Ανώτατο Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης

Σχολή : Διοίκηση και οικονομία

Τμήμα: Διοίκηση Επιχειρήσεων

Πτυχιακή Εργασία

«Το Ψηφιακό Νόμισμα Bitcoin»

Ονοματεπώνυμο: Κωνσταντίνα Μαυρέλη **Α.Μ: 3821**

Επιβλέπων Καθηγητής: Δρ. Ιωάννης Βάρδας

ΗΡΑΚΛΕΙΟ 2015

Copyright

Η εργασία με θέμα «ΤΟ ΨΗΦΙΑΚΟ ΝΟΜΙΣΜΑ BITCOIN», πραγματοποιήθηκε στα πλαίσια πτυχιακής εργασίας. Διεξήχθη από την προπτυχιακή φοιτήτρια Μαυρέλη Κωνσταντίνα, την περίοδο του εαρινού εξαμήνου 2015. Με κάθε επιφύλαξη έχει τηρηθεί η διαδικασία πνευματικής ιδιοκτησίας της παρούσας εργασίας. Επίσης, το ΤΕΙ Κρήτης καθώς και ο επιβλέπων καθηγητής δεν φέρουν καμία ευθύνη σε περίπτωση κλοπής πνευματικών δικαιωμάτων.

Ευχαριστίες

Η παρούσα πτυχιακή εργασία με θέμα «Το ψηφιακό νόμισμα Bitcoin», πραγματοποιήθηκε, στο πλαίσιο της πτυχιακής εργασίας του τμήματος Διοίκησης Επιχειρήσεων του Ανώτατου Τεχνολογικού Εκπαιδευτικού Ιδρύματος Κρήτης. Στο σημείο αυτό αισθάνομαι την ανάγκη να εκφράσω τις ειλικρινείς και θερμές ευχαριστίες μου σε όσους συνέβαλαν στην ολοκλήρωση αυτής της προσπάθειας. Και πρώτα απ' όλα, στον επιβλέποντα καθηγητή μου κ. Βάρδα Ιωάννη. Επίσης θα ήθελα να ευχαριστήσω θερμά την κ. Ιωάννα Συγλέτου και τον κ. Χαράλαμπο Ανδρεάδη για την πολύτιμη βοήθεια τους σχετικά με το υλικό αλλά και με την διευθέτηση της πτυχιακής μου εργασίας. Τέλος, θέλω να ευχαριστήσω όλους εκείνους που με έμαθαν να «προσπερνώ» και βοήθησαν να γίνουν «ανεκτοί» οι συμβιβασμοί των τελευταίων χρόνων: την οικογένεια μου, τους φίλους μου, τους συναδέλφους μου. Σε αυτούς, που με την καθημερινή τους συμπαράσταση, την υπομονή τους και την θετική τους σκέψη, ιδιαίτερα τις εποχές των μεγάλων διλλημάτων, συνέβαλαν στην εκπλήρωση του στόχου μου, αφιερώνεται η εργασία αυτή.

Περίληψη

Η αλματώδης εξέλιξη της τεχνολογίας και η αύξηση του όγκου των διαδικτυακών συναλλαγών, οδήγησαν την οικονομία στη δημιουργία ψηφιακών νομισμάτων με σκοπό να γίνει μία μέθοδος αγοροπωλησίας, πληρωμών και συνεπώς μορφή εναλλακτικού χρήματος γενικότερα. Διευκολύνει την πράξη αυτή, διότι, οι συναλλαγές γίνονται μέσω του διαδικτύου και όπως είναι κατανοητό ο κάθε ένας μπορεί να πραγματοποιήσει μια συναλλαγή με πολύ απλό τρόπο από το σπίτι του. Ωστόσο, δεν αποτελεί αποδεκτή μέθοδο πληρωμής σε αρκετές εταιρίες στον κόσμο. Μάλιστα, ακριβώς, επειδή πρόκειται για ένα ψηφιακό νόμισμα, που συναλλάσσεται μέσω του διαδικτύου δημιουργεί αμφιβολίες για την αξία του. Παρ' όλα αυτά, αξίζει να αναφερθεί ότι ίσως αποτελεί περισσότερο επένδυση παρά μία μέθοδο πληρωμών, με την κλασική έννοια του χρήματος, όπως όλοι γνωρίζουν σήμερα, διότι η αξία του αυξομειώνεται ανάλογα με την προθυμία των χρηστών να αποκτήσουν τα κρυπτονομίσματα αυτά.

Summary

The rapid evolution of technology and the increasing volume of the online transactions, led the economy to create digital currencies in order to become a method of buying/selling and payments in general. This practice is facilitated because the transactions are being made via the internet and as it is clearly understood, everybody can carry out a transaction in a very simple way from home. However, it is not an acceptable payment method for several companies in the world. Furthermore, exactly because it is a digital currency that is being used for transactions via the Internet, it creates doubts about its value. Nevertheless, it is worth mentioning that it might constitutes more an investment than one payment method, with the classical concept of money as we all know today, because its value fluctuates depending on the willingness of the users to acquire this cryptocurrency.

Πίνακας περιεχομένων

ΕΙΣΑΓΩΓΗ

Η εκπόνηση της παρούσας διπλωματικής εργασίας σκοπεύει να αναδείξει και να ερευνήσει, κατά πόσο το ψηφιακό κρυπτονόμισμα Bitcoin μπορεί να θεωρηθεί πραγματικό χρήμα, συγκρίνοντας τις λειτουργίες του και την χρησιμότητα του με τους διάφορους τύπους χρήματος ανά την ιστορία. Αρχικά, θα αναλυθεί η έννοια και η λειτουργία του συστήματος Bitcoin. Επιπροσθέτως, θα γίνει παραπομπή στους διάφορους τύπους χρήματος καθώς και στην προέλευση τους. Επίσης, θα γίνει αναφορά τόσο στην επιρροή που έχει ασκήσει το ψηφιακό νόμισμα Bitcoin στην παρούσα αγορά όσο και στο κίνητρο που έχει δώσει στους προγραμματιστές/ χρηματιστές να δημιουργήσουν μορφές εναλλακτικού χρήματος αντίστοιχο του Bitcoin. Το ρίσκο και οι ενδεχόμενες επιπλοκές θα συζητηθούν δίνοντας έμφαση στον ρόλο που παίζουν οι χρηματιστές. Θα μελετηθούν οι λόγοι που το Bitcoin ενδεχομένως δεν θεωρείται πραγματικό χρήμα με την παραδοσιακή έννοια του όρου, μιας και όλες οι συναλλαγές γίνονται μέσω διαδικτύου. Λόγω του ότι το σύστημα Bitcoin έχει δεχτεί ισχυρή κριτική για τους τρόπους με τους οποίους έχει χρησιμοποιηθεί για παράνομες δραστηριότητες, θα γίνει προσπάθεια να αναλυθούν και να αποσαφηνιστούν τα λάθη που έχουν γίνει εξαρχής τα οποία οδήγησαν ορισμένους να βλέπουν καχύποπτα το όλο σύστημα. Τέλος, παρόλο που το Bitcoin ενδεχομένως να μην μπορεί να θεωρηθεί πραγματικό χρήμα, θα αναφερθούν επιχειρήματα που θα εξισώσουν το ψηφιακό νόμισμα αυτό σαν τύπο εναλλακτικού χρήματος, το οποίο μπορεί να έχει την ενδιάμεση χρήση ανάμεσα στο πραγματικό και στο εικονικό χρήμα.

Κεφάλαιο 1

1.1 Χρήμα

Με την γνωστή σε όλους μας ορολογία χρήμα εννοείται το κάθε περιουσιακό στοιχείο, το οποίο χρησιμοποιείται και είναι ευρέως γνωστό για οποιουδήποτε είδους πληρωμή. Είναι το οποιοδήποτε αντικείμενο, το οποίο είναι ικανό να χρησιμοποιηθεί από μια κοινωνία ως μέσο συναλλαγής/ανταλλαγής, ως μονάδα υπολογισμού όσον αφορά την αγοραστική δύναμη και την εμπορική αξία, εν ολίγοις ως υποκατάστατο αξίας. Η αξία του χρήματος προκύπτει κατά ένα μέρος από την χρησιμότητά του ως μέσο ανταλλαγής. Η αναγνώριση της αγοραστικής του αξίας συνδέεται από την χρησιμότητά του ως μέσον ανταλλαγής, συνεπώς αυτές οι δύο πτυχές του χρήματος είναι αλληλένδετες, το πρώτο είναι η αιτία για το αποτέλεσμα του δεύτερου και το αντίστροφο. Ανά την ιστορία έχουν υπάρξει διάφορες μορφές χρήματος (θα αναφερθούν αναλυτικότερα παρακάτω) των οποίων η φυσική μορφή διαφέρει κατά πολύ συμφώνα με αυτό που υπάρχει σήμερα στο μυαλό της ανθρωπότητας. Οι κοινωνίες δημιουργούσαν, δημιουργούν και θα συνεχίζουν να δημιουργούν μέσα/μορφές συναλλαγών, όταν δεν υπήρχε/υπάρχει κανένα άλλο, δεδομένου ότι οι φυσικές ανθρώπινες ανάγκες προκύπτουν ενστικτωδώς. Ωστόσο, για να αποφθεχθεί κάθε είδους παραπλάνηση θα ήταν σωστό να προσδιοριστεί με ακρίβεια και σαφήνεια η διάκριση ανάμεσα στα χρηματικά περιουσιακά στοιχεία και στα μη – χρηματικά περιουσιακά στοιχεία, τα οποία μπορούν να είναι το οτιδήποτε πέραν του χρήματος. Στην σύγχρονη οικονομία ο προσδιορισμός της έννοιας αυτής είναι πολύ συγκεκριμένος, διότι οτιδήποτε άλλο εκτός των νομισμάτων , των τραπεζογραμματίων και των καταθέσεων δεν είναι χρήμα. Το σύνολο των κερμάτων και των χαρτονομισμάτων, αξίζει να σημειωθεί ότι το τραπεζογραμμάτιο είναι συνώνυμο με την έννοια χαρτονόμισμα, ονομάζεται σύνολο νομισματικής κυκλοφορίας. Παρ ’όλα αυτά όμως χρήμα δεν είναι μόνο αυτό, διότι χρήμα θεωρούνται αφενός οι καταθέσεις των ιδιωτών στις εμπορικές τράπεζες, αφετέρου οι καταθέσεις των εμπορικών τραπεζών στην κεντρική τράπεζα. Παραδείγματος χάριν, η επιταγή θεωρείται μια εκ των πολλών μορφή χρήματος σύμφωνα με τον χρηματικό ορισμό του σήμερα. Επιπλέον, η χρέωση των πιστωτικών και χρεωστικών καρτών είναι χρήμα. Αντιθέτως, τα ομόλογα και άλλα παρόμοια χρεόγραφα, τα αξιόγραφα, όπως για παράδειγμα είναι οι μετοχές, καθώς και τα αμοιβαία κεφάλαια δεν είναι αποδεκτά από την οικονομία ως χρήμα παρά το γεγονός ότι θα ήταν δυνατό να γίνει απευθείας συναλλαγή. Γι’ αυτόν ακριβώς τον λόγο, των διαφόρων ειδών χρηματοδοτικά αξιόγραφα ονομάζονται χρηματοδοτικά ή χρηματοοικονομικά **προϊόντα**.

1.2 Ιστορία του χρήματος

1.2.1 Η εμφάνιση του χρήματος

Στην αρχαιότητα οι άνθρωποι πραγματοποιούσαν τις συναλλαγές τους με εντελώς διαφορετικά μέσα από τα μέσα που είναι κοινώς αποδεκτά στην σύγχρονη οικονομία. Η τότε διαδεδομένη μέθοδος ήταν στην ουσία η ανταλλαγή διαφόρων αγαθών. Για παράδειγμα, ο παραγωγός ενός προϊόντος αντάλλαζε τα επιπλέον προϊόντα του με τα πλεονάζοντα προϊόντα άλλου παραγωγού. Η μέθοδος αυτή της ανταλλαγής των αγαθών χρονολογείται σε τουλάχιστον 100.000 χρόνια πριν, αν και πρέπει να αναφερθεί ότι δεν υπάρχει κανένα ιστορικό στοιχείο που να αποδεικνύει ότι βασιζόταν η οικονομία και η κοινωνία εξ' ολοκλήρου στην μέθοδο αυτή. Αρκετοί πολιτισμοί σε όλον τον κόσμο δημιούργησαν και ανέπτυξαν την χρήση κάποιου είδους χρήματος όπου η αξία του υλικού από το οποίο ήταν φτιαγμένο καθόριζε και την αξία του χρήματος αυτού. Μια μονάδα χρήματος αλλά και μονάδα βάρους ονομαζόταν σε εκείνα τα χρόνια σίγλος ή σέκελ. Η πρώτη χρήση του όρου αυτού προήλθε από την Μεσοποταμία γύρω στο 3000 π. Χ. Επίσης, ξεκίνησαν να χρησιμοποιούν όστρακα αντί για χρήμα πολιτείες στην Αμερική, την Ασία , την Αφρική και την Αυστραλία. Χρησιμοποιήθηκαν πολλά αντικείμενα έναντι του χρήματος την τότε εποχή από τα φυσικά πολύτιμα μέταλλα που υπήρχαν, από κοχύλια και τσιγάρα έως τα νομίσματα και χαρτονομίσματα. Τα πρώτα νομίσματα κατασκευάστηκαν από χαλκό και στην συνέχεια από σίδηρο. Το υλικό από το οποίο ήταν φτιαγμένο το μέταλλο καθόριζε την χρηματική αξία των νομισμάτων. Στην συνέχεια αντικαταστάθηκαν τα νομίσματα σιδήρου, από άλλο μέταλλο, το ασήμι από τον Βασιλιά Φείδων του Άργους, το 700 π.Χ περίπου. Ο Βασιλιάς Φείδων κατασκεύασε τα ασημένια νομίσματα στην Αίγινα και χάραξε πάνω της μία χελώνα , η οποία χρησιμοποιείται ακόμα και σήμερα ως σύμβολο κεφαλαιοκρατίας. Τα νομίσματα αυτά πάνω στα οποία ήταν χαραγμένη η χελώνα έγιναν ευρέως αποδεκτά, τα οποία μάλιστα χρησιμοποιήθηκαν ως διεθνές μέσο συναλλαγής μέχρι την αντικατάσταση τους στον πελοποννησιακό πόλεμο από την Αθηναϊκή δραχμή.

1.2.2 Η εξέλιξη του χρήματος

Η μέθοδος σύμφωνα της οποίας η αξία του υλικού από το οποίο ήταν κατασκευασμένο το νόμισμα καθόριζε την αξία γενικότερα του νομίσματος, εξελίχθηκε τελικά στην μέθοδο του αντιπροσωπευτικού χρήματος, όπως είναι γνωστό σε όλους μας σήμερα. Αυτό συνέβη διότι οι έμποροι χρυσού και αργυρού ή οι τράπεζες εξέδιδαν αποδείξεις στους καταθέτες με χρήματα πραγματικής αξίας τα οποία είχαν κατατεθεί και κατά συνέπεια αυτού του είδους οι αποδείξεις καθιερώθηκαν, έγιναν δηλαδή ευρέως γνωστές και κοινώς αποδεκτές ως μέσο πληρωμής και έτσι ξεκίνησαν να έχουν το ρόλο του χρήματος. Αξίζει να αναφερθεί ότι τα χαρτονομίσματα χρησιμοποιήθηκαν για πρώτη φορά στην Κίνα κατά την διάρκεια της δυναστείας των Σονγκ[1]. Αυτά τα

[1] Η δυναστεία των Σονγκ ήταν μια εποχή της κινεζικής ιστορίας που ξεκίνησε το 960 και συνεχίστηκε μέχρι το 1279 .πέτυχε την περίοδο των πέντε δυναστειών και των δέκα βασιλείων και ακολούθησε η δυναστεία Yuan

τραπεζογραμμάτια, χρυσού ως χρήμα. Αργότερα, στις αρχές του 20ου αιώνα σχεδόν όλες οι χώρες υιοθέτησαν αυτό το νομισματικό σύστημα, δηλαδή για κάθε πιστοποιητικό που εξέδιδαν, υπήρχε συγκεκριμένη ποσότητα χρυσού προς εξαργύρωση. Πιο πρόσφατα, μετά τον δεύτερο παγκόσμιο πόλεμο οι χώρες υιοθέτησαν το παραστατικό χρήμα τα χαρτονομίσματα γνωστά ως "Jiaozi[2]" εξελίχθηκαν σε χρεόγραφα που ξεκίνησε η χρήση τους από τον 7ο αιώνα μ. Χ, ωστόσο, στο διάστημα αυτό συνεχιζόταν παράλληλα η χρήση των νομισμάτων πραγματικής αξίας. Στην συνέχεια εκδόθηκαν στην Ευρώπη το 1661 τα πρώτα τραπεζογραμμάτια, τα οποία χρησιμοποιήθηκαν μαζί με κέρματα από την Stockholms Banco. Τα πλεονεκτήματα που παρείχε η έκδοση των τραπεζογραμματίων από τις τράπεζες ήταν αρκετά, διευκολύνθηκαν με τέτοιο τρόπο οι συναλλαγές ώστε να καθιερωθούν τα χαρτονομίσματα έως την πλέων ασφαλή συναλλαγματική πρακτική. Στην Ευρώπη μεταξύ του 17ου και 19ου αιώνα αντικαταστάθηκαν τα χρυσά νομίσματα με αυτό το συναλλαγματικό σύστημα που αναφέρεται παραπάνω, όπου τα χαρτιά πλέον είναι το μέσο συναλλαγής, τα οποία είναι δυνατό να μετατραπούν σε προκαθορισμένες, σταθερές ποσότητες χρυσού. Ωστόσο, αποθαρρύνθηκε η ρευστοποίηση του σε χρυσό παρ' όλα αυτά νομιμοποιήθηκαν αυτά τα πιστοποιητικά τα οποία είναι γνωστά με την ορολογία fiat[3] των οποίων η τιμή καθοριζόταν βάσει του δολαρίου των Η.Π.Α (USD). Και στην συνέχεια το αμερικάνικο δολάριο με την σειρά του καθορίστηκε βάσει του χρυσού. Η κυβέρνηση των Η.Π.Α σταμάτησε την μετατροπή του αμερικάνικου δολαρίου σε χρυσό και αυτό ήταν η αιτία κατά κάποιον τρόπο να ακολουθήσουν το παράδειγμα των Ηνωμένων πολιτειών και άλλες πολλές χώρες με αποτέλεσμα η πλειονότητα των χρημάτων παγκοσμίως να σταματήσει να υποστηρίζεται με αποθέματα χρυσού. Με την πάροδο των τόσων χρόνων, από τότε που πρωτοεμφανίστηκαν τα χρήματα ή καλυτέρα μέσα με τα οποία πραγματοποιούνταν οι ανταλλαγές, ερχόμαστε στο σήμερα, στο σημείο όπου η τεχνολογία έχει πραγματοποιήσει τεράστια πρόοδο και δίνει την δυνατότητα σε όλον τον κόσμο να χρησιμοποιεί ψηφιακά, ηλεκτρονικά μη απτά νομίσματα. Νομίσματα που είναι ικανά να πραγματοποιήσουν συναλλαγές, όπως ακριβώς είναι σε θέση να πραγματοποιήσουν τα χαρτονομίσματα, τα κέρματα, οι επιταγές και όλα τα μέσα που είναι χρήματα με διαφορετική μορφή το καθένα εξ' αυτών. Υπάρχουν αρκετά ψηφιακά νομίσματα τα οποία θα αναφερθούν και θα αναλυθούν παρακάτω. Το πιο διαδεδομένο εξ' αυτών είναι το ψηφιακό νόμισμα **Bitcoin.**

[2] είναι ένα είδος κινέζικων ζυμαρικών, συνήθως τρώγονται σε όλη την Ανατολική , Κεντρική και Δυτική Ασία .

[3] Παραστατικό χρήμα (fiat money) ή αλλιώς χρήμα αναγκαστικής κυκλοφορίας είναι το μέσον πληρωμής το οποίο δεν καλύπτεται από αποθεματικό άλλων υλικών και επομένως στερείται κάποιας εσωτερικής αξίας έστω και έμμεσα.

Κεφάλαιο 2

2.1 Ιστορία του Bitcoin

Το 2008 για πρώτη φορά αναφέρεται το bitcoin σε ένα έγγραφο, το οποίο δημοσιεύεται με την υπογραφή του Satoshi Nakamoto, στις αρχές του 2009, συγκεκριμένα στις 9 Ιανουαρίου ξεκινά και η λειτουργία του. Ωστόσο, το ξεκίνημα του νομίσματος αυτού δεν ήταν ιδιαίτερα καλό διότι προέκυψαν από νωρίς τεχνικά προβλήματα, όπου στην διάρκεια του έτους 2009 επετράπη η δημιουργία απεριόριστων bitcoins από ένα bug. Δύο χρόνια αργότερα, το 2011 η αξία του ενός bitcoin αυξήθηκε κατά πολύ στα $32 από τα $0,30, ενώ στην συνέχεια μειώνεται η αξία του και πάλι στα $2. Ένα χρόνο αργότερα, στα τέλη του 2012 το κρυπτονόμισμα bitcoin καταφέρνει να διεγείρει το ενδιαφέρον των μέσων μαζικής ενημέρωσης και έκτοτε έχουν γραφτεί πολλά άρθρα γι' αυτό. Ορισμένες υπηρεσίες άρχισαν να δέχονται πληρωμές γι' αυτό, κάποιες από αυτές είναι η OkCupid, Footler, Baidu, κτλ. Κατά την διάρκεια του Νοέμβριου του 2013, το bitcoin στο ανταλλακτήριο BTC China[4] ξεπέρασε το Ιαπωνικό Mt. Gox[5] και το Ευρωπαϊκό Bitstamp[6], μάλιστα είναι το μεγαλύτερο ανταλλακτήριο σε όγκο συναλλαγών χρηματιστηριακής διαπραγμάτευσης για bitcoins. Η αξία του bitcoin αυξήθηκε σημαντικά φτάνοντας ως και τα 900 αμερικάνικα δολάρια στις 19 Νοεμβρίου του 2013, αυτό ήταν η απόρροια ύστερα από την ακρόαση που διεξήχθη στην επιτροπή της Γερουσίας των Ηνωμένων πολιτειών της Αμερικής κατά της διάρκεια της οποίας πραγματοποιήθηκε μία ανακοίνωση που έλεγε ότι τα εικονικά, ψηφιακά νομίσματα είναι μια νόμιμη οικονομική υπηρεσία. Αυτή η ακρόαση οδήγησε την ίδια μέρα κιόλας στην διαπραγμάτευση του ενός bitcoin στα $1.100 στο BTC China. Με περίπου 12.000.000 bitcoins σε κυκλοφορία τον Νοέμβριο του 2013, αυτή η τιμή σημαίνει πως η κεφαλαιοποίηση του bitcoin είναι τουλάχιστον $7.200.000.000.

[4] BTC Κίνα , με έδρα τη Σαγκάη της Κίνας, είναι το δεύτερο μεγαλύτερο χρηματιστήριο Bitcoin στον κόσμο από πλευράς όγκου από τον Οκτώβριο του 2014.

[5] Mt. Gox ανταλλακτήριο για Bitcoin το οποίο βασίζεται στο Τόκιο , Ιαπωνία

[6] Bitstamp , ανταλλακτήριο για Bitcoin με έδρα το Ηνωμένο Βασίλειο . Από τον Σεπτέμβριο του 2014 ήταν παγκοσμίως δεύτερη μεγαλύτερη σε όγκο συναλλαγών

2.2 Λίγα λόγια για το Bitcoin

Το bitcoin με κωδικό BTC ή XBT είναι ένα ψηφιακό νόμισμα “peer to peer” του οποίου η λειτουργία δεν ελέγχεται από κάποια κεντρική αρχή. Ονομάστηκε κρυπτονόμισμα (cryptocurrency) για τους εξής λόγους, επειδή χρησιμοποιεί κρυπτογράφηση για τον έλεγχο των συναλλαγών και είναι αποκεντρωμένο με αποτέλεσμα να αποφεύγεται η διπλή δαπάνη, κατι το οποίο είναι σύνηθες πρόβλημα όσον αφορά τα ψηφιακά νομίσματα. Την στιγμή που θα βρεθούν όλα τα bitcoins από την διαδικασία παραγωγής τους, δηλαδή όταν ολοκληρωθεί η συνολική τους έκδοση, κάθε μεμονωμένη, ξεχωριστή συναλλαγή θα έχει κατοχυρωθεί μόνιμα σε έναν δημόσιο λογαριασμό ο οποίος είναι γνωστός με τον όρο Blockchain. Υπάρχει ειδικά προσαρμοσμένο δίκτυο ηλεκτρονικών υπολογιστών μέσα στο οποίο γίνεται η διαδικασια παραγωγής μέσω της επεξεργασίας των block. Οι φορείς των υπολογιστών αυτών είναι γνωστοί με την αγγλική ορολογία miners “σκαπανείς” οι οποίοι ανταμείβονται από την απόδοση μεταφοράς των νεόκοπων Bitcoins στα πορτοφόλια τους για τα έξοδα miningς.(Daniel Forrester, Mark Solomon,2013). Τα Bitcoins αποθηκεύονται σε κάποια αρχεία ουσιαστικά, τα οποία ονομάζονται **πορτοφόλια** και αποθηκεύονται εκεί μέσω της σύνδεσης τους. Μπορούν να αποθηκευτούν σε υπηρεσίες web, σε εξωτερικές μονάδες αποθήκευσης συσκευών, σε υπολογιστές ή φορητές συσκευές, είτε με την εκτύπωσή τους σε χαρτί. Καλό είναι να αναφερθεί πως συχνά έχουν απασχοληθεί τα μέσα μαζικής ενημέρωσης με τις κλοπές των bitcoins από τα online πορτοφόλια και από τις υπηρεσίες web, ισχυριζόμενοι πως ο ασφαλέστερος και αποτελεσματικότερος τρόπος όσον αφορά την αποθήκευση του κρυπτονομίσματος bitcoin είναι τα πορτοφόλια εκτυπωμένα σε χαρτί. Συγκεκριμένα, το 2012 αναφέρει και αναλύει το περιοδικό The Economist, το οποίο σχολίασε το δημοφιλές ψηφιακό νόμισμα κατηγορώντας ουσιαστικά ακριβώς το γεγονός ότι είναι δημοφιλές εξαιτίας του “ρόλου του σε online πονηρές αγορές”, όπου ένα χρόνο αργότερα κλείνει η υπηρεσία Silk Road από το FBI, η οποία έγινε γνωστή λόγω της ενασχόλησης της με την παράνομη διακίνηση ναρκωτικών. Σε αυτό το σημείο αξίζει να αναφερθεί ότι αυτό αποτέλεσε αφορμή ώστε να ξεκινήσει το FBI να ελέγχει το 1,5% του συνόλου των ψηφιακών νομισμάτων Bitcoins που βρίσκονται σε κυκλοφορία. Παρά το γεγονός αυτό, αυτό το σκοτεινό σημείο, τα bitcoins χρησιμοποιούνται όλο και περισσότερο ως πληρωμή για την αγορά νόμιμων προϊόντων και υπηρεσιών, μάλιστα συμφέρει τους εμπόρους να δεχθούν το ψηφιακό νόμισμα διότι τα τέλη συναλλαγής είναι χαμηλότερα κατά 2% έως και 3% σε σχέση με εκείνα που επιβάλλονται από τις εταιρίες επεξεργασίας των συναλλαγών με τις πιστωτικές κάρτες. Σημαντικό είναι να αναφερθούν ποιες εταιρίες είναι αυτές, οι οποίες δέχονται αυτόν τον τρόπο πληρωμής. Είναι οι εξής: OkCuppid, Reddit, WordPress, και ο κινέζικος κολοσσός του διαδικτυακού κόσμου το Baidu.

2.3 Satoshi Nakamoto

Ο Satoshi Nakamoto είναι ο δημιουργός ή ενδεχομένως οι δημιουργοί του ψηφιακού νομίσματος Bitcoin, καθώς δεν έχει γίνει σαφές μέχρι σήμερα εάν επρόκειτο για πραγματικό όνομα ή απλώς για κάποιο ψευδώνυμο. Αυτός, αυτή ή αυτοί δημοσίευσε/σαν ένα έγγραφο το 2008 “The Cryptography list” στην επίσημη ιστοσελίδα metzdowd.com, μέσω της οποίας γίνεται η περιγραφή του κρυπτονομίσματος Bitcoin. Το 2009 κυκλοφόρησε η πρώτη έκδοση λογισμικού του Bitcoin και μέσω αυτού

δημιουργήθηκε το δίκτυο, καθώς και το συνάλλαγμα που ονομάστηκε Bitcoin(s). Ο δημιουργός συνέχισε να συμβάλλει, όπως λέγεται, στην απελευθέρωση του λογισμικού Bitcoin σε συνεργασία με άλλους προγραμματιστές, μέχρι να έρθει σε επαφή με την δική του ομάδα και κοινότητα άρχισε σταδιακά να ξεθωριάζει στα μέσα του 2010. Λίγο αργότερα ο Satoshi Nakamoto παρέδωσε τον έλεγχο του πηγαίου κώδικα και τις βασικές λειτουργίες ειδοποίησης του λογισμικού στον Gavin Andresen[7]. Την ίδια περίοδο παρέδωσε επίσης και τον έλεγχο της ιστοσελίδας Bitcoin.org καθώς επίσης και άλλους πολλούς τομείς σε εξέχοντα μέλη της κοινότητας Bitcoin. Επιπροσθέτως, φημολογείται ότι στην κατοχή του Satoshi Nakamoto υπάρχει 1.000.000 Bitcoins. Το πόσο αυτό ήταν ισοδύναμο με 1,1 δισεκατομμύριο αμερικάνικων δολαρίων. Ο Satoshi Nakamoto αποσύρθηκε από το κοινό τον Απρίλιο του 2011, αφήνοντας την ευθύνη της ανάπτυξης του κώδικα και του δικτύου σε μια ακμάζουσα ομάδα εθελοντών. Η ταυτότητα του προσώπου ή τους ανθρώπους πίσω από το Bitcoin είναι ακόμα άγνωστη. Ωστόσο, ούτε ο Satoshi Nakamoto ούτε οποιοσδήποτε άλλος ασκεί τον έλεγχο του συστήματος Bitcoin, το οποίο λειτουργεί με βάση τις πλήρως διαφανή μαθηματικές αρχές. Η ίδια η εφεύρεση είναι πρωτοποριακή και έχει ήδη γεννήσει νέα επιστήμη στα πεδία των κατανεμημένων συστημάτων πληροφορικής, την οικονομία και οικονομετρίας.(Sam Patterson, 2013)

[7] Gavin Andresen (γεννημένος στο Gavin Bell) επικεφαλής επιστήμονας στο Ίδρυμα Bitcoin . Έχει πρόσβαση στο κλειδί ειδοποίησης που του επιτρέπει να μεταδίδει τα μηνύματα σχετικά με τα κρίσιμα προβλήματα του δικτύου σε όλους τους πελάτες

Κεφάλαιο 3

3.1 Τι είναι το ψηφιακό νόμισμα Bitcoin

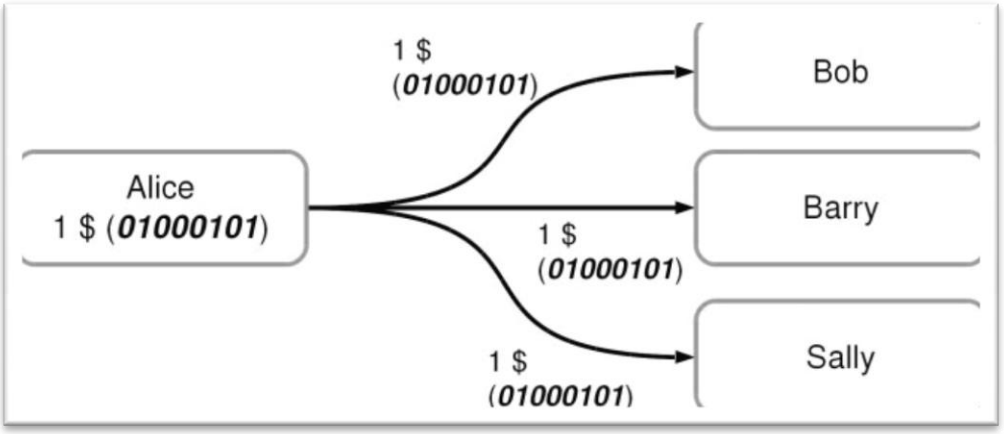
Το ψηφιακό νόμισμα Bitcoin είναι μία συλλογή ιδεών και τεχνολογιών, η οποία αποτελεί την βάση για ένα ψηφιακό χρηματικό οικοσύστημα. Μονάδες του νομίσματος που ονομάζονται bitcoins χρησιμοποιούνται για την αποθήκευση και την μετάδοση αξίας μεταξύ των συμμετεχόντων του δικτύου Bitcoin. Οι χρήστες του νομίσματος αυτού επικοινωνούν μεταξύ τους, χρησιμοποιώντας το πρωτόκολλο Bitcoin κυρίως μέσω του διαδικτύου, αν και είναι δυνατό να χρησιμοποιηθούν και άλλα δίκτυα μεταφορών. Η στοίβα πρωτοκόλλου Bitcoin, το διαθέσιμο λογισμικό ανοιχτού κώδικα, μπορεί να τρέξει σε ένα ευρύ φάσμα των υπολογιστικών συσκευών, συμπεριλαμβανομένων των φορητών υπολογιστών και των smartphones, καθιστώντας την τεχνολογία εύκολα προσβάσιμη. Οι χρήστες μπορούν να μεταφέρουν bitcoins μέσω του διαδικτύου ακριβώς όπως θα πραγματοποιούσαν συναλλαγές με συμβατικά νομίσματα, όπως για παράδειγμα να έχουν την δυνατότητα να αγοράζουν και να πωλούν αγαθά, να στέλνουν χρήματα σε άτομα ή οργανώσεις ή να επεκτείνουν την πίστωση. Τα Bitcoins μπορούν να αγοραστούν, να πωληθούν και να ανταλλάσσονται με άλλα νομίσματα σε εξειδικευμένες συναλλαγματικές ισοτιμίες. Κατά μία έννοια, θα μπορούσε να ειπωθεί ότι το Bitcoin είναι η τέλεια μορφή χρήματος για το Internet, επειδή είναι γρήγορο, ασφαλές και χωρίς σύνορα. Σε αντίθεση με τα παραδοσιακά νομίσματα, τα bitcoins είναι εντελώς εικονικά. Δεν υπάρχουν φυσικά νομίσματα ή ακόμη και ψηφιακά νομίσματα καθ' αυτού. Τα κέρματα συνεπάγονται με συναλλαγές που μεταφέρουν αξία από τον αποστολέα στον παραλήπτη. Οι χρήστες του Bitcoin έχουν δικά τους κλειδιά "private key" τα οποία αποδεικνύουν την κυριότητα των συναλλαγών στο δίκτυο Bitcoin, χρησιμοποιώντας το κλειδί αυτό ξεκλειδώνεται η τιμή και έτσι περνάει, μεταφέρεται σε ένα νέο παραλήπτη . Τα εν λόγω κλειδιά συχνά αποθηκεύονται σε ένα ψηφιακό πορτοφόλι στον υπολογιστή του κάθε χρήστη. Η μόνη προϋπόθεση που είναι απαραίτητη για την πραγματοποίηση της συναλλαγής είναι η κατοχή του μοναδικού κλειδιού που έχει ο χρήστης, ώστε να ξεκλειδωθεί η τιμή και να περαστούν τα bitcoins στον λογαριασμό του, η όλη διαδικασία είναι εξ' ολοκλήρου στα χέρια του κάθε χρήστη. Τα Bitcoins είναι ένα κατανεμημένο peer - to - peer σύστημα. Ως εκ τούτου, δεν υπάρχει "κεντρικός" server ή σημείο ελέγχου. Τα Bitcoins δημιουργούνται και

αποκτιούνται μέσω μιας διαδικασίας που ονομάζεται «mining», το οποίο περιλαμβάνει κάτι σαν ανταγωνισμό όπου βρίσκονται λύσεις σε ένα μαθηματικό πρόβλημα κατά την επεξεργασία των συναλλαγών Bitcoin. Κάθε άτομο που συμμετάσχει στο δίκτυο Bitcoin (δηλαδή, ο κάθε ένας που χρησιμοποιεί μια συσκευή που εκτελεί το πλήρες Bitcoin πρωτόκολλο) μπορεί να λειτουργήσει ως miner, χρησιμοποιώντας την επεξεργαστική ισχύ του υπολογιστή του, να επαληθευτούν και να καταγραφούν οι συναλλαγές . Κάθε 10 λεπτά κατά μέσο όρο, κάποιος είναι σε θέση να επικυρώσει τις πράξεις του, τα τελευταία 10 λεπτά ανταμείβεται με ολοκαίνουργια bitcoins. Ουσιαστικά, το «Bitcoin miningς» αποκεντρώνει την έκδοση του νομίσματος, πραγματοποιεί εκκαθάριση στις λειτουργίες μιας κεντρικής τράπεζας και αντικαθιστά την ανάγκη για κάθε κεντρική τράπεζα με αυτό το παγκόσμιο ανταγωνισμό. Το πρωτόκολλο Bitcoin περιλαμβάνει ενσωματωμένους αλγόριθμους που ρυθμίζουν τη λειτουργία του mining σε όλο το δίκτυο. Η δυσκολία του εγχειρήματος επεξεργασίας που οι miners πρέπει να εκτελέσουν, είναι να καταγράψουν με επιτυχία ένα block των συναλλαγών για το δίκτυο Bitcoin, το οποίο ρυθμίζεται δυναμικά, έτσι ώστε κάποιος να έχει την δυνατότητα να τα καταφέρει, κατά μέσο όρο, κάθε 10 λεπτά, ανεξάρτητα από το πόσο πολλοί miners εργάζονται για την ίδια δουλειά ανά πάσα στιγμή. Το πρωτόκολλο επίσης διαιρεί στα δύο τον ρυθμό με τον οποίο τα νέα bitcoins δημιουργούνται κάθε τέσσερα χρόνια και περιορίζει τον συνολικό αριθμό των bitcoins που θα δημιουργηθούν σε ένα σταθερό σύνολο των 21 εκατομμυρίων κερμάτων. Το αποτέλεσμα είναι ότι ο αριθμός των bitcoins σε κυκλοφορία ακολουθεί πιστά μια εύκολα προβλέψιμη καμπύλη που φτάνει τα 21 εκατομμύρια μέχρι το έτος 2140. Επιπλέον, δεν είναι δυνατό να εκτυπωθεί νέο χρήμα πέρα και πάνω από τον αναμενόμενο ρυθμό έκδοσης. Αξίζει να σημειωθεί ότι Bitcoin είναι και το όνομα του πρωτοκόλλου και μάλιστα είναι κατανεμημένο σαν την πλέον επεξεργαστική καινοτομία. Η πρώτη εφαρμογή αυτής της εφεύρεσης είναι πραγματικά το κρυπτονόμισμα Bitcoin.(Αντωνόπουλος. Μ. Ανδρέας, 2014)

3.1.1 Λογισμικό – Τεχνολογία

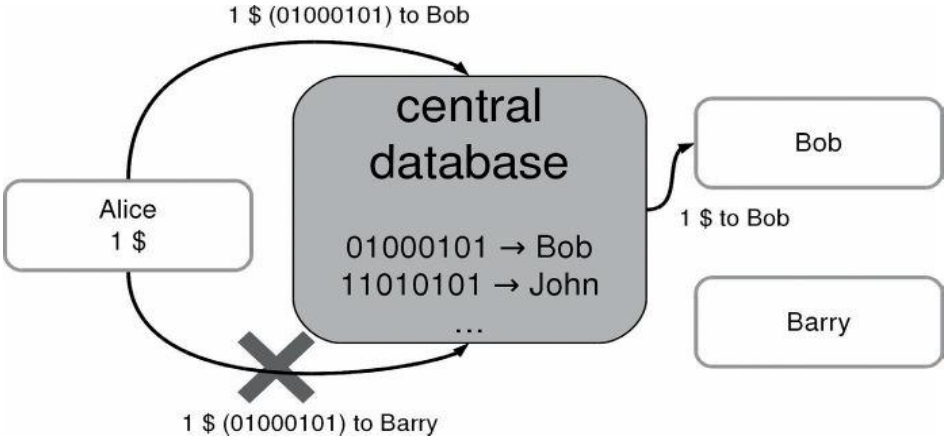
Το bitcoin είναι στημένο σε λογισμικό ανοιχτού κώδικα. Ο κώδικας αυτός είναι δημόσιος και διαθέσιμος για όλους και αυτό δίνει την δυνατότητα σε όποιον θελήσει να μπορεί να ελέγξει τις λεπτομέρειες της λειτουργίας του. Επίσης λόγω του γεγονότος ότι το bitcoin είναι στημένο με ανοιχτό κώδικα παρέχει την δυνατότητα στον καθένα να αντιγράψει τον κώδικα αυτόν και να αναπτύξει νέο λογισμικό βασισμένο στο ήδη υπάρχον, όπως γίνεται κατανοητό, καθίσταται δυνατή η ύπαρξη πολλών διαφορετικών εκδόσεων και εκδοχών του ταυτόχρονα, καθώς με την αντιγραφή του κώδικα μπορεί οποιοσδήποτε να δημιουργήσει ένα παρόμοιο δίκτυο, με τις απαραίτητες ικανότητες, προσθέτοντας ή αλλάζοντας ό,τι κανόνες επιθυμεί. Η θέσπιση κριτηρίων παραγωγής καθώς και συναλλαγής των bitcoins, η διατήρηση πληροφοριών ιδιοκτησίας των ήδη παραχθέντων bitcoins και η δυναμική επιβεβαίωσης της εγκυρότητας των προηγουμένων χωρίς την αναγκαία ύπαρξη κεντρικής οντότητας ελέγχου, πιστοποίησης ή διακρίβωσης. Αυτοί είναι οι στόχοι που επιτυγχάνονται μέσω της μεθόδου του λογισμικού. Η βασική λειτουργιά του εν λόγω λογισμικού είναι η εκτέλεση συναλλαγών bitcoins και η αναμετάδοση πληροφοριών ανάμεσα σε κόμβους και η επιβεβαίωση της εγκυρότητας τους από το υπόλοιπο δίκτυο. Το λογισμικό μπορεί να χρησιμοποιηθεί δωρεάν και είναι διαθέσιμο σε όλες τις χώρες με την μόνη προϋπόθεση να υπάρχει σύνδεση στο internet. Η ισχύς του συγκεκριμένου δικτύου εξασφαλίζεται από την αποδοχή του από τους χρήστες του. Οι αλλαγές που αφορούν τον κώδικα προτείνονται στην κοινότητα, αλλά το δίκτυο δημιουργείται από την συναίνεση της κοινότητας των χρηστών και την αποδοχή τους. Η διαφάνεια του πηγαίου κώδικα, η ακεραιότητα όπως και η διαφάνεια των πληροφοριών που

συναλλάσσονται, επίσης η προστασία του δικτύου από τις κακόβουλες επιθέσεις, καθώς και η παραγωγή περιορισμένων bitcoins και τέλος η προστασία που παρέχουν οι κρυπτογραφικοί αλγόριθμοι που χρησιμοποιούνται ενάντια στη κακόβουλη εκμετάλλευση του δικτύου. Αυτοί είναι οι λόγοι που είναι υπεύθυνοι για την αποδοχή του λογισμικού από τους χρήστες, αλλά και την εξάπλωσή του σε νέους χρήστες. Η αξία ανταλλαγής των bitcoins διαμορφώνεται από τους νόμους της προσφοράς και της ζήτησης χωρίς ενδιάμεσα μέρη. Η αξία που βρίσκουν οι χρήστες αποτυπώνουν την αξία που είναι διατεθειμένοι να πραγματοποιήσουν κάποια ανταλλαγή. Το λογισμικό και οι εξελίξεις του αποτελούν τον πυρήνα του συστήματος συναλλαγής bitcoins. Η δυνατότητα ανταλλαγής πληροφοριών με ακεραιότητα ανεξαρτήτως αποδέκτη εντός του δικτύου, η περιορισμένη διάθεση και η πεπερασμένη ποσότητα των bitcoins, δημιουργεί τις βασικές προδιαγραφές για ένα δίκτυο ανταλλαγής αξίας.
Ο ποιος σωστός τρόπος να προσπαθήσει κανείς να δημιουργήσει ψηφιακή αξία είναι να ορίσει την αξία σε ένα ορισμένο στοιχείο δεδομένων, βασικά μια σειρά από μηδέν και ένα. Το πρόβλημα με αυτή την προσέγγιση είναι ότι η ψηφιακή πληροφορία είναι εύκολο να αντιγραφεί χωρίς βασικό κόστος. Στην εικόνα φαίνονται οι αρχές του προβλήματος διπλής κατανάλωσης. (βλέπε εικόνα 1)



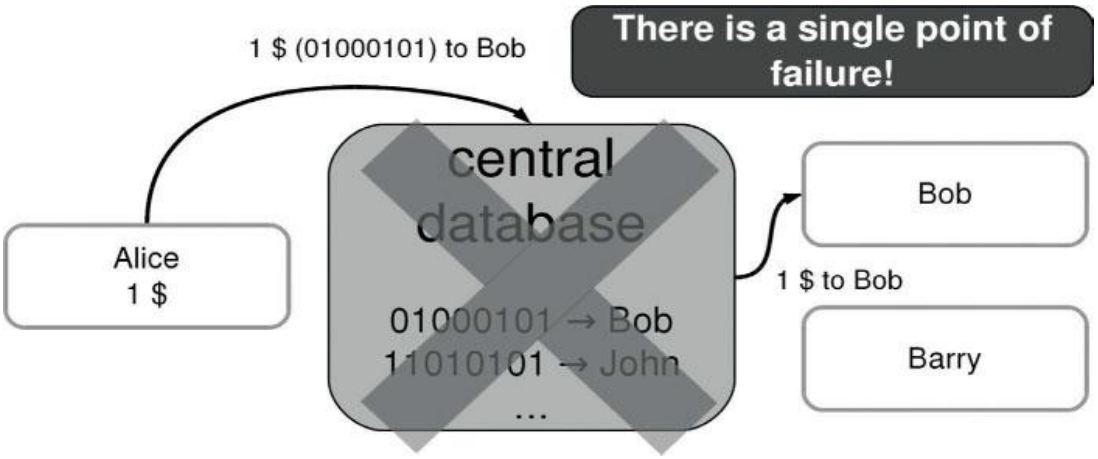
Εικόνα 1. Πρόβλημα διπλής κατανάλωσης

Έστω ότι η Alice έχει ένα ψηφιακό νόμισμα, αντιπροσωπεύεται από το δυαδικό αριθμό 01000101. Μπορεί να μεταφέρει την αξία αυτή στον Bob στέλνοντας ένα μήνυμα με τον αριθμό έτσι ώστε να έχει αντίγραφο του αριθμού και κατά συνέπεια της αξίας. Το πρόβλημα είναι προφανώς ότι τίποτα δεν αποτρέπει την Alice από το να στείλει τον ίδιο αριθμό σε έναν άλλο χρήστη ή για την ακρίβεια σε πολλούς άλλους χρήστες. Έτσι η ψηφιακή αξία δεν μπορεί να αντιπροσωπευτεί, απλά ως αριθμός επειδή η ψηφιακή αξία είναι πολύ εύκολο να αντιγραφεί πολλές φορές, επομένως η γνώση του αριθμού δεν έχει καμία αξία. Όπως προτείνει η κοινή λογική , κάτι που έχει αξία πρέπει να είναι σπάνιο. Επομένως, η πρόκληση είναι πώς να δημιουργηθεί σπανιότητα χρησιμοποιώντας ψηφιακές τεχνολογίες που να επιτρέπουν την τέλεια αντιγραφή πληροφοριών. Το επόμενο βήμα είναι για την κατασκευή ενός ψηφιακού συστήματος πληρωμής είναι η δημιουργία μιας κεντρικής βάσης δεδομένων, που θα περιέχει την λίστα των χρηστών και των κεφαλαίων που κρατούνται από αυτούς.



Εικόνα 2. Κεντρικός αντισυμβαλλόμενος κρατάει μια κεντρική βάση δεδομένων

Τώρα αν η Alice θέλει να μεταφέρει μια νομισματική μονάδα, ας το πούμε σημείο, που αντιπροσωπεύεται από τον αριθμό 01000101 στον Bob, επικοινωνεί με τον server τρέχοντας την κεντρική βάση δεδομένων και το κατευθύνει για να μεταφέρει αυτό το σημείο στον Bob. Ο server ενημερώνει την βάση δεδομένων και το σημείο τώρα ανήκει στον Bob. Αν η Alice προσπαθήσει να κάνει διπλή κατανάλωση στο σημείο 01000101, στέλνοντας στον Barry τώρα, θα πρέπει να συνδεθεί ξανά στον κεντρικό server και να το κατευθύνει για να το μεταφέρει στον Barry. Όταν όμως γίνει έλεγχος από τον server στην βάση δεδομένων θα διαπιστώσει ότι το σημείο αυτό, 01000101, δεν ανήκει πλέον στην Alice κατ' επέκταση δεν έχει την αρμοδιότητα να το ξοδέψει. Η κεντρική βάση δεδομένων λύνει το πρόβλημα της διπλής κατανάλωσης. Υπάρχουν όμως θέματα που συνδέονται με την κεντρική βάση δεδομένων. Καταρχάς, όλοι οι χρήστες θα πρέπει προηγουμένως να έχουν κάνει εγγραφή στον κεντρικό server προκειμένου να λειτουργήσει. Έπειτα η κεντρική βάση δεδομένων αναγνωρίζει τις ταυτότητες όλων των χρηστών και συλλέγει το οικονομικό ιστορικό τους. Επίσης μια κεντρική βάση δεδομένων είναι εύκολο να γίνει στόχος επιθέσεων είτε από εσωτερικούς είτε από εξωτερικούς παράγοντες. Εάν το άτομο που θα επιτεθεί πάρει τον έλεγχο της κεντρικής βάσης δεδομένων τότε μπορεί να αλλάξει την ιδιοκτησία των κεφαλαίων και να τα κλέψει από τους νόμιμους ιδιοκτήτες ή θα μπορούσε να δημιουργήσει νέα κεφάλαια (σημεία) και να τα ορίσει στον εαυτό του. Ίσως το κυριότερο μειονέκτημα ενός κεντρικού server είναι ότι αποτελείται από ένα ενιαίο σημείο αποτυχίας, όπως φαίνεται στην εικόνα (βλέπε εικόνα 3) το σύστημα πληρωμής μπορεί άνετα να απορριφθεί κλείνοντας τον κεντρικό server.



Εικόνα 3. Σημείο αποτυχίας κεντρικής καταμέτρησης

Μερικά πρόωρα ψηφιακά συστήματα πληρωμής βασίστηκαν στην ιδέα μιας κεντρικής βάσης δεδομένων που θα διατηρεί τις θέσεις όλων των χρηστών όπως είναι το e-gold[8] και Liberty Reserve[9]. (Pedro Franco, 2014)

3.2 The Blockchain ή αλυσίδα των block

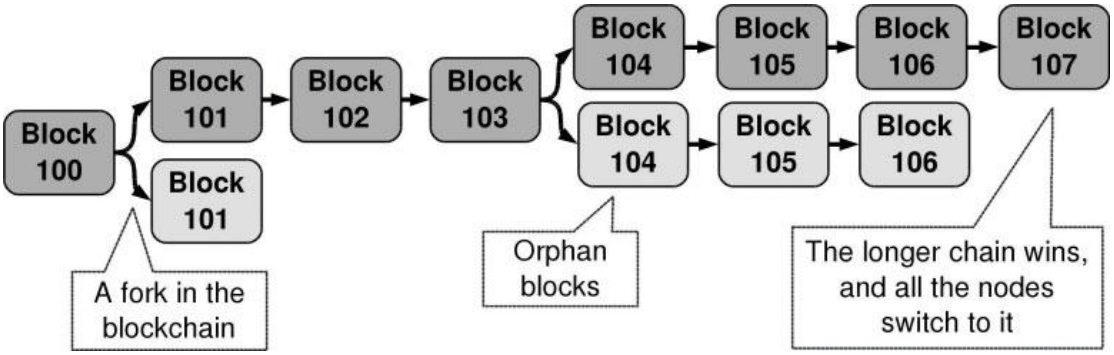
Η κατανεμημένη βάση δεδομένων των Bitcoins ονομάζεται blockchain. Οι συναλλαγές ομαδοποιούνται κατά προσέγγιση κάθε δέκα λεπτά. Αυτές οι ομάδες συναλλαγών είναι οι καταγεγραμμένες έπειτα από αλυσίδες ομάδων, γι' αυτό και το όνομα blockchain. Μπορεί να είναι παράξενος τρόπος καταγραφής πληροφοριών εν συγκρίσει με μια συνηθισμένη σχεσιακή βάση δεδομένων. Το blockchain σχεδιάστηκε για να είναι ευέλικτο σε περίπτωση που γίνει επίθεση στο δίκτυο. Οι ομάδες είναι συνδεδεμένες να δημιουργούν αρχείο του ιστορικού των συναλλαγών που δεν μπορεί να αλλαχθεί. Ο σύνδεσμος μεταξύ των ομάδων είναι κρυπτογραφημένος σύνδεσμος που δεν μπορεί να χτυπηθεί εκτός αν το άτομο που επιτίθεται έχει απέραντους υπολογιστικούς όρους στην διάθεση του. Το blockchain είναι αναμφισβήτητα η πιο σημαντική καινοτομία που εισήγαγε το Bitcoin. Είναι ο συνδετικός κρίκος που κάνει δυνατή την διανομή των peer-to-peer ψηφιακών νομισμάτων. Το blockchain είναι στην ουσία μια κατανεμημένη βάση δεδομένων που κατέχει όλες τις συναλλαγές Bitcoin από την αρχή (3 Ιανουαρίου του 2009) και είναι μια μέθοδος που εξασφαλίζει αυτή τη βάση δεδομένων. Διατηρεί έναν ασφαλή κατάλογο όλων των συναλλαγών. Ωστόσο, υπάρχει και ένα σχετικό ερώτημα, όπως το αν μια συγκεκριμένη συναλλαγή είναι διαθέσιμη να ξοδευτεί κάτι το οποίο δεν απαντάται άμεσα από το blockchain. Το λογισμικό που χρησιμοποιεί το blockchain, όπως για παράδειγμα κόμβους εξόρυξης "mining" ή πορτοφόλια, είναι κάτι το οποίο πρέπει να αναλύσει το blockchain, έτσι ώστε να εξάγει τις σχετικές πληροφορίες. Αυτή η πληροφορία που εξάγεται από το blockchain συνήθως τροφοδοτείται σε μια βάση δεδομένων. Για παράδειγμα, ο κόμβος του λογισμικού Bitcoin χρησιμοποιεί LevelDB, ένα «κατάστημα» τιμή-κλειδί το οποίο θα κρατήσει ένα αντίγραφο της συναλλαγής που δεν έχει πραγματοποιηθεί. Το blockchain χρησιμοποιεί απόδειξη της εργασίας για να εξασφαλίσει την κατανεμημένη βάση

[8] e - Gold ήταν ένα ψηφιακό χρυσό νόμισμα που λειτουργεί από το Gold & Silver Reserve Inc

[9] Liberty Reserve ήταν μια κεντρική ψηφιακή υπηρεσία νομίσματος από την Costa Rica η οποία αξιολογείται ως ο παλαιότερος, πιο ασφαλής και πιο δημοφιλής επεξεργαστής πληρωμών

δεδομένων. Αυτό σημαίνει πως το blockchain ασφαλίζεται έναντι κάποιας προσπάθειας ενδεχόμενης παραβίασης από την επεξεργαστική ισχύ που έχει εφαρμοστεί για τη δημιουργία του. Ένας χρήστης που επρόκειτο να επιτεθεί, επιθυμεί να αλλάξει το blockchain, σε αυτήν την περίπτωση θα πρέπει να εφαρμοστεί μια επεξεργαστική ισχύ ισοδύναμη με όλη την επεξεργαστική ισχύ από ότι χρονική στιγμή που δαπανάται η συναλλαγή μέχρι την παρούσα. Επιπλέον, ο εισβολέας θα πρέπει να ξεπεράσει το νόμιμο δίκτυο Bitcoin, το οποίο διατηρεί την προσθήκη καταχωρήσεων στην κατανεμημένη βάση δεδομένων. Είναι εύκολο να ρυθμιστεί η δυσκολία των block και αυτό εξαρτάται ανάλογα με την αύξηση του αριθμού των αρχικών μηδενικών των δυαδικών ψηφίων. Το πρωτόκολλο Bitcoin προσαρμόζει την δυσκολία του στα 10 λεπτά μεταξύ των block. Αυτού του είδους η δυσκολία αποτελεί μέρος των κανόνων του Bitcoin και είναι κωδικοποιημένο σε κάθε πελάτη του δικτύου Bitcoin. Η δυσκολία των block ρυθμίζεται κάθε 2.016 block ή περίπου κάθε δύο βδομάδες. Η προσαρμογή λαμβάνει υπόψη της τη μεταβολή της επεξεργαστικής ισχύς του συνολικού δικτύου από την τελευταία αναπροσαρμογή. Όταν η δύναμη της εξόρυξης έρχεται να προστεθεί στο δίκτυο, τα blocks θα προσαρμόσουν την δυσκολία σε διάστημα μικρότερο των 10 λεπτών. Ωστόσο, η δυσκολία θα προσαρμοστεί σε υψηλότερο επίπεδο αλλά θα μειωθεί η δύναμη του δικτύου. Η καινοτομία που παρουσιάζει το Bitcoin είναι ο συνδυασμός του time-stampimg και του Hashcash σαν απόδειξη λειτουργίας. (Conrad Barski, Chris Wilmer, 2014). Το blockchain είναι μια συνεχώς αυξανόμενη αλυσίδα από blocks. Κάθε block περιέχει μια ομάδα από νέες συναλλαγές και ένα link στο προηγούμενο block της αλυσίδας. Οι νέες συναλλαγές στο δίκτυο συλλέγονται στο block που προσαρτάται στο blockchain. Σημειώνεται ότι η παλιά συναλλαγή βρίσκεται ακόμα στο blockchain: τα παλιά blocks δεν αφαιρούνται ποτέ από το blockchain έτσι το blockchain μπορεί μόνο να μεγαλώνει το μήκος του. Κάθε block περιλαμβάνει μια ειδική συναλλαγή που ονομάζεται νομισματική βάση, η οποία είναι και η πρώτη συναλλαγή μέσα στο block. Έχει επίσης, μόνο μια συναλλαγή εισροών που δεν συνδέεται με καμία προηγούμενη συναλλαγή εκροών και δεν εξυπηρετεί κανένα σκοπό. Από την άλλη πλευρά η νομισματική βάση έχει πολλές εκροές. Το άθροισμα των τιμών αυτών των εκροών ισούται με την ανταμοιβή του block, καθώς και το άθροισμα όλων των χρεώσεων που καταχωρούνται από τις συναλλαγές που συλλέγονται στο block. Τα blocks συνήθως περιλαμβάνουν πολλές συναλλαγές εκτός από την νομισματική βάση. Αλλά ένα έγκυρο block μπορεί να δημιουργηθεί χωρίς να συμπεριλάβει καμία άλλη συναλλαγή εκτός από την νομισματική βάση. Στην πραγματικότητα, αυτού του είδους το block ήταν το συνηθέστερο στο ξεκίνημα του δικτύου bitcoin, όταν πολύ λίγες συναλλαγές αναμεταδίδονταν. Αυτά τα “άδεια” blocks βοηθούν να διασφαλίζεται το blockchain και αναθέτουν στους miners του block την ανταμοιβή τους. Οι miners μπορούν να επιλέξουν ποια συναλλαγή θα συμπεριλάβουν στο mine του block και συνήθως αποφασίζουν να εισάγουν βασιζόμενα στην χρέωση που θα πληρώσουν. Η διαδικασία επίλυσης των blocks ονομάζεται εξόρυξη (mining) και είναι ανάλογη με την εξόρυξη πολύτιμων μετάλλων. Οι miners ανταμείβονται με το νέο νόμισμα. Αυτή η αναλογία αν και χρήσιμη μπορεί να διαρκέσει πολύ. Η ανταμοιβή του block ρυθμίζεται από το πρωτόκολλο και δεν επηρεάζεται από τον αριθμό των miners ή από το έργο που παράγουν. Σε αντίθεση με την εξόρυξη των πολύτιμων μετάλλων, η επένδυση στην αύξηση των ανθρακωρύχων (miners) δεν θα αυξήσει και τα κυκλοφορούντα bitcoins. Η επένδυση στην αύξηση των ανθρακωρύχων (miners) θα αυξήσει το συνολικό ποσοστό του κατακερματισμού, μειώνοντας έτσι τα ποσοστά των αρχικών ανθρακωρύχων (miners), κρατώντας έτσι ολόκληρη την ανταμοιβή για την συνέχιση του δικτύου. Το block που προηγείται από ένα συγκεκριμένο block ονομάζεται γονέας (parent block). Κάθε block αναφέρει τον γονέα του (parent block) στο blockchain προσθέτοντας τον κατακερματισμό στην δομή δεδομένων του, έτσι το blockchain κρατάει τα blocks με χρονολογική σειρά. Το πρώτο block στο blockchain ονομάζεται genesis block και δημιουργήθηκε από τον Satoshi στις 3 Ιανουαρίου 2009. Η σειρά ενός block στο blockchain ξεκινώντας από το genesis block ονομάζεται block height. Το τελευταίο block που προστίθεται στο blockchain ονομάζεται blockchain head. Τα

νέα blocks προστίθενται πάνω από το blockchain head. Ένα “πιρούνι”(fork) συμβαίνει όταν δύο ανθρακωρύχοι (miners) φτάσουν σε ένα νέο block περίπου την ίδια ώρα. Και τα δύο blocks λύνουν το πρόβλημα μερικής αναστροφής κατακερματισμού, αλλά μόνο ένα από αυτά μπορεί να είναι μέρος του μακροπρόθεσμου blockchain. Το block που απορρίπτεται ονομάζεται orphan block.



Εικόνα 4. Dynamics of the blockchain

Όπως φαίνεται στην εικόνα (βλέπε εικόνα 4) μπορεί να παρουσιαστεί “πιρούνι” (fork) αρκετές φορές. Αυτό συμβαίνει όταν υπάρχει διαχωρισμός στο δίκτυο και οι ανθρακωρύχοι θεωρούν ότι ένα “υποκατάστημα”/branch του “πιρουνιού” (fork) είναι το νόμιμο blockchain ενώ οι υπόλοιποι ακολουθούν το άλλο “υποκατάστημα”/branch. Το πρωτόκολλο καθορίζει ότι το σωστό blockchain είναι το μεγαλύτερο. Έτσι οι ανθρακωρύχοι έχουν κίνητρο το σταμάτημα των εργασιών μόλις είναι προφανές ότι θα είναι ορφανό (orphaned) διότι θα ήταν χάσιμο χρόνου να συνεχίσουν να δουλεύουν σε τέτοιου είδους “υποκατάστημα”/branch. Υπάρχουν “πιρούνια” που βρίσκουν την λύση τους γρήγορα και μόνα τους, συνήθως σε ένα block. Ο μέσος αριθμός “πιρουνιών” είναι γύρο στο 2%, για παράδειγμα για κάθε 50 blocks υπάρχει ένα “πιρούνι” στο blockchain. Τα “πιρούνια” σε περισσότερα από ένα block είναι πολύ συνηθισμένα. Οι συναλλαγές που συμπεριλαμβάνονται στο block ενός “πιρουνιού” (fork) δεν χάνονται. Όταν ένα “πιρούνι” επιλυθεί και το υποκατάστημα του blockchain απορρίπτεται, οι συναλλαγές στον εν λόγω κλάδο εισάγονται και πάλι στις ανεπιβεβαίωτες συναλλαγές memory pool, έτοιμο να συμπεριληφθεί στο επόμενο block εξόρυξης. Ορισμένες από αυτές τις συναλλαγές μπορεί να εμφανίζονται ήδη σε ένα block του νόμιμου “υποκαταστήματος” του “πιρουνιού”. Σε αυτή την περίπτωση, η συναλλαγή απορρίπτεται και εξαιρείται από τις ανεπιβεβαίωτες συναλλαγές memory pool. Κάθε ανάλυση του “πιρουνιού” παράγει νικητές (οι ανθρακωρύχοι που λύνουν το block στο αποδεκτό “υποκατάστημα”/branch) και ηττημένους (οι ανθρακωρύχοι που λύνουν τα ορφανά blocks). Το πρωτόκολλο αποφεύγει να έχει κεντρικό κόμμα ή ομάδα που θα αποφασίζει για το σωστό “υποκατάστημα”/branch, σύμφωνα με την φιλοσοφία αποκέντρωσης του Bitcoin. Το πρωτόκολλο του Bitcoin λύνει το “πιρούνι” για χάρη του μεγαλύτερου blockchain. Το μήκος του blockchain μετράται από το συνδυασμό της δυσκολίας όλων των blocks στην αλυσίδα. Εάν η δυσκολία του blockchain μετριόταν από τον αριθμό των blocks ένας που θα ήθελε να επιτεθεί στο σύστημα θα μπορούσε να δημιουργήσει πολλά “διαθέσιμα” blocks με μικρότερη δυσκολία από ότι το νόμιμο blockchain, έτσι θα κέρδιζε τον αγώνα του blockchain κλέβοντας. Το δίκτυο του Bitcoin

αποτελείται από κόμβους. Οι κόμβοι είναι οι υπολογιστές που είναι συνδεδεμένοι στο Internet, που τρέχουν το λογισμικό του Bitcoin. Το δίκτυο του Bitcoin είναι peer-to-peer δίκτυο: όλοι οι κόμβοι είναι ομοιογενείς. Οι κόμβοι λαμβάνουν συναλλαγές και blocks από άλλους κόμβους και αναμεταδίδουν αυτές τις συναλλαγές και τα blocks σε άλλους κόμβους. Κάθε κόμβος κρατά ένα ολόκληρο αντίγραφο του blockchain. Μια νεοϊδρυθείσα συναλλαγή που δεν έχει συμπεριληφθεί σε κανένα block ονομάζεται ανεπιβεβαίωτη συναλλαγή. Μόλις η συναλλαγή συμπεριληφθεί σε ένα block λέγεται ότι επιβεβαιώθηκε. Εάν η συναλλαγή είναι επιβεβαιωμένη εξαρτάται από τον βαθμό: όσο ποιο πολλά blocks προστεθούν στην κορφή της blockchain τόσο ποιο δύσκολο είναι να δημιουργηθεί επίθεση διπλής κατανάλωσης ενάντια σε μια συναλλαγή. Τέλος εκτός από το ολόκληρο αντίγραφο του blockchain ο κόμβος κρατάει επίσης επιπρόσθετες δομές δεδομένων όπως την μνήμη των μη ξοδεμένων συναλλαγών εκροών ή τις μη επιβεβαιωμένες συναλλαγές από την memory pool, έτσι ώστε να μπορεί γρήγορα να επικυρώσει νέες παραλαβές συναλλαγών και blocks που έχουν περάσει την διαδικασία της εξόρυξης. Εάν η παραλαβή της συναλλαγής ή του block είναι έγκυρη, οι κόμβοι ενημερώνουν τις δομές δεδομένων και το αναμεταδίδουν στους συνδεδεμένους κόμβους. Είναι σημαντικό να σημειωθεί ότι ένας κόμβος δεν χρειάζεται να εμπιστεύεται άλλους κόμβους, γιατί επικυρώνει ανεξάρτητα όλες τις πληροφορίες που λαμβάνει από αυτούς. (Pedro Franco, 2014)

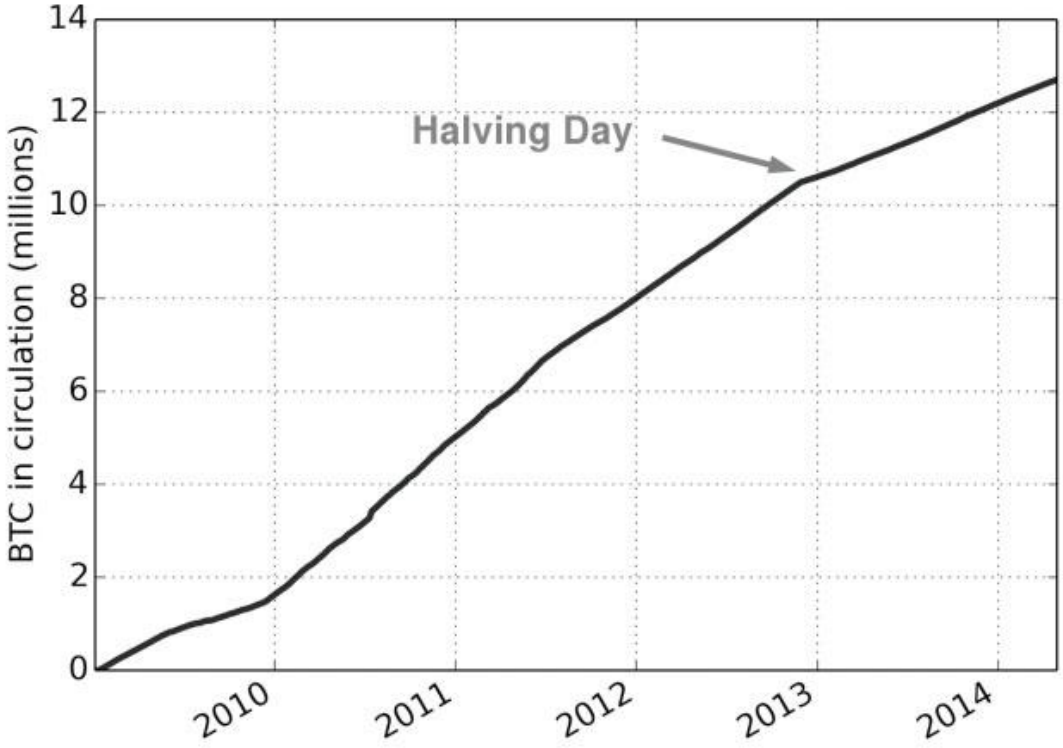
3.4 Mining ή «εξορύξεις»

Το mining είναι η διαδικασία προσθήκης αρχείων στο blockchain. Οι miners συνεισφέρουν με την εξουσία που έχουν πάνω στους υπολογιστές να επιλύσουν τα αρχεία που προστίθενται στο blockchain, το διαδίκτυο αμείβει τους miners με τα τέλη που εισπράττονται από όλες τις συναλλαγές που περιλαμβάνονται στο αρχείο. Οι miners λύνουν το πρόβλημα κατακερματισμού με μερική αναστροφή. Για να βρεθεί μια λύση, το λογισμικό mining συνήθως αυξάνει το nonce[10] των αρχείων και τρέχει τον αλγόριθμο, ο οποίος αλγόριθμος αποδεικνύει αν το επιλεγμένο nonce δημιουργεί έναν σωστό κατακερματισμό των αρχείων, δηλαδή έναν κατακερματισμό των αρχείων που πληροί τις απαιτήσεις. Η τυπική βελτιστοποίηση που χρησιμοποιείται από τους miners είναι να προϋπολογιστεί ο κατακερματισμός του αρχικού τμήματος της κεφαλίδας του αρχείου που περιέχει τον προηγούμενο κατακερματισμό του αρχείου και το δέντρο συναλλαγής Merkle.[11] Αυτό το μέρος της κεφαλίδας του αρχείου είναι σταθερή κατά τη διάρκεια της διαδικασίας mining και ως εκ τούτου μπορούν να αποθηκευτούν σε ένα ρυθμιστικό απόθεμα. Ένα από τα πλεονεκτήματα του μηχανισμού mining είναι η έγκαιρη ανταμοιβή αυτών που την υιοθετούν για την υποστήριξη του δικτύου. Το mining είναι παρόμοιο με μια αγορά με τέλειο ανταγωνισμό εφ 'όσον υπάρχει κέρδος, οι νεοεισερχόμενοι θα εισέλθουν στην αγορά έως ότου η ευκαιρία κέρδους να εξαντληθεί. Η δυσκολία του mining αυξάνεται καθώς περισσότεροι miners εισέρχονται στο δίκτυο, αλλά το σύνολο ανταμοιβής των αρχείων παραμένει το ίδιο. Κατά τη δημιουργία του Bitcoin, η ανταμοιβή των αρχείων ήταν 50 bitcoins. Αυτή η ανταμοιβή υποδιπλασιάζεται κάθε 210.000 blocks ή περίπου κάθε 4 χρόνια, για να συμμορφωθούν με τον ρυθμό δημιουργίας χρημάτων που καθορίζεται στο

[10] Το " nonce " σε ένα αρχείο Bitcoin είναι 32 -bit (4 - byte) πεδίο του οποίου η τιμή έχει οριστεί έτσι ώστε ο κατακερματισμός του αρχείου θα περιέχει στο τρέξιμο μηδενικά .

[11] Στην κρυπτογραφία και την επιστήμη των υπολογιστών , ένα δέντρο κατακερματισμού ή Merkle δέντρο είναι ένα δέντρο στο οποίο κάθε κόμβος μη - φύλλο επισημαίνεται με τον κατακερματισμό των ετικετών των κόμβων “παιδιών” του .

πρωτόκολλο. Σημειωτέον, η έκδοση των νέων bitcoins δεν είναι μια ομαλή διαδικασία, καθώς η εισαγωγή της νέας παραγωγικής ικανότητας του mining αυξάνει προσωρινά το ρυθμό δημιουργίας νέων θέσεων κατά κατηγορία μέχρι την ανατροφοδότηση του μηχανισμού των αλιευμάτων. Έτσι, σύμφωνα με τον αυξανόμενο ρυθμό κατακερματισμού του διαδικτύου, η έκδοση των νέων bitcoins επιταχύνεται κάπως. Στις 28 Νοεμβρίου του 2012 ένα μήνα πριν από το χρονοδιάγραμμα, η ανταμοιβή των αρχείων μειώθηκε κατά το ήμισυ σε 25 bitcoins. Την μέρα που γράφτηκε αυτό , η ανταμοιβή των πρωτόκολλων ήταν περίπου $24 \cdot 6 \cdot 25 = 3.600$ bitcoins κάθε μέρα. (Pedro Franco, 2014)



Εικόνα 5. Halving Day

Το Bitcoin είναι ένα δίκτυο peer-to-peer όπου ο καθένας μπορεί να συνδεθεί σε αυτό και να αρχίσει το mining του αμέσως. Οι νεοεισερχόμενοι δεν χρειάζεται να ζητήσουν κάποια άδεια ή να προσκολληθούν σε ένα σύνολο κανόνων ή σε κάποιους κανονισμούς πριν την είσοδό τους στην αγορά. Ούτε μπορούν οι κατεστημένοι φορείς να συνωμοτήσουν για την πρόληψη νέων συμμετεχόντων όσον αφορά την είσοδο τους. Έτσι, οι νέες επενδύσεις θα εισαχθούν στο διαγωνισμό για να πάρουν την ανταμοιβή των αρχείων, μειώνοντας την αμοιβή όλων των miners που είναι ήδη στο δίκτυο. Έτσι, το σενάριο της αύξησης της τιμής Bitcoin ή η αυξανόμενη τεχνολογική πρόοδο, οι miners θα πρέπει να κρατήσουν την αύξηση του ρυθμού κατακερματισμού τους, προκειμένου να επιτευχθεί η ίδια ανταμοιβή, σε μια διαδικασία παρόμοια με την Red Queen Effect[12]. Αυτή η διαδικασία θα συνεχιστεί μέχρι το οριακό κόστος του τελευταίου miner που θα ισούται με τα προσδοκώμενα κέρδη του. Σε αυτό το σημείο,

[12] Η Red Queen Effect αναφέρεται σε καταστάσεις όπου οι ανταγωνιστές θα πρέπει συνεχώς να εξελίσσονται , να μην κερδίσουν κανένα πλεονέκτημα , αρκεί απλώς να επιβιώσουν σε ένα άκρως ανταγωνιστικό περιβάλλον .

το δίκτυο έχει φτάσει σε μια ισορροπία, η οποία μπορεί να διαταραχθεί μόνο από κάποιον εξωτερικό παράγοντα, όπως μία περαιτέρω αύξηση των τιμών του Bitcoin.

- **Technological advantage.** Αυτό το τεχνολογικό πλεονέκτημα θα μπορούσε να προέρχεται είτε από μια καινοτομία στην εφαρμογή του αλγόριθμου «απόδειξη εργασίας» SHA256 ^2 στο υλικό από σιλικόνη είτε θα μπορούσε να προέρχεται από κάποιον miner που ακολουθεί μια βελτιωμένη διαδικασία παραγωγής chip , με τον ίδιο τρόπο που ένας παραγωγός chip εισέρχεται στον επιχειρησιακό κόσμο του mining.
- **Hedging Bitcoin volatility.** Ένας miner έχει το πλεονέκτημα εάν είναι σε θέση να αντισταθμίσει τη μεταβλητότητα της τιμής Bitcoin πιο αποτελεσματικά απ' ότι οι ανταγωνιστές του. Κάθε miner μπορεί να αντισταθμίσει την αστάθεια της τιμής Bitcoin χρησιμοποιώντας Bitcoin futures[13], στην παρούσα φάση, αυτή η αγορά είναι σχεδόν ανύπαρκτη. Αυτό το πλεονέκτημα θα μπορούσε να είναι ιδιαίτερα σημαντικό κατά τη διάρκεια της περιόδου όπου η τιμή του Bitcoin είναι σε ύφεση και οι ανταγωνιστές είναι αναγκασμένοι να κλείσουν στην τιμή αυτή[14]. Ακόμη περισσότερο, όταν ένας miner που είναι σε θέση να καλύψει την μεταβλητότητα των εσόδων του θα απαιτούσε ένα χαμηλότερο ποσοστό απόδοσης των επενδύσεων του.
- **Lower electricity prices**. Οι miners οι οποίοι είναι σε θέση να εξασφαλίσουν χαμηλές τιμές της ηλεκτρικής ενέργειας έχουν πλεονέκτημα κόστους. Το Bitcoin mining είναι πιθανό να μεταναστεύσει σε περιοχές με άφθονη και μειωμένη τιμή ηλεκτρικής ενέργειας, όπως για παράδειγμα η Ισλανδία. Αυτό ενδεχομένως να μειώσει το περιβαλλοντικό αντίκτυπο του Bitcoin mining, ως τόπος με φθηνότερη τιμή της ηλεκτρικής ενέργειας είναι σε θέση να παράγει φιλικές προς το περιβάλλον πηγές, όπως υδροηλεκτρικές εγκαταστάσεις.

Εν ολίγοις, οι φραγμοί εισόδου στην μεταλλευτική επιχείρηση είναι γενικά χαμηλή, καθώς δεν υπάρχει τρόπος για τους κατεστημένους φορείς να βρουν κάποιο μέσο και να αποτρέψουν την είσοδο του διαδικτύου στον νέο ανταγωνισμό. Ως εκ τούτου, το ποσοστό κατακερματισμού του διαδικτύου κατά πάσα πιθανότητα θα σταθεροποιηθεί σε ποσοστό όπου η ανταμοιβή του mining θα καλύπτει μόνο το οριακό κόστος της λειτουργίας του εξοπλισμού του mining. Το οριακό κόστος της λειτουργίας του εξοπλισμού mining περιλαμβάνει το κόστος της ηλεκτρικής ενέργειας αλλά και τις δαπάνες ενοικίασης του κέντρου δεδομένων, το κόστος ψύξης, συντήρησης, και ούτω καθεξής. Υπάρχει ωστόσο και το κόστος απόσβεσης του ίδιου του εξοπλισμού ή κόστος ευκαιρίας. Αξίζει να αναφερθεί ότι είναι το μόνο σήμερα με βιώσιμη τεχνολογία ASIC η οποία βελτιστοποιεί το mining Bitcoin, μάλιστα δεν υπάρχει καμία άλλη εναλλακτική για χρήση. Αυτοί οι παράγοντες, σε συνδυασμό με την καθυστέρηση στην παραγωγή του εξοπλισμού mining σε απάντηση στις αυξήσεις των τιμών του Bitcoin, θα μπορούσε να δημιουργήσει «ένα μπαμ» στη μεταλλευτική αγορά. (Pedro Franco, 2014)

[13] Μια σύντομη θέση Bitcoin στο μέλλον θα καταβάλει τη διαφορά μεταξύ της τιμής του Bitcoin κατά τη έναρξη της σύμβασης και την τιμή του Bitcoin σε προκαθορισμένη ημερομηνία. Για παράδειγμα, εάν η τιμή από ένα Bitcoin έχει μειωθεί από 600 δολάρια σε 500 δολάρια, στο σύντομο μέλλον θα πληρώσει 600 δολάρια - 500 USD = 100 δολάρια. Ένας miner που κατέχει αρνητική θέση σε αυτή τη μελλοντική σύμβαση θα μπορούσε στην πράξη να κλειδώσει μια μελλοντική τιμή Bitcoin 600 USD: 500 δολάρια που προέρχονται από την αγορά κατά τη λήξη της σύμβαση και 100 δολάρια που προέρχονται από την εξόφληση της μελλοντικής σύμβασης.

[14] Αυτό μπορεί να αποδειχθεί ότι δεν είναι σημαντικό πλεονέκτημα: επειδή, ακόμα κι αν μερικοί miners απενεργοποιήσουν την mining του υλικού κατά τη διάρκεια ορισμένων περιόδων, το υλικό όμως θα είναι ακόμα εκεί και θα μπορούσε να μετατραπεί στην περίπτωση που η τιμή του Bitcoin ανακτηθεί.

3.5 Wallets ή πορτοφόλια

Το λογισμικό αυτό το οποίο είναι σε θέση να βοηθήσει έναν χρήστη όσον αφορά την διαχείριση των κεφαλαίων του, ονομάζεται πορτοφόλι ή wallet. Οι λειτουργίες του λογισμικού αυτού εν ονόματι πορτοφόλι είναι να κρατάει με ασφάλεια τα ιδιωτικά κλειδιά του χρήστη, τη δημιουργία συναλλαγών οι οποίες αποστέλλονται στο διαδίκτυο και στην συνέχεια συλλέγουν τις εισερχόμενες και εξερχόμενες συναλλαγές ώστε να φανεί η ισορροπία των κεφαλαίων που είναι διαθέσιμα για τον χρήστη. Καθώς ένας χρήστης μπορεί να είναι ιδιοκτήτης πολλών διευθύνσεων, τα περισσότερα πορτοφόλια λογισμικού είναι έτοιμα να διαχειριστούν πολλαπλές διευθύνσεις και συνεπώς την άθροιση των κεφαλαίων μεταξύ τους. Ολόκληρο το λογισμικό αυτό μπορεί να δημιουργήσει νέες διευθύνσεις όταν εκτελείται για πρώτη φορά. Η δημιουργία μίας διεύθυνσης Bitcoin είναι απλή και άμεση. Το πορτοφόλι υλοποιεί επίσης το πρωτόκολλο κρυπτογράφησης για να υπογραφεί μια συναλλαγή με το ιδιωτικό κλειδί. Τα ιδιωτικά κλειδιά συνήθως φυλάσσονται στη συσκευή. Η απώλεια αυτών των ιδιωτικών κλειδιών εμποδίζουν την πρόσβαση στα κεφάλαια του χρήστη. Τα κεφάλαια δεν έχουν διανεμηθεί ακόμα στο καθολικό αλλά χωρίς τα ιδιωτικά κλειδιά δεν υπάρχει κανένας τρόπος να υπογραφεί και να περαστεί σωστά μια συναλλαγή και ως εκ τούτου, θεωρούνται χαμένα. Έτσι, συνιστάται, ιδιαίτερα, η δημιουργία αντίγραφων ασφαλείας των ιδιωτικών κλειδιών που δημιουργούνται. Τα περισσότερα πορτοφόλια βοηθούν τον χρήστη στη δημιουργία ψηφιακών αντίγραφων ασφαλείας. Ένας άλλος κίνδυνος των πορτοφολιών είναι “οι εισβολείς” οι οποίοι είναι πρόσωπα μη εξουσιοδοτημένα και σκοπός τους είναι να πάρουν στα χέρια τους τα ιδιωτικά κλειδιά. Εάν κάποιος εισβολέας επιτεθεί προκειμένου να αποκτήσει πρόσβαση στα ιδιωτικά κλειδιά, αυτό μπορεί να στείλει τα κεφάλαια στις διευθύνσεις που σχετίζονται με ορισμένες διευθύνσεις υπό τον έλεγχό του. Επομένως, είναι ξεκάθαρο πόσο σημαντικό είναι να ασφαλιστούν σωστά τα ιδιωτικά κλειδιά τα οποία αποθηκεύονται σε συσκευές που είναι συνδεδεμένες στο διαδίκτυο. Πολλά πορτοφόλια προσφέρουν κρυπτογράφηση του ιδιωτικού κλειδιού πριν αποθηκευτούν τοπικά. Αυτό μειώνει την ευκολία για το χρήστη, ο οποίος θα πρέπει να πληκτρολογήσει τον κωδικό πρόσβασης για την αποκρυπτογράφηση των ιδιωτικών κλειδιών πριν την χρήση τους, όπως ακριβώς συμβαίνει κατά την αποστολή μιας συναλλαγής. Σε περίπτωση που η συσκευή είναι σε κίνδυνο, ο εισβολέας θα είναι σε θέση να πάρει μόνο ένα αντίγραφο των κρυπτογραφημένων ιδιωτικών κλειδιών. (Conrad Barski, Chris Wilmer, 2014) και (Pedro Franco, 2014)

3.5.1 Offline wallets ή πορτοφόλια εκτός σύνδεσης

Συνήθως η συσκευή που διαθέτει ένα πορτοφόλι είναι συνδεδεμένο στο διαδίκτυο, προκειμένου να επικοινωνεί με το δίκτυο Bitcoin (όπου λαμβάνει υπόψη την κατάσταση του λογαριασμού, την αποστολή των συναλλαγών, την παρατήρηση των επιβεβαιώσεων και ούτω καθεξής). Αυτό που προαναφέρθηκε, ονομάζεται online πορτοφόλι ή αλλιώς “hot” πορτοφόλι. Κάθε συσκευή, η οποία είναι συνδεδεμένη στο διαδίκτυο είναι λογικό να διακατέχει κάποιον κίνδυνο, καλό θα ήταν να παραμείνουν στα πορτοφόλια τα απαραίτητα κεφάλαια της καθημερινής λειτουργίας σε απευθείας σύνδεσης. Το υπόλοιπο των κεφαλαίων του χρήστη θα πρέπει να διατηρείται σε πορτοφόλια εκτός δικτύου για μεγαλύτερη ασφάλεια, του οποίου τα ιδιωτικά κλειδιά δεν έχουν καμία πρόσβαση στο διαδίκτυο. Αξιοσημείωτο είναι ότι ένα μη συνδεδεμένο πορτοφόλι μπορεί να πραγματοποιήσει συναλλαγές εκτός σύνδεσης. Η αποθήκευση αναφέρεται σε ένα μέρος όπου τα ιδιωτικά κλειδιά φυλάσσονται και δεν είναι προσπελάσιμη από το διαδίκτυο. Ιδιωτικά κλειδιά που διατηρούνται σε προσωρινή

παύση, πρέπει να εισάγονται σε ένα πορτοφόλι (είτε πρόκειται για ένα online ή offline πορτοφόλι) πριν από την διάθεση του κεφαλαίου. (Pedro Francon, 2014)

- **Paper wallet:** Ένας άλλος τρόπος για να δημιουργήσουν οι χρήστες προσωρινή παύση όσον αφορά τα ιδιωτικά κλειδιά είναι να εκτυπωθούν σε ένα κομμάτι χαρτί μέσω του οποίου θα είναι ασφαλέστερα σε περίπτωση κλοπής. Αυτά ονομάζονται χάρτινα πορτοφόλια, αν και τεχνικά δε θεωρούνται πορτοφόλια. Σε ένα χάρτινο πορτοφόλι, τα δημόσια κλειδιά ή οι διευθύνσεις Bitcoin συνήθως εκτυπώνονται μαζί με τα ιδιωτικά κλειδιά, έτσι ώστε το χάρτινο πορτοφόλι να μπορεί να προσδιοριστεί εύκολα, χωρίς να χρειάζεται να εισαχθεί το ιδιωτικό κλειδί. Εάν τα ιδιωτικά κλειδιά που δημιουργούνται τυχαία, όπως ακριβώς δημιουργούνται στον πυρήνα του πορτοφολιού Bitcoin, θα πρέπει να εκτυπωθεί ένα αντίγραφο κάθε ιδιωτικού κλειδιού. (Sam Patterson, 2013)
- **Hardware wallet:** είναι συσκευές οι οποίες αποθηκεύουν τα ιδιωτικά κλειδιά μέσω των οποίων πραγματοποιούνται οι συναλλαγές. Τα ιδιωτικά κλειδιά αυτά δεν εγκαταλείπουν ποτέ την συσκευή και έτσι δεν είναι δυνατόν να κατασχεθούν από τυχόν κακόβουλο λογισμικό στον υπολογιστή του χρήστη. Το hardware πορτοφόλι επικοινωνεί με ένα λογισμικό πορτοφόλι του πελάτη σε έναν υπολογιστή. Ο πελάτης αυτός μπορεί να είναι είτε ένα πρόγραμμα το οποίο είναι πορτοφόλι είτε ένα ηλεκτρονικό πορτοφόλι το οποίο τρέχει μέσα σε ένα πρόγραμμα περιήγησης στο διαδίκτυο. Σε κάθε περίπτωση, ο πελάτης ενεργεί μόνο ως μεσάζων μεταξύ του hardware πορτοφολιού και του blockchain, απλή διαβίβαση των συναλλαγών που πραγματοποιούνται μέσα στο hardware πορτοφόλι. Μερικά projects του software πορτοφολιού περιλαμβάνουν υποστήριξη για τα hardware πορτοφόλια. Οι συναλλαγές που αποστέλλονται από το πορτοφόλι του πελάτη στον υπολογιστή και μετά στο hardware πορτοφόλι μέσω κάποιας σύνδεσης, συνήθως αυτό είναι το USB. Οι συναλλαγές που έχουν πραγματοποιηθεί επιστρέφουν από το hardware πορτοφόλι μέσω της ίδιας σύνδεσης. Hardware πορτοφόλια έχουν συνήθως μια μικρή οθόνη οι οποίες δείχνουν στο χρήστη πληροφορίες σχετικές με τη συναλλαγή και μερικά κουμπιά τα οποία δίνουν την επιλογή στον χρήστη να αποφασίσει αν θα υπογράψει τη συναλλαγή ή θα την απορρίψει. Στην περίπτωση που το κακόβουλο λογισμικό έχει εγκατασταθεί στον υπολογιστή του χρήστη ενδεχομένως να αλλάξει τα στοιχεία της συναλλαγής που αποστέλλονται μέσω hardware πορτοφολιού. Η οθόνη του πορτοφολιού αυτού δείχνει λεπτομέρειες της συναλλαγής σχετικές με το αν υπογράφηκε πράγμα που σημαίνει ότι υπάρχει προστασία ενάντια σε αυτού του είδους την επίθεση. Είναι επίσης συνηθισμένο να απαιτείται ένας κωδικός πρόσβασης για να αποδέχεται τις συναλλαγές που προέρχονται από την σύνδεση. (Pedro Franco, 2014)

3.5.2 Web wallets ή πορτοφόλια μέσω διαδικτύου

Τα web πορτοφόλια είναι online λογαριασμοί συνδεδεμένα στο διαδίκτυο δηλαδή, με εξωτερικό πάροχο, κάτι που επιτρέπει στον χρήστη να μπορεί να καταθέσει τα χρήματα του. Τα κεφάλαια αυτά ελέγχονται από τον πάροχο του web πορτοφολιού. Μέσω της επαλήθευσης της ταυτότητας μαζί τον πάροχο του web πορτοφολιού, ο χρήστης έχει αργότερα την δυνατότητα πρόσβασης στα κεφάλαια αυτά, δηλαδή μπορεί να πραγματοποιήσει συναλλαγές. Το κύριο πλεονέκτημα του web πορτοφολιού δεν είναι άλλο από την εύκολη και γρήγορη εγγραφή του, συνεπώς η δημιουργία ενός λογαριασμού σε μια υπηρεσία μέσω διαδικτύου, αυτό σημαίνει ότι η δημιουργία των ιδιωτικών κλειδιών γίνεται από τον πάροχο του εν λόγω πορτοφολιού, μειώνοντας με

αυτόν τον τρόπο το εμπόδιο για την είσοδο νέων χρηστών. Υπάρχουν επιπλέον πλεονεκτήματα, όπως η χαμηλότερη προμήθεια στις συναλλαγές ή δυνατότητα να πραγματοποιούνται συναλλαγές μεταξύ των χρηστών της ίδιας υπηρεσίας ακαριαία και σε μηδέν τέλη. Πολλές από τις υπηρεσίες που προσφέρονται από τους παρόχους του web πορτοφολιού, προσφέρονται επίσης ανταλλαγές μέσω του διαδικτύου, τα οποία ονομάζονται τράπεζα Bitcoin, έτσι ώστε οι εκτιμήσεις του παρόντος τμήματος να εφαρμόζονται επίσης σε αυτές τις επιχειρήσεις. Τα πορτοφόλια Web είναι παρόμοια με τις τραπεζικές συναλλαγές που γίνονται μέσω διαδικτύου, υπό την έννοια ότι τα κεφάλαια φυλάσσονται από τον πάροχο του web πορτοφολιού. Ωστόσο, σε αντίθεση με την πολιτική της τράπεζας όπου οι καταθέσεις καλύπτονται με ασφάλεια τραπεζικών καταθέσεων, ο χρήστης δε θα μπορεί να προσφύγει νομικά κατά του παρόχου του web πορτοφολιού, ο οποίος ενδεχομένως να εξαφανιστεί με το κεφάλαιο. Επιπλέον, οι πάροχοι των web wallets δεν ελέγχονται διεξοδικά, όπως ακριβώς συμβαίνει στις τράπεζες και αυτό είναι ικανό να τονίσει ή να αυξήσει τυχόν αμφιβολίες όσον αφορά την φερεγγυότητα τους και την αξιοπιστία τους. Οι πρακτικές ασφαλείας για τους παρόχους των web wallets ή για τις ανταλλαγές είναι παρόμοιες με τις πρακτικές που υφίστανται όσον αφορά τους μεμονωμένους χρήστες. Όπου οι χρήστες θα πρέπει να αποθηκεύουν σε απευθείας σύνδεση πορτοφόλια μόνο το απαραίτητο κεφάλαιο της καθημερινής λειτουργίας και αντίθετα, να αποθηκευτεί το υπόλοιπο κεφάλαιο σε πορτοφόλια εκτός σύνδεσης ή σε προσωρινή παύση. Αξίζει να σημειωθεί ότι εκτός από τον κίνδυνο που διακατέχουν οι χρήστες, να κλαπεί δηλαδή το κεφάλαιο τους από το web wallet, υπάρχει ο κίνδυνος να χαθούν τα χρήματα επειδή ο πάροχος του πορτοφολιού είναι «χακαρισμένος», καθιστώντας την υπηρεσία μη φερέγγυα. Η χρήση των web wallets έχει επιπτώσεις στην ιδιωτική ζωή πάρα πολύ. Αφενός, η ανωνυμία του χρήστη διατηρείται, εφόσον οι διευθύνσεις που χρησιμοποιούνται στις συναλλαγές είναι εκείνες του πορτοφολιού χωρίς να υπάρχει άμεση σχέση με το χρήστη. Αφετέρου, η ανωνυμία δεν βρίσκεται σε τέτοιο βαθμό ώστε η λέξη αυτή να έχει την σημασία που αποδίδει στο 100%, διότι ο πάροχος του web πορτοφολιού συνήθως κρατά ένα αρχείο των συναλλαγών και με αυτόν τον τρόπο διατηρούνται οι προσωπικές πληροφορίες του χρήστη.

- **Hybrid web wallets** είναι τα web πορτοφόλια όπου τα ιδιωτικά κλειδιά αποθηκεύονται στον υπολογιστή αλλά η διαχείρισή του λογισμικού πραγματοποιείται από την υπηρεσία του παρόχου του πορτοφολιού. Οι συναλλαγές αρχίζουν από τους χρήστες, ανακοινώνονται πρώτα στον πάροχο του πορτοφολιού, ο οποίος αργότερα τις δημοσιεύει στο blockchain . Το πλεονέκτημα είναι η μειωμένη έκθεση του χρήστη στον πάροχο υπηρεσιών ενώ το μειονέκτημα είναι η αύξηση του κόστους για την διατήρηση ενός ασφαλούς συστήματος του χρήστη.

3.5.3 Brain wallets

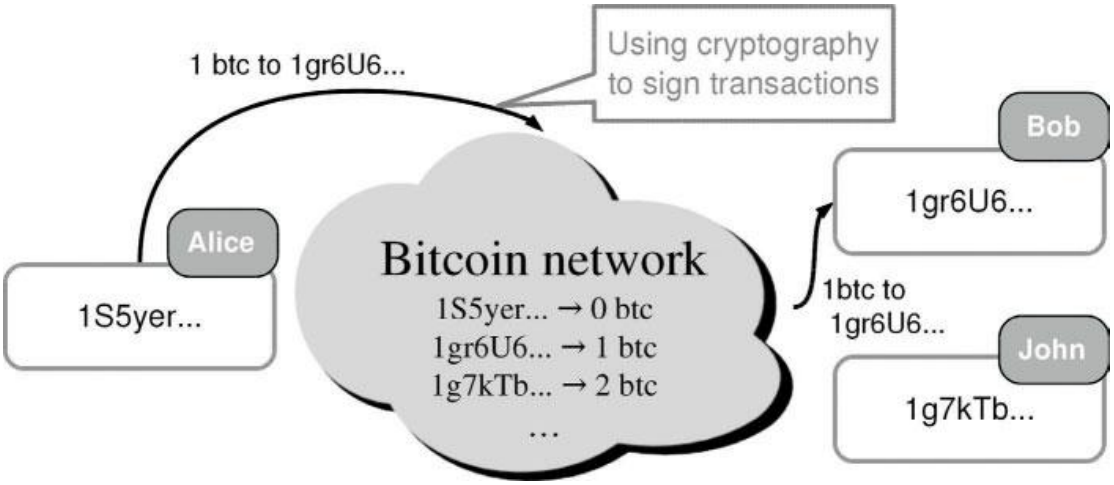
Τα brain πορτοφόλια έχουν την δυνατότητα να δημιουργούν ένα ιδιωτικό κλειδί από τον κατακερματισμό ενός μεγάλου κωδικού πρόσβασης ή μιας φράσης πρόσβασης. Τα ιδιωτικά κλειδιά του Bitcoin έχουν την δυνατότητα μεγέθους 256 bits, έτσι ώστε μια συνάρτηση κατακερματισμού που παράγει ένα κομμάτι 256 bits, όπως συμβαίνει στο SHA256[15], να μπορούν να χρησιμοποιηθούν. Ο κωδικός πρόσβασης ενός τέτοιου πορτοφολιού δεν χρειάζεται να αποθηκευτεί σε μια συσκευή διότι αποθηκεύεται στην μνήμη του χρήστη, εξ' ου και το όνομα του συγκεκριμένου πορτοφολιού. Αυτό έχει το πλεονέκτημα να μην απαιτούνται αντίγραφα ασφαλείας, με την προϋπόθεση, ωστόσο,

[15] Η Secure Hash Algorithm είναι μια οικογένεια κρυπτογραφικών hash λειτουργιών που δημοσιεύθηκαν από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) των ΗΠΑ ως ένα ομοσπονδιακό πρότυπο Επεξεργασίας Πληροφοριών

ο χρήστης να είναι σε θέση να θυμηθεί τον κωδικό πρόσβασης. Ο κωδικός πρόσβασης θα πρέπει ωστόσο να εισαχθεί σε ένα πραγματικό πορτοφόλι ώστε ο χρήστης να έχει πρόσβαση στο κεφάλαιο. Τα brain πορτοφόλια έχουν ένα μεγάλο μειονέκτημα που είναι λογικό να αποθαρρύνει τους χρήστες του. Υπόκεινται σε άγριες επιθέσεις μέσω της οποίας είναι δυνατό να κλαπούν όλα τα χρήματα από το πορτοφόλι σε περίπτωση επιτυχίας. Μια επίθεση τέτοιου τύπου δοκιμάζει πολλούς κωδικούς πρόσβασης και ελέγχει αν η διεύθυνση που παράγεται από τον κωδικό αυτόν υπάρχει και αν έχει χρήματα. Οι πιθανότητες επιτυχίας από αυτές τις επιθέσεις είναι πολύ υψηλή.

3.6 Transactions ή Συναλλαγές

Στο κέντρο του δικτύου Bitcoin είναι ένα αποκεντρωμένο καθολικό που περιέχει το υπόλοιπο του κάθε χρήστη. Το Bitcoin αναγνωρίζει τους χρήστες από μεγάλες συμβολοσειρές γραμμάτων και αριθμών όπως “13mckXc….” Η διεύθυνση είναι το δημόσιο μέρος ενός δημόσιου-απόρρητου κρυπτογραφικού κλειδιού . Το απόρρητο κομμάτι του κλειδιού είναι κάτω από τον έλεγχο του χρήστη.



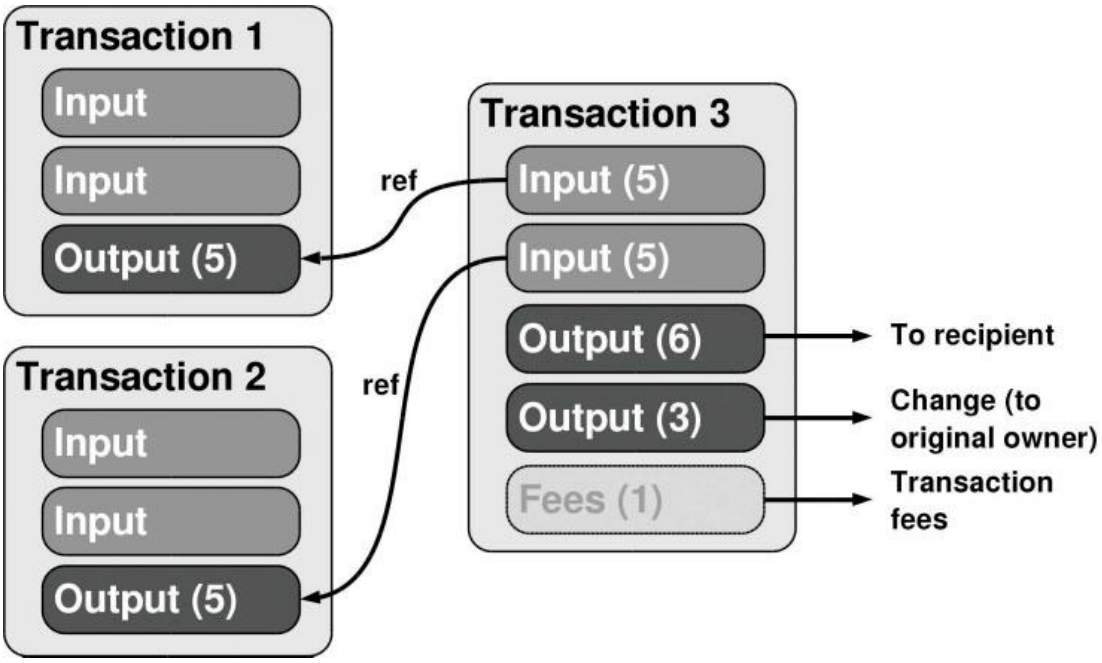
Σχήμα 6. User sending funds. State of the database after the transaction has settled

Το σχήμα δείχνει πως ένας χρήστης (Alice) στέλνει μερικά κεφάλαια σε έναν άλλο χρήστη (βλέπε σχήμα 6). Η Alice χρησιμοποιεί το δικό της ιδιωτικό κλειδί για να υπογράψει ένα μήνυμα λέγοντας «θέλω να στείλω 1 Bitcoin στο 1gr6U6.. που ανήκει στον Bob » που αυτή έστειλε στο δίκτυο. Να σημειωθεί ότι η Alice δεν προσδιορίζει τον χρήστη που θέλει να στείλει τα κεφάλαια αλλά την διεύθυνση που θα λάβει τα κεφάλαια. Έτσι η Alice πρέπει να ανακαλύψει την διεύθυνση του Bob με άλλους τρόπους. Μόλις λάβουν το μήνυμα της Alice, οι διαδικτυακοί κόμβοι ακολουθούν τα εξής βήματα:

- Επιβεβαιώνουν ότι η υπογραφή είναι σωστή. Εάν δεν είναι, απορρίπτουν το μήνυμα
- Ελέγχουν την διεύθυνση που εκτελεί την συναλλαγή ότι έχει αρκετά κεφάλαια για να τιμήσει την συναλλαγή. Αν δεν υπάρχουν αρκετά πιστωμένα κεφάλαια στη διεύθυνση, η συναλλαγή ακυρώνεται.

- Τέλος, ενημερώνουν τη βάση δεδομένων, αφαιρώντας τα κεφάλαια από την μια διεύθυνση και τα πιστώνουν στην άλλη.

Μια βασική λεπτομέρεια είναι ότι οι κόμβοι του δικτύου δεν γνωρίζουν τις ταυτότητες της Alice και του Bob, σαν χρήστες αναγνωρίζονται μόνο από τις διευθύνσεις τους. Οι χρήστες του Bitcoin αναγνωρίζονται από το ψευδώνυμο: το Bitcoin παρέχει ψευδωνυμία. Μια άλλη βασική λεπτομέρεια είναι ότι οι διευθύνσεις δεν χορηγούνται από το δίκτυο. Δημιουργούνται μέσα στις συσκευές των χρηστών όταν "τρέξουν" το λογισμικό του Bitcoin που κρυπτογραφεί τα δημόσια και τα ιδιωτικά κλειδιά. Καθώς τα δημόσια και τα ιδιωτικά κλειδιά είναι αλληλένδετα, πρέπει να παραχθούν από κοινού και τοπικά στην συσκευή του χρήστη. Η διαδικασία παραγωγής διεύθυνσης είναι απλή και μπορεί να πραγματοποιηθεί σχεδόν ακαριαία από οποιαδήποτε συσκευή όπως laptop ή Smartphone. Δεν υπάρχει επίσης περιορισμός στον αριθμό των διευθύνσεων που μπορεί να δημιουργήσει ένας χρήστης. Πράγματι, συνιστάται οι χρήστες να παράγουν πολλές διευθύνσεις για να ενισχύσουν την προστασία των δεδομένων τους. Δεν είναι απαραίτητο να έχει κάνει κανείς εγγραφή για να χρησιμοποιήσει το Bitcoin. Στην πραγματικότητα, οι νέοι χρήστες δεν χρειάζεται να ανακοινώσουν τις διευθύνσεις τους στο δίκτυο για να είναι σε θέση να λάβουν κεφάλαια. Ένας χρήστης, ας πούμε ο Bob, μπορεί να δημιουργήσει μια διεύθυνση και να ανακοινώσει αυτή την διεύθυνση στην Alice με άλλα μέσα, όπως e-mail ή με την σύζευξη δύο Smartphones. Η Alice μπορεί να στείλει τώρα κεφάλαια στην διεύθυνση του Bob και το δίκτυο θα δεχτεί την συναλλαγή και ας μην έχει συναντήσει ξανά αυτή την διεύθυνση. Στο κεντρικό σύστημα τα κεφάλαια κατέχονται από έναν κεντρικό φορέα, που κατέχει επίσης τα μέσα για τον έλεγχο αυτών των κεφαλαίων, λέγοντας με την αλλαγή των μητρώων στο καθολικό. Σε αντίθεση, σε ένα μη κεντρικό σύστημα, το απόρρητο κλειδί που δίνει πρόσβαση στα κεφάλαια είναι αποκλειστικά στα χέρια των τελικών χρηστών. Τα Bitcoins δεν κατοικούν στον υπολογιστή του χρήστη. Είναι καταχωρήσεις σε μια κατανεμημένη βάση δεδομένων που ονομάζεται blockchain. Οι συναλλαγές αποτελούνται από μια λίστα συναλλαγών εισροής (TxIn) και μια λίστα συναλλαγών εκροών (TxOut). Κάθε εκροή (TxOut) κατέχει δύο κομμάτια των δεδομένων: ένα ποσό και τη διεύθυνση του δικαιούχου. Η διεύθυνση προέρχεται από το δημόσιο κλειδί. Έτσι, μόνο ο ιδιοκτήτης του ιδιωτικού κλειδιού μπορεί να ξεκλειδώσει τα κεφάλαια που αποθηκεύονται στο TxOut . Για να ξεκλειδωθούν τα κεφάλαια, ο ιδιοκτήτης του ιδιωτικού κλειδιού πρέπει να υπογράψει μια συναλλαγή στέλνοντας τα κεφάλαια σε μια νέα διεύθυνση Bitcoin. Οι συναλλαγές εισροών κρατάνε αναφορά της προηγούμενης συναλλαγής εκροών και μια υπογραφή που αποδεικνύει ότι τα κεφάλαια της προηγούμενης αναφερόμενης συναλλαγής εκροών μπορούν να ξοδευθούν. Αυτή η υπογραφή πρέπει να γίνει με το απόρρητο κλειδί υποστηριζόμενο από το δημόσιο κλειδί της διεύθυνσης του Bitcoin. Εάν η υπογραφή δεν ταιριάζει, η συναλλαγή θεωρείται άκυρη και εγκαταλείπεται από το δίκτυο. Για να είναι έγκυρη η συναλλαγή, πρέπει το άθροισμα του ποσού των εισροών να είναι μεγαλύτερο ή ίσο με το άθροισμα του ποσού των εκροών. Η διαφορά μεταξύ εισροών και εκροών εάν υπάρχει είναι η χρέωση των συναλλαγών. Οι χρεώσεις των συναλλαγών συλλέγονται από τους miners που συμπεριλαμβάνουν την συναλλαγή στο block. Οι εκροές στο blockchain μπορούν να ξοδευθούν μόνο μια φορά και πρέπει να γίνει εξολοκλήρου η καταβολή τους. Εάν το ποσό των εκροών είναι μεγαλύτερο από το ποσό που θα ξοδευτεί, η συναλλαγή δίνει ρέστα. Ο αποστολέας της συναλλαγής μπορεί να συλλέξει τα ρέστα προσθέτοντας μια διεύθυνση μεταβολής σαν επιπρόσθετη εκροή στην συναλλαγή. Το γεγονός ότι η διεύθυνση μεταβολής συνήθως ελέγχεται από τον αποστολέα της συναλλαγής μπορεί ενεργά να χρησιμοποιηθεί από τα δεδομένα του αλγορίθμου του mining που εφαρμόζεται στο blockchain. Η διεύθυνση προέλευσης των κεφαλαίων μπορεί να χρησιμοποιηθεί ως διεύθυνση μεταβολής σε μια συναλλαγή, αλλά συνιστάται να δημιουργηθεί μια ολοκαίνουργια διεύθυνση μεταβολής για κάθε συναλλαγή προκειμένου να αυξηθεί η προστασία δεδομένων.



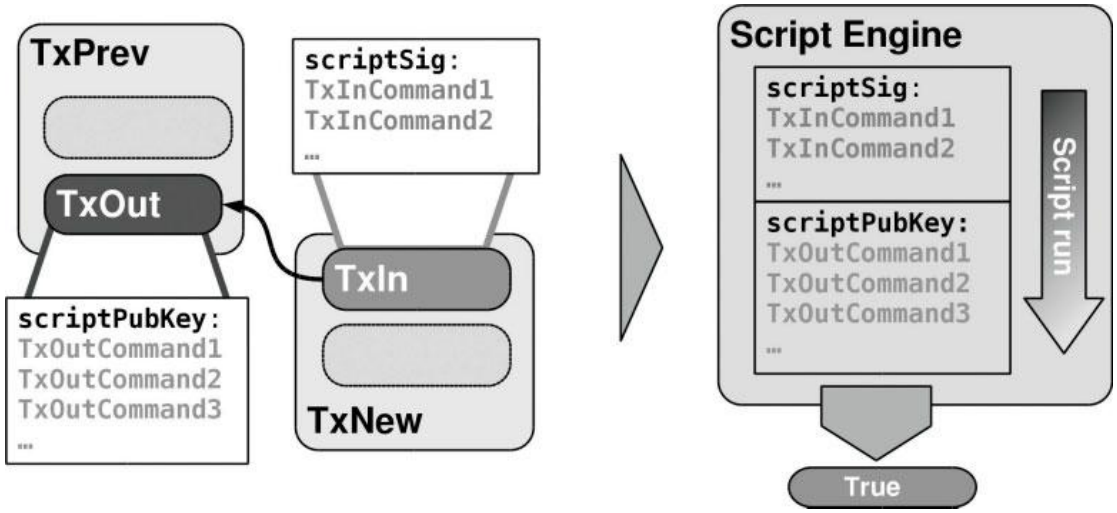
Σχήμα 7. Transactions

Στην εικόνα απεικονίζεται ένα παράδειγμα συναλλαγών (βλέπε σχήμα 7). Σε αυτό το παράδειγμα ο αποστολέας θέλει να στείλει έξι Bitcoins στον παραλήπτη. Όμως ο αποστολέας δεν έχει στην διάθεσή του συναλλαγή εκροών με τον ακριβή αριθμό των έξι Bitcoins. Ελέγχει μόνο δύο συναλλαγές εκροών με πέντε Bitcoins η κάθε μια. Έτσι δημιουργεί μια επιπλέον συναλλαγή που ομαδοποιεί τις δυο προηγούμενες συναλλαγές εκροών και στέλνει στον παραλήπτη έξι Bitcoins. Ο αποστολέας προσθέτει μια συναλλαγή εκροών κάτω από τον έλεγχο του για να παραλάβει τα ρέστα (3 Bitcoins) και αφήνει ένα Bitcoin προμήθεια για τους miners. Πριν στείλει την συναλλαγή στο δίκτυο ο αποστολέας πρέπει να εγγράψει τις δύο συναλλαγές εισροής για να αποδείξει ότι ελέγχει την διεύθυνση που προτείνεται από αυτές. Η συναλλαγή στέλνεται έπειτα στο δίκτυο. Πρώτος κόμβος του δικτύου που παραλαμβάνει την συναλλαγή επικυρώνει ότι είναι έγκυρη η συναλλαγή. Εάν η συναλλαγή είναι σωστή, ο κόμβος το ελευθερώνει στους επόμενους κόμβους του δικτύου. Για να επικυρωθεί η εγκυρότητα της συναλλαγής, ο κόμβος ακολουθεί τα εξής βήματα:

- Ελέγχει ότι η προηγούμενη εκροή που αναφέρεται από την συναλλαγή όντως υπάρχει και ότι δεν έχει ξοδευθεί. Ο κόμβος συνεχίζει τον έλεγχο συμβουλευόμενος τις αξόδευτες συναλλαγές εκροών.
- Ελέγχει επίσης ότι το άθροισμα των τιμών στις εισροές είναι μεγαλύτερο ή ίσο του αθροίσματος των εκροών. Ελέγχει ότι η συναλλαγή δεν ξοδεύει περισσότερα από τις διαθέσιμες εισροές. Η διαφορά του αθροίσματος της τιμής των εκροών και του αθροίσματος της τιμής των εισροών θεωρείται ότι είναι η προμήθεια που αφήνουν στον miner και περιλαμβάνεται στην βάση νομισμάτων της συναλλαγής.
- Και τέλος ελέγχει ότι η υπογραφή για κάθε εισροή είναι έγκυρη, ότι κάθε εισροή είναι εγγεγραμμένη με απόρρητο κλειδί συνοδευόμενο από το δημόσιο κλειδί συνεργαζόμενα με την διεύθυνση που προτείνεται.

Μέχρι αυτό το σημείο οι εκροές συναλλαγής θεωρείται ότι θα πρέπει να αποστέλλονται στην διεύθυνση Bitcoin. Κάθε συναλλαγή εκροών δημιουργεί ένα μαθηματικό puzzle που πρέπει να επιλυθεί προκειμένου να «περάσουν» την έξοδο. Το puzzle για να ξεκλειδώσει τα κεφάλαια και η λύση του puzzle εκπροσωπούνται από δύο σενάρια. Το

σενάριο που δημιουργεί το puzzle ονομάζεται « scriptPubKey» , επειδή είναι το μέρος του σεναρίου που περιέχει το δημόσιο κλειδί . Το puzzle που λύνει το «scriptPubKey», ξεκλειδώνοντας έτσι τα κεφάλαια, ονομάζεται «scriptSig» , επειδή είναι το μέρος του σεναρίου που περιέχει την υπογραφή.



Σχήμα 8. Scripting

Στην εικόνα παρουσιάζεται η διαδικασία όπου ξοδεύεται μια εκροή (βλέπε σχήμα 8). Μια εκροή (TxOut) δημιουργεί ένα «scriptPubKey» που πρέπει να επιλυθεί για να ξοδευθούν τα κεφάλαια που περιέχονται σε αυτή την εκροή. Το πρωτόκολλο ελέγχει ότι το «scriptSig» λύνει το μαθηματικό πρόβλημα που δημιουργήθηκε από το «scriptPubKey». Για να το κάνει αυτό, το πρωτόκολλο δημιουργεί ένα πλήρες σενάριο με συνένωση του «scriptSig» με το «scriptPubKey» και τρέχει ολόκληρο το σενάριο. Αν το τελικό αποτέλεσμα είναι αληθές, τότε η είσοδος θεωρείται έγκυρη. Αν το σενάριο αποτύχει στη μέση ή αν το τελικό αποτέλεσμα δεν αποτιμάται πραγματικά, η είσοδος της συναλλαγής είναι άκυρη και η όλη συναλλαγή καθίσταται άκυρη και εγκαταλείπεται. Κλείνοντας το κεφάλαιο των συναλλαγών οι κύριοι τρόποι συναλλαγών είναι έξι:

- **TX_PUBKEY** ή pay-to-public-key. Το «scriptPubKey» αυτού του είδους της συναλλαγής είναι [OP_PUBKEY OP_CHECKSIG].
- **TX_PUBKEYHASH** ή pay-to-address. Το «scriptPubKey» αυτού του είδους της συναλλαγής είναι [OP_DUP OP_HASH160 OP_PUBKEYHASH OP_EQUALVERIFY OP_CHECKSIG].
- **TX_SCRIPTHASH** ή pay-to-script-hash (P2SH). Το «scriptPubKey» αυτού του είδους της συναλλαγής είναι [OP_HASH160 <20-byte-hash> OP_EQUAL]. Μη-κλασική συναλλαγή αν τοποθετηθεί στο *«scriptSig»* ενός P2SH δεν επιτρέπεται.
- **TX_MULTISIG** ή multi signature transaction. Το «scriptPubKey» αυτού του είδους της συναλλαγής είναι [m sig1 ... sign n OP_CHECKMULTISIG]. Μια τέτοια συναλλαγή θεωρείται κλασική εάν $n \leq 3$ και $m \leq n$.
- **TX_NULL_DATA** γνωστή και ως OP_RETURN transactions. Το <scriptPubKey> αυτού του είδους της συναλλαγής είναι [OP_RETURN <data>].
- **TX_NONSTANDARD** εάν δεν είναι καμία από τις προηγούμενες συναλλαγές.

Οι πέντε πρόωρες συναλλαγές θεωρούνται κλασικές συναλλαγές. Μέχρι τώρα μόνο οι κλασικές συναλλαγές προωθούνται από τους κόμβους στο προτεινόμενο λογισμικό του Bitcoin. Για να συμπεριληφθεί η μη-κλασική συναλλαγή (**non-standard transaction**)

στο blockchain, πρέπει να γίνει συμφωνία με τους miner και συμπεριλαμβάνεται όταν οι miners λύσουν το block.

Κεφάλαιο 4

4.1 Εναλλακτικά νομίσματα

Τα εναλλακτικά κέρματα είναι αυτά τα οποία έχουν αντιγράψει πολλά από τα χαρακτηριστικά του Bitcoin. Τα περισσότερα από τα νομίσματα αυτά βασίζονται στον πηγαίο κώδικα του Bitcoin με κάποιες αλλαγές. Όπως για παράδειγμα ο κωδικός Bitcoin που εκδίδεται υπό μια άδεια ανοιχτού κώδικα, είναι αποδεκτό να λαμβάνει ένα αντίγραφο του κώδικα, να τροποποιηθεί και να απελευθερώσει ένα νέο cryptocurrency. Πολλοί προγραμματιστές έχουν κάνει ακριβώς αυτό που προαναφέρθηκε, δημιουργώντας πολλά εναλλακτικά νομίσματα. Η ανάπτυξη του Bitcoin ήταν συντηρητική και διατηρεί την αξία, με έμφαση την αποφυγή των ενδεχόμενων σφαλμάτων. Σε αντίθεση με το Bitcoin, τα εναλλακτικά κέρματα συχνά δεν έχουν περιορισμούς του συστήματος παραγωγής, όπως για παράδειγμα απαίτηση ως προς τα την συμβατότητα που τους επιτρέπει να δοκιμάσουν νέες «μικρορυθμίσεις» και χαρακτηριστικά. Θα αναφερθούν και αναλυθούν παρακάτω τα εξής νομίσματα:

Litecoin (LTC): Είναι αναμφισβήτητα το πιο επιτυχημένο εναλλακτικό νόμισμα το οποίο εκδόθηκε το 2011 και την στιγμή που γράφτηκε αυτό το κείμενο είχε κεφαλαιοποίηση της τάξης του 5%. Μερικές φορές αναφέρεται ως “silver to Bitcoin’s gold”. (Pedro Franco,2013)

Peercoin (PPC):Το νόμισμα αυτό εισήχθη το 2012. Η βασική καινοτομία του είναι ότι χρησιμοποιεί μια υβριδική απόδειξη της συμμετοχής της λειτουργίας του συστήματος. Σε ένα σύστημα που αποδεικνύει την συμμετοχή των νέων αρχείων είναι ανάλογο με την εξόρυξη από τους κατόχους των νομισμάτων κατ 'αναλογία προς τον αριθμό των κερμάτων που ελέγχονται. Απόδειξη της συμμετοχής δεν συνεπάγεται με την επίλυση ενός προβλήματος κατακερματισμού με μερική αναστροφή και έτσι απαιτεί ελάχιστη κατανάλωση ηλεκτρικής ενέργειας. Για το λόγο αυτό υποστήριξε ότι Peercoin είναι μια πράσινη εναλλακτική λύση του Bitcoin. (Pedro Franco,2013)

Freicoin (FRC) εκδόθηκε το 2012. Πρόκειται για ένα εναλλακτικό νόμισμα το οποίο βασίζεται στο Bitcoin με την κύρια διαφοροποίηση ότι έχει τόκο υπερημερίας. Η επισταλία εφαρμόζεται σαν φόρος επί των συναλλαγών που παρακρατάει ένα συγκεκριμένο κλάσμα από τα freicoins. Αυτό το κλάσμα αυξάνει σύμφωνα με τον χρόνο που μεσολάβησε από την τελευταία συναλλαγή που πραγματοποιήθηκε με

freicoin. Έτσι, η επισταλία δρα σαν αρνητικό επιτόκιο στους κατόχους νομισμάτων. Το freicoin εφαρμόζει ένα ετήσιο τόκο υπερημερίας της τάξης του 5% που εξαρτάται από συγκεκριμένες κινήσεις στο διαδίκτυο (Freicoin, 2014). Το ονομα Freicoin αποτελεί φόρο τιμής στο νομισματικό σύστημα Freigeld που είχε προτείνει ο Silvio Gesell.[16] (Pedro Franco,2013)

Namecoin (NMC): Είναι τόσο κρυπτονόμισμα όσο και αποκεντρωμένο κατάστημα κλειδιού / τιμής το οποίο χρησιμοποιείται για να εφαρμοστεί μια εναλλακτική Domain Name System[17] διευθύνσεις που πρέπει να επιλυθούν με το IP addresses. (Pedro Franco,2013)

Primecoin (XMP): εκδόθηκε το 2013. Η κύρια καινοτομία του εναλλακτικού νομίσματος αυτού είναι η απόδειξη της λειτουργία του, η οποία παράγει επιστημονικά αποτελέσματα. Αυτό έρχεται σε αντίθεση με τα περισσότερα εναλλακτικά νομίσματα όσον αφορά τα “proof of work” όπως για παράδειγμα το SHA256, τα αποτελέσματα των οποίων δεν έχουν καμία αξία εκτός από την εξασφάλιση του blockchain.(Pedro Franco, 2013)

Auroracoin (AUR): εκδόθηκε το Φεβρουάριο του 2014. Πρόκειται ξεκάθαρα για μία διακλάδωση, δηλαδή βασίζεται ουσιαστικά στα χαρακτηριστικά του Litecoin. Η βασική καινοτομία του δεν βρίσκεται στο τεχνικό κομμάτι αλλά στην κατανομή του νομίσματος. Το Auroracoin προεξορύσσεται στο 50%, δηλαδή το 50% του συνόλου της προσφοράς χρήματος το οποίο έχει ήδη δημιουργηθεί κατά την ίδρυσή του. Το υπόλοιπο 50% της νομισματικής προσφοράς θα απονεμηθεί σους miners. Ο σκοπός του 50% του “pro-mine” ήταν να διανείμει στον πληθυσμό της Ισλανδίας, την χρήση του εθνικού συστήματος ταυτοποίησης. (Pedro Franco, 2014)

4.2 Το Bitcoin απέναντι στα άλλα νομίσματα

Τα bitcoins είναι ουσιαστικά ένα εικονικό ηλεκτρονικό νόμισμα. Το δίκτυο του bitcoin μοιάζει με τα γνωστά μας δίκτυα πληρωμής, όπως οι πιστωτικές κάρτες, παρ’ όλα αυτά διαφέρει κατά πολύ. Το δίκτυο αυτό δεν ανήκει σε κανέναν, δεν έχει κερδοσκοπικό χαρακτήρα και επομένως κανείς δεν έχει κέρδος και όφελος από τις συναλλαγές που διεξάγονται μέσα από αυτό. Η δομή που ακολουθεί ονομάζεται peer-to-peer και για την ομαλή λειτουργία της συνεργάζονται εκατοντάδες υπολογιστές. Τα παραπάνω χαρακτηριστικά κάνουν το Bitcoin το πρώτο εντελώς ανοιχτό χρηματοπιστωτικό δίκτυο του κόσμου. Το δίκτυο Bitcoin χρησιμοποιεί το δικό του νόμισμα. Όλα τα υπόλοιπα δίκτυα κάνουν χρήση συμβατικών νομισμάτων. Στο δίκτυο αυτό δεν υπάρχουν ενδιάμεσοι ούτε προμήθειες. Δεν υπάρχουν κανόνες και κριτήρια για να αποκτήσεις Bitcoins.
Είναι λοιπόν τα Bitcoins χρήματα; Η μόνη περίπτωση να γίνει κατανοητό το bitcoin, είναι να διερευνηθούν οι έξι συνιστώσες του χρήματος: βιώσιμη ανάπτυξη, φορητότητα, διαιρετότητα, ομοιογένεια και συμμόρφωση προς το πρότυπο, σπανιότητα (ανάγκη αποθεμάτων) και αποδοχή. Θα πρέπει λοιπόν, να εξεταστεί το πώς αυτές οι πτυχές συσσωρεύονται στο bitcoin. Μόλις δει κανείς το νόμισμα αυτό υπό το πρίσμα αυτών των κατηγοριών, αυτό που προκύπτει είναι ένα πολύ ιδιαίτερο πρότυπο αξίας που

[16] Ο Silvio Gesell γεννήθηκε στις 17 Μαρτίου 1862και πέθανε στις 11 Μαρτίου 1930, ήταν ένας Γερμανός έμπορος, θεωρητικός οικονομολόγος, κοινωνικός ακτιβιστής, αναρχικός και ιδρυτής του Freiwirtschaft (free economy)

[17] Το DNS είναι το κομμάτι της υποδομής του Διαδικτύου που επιτρέπει την ανάγνωση του από τον άνθρωπο

υπερέχει και αποτυγχάνει ταυτόχρονα, όπως άλλωστε και τα χρήματα αλλά με διαφορετικούς τρόπους. Αυτό ακριβώς καθιστά δύσκολο τον ουσιαστικό και ακριβή καθορισμό του Bitcoin. Η βιώσιμη ανάπτυξη είναι ένα χαρακτηριστικό παράδειγμα. Το Bitcoin φαίνεται πως έχει αντέξει στον χρόνο και, ως εκ τούτου, παίρνει τα εύσημα. Δεδομένου ότι τα Bitcoins δημιουργούνται με σήμα δεδομένων, μπορούν να γίνονται άπειρες εμπορικές συναλλαγές χωρίς να καταρρεύσουν. Θα μπορούσε να συναλλαχθεί το ίδιο bitcoin ξανά και ξανά χωρίς ποτέ να χάσει την ακεραιότητά του. Αν για παράδειγμα σταλθούν τα νομίσματα σε λάθος διεύθυνση, ενδέχεται να χαθούν οριστικά. Η αποθήκευση τους εκτός σύνδεσης μπορεί να αποβεί αναξιόπιστη αφού κάποια στιγμή ίσως να «κρασάρει» ο υπολογιστής, κάτι που μπορεί να συμβεί και στα καλύτερα μηχανήματα. Αυτό, όμως, δεν ισχύει με το καθορισμένο συνάλλαγμα. Τα παραδοσιακά χρήματα δεν εξαρτώνται από τα μηχανήματα μα από τους ανθρώπους και είναι πολύ πιο ανθεκτικά. Όσον αφορά την φορητότητα. Έχοντας ως δεδομένο ότι πρόκειται για ψηφιακά νομίσματα, θα ήταν σωστό να ειπωθεί πως το bitcoin είναι το πιο φορητό νόμισμα στην ιστορία. Πιθανότατα, αυτήν την στιγμή θα μπορούσε να χωρέσει ολόκληρο το blockchain του bitcoin σ' έναν μεγάλο σκληρό δίσκο. Βεβαίως, αυτό είναι κάτι που ενδεχομένως να μην ισχύει στο μέλλον. Μέρος του πρωτοκόλλου Bitcoin είναι ότι πρέπει να καταγραφεί κάθε συναλλαγή που γίνεται με το κάθε bitcoin. Όσο περνάει λοιπόν ο καιρός, το blockchain του bitcoin θα καταλαμβάνει όλο και περισσότερο χώρο στους υπολογιστές. Ίσως υπάρχει μια τεχνική λύση στο πρόβλημα αυτό, η οποία θα μπορούσε να εφαρμοστεί στο μέλλον αλλά και πάλι, ο χρόνος θα δείξει. Εκεί, όμως που αποδεικνύεται η ανωτερότητά του Bitcoin είναι αναφορικά με την διαιρετότητα, την ομοιογένεια και την συμμόρφωσή τους προς το πρότυπο. Είναι κάτι που δεν μπορεί κανείς να το αμφισβητήσει. Τα Bitcoins μπορούν να διαιρεθούν μέχρι το εκατομμυριοστό δεκαδικό. Πιθανότατα, δεν έχει υπάρξει νόμισμα πιο διαιρετό. Το ίδιο ισχύει και όσον αφορά την ομοιογένειά του. Δεδομένης της ψηφιακής φύσης του bitcoin, όλες οι μονάδες είναι ακριβώς ίδιες. Αν το bitcoin ήταν υλικό στοιχείο, κάθε μονάδα θα ήταν κλώνος του ατόμου. Όσον αφορά τώρα την άλλη συνιστώσα του χρήματος, την σπανιότητα και πάλι κάνει αίσθηση η διπλή φύση του Bitcoin. Συγκριτικά με οποιοδήποτε άλλο νόμισμα, το bitcoin έχει την πιο μετρίσιμη προμήθεια. Ο αριθμός των bitcoins ποτέ δεν θα αυξήσει πέρα από ένα ορισμένο σημείο. Το γεγονός ότι τα bitcoins μπορεί να χαθούν εξαιτίας κάποιου υπολογιστή που κράσαρε ή εξαιτίας της απώλειας κάποιων κωδικών πρόσβασης, σημαίνει ότι θα καταστούν δυσεύρετα με την πάροδο του χρόνου. Βεβαίως, αυτό δεν θα εμποδίσει κάποιους να ξεκινήσουν το δικό τους ψηφιακό νόμισμα, κάτι σαν το Litecoin ή το Peercoin. Ο καθένας μπορεί να δημιουργήσει το δικό του ψηφιακό νόμισμα με ό,τι όρια αποφασίσει αυτός. Φυσικά, όλα τα υπόλοιπα κρυπτονομίσματα «τρέχουν» χάριν στην αποδοχή του bitcoin που κυριάρχησε στην αγορά. Μέρα με τη μέρα όλο και περισσότερες επιχειρήσεις αποδέχονται το bitcoin και υπάρχει ήδη ένας μακρύς κατάλογος καθημερινών προϊόντων και υπηρεσιών που μπορούν να αγοραστούν με τα bitcoins. Είναι προφανές πλέον πως τα bitcoins είναι πολύτιμα, ίσως περισσότερο και από το παραδοσιακό νόμισμα. Είναι σημαντικό να τονιστεί, ότι είναι πολύτιμα χωρίς να υποστηρίζονται από τίποτα. Ενώ η αξία τους φαίνεται κάπως ομοιόμορφη στις διάφορες ιστοσελίδες που έχουν να κάνουν με το bitcoin, αν ποτέ γίνει προσπάθεια να αγοραστούν bitcoin από κάποιον, θα διαπιστωθεί πως η τιμή του μπορεί να είναι υποκειμενική. Αυτό, καθιστά κάτι σαν υλικό ανταλλαγής, μα δεν είναι ακριβώς έτσι λόγω των καταπληκτικών του ιδιοτήτων, της διαιρετότητας και της ομοιομορφίας του. Δεν υποστηρίζεται από τίποτα, εν' αντιθέσει με τον χρυσό. Αλλά ούτε μπορεί να πληγεί από τον πληθωρισμό, όπως το χαρτονόμισμα. Το bitcoin δεν είναι νόμισμα, αλλά σίγουρα δίνει αξία στα χρήματά μας. Όταν αγοραστούν bitcoins, δεν πραγματοποιείται ανταλλαγή ενός νομίσματος έναντι κάποιου άλλου. Αυτό που στην πραγματικότητα συμβαίνει είναι η πραγματοποίηση μιας αγοράς. Ένα προϊόν που παρέχει μια σωσίβια λέμβο από το μονοπώλιο της κυβέρνησης στα χρήματα.

Κεφάλαιο 5

5.1 Τα μειονέκτημα του Bitcoin

5.1.1 Κερδοσκοπία

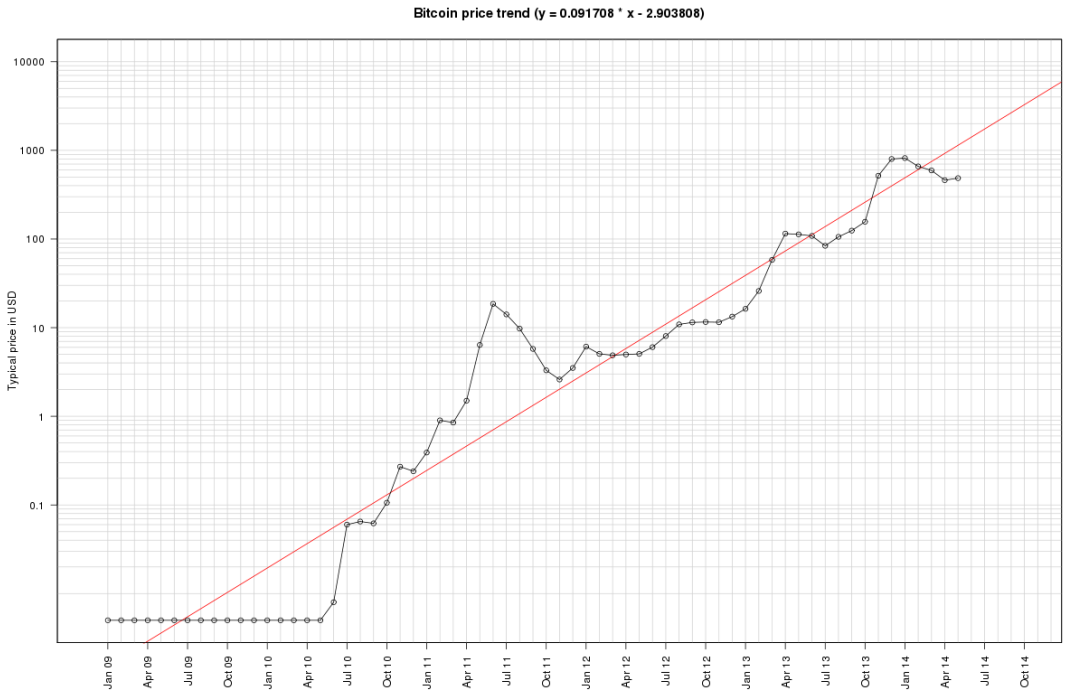
Οι κερδοσκόποι αναμένουν να διευρυνθεί η δημοτικότητα του bitcoin μέσω της αύξησης της αξίας του ώστε να αποτελέσει αντικείμενο διαπραγμάτευσης ως επένδυση. Ωστόσο, το γεγονός ότι η αξία του νομίσματος αυτού εξαρτάται από το κατά πόσο είναι πρόθυμοι οι χρήστες να το αποδεχθούν και ότι μπορεί εύκολα ένας hacker να έχει πρόσβαση στα δεδομένα των χρηστών, δημιουργεί μία αμφιβολία όσον αφορά την αξία του. Αξίζει να αναφερθεί ότι υπάρχουν ελάχιστα διαθέσιμα των παράγωγων των bitcoins και προσφέρονται επιπλέον συμβόλαια μελλοντικής εκπλήρωσης έναντι πολλαπλών νομισμάτων. Επίσης, έχουν δείξει ενδιαφέρον για το bitcoin, ορισμένα επενδυτικά κεφάλαια, για παράδειγμα το Winklevoss έχει κάνει μία προσωπική επένδυση του 1,5 εκατομμυρίου δολαρίων και το Peter Thiel's Founders Fund 3 εκατομμύρια δολάρια.

5.1.2 Bubbles ή «φούσκες»

Μερικοί έχουν προτείνει ότι το bitcoin κερδίζει σε δημοτικότητα στις χώρες με προβλήματα που μαστίζουν τα εθνικά τους νομίσματα, καθώς μπορεί να χρησιμοποιηθεί για την παράκαμψη του πληθωρισμού, των κεφαλαιακών ελέγχων και των διεθνών κυρώσεων. Τα bitcoins χρησιμοποιούνται από μερικούς Αργεντινούς ως εναλλακτική λύση στο επίσημο πληθωρισμένο εθνικό νόμισμα, εμποδίζοντας έτσι τον πληθωρισμό και τους αυστηρούς ελέγχους κεφαλαίου. Επιπλέον, ορισμένοι Ιρανοί χρησιμοποιούν τα bitcoins για να αποφύγουν τις κυρώσεις στο νόμισμά τους. Μάλιστα πολλοί έχουν αναφερθεί στις κερδοσκοπικές φούσκες σε σχέση με το bitcoin. Ο καθηγητής John Quiggin του Πανεπιστημίου του Queensland έχει σημειώσει ότι το bitcoin από τον σχεδιασμό του, δεν έχει καμία εγγενή αξία και συνεπώς είναι "ίσως το καλύτερο παράδειγμα μια καθαρής φούσκας" που είναι σήμερα γνωστή και

προειδοποιεί ότι δεν έχουμε κανένα τρόπο να προβλέψουμε το πότε η αξία των bitcoins θα επιστρέψει στο μηδέν. Επίσης, δημοσιογράφοι και οικονομικοί αναλυτές ανέφεραν ότι υπήρχε πιθανή σχέση μεταξύ της υψηλότερης χρήσης του bitcoin στην Ισπανία στην Κύπρο κατά την οικονομική κρίση το 2012-2013. Κάποιοι το έχουν κάνει «επάγγελμα» και μάλιστα φαίνεται να τα χρησιμοποιούσαν ως νόμισμα για να εξασφαλίσουν παράνομα αγαθά και υπηρεσίες. Τα πρώτα ATM που τα ανταλλάζουν με πραγματικά χρήματα έκαναν ήδη την εμφάνισή τους. Επίσης, ένας Καναδός πουλά το σπίτι του για αυτά και ένας Νορβηγός αγόρασε 5000 bitcoin για 20 ευρώ, το 2009 ανακάλυψε ότι η αξία τους εκτοξεύθηκε στις 650 χιλιάδες, ποσό ικανό να του εξασφαλίσει νέο σπίτι. Ο διαχειριστής χαρτοφυλακίου της επενδυτικής εταιρίας Glendevon King Asset Management με έδρα το Λονδίνο, είπες πως θεωρεί αδύνατο να δοθεί μια ορθολογιστική αξία στο κρυπτονόμισμα αυτό, από τον οποίο ολοένα και περισσότεροι πελάτες ζητούν πληροφορίες. Ακόμα, μιλάει για μια την σύγχρονη εκδοχή της «φούσκας της τουλίπας[18]» του 17ου αιώνα, ο χρηματιστής της UBS. Πρόκειται για ένα ιδιαίτερα ευμετάβλητο εικονικό νόμισμα, το οποίο εμφανίζει πολλά από τα χαρακτηριστικά μιας φούσκας. Το 2011, το κρυπτονόμισμα έκανε έναν τρομερό κύκλο όπου τα 2 δολάρια έγιναν 30 δολάρια και το αντίστροφο. Πολλοί αναλυτές υποστηρίζουν ότι η εκτίναξή του μπορεί να προκλήθηκε από Ρώσους και Κυπρίους επενδυτές που αγοράζουν bitcoins, με φόντο την κρίση της Κύπρου. Με το κούρεμα των καταθέσεων της Κύπρου, πολλοί είδαν το Bitcoin ως μια καλή εναλλακτική του ευρώ.

Γράφημα 5.1: Monthly average USD/bitcoin price & trend



[18] Όταν αναφέρεται κάποιος στην κρίση της τουλίπας, εννοεί την κατάρρευση της τιμής της τουλίπας που έλαβε χώρα στην Ολλανδία το Φεβρουάριο του 1637. Της κρίσης προηγήθηκε η ξέφρενη αύξηση των τιμών της τουλίπας κατά τα προηγούμενα έτη, μια περίοδος που ονομάζεται σήμερα ως τουλιπονανία και αποτελεί την πρώτη ευρέως καταγεγραμμένη «φούσκα» στη σύγχρονη ιστορία. Η τουλίπα εισήχθη στην Ολλανδία από την Οθωμανική αυτοκρατορία τον 16ο αιώνα και άρχισε να καλλιεργείται συστηματικά γύρω στο 1593. Σιγά σιγά εξελίχθηκε σε είδος πολυτελείας και η τιμή του ανέβηκε.

Το Bitcoin δημιουργήθηκε 5 χρόνια πριν περίπου και αναπτύχθηκε με σκοπό τη διευκόλυνση στις online συναλλαγές παγκοσμίως μεταξύ των χρηστών του internet. Η άνοδος της αξίας του τον τελευταίο καιρό οφείλεται στην κατάρρευση της εμπιστοσύνης προς το διεθνές τραπεζικό σύστημα, λόγω των εξελίξεων στο θέμα της Κύπρου, τη στιγμή που το Bitcoin παρουσιάζεται «ασφαλές», καθώς δεν εξαρτάται από τραπεζικά ιδρύματα και κρατικούς φορείς, ενώ εγγυάται ανωνυμία για όσους την επιθυμούν. Γι' αυτό το λόγο άλλωστε είναι διαδεδομένη η χρήση Bitcoins για παράνομη δραστηριότητα. Αξίζει να σημειωθεί ότι τον Οκτώβριο του 2012, η Ευρωπαϊκή Κεντρική Τράπεζα είχε εκφράσει την ανησυχία της για την ανάπτυξη των εικονικών νομισμάτων, όπως το Bitcoin και το Linden Dollar του διαδικτυακού παιχνιδιού Second Life. Όπως τόνιζε τότε η κεντρική τράπεζα, θα μπορούσε να έχει αρνητικό αντίκτυπο στην καλή φήμη των κεντρικών τραπεζών λόγω της εγγενούς αστάθειας τους. Οι Κεντρικές Τράπεζες ανά τον κόσμο παρακολουθούν με μεγάλη προσοχή τη δημοτικότητα του μεγαλύτερου εικονικού νομίσματος και την ισοτιμία του να μεγαλώνει.

5.1.3 Εγκληματικές δραστηριότητες

Η σύνδεση του bitcoin με εγκληματικές δραστηριότητες έχει ως αποτέλεσμα να εμποδίσει την επίτευξη του ως μιας διαδεδομένης, κύριας χρήσης και, αντιθέτως, έχει προσελκύσει την προσοχή των οικονομικών ρυθμιστικών αρχών, των νομοθετικών σωμάτων, και των αρχών επιβολής του νόμου. Η Washington Post αναφέρει χαρακτηριστικά σε δημοσίευμα της "το νόμισμα επιλογής για τις άθλιες online δραστηριότητες" και το CNN ανέφερε ότι το bitcoin είναι "το σκιώδες online νόμισμα". Έχει ζητηθεί από την Γερουσία των Η.Π.Α, την Πολιτεία της Νέας Υόρκης και το FBI να γίνει έλεγχος για την ενδεχόμενη εμπλοκή του κρυπτονομίσματος σε εγκληματικές δραστηριότητες. Ωστόσο, το FBI δήλωσε το 2012 ότι «τα bitcoins θα συνεχίσουν ενδεχομένως να προσελκύουν εγκληματίες του κυβρνοχώρου που το βλέπουν ως το μέσο για να μετακινήσουν ή να κρύψουν τα κεφάλαια τους». Κάποια μάλιστα θεωρούν πως οι κυβερνήσεις θα «έπρεπε» να θέσουν εκτός νόμου το νόμισμα ακριβώς για τους λόγους που προαναφέρθηκαν. Συγκεκριμένα, ο ισχυρισμός αυτός προέρχεται από τον καθηγητή δημόσιας πολιτικής στο πανεπιστήμιο Χαρβαρντ, εν ονόματι Steven Strauss. Και τέλος, ο ειδικός πράκτορας του FBI, Christopher Tarbell είπε πως τα αυτά τα νομίσματα δεν είναι παράνομα από την φύσης του και ότι έχουν γίνει γνωστές νόμιμες χρήσεις τους αντίστοιχα. Σε διάφορες δημοσιεύσεις, βλέπει κανείς ένα από τα πιο γνωστά περιστατικά που έφερε στο στόχαστρο το Bitcoin, το οποίο έγινε τον Ιανουάριο του 2011 περίπου μέχρι και τον Σεπτέμβριο του 2013, όπου η κρυφή ιστοσελίδα με το όνομα silk road λειτούργησε ως μία online αγορά, όπου παράνομα ναρκωτικά και άλλα παρόμοια προϊόντα και υπηρεσίες τακτικά αγοράζονταν και πωλούνται από τους χρήστες της ιστοσελίδας. Η κρυφή ιστοσελίδα silk road είχε σχεδιαστεί για να διευκολύνει το παράνομο εμπόριο που φιλοξενείται στην ιστοσελίδα, παρέχοντας πλήρη ανωνυμία στους χρήστες της, απαιτώντας όλες οι συναλλαγές τους να καταβάλλονται σε Bitcoins.

5.1.4 Η ασφάλεια του δικτύου

Έως τώρα, πολλά από τα προβλήματα που έχουν προκύψει σχετικά με την ασφάλεια του δικτύου, έχουν διορθωθεί εντός λίγων ωρών από την εμφάνιση τους, χωρίς ουσιαστικές επιπτώσεις στην λειτουργία του. Τα τελευταία 4 χρόνια όμως που είναι σε λειτουργία το δίκτυο, έχουν διασαφηνιστεί ακόμα περισσότερο οι πιθανές επιθέσεις που μπορεί να δεχτεί το δίκτυο. Το νεαρό της ηλικίας του δικτύου όμως και η κλιμάκωση του σε περισσότερους χρήστες, όπως και οι εξελίξεις του λογισμικού, ενδεχομένως να επιφέρουν νέα προβλήματα που δεν έχουν προβλεφθεί έως τώρα. Κάθε χρήστης μπορεί βέβαια να προτείνει λύσεις σε αυτά και όποιες εύλογες ανησυχίες εμφανίζονται, εξετάζονται με σοβαρότητα και εις βάθος, ώστε να κριθούν ενδεχόμενες διορθωτικές ενέργειες. Μια περίπτωση που θα μπορούσε να πλήξει τραγικά την ασφάλεια του δικτύου από ένα μόνο άτομο. Αυτό θα έχει ως συνέπεια την αυξημένη πιθανότητα για διπλές συναλλαγές (double spending). Σε κάθε περίπτωση δεν θα επηρεάζονταν οι συναλλαγές που έχουν εκτελεστεί πριν από την επίθεση, θα θιγόταν όμως σημαντικά η συνοχή του δικτύου όπως και η εμπιστοσύνη των χρηστών στην στιβαρότητά του. Ένα ακόμα σοβαρό πρόβλημα, το οποίο έχει απασχολήσει ιδιαίτερα τα forums και τα μέσα είναι η παραβίαση των αλγόριθμων κρυπτογράφησης του δικτύου. Αυτό όπως και άλλα πρότυπα που χρησιμοποιούνται στην προστασία και στην λειτουργία του δικτύου, αποτελούν διεθνώς τυποποιημένα και ευρέως χρησιμοποιούμενα πρωτόκολλα. Στο παρελθόν, οι αδυναμίες τους έχουν προκύψει σταδιακά με αρκετό χρόνο πρόνοιας ώστε τα ευαίσθητα συστήματα χωρών, τραπεζών και άλλων οργανισμών να μην προσβληθούν. Στην περίπτωση που συμβεί κάτι τέτοιο, πιθανότατα το δίκτυο του Bitcoin έχει σημαντικότερα μικρότερο χρόνο αντίδρασης απ' ότι τα περισσότερα άλλα σημεία που χρησιμοποιείται. Τέλος, αν και η αντικατάσταση του bitcoin από κάποιο λογισμικό ανώτερης σχεδίασης και μεγαλύτερου δικτύου, χωρίς αλληλουχία με την παρούσα αλυσίδα συναλλαγών έχει αποφευχθεί προς το παρόν ο κίνδυνος συνεχίζει να υπάρχει.

5.1.5 Ασαφές νομικό πλαίσιο

Παρόλο που η ευρωπαϊκή νομοθεσία έχει λάβει μέτρα για την θέσπιση όρων σε ότι αφορά κεντρικά ελεγχόμενα ή εκδιδόμενα ψηφιακά νομίσματα, η φύση των bitcoin, όπως και άλλα από τα χαρακτηριστικά τους, εισάγουν νέες παραμέτρους που δεν έχουν εξεταστεί σε όλο τους το εύρος ακόμα, σε καμία χώρα. Εντός της Ευρώπης , η Γερμανία τα έχει καθορίσει ως «ιδιωτικά χρήματα» (Private money) και η Ολλανδία ως κάτι στο οποίο δεν χρειάζεται η παρέμβαση ή ο έλεγχος της κεντρικής τράπεζας της χώρας. Στις Η.Π.Α, η κύρια επίσημη οδηγία έως τώρα έγκειται στην προσπάθεια αποφυγής εγκληματικών οικονομικών δραστηριοτήτων, με αμφισβητούμενη ως τώρα επιτυχία, πέρα από την επιβράδυνση των επιχειρηματικών δραστηριοτήτων που σχετίζονται με το bitcoin και αφορούν πελάτες από τις Η.Π.Α. Θεωρείται απίθανο κάποια χώρα να απαγορεύσει ολοκληρωτικά τις συναλλαγές με bitcoin και κάτι τέτοιο είναι εξαιρετικά δύσκολο να εφαρμοστεί πρακτικά. Δεν αποκλείεται στην προσπάθεια διερεύνησης του περιβάλλοντος όμως, να ισχύσουν οδηγίες με αναδρομική ισχύ (όπως στην περίπτωση των Η.Π.Α) που να αλλάζουν το τοπίο, κυρίως επηρεάζοντας τις απαιτήσεις από τις επιχειρήσεις αλλά όχι τόσο από τους χρήστες και την ιδιοκτησία τους. Το κύριο σημείο στο οποίο προβλέπεται ότι θα ασκηθεί κρατική επίβλεψη είναι το σημείο ανταλλαγής με τα κρατικά νομίσματα και ειδικότερα ό, τι έχει σχέση με τα νομικά πλαίσια τοπικά και διεθνώς.

5.1.6 Διακύμανση ισοτιμίας

Καθώς τα bitcoin δεν έχουν κάποια κεντρική αρχή να παρεμβαίνει στις διακυμάνσεις, στην προσφορά και την ζήτηση όπως συμβαίνει με τα κρατικά νομίσματα για παράδειγμα, είναι επιρρεπές σε μεγαλύτερες διακυμάνσεις της ισοτιμίας όπως συμβαίνει με τα περισσότερα νομίσματα. Ένας παράγοντας που επηρεάζει το παραπάνω φαινόμενο είναι το σχετικά μικρό βάθος της αγοράς, πράγμα που σημαίνει ότι όταν συναλλάσσονται μεγάλοι όγκοι bitcoin, επηρεάζουν δυσανάλογα τις ισοτιμίες στα ανταλλακτήρια. Αυτό προβλέπεται ότι θα ελαττωθεί με την πάροδο του χρόνου, εφόσον η οικονομία αναπτυχθεί αρκετά ώστε να μπορούν να εμπλακούν και να αναπτυχθούν κατάλληλες υποδομές που ήδη υφίστανται στις κλασικές κεφαλαιαγορές. Ένας επιπλέον παράγοντας που επηρεάζει τη διακύμανση των ισοτιμιών είναι η φύση των νομισμάτων και ειδικότερα το γεγονός ότι μπορούν να μεταφερθούν ταχύτατα οπουδήποτε στον κόσμο. Αυτό προκαλεί πολύ μεγαλύτερη αμεσότητα στις δράσεις και αντιδράσεις μεταξύ προσφοράς και ζήτησης απ' ότι με τις συμβατικές αξίες. Ένας τελευταίος παράγοντας είναι οι κερδοσκοπικές πιέσεις που ασκούνται στα ανταλλακτήρια, καθώς έχουν ακόμα σχετικά μικρή ρευστότητα και όγκο συναλλαγών, όπως συμβαίνει αντίστοιχα και στα μικρά ψηφιακά ανταλλακτήρια συναλλάγματος.

5.1.7 Υψηλή κατανάλωση ενέργειας

Για να πραγματοποιήσει κάποιος εξόρυξη των κρυπτονομισμάτων bitcoin χρειάζεται επεξεργαστική ισχύ όπως έχει προαναφερθεί στο κεφάλαιο "mining". Αρχικά η εξόρυξη γινόταν κάνοντας χρήση του κεντρικού επεξεργαστή ενός ηλεκτρονικού υπολογιστή. Σύντομα όμως παρατηρήθηκε ότι ο κεντρικός επεξεργαστής είναι πολύ πιο αργός σε σχέση με έναν επεξεργαστή γραφικών. Έτσι τα προγράμματα επεκτάθηκαν και τροποποιήθηκαν ώστε να χρησιμοποιούνται επεξεργαστές γραφικών για τους σύνθετους υπολογισμούς του Bitcoin Mining. Παρά το γεγονός ότι οι σημερινές κάρτες γραφικών μπορούν να παράγουν μεγαλύτερα κομμάτια κώδικα κάθε δευτερόλεπτο, έχουν υψηλή κατανάλωση ενέργειας και αντίστοιχα μεγάλη απαγωγή θερμότητας, δημιουργώντας έτσι σοβαρά προβλήματα για την τροφοδότηση τους αλλά και για την ψύξη τους.

5.1.8 Απαγόρευση της χρήσης του

Η φήμη του Bitcoin έχει πληγεί από πολλά γεγονότα και πλέον οι τράπεζες και οι κυβερνήσεις είναι διστακτικές με την χρήση του. Αν και η αποδοχή του νομίσματος έχει αρχίσει με μικρά βήματα στην Κίνα και στις Η.Π.Α, δεν συμβαίνει το ίδιο και στην Ευρώπη. Πιο συγκεκριμένα, η Ευρωπαϊκή Τραπεζική Αρχή (ΕΒΑ), έχει ήδη εκδώσει ανακοίνωση στην οποία αναλύει τους κινδύνους που προκύπτουν σε σχέση με το Bitcoin. Επιπλέον, έχει καταστήσει σαφές ότι ήδη επεξεργάζεται κανόνες ρύθμισης της κυκλοφορίας ψηφιακών νομισμάτων σε παγκόσμιο επίπεδο, Στην ίδια ανακοίνωση ενημερώνει τους Ευρωπαίους καταναλωτές ότι οποιαδήποτε επένδυση τους στο ψηφιακό νόμισμα μπορεί σύντομα να τους οδηγήσει στην απώλεια του συνόλου της επένδυσης τους . Οι φήμες για την διακοπή χρήσης του bitcoin αποδείχτηκαν αβάσιμες όταν έγινε για αυτές ο λόγος σε άλλες χώρες.

5.2 Τα πλεονεκτήματα του Bitcoin

5.2.1 Διαφάνεια συναλλαγών και κανόνων

Όλες οι συναλλαγές που έχουν εκτελεστεί ποτέ στο δίκτυο είναι δημόσια διαθέσιμες και διαφανείς. Έτσι, οποιοσδήποτε μπορεί να εξετάσει οποιαδήποτε διεύθυνση και να δει τις προηγούμενες συναλλαγές που έχουν εκτελεστεί με αυτήν, το πλήθος των bitcoin που έχουν μετακινηθεί, όπως και το που έχουν σταλεί. Αυτό ισχύει για όλες τις συναλλαγές που έχουν εκτελεστεί ποτέ στο δίκτυο έως την πρώτη. Το ίδιο ακριβώς ισχύει για όλους τους κανόνες σύμφωνα με τους οποίους δουλεύει το λογισμικό και στο οποίο συναινούν οι χρήστες. Δεν υπάρχει κανένας κρυφός κανόνας μέσα στο λογισμικό και δεν είναι δυνατόν να υπάρξει, καθώς οι χρήστες δε θα το αποδέχονταν.

5.2.2 Ιδιωτικότητα συναλλαγών

Κάθε χρήστης μπορεί να δημιουργήσει, μέσω του λογισμικού, σχεδόν απεριόριστο αριθμό διευθύνσεων μέσω των οποίων να εκτελέσει τις συναλλαγές του. Αυτές οι διευθύνσεις είναι ψευδώνυμες, δεν έχουν δηλαδή κάποια άμεση σχέση με τα πραγματικά στοιχεία ή την τοποθεσία του χρήστη, παρόλο που έχουν αναγνωρίσιμα χαρακτηριστικά ώστε να εντοπίζονται από το δίκτυο. Με αυτό τον τρόπο μπορεί να ο χρήστης να διατηρήσει την ιδιωτικότητά του απεμπλέκοντας τις συναλλαγές του από τα προσωπικά του στοιχεία. Αυτό δεν συνεπάγεται εξ' ορισμού ανωνυμία συναλλαγών καθώς όλες οι συναλλαγές δημοσιεύονται και έστω και μία συναλλαγή να έχει γνωστό (δημόσιο) αποδέκτη, ίσως μπορεί να εξαχθεί από συμπληρωματικά στοιχεία η ταυτότητα του χρήστη. Αυτός είναι και ο κύριος λόγος για τον οποίο η χρήση bitcoins δεν ενδείκνυται για συναλλαγές παράνομων δραστηριοτήτων, ιδιαίτερα μεγάλης κλίμακας καθώς το ίχνος των συναλλαγών όχι μόνο δεν διαγράφεται με το πέρασμα του χρόνου αλλά παραμένει διαθέσιμο για εξέταση από όλους και για πάντα.

5.2.3 Έλεγχος από τον χρήστη

Καθώς ο χρήστης είναι ο μόνος που έχει την δυνατότητα να εκτελέσει συναλλαγές και εφόσον δεν έχει παραχωρήσει αυτό το δικαίωμα και έχει προστατεύσει λογικά την πρόσβαση στα bitcoin του, είναι πρακτικά αδύνατο να κλαπούν από τρίτους (εφόσον η κρυπτογράφηση δεν παραβιαστεί). Περαιτέρω προβλέψεις επιτρέπουν την δυνατότητα μεταφοράς τους μόνο υπό ορισμένες συνθήκες, όπως μόνο από ορισμένα προσυμφωνημένα μέρη, κάτι που επιτρέπει την αποφυγή μονομερών εκθέσεων ή μόνο μετά από συγκεκριμένο χρόνο.

5.2.4 Εξαιρετικά χαμηλό κόστος συναλλαγών

Το κόστος για κάθε συναλλαγή με bitcoins, ανεξαρτήτως μεγέθους, είναι εξαιρετικά χαμηλό και δύναται να προσεγγίσει πολύ χαμηλότερες τιμές σε ακόμα πιο σύνθετα δίκτυα υπό την σκέπη επί μέρους ελεγκτικών δικτύων. Αυτή τη στιγμή το κόστος

συναλλαγής ανάγεται περίπου στα 5 cents και είναι προαιρετικό αν δεν υπάρχει βιασύνη επιβεβαίωσης της συναλλαγής. Το ποσό αυτό αποδίδεται αυτόματα στους χρήστες που εκτελούν τους ελέγχους των συναλλαγών και τν επιβεβαίωση της αντικειμενικότητας του, ως αμοιβή για την επεξεργαστική ισχύ που επενδύουν στην προστασία του δικτύου από επιθέσεις.

5.2.5 Ταχύτητα συναλλαγών και η διεθνής φύση τους

Οι συναλλαγές σε bitcoin συμβαίνουν άμεσα και ανακοινώνονται ταυτόχρονα σε όλο το δίκτυο ανά τον πλανήτη. Αυτό δεν απαιτεί άλλες υποδομές πέρα από κάποια μορφή του δωρεάν λογισμικού σε υπολογιστή και σύνδεση στο διαδίκτυο.

5.2.6 Συναινετική φύση χρήσης του δικτύου

Η αλλαγή οποιουδήποτε χαρακτηριστικού του λογισμικού ή των κανόνων του, έχει ουσιαστικά εφαρμογή μόνο όταν τις δεχτεί η κοινότητα που απαρτίζει το δίκτυο. Με αυτόν τον τρόπο αποφεύγονται κακόβουλες αλλαγές που θα μπορούσαν να αλλάξουν θεμελιωδώς το λογισμικό (καθώς η πλειοψηφία των χρηστών θα τις αναγνωρίσει και δεν θα τις δεχτεί) αλλά και μεγάλη ευελιξία και ταχύτητα αντίδρασης σε περίπτωση εντοπισμού σφαλμάτων ή απρόβλεπτων αστοχιών κατά τη λειτουργία. Η ύπαρξη μιας παγκόσμιας, εξειδικευμένης και δραστήριας κοινότητας, που αντιμετωπίζει με επαγγελματισμό την ποιότητα του λογισμικού ενώ είναι απολύτως ανοιχτή σε σχόλια, εισηγήσεις και κριτική από όλα τα μέρη είναι ανεκτίμητη για την βιωσιμότητα του λογισμικού.

5.2.7 Αποκεντρωμένη φύση του δικτύου

Ένα από τα πιο σημαντικά χαρακτηριστικά του δικτύου, είναι η αποκεντρωμένη φύση του. Δεν απαιτεί καμία κεντρική αρχή ελέγχου ή επιβεβαίωσης. Κάθε κόμβος του δικτύου το ενισχύει περαιτέρω, αλλά αν προσβληθεί με κάποιο τρόπο, η λειτουργία του συνολικού δικτύου δεν επηρεάζεται ανάλογα. Η προσβολή ακόμα και πολύ μεγάλου μέρους των υπολογιστών που απαρτίζουν το δίκτυο δεν θα επηρέαζε σε σημαντικό βαθμό τη λειτουργία του. Ο μόνος τρόπος να σταματήσει να δουλεύει το δίκτυο του bitcoin είναι να αποκοπούν όλοι οι υπολογιστές του δικτύου μεταξύ τους, με δύο λόγια να κοπεί το διαδίκτυο σε όλο τον πλανήτη, κάτι που είναι πέρα από τις δυνάμεις οποιουδήποτε στην παρούσα πραγματικότητα. Ακόμα και τότε, με την επαναλειτουργία του διαδικτύου, το δίκτυο συνεχίζει ακριβώς εκεί που σταμάτησε. Ακόμα και μόνο ένας υπολογιστής να παραμείνει συνδεδεμένος που περιέχει το αρχείο της αλυσίδας των προηγούμενων συναλλαγών το δίκτυο λειτουργεί κανονικά.

5.2.8 Υποδιαιρέσεις

Κάθε bitcoin είναι υποδιαιρέσιμο έως 8 δεκαδικά ψηφία (δηλαδή έως 0,00000001). Αυτό επιτρέπει μικρό-συναλλαγές που δεν είναι δυνατές με άλλα μέσα ή συμβατικά νομίσματα. Η προσθήκη περισσότερων ακόμα δεκαδικών ψηφίων επαφίεται στην συναίνεση του δικτύου αν αυτό χρειαστεί στο μέλλον.

5.2.9 Μην αντιστρέψιμη φύση του δικτύου

Όλες οι συναλλαγές με bitcoin είναι τελικές και μη αντιστρέψιμες. Αυτό έχει το επιπλέον πλεονέκτημα προς όσους διαθέτουν προϊόντα για bitcoin ότι δεν είναι δυνατό να ανακληθούν συναλλαγές όπως είθισται στις απάτες με πιστωτικές κάρτες. Αυτό συνήθως δίνει επιπλέον κίνητρα σε επιχειρήσεις να προσφέρουν τα προϊόντα τους σε χαμηλότερες τιμές, εξαιτίας της άμεσης και αμετάκλητης πληρωμής. Αυτό δε σημαίνει βέβαια πως οι χρήστες που εκτελούν αγορές με bitcoin δεν πρέπει να είναι προσεκτικοί στις επιλογές τους, καθώς ένας πάροχος προϊόντων ή υπηρεσιών που δεν έχει ιστορικό κινήσεων ή έμπιστη παρουσία στην αγορά μπορεί να μην είναι αυτό που δείχνει.

5.2.10 Αλεξίσφαιρο απέναντι στην κρίση

Η κρίση που προκλήθηκε με τα πρόσφατα γεγονότα στην πραγματικότητα όχι μόνο δεν έβλαψε το bitcoin αλλά όπως βλέπουμε, είχε θετική τροπή στην αξία του. Η προσοχή που δείχνουν τα ΜΜΕ, έστω και αρνητική τραβάει όλο και περισσότερη προσοχή στο bitcoin είναι από τα ελάχιστα νομίσματα που αντέχει την πίεση και τα προβλήματα της οικονομίας αυτή τη στιγμή.

Συμπεράσματα

Το bitcoin δεν είναι κάτι καινούριο. Μετράει ήδη έξι χρόνια ζωής περίπου και κερδίζει ολοένα και περισσότερους φανατικούς χρήστες,. Αν και γνωστό από παλιά ως "χρήματα των hackers" ή και ως μέσο ξεπλύματος μαύρου χρήματος, πλέον αποκτά ολοένα και μεγαλύτερη δημοτικότητα, με πολλά καταστήματα, μάλιστα να το αποδέχονται και ως εναλλακτικό μέσω πληρωμής. Πλέον έχει αναγνωριστεί ακόμα σαν «τράπεζα» η οποία μπορεί να λαμβάνει και να αποστέλλει χρήματα από κα προς άλλες τράπεζες, να εκδίδει χρεωστικές κάρτες bitcoins και φυσικά να καθορίζει την ισοτιμία αληθινών χρημάτων ή bitcoins και αντίστροφα. Η δημοτικότητα που λαμβάνει ωστόσο μπορεί να θεωρηθεί και κίνητρο για περισσότερη εμπιστοσύνη σε αυτό το νέο χρηματικό μοντέλο, ειδικά αν αναλογιστεί κανείς πως τα γεγονότα στην Κύπρο αύξησαν την αξία του νομίσματος από 40 έως 72 δολάρια σε μια μόλις εβδομάδα, με τις τράπεζες μάλιστα να υπολειτουργούν. Τα ίδια δημοσιεύματα θέλουν επίσης το νέο νόμισμα να γίνεται ολοένα και πιο δημοφιλές στην Ισπανία μέσω εφαρμογών για συσκευές κινητών όπως bitcoin gold, bitcoin ticker και bitcoin app. Όπως είναι φανερό λοιπόν, το bitcoin έχει ξεκάθαρη προοπτική ανάπτυξης και ήτο δυνατό να γίνει σημαντικός τρόπος πληρωμής μέσω διαδικτύου, συναλλαγών και μεταφορών χρήματος. Δεν υπάρχει αμφιβολία ότι το bitcoin ενέχει κάποιο ρίσκο βέβαια, αλλά πρέπει επίσης να αναγνωριστεί το γεγονός ότι το bitcoin έχει παίξει μεγάλο ρόλο σε χώρες όπου οι πολίτες αντιμετωπίζουν υψηλή φορολογία, ελέγχους στη διακίνηση κεφαλαίων ή ακόμα και ισχυρό κίνδυνο κατάσχεσης. Γι' αυτό αν πάρει κανείς για παράδειγμα την Κίνα και την σχέση της με το bitcoin, για την οποία έχουν δημοσιευτεί πολλά άρθρα, παρατηρείται τεράστια αυξανόμενη ζήτηση για τα bitcoins. Έτσι παρατηρείται ότι η μέχρι σήμερα η αποδοχή του από το ευρύ κοινό αλλά και μεγάλο μέρος της ακαδημαϊκής κοινότητας δείχνει ότι το εγχείρημα μπορεί να είναι βιώσιμο. Θα μπορούσε να φτάσει ίσως μέχρι και την δημιουργία ενός ιδανικού χρηματοπιστωτικού συστήματος χωρίς μεσάζοντες, τραπεζίτες και τοκογλύφους. Αν κάτι τέτοιο πραγματοποιηθεί οι τράπεζες θα περιοριστούν σε βοηθητικό ρόλο (διεθνείς συναλλαγές, συνάλλαγμα, ευνοϊκά δάνεια). Σε αυτό το σημείο θα ήταν σωστό να απαντηθούν κάποια ερωτήματα όπως: τι θα γινόταν αν το χρήμα με το οποίο συναλλάσσεται κάποιος έπαυε να είναι υπό τον έλεγχο κυβερνήσεων και τραπεζών; αν κανένας δεν γνώριζε ποιος πλήρωσε ποιον και κανένας δεν κρατούσε προμήθεια από κάθε τους κίνηση; πως είναι δυνατόν να είναι αξιόπιστη μία τέτοια μορφή χρήματος και το κυριότερο αν είναι νόμιμο και τι αλλαγές θα φέρει στον κόσμο μας αν επικρατήσει; Η εμφάνιση αυτού του εναλλακτικού χρήματος, χωρίς κεντρική εκδότρια αρχή να το ελέγχει και χωρίς μεσάζοντες τραπεζίτες ή τοκογλύφους να κερδοσκοπούν με αυτό, συνδέθηκε με πολλά όνειρα ανθρώπων. Στην αρχή ήταν τα όνειρα όσων ήθελαν να συναλλάσσονται ελεύθερα, χωρίς επόπτες. Έπειτα προστέθηκαν εκείνοι που δεν ήθελαν πια να πληρώνουν τα υψηλά ποσοστά που ζητούσαν οι πιστωτικές κάρτες στις διαδικτυακές τους αγοραπωλησίες. Επίσης, με το γιγάντωμα της παγκόσμιας οικονομικής κρίσης τα τελευταία χρόνια, προστέθηκαν και όσοι δεν ανέχονται τα

χρηματιστηριακά παιχνίδια με τις ισοτιμίες των νομισμάτων ή το τύπωμα του πληθωριστικού χρήματος χωρίς αντίκρισμα στα αποθέματα σε χρυσό. Ακόμη και ως αντίδραση στα λάθη του συστήματος ή και ως μοναδική ελπίδα να γκρεμιστεί, νέοι οπαδοί του bitcoin εντάσσονται καθημερινά στις γραμμές του. Σίγουρα το bitcoin όπως και τόσες άλλες πρωτοπόρες ιδέες μπορεί να χρησιμοποιηθούν με λάθος τρόπους. Όπως αναφέρθηκαν και παραπάνω, υπάρχουν άλλωστε πολλά παραδείγματα που θα έκαναν τον καθένα να είναι εξαιρετικά επιφυλακτικός απέναντί του. Έχει χρησιμοποιηθεί ως μέσο για παράνομες δραστηριότητες, ακόμα και ως τζόγος. Αυτό από μόνο του όμως δεν μπορεί να καταστήσει το bitcoin κακό. Η λανθασμένη χρήση του, αν και επιφέρει δυσφήμιση, δεν μπορεί να καταστρέψει το μέλλον του δικτύου. Τα προβλήματα αυτά, δεν είναι εγγενή στο bitcoin, αλλά στον τρόπο που επιλέγουν οι άνθρωποι να το χρησιμοποιήσουν. Αλλά αν εξεταστούν τα προβλήματα που θα δημιουργηθούν από την λάθος χρήση των πραγμάτων και θεσμών, τότε αυτομάτως θα πρέπει να ανακηρυχθούν όλοι θεσμοί λανθασμένοι και επικίνδυνοι. Μελετήθηκαν όλοι οι κίνδυνοι που συνδέονται με το bitcoin αλλά και τα θετικά του σημεία, τις προοπτικές του δικτύου, καταλήγοντας στο συμπέρασμα πως έχει πολλά να προσφέρει ακόμα. Πρέπει να γίνει σαφές ότι πέρα από τον συγκεκριμένο αλγόριθμο, το bitcoin εισήγαγε ουσιαστικά την πρωτοποριακή ιδέα ότι μπορεί να υπάρξει και άλλος τρόπος συναλλαγών των ανθρώπων, που να μην ελέγχεται και να χειραγωγείται κεντρικά, είτε αυτός ονομάζεται bitcoin είτε κάπως αλλιώς. Τα bitcoins δεν αποτελούν την άμεση μετάφραση ή μετατροπή μιας νομισματικής μονάδας σε μία άλλη. Μπορούν να παραχθούν από τους ίδιους τους χρήστες της ιδέας. Είναι σίγουρα κάτι πολύ περισσότερο από μία μικροσυναλλαγματική διευκόλυνση.

Βιβλιογραφία

Βιβλία

Daniel Forrester, Mark Solomon, "Bitcoin Explained: Today's Complete Guide to Tomorrow's Currency"

Andreas M. Antonopoulos, "Mastering Bitcoin: Unlocking digital crypto-currencies"

Pedro Franco, "Understanding Bitcoin: Cryptography, Engineering and Economics"

Conrad Barski, Chris Wilmer, "Bitcoin for the Befuddled"

Sam Patterson, Bitcoin Beginner A Step By Step Guide To Buying, Selling And Investing In Bitcoins

A.H. Smithers "Everything you need to know about buying, selling and investing in Bitcoin"

Benjamin Guttmann "The Bitcoin Bible Paperback"

Brett Combs "Bitcoin Decoded: Bitcoin Beginner's Guide to Mining and the Strategies to Make Money with Cryptocurrencies"

Marc A. Carignan "The Bitcoin Tutor: Unlocking the Secrets of Bitcoin"

Jose Pagliery "Bitcoin: And the Future of Money"

Paul Vigna "The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order"

Melanie Swan "Blockchain: Blueprint for a New Economy"

Brian Kelly "The Bitcoin Big Bang: How Alternative Currencies Are About to Change the World"

Ιστοσελίδες

http://chimera.labs.oreilly.com/books/1234000001802/index.html

http://el.wikipedia.org/wiki/%CE%A7%CF%81%CE%AE%CE%BC%CE%B1

http://en.wikipedia.org/wiki/Song_dynasty

http://el.wikipedia.org/wiki/%CE%A0%CE%B1%CF%81%CE%B1%CF%83%CF%84%CE%B1%CF%84%CE%B9%CE%BA%CF%8C_%CF%87%CF%81%CE%AE%CE%BC%CE%B1

http://waves.pirateparty.gr/content/bitcoin-%CF%84%CE%BF-%CF%88%CE%B7%CF%86%CE%B9%CE%B1%CE%BA%CF%8C-%CE%BD%CE%BF%CE%BC%CE%B9%CF%83%CE%BC%CE%B1

http://en.wikipedia.org/wiki/Liberty_Reserve

http://en.wikipedia.org/wiki/E-gold

http://en.wikipedia.org/wiki/Secure_Hash_Algorithm

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

http://en.wikipedia.org/wiki/Merkle_tree

http://oikonomica.com/2012/01/14/tulip_mania/

http://www.dealnews.gr/agores/item/69991-Bitcoin-%CE%A6%CE%BF%CF%8D%CF%83%CE%BA%CE%B1-%CE%AE-%CF%87%CF%81%CF%85%CF%83%CE%AC%CF%86%CE%B9#.VNjRIfmsXn8

http://bitcoinx.gr/%CF%84%CE%BF-bitcoin-%CE%B4%CE%B5%CE%BD-%CE%B5%CE%AF%CE%BD%CE%B1%CE%B9-%CF%86%CE%BF%CF%8D%CF%83%CE%BA%CE%B1-%CE%AE-%CF%80%CF%85%CF%81%CE%B1%CE%BC%CE%AF%CE%B4%CE%B1-2/

http://www.pathfinder.gr/stories/3405539/bitcoin-foyska-h-oikonomiko-thayma