ΖΔΡΑΓΚΑ ΚΑΛΛΙΟΠΗ

Α.Μ. :2008157

Περιεχόμενα

Περίληψη

Από τα αρχαία χρόνια μέχρι σήμερα, υπάρχει μια διαρκής αναζήτηση για τον τρόπο, με τον οποίο θα πραγματοποιούνταν οι συναλλαγές. Με την πάροδο των ετών, υιοθετήθηκαν διάφοροι τρόποι συναλλαγών αλλά απερρίφθησαν όλων αδυναμιών. Έτσι, καθιερώθηκε το νόμισμα, το οποίο μετεξελίχθηκε και επικράτησε με την σημερινή του μορφή. Η αλματώδης ανάπτυξη της πληροφορικής και των υπολογιστών συνέβαλε, μεταξύ άλλων, και στην δημιουργία ενός νέου νομίσματος, του ηλεκτρονικού κρυπτονομίσματος. Το δημοφιλέστερο κρυπτονόμισμα είναι το BitCoin, το οποίο αποτελεί πιθανώς τη μεγαλύτερη αλλαγή στο χρηματοοικονομικό σύστημα εδώ και έναν αιώνα.

Το Bitcoin έχει εισβάλει τους τελευταίους μήνες για τα καλά στην παγκόσμια οικονομική πραγματικότητα, ανοίγοντας το παράθυρο σε ένα παντελώς νέο «νομισματικό» σύστημα. Βέβαια, δεν είναι παρά το πιο παλιό και πιο γνωστό από μια πλειάδα αντίστοιχων ψηφιακών νομισματικών μέσων υπό τον όρο κρυπτονομίσματα. Δημιουργήθηκε από κάποιον με το ψευδώνυμο Satoshi Nakamoto το 2009 και ακολούθησαν το Namecoin, Litecoin, Peercoin και τα πιο πρόσφατα Ripple, Dogecoin, Mastercoin και Primecoin, όλα βασισμένα στην ίδια αρχιτεκτονική.

Η αναγνώριση του BitCoin από τα παγκόσμια χρηματοπιστωτικά ιδρύματα και τις εταιρίες – κολοσσούς έφεραν ντόμινο εξελίξεων. Οι συναλλαγές διεξάγονται μεταξύ των διασυνδεδεμένων ηλεκτρονικών υπολογιστών μέσω ενός ειδικού λογισμικού-εξυπηρετητή του Bitcoin client ενώ δεκάδες ανταλλακτήρια δίνουν την δυνατότητα ανταλλαγής των BitCoins με άλλα ισχυρά νομίσματα (Ευρώ, Δολάρια).

Abstract

From ancient times until today, there was a constant search for the way in which the transactions were made. Over the years, adopted different ways of trading, but rejected all weaknesses. Thus, the currency was introduced, which evolved and prevailed in its current form. The rapid development of information technology and computers has contributed, among other things, the creation of a new currency, the e cryptocurrency. The most popular is the cryptocurrency BitCoin, which is probably the biggest change in the financial system nearly a century.

The Bitcoin has invaded in recent months for good in global economic reality, opening the window to a completely new "monetary" system. Of course, there is only the oldest and most famous of a plurality of respective digital monetary instruments provided cryptocurrency. Created by someone under the pseudonym Satoshi Nakamoto in 2009 and followed Namecoin, Litecoin, Peercoin and latest Ripple, Dogecoin, Mastercoin and Primecoin, all based on the same architecture.

The recognition of BitCoin by global financial institutions and companies - giants brought domino developments. Transactions conducted between interconnected computers through a special software-server Bitcoin client and dozens exchanges enable exchange BitCoins other major currencies (EUR, USD).

Επινοήθηκαν διάφοροι τρόποι ώστε να απλοποιηθεί ο τρόπος συναλλαγών. Η χρήση αντικειμένων με αντιπροσωπευτική αξία αποτέλεσε ο νέος τρόπος συναλλαγών, ο οποίος λάνσαρε έναν καινούργιο τρόπο στην αγοραπωλησία των προϊόντων. Ως πρώτο αντικείμενο χρησιμοποιήθηκε το κοχύλι και συναποφάσισαν, δηλαδή, ότι για να πάρει κάποιος 1 κιλό μήλα, έπρεπε να δώσει 10 κοχύλια ή ότι κρέας αξίας 1 κιλού αντιστοιχούσε σε 20 κοχύλια. Όπως φαίνεται και στην παραπάνω εικόνα, οι προαναφερθείσες συναλλαγές πραγματοποιήθηκαν γύρω το 6000 πχ, στα πλαίσια της ανταλλακτικής οικονομίας[1].

Στην συνέχεια, όταν οι άνθρωποι άρχισαν να επεξεργάζονται το μέταλλο, η έννοια του χρήματος άρχισε να εξελίσσεται ακόμα περισσότερο. Οι άνθρωποι άρχισαν να επεξεργάζονται το μέταλλο σε διαφορετικές εποχές ανάλογα με την περιοχή.

Η επινόηση του νομίσματος, περίπου τον 7 αιώνα π.Χ., υπήρξε καθοριστικός παράγοντας στις εμπορικές σχέσεις των χωρών. Με αυτό τον τρόπο διευκολύνθηκαν περαιτέρω οι μεταξύ τους συναλλαγές, απλουστεύοντας τα ήδη υπάρχοντα μέσα. Ως μέσο συναλλαγής τα νομίσματα είναι το αποτέλεσμα μίας μακρόχρονης, επίπονης εξέλιξης και αναζήτησης για την βελτίωση των μέσων συναλλαγής. Τα νομίσματα αποτελούν μια βασική μονάδα μέτρησης του χρήματος. Τα νομίσματα άλλαξαν, μεταβλήθηκαν, προσαρμόστηκαν στις εκάστοτε αλλαγές που προκάλεσαν ή προκλήθηκαν από διαφορετικές αιτίες παρακολουθώντας κοινωνικές, οικονομικές και ιστορικές συνθήκες.

Από την επινόηση του νομίσματος έως σήμερα, οι μορφές και οι όψεις των νομισμάτων τροποποιήθηκαν ιδιαιτέρα. Τα πρώτα νομίσματα κατασκευάστηκαν στη Μ. Ασία από ήλεκτρο, κράμα χρυσού και αργύρου. Το πολύτιμο μέταλλο έδινε την αξία, το μικρό σχήμα το έκανε εύκολο στη μεταφορά, το σύμβολο της κάθε εκδίδουσας αρχής, που προστέθηκε αργότερα, έδινε την εγγύηση για το βάρος και την αυθεντικότητά του. Τον 8^{ο} αιώνα μ.Χ έκανε την εμφάνιση του, στην Κίνα, το

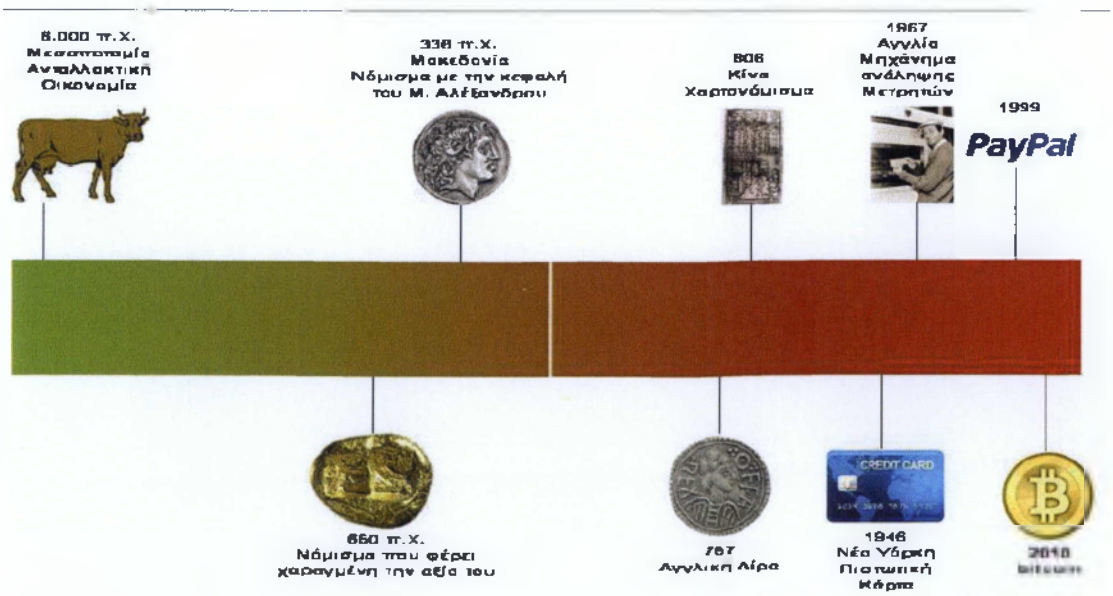
[1] http://www.oikade.gr/Children/usefull/money/i-istoria-tou-xrimatos/

Κεφάλαιο 1.

1.1 Εισαγωγή

Το χρήμα είναι μία από τις αρχαιότερες και πιο σημαντικές εφευρέσεις του ανθρώπου. Κι αυτό, γιατί χάρη στο χρήμα, κατάφερε να δημιουργήσει πιο καλά οργανωμένες κοινωνίες. Αν κάνουμε μια σύντομη αναδρομή από την προϊστορία μέχρι σήμερα, θα αντιληφθούμε ότι ο τρόπος, τον οποίο πραγματοποιούνταν οι συναλλαγές μεταβάλλεται και πάντα τείνει να προσαρμόζεται με τις εκάστοτε συνθήκες της εποχής.

Ο άνθρωπος, στις πρώτες του συναλλαγές, έκανε ανταλλαγές προϊόντων ώστε να δίνει το προϊόν που έχει σε επάρκεια και να προμηθεύεται το προϊόν που έχει σε έλλειψη. Με το πέρας των ετών, οι άνθρωποι συνειδητοποίησαν ότι αυτές οι ανταλλαγές δεν ήταν πάντοτε δίκαιες. Γιατί, για παράδειγμα, ένα κιλό λάδι δεν είχε την ίδια αξία με ένα κιλό μήλα! Επίσης, προέκυψε το πρόβλημα της εποχικότητας των προϊόντων καθώς ένας παραγωγός ντομάτας θα έχει την δυνατότητα να ανταλλάσει προϊόντα τον χειμώνα αφού δεν θα είχε διαθέσιμα προϊόντα.



Εικόνα 1.Ιστορική αναδρομή του χρήματος

πρώτο χαρτονόμισμα, το 1946, δημιουργείται η πρώτη πιστωτική κάρτα «ανοίγοντας» τον δρόμο στις ηλεκτρονικές συναλλαγές, το 1999 συναντάμε το PayPal και το 2010, δημιουργείται το πρώτο ψηφιακό νόμισμα, το Bit Coin.

1.2 Περίγραμμα πτυχιακής

Η παρούσα πτυχιακή εργασία οργανώνεται στα παρακάτω κεφάλαια:

Στο κεφάλαιο 2 γίνεται μία εκτενή αναφορά για τις ηλεκτρονικές συναλλαγές. Οι ηλεκτρονικές συναλλαγές εμφανίστηκαν κατά την δεκαετία του 1960 και αποτέλεσαν «επανάσταση» στις καθημερινές συναλλαγές. Οι ηλεκτρονικές συναλλαγές μπορούν να πραγματοποιηθούν με διάφορα μέσα, όπως πιστωτικές ή χρεωστικές κάρτες, paypal και πλέον με τα ψηφιακά νομίσματα, με δημοφιλέστερα τα Bitcoins. Βέβαια, η χρήση όλων των παραπάνω προϋποθέτουν μηχανισμούς και πρωτόκολλα ασφαλείας, τα οποία θα παρουσιαστούν στην συνέχεια αυτού του κεφαλαίου.

Στο κεφάλαιο 3 γίνεται μια πρώτη γνωριμία με το BitCoin. Αναφέρονται βασικές έννοιες ώστε να καταλάβουμε καλύτερα το νέο κρυπτονόμισμα και παραθέτονται τα πλεονεκτήματα, τα μειονεκτήματα, καθώς και η νομοθετική όψη του Bitcoin.

Στο κεφάλαιο 4 παρουσιάζονται τα «συστατικά» του BitCoin. Γίνεται μια λεπτομερή αναφορά της αλυσίδας των block (BlockChain), των συναλλαγών με τα BitCoins, της διαδικασίας εξόρυξης.

Στο πέμπτο κεφάλαιο παρουσιάζονται τα εργαλεία του BitCoin. Παραθέτουμε στοιχεία για τις διευθύνσεις και τους BitCoin Clients, καθώς και επίσης παρουσιάζονται τα σημαντικότερα ανταλλακτήρια BitCoins και κρυπτονομισμάτων.

Κεφάλαιο 2 – Ηλεκτρονικές Συναλλαγές

2.1 Εισαγωγή στις Ηλεκτρονικές Συναλλαγές

Η εφαρμογή και η διείσδυση του Ηλεκτρονικού Εμπορίου στο σύγχρονο επιχειρηματικό περιβάλλον δημιούργησε την ανάγκη ανάπτυξης νέων πιο ευέλικτων μορφών πληρωμών, τέτοιες ώστε να συμβαδίζουν με την καλπάζουσα ανάπτυξη του ηλεκτρονικού εμπορίου και τις ανάγκες τις ηλεκτρονικής επιχειρηματικότητας. Έτσι, αναπτύχθηκαν τα λεγόμενα «Συστήματα Ηλεκτρονικών Πληρωμών» τα οποία δίνουν λύση στις ηλεκτρονικές πλέον διεκπεραιώσεις των οφειλών.

Οι ηλεκτρονικές πληρωμές αποτελούν αναπόσπαστο τμήμα του Ηλεκτρονικού Εμπορίου. Υπό μίαν ευρεία έννοια, ως ηλεκτρονική πληρωμή μπορεί να ορισθεί η οικονομική συναλλαγή η οποία λαμβάνει χώρα on-line μεταξύ πωλητών και αγοραστών, οι οποίοι μπορεί να βρίσκονται σε μεγάλη ή μικρή απόσταση μεταξύ τους, χωρίς να απαιτείται η φυσική παρουσία τους. Το περιεχόμενο αυτής της συναλλαγής έχει τη μορφή κάποιου ψηφιακού οικονομικού μέσου (πχ κρυπτογραφημένους αριθμούς πιστωτικών καρτών, ηλεκτρονικές επιταγές, ή ψηφιακό χρήμα) το οποίο μέσον υποστηρίζεται από κάποιον χρηματοπιστωτικό οργανισμό, τράπεζα ή άλλον ενδιάμεσο φορέα. (Δουκίδης Γ., Πουλυμενάκου Α., Γεωργόπουλος Ν., Μότσιος Θ., 2001).

2.2 Ηλεκτρονικές Πληρωμές

Τα συστήματα πληρωμών που χρησιμοποιούν ηλεκτρονικά δίκτυα διανομής αποτελούν διαδεδομένη πρακτική στο χώρο των τραπεζών και των επιχειρήσεων ήδη από την δεκαετία του 1960 ειδικά για την μεταφορά μεγάλων χρηματικών ποσών. Μέσα στις τέσσερις δεκαετίες που μεσολάβησαν από την εμφάνιση τους έχουν λάβει χώρα σημαντικές τεχνολογικές εξελίξεις που αφενός διεύρυναν τις δυνατότητες των συστημάτων ηλεκτρονικών πληρωμών και αφετέρου

δημιούργησαν καινούριες κοινωνικές πρακτικές που καθιστούν τη χρήση των συστημάτων αυτών αναγκαία. Οι μεταβολές αυτές όπως είναι φυσικό έχουν επηρεάσει και των ορισμό των ηλεκτρονικών πληρωμών που μετεξελίσσεται ανάλογα με τις ανάγκες κάθε περιόδου.

Στην πιο γενική του μορφή, ο όρος ηλεκτρονικές πληρωμές (electronic payments) περιλαμβάνει κάθε πληρωμή προς τις επιχειρήσεις, τις τράπεζες ή τις δημόσιες υπηρεσίες από πολίτες ή επιχειρήσεις οι οποίες εκτελούνται με την μεσολάβηση ενός τηλεπικοινωνιακού ή ηλεκτρονικού δικτύου με χρήση της σύγχρονης τεχνολογίας. Η έννοια, επομένως, περικλείει αφενός την μεταφορά χρημάτων ή πληροφοριών σχετικά με τους λογαριασμούς των εμπλεκομένων μερών στη συναλλαγή και αφετέρου τα τεχνολογικά μέσα ή κανάλια διανομής μέσω των οποίων πραγματοποιείται η συναλλαγή. Το εύρος του ορισμού έχει ως αποτέλεσμα να είναι εφικτές οι πολλαπλές ταξινομήσεις του φαινομένου.

2.3 Μέθοδοι Ηλεκτρονικών Πληρωμών

Έτσι, με την πάροδο των ετών, υλοποιήθηκαν διάφοροι τρόποι ηλεκτρονικών πληρωμών, οι οποίοι εξελίσσονται διαρκώς και «κερδίζουν» ολοένα και περισσότερους πελάτες. Έρευνα έδειξε ότι 67% του καταναλωτικού κοινού χρησιμοποιούν και εμπιστεύονται τους μεθόδους που θα αναλύσουμε παρακάτω, καθώς δηλώνουν ότι τους θεωρούν πιο ευέλικτους και πιο ασφαλή.

2.3.1 Πιστωτικές Κάρτες

Μορφή του λεγόμενου "πλαστικού χρήματος", σύγχρονου και διαδεδομένου τρόπου συναλλαγών, που παρέχει τη δυνατότητα αγοράς αγαθών ή υπηρεσιών χωρίς άμεση εκταμίευση μετρητών για πληρωμή της αξίας τους. Οι πιστωτικές κάρτες εκδίδονται κυρίως από πιστωτικά ιδρύματα (π.χ. τράπεζες) και μεταξύ άλλων η χρήση τους παρέχει και τα ακόλουθα πλεονεκτήματα: α) ευκολία στις συναλλαγές σε όσες περιπτώσεις ο κάτοχος της κάρτας δεν έχει ή δεν θέλει να έχει

είναι διασυνοριακή, δηλαδή συναλλαγές μεταξύ διαφορετικών κρατών. Το σύστημα αυτό χρησιμοποιείται ιδιαίτερα από το διαδίκτυο ως πλατφόρμα επικοινωνίας.

2.3.3 Χρεωστικές Κάρτες

Οι χρεωστικές κάρτες είναι παρόμοιες με τις πιστωτικές κάρτες, με τη βασική διαφορά ότι το ποσό της συναλλαγής μεταφέρεται αυτόματα από το λογαριασμό του κατόχου στο λογαριασμό του εμπόρου και δεν πιστώνεται στον λογαριασμό του χρήστη της κάρτας όπως στις πιστωτικές κάρτες. Αν δεν υπάρχει δηλαδή διαθέσιμο ποσό στον λογαριασμό με τον οποίο είναι συνδεδεμένη η χρεωστική κάρτα, η συναλλαγή δε θα πραγματοποιηθεί. Χρεωστικές κάρτες είναι συνήθως και οι κάρτες που χρησιμοποιούμε όλοι μας για την ανάληψη μετρητών από κάποιο ATM. Οι χρεωστικές κάρτες εξασφαλίζουν μεγαλύτερη ασφάλεια και στις συναλλαγές μέσω internet καθώς μπορείτε να δημιουργήσετε έναν ξεχωριστό λογαριασμό, με ποσό που θα ελέγχετε εσείς , για χρήση αποκλειστικά με την συγκεκριμένη χρεωστική κάρτα.

Οι περισσότερες χρεωστικές κάρτες μπορούν να συνδεθούν με παραπάνω από έναν τραπεζικούς λογαριασμούς και να χρησιμοποιηθούν για να εξοφλείτε τις πάγιες μηνιαίες χρεώσεις σας όπως λογαριασμοί ΟΤΕ, ΔΕΗ, κινητής τηλεφωνίας αλλά και για την πληρωμή δανείων και πιστωτικών καρτών με αυτόματη χρέωση του τραπεζικού σας λογαριασμού. Επίσης με τις χρεωστικές κάρτες μπορείτε να πραγματοποιείτε μέσω του ATM κατάθεση μετρητών, μεταφορά ποσών μεταξύ λογαριασμών σας, ενημέρωση υπολοίπου και εκτύπωση των τελευταίων κινήσεων του λογαριασμού σας[2].

2.3.4. Έξυπνες Κάρτες

Η Έξυπνη κάρτα (smart card) είναι μια κάρτα, η οποία μοιάζει πολύ εξωτερικά με τη γνωστή πιστωτική κάρτα. Εσωτερικά, όμως, διαφέρει σημαντικά από αυτήν. Η

[2] http://www.monevexpert.gr/gr/Χρήμα

μαζί του μετρητά, β) ασφάλεια στις συναλλαγές, γιατί ο κάτοχος της κάρτας δεν χρειάζεται να έχει μαζί του μετρητά διακινδυνεύοντας έτσι να τα χάσει, γ) εξασφάλιση περιόδου χάριτος αρκετών ημερών (π.χ. 25 ή 40 ημέρες) χωρίς τόκου από την ημερομηνία έκδοσης του λογαριασμού έως την ημερομηνία πληρωμής· δ) (λειτουργώντας ως κάρτες ηλεκτρονικών συναλλαγών) παροχή της δυνατότητας στους κατόχους τους να διενεργούν τραπεζικές πράξεις μέσω των Αυτόματων Ταμειολογιστικών Μηχανών (ATM), όπως αναλήψεις, καταθέσεις, μεταφορά ποσών από λογαριασμό σε λογαριασμό κ.ά.

Τα τελευταία χρόνια η ευρεία διάδοση των πιστωτικών καρτών και ο τραπεζικός ανταγωνισμός έχουν οδηγήσει σε μια συνεχή επέκταση των παρεχόμενων υπηρεσιών, διευρύνοντας έτσι την κλασική λειτουργία της κάρτας ως μέσου πληρωμών. Έτσι, προστέθηκαν ασφαλιστικές καλύψεις (ταξιδιωτική ασφάλιση, ιατρική και νομική βοήθεια), καταρτίστηκαν ειδικά προγράμματα συνεργασίας τραπεζών με επιχειρήσεις, ώστε να παρέχονται εκπτώσεις για την αγορά αγαθών ή υπηρεσιών, και τελευταία άρχισαν να εφαρμόζονται προγράμματα σύνδεσης πιστωτικών καρτών με οργανισμούς, σωματεία, λέσχες, φιλανθρωπικές ή οικολογικές οργανώσεις κ.ά. Η προσπάθεια αυτή εμπλουτισμού των πιστωτικών καρτών με στοιχεία που δεν σχετίζονται άμεσα με την κύρια λειτουργία τους αποσκοπεί κυρίως στη διεύρυνση της πελατείας του τραπεζικού φορέα, στην εξυπηρέτηση και ικανοποίηση του πελάτη και στην προβολή του συνεργαζόμενου φορέα (π.χ. ποδοσφαιρικό ή φιλανθρωπικό σωματείο).

Εικόνα 2.Πιστωτικές Κάρτες

2.3.2 Ηλεκτρονική Μεταφορά Κεφαλαίων

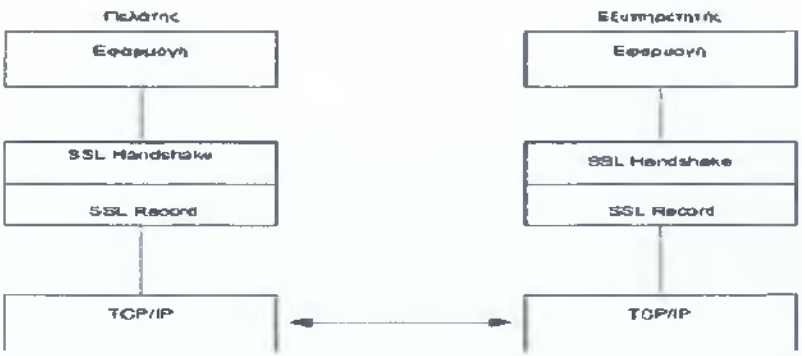
Η ηλεκτρονική μεταφοράς πίστωσης είναι πράξη με πρωτοβουλία του εντολέως μέσω ιδρύματος ή υποκατάστημα ιδρύματος, με σκοπό να τεθεί στην διάθεση του δικαιούχου χρηματικό ποσό. Η ηλεκτρονική μεταφορά κεφαλαίων είναι δυνατόν να

μπορεί να χρησιμοποιήσει είτε τον αλγόριθμο κατακερματισμού MD5, είτε τον SHA. Για την πιστοποίηση, το SSL μπορεί να χρησιμοποιήσει τα RSA δημόσια κλειδιά ή να λειτουργεί σε μία ανώνυμη κατάσταση, στην οποία χρησιμοποιείται ο αλγόριθμος ανταλλαγής κλειδιού Diffie-Hellman. Ο συνδυασμός του συμμετρικού αλγορίθμου κρυπτογράφησης, της μεθόδου συγχώνευσης μηνυμάτων και της μεθόδου πιστοποίησης, είναι γνωστός ως κρυπτογραφική συλλογή (cipher suite)[5].

Αρχικά όταν ένας SSL πελάτης (SSL client) επικοινωνεί με τον server, και οι δύο διαπραγματεύονται πια κρυπτογραφική συλλογή (cipher suite) θα χρησιμοποιήσουν. Γενικά, και οι δύο προσπαθούν να επιλέξουν την πιο ισχυρή μέθοδο κρυπτογράφησης που τους είναι διαθέσιμη. Εάν για παράδειγμα, ένας Web browser που υποστηρίζει κλειδιά συνόδου μόνο των 40-bit, επικοινωνήσει με έναν Web server που δεν έχει αυτόν τον περιορισμό, ο server τελικά θα διαπραγματευτεί και αυτός στα 40 bits. Μερικοί Web servers δίνουν την δυνατότητα στο διαχειριστή να ρυθμίσει την διαδικασία διαπραγμάτευσης. Για παράδειγμα, ο διαχειριστής μπορεί να επιτρέψει την πρόσβαση σε ένα συγκεκριμένο directory, μόνο σε αυτούς τους clients που υποστηρίζουν ισχυρή κρυπτογράφηση[6] [7].

2.4.1.2 Αρχιτεκτονική SSL

Η αρχιτεκτονική τοποθέτηση του SSL απεικονίζεται στο εικόνα 6.



Εικόνα 7.Αρχιτεκτονική Τοποθέτηση του SSL.

[5] http://en.kryptotel.net/ssl.html
[6] http://searchsecurity.techtarget.com/definition/Secure-Sockets-Layer-SSL
[7] https://www.digicert.com/ssl.htm

πιστωτική κάρτα είναι ένα απλό κομμάτι πλαστικού, στο οποίο έχει ενσωματωθεί μια μαγνητική ταινία (magnetic stripe), στην οποία είναι εγγεγραμμένα κάποια στοιχεία του χρήστη. Η έξυπνη κάρτα, αντίθετα, ενσωματώνει ένα μικροεπεξεργαστή, ο οποίος βρίσκεται κάτω από μια επαφή από χρυσό, προσαρμοσμένο στη μια πλευρά της.

Η βασική διαφορά των δύο τύπων καρτών είναι ότι, ενώ τα δεδομένα στη μαγνητική ταινία είναι εύκολο να παραλλαχθούν ή και να διαγραφούν (ακόμη και τυχαία), αυτό δεν είναι δυνατό στην έξυπνη κάρτα, γιατί ο μικροεπεξεργαστής της δεν περιέχει δεδομένα για το χρήστη: Ο μικροεπεξεργαστής της κάρτας και ο υπολογιστής, με τον οποίο συνδέεται, επικοινωνούν πριν ο μικροεπεξεργαστής επιτρέψει την πρόσβαση στα δεδομένα που περιέχονται στη μνήμη της κάρτας. Με τον τρόπο αυτό αποτρέπεται η παραχάραξη των δεδομένων κι έτσι ο χρήστης διασφαλίζεται, αν η κάρτα του βρεθεί σε διαφορετικά από τα δικά του χέρια.

Εικόνα 3.Έξυπνη Κάρτα

2.3.5. Paypal

Το PayPal είναι πύλη ηλεκτρονικών πληρωμών μέσω της οποίας διεκπεραιώνονται μεταφορές χρημάτων μέσω του Διαδικτύου. Το PayPal χρησιμεύει ως ηλεκτρονική εναλλακτική λύση στις παραδοσιακές μεθόδους, λόγου χάριν οι επιταγές και οι εντολές πληρωμών.

Ένας λογαριασμός PayPal μπορεί να χρηματοδοτηθεί με ηλεκτρονική πίστωση από ένα τραπεζικό λογαριασμό ή από μια πιστωτική κάρτα. Το PayPal είναι ένα παράδειγμα μιας πληρωμής σε υπηρεσίες διαμεσολαβήσεως, που διευκολύνει τον κόσμο κατά το ηλεκτρονικό εμπόριο.

Το PayPal εκτελεί την επεξεργασία των πληρωμών για online πωλήσεις, δημοπρασίες χώρων, καθώς και άλλους εμπορικούς χρήστες, για την οποία χρεώνει

αμοιβή. Φορτίζει μερικές φορές επίσης τέλος συναλλαγής για τη λήψη χρημάτων (ένα ποσοστό του ποσού που απέστειλε συν ένα πρόσθετο σταθερό ποσό). Το επίπεδο των τελών εξαρτάται από το χρησιμοποιούμενο νόμισμα, την επιλογή πληρωμής που χρησιμοποιείται, τη χώρα του αποστολέα, τη χώρα του δικαιούχου, το ποσό που αποστέλλεται και τον τύπο του λογαριασμού του δικαιούχου.

Εικόνα 4. Λογότυπο του Paypal

Επιπλέον, το eBay σε αγορές που γίνονται με πιστωτική κάρτα μέσω PayPal μπορεί να αναλάβει μια «αλλαγή του νομίσματος της συναλλαγής», αν ο πωλητής βρίσκεται σε άλλη χώρα, όπως και οι εκδότες πιστωτικών καρτών αυτόματα ενημερώνονται για τη χώρα προέλευσης του πωλητή.

Στις 3 Οκτωβρίου 2002, το PayPal έγινε πλήρως ελεγχόμενη θυγατρική του eBay. Εταιρική έδρα του είναι στο Σαν Χοσέ της Βόρειας Καλιφόρνιας των Ηνωμένων Πολιτειών. Η εταιρεία έχει επίσης σημαντικές δραστηριότητες εκτός Η.Π.Α και σε Chennai, Δουβλίνο, Βερολίνο και Τελ Αβίβ. Τον Ιούλιο του 2007 δραστηριοποιείται σε όλη την Ευρώπη. Στις 17 Μαρτίου 2010, το PayPal συνάπτει συμφωνία με το China UnionPay (CUP) , οργανισμός της Κίνας για έκδοση πιστωτικών καρτών, για να επιτρέψει στους Κινέζους καταναλωτές να χρησιμοποιήσουν το PayPal για να ψωνίσουν online. Το PayPal σχεδιάζει να επεκτείνει το προσωπικό του στην Ασία σε 2.000 άτομα μέχρι το τέλος του έτους[3].

2.3.6. Bitcoins

Το bitcoin είναι ένα "εναλλακτικό" νόμισμα ψηφιακής μορφής. Δεν έχει υλική υπόσταση πράγμα που σημαίνει ότι δεν υπάρχουν χαρτονομίσματα ή κέρματα bitcoin. Ουσιαστικά πρόκειται για έναν αλγόριθμο στον υπολογιστή ο οποίος παράγει νομίσματα με ένα συγκεκριμένο και απόλυτα αυτοματοποιημένο τρόπο. Το λογισμικό είναι ανοιχτού κώδικα (open source) που σημαίνει ότι ο πηγαίος κώδικας είναι διαθέσιμος σε όποιον θέλει να τον επεξεργαστεί.

[3] http://el.wikipedia.org/wiki/PayPal

Η διαδικασία που πρέπει να ακολουθήσει κανείς για να αποκτήσει bitcoins ονομάζεται εξόρυξη (Mining) κατά αντιστοιχία με την διαδικασία που ακολουθούσαν οι χρυσοθήρες του περασμένου αιώνα. Η διαδικασία της εξόρυξης είναι ουσιαστικά η προσπάθεια επίλυσης ολοένα και δυσκολότερων υπολογιστικών προβλημάτων και τα εργαλεία των σύγχρονων κυνηγών είναι πανίσχυροι υπερυπολογιστές ή συστοιχία υπολογιστών με τεράστια υπολογιστική ισχύ[4].

Εικόνα 5.Λογότυπο του Bitcoin

2.4 Ασφάλεια Ηλεκτρονικών Συναλλαγών

Η ασφάλεια των ηλεκτρονικών συναλλαγών αποτελεί το σημαντικότερο ασαφές θέμα στους κόλπους του διαδικτύου καθώς εδώ και χρόνια οι προγραμματιστές και αναλυτές προσπαθούν να καλύπτουν τα προγραμματιστικά κενά ασφαλείας που διαθέτουν οι διαδικτυακές εφαρμογές ή οι ιστοσελίδες ηλεκτρονικών συναλλαγών. Οι λύσεις που έχουν δοθεί είναι είτε η υλοποίηση πρωτοκόλλων ασφαλείας είτε οι βελτιωμένες εκδόσεις του κώδικα που «τρέχουν» οι εφαρμογές. Έτσι, μετά από πολυετή προσπάθεια, επαληθεύεται η γενική αλήθεια ότι είναι αδύνατο να επιτευχθεί η απόλυτη ασφάλεια στις ηλεκτρονικές εφαρμογές.

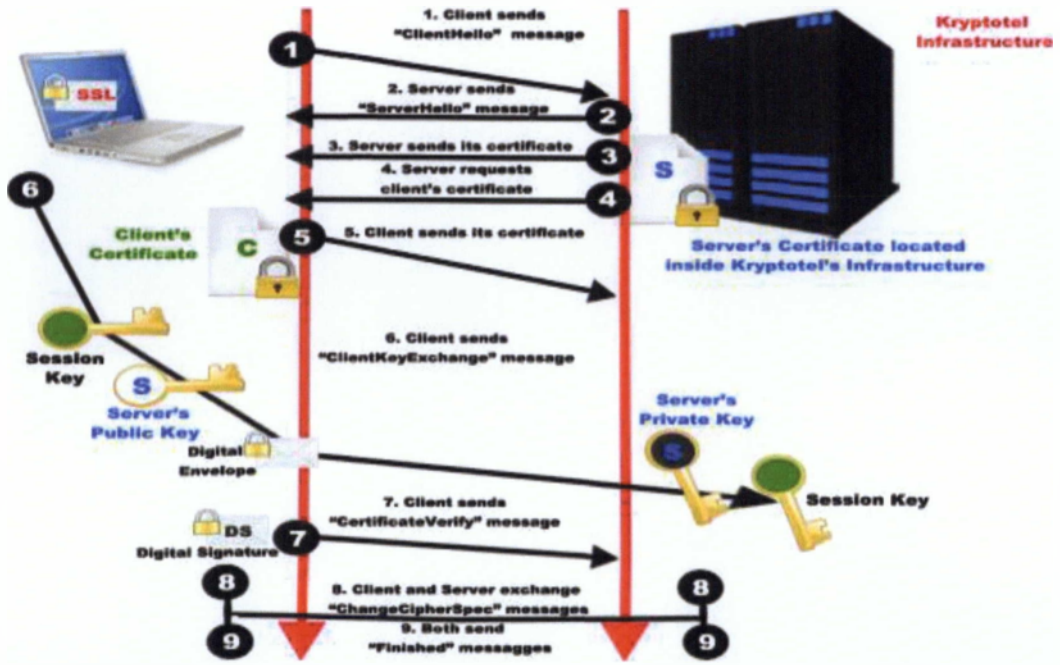
2.4.1 Πρωτόκολλο Ασφαλείας SSL

Το πρωτόκολλο SSL λειτουργεί στο επίπεδο μεταφοράς του TCP/IP (TCP/IP transport layer). Ένα επίπεδο δηλαδή πιο κάτω από το επίπεδο που βρίσκονται τα πρωτόκολλα εφαρμογής όπως, είναι το NNTP (news), HTTP (Web), και SMTP (e-mail). Αυτή είναι και η πιο σημαντική διαφορά με το S-HTTP πρωτόκολλο. Τα χαρακτηριστικό αυτό δίνει στο SSL ευελιξία και ανεξαρτησία. Οποιοδήποτε πρόγραμμα χρησιμοποιεί το TCP. μπορεί να τροποποιηθεί για να χρησιμοποιήσει και ασφαλείς SSL συνδέσεις με μερικές μόνον αλλαγές στο πηγαίο κώδικα του. Επιπλέον εκτός από τους Web browsers που υποστηρίζουν το SSL πρωτόκολλο,

[4] http://coolweb.gr/bitcoin-ti-einai/

υπάρχει και ένα πλήθος άλλων προγραμμάτων, όπως TELNET προγράμματα, προγράμματα για news και e-mail που υποστηρίζουν το πρωτόκολλο αυτό.

Το βασικό μειονέκτημα της προσθήκης του SSL πρωτοκόλλου στο επίπεδο μεταφοράς (transport layer) του TCP/IP, είναι ότι επειδή δεν είναι ειδικά διαμορφωμένο για την συνεργασία του με το HTTP πρωτόκολλο, το Web browsing μπορεί και να μην είναι και τόσο αποτελεσματικό, όπως θα μπορούσε να ήταν. Ένας άλλος μη σημαντικός περιορισμός είναι ότι μία SSL σύνδεση πρέπει να χρησιμοποιεί μία αποκλειστική TCP/IP υποδοχή (TCP/IP socket). Όταν ένας Web server βρίσκεται σε SSL λειτουργία, χρησιμοποιεί μία ξεχωριστή δικτυακή θύρα (συνήθως την θύρα 442) για την κρυπτογραφημένη επικοινωνία του.



Εικόνα 6.Διαδικασία Αυθεντικοποίησης μέσω πρωτοκόλλου SSL. Διαθέσιμο στο: http://en.kryptotel.net/ssl.html

Ένα άλλο σημαντικό χαρακτηριστικό του SSL είναι η ευελιξία, λαμβάνοντας υπόψη του τις βασικές λειτουργίες επιλογής του αλγορίθμου συμμετρικής κρυπτογράφησης, συγχώνευσης μηνυμάτων και μεθόδου πιστοποίησης. Για την συμμετρική κρυπτογράφηση, το SSL μπορεί να χρησιμοποιήσει οποιονδήποτε από τους DES, triple-DES, RC2, ή RC4 αλγορίθμους. Για την συγχώνευση μηνυμάτων

Το SSL μπορεί να λειτουργήσει πάνω από οποιοδήποτε πρωτόκολλο μεταφοράς. Δεν εξαρτάται από την ύπαρξη του TCP/IP και υποστηρίζει πρωτόκολλα εφαρμογών όπως τα HTTP, FTP και TELNET. Το TCP/IP (Transmission Control Protocol/Internet Protocol),όπως αναφέρθηκε και στο πρώτο μέρος, είναι το πρωτόκολλο επικοινωνίας (communication protocol) για την επικοινωνία ανάμεσα σε υπολογιστές που είναι συνδεδεμένοι στο διαδίκτυο.

Τα αρχικά TCP/IP αναφέρονται σε δύο από τα σημαντικότερα πρωτόκολλα που χρησιμοποιούνται στο διαδίκτυο, δηλ. στο TCP και στο IP. Το FTP (File Transfer Protocol) είναι ένα πρωτόκολλο μεταφοράς αρχείων, το οποίο φροντίζει για τη διακίνηση αρχείων μέσα στο διαδίκτυο, και το TELNET είναι ουσιαστικά μια υπηρεσία του διαδικτύου με την οποία οι χρήστες αποκτούν απευθείας πρόσβαση σε άλλους υπολογιστές στο διαδίκτυο. Είναι σημαντικό κάθε καινούργιο πρωτόκολλο επικοινωνίας να συμμορφώνεται με το μοντέλο διασύνδεσης ανοικτών συστημάτων (Open System Interconnection, OSI), έτσι ώστε να μπορεί να αντικαταστήσει εύκολα κάποιο υπάρχον πρωτόκολλο ή να ενσωματωθεί στην υπάρχουσα δομή πρωτοκόλλων. Το SSL λειτουργεί προσθετικά σε σχέση με την υπάρχουσα δομή του OSI και όχι ως πρωτόκολλο αντικατάστασης. Επιπλέον η χρήση του SSL δεν αποκλείει τη χρήση άλλου μηχανισμού ασφαλείας που λειτουργεί σε υψηλότερο επίπεδο, όπως για παράδειγμα το S/HTTP που εφαρμόζεται στο επίπεδο εφαρμογής πάνω από το SSL. Το S/HTTP (Secure HTTP) πρωτόκολλο φροντίζει για την ασφαλή μεταφορά δεδομένων στο διαδίκτυο.

Ένα σημαντικό πλεονέκτημα της ασφάλειας επιπέδου μεταφοράς γενικά και του SSL ειδικότερα είναι η ανεξαρτησία από την εφαρμογή, που σημαίνει ότι μπορεί να χρησιμοποιηθεί για να παρέχει ασφάλεια διαφανώς σε οποιαδήποτε TCP/IP εφαρμογή στρωματοποιείτε στην κορυφή του.

Το πρωτόκολλο SSL παρέχει TCP/IP ασφάλεια σύνδεσης, η οποία έχει τρεις βασικές ιδιότητες:

- Οι επικοινωνούντες μπορούν να αυθεντικοποιούνται αμοιβαία χρησιμοποιώντας κρυπτογραφία δημοσίου κλειδιού.
- Επιτυγχάνεται εμπιστευτικότητα των μεταδιδόμενων δεδομένων αφού η σύνδεση κρυπτογραφείται διαφανώς μετά από μια αρχική χειραψία και τον καθορισμό ενός κλειδιού συνόδου.
- Προστατεύεται η ακεραιότητα των μεταδιδόμενων δεδομένων, καθώς τα μηνύματα αυθεντικοποιούνται διαφανώς και ελέγχονται ως προς την ακεραιότητα τους κατά τη μετάδοση με χρήση MACs.

Για τη γενική λειτουργία του πρωτοκόλλου SSL υπάρχουν δύο βασικές οντότητες: σύνοδος SSL και σύνδεση SSL. Η σύνοδος SSL αποτελεί τη δημιουργία μιας σχέσης μεταξύ ενός πελάτη και ενός εξυπηρετητή. Οι σύνοδοι δημιουργούνται από το SSL Handshake protocol και είναι ομάδες παραμέτρων ασφάλειας, οι οποίες μπορούν να διαμοιραστούν ταυτόχρονα σε πολλές συνδέσεις. Ο κύριος λόγος για αυτό είναι η αποφυγή χρονοβόρων διαπραγματεύσεων νέων παραμέτρων ασφάλειας για κάθε νέα σύνδεση. Οι παράμετροι που περιέχονται και μοιράζονται σε μια σύνοδο είναι οι ακόλουθοι:

- ✓ Αναγνωριστικό συνόδου: επιλέγεται από τον εξυπηρετητή για αναγνώριση μιας ενεργούς ή επαναληπτικής κατάστασης συνόδου.
- ✓ Ψηφιακό πιστοποιητικό (μεταξύ ομότιμων οντοτήτων).
- ✓ Μέθοδος συμπίεσης των δεδομένων: Αλγόριθμος που χρησιμοποιείται για συμπίεση δεδομένων πριν την κρυπτογράφηση.
- ✓ Αλγόριθμος κρυπτογράφησης των δεδομένων.
- ✓ Κύριο μυστικό (master secret): Μοναδικός αριθμός μήκους 48-byte, κοινό μυστικό μεταξύ εξυπηρετητή και πελάτη.
- ✓ Δυνατότητα επανεκκίνησης της συνόδου[8].

[8] http://www.hit.bme.hu/~buttyan/courses/BMEVIHI4372/ssl.pdf

2.4.2. Πρωτόκολλο ασφαλείας SET (Secure Electronic Transactions)

2.4.2.1 Ορισμός

Το SET (Secure Electronic Transaction) είναι ένα πρωτόκολλο εμπορικών συναλλαγών με τη χρήση καρτών σε ανοικτά δίκτυα, το οποίο αναπτύχθηκε από την MasterCard και την Visa σαν μια μέθοδος εξασφάλισης των συναλλαγών με τη χρήση καρτών διαμέσου του Internet. Η διαδικασία περιλαμβάνει ένα αριθμό ελέγχων ασφαλείας που πραγματοποιείται με τη χρήση ψηφιακών πιστοποιητικών που χορηγούνται στους εμπλεκόμενους αγοραστές, εμπόρους και τράπεζες[9].

2.4.2.2 Προδιαγραφές

Το SET έχει δημιουργηθεί βάση συγκεκριμένων προδιαγραφών που προήλθαν από τις απαιτήσεις των επιχειρήσεων και αφορούσαν τις συναλλαγές τους. Αυτές οι προδιαγραφές είναι:

1. Παροχή προστασίας των οικονομικών δεδομένων ή και άλλων που διακινούνται μαζί τους από υποκλοπή.
2. Διασφάλιση της ακεραιότητας των δεδομένων.
3. Παροχή διαδικασιών πιστοποίησης ταυτότητας του κατόχου κάρτας.
4. Παροχή υπηρεσιών πιστοποίησης των εμπόρων που μπορούν να δεχθούν την πληρωμή με τη χρήση τέτοιας μεθόδου, που προκύπτει από τη σχέση τους με κάποιο οικονομικό ίδρυμα παροχής καρτών.
5. Διασφάλιση της χρήσης των καλύτερων τεχνικών ασφάλειας και σχεδίασης συστημάτων για την προστασία όλων των νόμιμα εμπλεκομένων πλευρών.
6. Η δημιουργία ενός πρωτοκόλλου το οποίο να είναι ανεξάρτητο από τους μηχανισμούς ασφάλειας του επιπέδου μεταφοράς χωρίς όμως και να αποτρέπει τη χρήση τους.

---

[9] http://en.wikipedia.org/wiki/Secure_Electronic_Transaction

7. Να είναι διαλειτουργικό (όλοι οι κύριοι browsers δουλεύουν με όλους τους κύριους servers και οι τελευταίοι με τη σειρά τους δεν θα έχουν πρόβλημα συμβατότητας με τους Payment Gateway Servers).

2.4.2.3 Συστατικά Στοιχεία του SET

Τα συστατικά στοιχεία του συστήματος SET είναι τέσσερα και είναι τα παρακάτω:

- **Cardholder Wallet (Πορτοφόλι Χρήστη Κάρτας).**

  Είναι ένα προϊόν που χρησιμοποιεί ο καταναλωτής που βρίσκεται on-line και που επιτρέπει την πραγματοποίηση ασφαλών συναλλαγών σε ένα δίκτυο. Το Wallet πρέπει να δημιουργεί μηνύματα που τα αντιλαμβάνονται τα άλλα τρία προϊόντα που απαρτίζουν το SET (Merchant, Payment Gateway, Certificate Authority).

- **Merchant Server (Server - Έμπορος)**

  Είναι ένα προϊόν το οποίο τρέχει κάποιος on-line έμπορος για την επεξεργασία των στοιχείων των συναλλαγών και τη διεκπεραίωσή τους. Επικοινωνεί και αυτό με τα άλλα τρία μέρη του SET.

- **Payment Gateway (Πύλη Πληρωμών)**

  Είναι το προϊόν που τρέχει κάποιος τρίτος ο οποίος και επεξεργάζεται την πιστοποίηση των εμπόρων και των συναλλαγών (συμπεριλαμβανομένων οδηγιών πληρωμών από κατόχους καρτών). Επιπλέον αλληλεπιδρά και με ιδιωτικά εμπορικά δίκτυα.

- **Certificate Authority (Υπηρεσία Πιστοποιητικών)**

  Είναι το τελευταίο από τα συστατικά στοιχεία του SET το οποίο τρέχει μια αρμόδια υπηρεσία έκδοσης και πιστοποίησης ψηφιακών πιστοποιητικών για το σκοπό αυτό και όποτε ζητείται από τα Wallet, Merchant και Payment Gateway πάνω από δημόσια ή ιδιωτικά δίκτυα.

2.4.3. Κρυπτογράφηση Δημόσιου Κλειδιού

Η κρυπτογράφηση δημοσίου κλειδιού (Public Key Cryptography) ή ασύμμετρου κλειδιού (Asymmetric Cryptography) επινοήθηκε στο τέλος της δεκαετίας του 1970 από τους Whitfield Diffie και Martin Hellman και παρέχει ένα εντελώς διαφορετικό μοντέλο διαχείρισης των κλειδιών κρυπτογράφησης από την προγενέστερη κρυπτογράφηση συμμετρικού κλειδιού. Η βασική ιδέα είναι ότι ο αποστολέας και ο παραλήπτης δεν μοιράζονται ένα κοινό μυστικό κλειδί όπως στην περίπτωση της κρυπτογράφησης συμμετρικού κλειδιού, αλλά διαθέτουν διαφορετικά κλειδιά για διαφορετικές λειτουργίες.

Ένα δημόσιο κλειδί 1024 bits το οποίο αναπαρίσταται ως μία ακολουθία αλφαριθμητικών χαρακτήρων. Συγκεκριμένα κάθε χρήστης διαθέτει δύο κλειδιά κρυπτογράφησης: το ένα ονομάζεται ιδιωτικό κλειδί (private key) και το άλλο δημόσιο κλειδί (public key). Το ιδιωτικό κλειδί θα πρέπει ο κάθε χρήστης να το προφυλάσσει και να το κρατάει κρυφό, ενώ αντιθέτως το δημόσιο κλειδί μπορεί να το ανακοινώνει σε όλη τη διαδικτυακή κοινότητα ή σε συγκεκριμένους παραλήπτες. Υπάρχουν δε και ειδικοί εξυπηρετητές δημοσίων κλειδιών (public key servers) στους οποίους μπορεί κανείς να απευθυνθεί για να βρει το δημόσιο κλειδί του χρήστη που τον ενδιαφέρει ή να ανεβάσει το δικό του δημόσιο κλειδί για να είναι διαθέσιμο στο κοινό.

Εικόνα 8:Ένα δημόσιο κλειδί 1024 bits το οποίο αναπαρίσταται ως μία ακολουθία αλφαριθμητικών χαρακτήρων.

Τα δύο αυτά κλειδιά (ιδιωτικό και δημόσιο) έχουν μαθηματική σχέση μεταξύ τους. Εάν το ένα χρησιμοποιηθεί για την κρυπτογράφηση κάποιου μηνύματος, τότε το άλλο χρησιμοποιείται για την αποκρυπτογράφηση αυτού. Η επιτυχία αυτού του είδους κρυπτογραφικών αλγορίθμων βασίζεται στο γεγονός ότι η γνώση του δημόσιου κλειδιού κρυπτογράφησης δεν επιτρέπει με κανέναν τρόπο τον υπολογισμό του ιδιωτικού κλειδιού κρυπτογράφησης.

Η κρυπτογράφηση δημοσίου κλειδιού λύνει ένα σημαντικότατο πρόβλημα που υπήρχε στους κρυπτογραφικούς αλγόριθμους συμμετρικού κλειδιού. Συγκεκριμένα, οι κρυπτογραφικοί αλγόριθμοι συμμετρικού κλειδιού χρησιμοποιούν ένα κοινό μυστικό κλειδί, το οποίο το γνωρίζουν τόσο ο αποστολέας του κρυπτογραφημένου μηνύματος όσο και ο παραλήπτης. Αυτό το κοινό μυστικό κλειδί χρησιμοποιείται κατά τη διαδικασία κρυπτογράφησης και αποκρυπτογράφησης του μηνύματος. Προκύπτει όμως το εξής πρόβλημα: Εάν υποθέσουμε ότι το κανάλι επικοινωνίας δεν είναι ασφαλές, τότε πως γίνεται ο αποστολέας να στείλει το κλειδί κρυπτογράφησης στον παραλήπτη για να μπορέσει αυτός με τη σειρά του να αποκρυπτογραφήσει το μήνυμα; Αυτό το πρόβλημα είναι ιδιαίτερα έντονο στις σύγχρονες ψηφιακές επικοινωνίες όπου σε πολλές περιπτώσεις ο αποστολέας δεν γνωρίζει καν τον παραλήπτη και απέχει από αυτόν αρκετές χιλιάδες χιλιόμετρα. Οι κρυπτογραφικοί αλγόριθμοι δημοσίου κλειδιού λύνουν αυτό το πρόβλημα και ανοίγουν νέους δρόμους για εφαρμογές της κρυπτογράφησης (ηλεκτρονικά μηνύματα, διαδικτυακές αγορές κοκ).

2.4.3.1 Τρόπος Λειτουργίας

Δημιουργία κλειδιών

Η δημιουργία του δημόσιου και του ιδιωτικού κλειδιού γίνεται από ειδικές συναρτήσεις οι οποίες δέχονται ως είσοδο έναν μεγάλο τυχαίο αριθμό και στην έξοδο παράγουν το ζεύγος των κλειδιών. Είναι προφανές ότι όσο πιο τυχαίος είναι ο αριθμός που παρέχεται ως είσοδος στη γεννήτρια κλειδιών τόσο πιο ασφαλή είναι τα κλειδιά που παράγονται. Σε σύγχρονα προγράμματα κρυπτογράφησης ο τυχαίος

δικαιώματα. Πληροφορίες που βρίσκονται στον ένα κόμβο, ανάλογα με τα δικαιώματα που καθορίζονται, μπορούν να διαβαστούν από όλους τους άλλους και αντίστροφα.

2.4.4.1 Ιστορικό

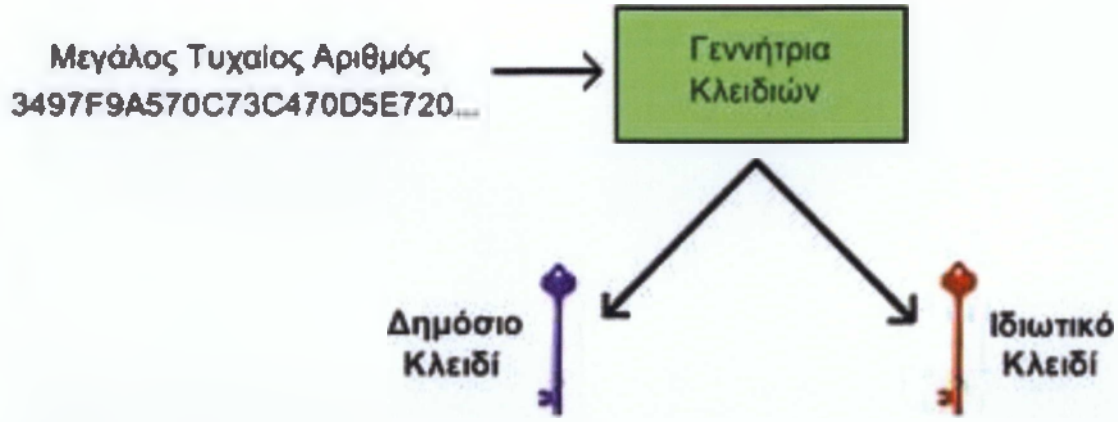
Στις αρχές του 1999 ο Σον Φάνινγκ (Shawn Fanning) ξεκίνησε την υλοποίηση μιας ιδέας, η οποία θα του έδινε τη δυνατότητα αυτός και οι φίλοι του να αναζητήσουν στο Διαδίκτυο μουσικά κομμάτια MP3 της προτίμησής τους. Μερικούς μήνες αργότερα, η Napster μετρούσε πάνω από 21 εκατομμύρια χρήστες. Σε καμία περίπτωση, όμως, ο 18χρονος τότε μαθητής δεν μπορούσε να φανταστεί ότι το δημιούργημά του θα άλλαζε τον τρόπο με τον οποίο απολαμβάνουμε πολυμεσικές εφαρμογές και γενικά να επικοινωνούμε.

Η βασική ιδέα πίσω από το Napster ήταν η δημιουργία μιας εφαρμογής-πρωτοκόλλου, η οποία θα συνδύαζε μια μηχανή αναζήτησης, ενός προγράμματος ανταλλαγής αρχείων βασισμένης στα πρωτόκολλα διαμοιρασμού αρχείων των Windows και του UNIX και ενός προγράμματος IRC, ώστε να είναι εφικτή η συζήτηση μεταξύ των χρηστών που βρισκόταν εκείνη τη στιγμή online. Το όνομα της εφαρμογής προήλθε από το παρατσούκλι του Φάνινγκ στο σχολείο λόγω του περίεργου κουρέματός του. Η εφαρμογή του Φάνινγκ έγινε νούμερο 1 στις προτιμήσεις των χρηστών στον Διαδικτυακό τόπο download.com και άνοιξε το δρόμο για την επανάσταση των δικτύων Peer-to-Peer, η οποία συνεχίζεται ως τις μέρες μας.

2.4.4.2 Αρχιτεκτονική

Οι κόμβοι (πρόκειται για προσωπικούς υπολογιστές, σταθμούς εργασίας, κλπ.) που μετέχουν σε ένα peer-to-peer σύστημα σχηματίζουν ένα δίκτυο επικάλυψης (overlay network) πάνω από την υπάρχουσα υποδομή του διαδικτύου. Διασυνδέονται, επικοινωνούν και ανταλλάσσουν πληροφορίες μεταξύ τους σε

αριθμός παράγεται ως εξής: Κατά τη διαδικασία κατασκευής των κλειδιών, το πρόγραμμα σταματάει για 5 λεπτά και καλεί τον χρήστη να συνεχίσει να εργάζεται με τον υπολογιστή. Στη συνέχεια για να παράξει τον τυχαίο αριθμό συλλέγει στα 5 αυτά λεπτά τυχαία δεδομένα που εξαρτώνται από τη συμπεριφορά του χρήστη (κινήσεις ποντικιού, πλήκτρα του πληκτρολογίου που πατήθηκαν, κύκλοι μηχανής που καταναλώθηκαν κοκ). Με βάση αυτά τα πραγματικά τυχαία δεδομένα υπολογίζεται ο τυχαίος αριθμός και εισάγεται στη γεννήτρια κλειδιών για να κατασκευαστεί το δημόσιο και το ιδιωτικό κλειδί του χρήστη.

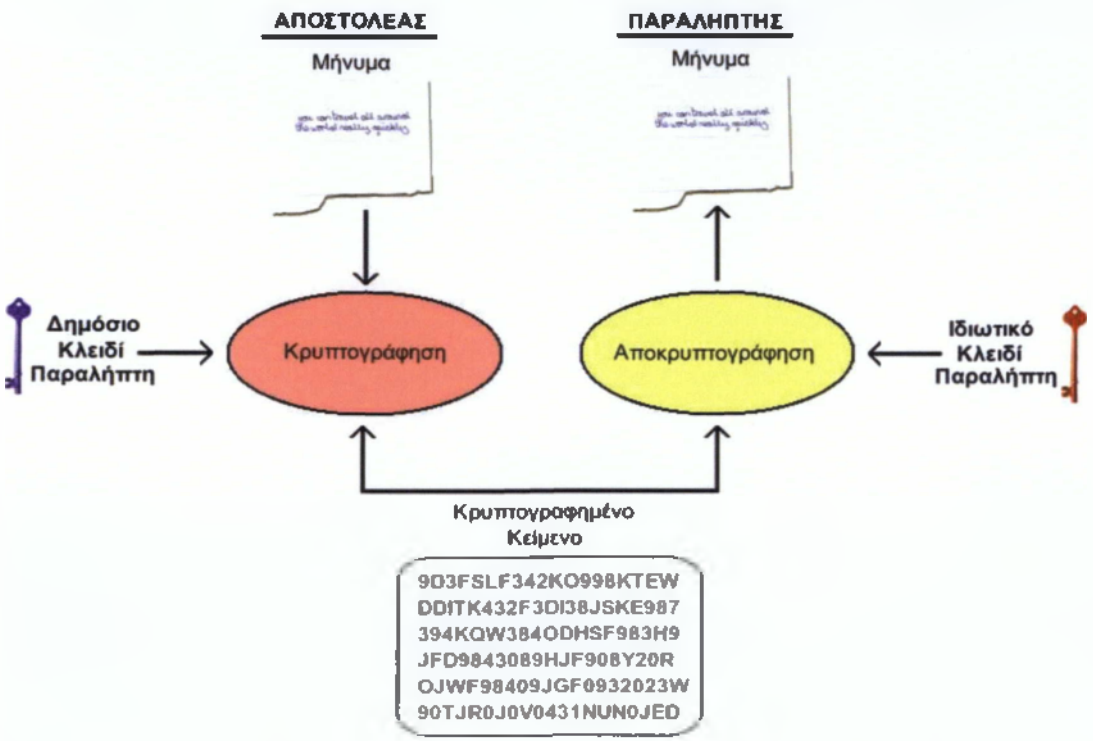


Εικόνα 9.Τρόπος λειτουργίας της γεννήτριας κλειδιών.

2.4.3.2 Εμπιστευτικότητα

Οι κρυπτογραφικοί αλγόριθμοι δημοσίου κλειδιού μπορούν να εγγυηθούν εμπιστευτικότητα (confidentiality), δηλαδή ότι το κρυπτογραφημένο μήνυμα που θα στείλει ο αποστολέας μέσω του διαδικτύου στον παραλήπτη θα είναι αναγνώσιμο από αυτόν και μόνο. Για να επιτευχθεί η εμπιστευτικότητα, ο αποστολέας θα πρέπει να χρησιμοποιήσει το δημόσιο κλειδί του παραλήπτη για να κρυπτογραφήσει το μήνυμα. Στη συνέχεια στέλνει το κρυπτογραφημένο μήνυμα στον παραλήπτη και ο τελευταίος μπορεί να το αποκρυπτογραφήσει με το ιδιωτικό κλειδί του. Δεδομένου ότι το ιδιωτικό κλειδί του παραλήπτη είναι γνωστό μονάχα

στον ίδιο και σε κανέναν άλλον, μονάχα ο παραλήπτης μπορεί να αποκρυπτογραφήσει το μήνυμα και να το διαβάσει. Άρα λοιπόν με αυτόν τον τρόπο ο αποστολέας γνωρίζει ότι το κρυπτογραφημένο μήνυμα μπορεί να αποκρυπτογραφηθεί μονάχα από τον παραλήπτη και έτσι διασφαλίζεται η εμπιστευτικότητα του μηνύματος.



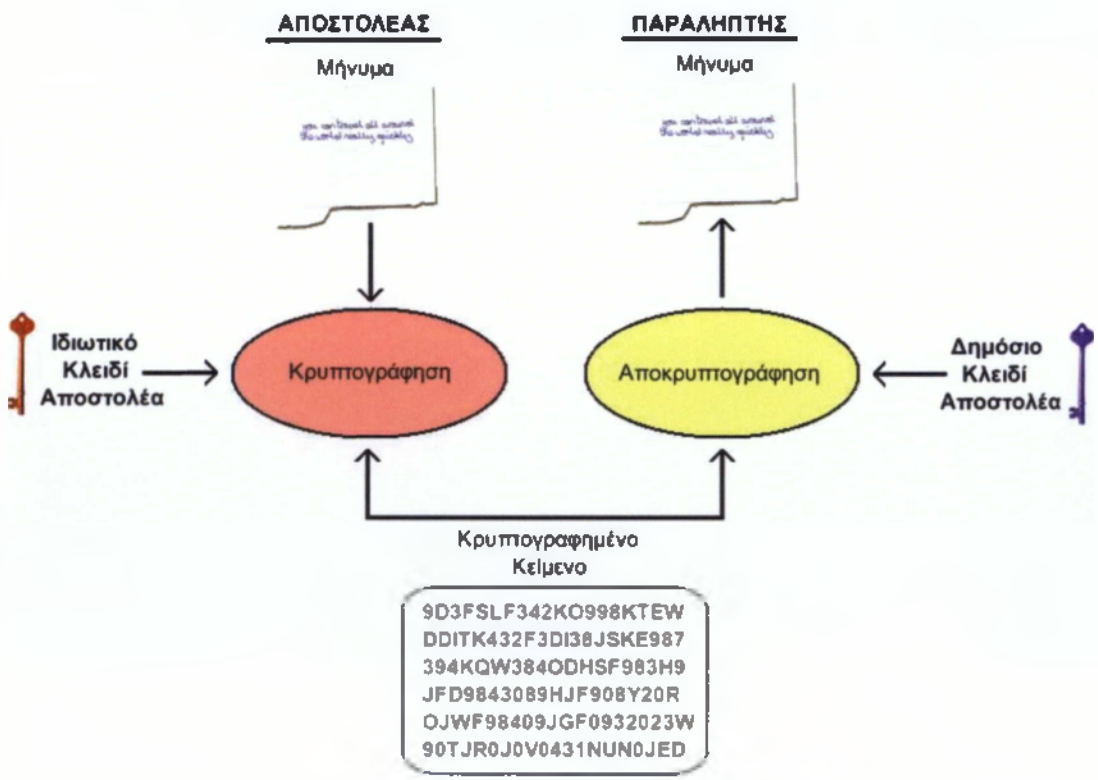
Εικόνα 10. Επίτευξη εμπιστευτικότητας αλλά όχι πιστοποίησης χρησιμοποιώντας κρυπτογραφικούς αλγόριθμους δημοσίου κλειδιού.

Η παραπάνω μέθοδος μπορεί να εξασφαλίσει την εμπιστευτικότητα αλλά όχι την πιστοποίηση του αποστολέα. Αυτό με λίγα λόγια σημαίνει πως η παραπάνω μέθοδος δεν μπορεί να εγγυηθεί την ταυτότητα του αποστολέα. Πράγματι, ο αποστολέας μπορεί να δηλώσει ψευδή ταυτότητα και ο παραλήπτης να νομίσει ότι το συγκεκριμένο μήνυμα προήλθε από άλλο πρόσωπο.

2.4.3.3 Πιστοποίηση

Χρησιμοποιώντας κατάλληλα τους κρυπτογραφικούς αλγορίθμους δημοσίου κλειδιού μπορεί να επιτευχθεί πιστοποίηση (authentication), δηλαδή ο παραλήπτης

να γνωρίζει με ασφάλεια την ταυτότητα του αποστολέα. Για να επιτευχθεί αυτό θα πρέπει ο αποστολέας να χρησιμοποιήσει το ιδιωτικό του κλειδί για την κρυπτογράφηση του μηνύματος. Στη συνέχεια στέλνει το μήνυμα στον παραλήπτη και ο τελευταίος χρησιμοποιεί το δημόσιο κλειδί του αποστολέα για την αποκρυπτογράφησή του. Δεδομένου ότι το ιδιωτικό κλειδί του αποστολέα είναι γνωστό μονάχα στον ίδιο, ο παραλήπτης μπορεί να είναι σίγουρος για την ταυτότητα του αποστολέα.



Εικόνα 11. Επίτευξη αυθεντικοποίησης αλλά όχι εμπιστευτικότητας χρησιμοποιώντας κρυπτογραφικούς αλγόριθμους δημοσίου κλειδιού.

2.4.4 Σύστημα Peer -to- Peer

Ένα δίκτυο υπολογιστών peer-to-peer (ή P2P) είναι ένα δίκτυο που επιτρέπει σε δύο ή περισσότερους υπολογιστές να μοιράζονται τους πόρους τους ισοδύναμα. Το δίκτυο αυτό χρησιμοποιεί την επεξεργαστική ισχύ, τον αποθηκευτικό χώρο και το εύρος ζώνης (bandwidth) των κόμβων. Όλοι οι κόμβοι του δικτύου έχουν ίσα

2.4.4.4 Μη Κεντρικοποιημένα peer-to-peer συστήματα

Μια άλλη κατηγορία αρχιτεκτονικών είναι οι μη-κεντρικοποιημένες όπου οι κόμβοι συγκροτούν το overlay δίκτυο είτε δομημένα ακολουθώντας κανόνες για τον σχηματισμό του δικτύου, είτε αδόμητα όπου δεν υπάρχει ούτε κεντρικό directory ούτε ακριβείς οδηγίες για τον σχηματισμό τοπολογίας του δικτύου και την τοποθέτηση των περιεχομένων.

2.4.4.5 Δομημένα peer-to-peer συστήματα

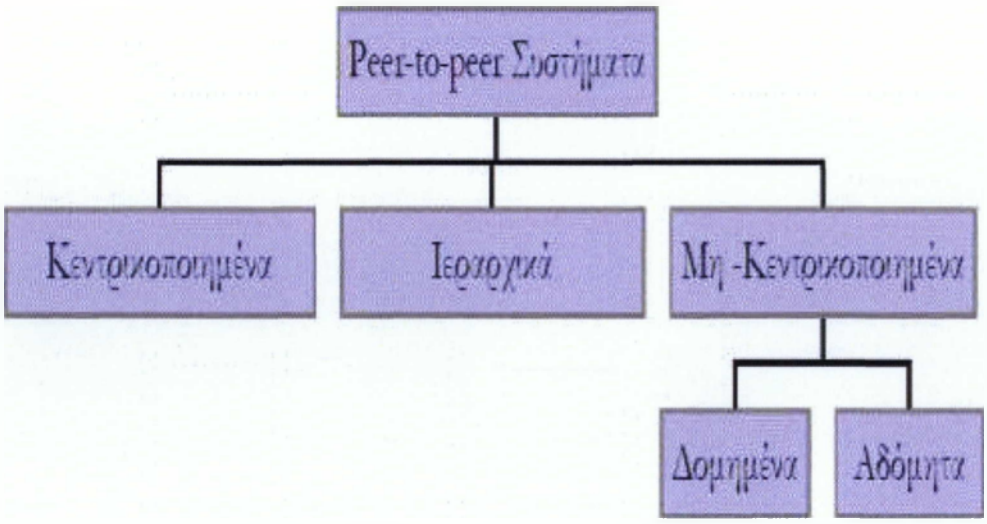
Στα δομημένα peer-to-peer συστήματα οι κόμβοι οργανώνονται σε δομημένο γράφο για το σχηματισμό του overlay δικτύου. Στα δεδομένα αντιστοιχίζεται ένα κλειδί και η τοποθέτηση τους στους κόμβους γίνεται με προκαθορισμένο τρόπο έτσι ώστε να διευκολύνεται η αναζήτησή τους και να επιτυγχάνεται η κλιμάκωση. Η τοποθέτηση των αρχείων στα χαλαρά δομημένα συστήματα βασίζεται στην εκτίμηση (on hints) για το που μπορεί να βρεθεί η αναζητούμενη πληροφορία. Στα αυστηρά δομημένα συστήματα τόσο η δόμηση του overlay δικτύου όσο και η τοποθέτηση των αρχείων είναι σαφώς καθορισμένη.

Ο εντοπισμός ενός αντικειμένου-δεδομένου από μια εφαρμογή στα δομημένα συστήματα γίνεται σε μικρό αριθμό βημάτων (network hops), υπό την απαίτηση βέβαια να διατηρείται ένας μικρός πίνακας δρομολόγησης σε κάθε κόμβο. Παραδείγματα τέτοιων συστημάτων αποτελούν τα [5]:

- ✓ Content Addressable Network (CAN),
- ✓ Chord,
- ✓ Tapestry,
- ✓ Pastry,
- ✓ Kademlia,
- ✓ Viceroy.

τοπολογίες ανεξάρτητα από το δίκτυο υποδομής (IP network) διατηρώντας την αυτονομία τους[10]. Η αρχιτεκτονική του δικτύου επηρεάζει τον μηχανισμό δρομολόγησης μηνυμάτων αναζήτησης, την απόδοση, την ικανότητα κλιμάκωσης, την προσαρμοστικότητα - ανοχή σε σφάλματα, κλπ. και στοχεύει στην υποστήριξη λειτουργιών όπως διαμοιρασμό αρχείων (file sharing), κατανεμημένο υπολογισμό (distributed computing), επικοινωνία – συνεργασία μεταξύ των χρηστών (collaboration network).

Υπάρχουν διάφορες αρχιτεκτονικές (Εικόνα 14) για τον σχηματισμό του overlay δικτύου[5]:



Εικόνα 12.Αρχιτεκτονικές Peer-to-peer

2.4.4.3 Κεντρικοποιημένα peer-to-peer συστήματα

Στις κεντρικοποιημένες αρχιτεκτονικές υπάρχει ένας κεντρικός εξυπηρέτης (Directory Server) στον οποίο απευθύνουν οι κόμβοι τα ερωτήματα τους για να πληροφορηθούν που βρίσκονται οι επιθυμητές πληροφορίες (π.χ Napster). Μια τέτοια αρχιτεκτονική αν και είναι αρκετά αποδοτική, δεν έχει την ιδιότητα της κλιμάκωσης ενώ έχει ενιαίο σημείο της αποτυχίας (bottleneck).

[10] Computer για όλους, "Peer To Peer Computing", Αριθμός Τεύχους: 202

να μοιράζονται. Οι χρήστες μπορούν να αναζητήσουν στους Index Servers αυτούς τα αρχεία που ψάχνουν, χρησιμοποιώντας ένα κατάλληλο πρόγραμμα-πελάτη. Όταν το αρχείο βρεθεί, ανοίγει μια σύνδεση μεταξύ των δύο χρηστών για τη μεταφορά του. Σε αυτή τη κατηγορία ανήκουν το Napster το DC++ και το WinMX.

Αποκεντρωτικά P2P δίκτυα

Η φιλοσοφία εδώ είναι εντελώς διαφορετική. Κάθε σύστημα που συμμετέχει αποτελεί ταυτόχρονα client και server (ή αλλιώς servent). Μόλις κάποιος συνδεθεί μέσω ενός ανάλογου προγράμματος-πελάτη P2P, κάνει γνωστή την παρουσία του σε ένα μικρό αριθμό υπολογιστών ήδη συνδεδεμένων οι οποίοι με τη σειρά τους προωθούν τη δήλωση παρουσίας του σε ένα μεγαλύτερο δίκτυο υπολογιστών κ.λ.π Πλέον ο χρήστης έχει τη δυνατότητα να αναζητήσει οποιαδήποτε πληροφορία μεταξύ των διαμοιραζόμενων αρχείων. Τα δίκτυα αυτά λέγονται και δεύτερης γενιάς. Η μεταφορά των αρχείων είναι όμοια με αυτή των συγκεντρωτικών P2P δικτύων. Σε αυτή τη κατηγορία ανήκουν το Kazaa, το Gnutella και το BearShare.

P2P δίκτυα τρίτης γενιάς

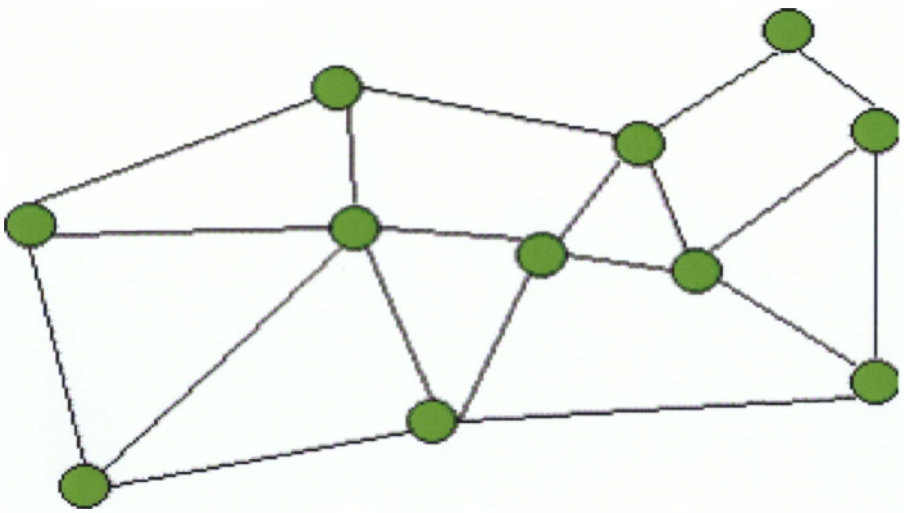
Είναι αυτά τα οποία διαθέτουν χαρακτηριστικά ανωνυμίας όπως το Freenet, το I2P και το Entropy. Είναι αποκεντρωτικού τύπου και η φιλοσοφία του βασίζεται εκτός από την ανωνυμία, στην υψηλή βιωσιμότητα του, στο συνεχή διαμοιρασμό των αρχείων και στην κωδικοποίησή τους έτσι ώστε κανείς να μην μπορέσει ποτέ να αποκτήσει κανένα είδος ελέγχου πάνω σε αυτό. Τα δίκτυα αυτού του τύπου είναι υπό ανάπτυξη και έχουν χαρακτηριστεί ως μικρά παγκόσμια δίκτυα.

2.4.4.8 Χρήση των Peer-to-Peer δικτύων

Είναι γενικά αποδεκτό ότι η χρήση τέτοιων δικτύων ενώνει χρήστες από όλο τον κόσμο λειτουργώντας χωρίς λογοκρισία, ελέγχους ή φραγμούς προάγοντας τη

2.4.4.6 Αδόμητα peer-to-peer συστήματα

Στα συστήματα αυτά δεν υπάρχει καμιά δομή στο overlay δίκτυο, όπως απεικονίζεται στην εικόνα 15. Τα περιεχόμενα τοποθετούνται σε κόμβους στο δίκτυο χωρίς γνώση της τοπολογίας ή άλλης συσχέτισης με αυτό. Τα μη δομημένα συστήματα είναι κατάλληλα σε περιπτώσεις όπου μεγάλο πλήθος κόμβων μετέχει παροδικά στο δίκτυο χωρίς όμως αποδοτικούς μηχανισμούς αναζήτησης, κλιμάκωσης, διαθεσιμότητας. Υποστηρίζουν καλύτερα πολύπλοκα ερωτήματα σε σχέση με τα δομημένα[11].



Εικόνα 13.Παράδειγμα Αδόμητου peer-to-peer συστήματος

2.4.4.7 Μορφές Peer-to-Peer δικτύων

Τα Peer-to-Peer δίκτυα χωρίζονται σε τρεις κατηγορίες:

Συγκεντρωτικά P2P δίκτυα

Πολλοί, όταν αναφέρονται σε αυτά, χρησιμοποιούν τη φράση «πρώτης γενιάς P2P δίκτυα». Εδώ, υπάρχει ένας κεντρικός Index Server στον οποίο αποθηκεύονται οι πληροφορίες για τα περιεχόμενα των καταλόγων που οι συμμετέχοντες επιθυμούν

[11] Ν. Κρεμμύδας, "Επισκόπηση στα Συστήματα Ομότιμων Κόμβων", Ε.Μ.Π., 2005

βασική ιδέα της δημιουργίας του παγκοσμίου ιστού που δεν είναι άλλη από την ελεύθερη διακίνηση ιδεών και τη δωρεάν παροχή υπηρεσιών και πληροφοριών.

Η απλή δομή, το μηδαμινό κόστος και η άναρχη ροή πληροφορίας είναι τα στοιχεία που καθιστούν τη λειτουργία των P2P δικτύων μοναδική. Η φιλοσοφία τους δίνει τη δυνατότητα στους συμμετέχοντες της δημιουργίας δυναμικά αναπτυσσόμενων χώρων, το περιεχόμενο των οποίων καθορίζεται από τους ίδιους τους χρήστες.

Από την άλλη τα δίκτυα p2p καθιστούν δυνατή την αντιγραφή και διανομή αρχείων μεταξύ χρηστών, τα οποία προστατεύονται από πνευματικά δικαιώματα, όπως τραγούδια, ταινίες και λογισμικό, χωρίς τη συναίνεση του κατόχου των πνευματικών δικαιωμάτων. Η ευρεία χρήση των δικτύων p2p για αυτόν τον σκοπό συντέλεσε ώστε τα δίκτυα να ταυτιστούν με έννοιες όπως «παρανομία» και να υποστούν πόλεμο τόσο τα ίδια και οι δημιουργοί τους, όσο και οι χρήστες τους. Ειδικά στα συγκεντρωτικά p2p δίκτυα όπως το Napster η κατηγορία ήταν ότι η μεσολάβηση μεταξύ των χρηστών και η αποθήκευση στον κεντρικό server της εταιρίας των στοιχείων που ήταν απαραίτητα για την ανταλλαγή αρχείων ήταν αρκετή, για να στοιχειοθετηθεί συνέργεια της εταιρίας που λειτουργούσε το δίκτυο στην παραβίαση της πνευματικής ιδιοκτησίας που τελούσαν οι χρήστες. Στην υπόθεση Napster στην Αμερική η ομώνυμη εταιρία καταδικάστηκε να καταβάλει υψηλές αποζημιώσεις σε πνευματικούς δημιουργούς και κατόχους πνευματικών δικαιωμάτων ως συνεργός στην παραβίαση των δικαιωμάτων τους που τελούσαν οι χρήστες, ανταλλάσσοντας παράνομα αντίγραφα μεταξύ τους. Σαν αντίδραση σε αυτήν τη νομολογία αναπτύχθηκαν τα αποκεντρωτικά συστήματα p2p, στα οποία δεν υπάρχει κεντρικός server που να αποθηκεύει την οποιαδήποτε πληροφορία σχετικά με τα ανταλλασσόμενα αρχεία, παρά μόνο ένα λογισμικό, το οποίο επιτρέπει τη διασύνδεση των υπολογιστών των τελικών. Το εγχείρημα αυτό γνωστό και ως LionShare βασίζεται στα δεύτερης γενιάς P2P δίκτυα και φτιάχνεται για το διαμοιρασμό στους χρήστες τους ακαδημαϊκού υλικού. Ένα άλλο ίσως πιο γνωστό τέτοιο δίκτυο είναι το SETI@home.

Κεφάλαιο 3 – Bitcoins

3.1 Εισαγωγή

Τα «κρυπτονομίσματα» είναι κρυπτογραφικώς κωδικοποιημένα ψηφιακά νομίσματα που χρησιμοποιούνται για την άμεση, ανέπαφη συναλλαγή μεταξύ ομότιμων χρηστών, παρακάμπτοντας οιοδήποτε ενδιάμεσο μέρος (κράτος, τράπεζες, αρχές). Οι συναλλαγές στηρίζονται σε ένα αποκεντρωμένο παγκόσμιο δίκτυο χρηστών P2P που καθορίζει την αξία του νομίσματος βάσει προσφοράς και ζήτησης.

Το πρώτο ανοιχτό λογισμικό παραγωγής «κρυπτονομίσματος» δημιουργήθηκε το 2009 (Davis, 2011) από κάποιον (ή κάποιους) υπό το ψευδώνυμο Satoshi Nakamoto και ονομάστηκε Bitcoin. Όταν γράφεται με κεφαλαίο γράμμα όπως εδώ, αναφέρεται στο λογισμικό και στο δίκτυο P2P που χρησιμοποιείται για να παράγει και να διακινεί χρήμα μέσω κρυπτογραφίας. Αντίθετα, τα bitcoins αναφέρονται στα ίδια τα νομίσματα που χρησιμοποιούνται για να επεξεργάζονται πληροφορίες από το λογισμικό. Τα νομίσματα παράγονται μέσω μιας διαδικασίας που αποκαλείται mining (εξόρυξη) και στην οποία οι συμμετέχοντες πιστοποιούν και καταγράφουν τις συναλλαγές με αντάλλαγμα προμήθειες συναλλαγών ή και καινούρια bitcoins[12].

Με απλά λόγια, το Bitcoin είναι ένα εντελώς ψηφιακό νόμισμα. Δεν υπάρχει επισήμως σε καμία φυσική μορφή, κερμάτων ή χαρτονομισμάτων. Δεν παράγεται από καμία συγκεκριμένη χώρα. Δεν ελέγχεται από καμία συγκεκριμένη τράπεζα. Η παραγωγή του, η αποθήκευσή του, και η διακίνησή του, και όλες οι συναλλαγές με αυτό γίνονται αποκλειστικά σε ηλεκτρονική μορφή. Το Bitcoin ονομάστηκε "cryptocurrency[13]" (κρυπτονόμισμα) επειδή είναι αποκεντρωμένο και χρησιμοποιεί κρυπτογράφηση για τον έλεγχο των συναλλαγών και την αποφυγή της διπλής

[12] http://coolweb.gr/bitcoin-ti-einai/
[13] http://en.wikipedia.org/wiki/Cryptocurrency

δαπάνης (double - Spending[14]), ένα πρόβλημα που υπάρχει με τα ψηφιακά νομίσματα. Όταν ολοκληρωθεί η συνολική του έκδοση (όταν βρεθούν όλα τα bitcoin από την διαδικασία παραγωγής του, που είναι η εξόρυξη από κρυπτογραφημένα μπλοκ), κάθε μεμονωμένη συναλλαγή θα έχει καταχωρηθεί μόνιμα σε έναν δημόσιο λογαριασμό-καθολικό που είναι γνωστός ως the blockchain (η αλυσίδα των μπλοκ). Η διαδικασία παραγωγής του γίνεται με την επεξεργασία των μπλοκ από ένα δίκτυο ιδιωτικών ηλεκτρονικών υπολογιστών που συχνά είναι ειδικά προσαρμοσμένα (υλισμικό και λογισμικό) για το έργο αυτό. Οι φορείς αυτών των υπολογιστών, που είναι γνωστοί ως "σκαπανείς" (miners), ανταμείβονται για τα έξοδα εξόρυξης με την απόδοση μεταφοράς των νεόκοπων Bitcoins στα πορτοφόλια τους.

3.1 Βασικές έννοιες του Bitcoin

Κατ' αντιστοιχία με τα σύγχρονα νομίσματα, τα Bitcoin νομίσματα είναι μια σύμβαση μεταξύ των χρηστών. Ένα Bitcoin νόμισμα δεν έχει υλική υπόσταση, είναι μια δημόσια δήλωση κατοχής ενός νομίσματος, η οποία έχει υπογραφεί ψηφιακά με το κλειδί του κατόχου και η οποία δήλωση έχει γίνει μαθηματικά αποδεκτή από το δίκτυο των ομοτίμων χρηστών.

3.1.1 Διευθύνσεις Bitcoin

Κάθε χρήστης χρησιμοποιεί ένα λογισμικό bitcoin client που υλοποιεί το bitcoin πρωτόκολλο και συνδέεται στο peer-to-peer δίκτυο του bitcoin. Ο χρήστης δημιουργεί τοπικά στον υπολογιστή, με τη βοήθεια του bitcoin client, ένα ψηφιακό πορτοφόλι (wallet). Το πορτοφόλι δεν είναι παρά ένα σύνολο ζευγών δημόσιου-ιδιωτικού κλειδιού. Σε κάθε δημόσιο κλειδί αντιστοιχεί μια bitcoin διεύθυνση. Ο χρήστης μπορεί να δημιουργήσει όσα ζεύγη κλειδιών -και επομένως διευθύνσεις- θέλει. Ο χρήστης χρησιμοποιεί τα κλειδιά/διευθύνσεις για να λάβει και να στείλει bitcoin νομίσματα.

[14] https://en.bitcoin.it/wiki/Double-spending

3.1.2 Συναλλαγές Bitcoin

Μια συναλλαγή Bitcoin είναι η μεταφορά νομισμάτων από μια bitcoin διεύθυνση σε μια ή περισσότερες διαφορετικές bitcoin διευθύνσεις. Ο αποστολέας και κάτοχος ενός νομίσματος bitcoin έχει το bitcoin νόμισμα στο πορτοφόλι του, και συγκεκριμένα το νόμισμα αυτό αντιστοιχεί σε μια bitcoin διεύθυνση/δημόσιο κλειδί. Ο αποστολέας, με τη βοήθεια του λογισμικού, υπογράφει ψηφιακά με το ιδιωτικό κλειδί του ζεύγους μια δήλωση που περιέχει το ποσό της συναλλαγής και τις bitcoin διευθύνσεις των παραληπτών. Η δήλωση αυτή, ψηφιακά υπογεγραμμένα μεταδίδεται προς όλους τους κόμβους του bitcoin δικτύου, ούτως ώστε όλοι οι χρήστες του bitcoin να ενημερωθούν για τη νέα συναλλαγή.

3.1.3 Απουσία κεντρικής αρχής και δημόσια καταγραφή όλων των συναλλαγών

Στα παραδοσιακά νομίσματα υπάρχουν κεντρικές αρχές, όπως οι τράπεζες ή τα κράτη, που υποτίθεται ότι είναι οι εγγυητές της αξιοπιστίας των νομισμάτων και των χρηματικών συναλλαγών. Στο bitcoin αφενός δεν υπάρχει καμία κεντρική αρχή, αφετέρου τα bitcoins είναι ψηφιακή πληροφορία, δεν έχουν υλική υπόσταση. Η εγγύηση της κάθε συναλλαγής γίνεται με τη βοήθεια του peer-to-peer δικτύου κάνοντας χρήση μαθηματικών και κρυπτογραφίας.

Το πρώτο πρόβλημα σε ένα αποκεντρωμένο και ψηφιακό περιβάλλον είναι ότι τα χρήματα δεν πρέπει να είναι αυτοδημιούργητα. Δηλαδή είναι απαραίτητο ο κάθε χρήστης να μην μπορεί αυθαίρετα να εκδώσει bitcoins τα οποία στη συνέχεια να υπογράψει ώστε να πραγματοποιήσει μία πληρωμή. Με λίγα λόγια, θέλουμε κάθε κόμβος στο δίκτυο να μπορεί να επιβεβαιώσει ότι ο εκάστοτε χρήστης πράγματι έχει στην κατοχή του τα bitcoins που ισχυρίζεται ότι μπορεί να χρησιμοποιήσει σε συναλλαγή. Ο μόνος τρόπος να επιτευχθεί κάτι τέτοιο, αφού δεν υπάρχει κάποια κεντρική αρχή, είναι γνωστοποιώντας σε όλο το δίκτυο κάθε συναλλαγή που πραγματοποιείται, δηλαδή ποιά διεύθυνση έχει πόσα νομίσματα. Αυτό είναι απαραίτητο ώστε να μπορούμε να βεβαιωθούμε ότι ένα νόμισμα είναι έγκυρο και ότι πρόκειται να ξοδευτεί από τον κάτοχό του μόνο μία φορά.

Για να μπορέσει να διατηρήσει κάθε κόμβος τη γνώση για το τι χρήματα υπάρχουν στο δίκτυο ανά πάσα στιγμή, είναι απαραίτητο να γνωστοποιούνται όλες οι νέες συναλλαγές. Κάθε νέα συναλλαγή μεταδίδεται σε όλο το δίκτυο και εφόσον είναι έγκυρη καταγράφεται στο συλλογικό ιστορικό των συναλλαγών. Το ιστορικό αυτό είναι γνωστό σε όλους. Έτσι, κάθε παραλήπτης μπορεί να επιβεβαιώσει ότι τα χρήματα που λαμβάνει από τον αποστολέα ήταν στην κατοχή του αποστολέα πριν την αποστολή τους.

Όταν κάποιος νέος κόμβος συνδέεται στο δίκτυο, οι κόμβοι με τους οποίους συνδέεται (γείτονες) τον ενημερώνουν για το πού ανήκουν τα νομίσματα που υπάρχουν στο δίκτυο. Πιο συγκεκριμένα, όταν ένας κόμβος συνδέεται στο δίκτυο ενημερώνεται για το πλήρες ιστορικό της ανταλλαγής χρημάτων που έχει διενεργηθεί στο δίκτυο από την αρχή της ύπαρξης του δικτύου μέχρι και τη στιγμή της σύνδεσής του κόμβου σε αυτό, διαδικασία που ονομάζεται συγχρονισμός.

3.1.4 Επικύρωση συναλλαγών - Δημιουργία block

Όπως είδαμε παραπάνω, κάθε κόμβος στο δίκτυο του Bitcoin έχει πλήρη γνώση όλων των έγκυρων συναλλαγών που έχουν εκτελεστεί ποτέ. Πώς επικυρώνεται όμως μια συναλλαγή; Κάθε συναλλαγή που πραγματοποιείται εντάσσεται σε μια "δεξαμενή" συναλλαγών που περιμένουν επικύρωση. Κάποιοι εξειδικευμένοι κόμβοι στο Bitcoin δίκτυο, είναι εθελοντικά επιφορτισμένοι με το να επικυρώνουν συναλλαγές. Αντλούν από την "δεξαμενή" έναν αριθμό συναλλαγών που εκκρεμούν, και προσπαθούν να λύσουν ένα μαθηματικό πρόβλημα που εμπεριέχει τις συναλλαγές αυτές.

Το μαθηματικό αυτό πρόβλημα είναι αρκετά δύσκολο να λυθεί, αλλά άπαξ και ένας κόμβος βρει μια λύση όλοι οι κόμβοι είναι σε θέση να επαληθεύσουν την εγκυρότητα της λύσης αυτής. Το μαθηματικό αυτό πρόβλημα μπορεί να παρομοιαστεί με ένα τεράστιο sudoku, με πολλές χιλιάδες γραμμές και στήλες. Η λύση ενός τέτοιου sudoku απαιτεί ένα χρονικό διάστημα ακόμα και όταν ο λύτης

είναι ένας υπολογιστής. Άπαξ όμως και βρεθεί μια λύση, τότε όλοι είναι σε θέση εύκολα και γρήγορα να την επαληθεύσουν.

Οι κόμβοι που προσπαθούν να επικυρώσουν ένα αριθμό συναλλαγών λύνοντας το μαθηματικό πρόβλημα, λέγονται miners. Ο miner που βρίσκει μια λύση στο πρόβλημα, κατασκευάζει μια δομή που περιέχει τις συναλλαγές που επικύρωσε, και η οποία δομή λέγεται block. Το block διαδίδεται στο δίκτυο του Bitcoin, και εφόσον είναι έγκυρη λύση για τις συναλλαγές που εμπεριέχει, δίνει αποδεκτό από όλους. Το block αυτό, προστίθεται αλυσιδωτά με το προηγούμενο block, συνθέτοντας την πλήρη ιστορία όλων των συναλλαγών του δικτύου, την λεγόμενη blockchain (αλυσίδα από blocks).

3.1.5 Δημιουργία νομισμάτων Bitcoin

Η δημιουργία νομίσματος πρέπει να είναι ελεγχόμενη και καθορισμένη, αλλιώς δεν υφίσταται καμία αξιοπιστία στις συναλλαγές. Αυτό ισχύει πολύ περισσότερο στον ψηφιακό κόσμο. Ένας χρήστης δεν πρέπει να είναι σε θέση να εμφανίσει bitcoins που δεν έχει ή να "αντιγράψει" τα bitcoins που διαθέτει. Πώς δημιουργούνται όμως τα bitcoins;

Για να επικυρωθούν οι συναλλαγές του δικτύου, ορισμένοι κόμβοι αναλαμβάνουν να λύσουν ένα μαθηματικό πρόβλημα και να δημιουργήσουν ένα block συναλλαγών. Η διαδικασία αυτή, που λέγεται mining, είναι διαδικασία που απαιτεί εξειδικευμένο hardware και δαπάνη ενέργειας. Ως κίνητρο και ανταπόδοση για την χρήσιμη εργασία που κάνουν οι miners, η ανεύρεση ενός block συναλλαγών ανταμείβει τον miner με 25 bitcoins. Με τον τρόπο αυτό, δημιουργούνται - ελεγχόμενα - νέα νομίσματα bitcoin[15].

[15] https://github.com/dionyziz/ntua-crypto/raw/master/bitcoin-paper.pdf

3.2 Ιστορικά στοιχεία του Bitcoins

✓ **Νοέμβρης 2008**

Προγραμματιστής με ψευδώνυμο, ή ομάδα προγραμματιστών, ο/οι Satoshi Nakamoto δημοσιεύουν τις λεπτομέρειες για το Bitcoin και λύνουν το θέμα του double-spending (διπλή - δαπάνη) και για να προστατέψουν το νόμισμα από τις αντιγραφές.

✓ **Ιανουάριος 2009**

Εγκαινιάζεται το σύστημα Bitcoin, ένα υπερπλήρες νέο σύστημα παραγωγής νομίσματος, που θα οδηγήσει στην παραγωγή 21 εκατομμυρίων bitcoins κατά την διάρκεια όλων των χρόνων μέχρι την το καταληκτικό έτος του, το 2040.

✓ **Μάιος 2010**

Η πρώτη συναλλαγή με Bitcoin λέγεται ότι έγινε πράξη όταν ένας άνθρωπος στην Φλόριντα, ο Laszlo Hanyecz, στέλνει 10.000 bitcoins σε έναν εθελοντή στο Ηνωμένο Βασίλειο, ο οποίος παραγγέλνει στο κατάστημα Papa John' s pizza και παραδίδουν μια πίτσα στο σπίτι του Hanyecz.

✓ **Αύγουστος 2010**

Ανακαλύπτεται μια ευπάθεια στο σύστημα (ακατάλληλη επαλήθευση των bitcoins) η οποία γίνεται αντικείμενο εκμετάλλευσης και δημιουργούνται 184 εκατομμύρια bitcoins. Αργότερα ανακαλύπτεται η απάτη και διαγράφονται αυτά τα πλαστά bitcoins, και όλο το σύστημα μεταφέρεται σε μια νέα ενημερωμένη έκδοση για το Bitcoin.

✓ **Οκτώβριος 2010**

Η Inter-governmental Financial Action Task Force (Διακυβερνητική Ομάδα Χρηματοπιστωτικής Δράσης) δημοσιεύει έγγραφο προειδοποιώντας για τη χρήση του ψηφιακού νομίσματος ως μέρος ενός χρηματοδοτικού μηχανισμού από τρομοκρατικές ομάδες.

✓ **Ιούνιος 2011**

Το WikiLeaks αρχίζει την αποδοχή δωρεών μόνο σε bitcoins, αφού απορρίφθηκε η δυνατότητα χρηματοδότησης του με δωρεές από τις τράπεζες και άλλες υπηρεσίες πληρωμών, όπως το PayPal, το προηγούμενο έτος. Εμφανίζεται η πρώτη φούσκα με Bitcoin, και πέφτει η αξία του από τα ~$30 στα ~$10. Στη συνέχεια, κατά τους επόμενους μήνες, η αξία του κατρακυλά σε κάτι λιγότερο από τα $3. Το ανταλλακτήριο για bitcoin, το Mt.Gox bitcoin παραβιάζεται από χάκερς και κλέβονται κέρματα. Το φόρουμ συζήτησης του Bitcoin καταγράφει μια λίστα με 28 παραβιάσεις/κλοπές με κλοπιμαία πάνω από 1.000 bitcoins για την κάθε μία. Ο Ιδιοκτήτης του Bitomat, το τρίτο μεγαλύτερο χρηματιστήριο Bitcoin, χάνει το πορτοφόλι με τα Bitcoin (Bitcoin wallet) του και τα 17.000 bitcoins που κρατούσε για λογαριασμό των πελατών του.

✓ **Αύγουστος, 2011**

Το MyBitcoin παραβιάζεται από χάκερς, χάνει 78.000 bitcoins πελατών του, το 51 τοις εκατό από τις συνολικές καταθέσεις.

✓ **Σεπτέμβριος 2011**

Τα Bitcoins γίνονται αποδεκτά για αγορά ναρκωτικών στην παράνομη αγορά "Silk Road" (Δρόμος του Μεταξιού)

✓ **Φεβρουάριος 2012**

Το κύριο ανταλλακτήριο σε Bitcoin, το TradeHill κλείνει.

✓ **Μάρτιος 2012**

Το TradeHill μηνύει ένα άλλο ανταλλακτήριο εικονικού νομίσματος, το Dwolla. Το ανταλλακτήριο Bitcoinica παραβιάζεται από χάκερς και πάνω από 43.000 bitcoins κλέβονται.

✓ **Απρίλιος 2012**

Το Reddit ανακοινώνει τις σκέψεις αποδοχής του για το νόμισμα, ικανοποιώντας τις λεγόμενες "Bitcoin strippers".

- ✓ **Μάιος 2012**

Διέρρευσε έκθεση του FBI που αποκαλύπτει τους φόβους που έχει η κυβέρνηση και οι υπηρεσίες επιβολής του νόμου για το Bitcoin, ως ένα εργαλείο που διευκολύνει τις πωλήσεις ναρκωτικών και όπλων και βοηθάει τους τρομοκράτες.

- ✓ **Ιούλιος 2012**

Ο Adam Draper εγκαινιάζει το BoostVC, μια θερμοκοιτίδα εκκίνησης για το Bitcoin.

- ✓ **Αύγουστος 2012**

Ανακοινώνεται η χρεωστική κάρτα Bitcoin. Το "Bitcoin Savings and Trust" κλείνει, αφήνοντας 5,6 εκατομμύρια δολάρια ανεξόφλητο χρέος. Το SEC (U.S. Securities and Exchange Commission) το διερευνά ως ένα σύστημα "πυραμίδας Ponzi". Κατατίθεται αγωγή εναντίον του Bitcoinica.

- ✓ **Σεπτέμβριος 2012**

Το ανταλλακτήριο Bitfloor παραβιάζεται από χάκερς κλέβονται 24.000 bitcoins, κλείνει προσωρινά και στη συνέχεια κάνει επανεκκίνηση με την υπόσχεση να πληρώσει τους πελάτες του πίσω, με μια απώλεια περίπου $250.000

- ✓ **Νοέμβριος 2012**

Η υπηρεσία blog WordPress δέχεται πληρωμές σε bitcoins.

- ✓ **Δεκέμβριος 2012**

Ανοίγει η πρώτη Bitcoin τράπεζα, με την συνεργασία του ανταλλακτηρίου bitcoin, το Bitcoin-Central και της Γαλλικής τράπεζας Credit Mutuel, το εταιρικό αυτό σχήμα θα λειτουργεί ως τράπεζα.

✓ **Φεβρουάριος 2013**

Μπορείτε να αγοράσετε πλέον πίτσα από διάφορες εταιρείες με bitcoin, συμπεριλαμβανομένων της Pizza Hut και της Dominos. Το Bitcoin αναζωογονεί τα διαδικτυακά τυχερά παιχνίδια. Η υπηρεσία ανταλλαγής/αποθήκευσης αρχείων, το Mega του Kim Dotcom αποδέχεται στις συναλλαγές του το νόμισμα. Το Internet Archive επιτρέπει δωρεές σε Bitcoin (link is external).

✓ **Μάρτιος 2013**

Η χρηματιστηριακή υπηρεσία BitInstant Social παραβιάζεται από χάκερς, κλέβονται $12.000. Δύο διαφορετικές εκδόσεις του λογισμικού Bitcoin συγκρούονται, προκαλώντας δυσλειτουργία στην αποτίμηση του Bitcoin. Το U.S. Treasury Department's Financial Crimes Enforcement Network ανακοινώνει κανονιστική θέση για τα εικονικά νομίσματα, ενθαρρύνοντας τους επενδυτές. Νέα ραγδαία άνοδος σε αποτιμήσεις της αξίας Bitcoin φέρνουν φόβους για μια νέα φούσκα. Η συνολική αγορά του Bitcoin εκτιμάται στα 400 εκατομμύρια δολάρια. Οι κεφαλαιουχικές επενδύσεις με Bitcoin σε νεοσύστατες επιχειρήσεις φτάνουν σε αποτίμηση τα 3 εκατομμύρια δολάρια. Καναδός βάζει το σπίτι του προς πώληση με αντίτιμο σε bitcoins. Ακόμα μια εταιρεία σχεδιάζει να εισαγάγει Bitcoin ATM, για να κάνει το ντεμπούτο του στην Κύπρο.

✓ **Απρίλιος 2013**

Το Bitcoin σπάει τα 100 δολάρια σε συναλλαγματική ισοτιμία για πρώτη φορά η συνολική αξία για το νόμισμα βρίσκεται στην κορυφή, στα 1 δισεκατομμύρια δολάρια. Η ισοτιμία του εμπορεύεται σήμερα στα 141,32 δολάρια, σύμφωνα με το Mt.Gox[16].

3.3 Το λογισμικό

Το μπίτκοϊν (Bitcoin) αποτελεί στη βάση του ένα λογισμικό ανοιχτού κώδικα (open source protocol). Κατά συνέπεια, ο πηγαίος κώδικας του λογισμικού είναι δημόσιος

[16] http://www.dailydot.com/business/bitcoin-complete-history-timeline/

και διαθέσιμος σε όποιον επιθυμεί να ελέγξει τις λεπτομέρειες της λειτουργίας του. Η ανωτέρω αρχή επιτρέπει σε οιονδήποτε την ελεύθερη και δωρεάν αντιγραφή και ανάπτυξη δικού του λογισμικού βασισμένου στο υπάρχον.

Το λογισμικό αποτελεί μία μέθοδο για την επίτευξη των παρακάτω κύριων στόχων:

- Θέσπιση κριτηρίων παραγωγής και συναλλαγής των ανταλλάξιμων μονάδων του λογισμικού (bitcoins),
- Διατήρηση των πληροφοριών ιδιοκτησίας των μονάδων των bitcoin που έχουν ήδη παραχθεί
- Δυναμική επιβεβαίωση της εγκυρότητας των παραπάνω, χωρίς την ανάγκη ύπαρξης κεντρικής οντότητας ελέγχου, πιστοποίησης ή διακρίβωσης

Η χρήση του λογισμικού είναι δωρεάν και διαθέσιμη σε όλες τις χώρες του κόσμου, εφόσον υπάρχει σύνδεση στο internet. Η βασική λειτουργία του λογισμικού έγκειται στην εκτέλεση συναλλαγών bitcoins και την αναμετάδοση πληροφοριών ανάμεσα σε κόμβους και την επιβεβαίωση της εγκυρότητάς τους για το υπόλοιπο δίκτυο. Καθώς το λογισμικό είναι ανοιχτού κώδικα, δύνανται να υπάρχουν πάρα πολύ διαφορετικές εκδόσεις και εκδοχές του.

Στην ουσία, ο καθένας θα μπορούσε με τις κατάλληλες ικανότητες να δημιουργήσει ένα αντίστοιχο δίκτυο, αντιγράφοντας σε μεγάλο βαθμό το λογισμικό του Bitcoin, προσθέτοντας ή διαφοροποιώντας με ότι κανόνες επιθυμεί. Κατά αυτήν την έννοια, τα συστατικά στοιχεία του λογισμικού, έχουν δημιουργηθεί συναινετικά από προγραμματιστές, ενσωματώνοντας καινοτομίες διαθέσιμες από άλλα λογισμικά ανοιχτού κώδικα, αλλά και νέα στοιχεία που δεν είχαν εμφανιστεί πριν.

Η ισχύς του δικτύου εξασφαλίζεται από την αποδοχή του από τους χρήστες. Το δίκτυο το οποίο αποτελούν οι χρήστες του Bitcoin, αποτελείται από χρήστες της ίδιας εκδοχής του λογισμικού. Αλλαγές στον κώδικα προτείνονται στην κοινότητα, αλλά η συναίνεση της κοινότητας των χρηστών και η αποδοχή τους είναι που δημιουργεί το δίκτυο.

Η πεποίθηση των χρηστών:

- Στην διαφάνεια του πηγαίου κώδικα του λογισμικού,
- Στην ακεραιότητα και διαφάνεια των συναλλασσόμενων πληροφοριών,
- Στην στιβαρότητα του δικτύου από κακόβουλες επιθέσεις,
- Στην προγραμματισμένα περιορισμένη παραγωγή bitcoins,
- Στην προστασία που παρέχουν οι κρυπτογραφικοί αλγόριθμοι που χρησιμοποιούνται ενάντια σε κακόβουλη εκμετάλλευση του δικτύου, όπως και άλλοι συμπληρωματικοί λόγοι, είναι συνολικά υπεύθυνοι για την αποδοχή του από τους χρήστες, αλλά και την εξάπλωσή του σε νέους. Αυτό 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 πεπερασμένη ποσότητα των bitcoins, δημιουργεί τις βασικές προδιαγραφές για ένα δίκτυο ανταλλαγής αξίας. Όποια αξία βρίσκουν οι χρήστες αποτυπώνεται αποκλειστικά στην αξία με την οποία είναι διατεθειμένοι να τα ανταλλάξουν, η οποία με τη σειρά της βασίζεται αποκλειστικά στους νόμους της προσφοράς και της ζήτησης, χωρίς ενδιάμεσα μέρη (χώρες, κεντρικούς εκδότες ή αρχές).

Για να μπορούν να είναι χρήσιμα σαν μέσο συναλλαγής πρέπει να εισάγονται στην κυκλοφορία σταδιακά για την κάλυψη των συναλλακτικών αναγκών, αλλά και να είναι πεπερασμένα σε συνολικό αριθμό. Αυτό επιτυγχάνεται τεχνητά και ο ρυθμός παραγωγής τους όπως και το μέγιστο πλήθος, αποτελούν μέρος των κανόνων του δικτύου. Ο μέγιστος αριθμός που θα παραχθεί ποτέ είναι 21.000.000 και ο ρυθμός παραγωγής τους θα ελαττώνεται σταδιακά έως περίπου το 2140 οπότε και θα παραχθεί το τελευταίο. Αυτή η μέθοδος σε κάποιο βαθμό, προσομοιάζει την πορεία διάθεσης ενός πολύτιμου μετάλλου (άργυρος, χρυσός) στην παγκόσμια αγορά. Αρχικά, η εξόρυξή του είναι εύκολη και σχετικά μεγάλες ποσότητες είναι πιο εύκολα διαθέσιμες, προοδευτικά όμως γίνεται σπανιότερο έως

νομισματική πολιτική και να προκαλέσει κατάρρευση – ή απλά να αποφασίσει να κατάσχει τα bitcoins των ανθρώπων, όπως η Ευρωπαϊκή Κεντρική Τράπεζα αποφάσισε να κάνει στην Κύπρο στις αρχές του 2013.

- **Είναι εύκολο να δημιουργηθεί**

Οι συμβατικές τράπεζες σας περνούν από αρκετές διαδικασίες να ανοίξετε έναν τραπεζικό λογαριασμό. Ωστόσο, μπορείτε να ορίσετε μια διεύθυνση Bitcoin σε δευτερόλεπτα, χωρίς ερωτήσεις και χωρίς καταβλητέα τέλη.

- **Είναι ανώνυμο**

Οι χρήστες μπορούν να κατέχουν πολλαπλές διευθύνσεις Bitcoin, και δεν συνδέονται με τα ονόματα, τις διευθύνσεις, ή άλλες προσωπικές πληροφορίες.

- **Είναι απολύτως διαφανής**

Το Bitcoin αποθηκεύει τις λεπτομέρειες της κάθε μεμονωμένης συναλλαγής που συνέβη ποτέ στο δίκτυο σε μια τεράστια εκδοχή του γενικού καθολικού, που ονομάζεται αλυσίδα μπλοκ . Η αλυσίδα μπλοκ τα λέει όλα. Εάν έχετε μια διεύθυνση bitcoin που χρησιμοποιείται δημοσίως, ο καθένας μπορεί να δει πόσα bitcoins αποθηκεύονται σε αυτή τη διεύθυνση. Απλώς δεν ξέρει ότι είναι η δική σας.

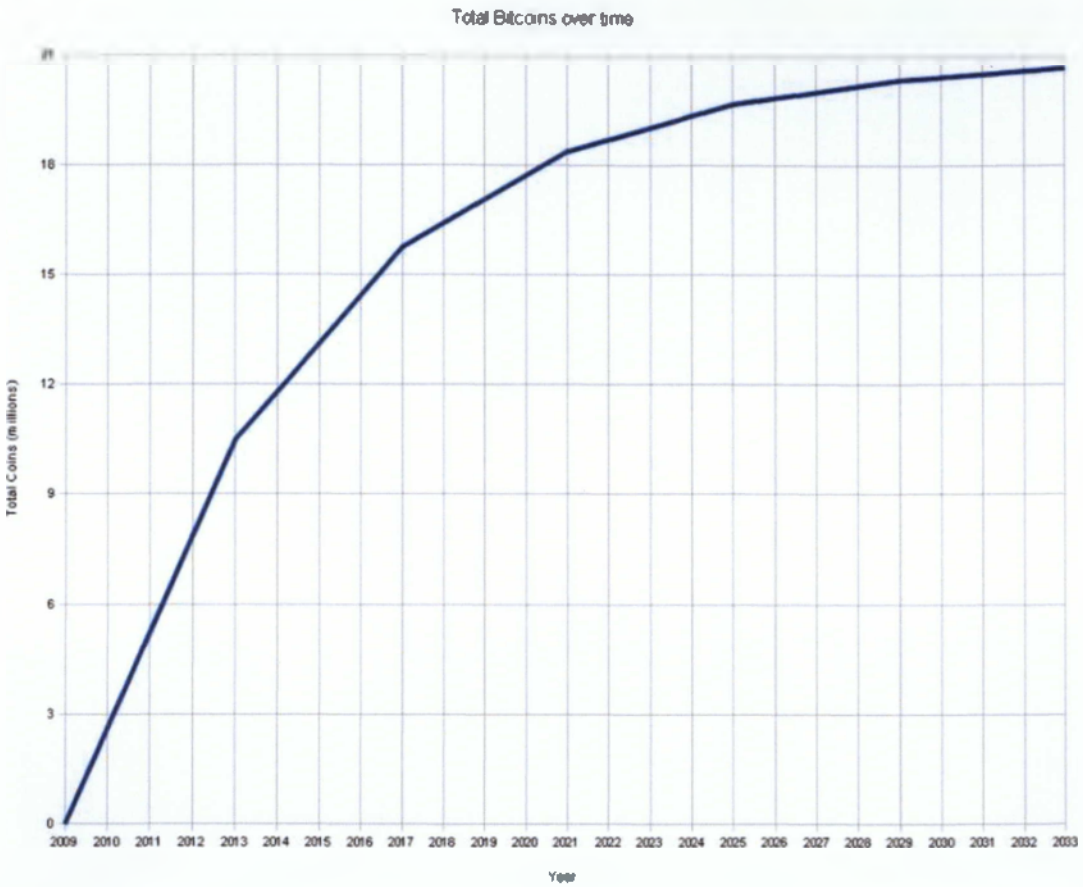
- **Οι αμοιβή συναλλαγής είναι πολύ μικρή**

Η τράπεζά σας μπορεί να σας χρεώσει ένα € 10 τέλος για τις διεθνείς μεταφορές. Το Bitcoin δεν το κάνει.

- **Είναι γρήγορο**

Μπορείτε να στείλετε χρήματα οπουδήποτε και θα φτάσει λεπτά αργότερα, μόλις το δίκτυο Bitcoin επεξεργάζεται την πληρωμή.

ότου εξαντληθούν τα αποθέματα του πλανήτη. Ο ρυθμός παραγωγής bitcoin προσαρμόζεται τεχνητά ώστε να ακολουθεί περίπου την παρακάτω καμπύλη:



Εικόνα 14.Ρυθμός Παραγωγής bitcoin. Διαθέσιμο στο: http://commons.wikimedia.org/wiki/File:Total_bitcoins_over_time.png.

3.4 Τα Χαρακτηριστικά του Bitcoin

Το Bitcoin έχει αρκετά σημαντικά χαρακτηριστικά που το ξεχωρίζουν από τα συνήθεις νομίσματα "fiat currencies".

- **Είναι αποκεντρωμένο**

Το δίκτυο Bitcoin δεν ελέγχεται από μια κεντρική αρχή. Κάθε μηχάνημα που εξάγει Bitcoins και επεξεργάζεται συναλλαγές αποτελεί ένα μέρος του δικτύου. Αυτό σημαίνει ότι, θεωρητικά, μία κεντρική αρχή δεν μπορεί να πειραματιστεί με τη

- **Είναι μη-αναστρέψιμο**

Όταν σας σταλούν bitcoins στον λογαριασμό σας, δεν υπάρχει κανένας που να μπορεί να τα πάρει τα πίσω, εκτός αν εσείς τα επιστρέψετε στον παραλήπτη.

3.5 Βασικά Πλεονεκτήματα

✓ **Ταχύτητα Συναλλαγών/Διεθνής Φύση** : 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 ή σε Smartphone, και σύνδεση στο διαδίκτυο.

✓ **Εξαιρετικά Χαμηλό κόστος συναλλαγών** : Το παρόν κόστος για κάθε συναλλαγή, ανεξαρτήτως μεγέθους, ανάγεται περίπου στα 5eurocents και είναι προαιρετικό αν δεν υπάρχει βιασύνη επιβεβαίωσης της συναλλαγής. Σε ακόμα πιο σύνθετα δίκτυα υπό την σκέπη επί μέρους ελεγκτικών δικτύων, το κόστος συναλλαγών/αγορών δύναται να προσεγγίσει πολύ χαμηλότερες τιμές. Το ποσό αυτό αποδίδεται αυτόματα στους χρήστες που εκτελούν τους ελέγχους των συναλλαγών και την επιβεβαίωση της αντικειμενικότητάς του, ως αμοιβή για την επεξεργαστική ισχύ που επενδύουν στην προστασία του δικτύου από κακόβουλες επιθέσεις.

✓ **Έλεγχος από το χρήστη/Προστασία από υφαρπαγή** : Καθώς ο χρήστης είναι ο μόνος που έχει τη 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 ή να υφαρπαχτούν από τρίτους (εφόσον η κρυπτογράφηση δεν παραβιαστεί). Περαιτέρω προβλέψεις επιτρέπουν την δυνατότητα μεταφοράς τους μόνο υπό πολύ ορισμένες συνθήκες, όπως μόνο από ορισμένα προσυμφωνημένα μέρη ταυτόχρονα για την αποφυγή μονομερών εκθέσεων ή μόνο μετά από συγκεκριμένο χρόνο.

✓ **Φορητότητα/αντίγραφα ασφαλείας** : Ανεξάρτητα από το πλήθος τους, τα bitcoins και τα «πορτοφόλια» αποθήκευσης ή οι κωδικού πρόσβασης σε αυτά είναι ουσιαστικά πάρα πολύ μικρά σε μέγεθος, και μπορούν να μεταφερθούν εύκολα, να καταγραφούν σε χαρτί, ακόμα και να απομνημονευτούν. Επίσης, κάτι αδύνατο για συμβατικές αξίες, μπορούν να αντιγραφούν ώστε να υπάρχουν αντίγραφα ασφαλείας σε περίπτωση καταστροφής των αρχικών. Βέβαια αν παραβιαστεί οποιοδήποτε από τα αντίγραφα, τα υπόλοιπα είναι επίσης παραβιασμένα.

✓ **Διαφάνεια Συναλλαγών/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 δεν θα το αποδέχονταν.

✓ **Συναινετική Φύση χρήσης/αλλαγών** : Η αλλαγή οιουδήποτε χαρακτηριστικού του λογισμικού ή των κανόνων του, έχει ουσιαστικά εφαρμογή μόνο όταν τις δεχτεί η κοινότητα που απαρτίζει το δίκτυο. Με αυτό 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. Αντίστοιχου βεληνεκούς επιτυχημένα εγχειρήματα ανοιχτού λογισμικού αποτελούν το Linux όπως και το Bit torrent.

✓ **Αποκεντρωμένη Φύση** : Ένα από τα πιο σημαντικά χαρακτηριστικά του δικτύου, είναι η αποκεντρωμένη φύση του, που 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 είναι να αποκοπούν όλοι οι υπολογιστές του δικτύου μεταξύ τους, με δυο λόγια να κοπεί το διαδίκτυο σε όλο τον πλανήτη, κάτι που είναι πέρα από τις δυνάμεις οιουδήποτε στην παρούσα. 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.

✓ **Υποδιαιρέσεις** : Κάθε bitcoin είναι υποδιαιρέσιμο έως 8 δεκαδικά ψηφία (έως 0,00000001), επιτρέποντας μικρο-συναλλαγές που δεν είναι δυνατές με άλλα μέσα ή συμβατικά νομίσματα. Η προσθήκη περισσότερων ακόμα δεκαδικών επαφίεται στην συναίνεση του δικτύου αν αυτό χρειαστεί στο μέλλον.

✓ **Μη αντιστρέψιμη φύση** : Όλες οι συναλλαγές με bitcoin είναι τελικές και μη αντιστρέψιμες. Αυτό έχει το επιπλέον πλεονέκτημα προς όσους διαθέτουν προϊόντα για bitcoin ότι δεν είναι δυνατόν να ανακληθούν συναλλαγές όπως πχ 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. Από την άλλη, οι χρήστες που εκτελούν αγορές με bitcoin 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.

✓ **Ιδιωτικότητα συναλλαγών** : Κάθε χρήστης μπορεί να δημιουργήσει, μέσω του λογισμικού, σχεδόν απεριόριστο αριθμό διευθύνσεων μέσω τον 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 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, για πάντα[17].

3.6 Μεταβλητότητα, κίνδυνοι και αρνητικές πτυχές

Επιγραμματικά, παρακάτω αναφέρονται τα βασικά μειονεκτήματα του Bitcoin.

- ✓ Η μεταβλητότητα μειώνει το κίνητρο για τη χρήση του
- ✓ Οι συναλλαγές κάνουν 50 λεπτά να πραγματοποιηθούν
- ✓ Η νομική του υπόσταση είναι ακόμη απροσδιόριστη
- ✓ Έχει μεγάλη διακύμανση η ισοτιμία του, μπορεί να χάσει εύκολα την αξία του
- ✓ Συνδέεται με αδιαφανείς-παράνομες συναλλαγές
- ✓ Όλες οι συναλλαγές είναι 100% μη αναστρέψιμες
- ✓ Απαιτεί τεχνολογική εξοικείωση

[17] http://en.wikipedia.org/wiki/Bitcoin

Πιο αναλυτικά:

- Το Bitcoin δεν είναι ένα πραγματικό peer to peer νόμισμα, αλλά οδηγεί και σε πιο ακραία ανισότητα

Μερικές φορές υποστηρίζεται ότι το Bitcoin είναι ένα peer to peer (ομότιμο) νόμισμα, επειδή κάθε υπολογιστής με το λογισμικό εξόρυξης μπορεί να δημιουργήσει το νόμισμα, αλλά δεν έχει ο καθένας μας πρόσβαση στον ίδιο αριθμό ηλεκτρονικών υπολογιστών και δεν έχει ο καθένας μας υπολογιστές, ως εκ τούτου, ο σχεδιασμός του Bitcoin, ο οποίος ευνοεί τους πρώιμα νεοεισερχόμενους και όσους επενδύουν σε δύναμη (υπολογιστές και τεχνολογία), είναι μια μηχανή ανισότητας.

Ο συντελεστής Gini του Bitcoin (ένα μέτρο/δείκτης καθορισμού της ανισότητας, γνωστός και ως Gini index ή Gini ratio[18]), είναι ένα επιβλητικό 0,87709 και σύμφωνα με το Bitcoinica[19], το 1% από το σύνολο των παικτών κατέχουν το 50% των bitcoins. Αυτή η ανισότητα δεν μειώνεται, αλλά αυξάνεται: σύμφωνα με το Bitcoin Trader[20], για μια δεδομένη περίοδο, "το top 100 των κατόχων του έχουν περάσει από το να κατέχουν συνολικά 1.776.434 bitcoin στο να κατέχουν 2.254.634 bitcoin, μια επιβλητική αύξηση κατά 27%!", και η ικανότητα εξόρυξης επίσης έχει ήδη ξεκινήσει να συγκεντρώνεται και αυτή, ειδικά μετά την κυκλοφορία στην αγορά των μηχανημάτων ASIC Miners[21] και με τις φάρμες μαζικής εξόρυξης του Bitcoin.

- Το Bitcoin δεν μπορεί να μας οδηγήσει από μόνο του σε μια "αποδιαμεσολαβημένη" κοινωνία.

Ζούμε σε μια εποχή τεχνο-ουτοπισμού με μια έντονη τάση για τεχνοκρατισμό. Το πρώτο σημαίνει ότι, πολλοί πιστεύουν πως η τεχνολογία από μόνη της καθορίζει συγκεκριμένα αποτελέσματα, ενώ στο δεύτερο θεωρούν ότι είναι θετικό το γεγονός

[18] https://en.wikipedia.org/wiki/Gini_coefficient
[19] https://en.bitcoin.it/wiki/Bitcoinica
[20] https://bitcoin-trader.biz/
[21] Bitcoin Mining Hardware http://www.bitcoinx.com/bitcoin-mining-hardware/

ότι οι ατελείς διεργασίες της ανθρώπινης φύσης αντικαθίστανται από "καθαρές" τεχνολογικές διαδικασίες. Και οι δύο αυτές τάσεις είναι πολύ επικίνδυνες.

Πρώτον, οι διαμοιραζόμενες τεχνολογίες δεν οδηγούν κατ' ανάγκη και σε διαμοιραζόμενα αποτελέσματα. Το έχουμε δει αυτό ιστορικά με την επίδραση της εφεύρεσης της τυπογραφίας, η οποία οδήγησε σε έναν εκδημοκρατισμό της γνώσης και της παιδείας, αλλά και με την πάροδο του χρόνου αντικατέστησε την τοπική αυτονομία των ελεύθερων μεσαιωνικών πόλεων με αυτή των πολύ πιο ισχυρών και ελεγχόμενων εθνών-κρατών, δηλαδή με περισσότερο πολιτικό συγκεντρωτισμό, όχι με λιγότερο.

Τα δίκτυα τα οποία δεν έχουν αντι-μέτρα για τη διατήρηση της ισότητας οδηγούνται αναπόφευκτα με την πάροδο του χρόνου για μια νέα συγκέντρωση των πόρων. Ως εκ τούτου, το Amazon και το iTunes, τα λεγόμενα και ως η μακριά ουρά της κατανάλωσης του πολιτισμού (long tail of culture consumption), όπως προέβλεψε ο Chris Anderson[22] δεν είναι πλέον λειτουργικά, και στο p2p κοινωνικό δανεισμό (Peer-to-peer lending [23]), το 80% των δανείων που παρέχονται είναι από μεγάλες τράπεζες και θεσμικά όργανα, οι ίδιες εκείνες δυνάμεις που υποτίθεται πως η τεχνολογία θα τις αναγκάσει να αποδιαμεσολαβηστούν.

Ξανά και ξανά, βλέπουμε ότι η ενδεχόμενη κατάργηση των μεσαζόντων της εξουσίας, η οποία μπορεί να επηρεάσει τις καθιερωμένες αρμοδιότητες, δημιουργεί νέους μεσάζοντες, όπως οι μονοπωλιακές πλατφόρμες. Οι τεχνολογίες είναι εκείνες που πράγματι, καθώς χρησιμοποιούνται από τις κοινωνικές δυνάμεις, στρεβλώνουν τις τεχνολογίες για τις δικές τους ανάγκες.

Η ανισότητα στην ιδιοκτησία των Bitcoin αναπόφευκτα θα επηρεάσει περαιτέρω τις δομές που κάνουν το ίδιο το Bitcoin λειτουργικό, οδηγώντας το σε νέα είδη και μορφές μονοπωλίων. Οι τεχνολογίες είναι πάντα εμποτισμένες με τις

[22] http://www.longtail.com/about.html
[23] https://en.wikipedia.org/wiki/Peer-to-peer_lending

ανθρώπινες αξίες, κανένας προγραμματισμός ή υποδομή δεν είναι πραγματικά ουδέτερη από αυτή την άποψη.

- Το Bitcoin χρηματοδοτεί μια επικίνδυνη ιδεολογία

Ο σχεδιασμός του Bitcoin είναι αναρχο-καπιταλιστικός, δηλαδή έχει σχεδιαστεί για να ευνοήσει την ελευθερία των ιδιοκτητών του και όσο πιο πολλά έχει κάποιος στην κατοχή του, τόσο πιο "ελευθεριακός" είναι.

Η αποτίμηση του Bitcoin σημαίνει μια σημαντική μεταφορά του κοινωνικού πλούτου σε αυτή την πολιτική τάση, η οποία συμμάχησε με τα κεφάλαια επιχειρηματικού κινδύνου και με τις ολιγαρχίες που επενδύουν σε Bitcoin, αλλοιώνοντας την ισορροπία της εξουσίας.

Οι πρόωροι ελευθεριακοί επενδυτές του Bitcoin, μπορούν να πωλούν τα Bitcoin τους με ένα ασφάλιστρο για τους νεοεισερχόμενους, συλλαμβάνοντας έτσι την ουσιαστική κερδοσκοπική αξία.

Έτσι, ενώ ο ισχυρισμός ότι το Bitcoin είναι μια πυραμίδα είναι προφανώς ψευδές, τείνει όμως να καθιερώσει ένα ενοίκιο-αντίτιμο που καταβάλλεται από τους νεοεισερχόμενους στους υπάρχοντες ιδιοκτήτες. Με αυτή την έννοια, το Bitcoin, μακριά από το να είναι ένα εργαλείο της κατανεμημένης ισότητας, η οποία αποτελεί ήδη έναν ψεύτικο εμπειρικό ισχυρισμό επί του παρόντος, είναι ένα ιδανικό εργαλείο για την ανάπτυξη των υπερ-καπιταλιστικών οικονομικών μοντέλων. Με αυτή την έννοια, το Bitcoin είναι ένα ιδανικό εργαλείο για τον δικτυοκρατικό καπιταλισμό, τις ιεραρχίες που ενεργοποιούν, αλλά και που ελέγχουν τα δίκτυα και που συλλαμβάνουν (απομυζούν ουσιαστικά) αξία από αυτά.

3.7 Οικονομικές τεχνικές και νομικές όψεις του bitcoin

Στην Ελλάδα δεν υφίσταται κανένα απολύτως ειδικό ρυθμιστικό πλαίσιο των αγορών Bitcoins. Δεν έχουν εκφέρει καμία άποψη τόσο οι αρμόδιες ελληνικές αρχές (Τράπεζα της Ελλάδος, Επιτροπή Κεφαλαιαγοράς), όσο και οι αντίστοιχες ευρωπαϊκές πέραν της προαναφερθείσας προειδοποίησης της Ευρωπαϊκής Αρχής Τραπεζών. Συνεπώς, θα πρέπει να εξεταστεί η υπαγωγή τους στο ισχύον νομοθετικό πλαίσιο. Ο ν. 3606/07, ο οποίος ενσωμάτωσε στην εσωτερική έννομη τάξη την οδηγία 2004/39/ΕΚ (MiFID), ρυθμίζει εκτενώς τις αγορές χρηματοπιστωτικών μέσων.

Ορίζει επακριβώς τα ρυθμιζόμενα πρόσωπα, αλλά και τις κατηγορίες των χρηματοπιστωτικών μέσων. Σύμφωνα λοιπόν με το άρθρο 3 ν. 3606/07 στο πεδίο εφαρμογής του νόμου εμπίπτουν οι Ανώνυμες Εταιρείες Παροχής Επενδυτικών Υπηρεσιών (ΑΕΠΕΥ), οι Ανώνυμες Εταιρίες Επενδυτικής Διαμεσολάβησης (ΑΕΕΔ), τα πιστωτικά ιδρύματα, εφόσον παρέχουν επενδυτικές υπηρεσίες, καθώς και οι Ανώνυμες Εταιρείες Διαχείρισης Αμοιβαίων Κεφαλαίων (ΑΕΔΑΚ). Σύμφωνα δε με το άρθρο 8 απαγορεύεται η παροχή επενδυτικών υπηρεσιών και η άσκηση επενδυτικών δραστηριοτήτων σε οποιοδήποτε άλλο πρόσωπο, πέραν των ανωτέρω, με μοναδική εξαίρεση τις ΕΠΕΥ που έχουν λάβει άδεια λειτουργίας και εποπτεύονται από την αρμόδια αρχή άλλου κράτους – μέλους της Ευρωπαϊκής Κοινότητας. Συνεπώς αν το Bitcoin είναι χρηματοπιστωτικό μέσο, απαγορεύεται η εκτέλεση των δραστηριοτήτων της παραγράφου 4, μεταξύ των οποίων η λήψη και διαβίβαση εντολών, για κατάρτιση συναλλαγών σε Bitcoins, η εκτέλεση εντολών, η οποία συνίσταται στην κατάρτιση συμβάσεων αγοράς ή πώλησης Bitcoins ή η φύλαξη και διοικητική διαχείριση Bitcoins για λογαριασμό πελατών.

Αυτό σημαίνει απλά, ότι οποιαδήποτε ηλεκτρονική πλατφόρμα ανταλλαγής ή απόθεσης Bitcoins, που λειτουργεί στην Ελλάδα θα ήταν παράνομη αν δεν διέθετε μορφή ΑΕΠΕΥ, ΑΕΕΔ ή πιστωτικού ιδρύματος, ώστε να εποπτεύεται από την Επιτροπή Κεφαλαιαγοράς και να ισχύουν οι προστατευτικές για τον επενδυτή

διατάξεις του ν. 3606/07. Όμως αν αναχθούμε στους ορισμούς των χρηματοπιστωτικών μέσων, κάτι τέτοιο φαίνεται εξαιρετικά δύσκολο να θεμελιωθεί. Διότι κατά το νόμο στα χρηματοπιστωτικά μέσα εμπίπτουν μεν οι κινητές αξίες και τα μέσα χρηματαγοράς, όμως ρητώς εξαιρούνται τα μέσα πληρωμών. Αν αναγνωριστεί στο Bitcoin ο χαρακτήρας του μέσου πληρωμών, σαφώς εκφεύγει του ν. 3606/07. Από την άλλη ακόμη και αν χαρακτηριστεί ως κινητή αξία, αυτή θα πρέπει να είναι δεκτική διαπραγμάτευσης στην κεφαλαιαγορά, δηλαδή «ένα πολυμερές σύστημα, το οποίο λειτουργεί υπό τη διεύθυνση διαχειριστή αγοράς και επιτρέπει ή διευκολύνει την προσέγγιση περισσοτέρων συμφερόντων τρίτων προσώπων, τα οποία κατευθύνονται στην αγοραπωλησία χρηματοπιστωτικών μέσων». Δεδομένης της προαναλυθείσας αρχιτεκτονικής των αγορών Bitcoins φαντάζει δύσκολη η υπαγωγή τους στην έννοια της «οργανωμένης αγοράς».

Ως προς τις προληπτικές εποπτικές διατάξεις του τραπεζικού δικαίου και συγκεκριμένα το ν. 3601/07 είναι σαφές ότι οι πλατφόρμες ανταλλαγής Bitcoins δεν είναι πιστωτικά ιδρύματα, υπό την έννοια της αποδοχής καταθέσεων ή άλλων επιστρεπτέων κεφαλαίων από το κοινό και της χορήγησης δανείων ή λοιπών πιστώσεων. Όμως, εξεταστέο είναι το ζήτημα της υπαγωγής τους στην έννοια των ιδρυμάτων ηλεκτρονικού χρήματος σύμφωνα με το ν. 4021/2011, ώστε να υπάρχουν προϋποθέσεις για την παροχή άδειας ίδρυσης και λειτουργίας, καθώς και κανόνες εποπτείας που διέπουν τη λειτουργία τους. Ως ίδρυμα ηλεκτρονικού χρήματος ορίζεται «επιχείρηση, εκτός του πιστωτικού ιδρύματος της περίπτωσης α΄ της παραγράφου 1 του άρθρου 2 ν. 3601/07, η οποία εκδίδει μέσα πληρωμής υπό μορφή ηλεκτρονικού χρήματος». Ηλεκτρονικό χρήμα είναι «νομισματική αξία, η οποία αντιστοιχεί σε απαίτηση έναντι του εκδότη και η οποία επιπλέον είναι αποθηκευμένη σε ηλεκτρονικό υπόθεμα, έχει εκδοθεί κατόπιν παραλαβής χρηματικού ποσού, και γίνεται δεκτή ως μέσο πληρωμής από επιχειρήσεις άλλες, εκτός από την εκδότρια». Εν προκειμένω, τα Bitcoins φαίνεται να εκδίδονται από τους τηρούντες τα block chains, αυτούς δηλαδή που καταγράφουν τις συναλλαγές και συνήθως εμπλέκονται και στην ανταλλαγή τους. Στην πραγματικότητα όμως δεν τα εκδίδουν αυτοί, αλλά το ίδιο το νομισματικό σύστημα, το δίκτυο, το οποίο δεν

ανήκει σε κανένα πρόσωπο. Το πρώτον τα Bitcoins δημιουργούνται από το δίκτυο ως σύνολο και καταβάλλονται στους καταχωρητές ως αμοιβή. Ενδεικτικό είναι το γεγονός ότι δεν ελέγχουν καν τη διαδικασία δημιουργίας νέων Bitcoins, όπως ο μεταλλωρύχος δεν δημιουργεί το πολύτιμο μέταλλο. Πέραν τούτου δεν προκύπτει ευχερώς και η προϋπόθεση της ύπαρξης απαίτησης έναντι του εκδότη του Bitcoin, ακόμη και αν θεωρήσουμε ως τέτοιους τους miners.

Όπως είναι λογικό το θεσμικό πλαίσιο ήταν αδύνατον να προβλέψει ρυθμίσεις για ένα τόσο καινοτόμο σύστημα πληρωμών - κινητών αξιών. Έτσι η «εξόρυξη» και ανταλλαγή ή και οποιασδήποτε άλλης μορφής επαγγελματική συναλλαγή Bitcoins στην Ελλάδα διαφεύγει του ελέγχου των θεσμικών εποπτών του χρηματοπιστωτικού συστήματος. Σε κάθε ανταλλαγή ή απόθεση κρυπτονομισμάτων ελλοχεύουν κίνδυνοι παρόμοιοι με τη διενέργεια μιας συναλλαγής στο δρόμο. Κανείς δεν ελέγχει τον αντισυμβαλλόμενο, δεν πληροί κάποια προϋπόθεση για να τελεί επαγγελματικά τέτοιες συναλλαγές, ούτε εγγυάται κανείς τις συναλλαγές αυτές.

Το Bitcoin, πολλώ δε μάλλον τα λοιπά ψηφιακά νομίσματα, αποκλείονται από το πεδίο του εν στενή έννοια χρήματος ή νομίσματος ήδη από τη νομοθετική επιταγή. Δεν εμπίπτει μάλιστα ούτε στον κατά το ν. 3601/07 και την οδηγία 2009/110/ΕΚ, ορισμό του ηλεκτρονικού χρήματος (οιαδήποτε αποθηκευμένη σε ηλεκτρονικό, μεταξύ άλλων και μαγνητικό υπόθεμα νομισματική αξία αντιπροσωπευόμενη από απαίτηση έναντι του εκδότη ηλεκτρονικού χρήματος, έχει εκδοθεί κατόπιν παραλαβής χρηματικού ποσού για τον σκοπό της πραγματοποίησης πράξεων πληρωμών όπως ορίζονται στο άρθρο 4 σημείο 5) της οδηγίας 2007/64/ΕΚ και η οποία γίνεται δεκτή από άλλα φυσικά ή νομικά πρόσωπα πέραν του εκδότη). Διότι το ηλεκτρονικό χρήμα είναι απλά ένα μέσο αποϋλοποίησης και ηλεκτρονικής αποθήκευσης, του νομίμου χρήματος. Δεν αποτελεί καθ' αυτό μέσο συναλλαγών. Τα συναλλασσόμενα με ηλεκτρονικό χρήμα μέρη, ως μέσο ανταλλαγής εξακολουθούν να χρησιμοποιούν την ενσωματωμένη στο ηλεκτρονικό υπόθεμα νομισματική αξία, το νόμιμο χρήμα. Αντίθετα, το Bitcoin συμπεριφέρεται αυτοτελώς ως νόμισμα, δεν ενσωματώνει συγκεκριμένη

νομισματική αξία για να την αποθηκεύσει ή να τη μεταφέρει. Η αρχική νομισματική αξία μετατρέπεται σε άλλη νομισματική αξία, η οποία υπόκειται στις δυνάμεις τις αγοράς, όπως κάθε άλλο νόμισμα.

Το νομικό μας σύστημα μάλλον ανακαλύπτει τα όριά του, υπό την πίεση της τεχνολογικής καινοτομίας, αν και οι γενικές ρήτρες του αστικού δικαίου είναι ακόμη ικανές να προσδώσουν την αναγκαία ρυθμιστική ζωντάνια. Παρουσιάζεται όμως εν γένει η ανάγκη κατανόησης των επερχόμενων νέων, αν και ακόμη υπό διαμόρφωση, ηλεκτρονικών συστημάτων πληρωμών και χρηματοοικονομικών συναλλαγών, με σκοπό την απαραίτητη για τη σταθερότητά τους δικαιϊκή ρύθμιση. Μόνο υπό καθεστώς ασφάλειας δικαίου είναι δυνατόν τα συστήματα αυτά να αποκτήσουν τόση πίστη από τους συναλλασσόμενους, ώστε ωριμάσουν και να γνωρίσουν μια γενική ανάπτυξη. Από την άλλη μεριά μονάχα η ευρεία διάδοσή τους στις συναλλαγές μπορεί να δημιουργήσει την απαραίτητη πίεση για να τραβήξουν την προσοχή του νομοθέτη. Το μόνο σίγουρο είναι ότι η φιλοσοφία της λειτουργίας των ψηφιακών νομισμάτων δεν μπορεί να οπισθοδρομήσει και στο άμεσο μέλλον τα παραδοσιακά νομισματικά συστήματα θα αναγκαστούν τουλάχιστον να συμβιώσουν με αυτά[24] [25].

[24] http://www.viannatsis.gr/download/bitcoin%20gr.pdf
[25] http://coindesk.com/goldman-sachs-bitoin-isnt-currency-underlying-tech-holds-promise

4 Δημιουργία των Bitcoins

Κάθε συναλλαγή που γίνεται στο δίκτυο του Bitcoin, ελέγχεται για την εγκυρότητά της και στη συνέχεια τοποθετείται μέσα σ" ένα block μαζί με άλλες συναλλαγές που έχουν ελεγθεί. Κάθε δέκα λεπτά περίπου, δημιουργείται και ένα νέο block για να φιλοξενήσει αυτές τις συναλλαγές, το οποίο σχετίζεται με το αμέσως προηγούμενο αλλά κι όλα τα υπόλοιπα blocks που έχουν δημιουργηθεί πριν από αυτό, σχηματίζοντας έτσι την αλυσίδα των μπλοκ (block chain). Ένας μαθηματικός αλγόριθμος χρησιμοποιείται για να γίνει ο συσχετισμός του νέου block με τα προηγούμενα. Μόλις βρεθεί η λύση του αλγόριθμου τότε θα δημιουργηθεί το νέο block και μαζί με αυτό δημιουργηθεί κι ένας συγκεκριμένος αριθμός νέων bitcoins, τα οποία θα αποδοθούν σε αυτόν ή αυτούς που βρήκαν τη λύση. Αυτή η διαδικασία ονομάζεται Mining κι έχει πάρει το όνομά της ως μια σύγχρονη αναπαράσταση των χρυσωρύχων του περασμένου αιώνα.

Για να μπορεί η λύση του αλγόριθμου (γρίφου) να προκύπτει κάθε δέκα λεπτά περίπου, ανεξάρτητα από το πόσοι χρήστες προσπαθούν ταυτόχρονα να τη βρουν, είναι προφανές πως θα πρέπει να τροποποιηθεί η δυσκολία του γρίφου. Αυτό γίνεται αυτόματα από το δίκτυο σε σχέση με το πόσοι χρήστες προσπαθούν να βρουν τη λύση. Συνεπώς, όσο περισσότεροι χρήστες προσπαθούν να λύσουν το γρίφο (δηλαδή όσο μεγαλύτερη επεξεργαστική ισχύ), τόσο μεγαλώνει η δυσκολία του κι αντίστροφα. Κάθε ηλεκτρονικός υπολογιστής ή συσκευή που αναζητά τη λύση του γρίφου, συμμετέχει παράλληλα και στην προστασία του δικτύου από επιθέσεις καθώς και στον έλεγχο και προώθηση των συναλλαγών στο δίκτυο, όπως αναφέρθηκε και παραπάνω[26].

4.1 Η αλυσίδα των μπλοκ (Block chain)

Μια αλυσίδα μπλοκ είναι μια βάση δεδομένων συναλλαγών, η οποία είναι κοινόχρηστη σε όλους τους κόμβους που συμμετέχουν σε ένα σύστημα με βάση το

[26] http://bitcoinx.gr/

πρωτόκολλο BitCoins. Ένα πλήρες αντίγραφο της αλυσίδας μπλοκ του νομίσματος περιέχει κάθε συναλλαγή που εκτελούνται στο νόμισμα. Με αυτές τις πληροφορίες, μπορεί κανείς να ανακαλύψει πόση αξία ανήκε σε κάθε διεύθυνση σε οποιοδήποτε σημείο στην ιστορία.

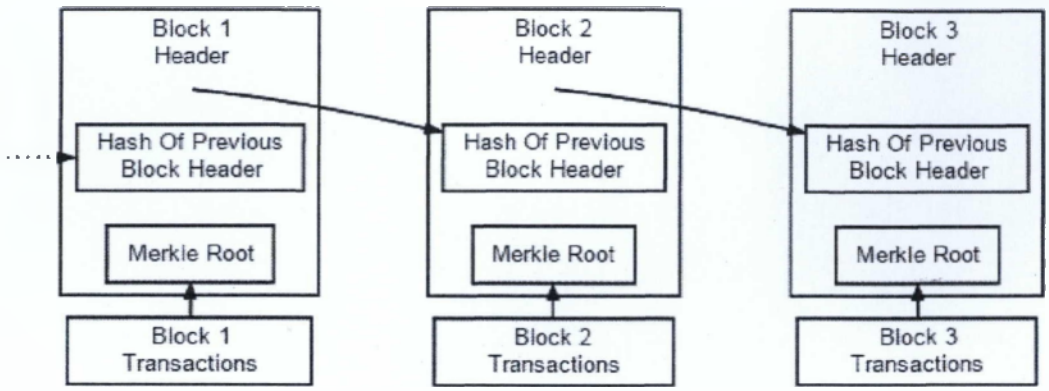
Κάθε μπλοκ περιέχει ένα " κατακερματισμένο μείγμα" του προηγούμενου μπλοκ. Αυτό έχει ως αποτέλεσμα τη δημιουργία μιας αλυσίδας από μπλοκ από το εναρκτήριο μπλοκ μέχρι το τρέχον. Κάθε μπλοκ εγγυάται ότι θα έρθει χρονολογικά μετά από προηγούμενο επειδή διαφορετικά ο κατακερματισμός του προηγούμενου δεν θα γίνει σωστά. Επίσης, κάθε μπλοκ είναι υπολογιστικά ανέφικτο να τροποποιήσει την στιγμή που υπήρξε στην αλυσίδα για λίγο επειδή κάθε μπλοκ μετά θα πρέπει επίσης να αναγεννηθεί. Η αλυσίδα μπλοκ είναι η κύρια καινοτομία του Bitcoin[27].

Η αλυσίδα μπλοκ παρέχει δημόσιο καθολικό ημερολόγιο συναλλαγών, το οποίο διαθέτει ταξινομημένη και χρονικά – χωρισμένη καταγραφή των συναλλαγών. Αυτό το σύστημα χρησιμοποιείται για την προστασία κατά της διπλό - εγγραφών και τροποποίηση των προηγούμενων αρχείων συναλλαγών.

Κάθε πλήρης κόμβος στο δίκτυο Bitcoin αποθηκεύει ανεξάρτητα μια αλυσίδα μπλοκ περιέχει μόνο επικυρωμένα μπλοκ από αυτόν τον κόμβο. Όταν πολλά κόμβοι έχουν όλα τα ίδια μπλοκ στην αλυσίδα τους, θεωρούνται να είναι σε συναίνεση. Οι κανόνες επικύρωσης αυτών των κόμβων, οι οποίοι διατηρούν τη συναίνεση ονομάζονται κανόνες συναίνεσης.

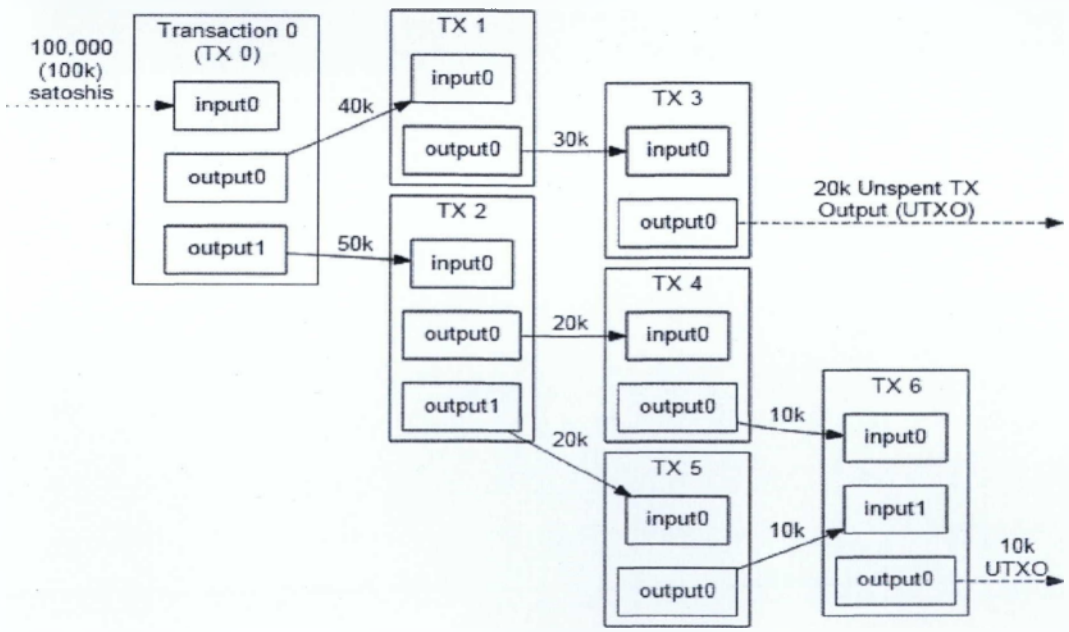
Η παρακάτω εικόνα δείχνει μια απλοποιημένη εκδοχή μιας αλυσίδας μπλοκ. Ένα μπλοκ από μία ή περισσότερες νέες συναλλαγές συλλέγεται μέσα στο τμήμα δεδομένων συναλλαγής ενός μπλοκ.

[27] https://en.bitcoin.it/wiki/Block_Chain



Εικόνα 15. Απλοποιημένη εκδοχή μιας αλυσίδας μπλοκ

Συναλλαγές επίσης συνδέονται μεταξύ τους. Το λογισμικό του πορτοφολιού BitCoins δίνει την εντύπωση ότι τα Satoshis[28] αποστέλλονται από και προς τα πορτοφόλια, αλλά τα bitcoins πραγματικά κινούνται από συναλλαγή σε συναλλαγή. Κάθε συναλλαγή ξοδεύει τα Satoshis που εισπράχτηκαν προηγουμένως από μία ή περισσότερες προηγούμενες συναλλαγές έτσι ώστε η είσοδος μιας συναλλαγής είναι η έξοδος μιας προηγούμενης[29].



Εικόνα 16.Πληρωμή Συναλλαγή με Συναλλαγή (Χρησιμοποιείται στα BitCoins)

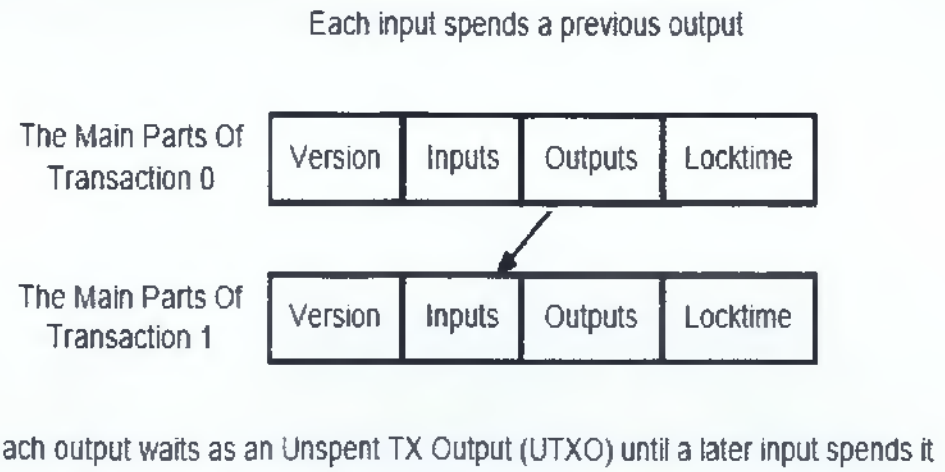
[28] είναι το μικρότερο κλάσμα του Bitcoin που μπορεί σήμερα να αποσταλεί: 0.00000001 BTC
[29] https://bitcoin.org/en/developer-guide#block-chain-overview

4.1.1 Μέγεθος μπλοκ

Όπως έχουμε εξηγήσει, η αλυσίδα των μπλοκ είναι η ραχοκοκαλιά του Bitcoin. Κάθε νέο μπλοκ που δημιουργείται, περιέχει κάποιες ή όλες τις πρόσφατες συναλλαγές που ελέχθησαν για την ορθότητά τους και βρέθηκαν σωστές. Τί μέγεθος όμως έχει ένα μπλοκ και πόσες συναλλαγές μπορεί να περιέχει; Το μέγεθος κάθε μπλοκ έχει προσδιοριστεί στο 1 MegaByte[30]. Το πλήθος των συναλλαγών που μπορούν να «στριμωχτούν» μέσα σε αυτό το 1MB εξαρτάται από το μέγεθος της κάθε συναλλαγής. Να σημειώσουμε ότι όταν αναφερόμαστε στο μέγεθος της συναλλαγής, δεν εννοούμε το αριθμητικό ποσό των Bitcoin που μεταφέρονται.

4.2 Συναλλαγές

Οι συναλλαγές επιτρέπουν στους χρήστες να ξοδεύουν Satoshis. Κάθε συναλλαγή είναι δομημένη από διάφορα μέρη τα οποία επιτρέπουν τόσο απλές άμεσες πληρωμές και περίπλοκες συναλλαγές. Σε αυτή την ενότητα θα περιγράψουμε λεπτομερώς κάθε μέρος και να δείξουμε πώς να τα χρησιμοποιούν από κοινού ώστε να δημιουργηθούν πλήρεις συναλλαγές.

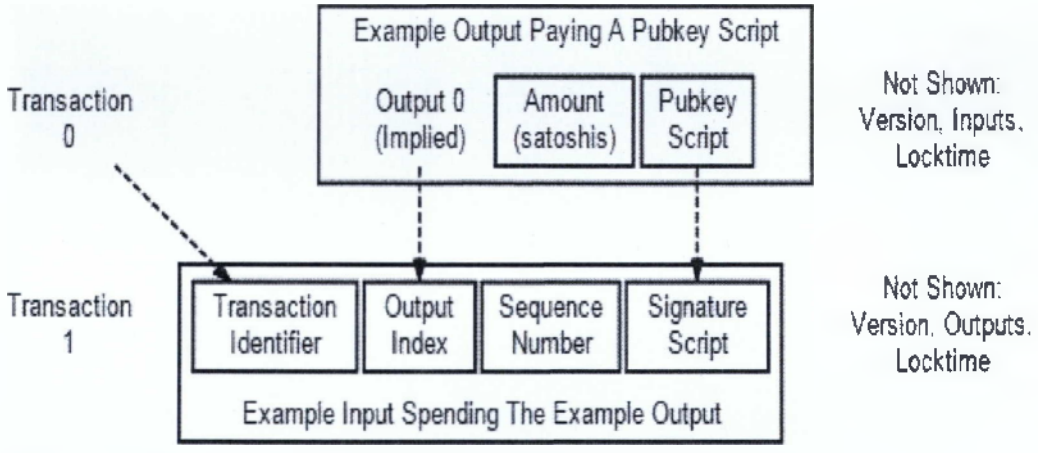


Εικόνα 17.Τα κύρια μέρη μιας συναλλαγής Bitcoin

[30] http://en.wikipedia.org/wiki/Megabyte

Το παραπάνω σχήμα δείχνει τα κύρια μέρη μιας συναλλαγής Bitcoin. Κάθε συναλλαγή έχει τουλάχιστον μία είσοδο και μία έξοδο. Κάθε είσοδος ξοδεύει τα satoshis που καταβάλλεται σε προηγούμενη έξοδο. Κάθε είσοδος καταναλώνει τα satoshis που συγκεντρώνει η προηγούμενη έξοδος. Κάθε έξοδος λειτουργία ως μια έξοδο – μη χρησιμοποιούμενων δαπανών (UTXO) - έως ότου να τα δαπανήσει η μεταγενέστερη είσοδος. Όταν το Bitcoin πορτοφόλι σας λέει ότι έχετε 10.000 Satoshi, αυτό σημαίνει πραγματικά ότι έχετε 10.000 satoshis αναμονής σε ένα ή περισσότερα UTXOs.

Κάθε συναλλαγή έχει πρόθεμα έναν αριθμό έκδοσης συναλλαγής τεσσάρων bytes, ο οποίος ορίζει, αφενός τον αριθμό των ομότιμων και "σκαπανέων" του bitcoin και αφετέρου τους κανόνες της χρήσης και της επικύρωσης του. Αυτό επιτρέπει στους προγραμματιστές να δημιουργήσουν νέους κανόνες για τις μελλοντικές συναλλαγές χωρίς να ακυρώνουν προηγούμενες συναλλαγές.



Εικόνα 18.Σύνοψη των συναλλαγών

Για να γίνει πιο αντιληπτό πως πραγματοποιείται μια συναλλαγή μέσω bitcoin, πρέπει να φέρουμε ένα παράδειγμα, περιγράφοντας αναλυτικά όλα τα στάδια της συναλλαγής. Στην εικόνα 20 φαίνεται αναλυτικά, η συναλλαγή μέσω bitcoin.

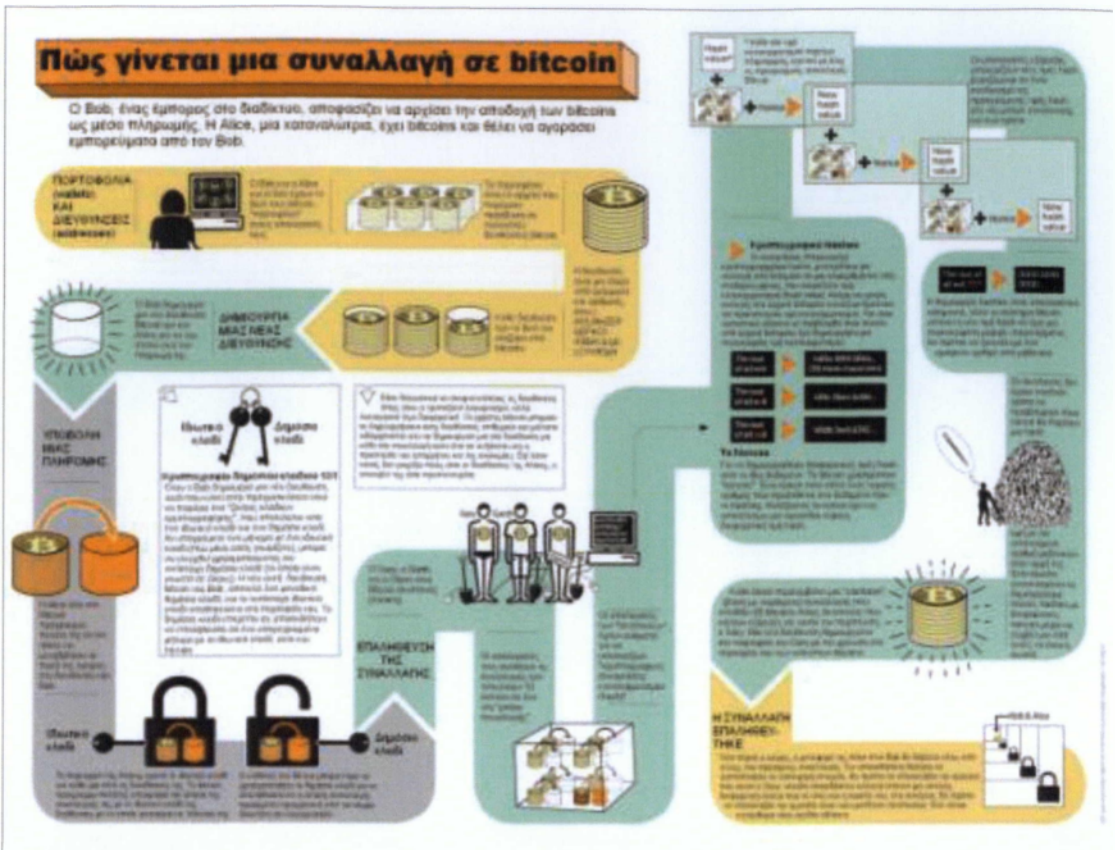
πληρωμής, η Alice λέει στο BitCoin πρόγραμμα – πελάτη της ότι θέλει να μεταβιβάσει το ποσό της αγοράς στην διεύθυνση του Bob. Ωστόσο, για να γίνει αυτό πρέπει να γίνει επαλήθευση της συναλλαγής. Αυτό γίνεται με χρήση του ιδιωτικού και δημοσίου κλειδιού.

Κατά την επαλήθευση και παραγωγή των Bitcoins έχουμε τα παρακάτω στάδια: Αρχικά επιστρατεύονται οι «σκαπανείς» για την παραγωγή των BitCoins και οι υπολογιστές τους συνδέουν τις συναλλαγές των τελευταίων 10 λεπτών σε ένα μπλοκ συναλλαγής (Block Chain). Επίσης, οι υπολογιστές των «σκαπανέων» έχουν ρυθμιστεί ώστε να υπολογίζουν «κρυπτογραφικές συναρτήσεις κατακερματισμού (Hash)».

Οι συναρτήσεις (παραγωγής) κρυπτογραφημένων hashs μετατρέπουν μια συλλογή από δεδομένα σε μια αλφαριθμητική λέξη σταθερού μήκους, που ονομάζεται τιμή κατακερματισμού (Hash Value). Στην συνέχεια δημιουργούνται τα nonces. Τα nonces είναι απλά ένας τυχαίος αριθμός που προστίθεται στα δεδομένα πριν το hashing. Αλλάζοντας το nonce έχει ως αποτέλεσμα να προκύψει μια τεράστια εύρους διαφορετική τιμή hash.

Στην συνέχεια, οι υπολογιστές εξόρυξης υπολογίζουν νέες τιμές hash, βασισμένοι σε έναν συνδυασμό της προηγούμενης τιμής hash, του νέο μπλοκ συναλλαγής και του νέου nonce. Όλη αυτή η διαδικασία έχει ως αποτέλεσμα την παραγωγή μιας βάση νομισμάτων που αποδίδει 50 bitcoins στους σκαπανείς που κάνουν την εξόρυξη. Έτσι, μια νέα διεύθυνση δημιουργείται στο πορτοφόλι του Gary (ένας από τους σκαπανείς) με την χρέωση στο πορτοφόλι του των νεόκοπων bitcoins.

Κατά την ολοκλήρωση – επαλήθευση της συναλλαγής, η μεταφορά της Alice στον Bob θα θάβεται κάτω από άλλες, πιο πρόσφατες συναλλαγές. Για οποιονδήποτε θελήσει να τροποποιήσει τα λεπτομερή στοιχεία, θα πρέπει να επαναλάβει την προηγούμενη εργασία - επειδή οποιαδήποτε αλλαγή απαιτεί μια εντελώς διαφορετική nonce.



Εικόνα 19.Διεξαγωγή συναλλαγής BitCoins.Διαθέσιμο στο:
http://osarena.net/wp-content/uploads/2013/11/habtw_how_a_bitcoin_transaction_works.jpg

Υποθέτουμε ότι ο Bob είναι έμπορος στο διαδίκτυο και αποφασίζει να αρχίσει την αποδοχή των bitcoins ως μέσο πληρωμής. Η Alice, μια καταναλώτρια, έχει bitcoins και θέλει να αγοράσει εμπορεύματα από τον Bob. Βασική προϋπόθεση για να πραγματοποιηθεί η συναλλαγή, ο καθένας να διαθέτει «ηλεκτρονικό πορτοφόλι» και «ηλεκτρονική διεύθυνση».

Αρχικά ο Bob και η Alice θα πρέπει να έχουν τα δικά τους BitCoins «πορτοφόλια» στον υπολογιστή τους, τα οποία είναι τα αρχεία που παρέχουν πρόσβαση σε πολλαπλές διευθύνσεις Bitcoins. Στο σημείο αυτό να αναφέρουμε ότι η διεύθυνση είναι μια σειρά από γράμματα και αριθμούς, όπως για παράδειγμα lUIHhkjhYU7676786yJHkjh.

Στην συνέχεια πρέπει να δημιουργηθεί μια νέα διεύθυνση ώστε να την στείλει στην Alice και να στείλει εκεί την πληρωμή της. Για την υποβολή της

4.2.1 Προτεινόμενη αμοιβή συναλλαγής

Το πρόγραμμα Bitcoin Core ελέγχει το μέγεθος της συναλλαγής και με βάση αυτό υπολογίζει την αμοιβή που θα χρειαστεί. Ο αναλυτικός αλγόριθμος υπολογισμού της αμοιβής είναι

148 * αριθμός εισόδων + 34 * αριθμός εξόδων + 10

Αν το αποτέλεσμα της πράξης είναι μικρότερο από 10.000 bytes και η συναλλαγή είναι υψηλής προτεραιότητας, τότε μπορεί να γίνει χωρίς αμοιβή. Σε διαφορετική περίπτωση χρειάζεται αμοιβή, η οποία έχει καθοριστεί στα 0,0001 bitcoins ανά 1000 bytes.

Ο παραπάνω κανόνας δεν αποτελεί μέρος του πρωτοκόλλου Bitcoin κι άρα είναι προαιρετικό το αν κάποιος Miner ή πρόγραμμα Bitcoin θα τον ακολουθήσει. Η μη συμπερίληψη αμοιβής σε μια Bitcoin συναλλαγή, εμπεριέχει τον κίνδυνο να καθυστερήσει πολύ η επιβεβαίωσή της και τοποθέτησή της σε κάποιο μπλοκ.

4.2.2 Επιλογή συναλλαγών στο μπλοκ

Ο αριθμός των συναλλαγών που θα χωρέσουν μέσα στο κάθε μπλοκ, εξαρτάται από το μέγεθος των συναλλαγών. Τί γίνεται όμως αν το συνολικό μέγεθος του πλήθους των συναλλαγών ξεπερνάει το 1MB του μεγέθους του μπλοκ; Είναι προφανές ότι επειδή δε θα χωρέσουν όλες, κάποιες θα μείνουν εκτός. Σε μια τέτοια περίπτωση, οι Miners επιλέγουν να ενσωματώσουν στο νέο μπλοκ τις συναλλαγές αυτές που έχουν τις υψηλότερες αμοιβές. Αν υποθέσουμε ότι αυξάνεται η δημοτικότητα του Bitcoin τόσο ώστε να υπάρχει συνεχώς πλήθος συναλλαγών που να μη χωράνε σε ένα μπλοκ, οι συναλλαγές χωρίς αμοιβή μπορεί να μην συμπεριληφθούν ποτέ. Όσο το πρόβλημα θα μεγαλώνει, σιγά-σιγά θα σταματήσουν να συμπεριλαμβάνονται και οι συναλλαγές με αμοιβή, γιατί θα υπάρχουν άλλες συναλλαγές με μεγαλύτερη

αμοιβή, δημιουργώντας έτσι μια κούρσα άτυπης αύξησης της χρέωσης των συναλλαγών ως μέτρο σιγουριάς ότι η συναλλαγή θα εκτελεστεί. Αυτό όμως αποτελεί μεγάλο δυνητικό πρόβλημα, το οποίο απειλεί ή θα απειλήσει κάποια στιγμή το Bitcoin.

4.3 Διαδικασία Εξόρυξης (Mining)

Η εξόρυξη bitcoins είναι η διαδικασία της δημιουργίας μπλοκ για την αλυσίδα μπλοκ, η οποία είναι ένας τρόπος επεξεργασίας και επαλήθευσης των συναλλαγών. Προσθέτοντας ένα μπλοκ στην αλυσίδα μπλοκ είναι δύσκολο, απαιτεί χρόνο και επεξεργαστική ισχύ για να επιτευχθεί. Το άτομο που καταφέρνει να παράγει ένα μπλοκ παίρνει μια ανταμοιβή. Ο παραγωγός μπλοκ παίρνει μια γενναιοδωρία κάποιων αριθμό bitcoins, η οποία είναι συμφωνημένη από το δίκτυο. Προς το παρόν αυτή γενναιοδωρία είναι 50 bitcoins.

Αυτή η δραστηριότητα είναι γνωστή ως "bitcoin εξόρυξης" - που χρησιμοποιούν την επεξεργαστική ισχύ για να προσπαθήσει να προσκομίσει το ισχύον μπλοκ, και ως «δικό μου», με αποτέλεσμα κάποια bitcoins. Όσο μεγαλύτερη είναι η συνολική δυσκολία, τόσο πιο δύσκολο είναι για έναν εισβολέα να αντικαταστήσετε την άκρη της αλυσίδας μπλοκ με το δικό του μπλοκ του (η οποία δίνει τη δυνατότητα να διπλασιάσει-περνούν τα κέρματα του[31] [32].

4.3.1 Λογισμικό Mining

ια να πραγματοποιηθεί η διαδικασία που περιγράψαμε παραπάνω (mining) πρέπει να διαθέτουμε το κατάλληλο λογισμικό. Τα διαθέσιμα λογισμικά φαίνονται παρακάτω:

- **Cgminer**

[31] http://bitcoinsgr.blogspot.gr/2011/10/bitcoins.html
[32] https://en.bitcoin.it/wiki/Mining

Χαρακτηριστικά :

- ✓ Είναι ανοιχτού κώδικα και διατίθεται σε λογισμικά Windows και Linux.
- ✓ Υποστηρίζει mining με κάρτες γραφικών, FPGAs

- **DiabloMiner**

Χαρακτηριστικά :

- ✓ Είναι ανοιχτού κώδικα και διατίθεται σε λογισμικά Windows και Linux.
- ✓ Long Polling
- ✓ BFI_INT
- ✓ Async nw
- ✓ Multipool
- ✓ 79xx GCN3

- **Ufasoft miner**

Χαρακτηριστικά :

- ✓ Είναι ανοιχτού κώδικα και διατίθεται σε λογισμικά Windows και Linux.
- ✓ BFI_INT
- ✓ X-Roll-NTime
- ✓ RPC w/LP
- ✓ MMP

- **FPGAminer**

Χαρακτηριστικά :

- ✓ Είναι ανοιχτού κώδικα και διατίθεται σε λογισμικά Windows και Linux.

- **BAMT**

Πρόκειται για διανομή Linux που περιέχει όλα τα απαραίτητα προγράμματα για bitcoin mining. Μπορεί να περαστεί και σ" ένα bootable USB Flash Disk, ώστε να μη χρειάζεται καθόλου σκληρός δίσκος.

- **RSMPPS** – Όπως και το SMPPS αλλά με προτεραιότητα πληρωμής στους πιο πρόσφατους miners

- **CPPSRB** – Όπως το PPS αλλά με όριο το οποίο προσδιορίζεται από τις πιο πρόσφατες αναδρομικές αποδοχές

- **SCORE** – Αναλογική αμοιβή στους miners με βάση το score τους. Κάθε πρόσφατο share έχει μεγαλύτερο score από κάποιο παλαιότερο κι όσο πιο παλιό είναι ένα share τόσο μικρότερο το score του. Με αυτό το σύστημα, ένας miner που θα σταματήσει την εξόρυξη στο συγκεκριμένο pool, το score του θα πέσει πολύ γρήγορα και συνεπώς και η αμοιβή του

PPLNS – Ο υπολογισμός των νομισμάτων γίνεται με βάση τα N shares με τα οποία συνείσφερε ο miner, τα οποία δεν αφορούν αποκλειστικά το συγκεκριμένο block. Με αυτό το σύστημα αποφεύγεται το φαινόμενο του pool hoping κατά το οποίο κάποιοι miners εξορύσσουν με στρατηγική σε διάφορα pools, ώστε ν" αυξήσουν το εισόδημά τους σε βάρος των υπολοίπων

Prop – Μόλις βρεθεί το block όλοι αμείβονται ανάλογα με τα πόσα shares έχει συνεισφέρει ο καθένας

4.3.3 Υλικό Mining

CPU Mining

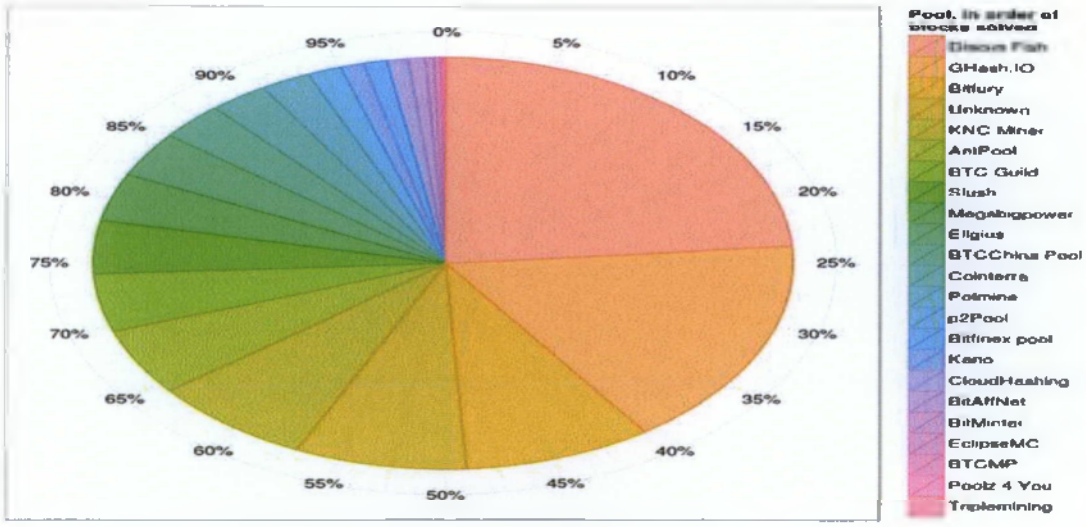
Η πρώτη κατηγορία είναι το CPU Mining. Για να κάνει κάποιος Bitcoin Mining χρειάζεται επεξεργαστική ισχύ. Αρχικά το mining γινόταν κάνοντας χρήση του κεντρικού επεξεργαστή (CPU) ενός ηλεκτρονικού υπολογιστή. Σύντομα όμως παρατηρήθηκε ότι ο κεντρικός επεξεργαστής είναι πολύ πιο αργός σε σχέση με έναν επεξεργαστή γραφικών (GPU)

4.3.2 Mining Pools

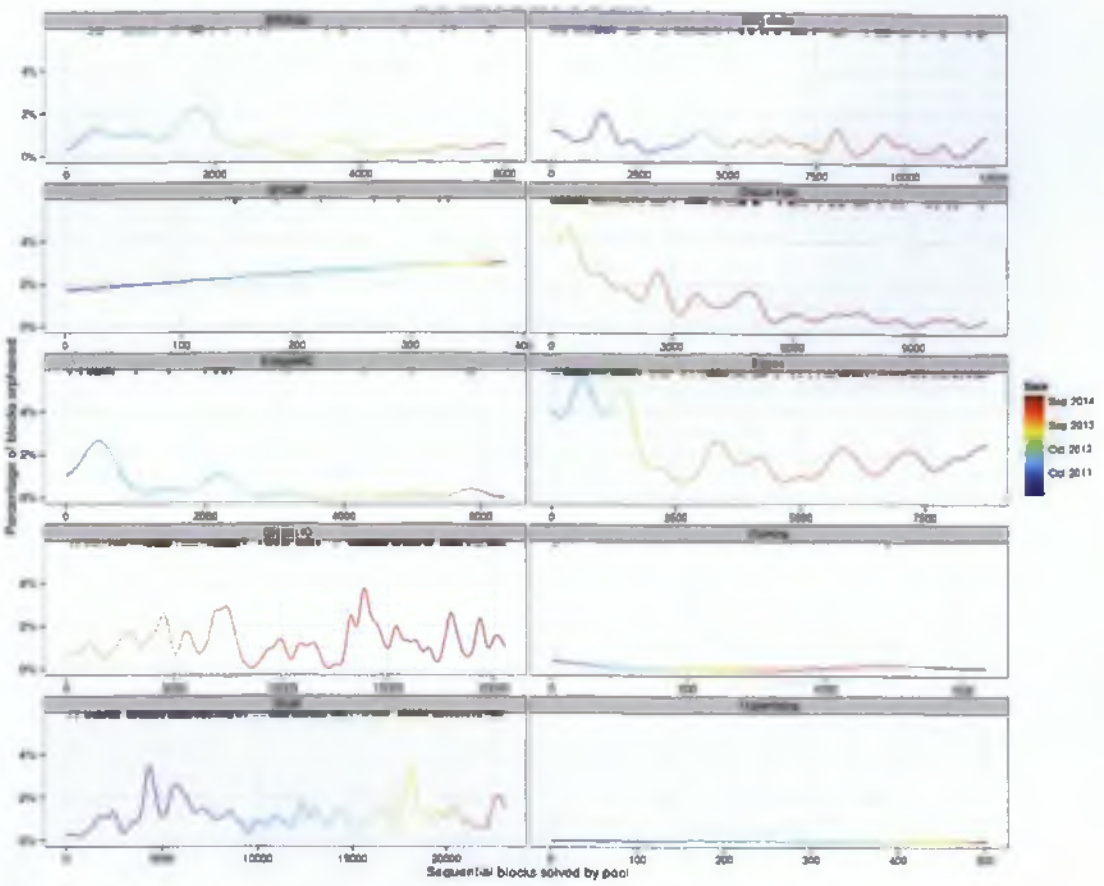
Η εξόρυξη νομισμάτων μπορεί να γίνεται από τους miners είτε αυτόνομα ο καθένας, είτε να εργάζονται πολλοί μαζί προς την ανακάλυψη ενός block. Στη δεύτερη περίπτωση, οι miners εργάζονται συντονισμένα σε ένα mining pool, μια πρακτική που είναι εξαιρετικά διαδεδομένη, αφού λόγω της υψηλής δυσκολίας για να δημιουργήσει ένας miner ενός block, θα χρειαστεί πολλούς μήνες. Τα νομίσματα που προκύπτουν από την εύρεση ενός block, μοιράζονται σε όλους όσους συμμετείχαν στο mining pool, ανάλογα με την προσπάθεια που κατέβαλαν.

Τα πιο διαδεδομένα mining pools είναι:

- **DeepBit** – PPS / Prop
- **BTCGuild** – PPS, PPLNS
- **Slush** – Score
- **OzCoin** – DGM / PPS
- **EclipseMC** – DGM / PPS
- **50BTC** – PPS
- **BitMinter** – PPLNS
- **P2Pool** – PPLNS



Εικόνα 20.Προσοστό των έγκυρων Mining Pools. Διαθέσιμο στο: https://bitcointalk.org/



Εικόνα 21.Ποσοστό των απωλειών των μπλοκ. Διαθέσιμο στο:
https://bitcointalk.org/index.php?topic=104664.0

Υπάρχουν διάφοροι τρόποι που το mining pool μοιράζει τα νομίσματα που προκύπτουν από τη δημιουργία ενός block στους συμμετέχοντες. Οι πιο διαδεδομένοι παρουσιάζονται παρακάτω μαζί με την εξήγηση.

- **PPS** – Ο πιο απλός τρόπος υπολογισμού. Κάθε share «ανταμείβεται» με συγκεκριμένο αριθμό νομισμάτων, συνήθως μερικών χιλιοστών του bitcoin.

- **SMPPS –** Το ίδιο με το προηγούμενο, αλλά το mining pool δεν πληρώνει ποτέ παραπάνω από όσα νομίσματα δημιουργήθηκαν από τα blocks

- **ESMPPS –** Όπως και το SMPPS αλλά με πιο δίκαιη διανομή των νομισμάτων

GPU Mining

Τα προγράμματα επεκτάθηκαν και τροποποιήθηκαν ώστε να χρησιμοποιούν τους επεξεργαστές γραφικών για τους σύνθετους υπολογισμούς του Bitcoin Mining. Παρά όμως το ότι οι σημερινές κάρτες γραφικών μπορούν να παράξουν πολλά εκατομμύρια hashes κάθε δευτερόλεπτο, έχουν υψηλή κατανάλωση ενέργειας κι αντίστοιχα μεγάλη απαγωγή θερμότητας, δημιουργώντας έτσι σοβαρά προβλήματα για την τροφοδότησή τους αλλά και για την ψύξη τους. Για τους λόγους αυτούς έγιναν προσπάθειες ώστε να βρεθούν άλλοι, πιο οικονομικοί τρόποι για Mining.

FPGA Mining

Οι συσκευές FPGA για mining, δημιουργήθηκαν για να έχουν μικρό μέγεθος κι εξαιρετικά μικρή κατανάλωση ενέργειας κι άρα αντίστοιχα μικρή απαγωγή θερμότητας, κάνοντας χρήση προγραμματιζόμενων επεξεργαστών. Πρόκειται συσκευές στο μέγεθος μιας πιστωτικής κάρτας με μεγαλύτερο ύψος, που μπορούν να παράγουν εκατομμύρια hashes σε κάθε δευτερόλεπτο, με καταναλώσεις ενέργειας που ξεκινούν από μόλις μερικά Watt. Έχουν υπάρξει και υλοποιήσεις από συστοιχίες FPGA αλλά το κόστος αγοράς τους ήταν απαγορευτικό.

ASIC Mining

Ενώ τα FPGA στην εποχή τους είχαν καλές επιδόσεις και χαμηλές καταναλώσεις, ο αγώνας δρόμου για ακόμα περισσότερα Mh/s (million hashes per second) συνεχίστηκε. Το αποτέλεσμα ήταν η παραγωγή ολοκληρωμένων κυκλωμάτων εξειδικευμένης χρήσης αποκλειστικά για Bitcoin Mining, τα επονομαζόμενα ASIC. Μια υλοποίηση βασισμένη σε ολοκληρωμένα ASIC, μπορεί να φτάσει πολλά δισεκατομμύρια hashes per second (Gh/s) και προς το παρόν (2014) αποτελεί τον μοναδικό τρόπο για Mining που να έχει νόημα κι ίσως κάποιο κέρδος.

Συνοψίζοντας, ταξινομημένα με χρονολογική σειρά, η δημιουργία bitcoins μέσω mining έκανε χρήση:

- Του κεντρικού επεξεργαστή ενός υπολογιστή (2009 – 2010)
- Της κάρτας γραφικών ενός υπολογιστή (2010 – 2012)
- Συσκευών FPGA (2011 – 2013)
- Συσκευών ASIC (2013 – σήμερα)

Οι πιο δημοφιλείς κάρτες γραφικών για mining ήταν οι κάρτες της AMD (ATI) των σειρών 58xx και 79xx. Μπορείτε να δείτε αναλυτικά την εκτιμώμενη απόδοση της κάθε κάρτας. Εδώ να τονίσουμε ότι δεν συνιστούμε το mining με επεξεργαστή (CPU) ή κάποια άλλη κάρτα γραφικών εκτός από ATI Radeon HD, γιατί το κόστος της ηλεκτρικής ενέργειας που θα καταναλωθεί θα είναι υψηλότερο από την αξία των bitcoins που θα παραχθούν.

Επειδή ο χρόνος εύρεσης ενός block είναι πολύ μεγάλος, αν κάποιος προσπαθεί μόνος του, έχουν δημιουργηθεί πολλά mining pools όπου οι χρήστες ενώνουν όλοι μαζί τις δυνάμεις τους για την εύρεση του block και κατόπιν μοιράζονται την αμοιβή ανάλογα με τη συνεισφορά του καθενός[33].

4.4 Υπολογισμοί Παραγωγής (Mining Calculators)

Ο χρήστης, έχει την δυνατότητα να υπολογίσει στο περίπου τον ρυθμό παραγωγής BitCoins από τον υπολογιστή τους. Αυτό βέβαια εξαρτάται από τον υλικό και το λογισμικό που διαθέτει. Παρακάτω εκθέτονται διάφορα εργαλεία υπολογισμού του ρυθμού παραγωγής Bitcoins, τον υπολογισμό του κέδρους και εργαλεία για τα mining pools.

[33] http://bitcoinx.gr/mining/

4.4.1 Bitcoin Mining Calculator

Υπολογισμός ρυθμού παραγωγής bitcoins ανάλογα με την επεξεργαστική ισχύ (Hashrate) και τη δυσκολία παραγωγής. (Difficulty). Ο υπολογιστής παραγωγής διατίθεται στο παρακάτω υπερσύνδεσμο: http://tpbitcalc.appspot.com/

Difficulty	40300030327.8910		Rig Cost	1000.00	$
Hash Rate	1000.00	MHash/s	Power Consumption	80.00	W
Exchange Rate	361.00	$/B	Price of Power	0.10	$/kWh
Bitcoins per Block	25.00	B	Investment Period	355	days

Calculate

Reset

Results:

Earnings	B	$
Hourly	0.000001	0.000188
Daily	0.000012	0.004505
Weekly	0.000087	0.031535
Monthly	0.000374	0.135150
Annual	0.004555	1.644328

Mining cost	0.008000$/h
Net hourly profit	-0.007812$/h
Net daily profit	-0.187495$/day
Net weekly profit	-1.31$/week
Net monthly profit	-5.62$/month
Net Annual profit	-68.44$/year
Break even after	Never days

Cost to generate 1B (with hardware cost)	241112.34$
Cost to generate 1B (without hardware cost)	15385.54$
B generated in Investment Period	0.00B
Money generated in Investment Period	1.60$
Net profit in Investment Period	-1066.56$

Time to generate one block	2003325.4 days
Blocks generated annually	0.000 blocks

Εικόνα 22.Υπολογισμός ρυθμού παραγωγής bitcoins

4.4.2 Υπολογιστής κέρδους

Υπολογισμός του κέρδους από την εξόρυξη bitcoins, αφού αφαιρεθεί το κόστος της ηλεκτρικής ενέργειας. Υπολογίζει επίσης και την απόσβεση του κόστους εξοπλισμού. Ο υπολογιστής κέρδους διατίθεται στο παρακάτω υπερσύνδεσμο: http://www.bitcoinx.com/profit/

4.4.4 Υπολογισμός χρόνου μέχρι την ανεύρεση Block

Κάθε Block που δημιουργείται στην αλυσίδα των Blocks (block chain), είναι το αποτέλεσμα πολλών εκατομμυρίων υπολογισμών. Για να μπορεί ο χρόνος δημιουργίας κάθε νέου Block να είναι σχεδόν σταθερός, κοντά στα δέκα λεπτά, προσαρμόζεται η δυσκολία των υπολογισμών ανάλογα με τη διαθέσιμη επεξεργαστική ισχύ του δικτύου. Για να υπολογίσουμε πόσο χρόνο θα χρειαστούμε για να δημιουργήσουμε μόνοι μας ένα Block με την επεξεργαστική ισχύ που διαθέτουμε, θα πρέπει να χρησιμοποιήσουμε τον παρακάτω τύπο:

Χρόνος (δευτερόλεπτα) = difficulty * 2^32 / hash rate[34]

4.5 Πορτοφόλια BitCoins

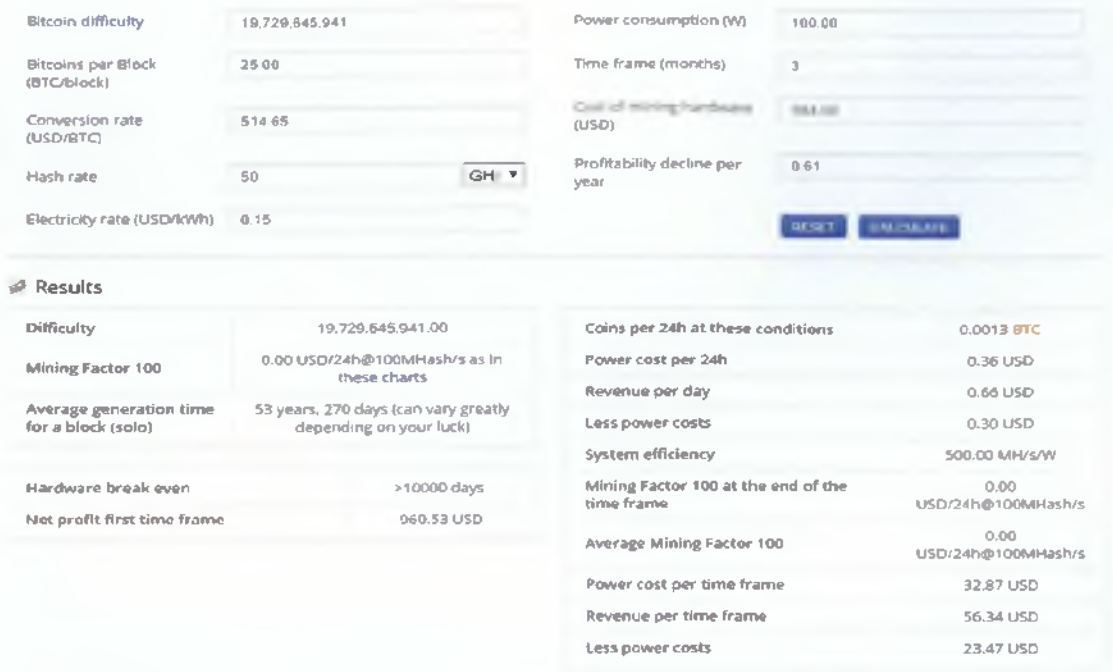
Τα πορτοφόλια Bitcoin περιέχουν τις πληροφορίες που χρειάζεστε για να πραγματοποιήσετε συναλλαγές: τις διευθύνσεις σας και τα κλειδιά σας. Θα χρειαστείτε το "κλειδί" μίας διεύθυνσης για να μπορέσετε να χρησιμοποιήσετε τα Bitcoin σας. Τα πορτοφόλια μπορούν να 'έχουν πολλές μορφές: desktop, apps, ή ιστοσελίδες[35].

4.5.1 Online Πορτοφόλια Bitcoin

Ένα ηλεκτρονικό πορτοφόλι είναι ένα πορτοφόλι που φιλοξενείται σε μια εξωτερική ιστοσελίδα. Το μεγαλύτερο ηλεκτρονικό πορτοφόλι με μεγάλη διαφορά είναι το BlockChain. Είναι ένα ηλεκτρονικό πορτοφόλι συνήθως πολύ εύκολο στην εγκατάσταση, και μπορείτε να έχετε πρόσβαση από οποιονδήποτε υπολογιστή με πρόσβαση στο internet. Υπάρχει αντίστοιχα iphone application για την διαχείρισης του wallet από το κινητό σας.

---

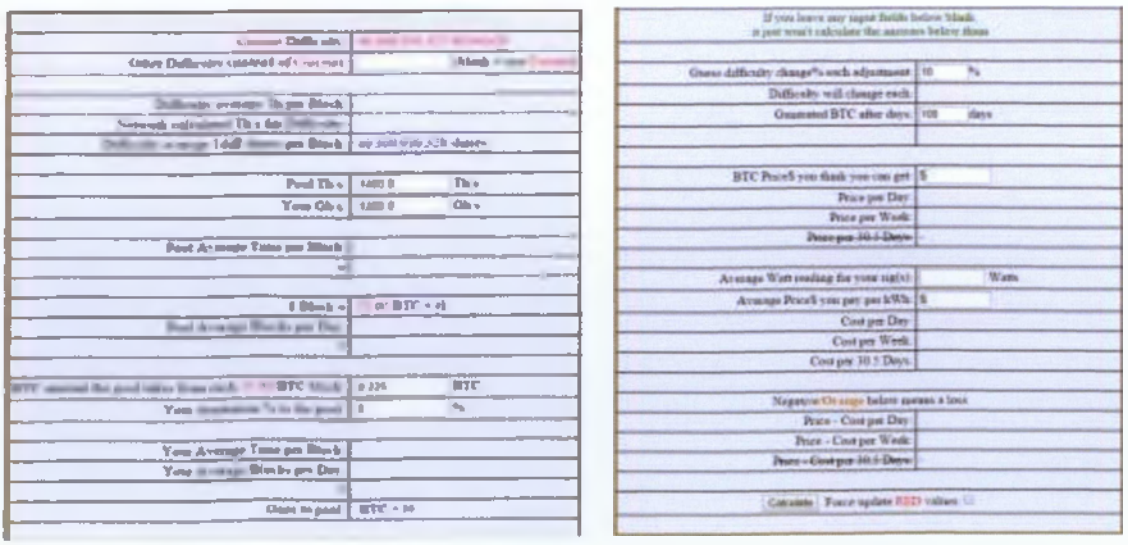
[34] http://bitcoinx.gr/mining-calculators/
[35] https://www.btcgreece.com/Help/HelpPageView/what-is-bitcoin-wallet



Εικόνα 23.Υπολογισμός του κέρδους από την εξόρυξη bitcoins

4.4.3 Υπολογισμός για Mining Pools

Υπολογισμός διαθεσιμότητας ενός Block από το Pools σας. Ο υπολογιστής για τα Mining Pools διατίθεται στο παρακάτω υπερσύνδεσμο: http://tradebtc.net/bitcalc.php

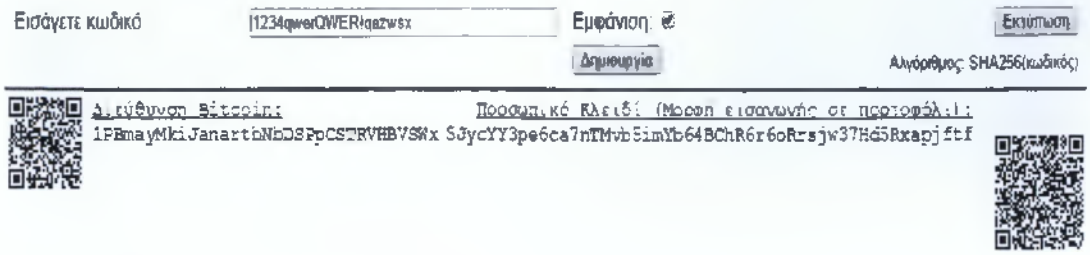


Εικόνα 24.Υπολογισμός διαθεσιμότητας Block

4.5.2 Offline Πορτοφόλια Bitcoin

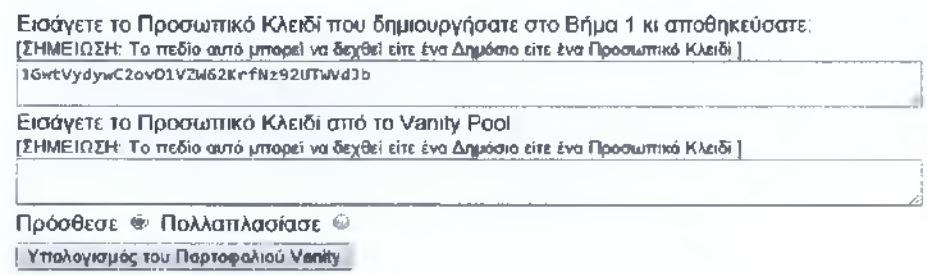
Τα αποσυνδεδεμένα πορτοφόλια αποθηκεύονται στον τοπικό υπολογιστή σας. Δεδομένου ότι έχετε τον έλεγχο του υλικού, μπορείτε να αποφασίσετε να εφαρμόσετε ότι επίπεδο ασφαλείας επιθυμείτε. BitcoinQT είναι το επίσημο πορτοφόλι του Bitcoin, αλλά έχει μόνο πολύ βασικές λειτουργίες και μπορεί να είναι δύσκολο να χρησιμοποιηθεί για Bitcoin αρχάριους. Απαιτεί, επίσης, ένα πολύ μεγάλο (4GB +).

Μνημονικό Πορτοφόλι



Εικόνα 28.Μνημονικό Πορτοφόλι BitCoins

Πορτοφόλι Vanity



Εικόνα 29.Πορτοφόλι Vanity BitCoins

Λεπτομέρειες Πορτοφολιού

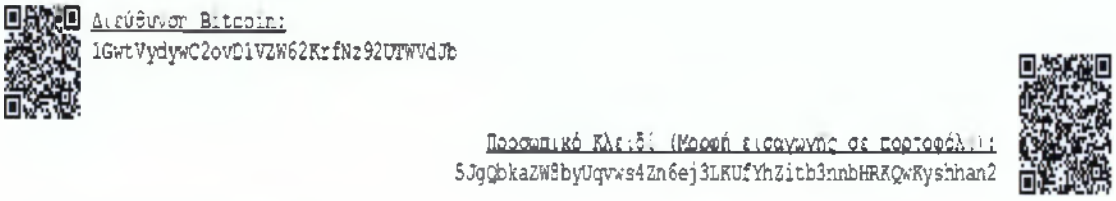
Εικόνα 30.Λεπτομέρειες Πορτοφολιού BitCoins[36]

[36] http://bitcoinx.gr/apps/bitaddress.html?culture=el

5 Εργαλεία BitCoins

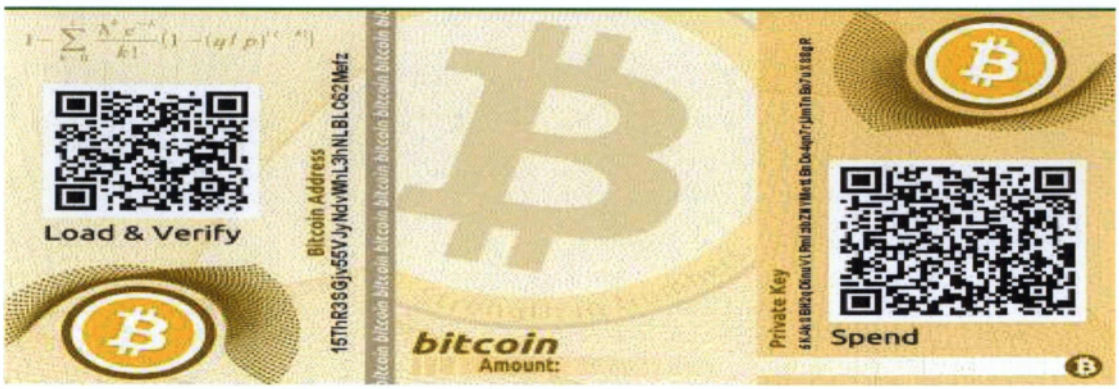
5.1 Δημιουργός Διευθύνσεων

✓ **Απλό Πορτοφόλι**



Εικόνα 25.Απλό Πορτοφόλι BitCoins

✓ **Χάρτινο Πορτοφόλι**



Εικόνα 26. Χάρτινο Πορτοφόλι BitCoins

Πολλαπλά Πορτοφόλια

Εικόνα 27.Πολλαπλά Πορτοφόλια BitCoins

5.2 Bitcoin clients

Παρακάτω μπορείτε να βρείτε τα πιο δημοφιλή προγράμματα Bitcoin Client για όλα τα λειτουργικά συστήματα.

- **Satoshi Bitcoin Client** – για Windows, Linux και MacOS X (Open Source). Ο πρώτος client που γράφτηκε για το Bitcoin.
- **Armory Client** – Open Source client με πληθώρα χρήσιμων χαρακτηριστικών (για πιο ισχυρούς υπολογιστές)
- **MultiBit** – Κατά πάσα πιθανότητα ο πιο απλός Open Source Bitcoin client
- **Electrum** – Ένας ελαφρύς client ο οποίος έχει το εκπληκτικό χαρακτηριστικό ότι δεν απαιτεί το κατέβασμα όλων των δεδομένων της αλυσίδας των μπλοκ.

Bitcoin Wallet – Android εφαρμογή που υποστηρίζει μεταξύ άλλων QR Codes και NFC.

Εκτός από τις προαναφερθέντες εφαρμογές για υπολογιστή και κινητό, υπάρχουν και Online υπηρεσίες πορτοφολιού (πορτοφόλια web). Μερικές από αυτές παρουσιάζονται παρακάτω. Στο σημείο αυτό να επισημάνουμε ότι Στα Online πορτοφόλια δεν έχετε τον πλήρη έλεγχο. Ανά πάσα στιγμή συμβεί κάτι στο Online πορτοφόλι, ενδέχεται να μην έχετε πρόσβαση στα bitcoins σας.

- **Blockchain.info** – Πρόκειται για ένα υβριδικό πορτοφόλι web για κινητά. Είναι επίσης διαθέσιμο για το iPhone σε έναν περιορισμένο τρόπο ώστε να πληροί τις πολιτικές της Apple. Περιλαμβάνει πολλά χαρακτηριστικά, όπως δημιουργία αντιγράφων ασφαλείας για το web πορτοφόλι.
- **BIPS** – Υπηρεσία web πορτοφολιού από τη WalletBit που επιτρέπει την εύκολη αγορά και πώληση bitcoins σε πολλές χώρες.
- **Coinase** – Μια υπηρεσία web πορτοφολιού στοχεύει να είναι η πιο εύκολη στη χρήση.

Αν έχουμε bitcoins και θέλουμε να τα μετατρέψουμε σε ευρώ, στέλνουμε αντίστοιχα τα bitcoins μας στο ανταλλακτήριο και πιστώνονται στον λογαριασμό μας. Μετά μπορούμε να τα πουλήσουμε για να λάβουμε ευρώ, τα οποία και θα πιστωθούν στον λογαριασμό μας στο ανταλλακτήριο. Στη συνέχεια, μπορούμε να ζητήσουμε τη μεταφορά των ευρώ που βρίσκονται στο λογαριασμό μας στο ανταλλακτήριο προς τον τραπεζικό μας λογαριασμό.

Αρχικά θα πρέπει να έχουμε υπόψιν μας ότι οι τραπεζικές συναλλαγές πάνω από ένα όριο, ελέγχονται. Αν παράγουμε bitcoins κι επιλέγουμε να τα ρευστοποιούμε σε κάποιο ανταλλακτήριο και συνεπώς υπάρχει συνεχόμενη ροή χρημάτων από κάποια τράπεζα στο εξωτερικό προς τη δική μας, θα κληθούμε να δώσουμε εξηγήσεις για την προέλευση των χρημάτων.

Οι τραπεζικές κινήσεις, από την τράπεζά μας προς το ανταλλακτήριο κι αντίστροφα, δεν είναι άμεσες και μπορεί να διαρκέσουν πολλές ημέρες. Καλό είναι επίσης να αποφύγουμε τραπεζικές κινήσεις που δεν είναι SEPA, αφού αυτές έχουν μεγάλη χρέωση.

Λόγω των πρόσφατων ρυθμίσεων, τα περισσότερα ανταλλακτήρια κάνουν πλέον ταυτοποίηση του χρήστη, για να τηρούν τις οδηγίες KYC και AML. Για να αρθούν κάποια όρια στις συναλλαγές, ή σε ορισμένες περιπτώσεις για να μπορούν να γίνουν οι συναλλαγές από και προς το ανταλλακτήριο, θα πρέπει να στείλουμε στο ανταλλακτήριο αντίγραφο της ταυτότητας ή του διαβατηρίου μας, σε ηλεκτρονική μορφή. Επίσης κάποια ανταλλακτήρια ζητούν και αντίγραφο κάποιου λογαριασμού κοινής ωφέλειας, που να είναι επίσης στο όνομά μας. Τέλος, θα πρέπει να στείλουμε στο ανταλλακτήριο χρήματα από κάποιο τραπεζικό λογαριασμό που είναι στο όνομά μας, αλλά και για να μπορούμε να λάβουμε χρήματα στο λογαριασμό που θα δηλώσουμε, θα πρέπει κι αυτός να είναι στο όνομά μας.

5.3 Παρακολούθηση τιμής

Το BitCoin, λόγω της δυναμικής του και της άξιας του έχει γνωρίσει ιδιαίτερη άνθηση τα τελευταία χρόνια. Αυτό έχει ως αποτέλεσμα την εφάμιλλη συμπεριφορά με τα υπόλοιπα ισχυρά νομίσματα. Έτσι, οι ιστοσελίδες που δραστηριοποιούνται στον οικονομικό κλάδο εισήγαγαν την χρηματιστηριακή κίνηση και την αξία των συναλλαγών του BitCoin και πλέον διατίθεται για ζωντανή παρακολούθηση. Στις παρακάτω εικόνες παρουσιάζονται οι σημαντικότερες εξ αυτών:

5.3.1 Bitcoinity.org

Εικόνα 31. Bitcoinity.org.

Δωρεάν υπηρεσία που παρέχει τις εξής δυνατότητες:

- ✓ Εύρος 10 λεπτά, 1 ώρα, 3 ώρες, 12 ώρες, 24 ώρες, 3 ημέρες, 7 ημέρες, 30 ημέρες, 6 μήνες
- ✓ Νομίσματα Ευρώ, Δολάριο Αμερικής, Δολάριο Καναδά, Λίρα Αγγλίας, Γιεν Ιαπωνίας και Ζλότι Πολωνίας

- ✓ Ανταλλακτήρια MtGox, Bitstamp, Bitcoin24, Bitfloor

Ο ιστοχώρος είναι προσβάσιμος στο: http://bitcoinity.org/markets

5.3.2 Bitcoin.clarkmoody.com

Εικόνα 32.Bitcoin.clarkmoody.com

Δωρεάν υπηρεσία που παρέχει τις εξής δυνατότητες:

- ✓ Εύρος 1 λεπτό, 3 λεπτά, 5 λεπτά, 15 λεπτά, 1 ώρα, 4 ώρες, 24 ώρες, 3 ημέρες, 1 εβδομάδα
- ✓ Εκτός από Ευρώ και Δολάριο Αμερικής υπάρχει επιλογή για άλλα 15 νομίσματα
- ✓ Ανταλλακτήρια MtGox

Ο ιστοχώρος είναι προσβάσιμος στο: https://zeroblock.com/

5.3.3 BitcoinTicker.co

Εικόνα 33.BitcoinTicker.co

Παρέχει αρκετά μεγάλη ιστορικότητα, με βήμα 10 λεπτών, ώρας, 3-12-24 ωρών, 3-7-30 ημερών, 3-6 μηνών. Δίνει τη δυνατότητα παρακολούθησης της ισοτιμίας για EUR, USD και GBP μόνο, από τα MtGox και bitstamp.

Ο ιστοχώρος είναι προσβάσιμος στο: http://bitcointicker.co/

5.4 Παρακολούθηση τιμής & τεχνικών πληροφοριών

5.4.1 Bitcoindashboard.com

Εκτός από πληροφορίες τιμής, παρέχει δωρεάν επιπλέον γραφήματα που αφορούν τα: τρέχον μέγεθος μπλοκ, μέσος όρος αξίας συναλλαγής, συνολικά νομίσματα, μέσος όρος χρόνου επιβεβαίωσης συναλλαγής, τρέχον hashrate, αμοιβή

συναλλαγής κι άλλα. Η συγκεκριμένη ιστοσελίδα δε συνίσταται σε απλούς χρήστες ή οικονομολόγους, λόγω των ιδιαίτερα τεχνικών στοιχείων που παρουσιάζονται.

Εικόνα 34.Bitcoindashboard.com

Ο ιστοχώρος είναι προσβάσιμος στο: http://www.bitcoindashboard.com/

5.4.2 bitcoincharts.com

Το bitcoincharts.com παρέχει πληροφορίες για τιμή από πολλά ανταλλακτήρια, hashrate, hashrate ανά mining pool και πολλοί τρόποι απεικόνισης.

Ο ιστοχώρος είναι προσβάσιμος στο:
http://bitcoincharts.com/charts/mtgoxEUR#rg60ztgSzm1g10zm2g25zv

Εικόνα 35.bitcoincharts.com

5.4.3 blockchain.info

Εικόνα 36.blockchain.info

Παρέχει πολλά και διάφορα διαγράμματα όπως Σύνολο Bitcoins σε κυκλοφορία, Κεφαλαιοποίηση, Αριθμός συναλλαγών, Αριθμός μοναδικών διευθύνσεων Bitcoin, Αριθμός συναλλαγών ανά μπλοκ, Εκτιμώμενος Όγκος Συναλλαγών, Κόστος ανά συναλλαγή κι άλλα.

Ο ιστοχώρος είναι προσβάσιμος στο: https://blockchain.info/charts

Εικόνα 37.Στατιστικά BitCoins μέσω του ιστοχώρου blockchain.info

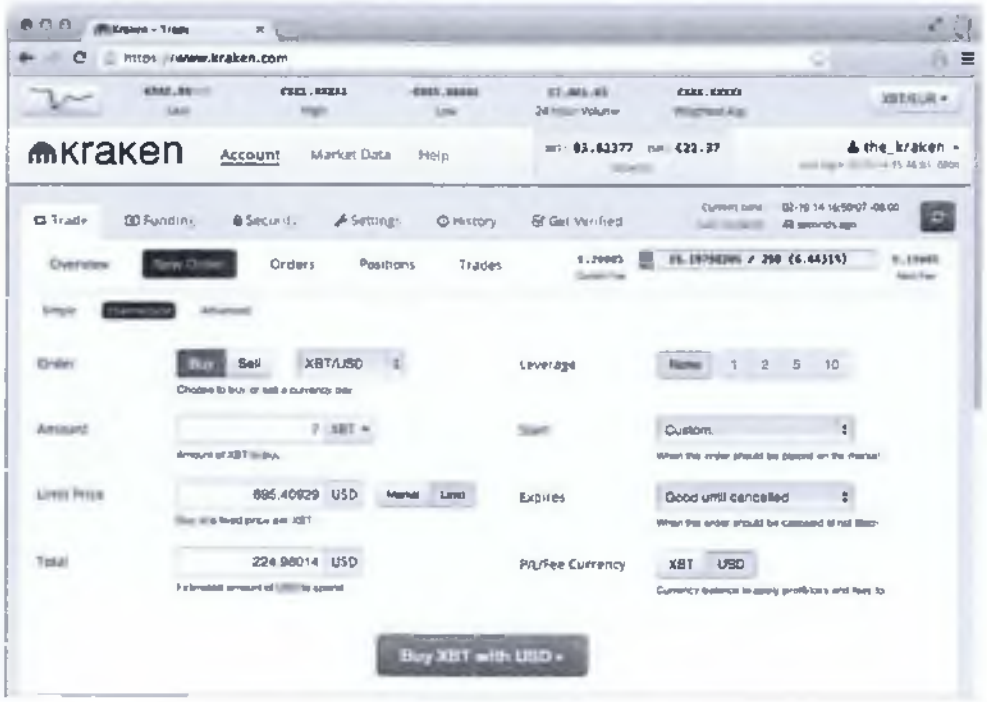
5.5 Ανταλλακτήρια BitCoins

Τα ανταλλακτήρια είναι ουσιαστικά οι ενδιάμεσοι που παίζουν το ρόλο της μετατροπής από ένα νόμισμα (ευρώ, δολάριο, κλπ) σε ένα άλλο (bitcoin, litecoin, κλπ). Ο τρόπος λειτουργίας τους είναι αρκετά απλός. Πρώτα θα πρέπει να δημιουργήσουμε ένα λογαριασμό σε κάποιο ανταλλακτήριο. Μόλις το κάνουμε αυτό, θα λάβουμε οδηγίες για το πως μπορούμε να στείλουμε χρήματα σε αυτό μέσω τράπεζας (SEPA ή SWIFT αν και το πρώτο είναι μακράν πιο οικονομικό). Τα χρήματα που θα στείλουμε, θα πιστωθούν στον λογαριασμό μας στο ανταλλακτήριο και θα μπορούμε να τα χρησιμοποιήσουμε για να αγοράσουμε bitcoins. Τα bitcoins που αγοράσαμε, μπορούμε στη συνέχεια να τα στείλουμε στο πορτοφόλι μας.

Kraken

Ανταλλακτήριο διαφόρων νομισμάτων με τα περισσότερα χαρακτηριστικά. Παρέχει δυνατότητα για εντολές Market, Limt, Stop limit, Take profit, Stop loss, Take profit limit, κ.α. Ανταλλάσσει μεταξύ Ευρώ, Δολάριο, Bitcoin, Litecoin, Dogecoin, Ripple και Namecoin.

Ο ιστοχώρος είναι προσβάσιμος στο: https://www.kraken.com/



Εικόνα 42.Kraken

5.6 Ανταλλακτήρια κρυπτονομισμάτων

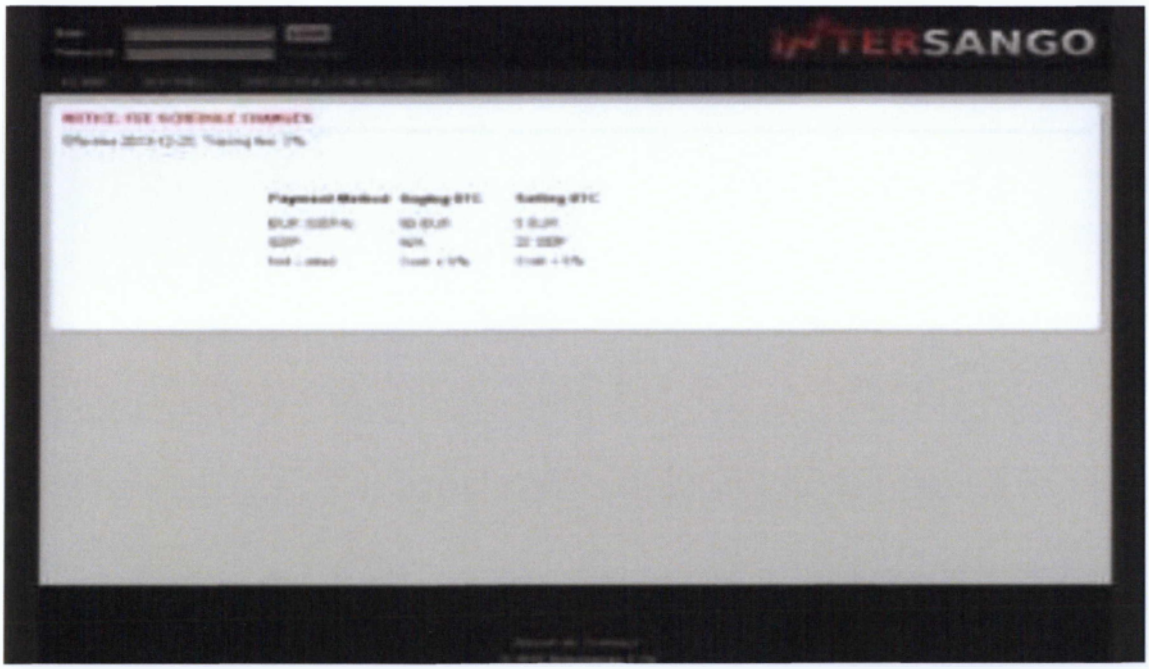
Εκτός από το Bitcoin, υπάρχουν πλέον εκατοντάδες άλλο νομίσματα που βασίζονται στην κρυπτογραφία, όπως και το Bitcoin. Για αυτό κι έχει αποδοθεί σε αυτά ο όρος κρυπτονομίσματα. Βασίζονται στην ίδια γενική ιδέα (ψηφιακά χωρίς υλική υπόσταση, με χρήση block chain, κλπ) αλλά διαφέρουν στις επιμέρους παραμέτρους (π.χ. κάθε πότε βρίσκεται ένα νέο block, πόσα νομίσματα περιέχει, πόσα θα είναι συνολικά τα νομίσματα που θα κυκλοφορήσου, ποιος είναι ο

5.5.1 Διαθέσιμα Ανταλλακτήρια BitCoins

Τα πιο διαδεδομένα ανταλλακτήρια, όπου μπορείτε ν" αγοράσετε αλλά και να πουλήσετε bitcoins είναι:

Intersango

Υποστηρίζει νομίσματα EUR, GBP, USD, PLN και φυσικά BTC. Η χρηματοδότηση και οι αναλήψεις γίνονται μέσω τραπεζικής κατάθεσης (EUR, GBP και PLN) και μέσω Dwolla (USD). Αναλυτικές πληροφορίες μπορείτε να βρείτε στη σχετική ιστοσελίδα ή στην αντίστοιχη συζήτηση. Οι αμοιβές είναι: 0,35% Maker και 0,95% Taker. Ωστόσο, οι χρεώσεις για ανάληψη αυξήθηκαν στα 10 ευρώ και το συγκεκριμένο ανταλλακτήριο δεν δέχεται πλέον νέες εγγραφές.



Εικόνα 38.Intersango

Bitcoin Central

Υποστηρίζει συναλλαγές από και προς ευρώ. Για χρήση της υπηρεσίας είναι απαραίτητο να στείλετε τα απαιτούμενα δικαιολογητικά όπως αντίγραφο

ταυτότητας, αντίγραφο δεύτερου εγγράφου ταυτοποίησης, ένα έγγραφο της τράπεζας όπου θα εμφανίζεται ο τραπεζικός σας λογαριασμός και αποδεικτικό μόνιμης κατοικίας.

Ο ιστοχώρος είναι προσβάσιμος στο: https://paymium.com/

Εικόνα 39.Bitcoin Central

Bitcoin.de

Παρέχει αγοροπωλησίες απευθείας μεταξύ χρηστών, με διασφάλιση των συναλλαγών. Ο πωλητής στέλνει τα bitcoins που θέλει να πουλήσει στην υπηρεσία. Μόλις λάβει την πληρωμή από τον αγοραστή, το καταχωρεί στο σύστημα και τότε τα νομίσματα αποστέλλονται στον αγοραστή. Χρέωση 1% επί της συναλλαγής, το οποίο επιμερίζεται εξίσου σε αγοραστή και πωλητή. Υποστηρίζει Liberty Reserve και Τραπεζικές συναλλαγές.

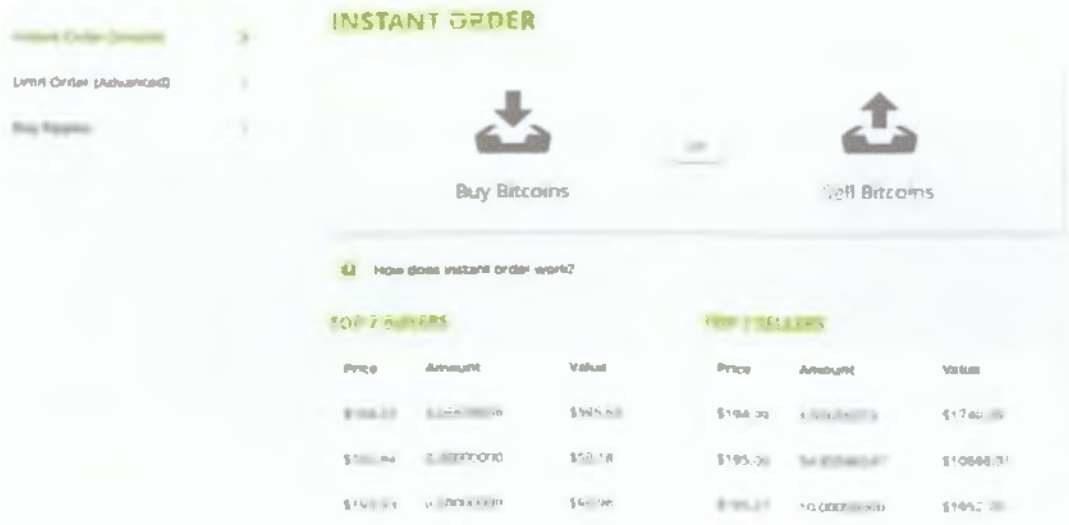
Ο ιστοχώρος είναι προσβάσιμος στο: https://www.bitcoin.de/r/m5f7u7

Εικόνα 40.Bitcoin.de

BitStamp

Κλιμακούμενες χρεώσεις συναλλαγών με μέγιστο 0,5% για μηνιαίο όγκο συναλλαγών μικρότερο των 500 δολαρίων κι ελάχιστο 0,2% για μηνιαίο όγκο συναλλαγών μεγαλύτερο των 150 χιλιάδων δολαρίων. Οι μεταφορές SEPA χρεώνονται με 0,9€ ανά εντολή με ελάχιστο ποσό εντολής τα 10 δολάρια.

Ο ιστοχώρος είναι προσβάσιμος στο: https://www.bitstamp.net/

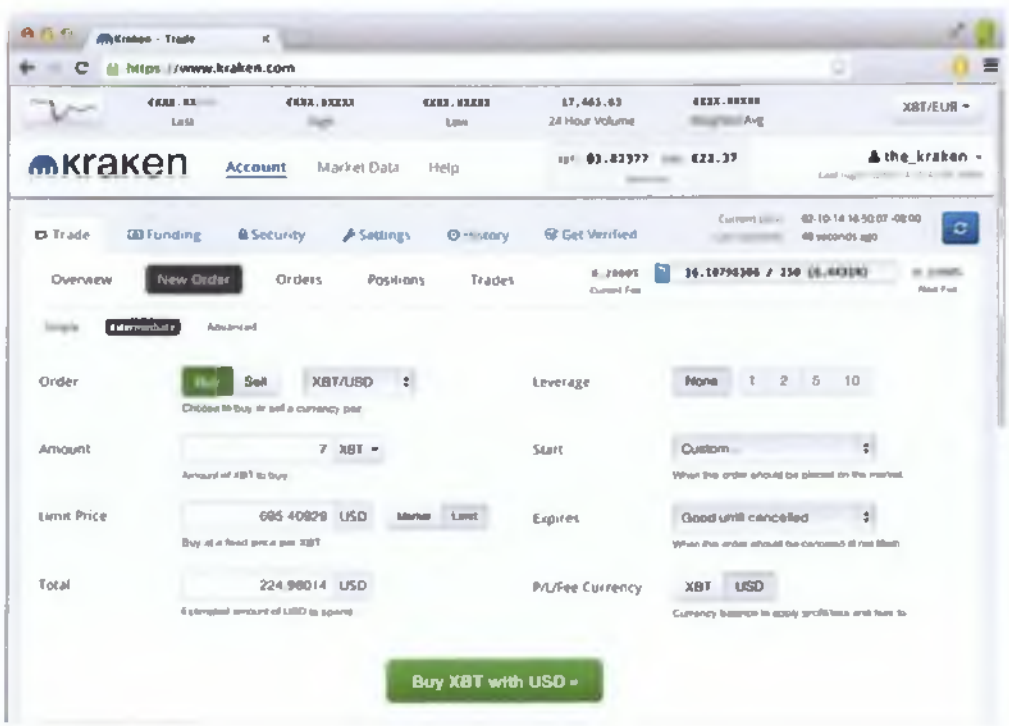


Εικόνα 41.BitStamp

Kraken

Ανταλλακτήριο διαφόρων νομισμάτων με τα περισσότερα χαρακτηριστικά. Παρέχει δυνατότητα για εντολές Market, Limt, Stop limit, Take profit, Stop loss, Take profit limit, κ.α. Ανταλλάσσει μεταξύ Ευρώ, Δολάριο, Bitcoin, Litecoin, Dogecoin, Ripple και Namecoin.

Ο ιστοχώρος είναι προσβάσιμος στο: https://www.kraken.com/



Εικόνα 42.Kraken

5.6 Ανταλλακτήρια κρυπτονομισμάτων

Εκτός από το Bitcoin, υπάρχουν πλέον εκατοντάδες άλλο νομίσματα που βασίζονται στην κρυπτογραφία, όπως και το Bitcoin. Για αυτό κι έχει αποδοθεί σε αυτά ο όρος κρυπτονομίσματα. Βασίζονται στην ίδια γενική ιδέα (ψηφιακά χωρίς υλική υπόσταση, με χρήση block chain, κλπ) αλλά διαφέρουν στις επιμέρους παραμέτρους (π.χ. κάθε πότε βρίσκεται ένα νέο block, πόσα νομίσματα περιέχει, πόσα θα είναι συνολικά τα νομίσματα που θα κυκλοφορήσου, ποιος είναι ο

αλγόριθμος κρυπτογράφησης κλπ). Αν θέλει κάποιος να πουλήσει bitcoins για ν" αγοράσει κάποιο άλλο κρυπτονόμισμα, μπορεί ν" απευθυνθεί στα ανταλλακτήρια κρυπτονομισμάτων. Παραθέτουμε μερικά παρακάτω:

- Cryptsy – Το πιο γνωστό και διαδεδομένο.
- Cryptorush
- Bter

6 Συμπεράσματα

Το κρυπτονόμισμα BitCoin, καθώς και οι «παραλλαγές» του (Namecoin, Litecoin, Peercoin, Ripple, Dogecoin, Mastercoin και Primecoin) πλέον αποτελεί ένα πολλά υποσχόμενο νόμισμα, το οποίο «κρύβει» από πίσω του μια σειρά από τεχνολογικές καινοτομίες. Το BitCoin, παρόλο που δεν διαθέτει ακόμα ολοκληρωμένη νομική και νομοθετική υπόσταση, και παρόλο τις συνεχείς «αποδοκιμασίες», κατάφερε να σταθεροποιηθεί και να ισχυροποιηθεί στην παγκόσμια χρηματιστηριακή αγορά.

Καθημερινά, η δημοτικότητα του BitCoin μεγαλώνει και μεγάλες εταιρίες - κολοσσοί αναγκάζονται να ενσωματώσουν τα κρυπτονομίσματα στους τρόπους συναλλαγών τους. Το BitCoin βασίζεται εξ' ολοκλήρου στην τεχνολογία των υπολογιστών και αυτός είναι ένας από τους λόγους που θεωρείται "εύθραυστο", καθώς έχουν σημειωθεί πολλές επιθέσεις από hackers, με αποτέλεσμα, πολλοί χρήστες να απολέσουν χιλιάδες BitCoins.

Συνοψίζοντας, το BitCoin χρειάζεται λίγα χρόνια ακόμα ώστε να «ωριμάσει» από τεχνολογικής και νομικής πλευράς. Παρόλο των προσωρινών αδυναμιών που διαθέτει, το BitCoin δύναται να κυριαρχήσει στις αγορές και ενδέχεται, σε λίγα χρόνια, μεγάλος αριθμός συναλλαγών να διεξάγονται μόνο με BitCoins.

7 Βιβλιογραφία

Ξένη Βιβλιογραφία

Davis, J., 2011. The Crypto-Currency: Bitcoin and its mysterious inventor. Εκδότης: The New Yorker, 2η Έκδοση

Dennis J, Wright M., 2013, Bitcoin Revolution: Ending Tyranny for Fun & Profit, Εκδότης: Success Council, 2η Έκδοση

Patterson S., 2013 Bitcoin Beginner: A Step By Step Guide To Buying, Selling And Investing In Bitcoins, Εκδότης: Better Life Publishers, 1η Έκδοση

Caughey M, 2013, Bitcoin Mining Step by Step, Εκδότης: Better Life Publishers, 1η Έκδοση

Smithers A., 2014, Everything you need to know about buying, selling and investing in Bitcoin, Εκδότης: A.H. Smithers

Forrester D., Solomon M., 2013, Bitcoin Explained: Today's Complete Guide to Tomorrow's Currency, Εκδότης: Grassroot Books

Rivenburgh K., 2013, Bitcoin Made Easy: The Easiest Guide to Bitcoin You Will Ever Read, Εκδότης: Rivenburgh Publishing

Rockwell E, 2013, Bitcoin For Beginners: A to Z, Step by Step Guide to Buying, Selling and Investing in Bitcoins in Plain English, Εκδότης: Rivenburgh Publishing

Bamert, T., 2013, Have a snack, pay with Bitcoins, Εκδότης: IEEE, 2013 IEEE Thirteenth International Conference on

Ελληνική Βιβλιογραφία

Ν. Κρεμμύδας, "Επισκόπηση στα Συστήματα Ομότιμων Κόμβων", Ε.Μ.Π., 2005

Computer για όλους, "Peer To Peer Computing", Αριθμός Τεύχους: 202

Ηλεκτρονική Βιβλιογραφία

http://www.oikade.gr/Children/usefull/money/i-istoria-tou-xrimatos/

http://www.monevexpert.gr/gr/Χρήμα

http://el.wikipedia.org/wiki/PayPal

http://en.kryptotel.net/ssl.html

http://searchsecurity.techtarget.com/definition/Secure-Sockets-Layer-SSL

http://www.hit.bme.hu/~buttyan/courses/BMEVIHI4372/ssl.pdf

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

https://en.bitcoin.it/wiki/Double-spending

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

http://www.dailydot.com/business/bitcoin-complete-history-timeline/

http://www.bitcoinx.com/bitcoin-mining-hardware/

https://bitcoin.org/en/developer-guide#block-chain-overview

https://www.btcgreece.com/Help/HelpPageView/what-is-bitcoin-wallet