-a-currency-or-form-of-money/

Taylor Bryan, A History of Universal Currencies, Global Financial Data, [doc] http://www.singleglobalcurrency.org/documents/ArticlebyBryanTaylorAHistoryofUnivesalCurrencies.doc

Tessier Benoit, 'You can play with your bitcoins but you can't pay with them':Russia may ban cryptocurrencies by 2015, RT, 12/09/2014, https://www.rt.com/business/187440-bitcoin-ban-russia-cryptocurrency/

The Data Team, How do Bitcoin transactions work?, 9/1/2015, The Economist, http://www.economist.com/blogs/graphicdetail/2015/01/daily-chart-3?fsrc=scn/fb/wl/dc/howdobitcointransactionswork

The great chain of being sure about things, The Economist, 31/10/2015, http://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable

The magic of mining, 8/1/2015, The Economist, http://www.economist.com/news/business/21638124-minting-digital-currency-has-become-big-ruthlessly-competitive-business-magic?fsrc=scn/fb/te/pe/ed/magicofmining

The trust machine, The Economist, 31/10/2015, http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine?fsrc=scn/fb/te/pe/ed/thetrustmachine

Thielman Sam, Silk Road operator Ross Ulbricht senteced to life in prison, The Guardian, 29/05/2015, http://www.theguardian.com/technology/2015/may/29/silk-road-ross-ulbricht-sentenced

Top EU court rules that Bitcoin exchange is tax-free in Europe, 22/10/2015, France24, http://www.france24.com/en/20151022-top-eu-court-rules-bitcoin-exchange-tax-free-europe?ns_campaign=reseaux_sociaux&ns_source=twitter&ns_mchannel=social&ns_linkname=editorial&aef_campaign_ref=partage_aef&aef_campaign_date=2015-10-22&dlvrit=66745

What are Bitcoin mining pools, 10/03/2014, CoinDesk, http://www.coindesk.com/information/get-started-mining-pools/

What can you buy with bitcoin?, CoinDesk, 19/10/2015, http://www.coindesk.com/information/what-can-you-buy-with-bitcoins/

What happens when all 21 milling bitcoins have been mined?, 7/1/2013, Reddit r/bitcoin https://www.reddit.com/r/Bitcoin/comments/163kdd/what_happens_when_all_21_million_bitcoins_have/

What is a Satoshi, 30/08/2011, Bitcoin beta Stack Exchange, http://bitcoin.stackexchange.com/questions/114/what-is-a-satoshi

What will happen to mining after the 20999999th Bitcoin?, Bitcoin beta Stack Exchange, 29/12/2014, http://bitcoin.stackexchange.com/questions/5275/what-will-happen-to-mining-after-the-20-999-999th-bitcoin

Who is Satoshi Nakamoto, CoinDesk, 20/05/2015, http://www.coindesk.com/information/who-is-satoshi-nakamoto/

Who is Satoshi Nakamoto, The Economist, 2/11/2015, http://www.economist.com/blogs/economist-explains/2015/11/economist-explains-1?fsrc=scn/fb/wl/ee/st/whoissatoshinakamoto

Will we ever need smaller amounts of Bitcoin than a Satoshi?, 30/08/2011, Bitcoin beta Stack Exchange, http://bitcoin.stackexchange.com/questions/122/will-we-ever-need-smaller-amounts-of-bitcoin-than-a-satoshi

Wilmoth Josiah, What is an Altcoin, 19/09/2014, https://www.cryptocoinsnews.com/altcoin/

Yashu Gola, Russia planning to criminalize bitcoin activities, NEWSBTC, 24/09/2015, http://www.newsbtc.com/2015/09/24/russia-planning-to-criminalize-bitcoin-activities/

Young Joseph, Greece to receive 1000 Bitcoin ATMs as trust in banks 'long gone', 18/08/2015, CoinTelegraph, http://cointelegraph.com/news/115143/greece-to-receive-1000-bitcoin-atms-as-trust-in-banks-long-gone

Αύξηση 57% στην αγορά του bitcoin στην Ελλάδα έφεραν τα capital controls, newmoney.gr, 25/10/2015, http://www.newmoney.gr/palmos-oikonomias/ellada/item/256058-aiksisi-57-stin-agora-tou-bitcoin-stin-ellada-eferan-ta-capital-controls

Γιαννάρου Λίνα, Γαρδουμπάκια και μπιφτέκια με Bitcoins, 22/07/2015, Η Καθημερινή, http://www.kathimerini.gr/824573/article/epikairothta/ellada/gardoympakia-kai-mpiftekia-me-bitcoins

Ενημέρωση για την χρήση εικονικών νομισμάτων, Τράπεζα της Ελλάδος, 11/02/2014, http://www.bankofgreece.gr/Pages/el/Bank/News/Announcements/DispItem.aspx?Item_ID=4517&List_ID=1af869f3-57fb-4de6-b9ae-bdfd83c66c95&Filter_by=AN

Και νέο "άλμα" για το Bitcoin, Capital.gr, 04/11/2015, http://www.capital.gr/story/3078078

Κυρίτσης Άγγελος, Bitcoin Mining: Γιατί δεν είναι πλέον για εμάς.., PC-Steps, 18/01/2014, http://www.pcsteps.gr/13927-bitcoin-mining/

Λαμπίρης Γιώργος, Όλη η αλήθεια για τα bitcoins, Newsbeast, 14/10/2015, http://www.newsbeast.gr/financial/arthro/1989979/oli-i-alithia-gia-ta-bitcoins

Μανδραβέλης Βαγγέλης, Αύξηση συναλλαγών Bitcoin έφεραν τα capital controls, 09/07/2015, Η Καθημερινή, http://www.kathimerini.gr/822812/article/oikonomia/ellhnikh-oikonomia/ay3hsh-synallagwn-me-bitcoin-eferan-ta-capital-controls

https://en.wikipedia.org/wiki/Cryptocurrency

https://bitcoinhelp.net/know/more/price-chart-history

http://bitcoinx.gr/mining-pools/

https://blockchain.info/pools

https://en.wikipedia.org/wiki/Cryptographic_hash_function

http://bitcoinsimplified.org/definitions/

https://bitcoin.org/en/vocabulary

https://en.bitcoin.it/wiki/Altcoin

http://satoshi.nakamotoinstitute.org/

https://en.bitcoin.it/wiki/Block_hashing_algorithm

https://en.bitcoin.it/wiki/Block

https://en.wikipedia.org/wiki/Node_(networking)

https://en.wikipedia.org/wiki/Bitcoin

https://en.bitcoin.it/wiki/Units

https://en.bitcoin.it/wiki/Satoshi_(unit)

https://bitcoin.org/bitcoin.pdf

https://www.bitstamp.net/

https://blockchain.info

https://www.btcgreece.com/

http://coinmarketcap.com/

https://99bitcoins.com/the-best-videos-to-understand-bitcoin/

http://bitcoin.cex.io/is-bitcoin-legal/

https://en.wikipedia.org/wiki/History_of_Bitcoin

https://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country

https://el.wikipedia.org/wiki/%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%B1%CF%86%CE%AF%CE%B1

https://en.wikipedia.org/wiki/Barter

*Όλες οι διαδικτυακές πηγές ήταν διαθέσιμες κατά την ημερομηνία παράδοσης της εργασίας, 18/11/2015

*Πηγές φωτογραφιών κατά σειρά εμφάνισης:

1.http://static.guim.co.uk/sys-images/Guardian/Pix/pictures/2014/8/13/1407941656947/bitcoin-digital-currency-014.jpg

2.https://www.informationelite.com/wp-content/uploads/2015/07/private-key-vs-public-key.png

3. https://media.licdn.com/mpr/mpr/p/6/005/074/005/11babfc.jpg

# ΠΑΡΑΡΤΗΜΑ

## Λεξικό Όρων

**Κρυπτογραφία** (cryptography): Τεχνική βάσει της οποίας γίνεται χρήση μαθηματικών αποδείξεων για την παροχή υψηλών επιπέδων ασφαλείας. Στο Bitcoin, χρησιμοποιείται για να καταστεί αδύνατη η δαπάνη χρημάτων από πορτοφόλι άλλου χρήστη ή η διαφθορά της blockchain. Ακόμα, μπορεί να χρησιμοποιηθεί για την κρυπτογράφηση πορτοφολιού ώστε να είναι απαραίτητος ένας κωδικός πρόσβασης για την χρήση του.

**P2P**: Το peer-to-peer αναφέρεται σε υπολογιστικά συστήματα ή συστήματα δικτύου που έχουν μία αρχιτεκτονική κατανεμημένων εφαρμογών που επιτρέπουν στο κάθε ισόκυρο και ισοδύναμο συμμετέχοντα να αλληλεπιδρά οργανωμένα και συλλογικά με άλλους. Το σύστημα αυτό επιτρέπει την παράκαμψη έμπιστων τρίτων μελών, όπως οι τράπεζες όταν πρόκειται για χρηματικές συναλλαγές.

**Bitcoin**: Με κεφαλαίο γράμμα περιγράφει το κρυπτοσύστημα στο σύνολό του. Με μικρό γράμμα, bitcoin, χρησιμοποιείται για την περιγραφή του κρυπτονομίσματος ως λογιστικής μονάδας.

**BTC**: συντομογραφία της λογιστικής μονάδας.

**Bit**: Αποτελεί υποδιαίρεση του bitcoin. Το 1 bitcoin ισούται με 1,000,000 bit.

**Altcoins** (alternative currencies): Τα Altcoins αποτελούν εναλλακτικά προς το Bitcoin κρυπτονομίσματα κι ως εκ τούτου, με τον όρο αυτό περιγράφουμε κάθε κρυπτονόμισμα που δεν είναι το Bitcoin. Ως επί το πλείστον είναι εξολοκλήρου βασισμένα στο πρωτότυπο πρωτόκολλο του πρώτου κρυπτονομίσματος.

**Blockchain**: Αποτελεί τον δημόσιο βιβλίο ισολογισμού του κρυπτονομίσματος. Σε αυτήν καταγράφονται όλες οι συναλλαγές που γίνονται σε χρονολογική σειρά ενώ είναι προσβάσιμη από όλους τους χρήστες.

**Block**: Η κάθε καταγραφή στην blockchain. Περιλαμβάνει τις ανεπιβεβαίωτες συναλλαγές και τις καταχωρεί στην blockchain. Περιέχοντας πληροφορίες του αμέσως προηγούμενου block, διασφαλίζει την εγκυρότητα των συναλλαγών και δημιουργεί μία ακέραια αλυσίδα που έχει τις βάσεις της στο πρώτο γενετήσιο block.

**Διπλοξόδεμα ή Double Spend**: Πρόβλημα που παρουσιάζεται στις ηλεκτρονικές συναλλαγές παντός τύπου και αφορά την πίστωση των ίδιων νομισματικών μονάδων σε δύο ξεχωριστούς παραλήπτες/χρήστες ταυτόχρονα. Το πρόβλημα αντιμετωπίζεται με την καταγραφή όλων των συναλλαγών στην blockchain και την επιβεβαίωση της εγκυρότητάς της.

**Επιβεβαίωση** (confirmation): Η αναμονή παραγωγής επόμενου block για διασφάλιση εγκυρότητας συναλλαγής. Όσες περισσότερες επιβεβαιώσεις υπάρξουν, δηλαδή όσα περισσότερα νέα blocks δημιουργηθούν, τόσο πιο ασφαλής η συναλλαγή.

**Hash**: Το output σε μία συνάρτηση κατακερματισμού, δηλαδή η μικρότερη, φαινομενικά τυχαία σειρά αριθμών και γραμμάτων που παράγεται από έναν μεγάλο όγκο πληροφοριών. Αποτελούν την "λύση" ενός block ενώ η διαδικασία παραγωγής τους αποτελεί στην ουσία το mining.

**Hash Rate**: Η ταχύτητα παραγωγής των hash.

**Δυσκολία** (difficulty): Αφορά τον βαθμό δυσκολίας στην επίλυση των hashes για παραγωγή των νέων block που θα μπουν στην blockchain. Η δυσκολία επαναπροσδιορίζεται ανά 2,016 blocks, για την παραγωγή των οποίων ιδανικός χρόνος θεωρούνται οι δύο εβδομάδες.

**Nonce**: Το μόνο κομμάτι δεδομένων που δύναται να αλλάζεται έως ότου παραχθεί το αναζητούμενο hash.

**Miners**: Οι ρυθμιστές του κρυπτοσυστήματος. Αφ' ενός επεξεργάζονται και καταχωρούν τις συναλλαγές στην blockchain κι αφ 'ετέρου εξορύσσουν τα νέα νομίσματα.

**Nodes**: Ελληνιστί κόμβοι. Αποτελούν ενεργές ηλεκτρονικές συσκευές συνδεδεμένες στο δίκτυο και ικανές να δημιουργήσουν, να λάβουν ή/και να διαβιβάσουν πληροφορίες διαμέσου ενός διαύλου επικοινωνίας. Τα nodes καλούνται να επιβεβαιώσουν την ορθότητα λύσης ενός hash. Η λειτουργία ως node δεν συνεπάγεται mining.

**Mining**: Η εργασία που επιτελούν οι miners που συνίσταται κατά κύριο λόγο στην παραγωγή νέων blocks και δευτερευόντως στην εξόρυξη νέων νομισμάτων.

**ASIC** (Application Specific Integrated Circuits): Κυκλώματα ειδικής κατασκευής των οποίων γίνεται χρήση για το mining σήμερα καθώς αποτελούν την πιο εξελιγμένη μέχρι στιγμής τεχνολογία. Έχουν αυξημένη αποδοτικότητα σε σχέση με παλαιότερα συστήματα, παράγοντας περισσότερα hashes ανά watt ισχύος.

**Διεύθυνση** (address): Μία διεύθυνση Bitcoin είναι παρόμοια με μία διεύθυνση ηλεκτρονικού ταχυδρομείου κι αποτελούν την μόνη πληροφορία που χρειάζεται να παρέχει κάποιος ώστε να του αποσταλλούν Bitcoin.

**Πορτοφόλι** (wallet): Ο χώρος όπου αποθηκεύονται οι πληροφορίες με τις οποίες ο κάθε χρήστης μπορεί να ξεκλειδώσει και να χρησιμοποιήσει τα bitcoin του.

**Cold Storage**: Πρόκειται για offline πορτοφόλια, δηλαδή πορτοφόλια χωρίς σύνδεση στο διαδίκτυο. Η απουσία διαδικτυακής σύνδεσης εκμηδενίζει την δυνατότητα κλοπής των ιδιωτικών κλειδιών μέσω hacking.

**Ιδιωτικό κλειδί** (private key): Αποτελεί τον κωδικό πρόσβασης στο πορτοφόλι και το μέσο παραγωγής της ψηφιακής υπογραφής. Πρέπει να διατηρείτε μυστικό.

**Υπογραφή** (signature): Η ψηφιακή ή κρυπτογραφική υπογραφή αποτελεί ένα μαθηματικό μηχανισμό που με την χρήση του ιδιωτικού κλειδιού επιτρέπει την απόδειξη της κυριότητας των bitcoin.

**Τέλη συναλλαγών** (transaction fees): Ένα μικρό, προς το παρόν προαιρετικό ποσό που επισυνάπτεται στην κάθε συναλλαγή. Τα τέλη συναλλαγών αποδίδονται στους miners ενώ μελλοντικά προσδοκάται ότι θα αποτελούν το κύριο κίνητρο για τους miners.