ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΚΡΗΤΗΣ

Σχολή Διοίκησης Οικονομίας

Τμήμα Διοίκησης Επιχειρήσεων, Άγιος Νικόλαος

“ Ψηφιακά νομίσματα – Η περίπτωση Bitcoin: Τάσεις και Προοπτικές ”

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Εισηγητής: Δρ. Χρήστος Λεμονάκης

Ονοματεπώνυμο εκπονητή: Πσενιτσίνιι Ντανιήλ

Α.Μ.: 227

Άγιος Νικόλαος

2018


bitcoin
CRYPTOCURRENCY

Πρόλογος

Τα τελευταία χρόνια τα κρυπτονομίσματα και ιδιαίτερα το πιο γνωστό από αυτά, το bitcoin έχουν κάνει αισθητή τη παρουσία τους στη διεθνή οικονομική σκηνή εμφανίζοντας μπροστά μας ένα εντελώς νέο ‘’νομισματικό’’ σύστημα. Το bitcoin δεν είναι παρά ένα μόνο από τα πολλά ψηφιακά νομίσματα που έχουν δημιουργηθεί , απλά είναι το πιο παλιό και το πιο διαδεδομένο και για τον λόγο αυτό πολλές φορές η έννοια του bitcoin εκφράζει την έννοια του κρυπτονομίσματος. Η πρόοδος της τεχνολογίας οδήγησε πολλές συναλλαγές να γίνονται μέσω Διαδικτύου και επομένως καθένας μπορεί να τελειώσει τις συναλλαγές του από το σπίτι.

Παρά το γεγονός ότι πολλές εταιρείες σε όλο τον κόσμο το έχουν αποδεχθεί ως επίσημο μέσο πληρωμών - πρόκειται για ένα ψηφιακό νόμισμα που δημιουργεί ακόμη αμφιβολίες και προβληματισμούς για την αξία αλλά και την αξιοπιστία του. Για το λόγο αυτό αποτελεί σήμερα περισσότερο ένα εναλλακτικό είδος επένδυσης παρά ένα μέσο συναλλαγής. Οι αντικρουόμενες απόψεις που ακούγονται συντηρούν τη μεγάλη μεταβλητότητα της αξίας του, αλλά δεν βοηθάνε στη καθιέρωση του ως μέσο καθημερινών συναλλαγών. Σε αυτό το αποτέλεσμα συντελούν επίσης όλα τα κρούσματα απάτης που κατά καιρούς ακούγονται.

Αν όμως το μέλλον των ψηφιακών νομισμάτων δεν είναι ακόμη ξεκάθαρο η τεχνολογία που χρησιμοποιήθηκε για τη δημιουργία τους, η τεχνολογία δηλαδή της blockchain, έχει τις καλύτερες προοπτικές να εξελιχθεί στο επόμενο μεγάλο τεχνολογικό επίτευγμα και να δημιουργήσει το επόμενο Διαδίκτυο.

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: κρυπτονομίσματα, bitcoins, blockchain, ψηφιακές απάτες,συνάρτηση κατακερματισμού

Εισαγωγή

Αυτή η εργασία στοχεύει στο να προσεγγίσει τον τομέα των ψηφιακών νομισμάτων και ιδιαίτερα αυτόν του Bitcoin. Η προσέγγιση θα είναι θεωρητική, τεχνολογική και πρακτική ως αποτύπωση της κατάστασης που επικρατεί σήμερα.

Στο 1ο κεφάλαιο γίνεται μια παρουσίαση της έννοιας του ‘’κρυπτονομίσματος’’ (cryptocurrency), ο ρόλος του κρυπτονομίσματος, τα βασικά χαρακτηριστικά του, οι εφαρμογές του και ο τρόπος δημιουργίας του.

Στο 2^{ο} κεφάλαιο περιγράφονται οι αρχές και τα χαρακτηριστικά της τεχνολογίας Blockchain που χρησιμοποιείται για τη δημιουργία των λεγόμενων κρυπτονομισμάτων.

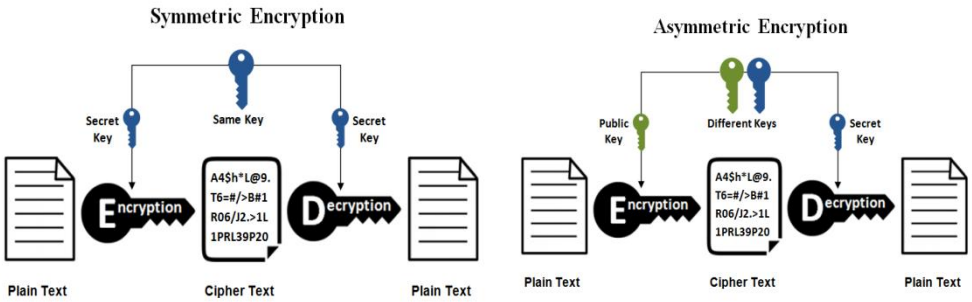
Στο 3^{ο} κεφάλαιο δίνεται πρώτα μια περιγραφή της εξελικτικής πορείας του Bitcoin, θα αναφέρουμε τα πλεονεκτήματα και τα μειονεκτήματα του, το πώς αυτό δημιουργείται και αποθηκεύεται και πως γίνονται οι συναλλαγές σε αυτό.

Στο 4^{ο} κεφάλαιο αναφέρονται οι διάφοροι τρόποι που εκδηλώνονται οι απάτες στο δίκτυο των κρυπτονομισμάτων, περιγράφονται οι βασικές τεχνικές αδυναμίες του όλου δικτύου που διευκολύνουν την εκδήλωση προσπαθειών απάτης και το πως αυτές αντιμετωπίζονται. Παρουσιάζει ενδιαφέρον να ερευνηθεί κατά πόσο τα μεγάλα

περιστατικά απάτης που έχουν επηρεάσει την εικόνα του δικτύου του Bitcoin ε΄χουν επιπτώσεις στη δυναμική των τιμών του. Τέλος, στο 5^{ο} κεφάλαιο περιγράφεται η εικόνα που η αγορά των κρυπτονομισμάτων παρουσιάζει σήμερα στην Ελλάδα, και στη συνέχεια γίνεται μια περίληψη των βασικών συμπερασμάτων από όλα τα επιμέρους κεφάλαια.

Κεφάλαιο 1ο

Η κρυπτογράφηση δεδομένων και τα cryptocurrencies



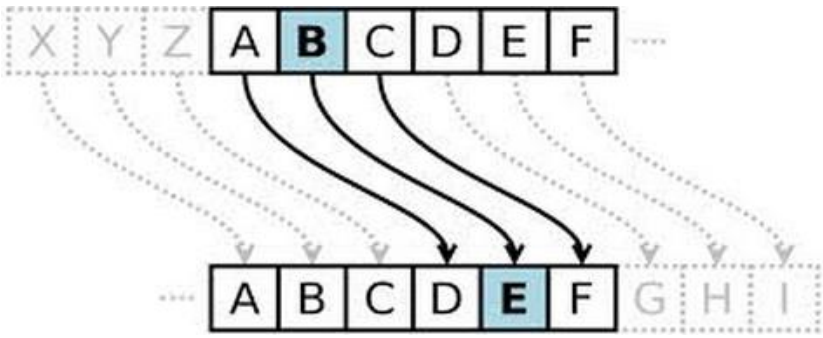
1.1 Εισαγωγή στη κρυπτογράφηση δεδομένων

Η φράση " κρυπτογράφηση δεδομένων" συνειρμικά κρύβει μέσα της μυστήριο καθώς μας έρχονται στο νού εικόνες από κατασκοπικά έργα στον κινηματογράφο. Όμως η αρχή της κρυπτογράφησης είναι στη πραγματικότητα πολύ απλή. Αφορά το πώς θα εμφανισθεί

τροποποιημένη μια πληροφορία, που μπορεί να είναι ένα σύνολο λέξεων, η μια μόνο λέξη ή αριθμός, έτσι ώστε όταν ένας τρίτος το βλέπει να μην μπορεί να το καταλάβει. Για να μπορέσει κάποιος να το διαβάσει και να το καταλάβει θα πρέπει να έχει το ‘’εργαλείο’’ (κλειδί) αποκρυπτογράφησης.

Ο τρόπος που επιλέγεται για να κρυπτογραφηθεί η πληροφορία λέγεται **αλγόριθμος κρυπτογράφησης.** Όποιος ξέρει τον αλγόριθμο κρυπτογράφησης έχει και το κλειδί της αποκρυπτογράφησης.

Από την αρχαιότητα είναι γνωστός ο αλγόριθμος Caesar cipher ή Caesar shift. Το όνομα του αλγορίθμου προέρχεται από τον Ιούλιο Καίσαρα, που χρησιμοποιούσε αυτή τη μέθοδο, σύμφωνα με τον ιστορικό Σουητώνιο, βάσει της οποίας κάθε προσπάθεια μεταβολής της μορφής της πληροφορίας στηρίζεται στην αντικατάσταση κάποιου γράμματος με το γράμμα εκείνο που βρίσκεται τρείς θέσεις πριν ή μετά από αυτό.



Με την εμφάνιση των υπολογιστών από τη μια πλευρά υπάρχει η δυνατότητα κρυπτογράφησης με τη χρήση πολύπλοκων αλγορίθμων αλλά παράλληλα υπάρχει πλέον η δυνατότητα με έναν ισχυρό υπολογιστή να αποκρυπτογραφηθεί πιο εύκολα η κάθε κρυπτογράφηση.

Η κρυπτογραφία είναι μια μέθοδος αποθήκευσης και μετάδοσης δεδομένων σε μια συγκεκριμένη μορφή, έτσι ώστε μόνο εκείνοι για τους οποίους προορίζεται να μπορούν να την διαβάσουν και να την επεξεργαστούν. Η κρυπτογραφική μέθοδος στηρίζεται στη χρήση μικροκουκίδων, τη συγχώνευση λέξεων με εικόνες και άλλους τρόπους απόκρυψης πληροφοριών κατά την αποθήκευση ή τη διακίνηση τους. Ωστόσο, με την

είσοδο του υπολογιστή στη ζωή μας, η κρυπτογραφία συνδέεται πιο πολύ με την τροποποίηση ενός κειμένου με πληροφορίες βάσει ενός κρυπτογραφήματος με τη μορφή αλγόριθμου (cypher) και στη συνέχεια την αποκρυπτογράφηση του βάσει ενός συγκεκριμένου εργαλείου αποκρυπτογράφησης. Μόνο όσοι διαθέτουν ένα μυστικό κλειδί μπορούν να αποκρυπτογραφήσουν το μήνυμα μετατρέποντας το σε απλό κείμενο. Η σύγχρονη κρυπτογραφία αναπτύχθηκε ώστε να καλύπτει τις εξής τέσσερεις ανάγκες :

Εμπιστευτικότητα: οι πληροφορίες δεν μπορούν να γίνουν κατανοητές από κανέναν εκτός από αυτόν για τον οποίο προορίζονται

Ακεραιότητα : οι πληροφορίες δεν μπορούν να μεταβληθούν κατά την αποθήκευση ή τη διακίνηση τους μεταξύ του αποστολέα και του προοριζόμενου δέκτη χωρίς να γίνει αντιληπτή η αλλοίωση

Χωρίς τη δυνατότητα αποκήρυξης : ο δημιουργός ή ο αποστολέας των πληροφοριών δεν μπορεί να αρνηθεί σε μεταγενέστερο στάδιο τη συμμετοχή του στη δημιουργία ή τη διαβίβαση των πληροφοριών

Έλεγχος ταυτότητας : Ο αποστολέας και ο παραλήπτης μπορούν να επιβεβαιώσουν την ταυτότητα του άλλου και την προέλευση ή τον προορισμό των πληροφοριών

Η κρυπτογραφία επιτρέπει επίσης στους αποστολείς και τους δέκτες να επαληθεύουν ο ένας τον άλλον μέσω της χρήσης ζεύγους κλειδιών. Υπάρχουν διάφοροι τύποι αλγορίθμων που χρησιμοποιούνται για κρυπτογράφηση και βασίζονται στη χρήση ζεύγους κλειδιών Στη τεχνολογία των υπολογιστών η κρυπτογράφηση της πληροφορίας μπορεί να γίνει με μία από τις δύο μεθόδους:

- Η συμμετρική κρυπτογράφηση με ένα κοινό κλειδί (Symmetric key encryption)
- Η ασύμμετρη κρυπτογράφηση (Public key ή Asymmetric key encryption)

Η **συμμετρική κρυπτογράφηση** είναι μια μέθοδος όπου υπάρχει ένα μυστικό κλειδί (secret key) το οποίο γνωρίζουν τόσο ο αποστολέας όσο και ο παραλήπτης. Με το κλειδί αυτό γίνεται τόσο η κρυπτογράφηση όσο και η αποκρυπτογράφηση. Παρέχει τη δυνατότητα να γίνονται με μεγάλη ταχύτητα, που μπορεί να υπερβεί τα 100Mbps, κρυπτογραφήσεις και αποκρυπτογραφήσεις. Ένα επιπλέον πλεονέκτημα της συμμετρικής κρυπτογράφησης είναι οι μικρές απαιτήσεις της σε μνήμη και υπολογιστική ισχύ (Huth, 2009).

Σε αντίθεση με την συμμετρική κρυπτογράφηση, στη κρυπτογράφηση με χρήση δημόσιου κλειδιού (PKC), ή και όπως πιο συχνά αναφέρεται **ασύμμετρη κρυπτογράφηση** καθένα από τα δύο μέρη χρησιμοποιεί ένα ζεύγος κλειδιά, ενώ υπάρχει και ένα κοινό κλειδί. Κάθε πλευρά χρησιμοποιεί το ένα από τα δύο κλειδιά που έχει για τη κρυπτογράφηση και το άλλο για την αποκρυπτογράφηση. Τα κλειδιά, αν και σχετίζονται μεταξύ τους με κάποια μαθηματική σχέση, είναι τελείως διαφοροποιημένα έτσι ώστε σε καμία περίπτωση η γνώση του ενός κλειδιού να μην μπορεί να οδηγήσει στον προσδιορισμό του άλλου κλειδιού.

Το δημόσιο κλειδί επαληθεύει ότι ο κάτοχος ενός συγκεκριμένου ιδιωτικού κλειδιού έστειλε τη πληροφορία που έχει κρυπτογραφηθεί με αυτό και την οποία μπορεί να αποκρυπτογραφήσει ο δέκτης με το δικό του ιδιωτικό κλειδί.

Στην ασύμμετρη κρυπτογράφηση μια πληροφορία που κρυπτογραφήθηκε με ένα δημόσιο κλειδί μπορεί να αποκρυπτογραφηθεί μόνο με ένα ιδιωτικό κλειδί και μια πληροφορία που κρυπτογραφήθηκε με ένα ιδιωτικό κλειδί μπορεί να αποκρυπτογραφηθεί μόνο με ένα δημόσιο κλειδί.

Το βασικό πλεονέκτημα της ασύμμετρης κρυπτογράφησης είναι η μεγάλη ασφάλεια που δημιουργείται. Πόσο σημαντικό είναι αυτό το χαρακτηριστικό φαίνεται από το εξής παράδειγμα.

Ο πρώτος σημαντικός αλγόριθμος που χρησιμοποιήθηκε για την κρυπτογράφηση μέσω υπολογιστή πληροφοριών και δεδομένων ήταν ο Data Encryption Standard (DES) που αναπτύχθηκε από την IBM αρχές της δεκαετίας του 70. Ο DES χρησιμοποιεί ένα κλειδί μήκους 56-bit, με το οποίο μπορεί να πραγματοποιήσει πάνω από 72 τετράκις εκατομμύρια πιθανούς συνδυασμούς (ο ακριβής αριθμός είναι 72.057.594.037.927.936, Αν και ο αριθμός αυτός ακούγεται εντυπωσιακά υψηλός, το 1998 δημιουργήθηκε η συσκευή EFF DES cracker ("Deep Crack"), με ειδικά κατασκευασμένα τσιπάκια, που επέτρεπαν σε έναν υπολογιστή να δοκιμάσει 90 δισεκατομμύρια κλειδιά το δευτερόλεπτο. Αν και θεωρητικά θα χρειαζόταν 9 ημέρες για να δοκιμάσει κάθε πιθανό συνδυασμό στη πράξη ο Deep Crack κατάφερε να σπάσει τον DES σε δύο ξεχωριστά τεστ, στο πρώτο σε 56 ώρες και στο δεύτερο σε 22 ώρες, αποδεικνύοντας πως ο συγκεκριμένος αλγόριθμος είναι ανεπαρκής για την κρυπτογράφηση δεδομένων σε πραγματικές συνθήκες (Κυρίτσης, 2016).

Σήμερα οι αλγόριθμοι που χρησιμοποιούνται διαθέτουν κλειδιά 128, 192 ή 256 bit. Ένα κλειδί 128-bit μπορεί να έχει πάνω από 300 δεκάκις εκατομμύρια πιθανούς συνδυασμούς. Ο μεγαλύτερος υπερυπολογιστής αυτή τη στιγμή στον κόσμο, που μπορεί να εκτελέσει 33,86 petaflop/s (τετράκις εκατομμύρια υπολογισμούς το δευτερόλεπτο) και θα μπορούσε θεωρητικά να σπάσει τον DES σε 2 δευτερόλεπτα, θα χρειαζόταν περίπου 250 δισεκατομμύρια χρόνια για να ελέγξει όλους τους συνδυασμούς του AES-128

Είναι υπολογιστικά ανέφικτο να υπολογιστεί το ιδιωτικό κλειδί με βάση το δημόσιο κλειδί. Εξαιτίας αυτού, τα δημόσια κλειδιά μπορούν να μοιραστούν ελεύθερα, επιτρέποντας στους χρήστες μια εύκολη και βολική μέθοδο κρυπτογράφησης περιεχομένου και επαλήθευσης ψηφιακών υπογραφών, ενώ τα ιδιωτικά κλειδιά μπορούν να παραμείνουν μυστικά, εξασφαλίζοντας ότι μόνο οι ιδιοκτήτες τους μπορούν να αποκρυπτογραφήσουν το περιεχόμενο και να δημιουργήσουν ψηφιακές υπογραφές.

Δεδομένου ότι τα δημόσια κλειδιά πρέπει να μοιράζονται αλλά είναι πολύ μεγάλα για να τα θυμάται κάποιος εύκολα, αποθηκεύονται σε ψηφιακά πιστοποιητικά για ασφαλή μεταφορά και κοινή χρήση. Αντίθετα, τα ιδιωτικά κλειδιά δεν μοιράζονται, απλώς αποθηκεύονται στο λογισμικό ή στο λειτουργικό σύστημα που κάποιος χρησιμοποιεί ή σε κάποιο εξωτερικό αποθηκευτικό μέσο που περιέχει προγράμματα οδήγησης που επιτρέπει τη χρήση τους στο λογισμικό που χρησιμοποιείται.

Η κρυπτογραφία συμμετρικού κλειδιού καλείται μερικές φορές κρυπτογράφηση μυστικού κλειδιού. Το πιο δημοφιλές σύστημα συμμετρικού κλειδιού είναι το πρότυπο κρυπτογράφησης δεδομένων (DES).

Σήμερα στη προσπάθεια να συνδυασθούν ασφάλεια και ταχύτητα χρησιμοποιείται η μικτή κρυπτογράφηση. Σε αυτήν μεταφέρονται με την ασύμμετρη κρυπτογράφηση μικρά μπλοκ δεδομένων, συνήθως το δημόσιο κλειδί, και στη συνέχεια χρησιμοποιείται το δημόσιο κλειδί για την συμμετρική κρυπτογράφηση της πληροφορίας.

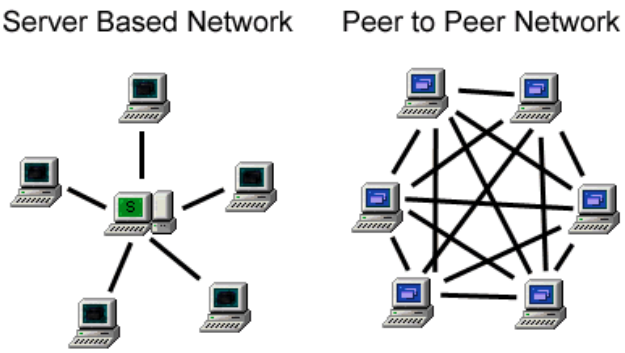
1.2 Τι είναι τα κρυπτονομίσματα

Το ακαδημαϊκό ενδιαφέρον για την έννοια του κρυπτονομίσματος είναι πολύ πρόσφατο καθώς τα πρώτα άρθρα σχετικά με το κρυπτονόμισμα εμφανίσθηκαν μόλις το 2011. Ως εκ τούτου δεν υπάρχει ακόμη κάποιος ορισμός του όρου που έχει δοθεί και έχει γίνει κοινά αποδεκτός.

Μπορούμε να πούμε ότι τα ψηφιακά νομίσματα ή κρυπτονομίσματα (cryptocurrencies) είναι ηλεκτρονικά χρήματα που δημιουργούνται με κρυπτογραφικές διαδικασίες και το λογισμικό τους είναι ανοικτού κώδικα.

Ο ορισμός του όρου ‘’κρυπτονόμισμα’’ (cryptocurrency) στην Wikipedia μας εμφανίζει μια σειρά από όρους, αρχικά, ελάχιστα κατανοητούς που όμως θα δούμε ότι περιγράφουν με σαφήνεια την έννοια του κρυπτονομίσματος. Σύμφωνα λοιπόν με τη Wikipedia ‘’το κρυπτονόμισμα είναι μία peer-to-peer αποκεντρωμένη ηλεκτρονική μορφή χρήματος η οποία βασίζεται πάνω στις αρχές της κρυπτογραφίας για την διασφάλιση του δικτύου και την επαλήθευση των συναλλαγών’’.

Σε ένα δίκτυο P2P, οι "συνομόλογοι" είναι συστήματα υπολογιστών που συνδέονται μεταξύ τους μέσω του Διαδικτύου. Τα αρχεία μπορούν να μοιράζονται απευθείας μεταξύ των συστημάτων στο δίκτυο χωρίς την ανάγκη κεντρικού διακομιστή. Με άλλα λόγια, κάθε υπολογιστής σε δίκτυο P2P γίνεται ταυτόχρονα διακομιστής αρχείων καθώς και πελάτης. Οι μόνες απαιτήσεις για έναν υπολογιστή που συμμετέχει σε ένα δίκτυο peer-to-peer είναι μια σύνδεση στο Internet και ένα λογισμικό P2P.



Εικόνα 1.1 η εικόνα δείχνει τη διαφορά μεταξύ ενός δικτύου P2P και ενός Server based δικτύου (πηγή: Computer Fluency)

Σε ένα δίκτυο υπολογιστών ως πόροι ορίζονται το σύνολο των κόμβων οι οποίοι είναι συνδεδεμένοι με γραμμές επικοινωνίας ώστε να επιτρέπεται η ανταλλαγή των δεδομένων (τερματικά, εκτυπωτές, servers). Καθώς επομένως υπάρχει συντονισμός των κόμβων, οι συναλλαγές που γίνονται μεταφέρονται από τον ένα κόμβο στον άλλο, ενώ ταυτόχρονα γίνεται και η επαλήθευση της μεταφοράς μεταξύ των κόμβων (Ahamad, Nair, & Varghese, 2013).

Σύμφωνα με έναν άλλο σχεδόν ισοδύναμο ορισμό "ένα κρυπτονόμισμα είναι ένας τύπος ψηφιακού νομίσματος που βασίζεται στην κρυπτογραφία, και μπορεί να μεταφερθεί

άμεσα και με ασφάλεια, χωρίς να χρειάζεται κάποιος αξιόπιστος τρίτος, μεταξύ οποιωνδήποτε δύο μερών, χρησιμοποιώντας την υποδομή και τη κρυπτογραφημένη ασφάλεια του Διαδικτύου. Η αξία ενός κρυπτονομίσματος δεν υποστηρίζεται από οποιαδήποτε κυβέρνηση ή οργανισμό "(Ametrano, 2014).

Μια διαφορετική προσέγγιση στην έννοια του cryptocurrency δίνεται με τον ακόλουθο ορισμό που λέει ότι "ένα cryptocurrency είναι ένα σύγχρονο ψηφιακό μέσο ανταλλαγής με ομότιμους χρήστες. Πρόκειται για ένα νέο αποκεντρωμένο, και περιορισμένο σύστημα πληρωμής καθώς ενώ μπορούν θεωρητικά να δημιουργηθούν πολλές νέες μονάδες νομίσματος το συνολικό ποσό είναι περιορισμένο''

Ενώ τα συμβατικά νομίσματα διέπονται από κεντρικές αρχές που καθορίζουν την ισοτιμία τους, τα cryptocurrencies βασίζονται σε ένα αποκεντρωμένο χρηματοπιστωτικό σύστημα. Καθώς λοιπόν δεν υπάρχει κάποιος επίσημος έλεγχος που παρακολουθεί και διαμορφώνει την αξία τους, όπως γίνεται στις μεγάλες χρηματαγορές με τα συμβατικά νομίσματα, οι τιμές των ψηφιακών νομισμάτων έχουν μεγάλη μεταβλητότητα όχι από μέρα σε μέρα αλλά και από λεπτό σε λεπτό (Franco, 2014).

Ταυτόχρονα, όλο και περισσότεροι άνθρωποι επιθυμούν να αποκτήσουν ένα ποσό από αυτά τα ηλεκτρονικά χρήματα. Ένας σημαντικός λόγος είναι πως αυτά τα νομίσματα δεν υπόκεινται σε κρατικό έλεγχο, από τη στιγμή που καμία χώρα ή οργανισμός δεν τα ελέγχει.

Ο πιο βασικός όμως λόγος της εξέλιξης στον τομέα των κρυπτονομισμάτων είναι το γεγονός ότι παρουσιάζουν εμφανή πλεονεκτήματα στον τομέα της διενέργειας των χρηματοπιστωτικών συναλλαγών. Τα πιο σοβαρά από τα πλεονεκτήματα αυτά είναι το πλήρως αποκεντρωμένο σύστημα συναλλαγών μεταξύ ισότιμων παρόχων, η εξάλειψη των κινδύνων της αδικαιολόγητης χρέωσης, το χαμηλότερο κόστος συναλλαγών, το αυξημένο επίπεδο ασφάλειας, η μεγαλύτερη ευκολία στη χρήση και η πλήρης υποστήριξη για τα κινητά (Grinberg, 2011)

1.3 Πώς δημιουργούνται τα κρυπτονομίσματα

Όλα τα cryptocurrencies χρησιμοποιούν τη κρυπτογραφική μέθοδο για να ελέγχουν κάθε στιγμή τόσο τη δημιουργία όσο και τη μεταβίβαση των ποσών που επιλέγονται και δημιουργούνται με την δράση ενός κρυπτογραφημένου κλειδιού, που λειτουργεί όπως ακριβώς μια ηλεκτρονική υπογραφή. Το κλειδί αυτό αποτελείται από ένα δημόσιο και

ένα ιδιωτικό μέρος. Τα κρυπτονομίσματα βασίζονται δηλαδή στην ύπαρξη ενός ζεύγους κλειδιών στο οποίο τα κλειδιά, αν και σχετίζονται μεταξύ τους με κάποια μαθηματική σχέση, είναι αρκετά διαφοροποιημένα μεταξύ τους ώστε η γνώση του ενός να μην επιτρέπει τη παραγωγή ή τη γνώση του άλλου. Από τα κλειδιά αυτά το ένα μπορεί να είναι ευρέως γνωστό , για το λόγο αυτό λέγεται και δημόσιο (public key), και χρησιμοποιείται για τη κρυπτογράφηση των δεδομένων. Το άλλο κλειδί, που είναι υποχρεωτικό να είναι ιδιωτικό (private key) χρησιμοποιείται για την αποκρυπτογράφηση των δεδομένων. Ο συνδυασμός των δύο κλειδιών, δημόσιο και ιδιωτικό είναι αυτός που κάνει τα κρυπτονομίσματα , όπως τα Bitcoins, ασφαλή (Wiatr, 2014).

Ένα ‘’πορτοφόλι’’ κρυπτονομίσματος αποθηκεύει ηλεκτρονικά δεδομένα από τα δημόσια και ιδιωτικά κλειδιά που μπορούν να χρησιμοποιηθούν για να λαμβάνουν ή να ξοδεύουν κρυπτονομίσματα.

Όταν εκτελείται μια συναλλαγή παύει να ισχύει το κλειδί του αποστολέα και εμφανίζεται ένα νέο κλειδί για τον παραλήπτη.

Όλα αυτά καταγράφονται, με τη βοήθεια όπως θα δούμε στη συνέχεια της τεχνολογίας Blockchain σε ένα αρχείο καταγραφών ώστε να εξασφαλίζεται η μοναδικότητα τους (Franco, 2014)

Τα περισσότερα κρυπτονομίσματα κάνουν χρήση μιας κατανεμημένης Βάσης Δεδομένων που αποτελεί τον κορμό του συστήματος τους. Αυτή η Βάση Δεδομένων ονομάζεται Blockchain. Η τεχνολογία Blockchain δημιουργεί μια αλυσίδα στοιχείων συνδεδεμένων μεταξύ τους. Στη περίπτωση ενός cryptocurrency οι συναλλαγές που γίνονται με αυτό καταχωρούνται σε μια λίστα εγγραφών που είναι ορατή δημοσίως. Οι καταχωρήσεις αυτές ομαδοποιούνται δημιουργώντας τα αντίστοιχα ‘’block’’ Τα blocks αυτά συνδέονται μεταξύ τους και με τον τρόπο αυτό δημιουργείτσαι τελικά μια αλληλουχία (αλυσίδα) blocks, η οποία ονομάζεται **blockchain.**

Το λογιστικό έγγραφο (ledger) που έχει δημιουργηθεί λειτουργεί ως ένα αποκεντρωμένο (decentralized) έγγραφο καταγραφών που λόγω της ορατής από όλους μορφής του μπορεί να κρατηθεί από καθένα ως απόδειξη των συναλλαγών προσφέροντας σε αυτές ασφάλεια και διαφάνεια. Αν και το έγγραφο καταγραφών μοιάζει με ένα συνηθισμένο λογιστικό φύλο του excel παρουσιάζει μια σημαντική διαφορά από αυτό καθώς αυτό δεν βρίσκεται σε ένα συγκεκριμένο σημείο καταχωρημένο, αλλά σε εκατομμύρια χρήστες ταυτόχρονα, που έχουν άμεση πρόσβαση στα δεδομένα του. Το γεγονός αυτό της δημόσιας

πρόσβασης αποτελεί τη βασική προϋπόθεση για τη διαφάνεια που υπάρχει στις συναλλαγές.

1.4 Ο ρόλος του ‘’κρυπτονομίσματος’’

Η βασική ιδέα πίσω από ένα ‘’κρυπτονόμισμα’’ είναι να προσφέρει έναν γρήγορο τρόπο μεταφοράς κεφαλαίων σε παγκόσμιο επίπεδο, ανεξάρτητο από κάποιο τρίτο μέρος (τράπεζα) για τη διαχείριση των συναλλαγών, με ελάχιστα έξοδα συναλλαγής και με επαρκή ιδιωτικότητα (δηλαδή τόσο ο αποστολέας όσο και ο παραλήπτης των συναλλαγών να παραμένουν ανώνυμοι). Οι συναλλαγές που γίνονται με Bitcoins και άλλα κρυπτονομίσματα είναι μη αναστρέψιμες, και με τον τρόπο αυτό ο αποδέκτης των κεφαλαίων είναι σίγουρος ότι κατέχει τα κεφάλαια με σιγουριά και επομένως δεν υπεισέρχεται τόσο ο παράγοντας της εμπιστοσύνης και η ανάγκη να επιβεβαιώνεται πρώτα ότι το άλλο μέρος της συναλλαγής είναι αξιόπιστο. Αν ο παραλήπτης λάβει τα κεφάλαια, αυτά δεν μπορούν να χρεωθούν πάλι.

Δεδομένου ότι το σύστημα είναι αποκεντρωμένο και τα χρήματα υπάρχουν μόνο εικονικά, απαιτείται να υπάρχει μόνο ένα σύστημα για να παρακολουθείται ποιος είναι κάθε φορά ο νόμιμος ιδιοκτήτης του εικονικού νομίσματος και για να αποφευχθεί η πιθανότητα δαπάνης των ίδιων χρημάτων δύο φορές (double spending attack) (Nakamoto, 2008). Το 2008 ο Satoshi Nakamoto πρότεινε την ιδέα της χρήσης μιας αλυσίδας ψηφιακών υπογραφών που βεβαιώνουν τη κάθε συναλλαγή. Η αλυσίδα αυτή επιτρέπει στους χρήστες να επαληθεύσουν τις συναλλαγές επαληθεύοντας μόνο τις υπογραφές. Ωστόσο, λόγω του ότι δεν υπάρχει κεντρική αρχή στο σύστημα, ο μόνος τρόπος για να επιβεβαιώσουμε ότι ένα κρυπτονόμισμα έχει δαπανηθεί μόνο μία φορά είναι να γνωρίζει κάποιος όλες τις συναλλαγές. Για να επιτευχθεί αυτό, όλες οι συναλλαγές είναι σε δημόσια χρήση και καταγράφονται σε μια θέση όπου κάθε συναλλαγή ‘’αλυσσοδένεται’’ ηλεκτρονικά με τη προηγούμενη (blockchain technology). Αν επομένως κάποιος είναι βέβαιος ότι μια αλυσίδα μπλοκ είναι σωστή, λόγω της αλυσιδωτής σύνδεσης των συναλλαγών θεωρούνται σωστές όλες οι συναλλαγές που υπάρχουν σε αυτήν.

Οι λεγόμενοι ‘’εξορύκτες’’ (miners) είναι χρήστες που χρησιμοποιούν την ισχύ του υπολογιστή τους για να κρυπτογραφήσουν όλες τις συναλλαγές σε μια αλυσίδα μπλοκ , ενημερώνοντας για το γεγονός αυτό όλο το δίκτυο Bitcoin. Με την επίλυση ενός υπολογιστικά δύσκολου προβλήματος,’’αποδεικνύουν’’, ότι επεξεργάστηκαν νόμιμα τη

συναλλαγή που καταγράφηκε στη blockchain (Babaioff, Dobzinski, Oren, & Zohar, 2012). Αυτή η πρακτική ονομάζεται ‘’απόδειξη της εργασίας’’ (proof of work) και διαμορφώνεται έτσι ώστε να είναι δύσκολο να επιλυθεί, δηλαδή είναι για τον ‘’εξορύκτη’’ μια δαπανηρή ή χρονοβόρα προσπάθεια , όσο κι αν είναι ασήμαντη υπόθεση η επαλήθευση της από άλλους για να διαπιστωθεί αν ο ‘’εξορύκτης’’ ο έχει πράγματι καταβάλει την απαιτούμενη προσπάθεια.

Αυτή η έννοια της ‘’απόδειξης της εργασίας’’ είναι απαραίτητη για το κρυπτονόμισμα επειδή εγγυάται την ακεραιότητα της αλυσίδας μπλοκ. Ένας εισβολέας στο σύστημα δεν αρκεί απλά να αλλάξει μια συναλλαγή σε ένα μπλοκ, θα πρέπει να αλλάξει ολόκληρη την blockchain από το σημείο που έγινε αυτή η συναλλαγή και, συνεπώς, χρειάζεται να ξανακάνει όλη τη δουλειά από την αρχή. Αν η ισχύς επεξεργασίας του δικτύου αυξάνεται (αν δηλαδή προστίθενται στο σύστημα νέοι υπολογιστές από νέους χρήστες) , αυξάνεται ανάλογα και η δυσκολία ανεύρεσης ενός μπλοκ. Αυτό γίνεται για να υπάρχει η βεβαιότητα ότι αν συμμετέχουν περισσότεροι υπολογιστές στο δίκτυο εξόρυξης η ποσότητα των blocks που μπορούν να παραχθούν ανά μονάδα χρόνου παραμένει η ίδια. Ως εκ τούτου, όσο μεγαλύτερη είναι η ισχύς επεξεργασίας του δικτύου, τόσο μεγαλύτερη είναι η δυσκολία και τόσο μεγαλύτερη είναι η ασφάλεια που παρέχει το σύστημα.

Εξαιτίας αυτής της εξάρτησης που υπάρχει οι ‘’εξορύκτες’’ ανταμείβονται για τις υπολογιστικές τους προσπάθειες. Κάθε φορά που ένας ανθρακωρύχος είναι ο πρώτος στην "δημιουργία" ενός νέου μπλοκ μιας blockchain, δημιουργείται μια προκαθορισμένη ποσότητα bitcoins που έρχεται στη κατοχή του. Δεδομένου ότι δεν υπάρχουν bitcoins

που εκδίδονται από μια κεντρική αρχή, η διαδικασία αυτή αποτελεί και τον μόνο τρόπο με τον οποίο τα bitcoins μπαίνουν στην κυκλοφορία. Αυτό όμως δεν σημαίνει ότι υπάρχει ένας άπειρος αριθμός bitcoins που εξορύσσονται. Λόγω των προδιαγραφών του πρωτοκόλλου Bitcoin μειώνεται εκθετικά ο αριθμός των bitcoins που κερδίζονται ανά μπλοκ εξόρυξης, με αποτέλεσμα να φτάνουν συνολικά τα 21 εκατομμύρια bitcoins σε κυκλοφορία. Κάθε ένα από αυτά τα bitcoins όμως διαιρείται σε 100 εκατομμύρια μονάδες που οδηγούν σε μια σχεδόν άπειρη ποσότητα τεμαχίων bitcoin σε κυκλοφορία.

1.5 Τα χαρακτηριστικά των ‘’κρυπτονομισμάτων’’

Υπάρχουν πολλοί διαφορετικοί τύποι κρυπτονομισμάτων και οι διαφοροποιήσεις που υπάρχουν μεταξύ τους μπορούν να φανούν σε μερικούς μόνο κύριους τομείς.

Σε αυτή την ενότητα θα περιγραφούν με συντομία τα πιο σημαντικά χαρακτηριστικά του ‘’Κρυπτονομίσματος’’.

Ξεκινώντας πρέπει να επισημάνουμε ότι όλα τα κρυπτονομίσματα έχουν το Bitcoin ως βάση για το σχεδιασμό τους, εξ ου και τους έχει δοθεί το όνομα "alt-coins ".

1.5.1 Η χρήση αλγορίθμων

Όλα τα Cryptocurrencies χρησιμοποιούν έναν συγκεκριμένο αλγόριθμο για τη λεγόμενη λειτουργία "proof-of-work" που χρησιμεύει στην εξασφάλιση της blockchain. Η πρώτη γενιά κρυπτονομισμάτων χρησιμοποίησε σε όλα τον αλγόριθμο SHA-256, ωστόσο πολλά νέα κρυπτονομίσματα που έχουν κυκλοφορήσει μεταγενέστερα έχουν μεταπηδήσει σε διαφορετικούς αλγόριθμους όπως ο Scrypt ή ο SHA-3. Αυτή η αλλαγή έχει γίνει για να κρατήσει την δραστηριότητα της εξόρυξης χωρίς αλλαγές. Το 2013 ένας εξειδικευμένος εξοπλισμός εξόρυξης, που ονομάσθηκε ASIC, εμφανίσθηκε στην αγορά έχοντας πολύ καλά αποτελέσματα στην εξόρυξη των νομισμάτων που βασίζονται στον αλγόριθμο εξόρυξης SHA-256 όπως είναι το bitcoin. Η αποτελεσματικότητα του έβγαλε εκτός παιγνιδιού όλους τους ερασιτέχνες εξορύκτες. Επομένως η εμφάνιση νέων αλγορίθμων ουσιαστικά αποκατέστησε την ισορροπία καθώς τα κρυπτονομίσματα που δημιουργούνται με τους νέους αλγόριθμους δεν μπορούν να εξορυχθούν από αυτούς τους εξειδικευμένους αλγόριθμους ASIC. Σήμερα πλέον υπάρχει μια συνεχής μάχη μεταξύ των κατασκευαστών κρυπτονομισμάτων και των κατασκευαστών εξειδικευμένου εξοπλισμού εξόρυξης και η κατάσταση συνεχώς αλλάζει και έχουν ήδη κυκλοφορήσει στην αγορά νέα συστήματα εξόρυξης ASIC για Scrypt. (M. B. Taylor, 2013)

1.5.2 Χρόνοι δημιουργίας μπλοκ και ποσότητα διαθέσιμη ανά μπλοκ

Ένα άλλο χαρακτηριστικό των cryptocurrencies είναι ο χρόνος παραγωγής μπλοκ και η ανταμοιβή που δίνεται με τη δημιουργία του κάθε μπλοκ. βραβείο ανά μπλοκ. Για παράδειγμα, το bitcoin έχει ένα χρόνο δημιουργίας μπλοκ 10 λεπτά, πράγμα που σημαίνει ότι κάθε 10 λεπτά εμφανίζεται ένα μπλοκ. Τη στιγμή της εμφάνισης ενός μπλοκ δημιουργούνται και 25 bitcoins. Αυτό σημαίνει ότι ο συνδυασμός του χρόνου δημιουργίας μπλοκ και της διάθεσης των bitcoins ανά μπλοκ καθορίζει πόσο γρήγορα η προσφορά νομισμάτων μεγαλώνει. Αν ο χρόνος δημιουργίας μπλοκ είναι πολύ χαμηλός ή η διάθεση bitcoins ανά μπλοκ είναι πολύ υψηλή, η προσφορά νομισμάτων θα αυξηθεί γρηγορότερα.

Ο χρόνος δημιουργίας του μπλοκ έχει επίσης αντίκτυπο στην επιβεβαίωση των συναλλαγών. Μόνο μετά από μια συναλλαγή που περιλαμβάνεται σε ένα παραγόμενο μπλοκ αυτό ονομάζεται "επιβεβαιωμένο". Αυτό σημαίνει ότι οι μικρότεροι χρόνοι δημιουργίας μπλοκ θα οδηγήσουν ταυτόχρονα και σε μικρότερο χρονικό διάστημα έως την επιβεβαίωση μιας συναλλαγής. Ωστόσο, οι σύντομοι χρόνοι δημιουργίας μπλοκ συνεπάγονται ότι η πιθανότητα εξόρυξης ενός ‘’ορφανού‘’ μπλοκ αυξάνεται. Ένα ‘’ορφανό’’ μπλοκ είναι όταν δύο εξορύκτες βρίσκουν ένα νέο μπλοκ

ταυτόχρονα ανεξάρτητα ο ένας από τον άλλο. Μόνο ένα από αυτά τα δύο μπλοκ θα καταλήξει στην αλυσίδα μπλοκ και θα χρησιμοποιηθεί ενώ το άλλο θα αχρηστευθεί. Στη

περίπτωση αυτή υπάρχει μια βεβαιωμένη σπατάλη εξορυκτικού αποτελέσματος.

1.5.3 Συνολική ποσότητα νομισμάτων

Μία από τις πιο σημαντικές λεπτομέρειες που χαρακτηρίζουν ένα κρυπτονόμισμα είναι η συνολική ποσότητα των κερμάτων που δημιουργούνται τελικά. Για το bitcoin αυτή η ποσότητα είναι 21 εκατομμύρια νομίσματα ενώ για το litecoin είναι 84 εκατομμύρια. Για πολλά νομίσματα αυτή η ποσότητα είναι σταθερή, υπάρχουν ωστόσο και κρυπτονομίσματα στα οποία δεν έχει καθοριστεί η συνολική ποσότητα των κυκλοφορούντων νομισμάτων. Για παράδειγμα, το dogecoin έχει μια συνολική ποσότητα 99 δισεκατομμυρίων νομισμάτων με 5 δισεκατομμύρια νομίσματα που προστίθενται κάθε χρόνο. Έτσι ακόμα κι αν δεν υπάρχει συνολική πεπερασμένη ποσότητα νομισμάτων, η τελική προμήθεια νομισμάτων μπορεί να είναι προβλέψιμη.

Η συνολική προσφορά κρυπτονομισμάτων είναι ένας καθοριστικός παράγοντας διαμόρφωσης της τιμής τους, και σήμερα υπάρχουν μόνο λίγα alt-coins που έχουν αξία κάποιες εκατοντάδες δολαρίων, ενώ αντίθετα υπάρχουν κρυπτονομίσματα, όπως το dogecoin που λόγω του μεγάλου αριθμού νομισμάτων που υπάρχουν έχει αξία ίση με λίγα μόνο χιλιοστά του δολαρίου.

Κεφάλαιο 2ο

Η Τεχνολογία Blockchain

2.1 Τα βασικά χαρακτηριστικά της κρυπτογράφησης

Για να υπάρχει μια συνέχεια επαναλαμβάνουμε τη λογική από την οποία κυριαρχείται η μέθοδος της κρυπτογράφησης.

Η κρυπτογραφία είναι μια μέθοδος αποθήκευσης και μετάδοσης δεδομένων σε μια συγκεκριμένη μορφή, έτσι ώστε να είναι ορατή και επεξεργάσιμη μόνο από εκείνους για τους οποίους προορίζεται. Ωστόσο, με την είσοδο του υπολογιστή στη ζωή μας, η

κρυπτογραφία συνδέεται πιο πολύ με την τροποποίηση ενός κειμένου με πληροφορίες βάσει ενός κρυπτογραφήματος με τη μορφή αλγόριθμου (cypher) και στη συνέχεια την αποκρυπτογράφηση του βάσει ενός συγκεκριμένου εργαλείου αποκρυπτογράφησης. Μόνο όσοι διαθέτουν ένα μυστικό κλειδί μπορούν να αποκρυπτογραφήσουν το μήνυμα μετατρέποντας το σε απλό κείμενο.

Υπάρχουν διάφοροι τύποι αλγορίθμων που χρησιμοποιούνται για κρυπτογράφηση και βασίζονται στη χρήση ζεύγους κλειδιών με πιο συνήθεις εκείνους που περιλαμβάνουν:

Κρυπτογραφία βάσει μυστικού κλειδιού (SKC) : χρησιμοποιείται μόνο ένα κλειδί τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση (συμμετρική κρυπτογράφηση).

Κρυπτογραφία με χρήση δημόσιου κλειδιού (PKC): στη μέθοδο αυτή χρησιμοποιούνται δύο κλειδιά. Αυτός ο τύπος κρυπτογράφησης ονομάζεται επίσης ασύμμετρη κρυπτογράφηση. Ένα κλειδί είναι το δημόσιο κλειδί δηλαδή ένα κλειδί του οποίου η ηλεκτρονική ταυτότητα είναι γνωστή και στα δύο μέρη. Το άλλο κλειδί είναι το ιδιωτικό κλειδί και μόνο ο ιδιοκτήτης του έχει πρόσβαση σε αυτό. Ο αποστολέας κρυπτογραφεί τις πληροφορίες χρησιμοποιώντας το δημόσιο κλειδί του δέκτη. Ο δέκτης αποκρυπτογραφεί το μήνυμα χρησιμοποιώντας το ιδιωτικό του κλειδί.

2.2 Η έννοια της συνάρτησης κατακερματισμού (Hash Function)

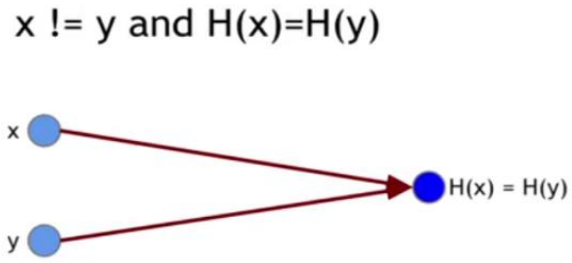
Η έννοια της κρυπτογράφησης μπορεί να επεκταθεί ώστε να συμπεριλάβει

Hash Functions: Αυτές είναι διαφορετικές από SKC και PKC. Δεν έχουν καθόλου κλειδί και ονομάζονται επίσης **μονόδρομες κρυπτογραφήσεις**. Οι λειτουργίες Hash χρησιμοποιούνται κυρίως για να διασφαλιστεί ότι ένα αρχείο παρέμεινε αμετάβλητο κατά τη διακίνηση του.

Μια **κρυπτογραφική συνάρτηση κατακερματισμού (Hash Function)** όπως είναι η πλήρης ονομασία τους δεν είναι παρά μια συνάρτηση, δηλαδή μια μαθηματική σχέση που μπορεί να πάρει ως είσοδο (το μήνυμα) ένα δεδομένο τυχαίου μεγέθους , και να το μετατρέψει σε ένα ακέραιο, μια αλφανουμερική ακολουθία δηλαδή, σταθερού μεγέθους στην έξοδο (το πιο συνηθισμένο μέγεθος είναι μια έξοδος 256 bits). Η έξοδος αυτή είναι γνωστή με τις ονομασίες 'hash value', 'message digest', 'digital fingerprint', ή 'checksum'.

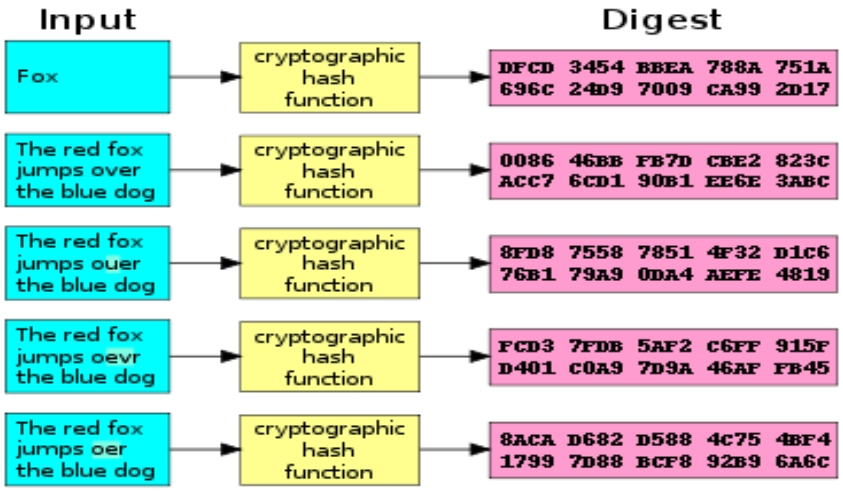
Μια Hash Function έχει τις εξής τρείς βασικές ιδιότητες που τη καθιστούν ιδιαίτερα χρήσιμη :

- μπορεί να υπολογιστεί πολύ εύκολα μέσω H/Y, πράγμα που σημαίνει ότι μέσα σε ένα λογικό χρονικό διάστημα, μπορεί κανείς να προσδιορίσει ποιό θα είναι το αποτέλεσμα που θα προκύψει (Hash function).
- είναι εξαιρετικά δύσκολο να προσδιορίσει κάποιος τη συμβολοσειρά εισόδου γνωρίζοντας μια συγκεκριμένη hash value
- είναι απίθανο να έχουν δύο μηνύματα εισόδου την ίδια hash value έστω και αν διαφέρουν ελάχιστα.



Όπως φαίνεται και στο παράπλευρο σχήμα είναι αδύνατο για οποιονδήποτε να βρει τιμές x και y, έτσι ώστε τα x και y να είναι διαφορετικά και παρόλα αυτά ο κατακερματισμός του x να είναι ίσος με τον κατακερματισμό του y.

Επομένως με τη χρήση μιας Hash Function δημιουργούνται λειτουργίες που είναι κρυπτογραφικά ασφαλείς, όπως δείχνει και το επόμενο παράδειγμα όπου με διαφορετικές παρουσιάσεις του όρου 'over' μέσα στη φράση έχουμε τελείως διαφορετικά αποτελέσματα στην έξοδο



Εικόνα 2.1 σχεδόν όμοια μηνύματα παράγουν τελείως διαφορετικό αποτέλεσμα (πηγή: wikipedia)

Επομένως με τη χρήση μιας Hash Function δημιουργούνται και διακινούνται μηνύματα που είναι κρυπτογραφικά ασφαλή, πάντα σύμφωνα με τα μέχρι σήμερα τεχνολογικά δεδομένα και δυνατότητες.

Μια εφαρμογή της ικανότητας που έχει η Hash Function στο να διακινεί πληροφροίες με ασφαλή τρόπο είναι όταν χρειάζεται να κατέβουν μεγάλα αρχεία από το Διαδίκτυο. Ταυτόχρονα με το download που γίνεται κατεβαίνει και ένα αρχείο αθροίσματος ελέγχου (checksum). Το Checksum είναι μια ακολουθία αριθμών και γραμμάτων που υπολογίζεται χρησιμοποιώντας μια συνάρτηση κατακερματισμού και χρησιμοποιείται για τον έλεγχο των δεδομένων για σφάλματα. Για να γίνει η επαλήθευση της ακεραιότητας του αρχείου, ένας χρήστης υπολογίζει το άθροισμα ελέγχου, με τη βοήθεια της Hash Function και κατόπιν συγκρίνει τις δύο συνόψεις για να βεβαιωθεί ότι ταιριάζουν.

Για να γίνει περισσότερο κατανοητό θεωρούμε ότι έχουμε μια έξοδο 256 bits ενώ στην είσοδο έχουμε μια σειρά από πιθανές εισροές που μπορεί να μια σειρά οποιουδήποτε μεγέθους. Αυτό σημαίνει ότι στην έξοδο υπάρχουν μόνο 2^{256} δυνατότητες να υπάρχει ταυτοποίηση, ενώ στην είσοδο υπάρχουν πολύ περισσότερες δυνατότητες. Πόσο όμως είναι εφικτό να υπάρχουν συγκρούσεις ανάμεσα σε δύο από αυτές; Χρειάζεται να υπολογίσουμε τη πιθανότητα οι δύο αυτές να έχουν την ίδια έξοδο. Αν υποθέσουμε ότι υπάρχουν, ως ένα τυχαίο παράδειγμα, 72 επιλεγμένες είσοδοι, η πιθανότητα να βρεθούν δύο από αυτές που μετά τον κατακερματισμό τους να συγκρουσθούν έχοντας την ίδια έξοδο είναι 2^{72} και καθώς, όπως αναφέρθηκε υπάρχουν 2^{256} δυνατότητες να υπάρχει ταυτοποίηση σημαίνει ότι για να βρεθεί ο κατάλληλος συνδυασμός που θα συγκρούεται χρειάζονται να γίνουν2^{256+72} συνδυασμοί που είναι ένας αστρονομικός αριθμός. Έτσι μπορούμε να πούμε ότι αν κάθε υπολογιστής που κατασκευάστηκε ποτέ από την ανθρωπότητα ξεκινούσε τους υπολογισμούς από την αρχή του σύμπαντος έως σήμερα, οι πιθανότητες ότι να είχε βρεθεί μια σύγκρουση θα ήταν ακόμη απεριόριστα μικρές.

Εφόσον λοιπόν γνωρίζουμε ότι οι λειτουργίες κατακερματισμού είναι πρακτικά ελεύθερες από τη πιθανότητα μιας σύγκρουσης, μπορούμε να τις χρησιμοποιήσουμε ως μια αναφορά βάσει της σύνοψης τους (hash). Σημαίνει δηλαδή ότι αν γνωρίζουμε ότι τα x και y έχουν την ίδια σύνοψη, τότε είναι ασφαλές να υποθέσουμε ότι τα x και y είναι τα ίδια και επομένως μπορεί να έχουμε την ίδια σύνοψη ως μια εικόνα ενός μηνύματος. Ας

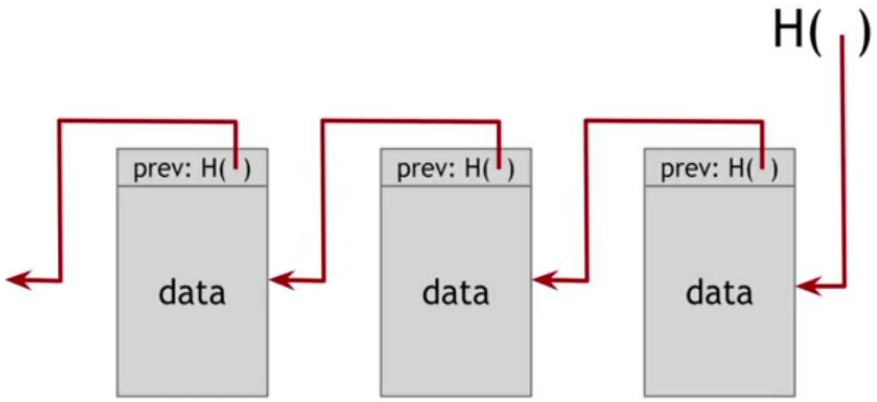
υποθέσουμε, για παράδειγμα, ότι είχαμε ένα πολύ μεγάλο αρχείο, και κάποια στιγμή θα θέλαμε να το συγκρίνουμε και να δούμε αν είναι ίδιο με ένα άλλο, μια μέθοδος για να γίνει αυτό είναι να δημιουργήσουμε και να συγκρίνουμε τα hashes των δύο αρχείων. Αν τα hashes είναι τα ίδια, τότε συμπεραίνουμε ότι τα αρχεία πρέπει να είναι τα ίδια. Αυτό μας δίνει έναν πολύ αποτελεσματικό τρόπο να θυμόμαστε τα πράγματα που έχουμε ξαναδεί και να τα αναγνωρίζουμε ξανά. Και, φυσικά, αυτό είναι χρήσιμο επειδή το αποτέλεσμα που έχει ο κατακερματισμός είναι μικρό, καθώς είναι μόνο 256 bit, ενώ το αρχικό αρχείο μπορεί να είναι πολύ μεγάλο.

Η δεύτερη βασική ιδιότητα που έχει η λειτουργία κατακερματισμού είναι ότι κρύβει την αφετηρία της. Αυτό σημαίνει ότι αν δούμε την έξοδο της συνάρτησης κατακερματισμού, H (x), τότε δεν υπάρχει εφικτός τρόπος να καταλάβουμε ή να προσδιορίσουμε ποιά μπορεί να είναι η είσοδος x. Το πρόβλημα είναι ότι αυτή η ιδιότητα δεν εμφανίζεται πάντοτε ακριβώς έτσι. Για να καταλάβουμε γιατί συμβαίνει αυτό, ας δούμε το παράδειγμα όπου πετάμε ένα κέρμα. Αν το αποτέλεσμα που προκύπτει μετά ήταν κορώνα θα προκύψει το hash της ακολουθίας "κορώνα" ενώ αν το αποτέλεσμα ήταν γράμματα , θα εμφανισθεί το hash της συμβολοσειράς "γράμματα".

Αν ζητηθεί από κάποιον που δεν είδε το αποτέλεσμα της διαδρομής του νομίσματος αλλά είδε μόνο την έξοδο του κατακερματισμού του είναι εύκολο να βρεί τι ήταν η συμβολοσειρά εισόδου, είναι επομένως εύκολο να βρεθεί το x. Απλώς εμφανίζει το hash της συμβολοσειράς "κορώνα" και το hash της συμβολοσειράς "γράμματα", και συγκρίνει με αυτό που έχει. Καθώς στη περίπτωση αυτή υπήρχαν μόνο δυο πιθανές τιμές του x εύκολα βρίσκει κάποιος την είσοδο. Αν όμως το x πρέπει να επιλεγεί μέσα από ένα ομοιογενές σύνολο μέσα από το οποίο κάποιος μπορεί να επιλέξει κάποιες πιθανές τιμές του x, δεν θα μπορεί να βρει ποιο είναι το σωστό x.

Αυτό δείχνει ότι η κρυμμένη ιδιότητα που πρέπει να προσδιορίσουμε είναι πιο περίπλοκη και ο τρόπος με τον οποίο πρόκειται να επιλύσουμε αυτό το πρόβλημα είναι ο εξής : έστω ότι θέλουμε να προσδιορίσουμε το x, σε πρώτο στάδιο συνενώνουμε με αυτό, μια τιμή, r, η οποία επιλέγεται από μια διανομή που είναι πραγματικά απλωμένη δηλαδή όλες οι τιμές που θα μπορούσε να έχει το r έχουν μόνο μια αμελητέα πιθανότητα εμφάνισης (στη πραγματικότητα 2^{256}. Έτσι, η συνάρτηση H (r | x), σημαίνει ότι παίρνουμε όλα τα bits του r και βάζουμε όλα τα bits του x μετά από αυτά. Με δεδομένο τον κατακερματισμό του r μαζί με εκείνο του x, είναι επομένως απίθανο να βρούμε x. Φαίνεται λοιπόν ότι ο κατακερματισμός του r ενισχύει τη δυσκολία ανεύρεσης του x.

Ένας **δείκτης κατακερματισμού** είναι ένα είδος δόμησης δεδομένων που στηρίζεται στη χρήση ενός δείκτη που δείχνει κάθε φορά τη θέση όπου αποθηκεύονται κάποιες πληροφορίες. Όταν έχει γίνει αποθήκευση μιας κρυπτογραφικής σύνοψης πληροφοριών ένας τακτικός δείκτης δίνει έναν τρόπο να ανακτηθούν οι πληροφορίες, ενώ ένας δείκτης κατακερματισμού θα επιτρέψει να ανακτήσουμε κατευθείαν τα στοιχεία αυτά και να επαληθεύσουμε παράλληλα ότι οι πληροφορίες δεν έχουν αλλάξει. Έτσι, ένας δείκτης κατακερματισμού μας λέει πού είναι κάτι και ποιά ήταν η αρχική αξία του.

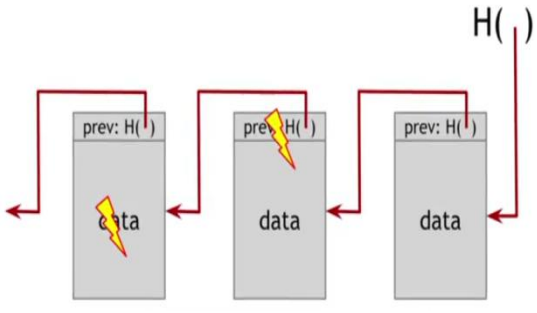


Εικόνα 2.2 η δημιουργία ενός μπλόκ (πηγή: www.hbr.org)

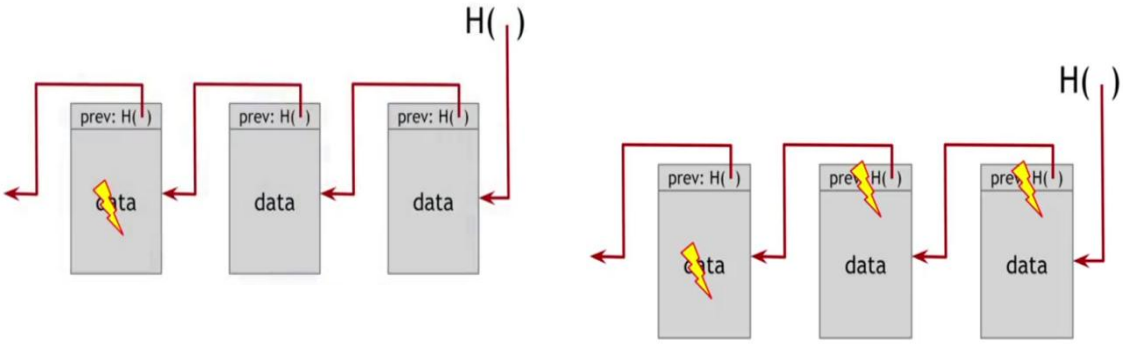
Χρησιμοποιώντας αυτές τις ιδιότητες, μπορούμε να πάρουμε δείκτες κατακερματισμού και να τους χρησιμοποιήσουμε για την κατασκευή δομών δεδομένων κάθε μορφής.

Για παράδειγμα, στο ανωτέρω σχήμα υπάρχει μια συνδεδεμένη λίστα που δημιουργήθηκε με τους δείκτες κατακερματισμού. Αυτή ακριβώς είναι μια δομή δεδομένων που πρόκειται να ονομάσουμε αλυσίδα κάποιων μπλοκ. Πρόκειται ακριβώς για μια συνηθισμένη λίστα όπου έχετε μια σειρά μπλοκ και κάθε μπλοκ έχει δεδομένα καθώς και έναν δείκτη που το συνδέει με το προηγούμενο μπλοκ στη λίστα, με τη διαφορά ότι εδώ ο προηγούμενος δείκτης του μπλοκ θα αντικατασταθεί με έναν δείκτη κατακερματισμού.

Με τη βοήθεια των δεικτών κατακερματισμού μπορούμε επίσης να μετατρέψουμε μια παρόμοια δομή δεδομένων σε μια ανθεκτική συλλογή δεδομένων που έχει τη δυνατότητα να μπορούμε να προσθέτουμε κάθε φορά δεδομένα στο τέλος του αρχείου καταγραφής και αν κάποιος προσπαθήσει αργότερα να μεταβάλλει τα δεδομένα που είναι ήδη εκεί, θα το εντοπίσουμε. Αυτό το είδος δομής δεδομένων ονομάζεται Blockchain και



για να καταλάβουμε το χαρακτηριστικό της αδυναμίας αλλοίωσης του ας δούμε τη γραφική παράσταση στο ακόλουθο σχήμα.



Εικόνα 2.3 η αναπαράσταση της αλλοίωσης δεδομένων (πηγή: www.hbr.org)

Όπως φαίνεται στο σχήμα, ο τελευταίος χρήστης άλλαξε τα περιεχόμενα του πρώτου μπλοκ και συνεπώς, η σύνοψη του στο επόμενο μπλοκ δεν πρόκειται να ταιριάζει. Θα υπάρχει επομένως μια δυσαρμονία μεταξύ του νέου περιεχομένου του 2^{ου} μπλόκ και του παλιού hash pointer και επομένως ο κατακερματισμός του δεύτερου μπλοκ θα είναι τώρα διαφορετικός. Αν χρησιμοποιήσουμε τον παλιό hash pointer 2 θα έχουμε νέο περιεχόμενο στο 2^{ο} μπλοκ ενώ αν προσαρμόσουμε το περιεχόμενο θα δημιουργήσουμε ένα νέο hash pointer 2 ο οποίος όμως θα δώσει ένα διαφορετικό κατακερματισμό του τρίτου μπλοκ και αυτό συνεχίζεται μέχρι να φθάσουμε στη ρίζα η οποία όμως δεν μπορεί να αλλάξει και επομένως θα εντοπισθεί η διαφοροποίηση.

2.3 Πώς ενεργεί η τεχνολογία Blockchain

Η τεχνολογία blockchain είναι ουσιαστικά η τεχνολογία που βρίσκεται πίσω από το Bitcoin – ο τρόπος δηλαδή που λειτουργεί το όλο σύστημα για την αποστολή και παραλαβή ψηφιακών νομισμάτων. Είναι μία σειρά καταχωρίσεων που αφορούν συναλλαγές, σε ένα δημόσιο κατάστιχο (ledger). Κάθε καινούρια ομάδα καταχωρήσεων (ένα νέο block) συνδέεται με τα προηγούμενα, δημιουργώντας μία «αλυσίδα» καταχωρίσεων, δηλαδή ένα blockchain.

Η όλη σύλληψη του Blockchain στηρίζεται ακριβώς στις ιδιότητες της συνάρτησης Hash. Ας δούμε σε ένα παράδειγμα πως αυτό ισχύει στη πράξη.

Έστω λοιπόν ότι υπάρχει ένας αριθμός, για παράδειγμα ο 23602. Θα πρέπει να ψάξουμε να βρούμε ποιος αριθμός μπορεί να προστεθεί σε αυτόν ώστε να βγάλει ως αποτέλεσμα μια λέξη που έχει μια συγκεκριμένη σύνοψη. Πρόκειται για μια απίθανη κατάσταση, που όπως είδαμε προηγουμένως ο μόνος τρόπος για να βρούμε τον αριθμό που αναζητούμε, είναι να δοκιμάσουμε κάθε διαθέσιμο αριθμό που υπάρχει. Δεχόμαστε, για να εξηγήσουμε τη μεθοδολογία, ότι μετά από πολλές προσπάθειες βρίσκουμε ότι ο αριθμός που ψάχνουμε είναι ο 43590 ,ο οποίος όταν προστεθεί στον 23602 δίνει το hash που έχουμε στη διάθεση μας.

Στη περίπτωση αυτή ο αριθμός 43590 που βρήκαμε γίνεται η σφραγίδα για τον αριθμό 23602. Αν λοιπόν υπάρχει μέσα στα στοιχεία μιας βάσης δεδομένων ένας κατάλογος ο οποίος έχει μια σελίδα με αριθμό σελίδας 23602 για να σφραγίσουμε τη σελίδα αυτή του καταλόγου θα την επισημάνουμε με τον αριθμό επισφράγισης 43590. Δηλαδή, στη συγκεκριμένη σελίδα στην οποία έχουν καταγραφεί διάφορες εγγραφές θα χρειασθεί να υπολογίσουμε ένα αρχικό δεδομένο, συνήθως αριθμό, ο οποίος όταν επισυναφθεί στη λίστα των εγγραφών και δοθεί στην είσοδο της συνάρτησης, δίνει ως έξοδο το υπάρχον hash. Αυτός ο αριθμός επισφράγισης είναι ο λεγόμενος “Proof Of Work”, ονομασία που υποδηλώνει ότι καταναλώθηκε προσπάθεια για τον υπολογισμό του αριθμού αυτού. Μόλις ο αριθμός αυτός υπολογιστεί, μετά την κατανάλωση χρόνου και ενέργειας, η σελίδα είναι πλέον σφραγισμένη. Ο αριθμός επιτρέπει στον καθένα να ελέγξει την ακεραιότητα της σελίδας, στην ενδεχόμενη προσπάθεια κάποιου να αλλάξει τα περιεχόμενά της. Για να ελέγξουμε αν μια σελίδα παραμένει αυτούσια ή έχει αλλαχθεί αρκεί πλέον να προσθέσουμε το περιεχόμενο της σελίδας με τον αριθμό επισφράγισης, να τροφοδοτήσουμε το αποτέλεσμα στη συνάρτηση Hash και να συγκρίνουμε τις δύο συνόψεις.

Σε μια ομάδα χρηστών που διενεργούν συναλλαγές μεταξύ τους, συναλλαγές που κάθε φορά καταγράφονται σε μια σελίδα ενός αρχείου φθάνει κάποτε η στιγμή να γεμίσει η σελίδα αυτή και χρειάζεται, σύμφωνα με τις ανάγκες της τεχνολογίας Blockchain να ανζητήσουν τον αριθμό σφράγισης ώστε να προχωρήσουν στην επόμενη σελίδα. Ο πρώτος ο οποίος, σύμφωνα με όσα αναφέρθηκαν πιο πάνω, ανιχνεύσει τον αριθμό, τον ανακοινώνει στους υπόλοιπους οι οποίοι διενεργούν ένα έλεγχο εγκυρότητας και αν το

αποτέλεσμα του ελέγχου ταυτίζεται με το αποτέλεσμα του περιεχομένου σφραγίζουν με τον αριθμό αυτό τη συγκεκριμένη σελίδα και την αποθηκεύουν.

Το δεδομένο που επαληθεύει τη πλειοψηφία των αναζητήσεων θεωρείται και ο αξιόπιστος αριθμός σφράγισης. Σε περίπτωση που ο έλεγχος εγκυρότητας για κάποιον δεν επαληθευθεί, αυτός θα πρέπει να ακυρώσει τη σελίδα του και να την αντιγράψει σωστά πλέον από κάποιον άλλον, ώστε να την βάλει έπειτα στον φάκελό του. Αν δεν το κάνει θα πάψει να αποτελεί μέρος του συνολικού δικτύου καθώς δεν θα μπορεί να προχωρήσει και να συνεχίσει να καταγράφει συναλλαγές.

Όλοι όσοι είναι μέρος του Blockchain έχουν δικαίωμα ανταμοιβών που δίνονται κάθε φορά σε όποιον πρώτος υπολογίσει τον αριθμό σφράγισης, καθώς με τον τρόπο αυτό ανταμείβεται για την υπολογιστική ισχύ και την ενέργεια που κατανάλωσε. Οι ανταμοιβές αυτές είναι χρηματικές και αυτός που θα αναταμειφθεί θα πάρει το καθορισμένο ποσό χωρίς όμως να το στερήσει από κάποιον άλλο. Με αυτόν τον τρόπο γεννήθηκε το Bitcoin καθώς αυτή ήταν η ανταμοιβή σε όποιον έβρισκε τον αριθμό σφράγισης κάθε σελίδας . Ήταν το πρώτο νόμισμα που διεκπεραιώθηκε σε Blockchain, και για να συνεχιστεί η προσπάθεια, ο κόσμος πληρωνόταν σε Bitcoin (Φυτίλης, 2017).

2.4 Οι εφαρμογές της τεχνολογίας Blockchain

Όπως είδαμε το κύριο χαρακτηριστικό της τεχνολογίας Blockchain είναι ότι επιτρέπει τη μεταφορά μιας ψηφιακής εγγραφής αλλά δεν επιτρέπει την αναπαραγωγή της σε οποιοδήποτε μέσον. Για την ιδιότητα της αυτή η τεχνολογίας Blockchain επομένως μπορεί να θεωρηθεί ως το επόμενο βήμα σε μια νέα μορφή του Διαδικτύου.

Η διάδοση του Bitcoin είναι η πρώτη εφαρμογή των δυνατοτήτων της τεχνολογίας Blockchain καθώς το ψηφιακό νόμισμα υπάρχει μόνο και μόνο επειδή το επιτρέπουν τα χαρακτηριστικά της τεχνολογίας blockchain, που αφήνουν ένα μεγάλο αριθμό συναλλαγών να καταγράφονται σε οργανωμένες ομάδες χωρίς όμως να δίνει τη δυνατότητα σε κάποιον να παρέμβει για να κάνει οποιεσδήποτε αλλαγές σε μια συναλλαγή. Αν και στην αρχή η τεχνολογία Blockchain είχε συνδεθεί στενά με την εμφάνιση του Bitcoin στη πορεία της παρουσίας της εμφανίζονται όλο και περισσότερες δυνατότητες χρησιμοποίησης της σε άλλες εφαρμογές.

Η αρχή της τεχνολογίας Blockchain δεν καταγράφει σε ένα υπολογιστικό φύλο μόνο χρηματικές συναλλαγές, όπως στη περίπτωση του Bitcoin αλλά μπορεί να καταγράψει

οποιοδήποτε δεδομένο μπορεί να έχει αξία. Στη συνέχεια, αυτό το υπολογιστικό φύλλο αντιγράφεται πολυάριθμες φορές σε ένα δίκτυο υπολογιστών και κάθε φορά που υπάρχει μια μεταβολή ενημερώνονται όλοι αυτοί οι κόμβοι ενώ όλες οι πληροφορίες που υπάρχουν στη Blockchain αποτελούν μιας μορφής κοινή βάση δεδομένων και συνεχούς ενημέρωσης για αυτούς που τις χειρίζονται. Όλες οι ομάδες συναλλαγών που βρίσκονται σε μια βάση δεδομένων Blockchain είναι ορατές και προσβάσιμες από όλους και εύκολα μπορούν να ελεγχθούν ανά πάσα στιγμή (Παπαϊωάννου, 2017).

Καθώς δεν υπάρχει ένα κεντρικό σύστημα αποθήκευσης που μεταφέρει και αναπαριστά την πληροφορία δεν υπάρχει τρόπος να παραβιαστεί το πρωτόκολλο της και να αλλοιωθεί η μορφή της πληροφορίας από οποιαδήποτε κακόβουλη ενέργεια. Επιπλέον, σε περιοδικά διαστήματα, κάθε 10 λεπτά, υπάρχει μια κατάσταση ελέγχου που επιβεβαιώνει κάθε συναλλαγή που έλαβε χώρα μέσα στο διάστημα αυτό.

Δύο πολύ σημαντικές ιδιότητες της τεχνολογίας blockchain προκύπτουν από την αρχή λειτουργίας της :

- τα δεδομένα που διασφαλίζουν τη διαφάνεια των συναλλαγών ενσωματώνονται στο σύνολο του δικτύου που είναι ανοικτό σε όλους τους χρήστες και , άρα είναι εξ ορισμού δημόσιο.
- Καμιά αλλοίωση (μεταβολή ή καταστροφή) ενός block δεν είναι δυνατή καθώς οποιαδήποτε επέμβαση στην μακριά αλυσίδα της Blockchain απαιτεί μια υπερβολικά μεγάλη υπολογιστική δύναμη καθώς όποιος ήθελε να παρέμβει θα έπρεπε να παρέμβει ταυτόχρονα σε ένα δίκτυο εκατομμυρίων υπολογιστών που όλοι μοιράζονται κάθε έγγραφο με τις συναλλαγές που έχουν γίνει σφόσον αυτή είναι η αρχή της τεχνολογίας Blockchain.

Από το σχεδιασμό του, το blockchain είναι μια αποκεντρωμένη τεχνολογία η οποία μπορεί να είναι περίπλοκη αλλα ταυτόχρονα αποτελεί τη πιο εφικτή από τεχνικής άποψης προσπάθεια για να αποκτήσουν οι συναλλαγές μια δημόσια έκθεση φανερή σε όλους καθώς κάθε ενέργεια γίνεται σε αυτήν γίνεται αμέσως γνωστή σε όλους. Οι κλασσικές εμπορικές συναλλαγές δεν χρειάζονται επαλήθευση καθώς πρόκειται για συναλλαγές one-off που ολοκληρώνονται σχεδόν ταυτόχρονα τη στιγμή που καταγράφονται σε ένα έγγραφο βάσει της τεχνολογίας Blockchain.

Όλα αυτά τα χαρακτηριστικά έχουν οδηγήσει τη τεχνολογία του Blockchain σε μια γρήγορη εξέλιξη ώστε να έχει περάσει σήμερα από το στάδιο διερεύνησης των

δυνατοτήτων της, σε μια τεχνολογία που μπορεί να παρέχει σημαντικές λύσεις σε κρίσιμα ζητήματα, που μπορεί να προκύψουν για μια επιχείρηση, όπως για παράδειγμα σε βασικές λειτουργίες οικονομικών και εφοδιαστικής αλυσίδας. Επίσης, καθώς η τεχνολογία Blockchain μπορεί και δημιουργεί «απαραβίαστα αρχεία» στα οποία καταγράφονται κάθε είδους συναλλαγές που αφορούν διάφορες μορφές δεδομένων όλο και περισσότερες εταιρείες που ασχολούνται με την ανάπτυξη της τεχνολογίας φιλοδοξούν να τη δουν να αξιοποιείται και εκτός του τομέα των ψηφιακών νομισμάτων στο τομέα της εμφάνισης χρήσιμων πληροφοριών. Η δυναμική της τεχνολογίας Blockchain είναι τέτοια που μπορεί να εξελιχθεί σε ένα σημαντικό συστατικό στοιχείο της παγκόσμιας υποδομής παροχής δεδομένων και ψηφιακών υπηρεσιών, εισάγοντας νέα μοντέλα στις κατανεμημένες και συνεργατικές εφαρμογές, καθώς και στην κοινή χρήση και διαχείριση δεδομένων. Με αυτή την έννοια, μπορεί οι εφαρμογές της να "ταράξουν τα νερά" σε πολλές επιχειρηματικές περιοχές, πέρα από την τραπεζική και τις χρηματοπιστωτικές συναλλαγές.

Είναι γεγονός ότι οι τεχνολογίες Blockchain καθιστούν εφικτή μια νέα γενιά εφαρμογών συναλλαγών (transactional) που χαρακτηρίζονται από ακεραιότητα, διαφάνεια και εμπιστοσύνη μεταξύ των ίδιων των συναλλασσόμενων μερών. Οι οργανισμοί που τις υιοθετούν μπορούν να αξιοποιήσουν ένα αποκεντρωμένο, αποτελεσματικό και ασφαλές ψηφιακό περιβάλλον. Οι τεχνολογίες Blockchain εισάγουν μια θεμελιώδη αλλαγή: από την κεντρική διαχείριση της πιστοποίησης, της εμπιστοσύνης και των υπηρεσιών, περνάμε σε μια κατανεμημένη αλληλεπίδραση τόσο στο επίπεδο των υπηρεσιών όσο και σε αυτό της πιστοποίησης της ακεραιότητας και της ασφάλειας. Η τεχνολογία blockchain, με τα εκατομμύρια κόμβους της ορίζει ένα νέο διοικητικό σύστημα, μέσω των οποίων μεταβιβάζονται σε περιφερειακά όργανα ορισμένες εξουσίες ή λειτουργίες με σκοπό να επιτευχθεί η αποσυμφόρηση των κεντρικών υπηρεσιών. Μια τέτοια αλλαγή δεν έρχεται χωρίς προκλήσεις, τόσο τεχνικές όσο και θεσμικές.

Με την εφαρμογή της τεχνολογίας Blockchain μπορούν να προκύψουν κάποιες ενδιαφέρουσες και σημαντικές εφαρμογές.

Η δημιουργία Blockchain επιτρέπει στους ανθρώπους να διαμορφώνουν ψηφιακές σχέσεις που ήταν αδύνατες πριν. Η τεχνολογία Blockchain προσφέρει ένα μέσο για την αυτόματη δημιουργία μιας καταγραφής για το ποιος έχει πρόσβαση σε πληροφορίες ή αρχεία και για τον καθορισμό των ελέγχων στα δικαιώματα που απαιτούνται για την προβολή των πληροφοριών. Τα δεδομένα αποκαλύπτονται διαφορετικά, εξασφαλίζονται

διαφορετικά και καταγράφονται διαφορετικά. Αυτό αλλάζει τις ψηφιακές σχέσεις, δημιουργώντας τη δυνατότητα αυτοματοποίησης του κώδικα μέσω «έξυπνων συμβολαίων»

Κεφάλαιο 3^{ο}

Το ψηφιακό νόμισμα bitcoin

3.1 Η ιστορική αναδρομή

Το bitcoin έχει μια μακρινή ιστορία, αυτή του ηλεκτρονικού χρήματος και μια πρόσφατη ιστορία που συνδέεται άμεσα με το ίδιο το bitcoin.

Θα μπορούσε κανείς να πει ότι η ιστορία του bitcoin ξεκίνησε το 1983 με το ερευνητικό έργο του David Chaum. Ο Chaum ήταν ένας Αμερικανός φοιτητής από το Πανεπιστήμιο της Καλιφόρνια στο Barclay που έκανε το διδακτορικό του στην

κρυπτογραφία και ενδιαφέρθηκε ιδιαίτερα για τη δυνατότητα αποστολής χρημάτων με ηλεκτρονικούς υπολογιστές ανώνυμα.

Το 1989, ο David Chaum εμπορευματοποίησε την ιδέα του δημιουργώντας την εταιρεία Digicash. Η Digicash ξεκίνησε την εφαρμογή ενός ανώνυμου συστήματος ηλεκτρονικού χρήματος το οποίο ονόμασαν "e-cash". Άλλες εταιρείες, όπως η First Virtual Holdings, η Cybercash και μια εταιρεία της Microsoft, θα ακολουθήσουν το παράδειγμά της λίγο αργότερα. Δημιουργήθηκε επίσης και η εταιρεία Gold & Silver Reserve Inc. η οποία ξεκίνησε ένα ηλεκτρονικό χρήμα του οποίου η αξία ήταν εγγυημένη από συγκεκριμένη ποσότητα χρυσού που ονομάσθηκε "e-gold". Ο στόχος ήταν να καταστεί δυνατή η ηλεκτρονική πληρωμή για την ανάπτυξη του ηλεκτρονικού εμπορίου που την εποχή εκείνη βρισκόταν ακόμη στην παιδική του ηλικία. Το 1998, ο Chaum προτείνει ένα αποσυνδεδεμένο σύστημα ηλεκτρονικού χρήματος σε συνεργασία με τις FIAT και NAOR (Stark, 2017).

Καθώς όμως η ιδέα αργούσε πολύ να διαδοθεί η Digicash κήρυξε το πτώχευση το 1998. Πριν όμως πτωχεύσει, η εταιρεία είχε ξεκινήσει την ανάπτυξη της έννοιας του ‘’φυσικού πορτοφολιού’’ για να αποτρέψει το ενδεχόμενο να χρησιμοποιήσει κάποιος το ίδιο ποσό πολλές φορές.

Την ιδέα αυτή θα πάρουν στη συνέχεια άλλες εταιρείες με πιο γνωστή τη Mondex, η οποίο θα αναπτύξει τις ιδέες του ‘’φυσικού πορτοφολιού’’ και της ‘’πλαστικής κάρτας’’πριν εξαγορασθεί από τη MasterCard.

Το 1991, οι Αμερικανοί Stuart Haber και Scott Stornetta προτείνουν ένα σύστημα εξασφάλισης εγγράφων που βασίζονται στη λειτουργία της χρονικής σήμανσης. Η χρονική σήμανση είναι ένας μηχανισμός που συνδυάζει μια ημερομηνία και ώρα με ένα γεγονός, πληροφορίες ή δεδομένα υπολογιστή. Συνήθως αποσκοπεί στην καταγραφή της στιγμής κατά την οποία πραγματοποιήθηκε μια πράξη. Έτσι, μόλις εκδοθεί ένα έγγραφο, δεν θα μπορούσαμε να αλλάξουμε την ημερομηνία της δημιουργίας του και επομένως είναι ένας αποτελεσματικός τρόπος να εγγυηθεί κάποιος το περιεχόμενο.

Το 1992, δύο κρυπτογράφοι ειδικοί η Cynthia Dwork και η Moni Naor και να προτείνει μια λύση στο πρόβλημα του spam (e-mail με μη εξουσιοδοτημένη διαφήμιση αρχικά) βασισμένη προηγουμένως στην επίλυση ενός παζλ. Πριν την αποστολή του μηνύματος ηλεκτρονικού ταχυδρομείου, θα πρέπει να επιλυθεί το παζλ και να συμπεριληφθεί η λύση στο μήνυμα ηλεκτρονικού ταχυδρομείου, διαφορετικά αυτό δεν θα αποσταλεί. Αν

σκεφθεί κάποιος ότι για να στείλει κάποιος 1000 e-mail θα πρέπει να λύσει 1000 γρίφους βλέπει πόσο πολύπλοκη είναι η αποστολή μηνυμάτων σε πολλούς παραλήπτες.

Το 1997, ο Adam Back έκανε μια παρόμοια πρόταση (σύστημα "hashcash") αλλά η πρόταση του σχετίζεται με το νόμισμα και την επίλυση ενός αλγορίθμου για την έκδοση χρημάτων.

Το 1998,ο Wei Dai δημιουργεί το σύστημα b-money όπου η έκδοση του νομίσματος γίνεται με την επίλυση ενός αλγορίθμου σε ένα δίκτυο peer-to-peer τόσο αποκεντρωμένο, όπου κάθε ηλεκτρονικός υπολογιστής διατηρεί το τοπικό του μητρώο λογαριασμών (legder). Την ίδια χρονιά, σύμφωνα με μια έρευνα που χρονολογείται από το 2005, ένας άλλος αμερικανός, ο Nick Nzabo δήλωσε ότι και αυτός είχε αναπτύξει ένα παρόμοιο σύστημα που ονόμασε "bitgold". Αυτές οι προτάσεις δεν αποτελούσαν δομημένες εφαρμογές αλλά είτε αποτελούσαν θέσεις σε μια λίστα διευθύνσεων ηλεκτρονικού ταχυδρομείου για τον Wei Dai ή και θέσεις σε ένα blog για τον Nzabo. Δεν υπάρχει όμως καμία θεωρητική προσέγγιση η προτεινόμενες λύσεις για προβλήματα που θα παρουσιαζόταν στο μέλλον ή ένας κώδικας για να εξελιχθούν τα προτεινόμενα συστήματα.

Η προσπάθεια δημιουργίας όμως ενός πραγματικά ανεξάρτητου ψηφιακού νομίσματος ξεκίνησε στις αρχές της δεκαετίας του 1990 και εδραιώθηκε το 2008 από ένα άτομο (ή ομάδα ατόμων) που είναι γνωστό μόνο με το ψευδώνυμο Satoshi Nakamoto. Ο Satoshi Nakamoto πρότεινε τη δημιουργία ενός κρυπτονομίσματος ως λύση στο πρόβλημα των διπλών δαπανών χρησιμοποιώντας ένα δίκτυο peer-to-peer. Μια αμιγώς ομότιμη (P2P) έκδοση ηλεκτρονικών μετρητών θα επέτρεπε τη σύνδεση από ένα μέρος σε άλλο ώστε οι ηλεκτρονικές πληρωμές να αποστέλλονται απευθείας από το ένα στο άλλο χωρίς να περάσουν από ένα κεντρικό χρηματοπιστωτικό ίδρυμα.

Ο Satoshi Nakatomo άρχισε να ασχολείται για το πώς θα δημιουργηθεί το bitcoin το Μάιο του 2007 σε συνεργασία με άτομα στο Διαδίκτυο που ενδιαφέρονταν για το θέμα και οι συνομιλίες τους εμφανιζόταν σε ένα φόρουμ που ονομάζεται «cyberpunks».

Τον Αύγουστο του 2008, ο Satoshi Nakatomo κατοχυρώνει το όνομα του τομέα bitcoin.org και στις 31 Οκτωβρίου 2008, δημοσίευσε το "white paper" του, που περιγράφει πλήρως το ολοκληρωμένο σύστημα που προσφέρει, στο οποίο χρησιμοποιεί για πρώτη φορά τον όρο «bitcoin» για την αναφορά στο νόμισμα και στο ίδιο το σύστημα. Αργότερα, μέσα στο ίδιο έτος δημοσίευσε τον κωδικό της εφαρμογής Bitcoin-

Qt 0.1 του λογισμικού και ζητάει, από τους συνομιλητές του στη πλατφόρμα, να την κατεβάσουν και να την εγκαταστήσουν στον υπολογιστή τους. Αυτή είναι η πρώτη έκδοση του κυρίως συστήματος bitcoin που ονομάζεται " bitcoin core".

Στις 3 Ιανουαρίου 2009, ο Satoshi Nakamoto εγκαινιάζει το bitcoin με το πρώτο μπλοκ (όλες οι συναλλαγές), που ονομάσθηκε "μπλοκ 0" ή το "μπλοκ γένεσης" όπου γράφει "«The Times 03 / Ιαν / 2009 Chancellor on brink of second bailout for banks. » δηλαδή "ο υπουργός Οικονομικών στα πρόθυρα της δεύτερης διάσωσης για τις τράπεζες". Πράγματι, το μήνυμά αυτό ήταν ο τίτλος της βρετανικής εφημερίδας The Times εκείνη την ημέρα.

Είναι αποδεδειγμένο ότι ο Satoshi ξεκίνησε από το έργο των Wei Dai και Nick Szabo για να καταλήξει στη δημιουργία του bitcoin και αυτό το επιβεβαιώνει και ο ίδιος αναφέροντας ότι " το bitcoin είναι η εφαρμογή των προτάσεων Wei Dai για το b-money και του Nick Szabo για το bitgold ".

Χρησιμοποίησε επίσης το έργο του Hal Finney σε ένα επαναχρησιμοποιήσιμο σύστημα ηλεκτρονικής απόδειξης της εργασίας, από το οποίο ο Satoshi εμπνεύσθηκε για να αναπτύξει την απόδειξη της δημιουργίας για την εφαρμογή του bitcoin.

Ο Satoshi συνεργάσθηκε για πολλά θέματα με τον Gavin Andressen, ο οποίος αργότερα ανέλαβε άτυπα τα καθήκοντα του επικεφαλής της ομάδας ανάπτυξης του Bitcoin.

Ο Satoshi φαίνεται να έχει εξαφανιστεί από το προσκήνιο εντελώς από τις 12 Δεκεμβρίου 2010, όταν ανέβασε μια τελευταία δημοσίευση πριν από την έκδοση της έκδοσης v0.3.19 του κύριως λογισμικού του bitcoin.

Κάποιες ημερομηνίες σταθμοί στην ιστορία του bitcoin είναι:

Η πρώτη αγορά με bitcoin έγινε στις 22 Μαΐου του 2010, στις ΗΠΑ, όπου ο Hanyecz Laszlo, ένας προγραμματιστής που ζει στο Τζάκσονβιλ, Φλόριντα, δηλώνει στη πλατφόρμα bitcointalk την επιθυμία να αγοράσει μια πίτσα με bitcoins. Θα λάβει από τον Papa John μια πίτσα πληρώνοντας 10.000 bitcoins. Αυτή θεωρείται ότι είναι η πρώτη εμπορική συναλλαγή με το bitcoin.

Στις 12 Ιουνίου 2010, η τιμή του bitcoin έναντι του δολαρίου δεκαπλασιάζεται, από 0,008 δολάρια για ένα bitcoin στα 0,08 δολάρια. Λίγες μέρες αργότερα, στις 17 Ιουλίου 2010, ο

Jed Mc Caleb ίδρυσε την αγορά του Mt Gox. Αυτή είναι η πρώτη αγορά όπου μπορεί κάποιος να αγοράσει ή να πουλήσει bitcoins όπως σε χρηματιστήριο.

Στις 6 Νοεμβρίου 2010, το bitcoin έφθασε σε κεφαλαιοποίηση ένα εκατομμύριο δολάρια ποσόν που υπολογίζεται πολλαπλασιάζοντας τον αριθμό των bitcoins σε κυκλοφορία εκείνη τη στιγμή με την πιο πρόσφατη τιμή του bitcoin στην αγορά Gox να είναι 0,50 δολάρια ανά bitcoin.

Στις 9 Φεβρουαρίου 2011, για πρώτη φορά ένα bitcoin αξίζει ένα δολάριο ΗΠΑ στην αγορά Mt Gox.

Στις 27 Μαρτίου του 2011, ξεκινάει στην αγορά Britcoin η διαπραγμάτευση του bitcoin έναντι της στερλίνας και λίγες μέρες μετά , στις 5 Απριλίου 2011, το bitmarket.eu εγκαινιάζει τις δραστηριότητες του για την πώληση και την αγορά bitcoins με το ευρώ.

3.2 Τι είναι το bitcoin

Το bitcoin είναι μια μορφή ψηφιακού χρήματος, το οποίο δημιουργήθηκε και διατηρείται ηλεκτρονικά, χωρίς να το ελέγχει κανείς. Τα bitcoins δεν εκτυπώνονται από ένα κεντρικό ίδρυμα όπως συμβαίνει με τα συμβατικά νομίσματα, μπορούν να δημιουργηθούν από οποιονδήποτε μέσω ενός λογισμικού. Είναι το πρώτο παράδειγμα μιας αναπτυσσόμενης κατηγορίας χρημάτων που είναι γνωστή ως «κρυπτονόμισμα».

Το πιο σημαντικό χαρακτηριστικό του bitcoin, αυτό που το καθιστά διαφορετικό από τα συμβατικά χρήματα, είναι ότι είναι αποκεντρωμένο. Το δίκτυο των bitcoins δεν ελέγχεται από κάποιο συγκεκριμένο φορέα, γεγονός που δίνει σε όσους το χρησιμοποιούν την ευκαιρία να απομακρυνθούν από τον έλεγχο των τραπεζών και (σε κάποιο βαθμό) από τον κρατικό παρεμβατισμό .

Το bitcoin δημιουργείται ψηφιακά, από ένα δίκτυο ανθρώπων, από μια κοινότητα στην οποία μπορεί να συμμετέχει ο καθένας. Οι συναλλαγές είναι που ορίζουν την ίδια τη ροή ολόκληρου του δικτύου του bitcoin, γεγονός που δεν αφήνει σε κανένα τη δυνατότητα ελέγχου ή πειραματισμού της νομισματικής ροής και πολιτικής. Το bitcoin , σε αντίθεση με τα συμβατικά νομίσματα που είναι συνδεδεμένα με το χρυσό, στηρίζεται σε βασικές αρχές των μαθηματικών καθώς όλα τα προγράμματα δημιουργίας κρυπτονομισμάτων σε όλο τον κόσμο ακολουθούν έναν μαθηματικό τύπο, και έτσι παράγουν bitcoins. Ο μαθηματικός τύπος είναι ελεύθερα διαθέσιμος, έτσι ώστε ο καθένας να μπορεί να τον ελέγξει. Επιπλέον, οι χρήστες συμμετέχουν ανώνυμα σε αυτό το δίκτυο συναλλαγών, χρησιμοποιώντας ένα ″ψηφιακό πορτοφόλι″. Οι συναλλαγές αυτές, μεταξύ των

ψηφιακών πορτοφολιών, ελέγχονται από όλους τους χρήστες, μέσω μαθηματικών πράξεων, και καθεμιά προστίθεται σε ένα κοινό, δημόσιο λογαριασμό. Αυτή η διαδικασία επαλήθευσης των συναλλαγών και η προσθήκη τους σε ένα καθολικό δίκτυο ονομάζεται ‘’εξόρυξη ‘’. Η δραστηριότητα της ‘’εξόρυξης ‘’ είναι που δημιουργεί περισσότερα bitcoins. Το δίκτυο όπου εμφανίζονται δημόσια όλες οι συναλλαγές ελέγχεται από όλους τους χρήστες και λειτουργεί βάσει της δέσμευσης από όλους ότι αν και είναι ελεύθεροι να επιλέγουν το λογισμικό που χρησιμοποιούν εν τούτοις θα χρησιμοποιούν το λογισμικό εκείνο που υπακούει σε κοινούς κανόνες.

Μια σημαντική παράμετρος που χρειάζεται να διευκρινισθεί αφορά τη διαφορά μεταξύ ενός δικτύου κρυπτογράφησης και του νομίσματος που αυτό καθορίζει. Για παράδειγμα, το δίκτυο Bitcoin εκφράζει τόσο την αναγκαία τεχνολογική υποδομή όσο και το πρωτόκολλο που επιτρέπει τις συναλλαγές των νομισμάτων. Ενώ λοιπόν υπάρχει ένα μόνο πρωτόκολλο Bitcoin, που μπορεί εξάλλου να χρησιμοποιηθεί, όπως θα δούμε στη συνέχεια και για άλλους σκοπούς υπάρχουν εκατομμύρια bitcoins. (Ametrano, 2014).

Η ανωνυμία των ψηφιακών νομισμάτων ελαχιστοποιεί τις πολιτικές ελέγχου, τον κρατικό παρεμβατισμό και την άσκηση κοινωνικής πολιτικής. Ωστόσο, αυτή η ανωνυμία έχει προκαλέσει κάποιες αρνητικές αντιδράσεις. Πολλοί είναι εκείνοι που συνδέουν το bitcoin με την αύξηση του παραεμπορίου.

Σήμερα, το bitcoin αναδύεται σε ένα όργανο παγκόσμιου εμπορίου, ξεπερνώντας κάθε δυσκολία και προσαρμόζοντας τα χαρακτηριστικά του στις ανάγκες της εποχής και των χρηστών, καταφέρνοντας, παράλληλα, να ανοίξει το δρόμο προς μια διαφανή χωρίς ενδιάμεσους και ανώνυμη οικονομία.

Ωστόσο, όπως συμβαίνει και με κάθε καινοτομία, είναι δύσκολο να προβλέψει κανείς την εξέλιξή του. Όσοι είναι σήμερα οι υποστηρικτές του Bitcoin πιστεύουν ότι η peer-to-peer αρχιτεκτονική της δομής του θα βάλει τα θεμέλια για τη δημιουργία μιας νέας γενιάς καινοτόμων χρηματοοικονομικών υπηρεσιών, σχεδόν με τον ίδιο τρόπο που η ανοικτή αρχιτεκτονική του Διαδικτύου οδήγησε σε καινοτόμες νέες ηλεκτρονικές υπηρεσίες.

Καθώς βρισκόμαστε ακόμα σε εμβρυακό στάδιο, ως προς την ψηφιακή οικονομία, κάθε προσπάθεια και πρωτοπορία θα πρέπει να ακολουθεί σταθερά βήματα ανάπτυξης ώστε να μη χάσει τον οποιοδήποτε ανθρωπιστικό χαρακτήρα της .

3.3 Τα πλεονεκτήματα και τα μειονεκτήματα των bitcoins

3.3.1 Οι γενικές σκέψεις

Το bitcoin και όλα τα ψηφιακά νομίσματα έχουν τα οφέλη και τα μειονεκτήματά τους. Στην ενότητα αυτή επεξεργαζόμαστε διάφορες πτυχές και χαρακτηριστικά των κρυπτονομισμάτων, που αποτελούν πλεονεκτήματα, μειονεκτήματα, κινδύνους και ευκαιρίες έναντι των συμβατικών νομισμάτων και προδιαγράφουν τη πορεία τους στο μέλλον.

Υπάρχουν διαφορετικές και αντικρουόμενες απόψεις σχετικά με το μέλλον των κρυπτονομισμάτων γενικά και των bitcoins ειδικότερα. Οι άνθρωποι με τις λιγότερο συμβατικές απόψεις είναι αισιόδοξοι και αγκαλιάζουν την ιδέα του ψηφιακού νομίσματος, ενώ κάποιοι άλλοι ειδικοί με πιο συντηρητικές απόψεις δεν είναι ιδιαίτερα ενθουσιασμένοι με τις εξελίξεις στο τομέα των κρυπτονομισμάτων στο σύστημα των χρηματοπιστωτικών συναλλαγών και ιδιαίτερα των πληρωμών. Όσοι εστιάζουν στα πλεονεκτήματα του bitcoin και των άλλων κρυπτονομισμάτων εκτιμούν ότι το μέλλον τους ανήκει, ενώ όσοι αναφέρονται στις αδυναμίες τους πιστεύουν είτε ότι τα κρυπτονομίσματα είναι μια φούσκα που θα σκάσει ή ότι θα υπάρχουν κρατικές παρεμβάσεις που θα εκμηδενίσουν τη σημασία τους και θα τα οδηγήσουν σε μη βιώσιμες καταστάσεις.

Στην συνέχεια παρουσιάζουμε τα βασικότερα πλεονεκτήματα και μειονεκτήματα του bitcoin και των άλλων κρυπτονομισμάτων (Ivaschenko, 2016)

3.3.2 Τα πλεονεκτήματα του bitcoin

1. Χρησιμοποιείται ένας ανοιχτός κώδικας για την εξόρυξη των κρυπτονομισμάτων και εφαρμόζονται οι ίδιοι αλγόριθμοι που χρησιμοποιούνται στην ηλεκτρονική τραπεζική. Η μόνη διαφορά των τραπεζικών συναλλαγών μέσω Διαδικτύου είναι ότι σε αυτές υπάρχει η δυνατότητα αποκάλυψη πληροφοριών σχετικά με τους χρήστες. Στο δίκτυο BTC μοιράζονται όλες οι πληροφορίες σχετικά με τη συναλλαγή, αλλά δεν υπάρχουν δεδομένα σχετικά με τον παραλήπτη και τον αποστολέα των κερμάτων, καθώς δεν υπάρχει πρόσβαση στις προσωπικές πληροφορίες του πορτοφολιού του κατόχου. Υπάρχουν κάποιοι που χαρακτηρίζουν το σύστημα Bitcoin ως «ψευδώνυμο» (pseudonymous) και όχι πλήρως ανώνυμο καθώς υποστηρίζουν ότι αν χρειασθεί υπάρχει η δυνατότητα να εντοπιστούν οι πραγματικές ταυτότητες των χρηστών (Moser, 2013).

2. Δεν υπάρχει πληθωρισμός, ο μέγιστος αριθμός κερμάτων περιορίζεται αυστηρά στα 21 εκατομμύρια bitcoins και καθώς δεν υπάρχει κάποιος κεντρικός φορέας που να μπορεί να αλλάξει αυτή τη σειρά δημιουργώντας νέα νομίσματα, δεν υπάρχει δυνατότητα ανάπτυξης του πληθωρισμού στο σύστημα.

3. Με τη χρήση των κρυπτονομισμάτων διευκολύνεται η μεταφορά κεφαλαίων μεταξύ δύο διακριτών μερών με μια μόνο πράξη που διευκολύνεται μέσω της χρήσης δημόσιων και ιδιωτικών κλειδιών για λόγους ασφαλείας.

4. Οι μεταφορές κεφαλαίων με τα ψηφιακά νομίσματα γίνονται με ελάχιστες χρεώσεις επεξεργασίας καθώς δεν υπάρχουν ενδιάμεσοι, επιτρέποντας στους χρήστες να αποφεύγουν τις υψηλές χρεώσεις που επιβάλλουν οι περισσότερες τράπεζες.

5. Ο τρόπος που γίνονται οι συναλλαγές στη πλατφόρμα του Bitcoin βοηθάει τους συναλλασσόμενους να αποδεικνύουν ότι έγινε η συναλλαγή καθώς αυτή, σε αντίθεση με τα μετρητά, αφήνει πάντοτε το αποτύπωμα της. Η πληρωμή σε bitcoins επομένως τους επιτρέπει να προστατεύονται όταν υπάρχουν μη πραγματικές χρεώσεις αντιλογισμού (chargebacks). Αντίθετα η συναλλαγή σε bitcoin δεσμεύει τον καταναλωτή να κρατήσει το προϊόν που αγόρασε.

6. Το Bitcoin χαρακτηρίζεται από την απλότητα στη χρήση του. Οι χρήστες δεν χρειάζεται να διαθέτουν έναν τραπεζικό λογαριασμό ή μια πιστωτική κάρτα για να το χρησιμοποιήσουν, καθώς αρκεί μια σύνδεση στο Internet για τη χρήση του σε όλα τα μέρη στον κόσμο (Murphy et al, 2015).

7. Σε ένα δίκτυο Peer-to-peer, όπως αυτό των κρυπτονομισμάτων δεν υπάρχει κάποιος κύριος διακομιστής, ο οποίος να είναι υπεύθυνος για όλες τις λειτουργίες. Η ανταλλαγή πληροφοριών (σε αυτή την περίπτωση - το χρήμα) γίνεται μόνο μεταξύ των χρηστών και υπάρχουν απεριόριστες δυνατότητες συναλλαγής, καθώς καθένας από τους κατόχους πορτοφολιών μπορεί να πληρώσει σε οποιονδήποτε, οπουδήποτε και οποιοδήποτε ποσό. Όλα τα προγράμματα-πορτοφόλια που έχουν οι χρήστες αποτελούν μέρος ενός δικτύου bitcoin. Οι συναλλαγές γίνονται από εκατοντάδες κατανεμημένους διακομιστές και πρακτικά δεν ελέγχονται από κανέναν.

8. Κάθε πελάτης αποθηκεύει ένα αρχείο όλων των διενεργηθεισών συναλλαγών και τον αριθμό των bitcoins που υπάρχει σε κάθε πορτοφόλι και με αυτό τον τρόπο δημιουργείται ένα μοναδικό σύστημα ηλεκτρονικών πληρωμών όπου ο λογαριασμός ανήκει μόνο στον κάτοχο.

9. Δεν υπάρχουν περιορισμοί και δεσμεύσεις και οι πληρωμές που γίνονται σε αυτό το σύστημα είναι αδύνατον να ακυρωθούν. Τα κέρματα δεν μπορούν να μην υπάρχουν, να αντιγράφονται ή να ξοδεύονται δύο φορές. Αυτές οι δυνατότητες εγγυώνται την ακεραιότητα ολόκληρου του συστήματος.

10. Διαφάνεια. Το BTC αποθηκεύει το ιστορικό όλων των συναλλαγών που έχουν πραγματοποιηθεί μέχρι κάποια στιγμή σε μια αλυσίδα μπλοκ που διατηρεί τις

πληροφορίες συνεχώς. Επομένως, αν κάποιος θέλει να ελέγξει κάποια διεύθυνση από ένα BTC, ενός τρίτου μπορεί και την ελέγχει και βλέπει τι συναλλαγές έχουν γίνει και αν το BTC πραγματικά ανήκει στον τρίτο που συναλλάσσεται.

11. Δεν υπάρχουν πιθανότητες να χρησιμοποιηθούν ορισμένα προσωπικά δεδομένα για διενέργεια απάτης, όπως αυτό μπορεί να γίνει με τις πιστωτικές κάρτες που χρειάζεται να πληκτρολογηθούν κάποια προσωπικά στοιχεία. Οι συναλλαγές του BTC δεν απαιτούν γνωστοποίηση οποιωνδήποτε προσωπικών δεδομένων. Αντίθετα, το BTC χρησιμοποιεί δύο κλειδιά: ένα δημόσιο και ένα ιδιωτικό. Το δημόσιο κλειδί είναι διαθέσιμο σε όλους (δηλ. η διεύθυνση του πορτοφολιού του bitcoin), αλλά το ιδιωτικό κλειδί είναι γνωστό μόνο στον κάτοχο. Η κάθε συναλλαγή πρέπει να υπογράφεται από τα ενδιαφερόμενα μέρη με την αλληλεπίδραση των ιδιωτικών κλειδιών που κατέχουν και την εφαρμογή μιας μαθηματικής σχέσης. Αυτή η διαδικασία δημιουργεί αποδείξεις ότι η συναλλαγή εκτελείται από τον ιδιοκτήτη.

12. Με τη χρήση των ψηφιακών νομισμάτων υπάρχει φορητότητα καθώς μπορεί κάποιος να πάρει μαζί του bitcoins σε ένα USB stick ή να τα μεταφέρει με ένα κινητό Android, χωρίς να χρειάζεται να τα δηλώσει πουθενά.

3.3.3 Τα μειονεκτήματα του bitcoin

Όσον αφορά τα μειονεκτήματα που παρουσιάζει το bitcoin τα πιο βασικά είναι:

1. Υπάρχει ισχυρή μεταβλητότητα - σχεδόν όλα τα σκαμπανεβάσματα της αξίας της BTC εξαρτώνται άμεσα από δηλώσεις των κυβερνήσεων των διαφόρων χωρών, από τις προθέσεις τους, τη πτώχευση διαφόρων πλατφορμών συναλλαγών σε bitcoins, τις κακόβουλες επιθέσεις χακαρίσματος . Αυτή η μεταβλητότητα στη μεγαλύτερη διάρκεια της περιόδου δημιουργεί το πρόβλημα .

Η μεταβλητότητα του Bitcoin είναι πιθανό να αποθαρρύνει πολλούς δυνητικούς αγοραστές.

2. Το γεγονός ότι λιγότερα από 50 άτομα , κατέχουν το ένα τρίτο των κρυπτονομισμάτων, ενέχει κινδύνους δημιουργίας ενός καρτέλ, το οποίο ενδεχομένως να έχει διάφορες επιδράσεις στη διαμόρφωση των τιμών του bitcoin , ειδικά όταν παρουσιασθεί ποτέ έλλειψη bitcoins στην αγορά

3. Υπάρχει κίνδυνος χρησιμοποίησης του bitcoin για πληρωμές παρανόμων πράξεων, όπως το ξέπλυμα χρήματος, η χρηματοδότηση τρομοκρατικών και άλλων παράνομων δραστηριοτήτων.

4. Δεδομένου ότι το Bitcoin είναι ένα αποκεντρωμένο νόμισμα και δεν υποστηρίζεται από οποιοδήποτε κεντρικό όργανο, στις περισσότερες περιπτώσεις, οι χρήστες δεν

μπορούν να ανακτήσουν κάποια από τις απώλειές τους, δεδομένου ότι δεν υπάρχει εξασφάλιση των καταθέσεων τους (Moore & Christin, 2014)

5. Δεν υπάρχει νομοθετικό ούτε θεσμικό πλαίσιο, και είναι άγνωστες οι επιπτώσεις που θα υπάρξουν αν κάποια στιγμή δημιουργηθεί κάποιο. Είναι επίσης αβέβαιο ακόμη και αν δημιουργηθεί αν θα μπορέσει να συμπεριλάβει όλες τις διαστάσεις καθώς επειδή είναι ένα λογισμικό ανοικτού κώδικα συνεχώς εξελίσσεται.

6. 'Ολες οι συναλλαγές είναι μη αναστρέψιμες και οποιοδήποτε λάθος δεν διορθώνεται. Ως εκ τούτου για τις συναλλαγές με bitcoin απαιτείται αυξημένη τεχνολογική εξοικείωση.

7. Η προσφορά bitcoins καθορίζεται από έναν μηχανισμό που δεν σχετίζεται με ένα μηχανισμό της αγοράς, και αυτό σημαίνει ότι υπάρχει ο κίνδυνος η αγορά bitcoins να είναι ρηχή και εύκολα χειραγωγήσιμη.

8. Υπάρχει ο κίνδυνος να χάσει κάποιος τα ιδιωτικά του κλειδιά, οπότε χάνει εντελώς στη περίπτωση αυτή και τον έλεγχο των bitcoins του.

3.4 Η αποθήκευση των bitcoins

Η αποθήκευση των bitcoins χρειάζεται να γίνεται για πολλούς ανεξάρτητους μεταξύ τους στόχους:

- Προστασία από τυχαία απώλεια
- Επαλήθευση ότι τα bitcoins είναι γνήσια
- Ιδιωτικότητα και προστασία από τρίτους
- Προστασία από κλοπή
- Εύκολη πρόσβαση για δαπάνες ή για τη διακίνηση bitcoins

Το όλο θέμα της αποθήκευσης bitcoins είναι για να βρίσκονται σε ασφάλεια τα ιδιωτικά κλειδιά που κατέχει κάποιος ενώ ταυτόχρονα αυτά θα είναι εύκολα διαθέσιμα όταν αυτά χρειάζονται για τις συναλλαγές. Η αποθήκευση διασφαλίζει επίσης τη γνησιότητα των bitcoins και την ιδιωτικότητα της περιουσίας σε ψηφιακά νομίσματα.

Σε αντίθεση με τα συμβατικά νομίσματα που αποθηκεύονται σε κανονικά πορτοφόλια και τραπεζικούς λογαριασμούς, τα κρυπτονομίσματα δεν χρησιμοποιούν πιστωτικά ιδρύματα ή θυρίδες για να αποθηκευτούν αλλά ο εκάστοτε χρήστης είναι και ο μοναδικός κύριος και υπεύθυνος των χρημάτων του. Τα bitcoins αποθηκεύονται σε κατάλληλα ''πορτοφόλια'' (wallets). Χωρίς ένα πορτοφόλι Bitcoin, δεν μπορεί κάποιος να στείλει ή να λάβει πληρωμές σε Bitcoin. Αλλά αντί να αποθηκεύει, με τη φυσική

έννοια Bitcoins, αυτό που αποθηκεύεται είναι πολλές σχετικές πληροφορίες όπως το ασφαλές ιδιωτικό κλειδί που χρησιμοποιείται για την πρόσβαση στις διευθύνσεις Bitcoin και τη διεξαγωγή συναλλαγών. Καθώς τα ψηφιακά νομίσματα δεν συνυπάρχουν σε ένα blockchain ή ένα κοινό δίκτυο και καθένα έχει το δικό του blockchain και δίκτυο χρηστών που το καθιστούν μοναδικό έχει και διαφορετικά ‘’πορτοφόλια’. Τα ‘’πορτοφόλια‘’ αυτά μπορεί να βρίσκονται μέσα στον υπολογιστή ή να βρίσκονται έξω από αυτόν.

Είναι προφανές ότι η έννοια της ‘’ψυχρής αποθήκευσης‘’ (cold storage) στον τομέα των bitcoins του Bitcoin αναφέρεται στη διατήρηση ενός αποθέματος bitcoins εκτός δικτύου. Αυτό είναι πολύ συχνά μια απαραίτητη προφύλαξη ασφάλειας, ειδικά για τη περίπτωση αποθήκευσης μεγάλων ποσοτήτων bitcoins.

Για παράδειγμα, σε ένα κέντρο ανταλλαγών bitcoins υπάρχει συνήθως η δυνατότητα άμεσης απόσυρσης και το κέντρο μπορεί να είναι διαχειριστής σε εκατοντάδες χιλιάδες Bitcoins. Για να ελαχιστοποιηθεί το ενδεχόμενο ένας εισβολέας να μπορεί να κλέψει ολόκληρο το απόθεμα σε περίπτωση παραβίασης της ασφάλειας, όπως για παράδειγμα συνέβη στο ανταλλακτήριο Mt.Gox, ο διαχειριστής του ιστότοπου ακολουθεί μια βέλτιστη πρακτική διατηρώντας το μεγαλύτερο μέρος του αποθεματικού σε ‘’ψυχρή αποθήκευση‘’ ή με άλλα λόγια δεν υπάρχει στο διακομιστή παρά μόνο το ποσό που απαιτείται για την κάλυψη των αναμενόμενων ημερήσιων αποσύρσεων.

Οι μέθοδοι αποθήκευσης εν ψυχρώ περιλαμβάνουν τη διατήρηση bitcoins σε :

- σε μια μονάδα USB ή σε άλλο μέσο αποθήκευσης δεδομένων σε ασφαλές μέρος (π.χ. θυρίδα ασφαλείας)
- σε πορτοφόλια χάρτινης μορφής, όπου αναγράφονται τα κλειδιά κρυπτογράφησης και φυλάσσονται σε θυρίδα
- σε ένα στοιχείο κομιστή, όπως ένα φυσικό bitcoin.
- σε ‘’ηλεκτρονικό πορτοφόλι’’ (Hardware wallet) για bitcoin εκτός σύνδεσης

Με τις μεθόδους ψυχρής αποθήκευσης υπάρχουν προβλήματα ασφαλείας, αλλά αυτά μπορούν εύκολα να μετριαστούν. Το πιο βασικό από αυτά είναι ότι σε ορισμένες περιπτώσεις τα μυστικά κλειδιά και οι εφεδρικές μονάδες μπορούν να χαθούν λόγω του μέσου στο οποίο αποθηκεύονται.

Ένα ‘’ηλεκτρονικό πορτοφόλι’’ γενικά είναι ένα πρόγραμμα λογισμικού που χρησιμοποιείται για την ασφαλή αποθήκευση, αποστολή και λήψη cryptocurrencies μέσω της διαχείρισης κάποιων ιδιωτικών και δημόσιων κρυπτογραφικών κλειδιών.

Τα ηλεκτρονικά πορτοφόλια χωρίζονται σε τρεις βασικές κατηγορίες ανάλογα το μέρος στο οποίο υπάρχουν. Η πρώτη κατηγορία και πιο διαδεδομένη, αφορά τα software wallets (πορτοφόλια λογισμικού).

Τα **software wallets** σε πολλές περιπτώσεις μπορεί να έχουν την ανάγκη δεκάδων GB αποθηκευτικού χώρου καθώς κάθε χρήστης κρατάει αποθηκευμένο μέσα στο πορτοφόλι του ένα αντίγραφο όλης της αλυσίδας των block (blockchain) και επομένως το κάθε πορτοφόλι αποτελεί ένα node (κόμβο) του δικτύου του συγκεκριμένου κρυπτονομίσματος. Τα software wallets είναι προγράμματα ανοιχτού κώδικα τα οποία εγκαθίστανται σε κάποιο από τα διαθέσιμα συστήματα που τρέχουν στο σύστημα που υπάρχει σε κάθε υπολογιστή, όπως Windows, Mac PC, Adnroid ή iOS smartphone και φυλάσσουν τα νομίσματα στον αποθηκευτικό χώρο της συσκευής. Τα εν λόγω πορτοφόλια αποτελούν την πρώτη λύση για εξοικειωμένους χρήστες καθώς δεν έχουν κανένα κόστος ενεργοποίησης ή χρήσης και δίνουν πλήρη έλεγχο στα κεφάλαια. (Κορδώνης, 2017).

Τα πορτοφόλια λογισμικού απαιτούν από τους ιδιοκτήτες τους να είναι πλήρως εξοικειωμένοι με τα θέματα των υπολογιστών και για το λόγο αυτό δεν μπορούν να χρησιμοποιηθούν εύκολα από όσους έτυχε να έχουν στη κατοχή τους cryptocurrencies αλλά δεν γνωρίζουν από ανάλογα θέματα .

Για το λόγο αυτό δημιουργήθηκαν οι διαδικτυακές υπηρεσίες αποθήκευσης ψηφιακών νομισμάτων, αλλιώς γνωστές και ως **Cloud Wallets.** Τα Cloud Wallets τρέχουν στη λειτουργία Cloud στο Διαδίκτυο και είναι προσβάσιμα από οποιαδήποτε υπολογιστική συσκευή σε οποιαδήποτε θέση. Πλέον αποτελούν την πρώτη λύση που θα σκεφτεί ένας νέος χρήστης, καθώς μπορούν να δημιουργηθούν σε δευτερόλεπτα, δεν απαιτούν καμία τεχνική ή εξειδικευμένη γνώση και δίνουν στο χρήστη τη δυνατότητα διαχείρισης από οποιοδήποτε μέρος του πλανήτη και από οποιαδήποτε συσκευή (Peterson & Van Weze, 2016). Ένα ακόμα πλεονέκτημα που έχουν τα Cloud Wallets έναντι των Software είναι η ικανότητά τους να αποθηκεύσουν παραπάνω από ένα είδος κρυπτονομίσματος. Οι υπηρεσίες έχουν αναπτύξει ειδικά πορτοφόλια τα οποία μπορούν να δεχθούν διαφόρων ειδών νομίσματα χωρίς να τα μπλέκουν μεταξύ τους.

Ενώ όμως είναι πιο βολικά για πρόσβαση, τα Cloud Wallets αποθηκεύουν τα ιδιωτικά κλειδιά online και ελέγχονται από ένα τρίτο μέρος γεγονός που τα καθιστά πιο ευάλωτα σε επιθέσεις και hacking. Οι διαδικτυακές υπηρεσίες ηλεκτρονικών πορτοφολιών, στην πλειοψηφία τους, αποποιούνται οποιαδήποτε ευθύνη σε περίπτωση απώλειας κεφαλαίων λόγω λαθών ή κλοπής από τρίτο και είναι πολλές οι περιπτώσεις που ακούγονται

επιθέσεις για hacking σε πορτοφόλια αυτής της μορφής με λεία εκατομμυρίων δολαρίων σε κρυπτονομίσματα ανυποψίαστων χρηστών.

Καθώς κάθε επιλογή που αναφέρθηκε έχει προτερήματα και μειονεκτήματα, πολλές εταιρείες, όπως οι Satoshi Labs και Ledger, στη προσπάθειά τους να δώσουν λύση δημιούργησαν τα πρώτα φυσικά ηλεκτρονικά πορτοφόλια γνωστά και ως **hardware wallets.** Το σκεπτικό των πορτοφολιών αυτής της μορφής είναι ότι πρόκειται για συσκευές, ειδικά σχεδιασμένες για την ασφαλή αποθήκευση και συναλλαγή ηλεκτρονικών νομισμάτων, δίνοντας στο χρήστη πλήρη εξουσία χωρίς να τον επιβαρύνουν με το blockchain. Όπως και τα cloud, έτσι και αυτά είναι ικανά να αποθηκεύσουν παραπάνω από ένα είδος κρυπτονομισμάτων.

Τα hardware wallets διαφέρουν από τα στο ότι αποθηκεύουν τα ιδιωτικά κλειδιά ενός χρήστη σε μια συσκευή υλικού όπως ένα USB. Παρόλο που τα hardware wallets πραγματοποιούν απευθείας συναλλαγές, αποθηκεύονται εκτός σύνδεσης και προσφέρουν αυξημένη ασφάλεια ενώ επιπλέον, η πραγματοποίηση μιας συναλλαγής είναι εύκολη. Οι χρήστες συνδέουν απλά τη συσκευή τους σε οποιονδήποτε υπολογιστή ή συσκευή με σύνδεση στο Internet, εισάγουν ένα αναγνωριστικό αριθμό , αποστέλλουν τη πληρωμή σε ψηφιακό νόμισμα και επιβεβαιώνουν. Τα hardware wallets καθιστούν δυνατή και εύκολη τη συναλλαγή ενώ παράλληλα κρατούν τα χρήματά εκτός σύνδεσης και επομένως μακριά από τον κίνδυνο (Franco, 2014)

Τα hardware wallets σε αντίθεση με τα software και cloud, κοστίζουν πραγματικά χρήματα για να τα αγοράσει κάποιος , ωστόσο σήμερα προσφέρουν τη μεγαλύτερη ασφάλεια που μπορεί να έχει κάποιος όσον αφορά την απώλεια και την κλοπή νομισμάτων.

Ενώ τα πορτοφόλια δεν συνδέονται με την πραγματική ταυτότητα ενός χρήστη, όλες οι συναλλαγές αποθηκεύονται δημοσίως και μόνιμα στην μπλοκ αλυσίδα, ως εκ τούτου τα κάθε είδους wallets το όνομα ή η προσωπική διεύθυνση του χρήστη δεν θα υπάρχουν, αλλά δεδομένα που υπάρχουν, όπως η διεύθυνση του πορτοφολιού του, θα μπορούσαν να εντοπίσουν την ταυτότητα του με διάφορους τρόπους.

Καθώς, όπως είδαμε υπάρχουν πολλές επιλογές για τα πορτοφόλια που χρειάζεται κάποιος για να αποθηκεύει τα χρήματα του κάθε φορά που χρειάζεται θα πρέπει να δίνει απαντήσεις σε τρεις βασικές ερωτήσεις που είναι

- χρειάζεται ένα πορτοφόλι για καθημερινές αγορές ή απλά για αποθήκευση ψηφιακών νομισμάτων για επένδυση

- σκοπεύει να χρησιμοποιήσει το πορτοφόλι για διάφορα ψηφιακά νομίσματα ή μόνο για ένα νόμισμα, π.χ. bitcoins
- χρειάζεται να έχει πρόσβαση στο ψηφιακό πορτοφόλι από οπουδήποτε ή μόνο από το σπίτι

και στη συνέχεια να κάνει την επιλογή του.

3.6 Τα εναλλακτικά ψηφιακά νομίσματα

Εικόνα 3.1 τα διάφορα κρυπτονομίσματα (πηγή: www.longreads.news247.gr)

3.6.1 Οι γενικές αρχές που υπάρχουν

Υπάρχουν πολλά διαφορετικά κρυπτονομίσματα που βασίζονται στις ίδιες αρχές με το bitcoin όσον αφορά τις συναλλαγές που γίνονται και παρουσιάζουν μόνο διαφορές σε επιμέρους χαρακτηριστικά. Αυτό οφείλεται στην ανοικτή φύση του λογισμικού του (open source) που διευκόλυνε πολλούς προγραμματιστές να τον τροποποιήσουν φτιάχνοντας νέα κρυπτονομίσματα. Τα κρυπτονομίσματα αυτά έχουν τις περισσότερες φορές αντιγράψει πολλά από τα χαρακτηριστικά του bitcoin καθώς συνήθως βασίζονται στον ίδιο κώδικα δημιουργίας με αυτό ή προέρχονται από τη δημιουργία κάποιου αντιγράφου του αλλά περιέχουν και βελτιώσεις ή και προσθήκες. Όσα κρυπτονομίσματα συνεισέφεραν στην απλούστευση των ηλεκτρονικών συναλλαγών κατάφεραν να επικρατήσουν και να συνδέσουν τη πορεία τους με εκείνη του bitcoin. Αντίθετα, όσα δεν προσέφεραν κάποιες ουσιαστικές και πρακτικές λειτουργίες ή και δημιουργήθηκαν για

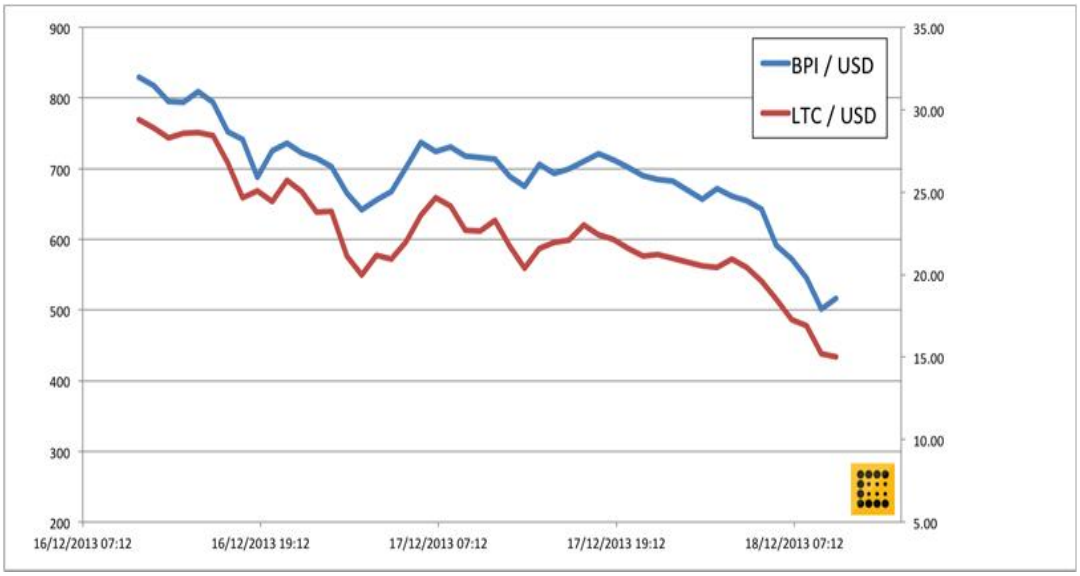
κερδοσκοπικούς λόγους εξαφανίσθηκαν. Όλα τα άλλα cryptocurrencies, εκτός από το bitcoin ονομάζονται Altcoins. Στη συνέχεια θα περιγράψουμε κάποια από αυτά όπως είναι το Litecoin, το Ripple και το Ethereum. Μέχρι σήμερα το bitcoin είναι μακράν το πιο σημαντικό υπόδειγμα κρυπτονομίσματος, αλλά πληθαίνουν τα Altcoins που στοχεύουν να μειώσουν κάποιους από τους περιορισμούς που παρουσιάζονται στα bitcoins και να εμφανίσουν νέες επιλογές που να έχουν περισσότερα συγκριτικά πλεονεκτήματα.

Στη συνέχεια παραθέτουμε ένα ενδιαφέρον γράφημα που δείχνει την ομοιότητα της συμπεριφοράς των cryptocurrencies. Στο γράφημα υπάρχει η εξέλιξη της σχέσης τιμής τόσο του bitcoin όσο και του Litecoin, που μέχρι το 2011 ήταν το κρυπτονόμισμα με την επόμενη μεγαλύτερη διάδοση μετά το bitcoin, ως προς το δολάριο ΗΠΑ. Είναι σαφές από το γράφημα ότι για τη συγκεκριμένη περίοδο η εξέλιξη των τιμών του Litecoin είναι σχεδόν ταυτόσημη με εκείνη του bitcoin.

Στη πραγματικότητα βέβαια οι τιμές των άλλων κρυπτονομισμάτων, έναντι οποιουδήποτε συμβατικού νομίσματος, συνδέονται άμεσα με την τιμή του bitcoin. Το bitcoin είναι μακράν το βασικό κρυπτονόμισμα και το μόνο επομένως νόμισμα στο οποίο αναφέρονται και όλα τα υπόλοιπα. Πέραν τούτου οι μεταβολές της αξίας των κρυπτονομισμάτων δεν ακολουθούν τη λογική που ερμηνεύει τις μεταβολές των συμβατικών νομισμάτων αλλά τη λογική που καθιερώνει η συμπεριφορά του bitcoin .

Αντίθετα με ότι συμβαίνει με τα bitcoins τα Altcoins τις περισσότερες φορές δεν έχουν περιορισμούς, που επιβάλλονται από το σύστημα παραγωγής τους, και για το λόγο αυτό είναι και πιο ευέλικτα. Εν γένει λοιπόν τα Altcoins μπορεί να διαφέρουν από το bitcoin με διάφορους τρόπους. Ορισμένα Altcoins βασίζονται σε ένα διαφορετικό οικονομικό μοντέλο ή σε μια διαφορετική μέθοδο δημιουργίας, άλλα χρησιμοποιούν διαφορετικούς PoW αλγόριθμους εξόρυξης, ίσως για να ξεπεράσουν την ανάγκη χρήσης κάποιου σε εξειδικευμένου hardware για την εξόρυξη, και άλλα ίσως δεν βασίζονται καν σε αποδείξεις εργασίας. Αρκετά Altcoins προσφέρουν μια πιο ευέλικτη γλώσσα προγραμματισμού για να χτισθούν κάποιες εφαρμογές στηριγμένες σε αυτά, ενώ άλλα πάλι προσφέρουν ακόμα πιο κλειστό περιβάλλον σε σχέση με το bitcoin. Και υπάρχουν επίσης Altcoins που εξυπηρετούν πολύ συγκεκριμένες περιπτώσεις μη χρηματικής χρήσης, όπως μητρώα ονομάτων, ονόματα τομέων ή δείκτες αποθήκευσης δεδομένων.

Στα συμβατικά νομίσματα οι αξίες μεταβάλλονται λόγω μιας σειράς γεγονότων που συμβαίνουν ή συνθηκών που αλλάζουν. Στην αγορά των cryptocurrencies η λογική που υπάρχει είναι διαφορετική.



Εικόνα 3.2 η εξέλιξη ως προς $USD για Bitcoin και Litecoin (πηγή: Coindesk)

Όταν η αξία του bitcoin ανεβαίνει, και οι αξίες των άλλων κρυπτονομισμάτων ανεβαίνουν, επειδή οι περισσότεροι πιστεύουν ότι αν το bitcoin ανεβαίνει, αυτό σημαίνει ότι οι αγορές των cryptocurrencies στο σύνολο τους είναι "υγιείς" και "ασφαλείς". Όταν πάλι το bitcoin πέφτει, είτε όλα τα κρυπτονομίσματα πέφτουν, είτε όλα τα άλλα ανεβαίνουν, επειδή οι επενδυτές μεταφέρουν τα χρήματά τους από το bitcoin στα άλλα alt-coins (Torpey, 2017).

Εκτός όμως από την εξέλιξη των τιμών των άλλων κρυπτονομισμάτων που ακολουθούν το bitcoin, ένας άλλος λόγος για τον οποίο οι όροι cryptocurrencies και bitcoins θεωρούνται ταυτόσημοι είναι ότι μέχρι πολύ πρόσφατα πάνω από το 80% όλων των κεφαλαίων που είχαν επενδυθεί σε κρυπτονομίσματα βρίσκονταν επενδυμένα σε bitcoins. Σήμερα οι συνθήκες φαίνεται ότι έχουν αλλάξει. Στην αγορά των κρυπτονομισμάτων υπάρχουν σήμερα 1585 είδη κρυπτονομισμάτων, όταν τον Αύγουστο του 2014 υπήρχαν μόνο 462. Η αγορά των bitcoins έχει σήμερα κεφαλαιοποίηση ύψους 144,7 δισ. δολαρίων αλλά αποτελεί πλέον ένα ποσοστό μόνο 38,3% της συνολικής κεφαλαιοποίησης της αγοράς cryptocurrencies ύψους $ 378,2 δισ. δολαρίων, όπως φαίνεται και στον πίνακα που ακολουθεί με τα έξι πιο διαδεδομένα κρυπτονομίσματα (CoinMarketCap, 2017)

Είδος	**Ύψος της κεφαλαιοποίησης**	**τιμή σε δολάρια**

κρυπτονομίσματος	(σε δισ. δολάρια)	
Bitcoin (BTC)	144,721	8519,3
Ethereum (ETH)	58,606	592,3
Ripple (XRP)	34,356	0,878
Bitcoin cash	19,015	1113,1
EOS	8,988	11,2
Litecoin (LTC)	8,546	152,2

Εικόνα 3.3. πίνακας με την αξία και τη κεφαλιοποίηση αγοράς για τα βασικά κρυπτονομίσματα (πηγή: www.coinmarketcap.com)

3.6.2 Κάποια από τα κρυπτονομίσματα

Το Litecoin (LTC):

Το Litecoin είναι ένα ψηφιακό νόμισμα που επιτρέπει τις άμεσες πληρωμές σε οποιονδήποτε, οπουδήποτε στον κόσμο.Το Litecoin χρησιμοποιεί την τεχνολογία ομότιμης συνεργασίας (peer-to-peer) για να λειτουργεί, και έχει, όπως και το bitcoin το χαρακτηριστικό το ότι δεν έχει δημιουργηθεί από μια κεντρική αρχή: η διαχείριση των συναλλαγών και η έκδοση χρημάτων πραγματοποιούνται συλλογικά από το δίκτυο. Το Litecoin Core είναι το όνομα του λογισμικού ανοιχτού κώδικα που επιτρέπει τη χρήση αυτού του νομίσματος.

Με βάση την κεφαλαιοποίηση της αγοράς (ή τα διαθέσιμα νομίσματα στην αγορά), το Litecoin είναι το τρίτο πιο διαδεδομένο κρυπτονόμισμα μετά το bitcoin και το XRP. Το Litecoin, όπως και τα άλλα ψηφιακά νομίσματα που εμφανίσθηκαν παράλληλα, λειτουργεί ως ένα σύστημα ηλεκτρονικών πληρωμών. Όπως το PayPal ή το ηλεκτρονικό δίκτυο μιας τράπεζας, οι χρήστες μπορούν να το χρησιμοποιήσουν για να ανταλλάξουν πληρωμές μεταξύ τους μόνο που αντί να χρησιμοποιούν δολάρια USD, πραγματοποιούν συναλλαγές σε μονάδες Litecoin. Αυτός είναι και ο λόγος για την ομοιότητα του Litecoin με τα περισσότερα παραδοσιακά νομίσματα και τα συστήματα πληρωμών.

Όπως όλες οι cryptocurrencies, το Litecoin δεν εκδίδεται από μια κυβέρνηση, η οποία ιστορικά ήταν η μόνη οντότητα που η κοινωνία εμπιστεύεται να εκδώσει χρήματα. Αντί να ρυθμίζονται από μια Κεντρική Τράπεζα τα Litecoins δημιουργούνται από την περίπλοκη διαδικασία που ονομάζεται εξόρυξη, η οποία συνίσταται στην επεξεργασία ενός καταλόγου συναλλαγών Litecoin. Σε αντίθεση με τα παραδοσιακά νομίσματα, η

προσφορά των Litecoins είναι σταθερή καθώς τελικά θα υπάρχουν μόνο 84 εκατομμύρια Litecoins σε κυκλοφορία. Κάθε 2,5 λεπτά (σε αντίθεση με τα 10 λεπτά για bitcoin), το δίκτυο Litecoins παράγει αυτό που ονομάζεται block, δηλαδή ένα αρχείο των πρόσφατων συναλλαγών Litecoins σε όλο τον κόσμο. Το μπλοκ επαληθεύεται από ένα λογισμικό εξόρυξης και γίνεται ορατό σε οποιονδήποτε εξορύκτη που θέλει να το δει. Μόλις το επαληθεύσει ο εξορύκτης , προστίθεται στην αλυσίδα το επόμενο μπλοκ, το οποίο με τη σειρά του αποτελεί αρχείο κάθε νέας συναλλαγής σε Litecoin. Η πιο βασική τεχνική διαφορά μεταξύ του bitcoin και του Litecoin είναι οι διαφορετικοί κρυπτογραφικοί αλγόριθμοι που χρησιμοποιούν. Το bitcoin χρησιμοποιεί τον κλασσικό αλγόριθμο SHA-256, ενώ το Litecoin χρησιμοποιεί έναν σχετικά νέο αλγόριθμο γνωστό ως Scrypt (Fernando, 2018)**.**

Το κίνητρο για την εξόρυξη είναι ότι ο πρώτος εξορύκτης που θα επαληθεύσει με επιτυχία ένα μπλοκ ανταμείβεται με 50 Litecoins. Ο αριθμός των litecoins που απονέμονται για τη περίσταση αυτή μειώνεται με την πάροδο του χρόνου. Τον Οκτώβριο του 2015 μειώθηκε στο μισό και η μείωση κατά το ήμισυ του υπάρχοντος τη συγκεκριμένη στιγμή αριθμού θα συνεχίζεται σε τακτά χρονικά διαστήματα έως ότου εξορυχθεί το 84.000.000^{ο} Litecoin.

Η εξόρυξη κρυπτονομισμάτων με ένα ρυθμό που αξίζει τον κόπο στους εξορύκτες να ασχοληθούν απαιτεί τεράστιες δυνατότητες επεξεργασίας συνοδεία ενός κατάλληλου, εξειδικευμένου εξοπλισμού.. Αυτό το χαρακτηριστικό οδηγεί σε ένα άλλο σημείο διαφοροποίησης για τα Litecoins, καθώς αυτά μπορούν να εξορύσσονται και με συνηθισμένους υπολογιστές αν και όσο είναι μεγαλύτερη η χωρητικότητα ενός υπολογιστικού συστήματος για εξόρυξη, τόσο αυξάνει η πιθανότητα να έχει ο εξορύκτης μια καλή απόδοση.

Οποιοδήποτε νόμισμα, ακόμα και το δολάριο των Η.Π.Α. USD, ακόμη και οι ράβδοι χρυσού είναι μόνο τόσο πολύτιμοι όσο το πιστεύει η κοινωνία. Αν η Ομοσπονδιακή Τράπεζα των ΗΠΑ έθετε σε κυκλοφορία πάρα πολλά τραπεζογραμμάτια, η αξία του δολαρίου θα έπεφτε βραχυπρόθεσμα, φαινόμενο γνωστό και ως πληθωριστικές πιέσεις από τη κυκλοφορία νέου χρήματος. Το φαινόμενο αυτό όμως ξεπερνά τα νομίσματα. Οποιοδήποτε αγαθό ή υπηρεσία γίνεται λιγότερο πολύτιμο, τόσο πιο εύκολα και φθηνότερα είναι διαθέσιμο και αυτό ισχύει και αντίστροφα. Οι δημιουργοί του Litecoin κατανοούσαν από την αρχή ότι θα ήταν δύσκολο για ένα νέο νόμισμα να αναπτύξει μια φήμη στην αγορά αλλά δηλώνοντας τον περιορισμό του αριθμού των Litecoins που

κυκλοφορούν, οι δημιουργοί του Litecoin καθησυχάζουν κάπως τους φόβους των ανθρώπων για υπερπαραγωγή κρυπτονομισμάτων.

Το Litecoin εμφανίζει κάποια εγγενή πλεονεκτήματα έναντι bitcoin καθώς

- το Litecoin μπορεί να χειριστεί περισσότερες συναλλαγές, δεδομένου του μικρότερου χρόνου δημιουργίας μπλοκ.
- το Litecoin έχει επίσης μια ελάχιστη χρέωση συναλλαγής κόστους 1/1000 ενός Litecoin για την επεξεργασία μιας συναλλαγής, ανεξάρτητα από το μέγεθός της ενώ για παράδειγμα 3% η αμοιβή του PayPal είναι 3%.

Μόλις ένα νόμισμα φθάσει να έχει μια κρίσιμη μάζα χρηστών που είναι βέβαιοι ότι το νόμισμα αξίζει πράγματι αυτό που αντιπροσωπεύει και πιθανότατα δεν θα χάσει την αξία του, μπορεί να καθιερωθεί ως μέθοδος πληρωμής.

Το Litecoin δεν είναι ελάχιστα αποδεκτό, καθώς ακόμη και οι ιδρυτές του παραδέχονται ότι έχει λιγότερους από 100.000 χρήστες. (ακόμη και το bitcoin έχει πιθανώς λιγότερους από μισό εκατομμύριο συνολικά χρήστες.) Καθώς όμως τα κρυπτονομίσματα γίνονται πλέον εύκολα αποδεκτές και οι αξίες τους σταθεροποιούνται, ένα ή δύο από αυτά, συμπεριλαμβανομένου και του litecoin, πιθανόν θα προκύψουν ως ψηφιακά νομίσματα για γενική χρήση (McFarlane, 2017).

Το Ripple (XRP)

Το Ripple είναι ένα δίκτυο ακαθάριστων συναλλαγών σε πραγματικό χρόνο (RTGS), και δεν είναι αποκεντροποιημένο αλλά συνδέεται με μία μόνο εταιρεία την εταιρεία Ripple. Το Ripple παρέχει τη δυνατότητα της αποστολής, χωρίς προβλήματα, σε όλο τον κόσμο χρημάτων χρησιμοποιώντας τη δύναμη του blockchain. Λειτουργεί επομένως όπως και το σύστημα αποστολής συμβατικών χρημάτων από τα χρηματοπιστωτικά ιδρύματα που προσχωρώντας στο δίκτυο της Ripple, μπορούν να επεξεργαστούν τις πληρωμές των πελατών τους οπουδήποτε στον κόσμο άμεσα, αξιόπιστα και με μικρότερο οικονομικό κόστος.

Δημιουργήθηκε το 2012 από την εταιρεία Ripple και βασίζεται σε ένα κατανεμημένο πρωτόκολλο διαδικτύου ανοιχτού κώδικα, ένα βιβλίο συναινέσεων και το κρυπτονόμισμα που εμφανίζεται σε συντομογραφία ως XRP. Στον πυρήνα του, το Ripple/XRP βασίζεται σε μια κοινόχρηστη και δημόσια βάση δεδομένων, ή ημερολόγιο, η οποία χρησιμοποιεί μια διαδικασία συναίνεσης που επιτρέπει πληρωμές, ανταλλαγές

και εμβάσματα σε μια κατανεμημένη διαδικασία. Το XRP φαίνεται ότι είναι το πρώτο "φιλικό" κρυπτονόμισμα προς το παραδοσιακό χρηματοπιστωτικό σύστημα, που έχει μάλιστα ως στόχο να προσφέρει σημαντικά οφέλη στον κλάδο. Η ιδέα για τη δημιουργία του ήταν να δημιουργηθεί ένα σύστημα άμεσης μεταβίβασης περιουσιακών στοιχείων (π.χ. χρημάτων, χρυσών κ.λπ.) που ρυθμίζεται σχεδόν σε πραγματικό χρόνο και είναι μια φθηνότερη, διαφανέστερη και ασφαλέστερη εναλλακτική λύση για τη μεταφορά αξιών που χρησιμοποιούν σήμερα οι τράπεζες (SWIFT). Οι τράπεζες και οι πάροχοι πληρωμών μπορούν να χρησιμοποιήσουν το ψηφιακό στοιχείο XRP για να μειώσουν περαιτέρω το κόστος τους και να αποκτήσουν πρόσβαση σε νέες αγορές, ως εκ τούτοτο Ripple/ XRP προσφέρει στις χρηματοοικονομικές συναλλαγές τις ίδιες δυνατότητες που προσέφερε το Διαδίκτυο στις άλλες μορφές πληροφόρησης. Επιδιώκει να επιτρέψει ασφαλείς, άμεσες και σχεδόν ελεύθερες παγκόσμιες οικονομικές συναλλαγές οποιουδήποτε μεγέθους, να συμβάλλει δηλαδή στη δημιουργία μίας ελεύθερης ροής χρήματος (Μωράτης, 2017) Υποστηρίζει συναλλαγές σε όλα τα συμβατικά νομίσματα, σε ψηφιακά νομίσματα, εμπορεύματα ή οποιαδήποτε άλλη μονάδα έχει αξία. τις μάρκες που αντιπροσωπεύουν το νόμισμα fiat, την κρυπτογράφηση, το εμπόρευμα ή οποιαδήποτε άλλη μονάδα αξίας, όπως για παράδειγμα τα μίλια συχνών πτήσεων ή τα κινητά λεπτά (www. Wikipedia). Μετατρέποντας αρχικά την αξία της μεταφοράς σε XRP, αντί του USD, τα τέλη ανταλλαγής εξαλείφονται και η επεξεργασία των πληρωμών μειώνεται σε δευτερόλεπτα.

Το XRP είναι μια μονάδα (token) που χρησιμοποιείται για την απεικόνιση της μεταφοράς αξίας μέσω του δικτύου Ripple. Διαφέροντας με το bitcoin, όπου συνεχώς δημιουργούνται νέα κέρματα (ως το ανώτατο όριο) ως ανταμοιβές για τους συμμετέχοντες που προσφέρουν υπολογιστική ισχύ για να διατηρήσουν το δίκτυο blockchain, η Ripple δημιούργησε 100 δισεκατομμύρια νομίσματα XRP κατά την εκκίνησή της.

Το Ripple πρόσθεσε πρόσφατα ένα νέο χαρακτηριστικό στο σύστημα, σύμφωνα με το οποίο, μέσω ενός έξυπνου συμβολαίου (escrows), η εταιρεία ελευθερώνει κάθε μήνα 1 δισεκατομμύριο XRP από όσα έχει στη κατοχή της για να χρηματοδοτήσει επιχειρηματικές δραστηριότητες, να ενθαρρύνει τους πελάτες και να πουλήσει σε διαπιστευμένους επενδυτές. Τυχόν αχρησιμοποίητες μάρκες θα τοποθετηθούν ξανά σε μεσεγγύηση. Σύμφωνα με εσωτερικές πηγές, τον προηγούμενο μήνα το Ripple χρησιμοποίησε περίπου 100 εκατομμύρια XRP και έβαλε επομένως πίσω τα υπόλοιπα 900 εκατομμύρια XRP πάλι σε μεσεγγύηση (Marr, 2018).

Τα XRP διακινούνται σε κέντρα ανταλλαγών cryptocurrencies όπως τα Binance και Poloniex. Συνήθως, δεν είναι δυνατή η αγορά τους με υπάρχοντα συμβατικά νομίσματα και επομένως θα πρέπει πρώτα να αγορασθούν bitcoins ή Ethereum και, στη συνέχεια, να γίνει η ανταλλαγή τους με XRP.

Το Ripple έχει σίγουρα δημιουργήσει μεγάλη δυναμική και η λίστα των οργανισμών που το χρησιμοποιούν δείχνει ότι τα XRP θα γίνουν βασικές αξίες από μόνες τους. Συνεργάζεται ήδη με πάνω από 90 τράπεζες, μερικές εκ των οποίων είναι οι BBVA, Santander, Axis Bank, Westpac, Union Credit, NBAD, UBS και Bank of Tokyo-Mitsubishi UFJ, ενώ ανάμεσα στους επενδυτές της βρίσκονται ονόματα γνωστά στους παραδοσιακούς επενδυτικούς κύκλους, όπως είναι η IDG Capital Partners, η Google, η Andreessen-Horowitz, η Seagate Technology και η Accenture. Στην πραγματικότητα, το 2017, η αύξηση της αξίας ενός XRP ξεπέρασε το Bitcoin ή οποιοδήποτε άλλο κρυπτονόμισμα. Στις αρχές του 2017 ένα XRP είχε αξία $ 0,006 δολάρια USD και μέσα σε δύο μήνες έφθασαν τα $ 5,65 δολάρια USD, πριν κατρακυλήσει πάλι στην τρέχουσα αξία του που είναι περίπου $ 1 δολάριο USD ανά XRP.

Ένα ακόμη πλεονέκτημα της χρήσης του κρυπτονομίσματος Ripple είναι η ταχύτητα με την οποία εκτελούνται οι συναλλαγές. Μία συναλλαγή με τη χρήση του Ripple χρειάζεται περίπου 4 δευτερόλεπτα για να ολοκληρωθεί, ενώ μία αντίστοιχη, μέσω του παραδοσιακού συστήματος, χρειάζεται 3-5 μέρες, μέσω του Ethereum περίπου 2 λεπτά και με τη χρήση του Bitcoin 1 ώρα. Ως εκ τούτου, το δίκτυο του Ripple μπορεί να διαχειριστεί 1.500 συναλλαγές το δευτερόλεπτο, ενώ το δίκτυο του Ethereum 15 συναλλαγές και του bitcoin 6 μόνο συναλλαγές (Μωράτης, 2017)

Το Ethereum

Πρόκειται για ένα ψηφιακό νόμισμα αλλά και μια πλατφόρμα blockchain ανοικτού κώδικα με προγραμματιζόμενη λειτουργία συναλλαγών. Η τεχνολογία blockchain είναι η κύρια διαφορά του Ethereum από το Bitcoin. Στο Ethereum η τεχνολογία blockchain δίνει την δυνατότητα να αναπτυχθούν διαφορετικές, ανεξάρτητες εφαρμογές που τρέχουν μέσω του δικού του δικτύου .

Αν το Διαδίκτυο προσφέρει μια αποκεντρωμένη πρόσβαση στην πληροφόρηση, αυξάνοντας έτσι την δυνατότητα άμεσης πρόσβασης στα διάφορα μέσα επικοινωνίας, το όραμα που υπάρχει όπως είδαμε για τη τεχνολογία blockchain είναι ότι θα αποκεντρωθεί

και θα μειώσει τα εμπόδια για τις συναλλαγές στον ψηφιακό κόσμο, εδραιώνοντας παράλληλα την εμπιστοσύνη σε αυτές.

Το Ethereum εμφανίσθηκε το 2014 από τον Ρωσοκαναδό Vitalik Buterin, καθώς φάνηκε ότι υπάρχουν περιορισμοί στη λειτουργία του bitcoin και συγκεκριμένα στο γεγονός ότι το bitcoin δεν έχει σχεδιαστεί για να χρησιμεύσει ως απάντηση του blockchain στο πρωτόκολλο ελέγχου μετάδοσης (TCP) ή στο πρωτόκολλο Internet (IP), τον κώδικα που αποτελεί τη βασική γλώσσα επικοινωνίας στο Διαδίκτυο (Mayer, 2018). Με την εμφάνιση του δημιουργήθηκε μια πλατφόρμα που επιτρέπει τις συναλλαγές στο Διαδίκτυο και οι υπηρεσίες που προσφέρονται μπορεί να είναι διαφόρων ειδών, όπως:

- δημιουργία ενός νέου συστήματος ψηφιακών πληρωμών
- ένα καινούργιο ηλεκτρονικό νόμισμα
- ανάπτυξη μιας marketplace όπου γίνονται αγοραπωλησίες σε κρυπτονομίσματα

Στο δίκτυο της Ethereum, οι εφαρμογές λέγονται smart contracts. Κατασκευάζονται κυρίως με την γλώσσα προγραμματισμού Solidity. Για κάθε εφαρμογή, ο δημιουργός θα πρέπει να καταβάλλει ένα αντίτιμο στο νόμισμα του δικτύου, το Ether (Μπάλας, 2017) .

Εξ ορισμού, η Ethereum είναι μια πλατφόρμα λογισμικού που στοχεύει να λειτουργεί ως αποκεντρωμένο Διαδίκτυο καθώς και ως αποκεντρωμένο κατάστημα εφαρμογών. Ένα τέτοιο σύστημα χρειάζεται ένα νόμισμα για να πληρώνει τους υπολογιστικούς πόρους που απαιτούνται για την εκτέλεση μιας εφαρμογής ή ενός προγράμματος και το νόμισμα αυτό είναι το Ether.

Το Ether είναι ψηφιακό στοιχείο που διακινείται χωρίς να απαιτεί από τρίτο να επεξεργαστεί την πληρωμή. Ωστόσο, το Ether δεν λειτουργεί μόνο ως ψηφιακό νόμισμα, αλλά λειτουργεί και ως ‘’καύσιμο’’ για τις αποκεντρωμένες εφαρμογές του δικτύου. Αν δηλαδή ένας χρήστης θέλει να αλλάξει κάτι σε μία από τις εφαρμογές του Ethereum, πρέπει να πληρώσει ένα τέλος συναλλαγής, έτσι ώστε το δίκτυο να μπορεί να επεξεργαστεί την αλλαγή (www.cointelegraph.com)

Τα τέλη συναλλαγών υπολογίζονται αυτόματα με βάση τη ποσότητα ‘’καύσιμου’’ που χρειάζεται μια ενέργεια. Η ποσότητα του απαιτούμενου καυσίμου υπολογίζεται με βάση πόση υπολογιστική ισχύς είναι απαραίτητη και πόσο χρόνο θα χρειαστεί για να τρέξει.

Ουσιαστικά, το Ethereum είναι μια παγκόσμια υπολογιστική μηχανή. Αποτελείται από τους δεκάδες χιλιάδες υπολογιστές που συνδέονται στο δίκτυο για να σφραγίσουν συναλλαγές και οι πόροι τους τρέχουν τις εφαρμογές που δημιουργούνται. Αυτό που προσφέρει το Ethereum είναι μια τεχνολογία blockchain με μια ενσωματωμένη ολοκληρωμένη γλώσσα προγραμματισμού Turing, που μπορεί να χρησιμοποιηθεί για τη δημιουργία "συμβολαίων" που χρησιμοποιούνται για την κωδικοποίηση λειτουργιών μετάβασης σε τυχαίες καταστάσεις, επιτρέποντας στους χρήστες να δημιουργήσουν οποιαδήποτε από τις εφαρμογές που περιγράφονται παραπάνω , καθώς και πολλές άλλες που δεν έχουν εμφανισθεί ακόμη γράφοντας τη λογική τους σε λίγες γραμμές κώδικα (Dannen, 2017).

Η φιλοσοφία που κρύβεται πίσω από το Ethereum ακολουθεί τις ακόλουθες αρχές:

Απλότητα: το πρωτόκολλο Ethereum θα πρέπει να είναι όσο το δυνατόν πιο απλό, έστω και αν θυσιάζεται χώρος αποθήκευσης ή ταχύτητα συναλλαγών. Ένας μέσος προγραμματιστής πρέπει ιδανικά να είναι σε θέση να ακολουθήσει και να εφαρμόσει ολόκληρη τη διαδικασία ώστε να αξιοποιηθεί πλήρως η αίσθηση της κοινοκτημοσύνης που προσφέρει η τεχνολογία των cryptocurrencies και το βασικό χαρακτηριστικό του Ethereum που είναι ένα πρωτόκολλο ανοιχτό σε όλους. Οποιαδήποτε βελτιστοποίηση που προσθέτει πολυπλοκότητα δεν πρέπει να περιλαμβάνεται εκτός αν η βελτιστοποίηση που γίνεται προσφέρει πολύ σημαντικό όφελος (www.cointelegraph.com)

Γενίκευση: ένα θεμελιώδες στοιχείο της φιλοσοφίας σχεδιασμού του Ethereum είναι ότι το Ethereum δεν έχει δικά του "χαρακτηριστικά". Αντ 'αυτού, το Ethereum παρέχει μια εσωτερική γλώσσα προγραμματισμού Turing-complete, την οποία ένας προγραμματιστής μπορεί να χρησιμοποιήσει για να κατασκευάσει, για δική του χρήση, κάθε έξυπνο συμβόλαιο ή τύπο συναλλαγής που μπορεί να οριστεί μαθηματικά, όπως για παράδειγμα ένα ιδιαίτερο χρηματοοικονομικό παράγωγο ή ιδιωτικό νόμισμα.

Συνδεσιμότητα (Modularity): Τα μέρη του πρωτοκόλλου Ethereum θα πρέπει να σχεδιάζονται έτσι ώστε να είναι όσο γίνεται πιο αρθρωτά και διαχωρίσιμα. Κατά τη διάρκεια της ανάπτυξης, ο στόχος είναι να δημιουργηθεί ένα πρόγραμμα όπου, αν κάποιος πρόκειται να κάνει μια μικρή τροποποίηση πρωτοκόλλου σε ένα μέρος του προγράμματος αυτού, όλες οι εφαρμογές να συνεχίσουν να λειτουργούν χωρίς περαιτέρω τροποποιήσεις. Οι όποιες καινοτομίες όπως το Ethash ή τα τροποποιημένα δέντρα θα πρέπει να δημιουργούνται και να χρησιμοποιούνται ως χωριστές βιβλιοθήκες και να

έχουν τέτοια χαρακτηριστικά που ακόμη και να δεν τα χρειάζεται το Ethereum να υπάρχουν για να χρησιμοποιηθούν αλλού και να διευκολύνουν με τον τρόπο αυτό την επεκτασιμότητα του Ethereum .

Ευελιξία: οι λεπτομέρειες για τα χαρακτηριστικά του πρωτοκόλλου Ethereum δεν είναι αμετακίνητες παρά το γεγονός, όπως προαναφέρθηκε, ότι δεν πρέπει να γίνονται αλλαγές για μη σοβαρές αιτίες. Αν η πράξη δείξει ότι ορισμένες τροποποιήσεις, π.χ. στην αρχιτεκτονική πρωτοκόλλου ή στην εικονική μηχανή Ethereum (EVM), θα βελτιώσουν σημαντικά την επεκτασιμότητα ή την ασφάλεια χρειάζεται το πρωτόκολλο να έχει τη δυνατότητα να τις δεχθεί.

Έλλειψη περιορισμών: το πρωτόκολλο δεν πρέπει να προσπαθεί να περιορίσει ή να αποτρέψει συγκεκριμένες κατηγορίες χρήσης. Όλοι οι ρυθμιστικοί μηχανισμοί στο πρωτόκολλο πρέπει να σχεδιάζονται έτσι ώστε να ρυθμίζουν άμεσα τυχόν βλάβες και να μην επιχειρούν να αντιταχθούν σε συγκεκριμένες ανεπιθύμητες εφαρμογές. Θα πρέπει επίσης ένας προγραμματιστής να έχει τη δυνατότητα να εκτελεί ακόμη και ένα άπειρο αριθμό προσπαθειών μέσα από το Ethereum για όσο διάστημα είναι διατεθειμένος να συνεχίζει να πληρώνει τα τέλη συναλλαγών ανά στάδιο υπολογισμού.

Μια από τις ιδέες που βρήκαν εφαρμογή στην πλατφόρμα του Ethereum, ήταν η δημιουργία ενός ανεξάρτητου και αυτόνομου οργανισμού με ψηφιακά κεφάλαια επιχειρηματικών συμμετοχών (venture capital funds). Ο σκοπός αυτών των οργανισμών είναι να υποστηρίζουν οικονομικά νέες startup επιχειρήσεις. Με απλά λόγια, να χρηματοδοτούν νέες καινοτόμες επιχειρηματικές ιδέες με σκοπό φυσικά το κέρδος. Η ιδέα ξεκίνησε τον Απρίλιο του 2016 όταν ο προγραμματιστής Christoph Jentzsch ανακοίνωσε τον οργανισμό μιας Decentralized Autonomous Organization (DAO) και με τη τεχνολογία των smart contracts του Ethereum, δημιούργησε τα νομίσματα DAO tokens (Μπάλας, 2017) με τα οποία, όσοι τα κατέχουν μπορούν αν θέλουν να συμμετέχουν μέσω της διαδικασίας των Initial Coin Offerings (ICOs) στην αύξηση του κεφαλαίου μιας startup επιχείρησης που, αν πετύχει, επιστρέφει μέρος των κερδών της στους επενδυτές ανάλογα με τα tokens συμμετοχής τους (Μπάλας, 2017).

Ενδεικτικό της επιτυχίας της ιδέας αυτής είναι ότι ένα μόλις μήνα μετά, τον Μάιο του 2016, η αξία των χρημάτων που επενδύθηκαν σε DAO tokens ξεπερνούσε τα $150 εκατομμύρια, προσελκύοντας πάνω από 11.000 επενδυτές ενώ παράλληλα η τιμή των κρυπτονομισμάτων συνεχώς στην αντίστοιχη αγορά.

Τον Ιούνιο του 2016, το DAO δέχτηκε διαδικτυακή επίθεση από hackers, οι οποίοι εκμεταλλεύθηκαν ορισμένα κενά ασφαλείας στα smart contracts του και έκλεψαν το ένα τρίτο των ψηφιακών περιουσιακών στοιχείων του, δηλαδή περίπου 50 εκ. δολάρια USD. Ο αντίκτυπος ήταν μεγάλος και για το Ethereum καθώς το DAO χρησιμοποιούσε το δίκτυο του με αποτέλεσμα η αξία του Ethereum να καταρρεύσει .

Αν και κατάφεραν οι προγραμματιστές της ομάδας του Ethereum να ξαναβρούν τα 48 από τα 50 εκ. δολάρια δημιουργήθηκε βασικό πρόβλημα για το πώς θα αναδιανεμηθούν τα νομίσματα που βρεθήκαν καθώς βασική αρχή των cryptocurrencies και της τεχνολογίας blockchain είναι ότι δεν μπορεί να γίνει επαναφορά (Fork) σε προηγούμενες καταστάσεις, όπως στη περίπτωση αυτή. Αν γίνει επαναφορά, τίθεται σε περαιτέρω κίνδυνο η αξιοπιστία και συνεπώς η αξία του νομίσματος.

Για το λόγο αυτό υπήρξε διχογνωμία στους χρήστες του Ethereum καθώς κάποιοι αντιδρούσαν να γίνει επαναφορά ενώ άλλοι την ήθελαν. Μετά την απόφαση που πάρθηκε το Ethereum χωρίστηκε στα δύο και όσοι διαφώνησαν συνεχίζουν στο δίκτυο του Ethereum Classic ενώ όσοι δέχθηκαν την επαναφορά, που ήταν και οι περισσότεροι μεταφέρθηκαν στο forked δίκτυο με το σκέτο όνομα Ethereum (Mayer, 2018).

Είναι σημαντικό να γίνει κατανοητό ότι παρόλο που συνεχώς συγκρίνονται μεταξύ τους, το Ethereum και το Bitcoin είναι δύο τελείως διαφορετικά κρυπτονομίσματα με εντελώς διαφορετικούς στόχους. Το Bitcoin είναι το πρώτο κρυπτονόμισμα και ένα σύστημα μεταφοράς χρημάτων, το οποίο βασίζεται και υποστηρίζεται από μια κατανεμημένη τεχνολογία ανοικτών σε όλους αρχείων που ονομάζεται Blockchain.

Η Ethereum παρέλαβε την τεχνολογία Blockchain από το Bitcoin και επέκτεινε σημαντικά τις δυνατότητές που παρείχε καθώς δημιούργησε ένα ολόκληρο δίκτυο, με δικό του πρόγραμμα περιήγησης στο Internet, γλώσσα κωδικοποίησης και σύστημα πληρωμών ενώ το ακόμη πιο σημαντικό είναι ότι επιτρέπει στους χρήστες να δημιουργούν αποκεντρωμένες εφαρμογές στον Blocker της Ethereum. Αυτό γίνεται γιατί ο σκοπός για τον οποίο δημιουργήθηκε το Ethereum δεν είναι για να υπάρχει ένα ακόμα ψηφιακό νόμισμα, αλλά για την δυνατότητα που προσφέρει να κατασκευάζονται αποκεντρωμένες εφαρμογές στο δίκτυό του (Dannen, 2017). Πολλές startup επιχειρήσεις επομένως θέλουν να δημιουργήσουν τα projects τους στο δίκτυο του Ethereum, ψάχνοντας επενδυτές μέσω της διαδικασίας του Initial Coin Offering και αυτός είναι ο λόγος που το Ether, το νόμισμα του Ethereum έχει ξανά υψηλή αξία.

Η αξία της μονάδας του Ethereum για τον τελευταίο χρόνο διακυμάνθηκε από $169,1 δολάρια USD την 13 Ιουλίου του 2017 μέχρι $1359,4 δολάρια USD την 15 Ιανουαρίου 2018 και βρίσκεται σήμερα στα $606,3 δολάρια USD. Βάσει της συνολικής αξίας του αποθέματος του, είναι το δεύτερο πιο ισχυρό ψηφιακό νόμισμα μετά το Bitcoin.

3.7 Οι συναλλαγές με bitcoins

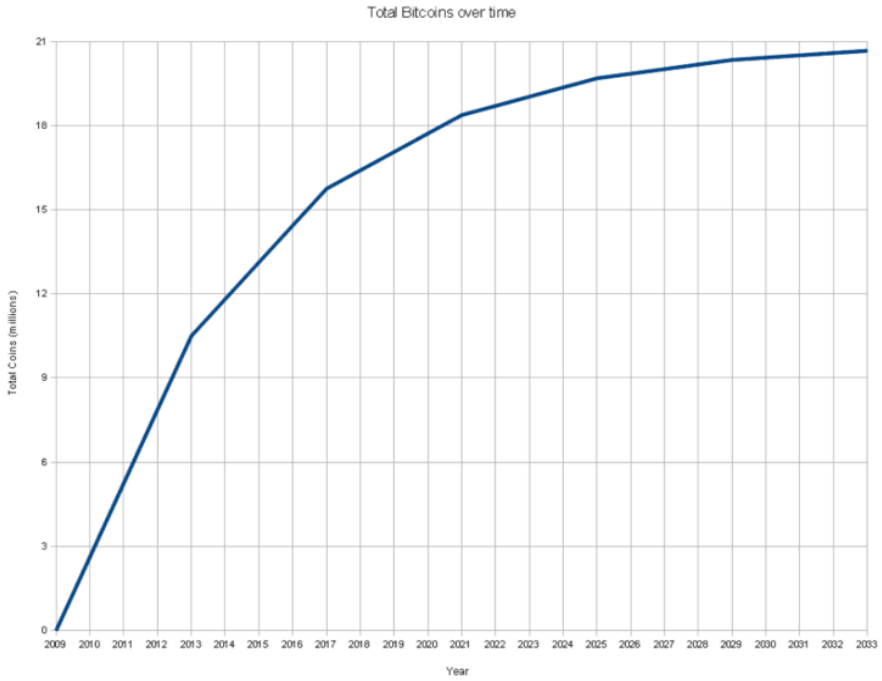
3.7.1 Η απόκτηση των bitcoins

Υπάρχουν τρεις βασικοί τρόποι για να αποκτήσει κάποιος bitcoins

1. Μπορεί να ζητήσει η πληρωμή του για τα όσα προσφέρει να γίνει σε bitcoins. Όλο και περισσότερες εταιρείες και άτομα συμφωνούν να πληρώνονται σε bitcoins και το μόνο που χρειάζονται είναι να έχουν εγκατεστημένο το wallet τους, στο οποίο θα αποθηκευθεί το αντίτιμο του κόστους για ότι προσφέρουν.

2. Αν κάποιος θέλει μπορεί να αγοράσει bitcoins μέσω των αντίστοιχων ιστοσελίδων ανταλλακτηρίων που υπάρχουν (π.χ. coinbase). Τα bitcoins αγοράζονται κάθε φορά βάσει της ισοτιμίας που υπάρχει μεταξύ bitcoin και δολαρίου και θα πρέπει να λαμβάνει κάποιος υπ' όψιν τη μεγάλη μεταβλητότητα και επομένως να κοιτάζει μέχρι τη τελευταία στιγμή ποιά είναι η τρέχουσα ισοτιμία. Για να γίνει μια συναλλαγή μέσω μιας τέτοιας ιστοσελίδας, ο χρήστης θα πρέπει να έχει εγκαταστήσει ένα wallet σε μορφή application στο κινητό του (π.χ. Copey) να στείλει στην ιστοσελίδα ένα έμβασμα με το ποσό που θέλει να διαθέσει και η ιστοσελίδα του στέλνει τα bitcoins στην εν λόγω application.

3. Ο τρίτος τρόπος που υπάρχει είναι αυτός της δημιουργίας bitcoins μέσω της εξόρυξης τους. Η εξόρυξη είναι μια διαδικασία με την οποία οι συναλλαγές επαληθεύονται μέσω σύνθετων μαθηματικών σχέσεων και προστίθενται στο δημόσιο βιβλίο, και όποιος το καταφέρνει ανταμείβεται για τη συνεισφορά του με bitcoins. Το bitcoin mining ουσιαστικά προσθέτει νέα bitcoins στην αγορά αλλά, όπως προαναφέρθηκε, βάσει του ανοιχτού κώδικα δεν μπορούν να δημιουργηθούν συνολικά περισσότερα από 21 εκατομμύρια bitcoins.



Εικόνα 3.4 η εξέλιξη του αριθμού των bitcoins μέσα στο χρόνο (πηγή: www.graph.png)

3.7.2 Πώς γίνονται οι συναλλαγές στο σύστημα του bitcoin;

Τα δίκτυα «peer-to-peer» (P2P) ή «αποκεντρωμένα συστήματα» λειτουργούν και συντηρούνται αποκλειστικά μόνο με τη βοήθεια εξειδικευμένου λογισμικού. Οι ανταλλαγές P2P επιτρέπουν στους συμμετέχοντες στην αγορά να πραγματοποιούν συναλλαγές απευθείας μεταξύ τους χωρίς να χρειάζεται η παρέμβαση τρίτων για να επεξεργασθούν τις συναλλαγές τους.

Τα ανταλλακτήρια κρυπτονομισμάτων είναι εταιρείες οι οποίες χρησιμεύουν ως μεσάζοντες για τις συναλλαγές μεταξύ των πελατών τους και πραγματοποιούν κέρδη με τη συλλογή ποσοστών επί των συναλλαγών. Αντίθετα, οι αλληλεπιδράσεις μεταξύ αντισυμβαλλομένων σε συναλλαγές P2P κατευθύνονται αποκλειστικά από προγραμματισμένο από πριν λογισμικό, χωρίς καμία απαίτηση για ανθρώπινους μεσάζοντες και είναι επομένως έντονα παραδείγματα της φιλοσοφίας αποκέντρωσης. Το όλο δίκτυο υποστηρίζεται από τη τεχνολογία blockchain, μια τεχνολογία κατανεμημένου καθολικού (distributed ledger).

Όπως αναφέρθηκε σε προηγούμενη ενότητα, η τεχνολογία blockchain αποτελεί τον κεντρικό πυλώνα της λειτουργίας του bitcoin καθώς πρόκειται για μια βάση δεδομένων στην οποία καταγράφονται ομαδοποιημένες όλες οι συναλλαγές που γίνονται με bitcoins.

Σε αυτή τη βάση δεδομένων έχουν πρόσβαση όλοι οι χρήστες που κάνουν συναλλαγές με bitcoins και ως εκ τούτου είναι πρακτικά αδύνατον να αλλοιωθεί κάποια από τις εγγραφές καθώς όλοι έχουν πρόσβαση σε αυτές (Πανσεληνά, 2018).

Το bitcoin είναι απλό για τον χρήστη, αλλά ο τρόπος με τον οποίον γίνονται οι συναλλαγές είναι αρκετά σύνθετος. Τα διάφορα βήματα που περιλαμβάνει μια συναλλαγή μεταξύ δύο ισοτίμων είναι τα εξής :

Βήμα $1^{ο}$: ο χρήστης Α επιθυμεί τη αποστολή ενός Χ ποσού bitcoin στον χρήστη Β. Για να γίνει αυτό πρέπει ο Α να αποδείξει ότι έχει στη κατοχή του τα Χ bitcoins με τη χρήση του ιδιωτικού κλειδιού του και να καταχωρήσει τη διεύθυνση του παραλήπτη του ποσού αναφέροντας το δημόσιο κλειδί του δέκτη. Οι συναλλαγές μαζεύονται σε blocks και αποτελούν κομμάτι του Blockchain. Ο δέκτης Β είναι πλέον κάτοχος του ποσού Χ και με τη χρήση του ιδιωτικού του κλειδιού μπορεί να το διαθέσει όπως θέλει.

Οι μεταφορές χρημάτων γίνονται άμεσα, ανεξαρτήτως ώρας και ημέρας, χωρίς καθυστέρηση. Ο χρήστης θα πρέπει να εγκαταστήσει ένα λογισμικό στον υπολογιστή του ή μια εφαρμογή στο κινητό του τηλέφωνο, το λεγόμενο «πορτοφόλι» (wallet), μέσω του οποίου μπορεί να προβαίνει σε συναλλαγές μέσα σε λίγα δευτερόλεπτα.

Για να θεωρείται ολοκληρωμένη μία συναλλαγή πρέπει να περιλαμβάνει και την αμοιβή συναλλαγής. Αυτό συμβαίνει γιατί κάθε συναλλαγή για να γίνει τελικά αποδεκτή στο δίκτυο πρέπει να ενσωματωθεί σε ένα block. Καθώς όμως το κάθε block δημιουργείται από τους miners, οι οποίοι για να το δημιουργήσουν δαπανούν υπολογιστική ισχύ, αυτοί έχουν το δικαίωμα να αρνηθούν να αποδεχθούν τη συναλλαγή και να την ενσωματώσουν στο δίκτυο αν θεωρήσουν χαμηλό το τίμημα.

Κεφάλαιο 4ο

Οι πιθανές απάτες στον τομέα των κρυπτονομισμάτων

4.1 Οι προβληματισμοί που υπάρχουν

Καθώς τα ψηφιακά νομίσματα είναι σχετικά νέα και καινοτόμα μέσα πληρωμής, για τις συναλλαγές με τα κρυπτονομίσματα δεν υπάρχουν ακόμη κανονιστικές αρχές και ρυθμίσεις. Επομένως, είναι δύσκολο αντικειμενικά να υπάρξει εύκολος τρόπος διάκρισης ανάμεσα στον σωστό και τον λάθος τρόπο χρήσης, εμπορίας ή πληρωμών με κρυπτονομίσματα. Εξαίρεση αποτελούν εκείνες οι χώρες , όπως οι ΗΠΑ, η ΕΕ και, πιο πρόσφατα, η Κίνα και η Ιαπωνία, όπου η ρυθμιστική αρχή της χώρας έχει ήδη θέσει σε ισχύ ένα νομικό πλαίσιο.

Αυτός είναι ο κύριος λόγος για τις πολυάριθμες προειδοποιήσεις που εκδίδονται σε όλο τον κόσμο από τράπεζες και χρηματοπιστωτικά ιδρύματα, προειδοποιώντας τους καταναλωτές για τους κινδύνους όταν χρησιμοποιούν μη ελεγχόμενα μέσα πληρωμών , όπως είναι τα cryptocurrencies. Όλο και περισσότερα αξιόπιστα παγκόσμια μέσα ενημέρωσης εξετάζουν θέματα που σχετίζονται με τα ψηφιακά νομίσματα και την ασφάλεια που προσφέρουν και δημοσιεύουν άρθρα, καθιστώντας τους αναγνώστες τους ενήμερους για τους κινδύνους που σχετίζονται με το bitcoin.

Η ασάφεια που περιβάλλει τις συναλλαγές σε bitcoin και τα άλλα cryptocurrencies κίνησε τη προσοχή των μέσων ενημέρωσης και των μέσων κοινωνικής δικτύωσης που γρήγορα ανακάλυψαν ότι αυτή η καινοτόμος μέθοδος συναλλαγών και η τεχνολογία πίσω από αυτή είναι ένα σπουδαίο θέμα για προβολή, το οποίο στη συνέχεια μπορούσαν να μεγεθύνουν όσο θα ήθελαν.

Ο φόβος που υπάρχει είναι ότι, μαζί με όσους προβάλλουν, για τις δικές τους έννομες επιδιώξεις, θέματα που αφορούν τα κρυπτονομίσματα, υπάρχουν και κάποιοι οι οποίοι εμφανίζονται με στόχο να παραπλανήσουν ή να εξαπατήσουν το κοινό με τις προθέσεις και τις αναφορές τους.

Όμως υπάρχει ο εξής προβληματισμός για τη σκοπιμότητα αναφοράς παρόμοιων πρακτικών. Πώς μπορούμε να διακρίνουμε την αλήθεια από το ψέμα όχι μόνο σε ότι ανεβαίνει στο Διαδίκτυο ως είδηση αλλά και ότι εμφανίζεται ως γνώμη ή κριτική.

Ακριβώς όπως συμβαίνει και με τις βιομηχανίες φαρμάκων, οι επιχειρήσεις που ασχολούνται με τα κρυπτονομίσματα είναι ένας εύκολος στόχος για δυσφήμιση που τον προτιμάνε πολλοί. Για τις εταιρείες Cryptocurrencies, αυτό κυρίως καθώς πρόκειται για ένα νέο μη ρυθμιζόμενο ακόμη κλάδο, που περιλαμβάνει νέα και δύσκολα στη κατανόηση τους τεχνολογικά θέματα, καθώς και του εξαιρετικά επιθετικού ανταγωνισμού και αντιπαράθεσης. Το πρόβλημα είναι ότι κανένας από όλους αυτούς που διαδίδουν ψεύτικες ειδήσεις δεν επωφελείται από αυτή την κατάσταση και αυτό τον πόλεμο δημοσιότητας.

4.2 Η περίπτωση της απάτης

'' Κάθε φορά που κάτι έρχεται στην επικαιρότητα, το μόνο που είναι σίγουρο είναι ότι οι απατεώνες θα το εντοπίσουν, όπως εντοπίζουν τα θερμικά βλήματα τον στόχο τους '' όπως έγραψε ο Wasik το 2017 στο Forbes, αναφερόμενος στο ψηφιακό νόμισμα bitcoin.

Για όσους ζουν χωρίς να έχουν επαφή με το Διαδίκτυο, το bitcoin είναι ένα ψηφιακό νόμισμα του οποίου η αξία, που δεν υποστηρίζεται από καμία κυβέρνηση ή κεντρική τράπεζα, καθορίζεται από ένα λογισμικό που ελάχιστοι άνθρωποι καταλαβαίνουν.

Δεδομένου ότι λίγοι άνθρωποι γνωρίζουν πραγματικά πως το bitcoin πραγματικά λειτουργεί, υπάρχουν ατελείωτες ευκαιρίες για παρερμηνείες και με τη διάδοση των κοινωνικών μέσων έχει δημιουργηθεί γόνιμο έδαφος για να διαπραχθούν πολλές απάτες .

Η ανθρώπινη φύση, όντας πάντα αισιόδοξη, θέλει να πιστεύει ότι η αξία του κάθε κρυπτονομίσματος με τη πάροδο του χρόνου αναγκαστικά θα αυξηθεί σε αξία, αλλά αυτό δεν συμβαίνει στη πραγματικότητα καθώς το κρυπτονόμισμα είναι πολύ ασταθές αν και λίγοι καταλαβαίνουν το γιατί. Εκτός όμως από την διάψευση των προσδοκιών υπάρχουν και άλλες συνέπειες που μπορεί να εμφανισθούν (ZeroFOX, 2017)

Το άρθρο αναφέρει ένα νέο είδος οικονομικής απάτης που αφορά το Bitcoin που εξαπλώνεται ταχύτατα σε όλα τα κοινωνικά δίκτυα είτε αυτά είναι κοινωνικά δίκτυα από πελάτες τραπεζών είτε είναι δίκτυα από χρήστες κινητών.

Όπως είδαμε οι συναλλαγές σε Bitcoins υλοποιούνται μέσα από συγκεκριμένες κρυπτογραφημένες ηλεκτρονικές καταγραφές που εμφανίζονται σε μια λίστα στην οποία

μπορεί να ανατρέξει καθένας που ενδιαφέρεται οποιαδήποτε στιγμή. Αυτό φαινομενικά βοηθά τους κατόχους των συγκεκριμένων ‘’πορτοφολιών’’ να αντιμετωπίζουν τα κλασσικά είδη απάτης, ή κλοπής και πρόσβασης σε ευαίσθητα προσωπικά δεδομένα που συμβαίνουν σε άλλους σύγχρονους τρόπους πληρωμής όπως οι πιστωτικές κάρτες και οι υπηρεσίες on-line μεταφοράς χρημάτων. Αλλά όμως, σε αντίθεση με όλα αυτά τα πλεονεκτήματα της ασφάλειας που προσφέρουν, τα ψηφιακά νομίσματα εισήγαγαν ένα τελείως καινούργιο είδος ψηφιακής απάτης.

Κατά ένα ειρωνικό τρόπο αυτό που κάνει τους ιδιοκτήτες των bitcoins ιδανικούς στόχους εξαπάτησης στα κοινωνικά μέσα, είναι ακριβώς το ίδιο πράγμα που κάνει το bitcoin και πιο ασφαλές, είναι δηλαδή ο αποκεντρωμένος, ανώνυμος και μη αναστρέψιμος χαρακτήρας του.

Αποκεντρωμένος χαρακτήρας του bitcoin: Σε αντίθεση με άλλα νομίσματα, το Bitcoin δεν ελέγχεται από κανένα χρηματοπιστωτικό ίδρυμα ή κυβέρνηση. Όταν διαπράττεται μια απάτη σε Bitcoin, η έλλειψη κεντρικής εξουσίας είναι ακριβώς αυτό που καθιστά αδύνατη την ανάκτηση τυχόν ζημιών. Μόλις εξαπατηθεί ο χρήστης η ιστορία σταματάει εκεί και δεν υπάρχει συνέχεια από κανένα, καθώς κανένα πιστωτικό ίδρυμα ή πιστωτική κάρτα δεν μπορεί να καλύψει αυτό το ρυθμιστικό κενό.

Ανώνυμος χαρακτήρας: Οποιοσδήποτε μπορεί να ανοίξει ένα ‘’πορτοφόλι’’ για να ξεκινήσει να συναλλάσσεται και να ξοδεύει Bitcoins χωρίς να παρέχει προσωπικές πληροφορίες. Δεν αποτελεί επομένως παραδοξότητα το γεγονός ότι το Bitcoin είναι ο προτιμώμενος τρόπος πληρωμής για τους συναλλασσόμενους εμπόρους ναρκωτικών στο Διαδίκτυο και τους πωλητές άλλων παράνομων εμπορευμάτων που λειτουργούν μέσα στο κρυμμένο άσχημο υπογάστριο του διαδικτύου που αναφέρεται ως "σκοτεινός ιστός". Τα προφίλ που ανεβαίνουν στα κοινωνικά δίκτυα αποκρύπτουν επίσης τις πραγματικές ταυτότητες των χρηστών τους, παρέχοντας ένα επιπλέον στρώμα ψευδωνυμοποίησης που καθιστά την αναγνωρισιμότητα του χρήστη ανέφικτη.

Μη αναστρέψιμος χαρακτήρας: Οι συναλλαγές bitcoin δεν μπορούν ούτε να αλλάξουν ούτε να ακυρωθούν (αφαιρεθούν). Αυτό είναι ένα χαρακτηριστικό του κάθε κρυπτονομίσματος, όχι ένα σφάλμα. Κανείς δεν μπορεί να αλλάξει τα αρχεία μετά τη δημιουργία τους, δημιουργώντας ένα αναλλοίωτο και μόνιμο βιβλίο που περιλαμβάνει όλη τη διαδρομή δημιουργίας και συναλλαγών μέχρι την πρώτη συναλλαγή που έγινε

ποτέ. Δεν υπάρχει επομένως κάποιος τρόπος να ανακτήσει κάποιος τις απώλειες μόλις δαπανηθούν τα bitcoins.

Για αυτούς τους λόγους, και για αρκετούς ακόμη πιο εξειδικευμένους τα cryptocurrencies, έχουν φθάσει να είναι η προτινώμενη μέθοδος πληρωμής των σύγχρονων ηλεκτρονικών απατεώνων (scammers). Τα κοινωνικά μέσα παρέχουν τη πρόσβαση σε ομάδες ψηφιακά συνδεδεμένων ατόμων που ενδιαφέρονται περισσότερο να δοκιμάσουν τη συμμετοχή τους στις διαδικασίες με τα bitcoins χωρίς να διαθέτουν όμως την εξειδικευμένη τεχνογνωσία που είναι απαραίτητη για να διακρίνουν μια νόμιμη από μια παράνομη συναλλαγή.

Με τη σημερινή κατάσταση στα κοινωνικά δίκτυα, η προσοχή και η πραγματοποίηση έρευνας σχετικά με τη ταυτότητα της κάθε ιστοσελίδας είναι απαραίτητες πορύποθέσεις πριν ξεκινήσει κάποιος να ασχολείται με τα κρυπτονομίσματα. Βέβαια και με τη πάροδο του χρόνου η αγορά παρουσιάζει επίσης σημάδια ωριμότητας, οδηγώντας σε μεγαλύτερη διαφάνεια και σαφέστερους καθώς και πιο ολοκληρωμένους κανόνες.

Ανεξάρτητα όμως, είναι ζωτικής σημασίας να εξετάζει κάποιος τις ευκαιρίες και να κατανοεί κάθε φορά τους κινδύνους και το κόστος που σχετίζεται με την εξόρυξη ή την επένδυση σε cryptocurrencies. Σε κάθε περίπτωση, το πρώτο βήμα κάθε έξυπνου επενδυτή θα πρέπει πάντα να είναι προσεκτική έρευνα για να διασφαλιστεί ότι οι επενδύσεις του είναι πάντα ασφαλείς.

Δεν χρειάζεται όμως φόβος αλλά χρειάζεται ιδιαίτερη προσοχή. Ενώ υπάρχουν σίγουρα κίνδυνοι στην αγορά των κρυπτονομισμάτων, υπάρχουν και οι ευκαιρίες που μπορεί να είναι ακαταμάχητες για ορισμένους. Ωστόσο, η επιφυλακτικότητα είναι πάντα απαραίτητη καθώς και η αναζήτηση αν υπάρχουν σαφή σημάδια απάτης που μπορούν να αναζητήσουν οι επενδυτές ώστε αποφεύγοντας τις παγίδες, να μπορούν να βελτιώσουν τις πιθανότητες επιτυχίας τους και να προστατεύσουν τις επενδύσεις τους.

4.3 Οι διάφορες περιπτώσεις απάτης στα Μέσα Κοινωνικής Δικτύωσης

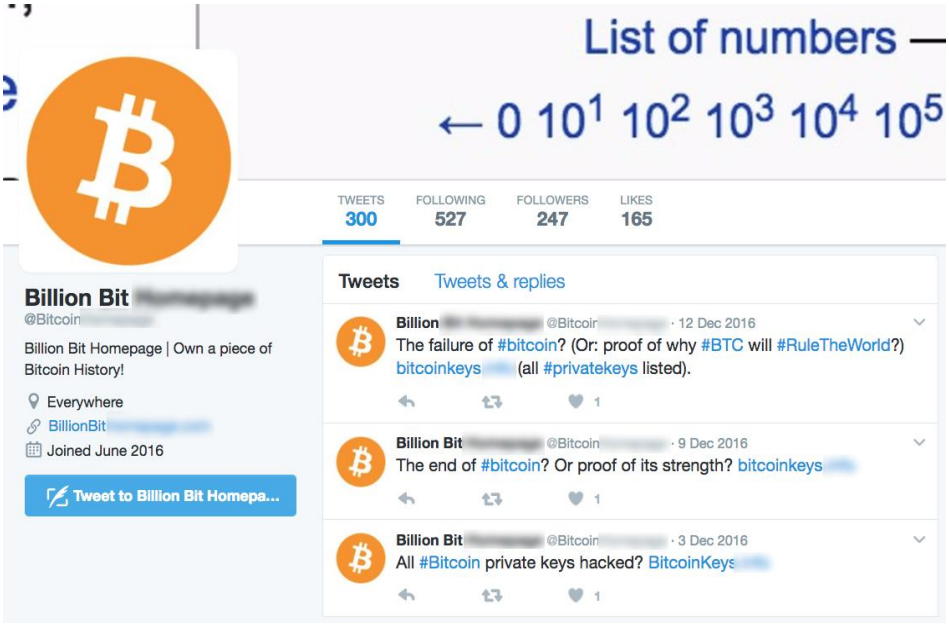
Στη συνέχεια παρατίθενται κάποια αντιπροσωπευτικά παραδείγματα απάτης που ξεκινάνε από τα κοινωνικά μέσα και σχετίζονται με συναλλαγές σε bitcoins και που η παράθεση των στατιστικών τους υπογραμμίζει τον αντίκτυπο και την ευρύτητά τους (Liebkind, 2018).

4.3.1 Η κλοπή μέσα από τα Hardware Wallets

Για χρήστες που ανησυχούν για την ασφάλεια και το απόρρητο των συναλλαγών τους, ένα Hardware Wallet που είναι μια φυσική συσκευή που μπορούν να αποθηκεύσουν τα ιδιωτικά κλειδιά τους, είναι μια ολοένα και πιο δημοφιλής επιλογή. Συνήθως, ένα Hardware Wallet είναι τόσο μικρό όσο οι μονάδες δίσκου USB με κλειδί, και αυτά τα πορτοφόλια προσφέρουν έναν τρόπο έξω από τον υπολογιστή για να βοηθήσουν τους χρήστες κρυπτογράφησης να προστατεύσουν ακόμη περισσότερο τα bitcoins τους. Ωστόσο, έχει αναφερθεί ότι ορισμένες από αυτές είναι ευάλωτες και μπορούν οι χάκερ να τις ανοίγουν οπότε θα μπορούσαν εύκολα να κλέψουν όλες τις αξίες που έχει τοποθετήσει ένας χρήστης (Newman, 2017). Σύμφωνα με τον Ofir Beigel, ιδιοκτήτη του 99Bitcoins.com, μια άλλη παραλλαγή της ίδιας απάτης είναι ‘’ η πώληση Hardware Wallets στα οποία υπάρχει εμφυτευμένη μια " προ-διαμορφωμένη "φράση κρυμμένη κάτω από μια scratch κάρτα. Μόλις ο χρήστης ξύσει τη κάρτα για να χρησιμοποιήσει το πορτοφόλι ενεργοποιείται μια δίοδος που επιτρέπει στους χάκερς να τραβήξουν όλες τις αξίες που υπάρχουν μέσα. Αυτές οι απάτες γίνονται όλο και πιο συνηθισμένες, αλλά μπορούν εύκολα να αποφευχθούν αν όλοι αναζητούν μόνο πορτοφόλια που προέρχονται από αξιόπιστες πηγές.

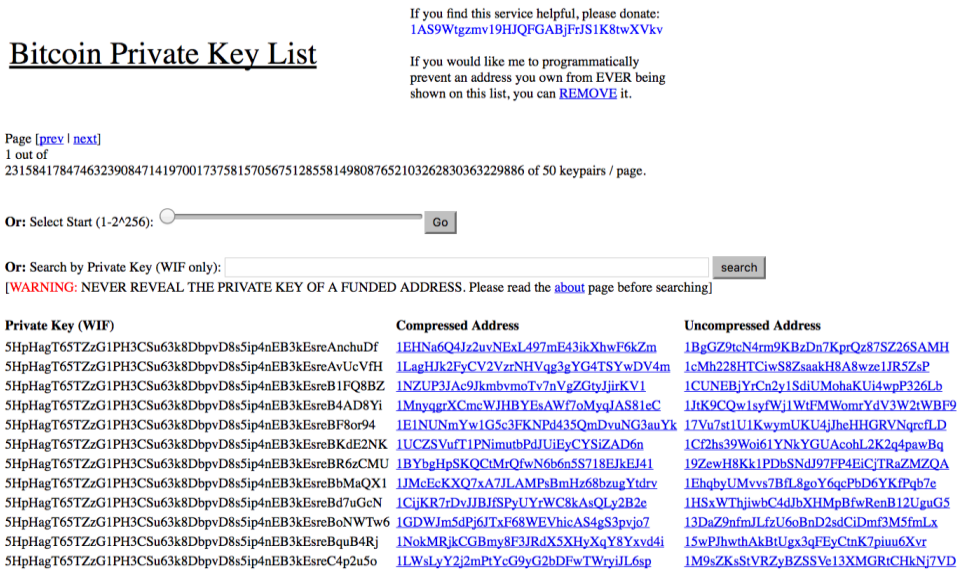
4.3.2 Η αναζήτηση (phishing) παραγωγών bitcoins:

Καθώς οι παραγωγοί bitcoins αναζητούν συνεχώς μέσα στα κοινωνικά δίκτυα νέες ευκαιρίες, η πλαστοπροσωπία του ίδιου του σήματος Bitcoin είναι μια τακτική που μπορεί να χρησιμοποιηθεί για να κερδίσουν οι ηλεκτρονικοί απατεώνες την εμπιστοσύνη των θυμάτων τους στην αξιοπιστία των ιστοσελίδων τους. Στην εικόνα που παρουσιάζεται, ένας επίδοξος δράστης απάτης χρησιμοποιεί το αναγνωρίσιμο λογότυπο Bitcoin ως avatar του Twitter και δημοσιεύει μηνύματα με φήμες και hashtags για την εξάπλωση κλικ για να εξαπλωθούν διευθύνσεις URL ηλεκτρονικού "ψαρέματος" σε όσους ακολουθούν την ιστοσελίδα.



Εικόνα 4.1 η αναζήτηση στο Tweeter προσεγγίσεων (πηγή: www.zerofox.com)

Στη δεύτερη εικόνα ο προορισμός της διεύθυνσης URL είναι μια ιστοσελίδα ηλεκτρονικού "ψαρέματος" (phishing) καθώς ο ιστότοπος υποτίθεται ότι προσφέρει μια υπηρεσία αναζήτησης που ζητάει από τους χρήστες να εισέλθουν με το ιδιωτικό τους κλειδί Bitcoin για να διαπιστώσουν αν το συγκεκριμένο υπάρχει στη βάση δεδομένων τους.



Bitcoin Private Key List

If you find this service helpful, please donate:
1AS9Wtgzmv19HJQFGABjFrJS1K8twXVkv

If you would like me to programmatically prevent an address you own from EVER being shown on this list, you can REMOVE it.

Page [prev | next]
1 out of
231584178474632390847141970017375815705675128558149808765210326283036322988 6 of 50 keypairs / page.

Or: Select Start (1-2^256): Go

Or: Search by Private Key (WIF only): search
[WARNING: NEVER REVEAL THE PRIVATE KEY OF A FUNDED ADDRESS. Please read the about page before searching.]

Private Key (WIF)	Compressed Address	Uncompressed Address
5HpHagT65TZzG1PH3CSu63k8DbpvD8s5ip4nEB3kEsreAnchuDf	1EHNa6Q4Jz2uvNExL497mE43ikXhwF6kZm	1BgGZ9tcN4rm9KBzDn7KprQz87SZ26SAMH
5HpHagT65TZzG1PH3CSu63k8DbpvD8s5ip4nEB3kEsreAvUcVfH	1LagHJk2FyCV2VzrNHVqg3gYG4TSYwDV4m	1cMh228HTCiwS8ZsaakH8A8wze1JR5ZsP
5HpHagT65TZzG1PH3CSu63k8DbpvD8s5ip4nEB3kEsreB1FQ8BZ	1NZUP3JAc9JkmbvmoTv7nVgZGtyJjirKV1	1CUNEBjYrCn2y1SdiUMohaKUi4wpP326Lb
5HpHagT65TZzG1PH3CSu63k8DbpvD8s5ip4nEB3kEsreB4AD8Yi	1MnyqgrXCmcWJHBYEsAWf7oMyqJAS81eC	1JtK9CQw1syfWj1WtFMWomrYdV3W2tWBF9
5HpHagT65TZzG1PH3CSu63k8DbpvD8s5ip4nEB3kEsreBF8or94	1E1NUNmYw1G5c3FKNPd435QmDvuNG3auYk	17Vu7st1U1KwymUKU4jJheHHGRVNqrcfLD
5HpHagT65TZzG1PH3CSu63k8DbpvD8s5ip4nEB3kEsreBKdE2NK	1UCZSVufT1PNimutbPdJUiEyCYSiZAD6n	1Cf2hs39Woi61YNkYGUAcohL2K2q4pawBq
5HpHagT65TZzG1PH3CSu63k8DbpvD8s5ip4nEB3kEsreBR6zCMU	1BYbgHpSKQCtMrQfwN6b6n5S718EJkEJ41	19ZewH8Kk1PDbSNdJ97FP4EiCjTRaZMZQA
5HpHagT65TZzG1PH3CSu63k8DbpvD8s5ip4nEB3kEsreBbMaQX1	1JMcEcKXQ7xA7JLAMPsBmHz68bzugYtdrv	1EhqbyUMvvs7BfL8goY6qcPbD6YKfPqb7e
5HpHagT65TZzG1PH3CSu63k8DbpvD8s5ip4nEB3kEsreBd7uGcN	1CijKR7rDvJJBJfSPyUYrWC8kAsQLy2B2e	1HSxWThjiwbC4dJbXHMpBfwRenB12UguG5
5HpHagT65TZzG1PH3CSu63k8DbpvD8s5ip4nEB3kEsreBoNWTw6	1GDWJm5dPj6JTxF68WEVhicAS4gS3pvjo7	13DaZ9nfmJLfzU6oBnD2sdCiDmf3M5fmLx
5HpHagT65TZzG1PH3CSu63k8DbpvD8s5ip4nEB3kEsreBquB4Rj	1NokMRjkCGBmy8F3JRdX5XHyXqY8Yxvd4i	15wPJhwthAkBtUgx3qFEyCtnK7piuu6Xvr
5HpHagT65TZzG1PH3CSu63k8DbpvD8s5ip4nEB3kEsreC4p2u5o	1LWsLyY2j2mPtYcG9yG2bDFwTWryiJL6sp	1M9sZKsStVRZyBZSSVe13XMGRtCHkNj7VD

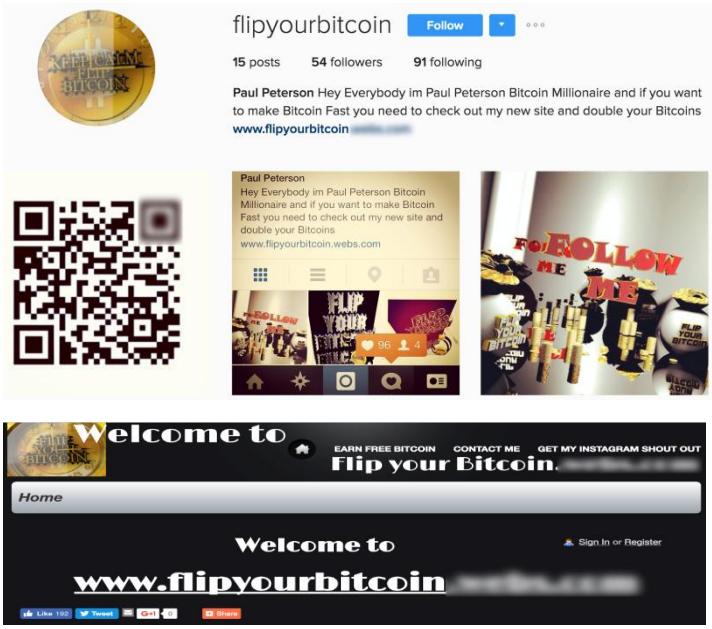
Εικόνα 4.2 η διεύθυνση μιας ιστοσελίδας ηλεκτρονικού ψαρέματος (πηγή: www.zerofox.com)

Μόλις εισαχθεί, το ιδιωτικό κλειδί απλά θα καταργηθεί η ιστοσελίδα , επιτρέποντας στον απατεώνα να αδειάσει το πορτοφόλι με τα bitcoins του χρήστη.

Μια επιπλέον προστασία είναι οι χρήστες να ελέγχουν πάντοτε τις διευθύνσεις URL ανταλλαγών. Η επίσκεψη σε μη ασφαλείς ιστότοπους είναι μια λάθος κίνηση και οι χρήστες πρέπει να ξέρουν ότι οι διευθύνσεις ιστού πρέπει πάντα να ξεκινούν με το HTTPS, ένα σημάδι ότι η κίνηση είναι κρυπτογραφημένη και δεν μπορεί να παραβιασθεί εύκολα από άλλον.

4.3.3 Οι απάτες στις συναλλαγές

Παρά την αποκεντρωμένη φύση τους, τα περισσότερα cryptocurrencies εξακολουθούν να αγοράζονται και να πωλούνται σε ανταλλαγές. Ενώ αυτό διευκολύνει την εύρεση των νομισμάτων που επιθυμούν οι επενδυτές, δεν υπάρχει ακόμα ρυθμιστικό όργανο που να εποπτεύει αυτές τις ανταλλαγές σε πολλές χώρες. Έτσι, πολλοί επενδυτές έχουν χάσει τις περιουσίες τους όταν οι ανταλλαγές που συμμετείχαν αποδείχθηκαν ότι ήταν απάτη. Τον Δεκέμβριο, αναφέρθηκαν αρκετές νοτιοκορεατικές ψεύτικες ανταλλαγές, οι οποίες οδήγησαν σε προγραμματισμό θέσπισης αυστηρότερων κανονισμών από τις αρχές της χώρας. Αυτές οι απάτες δεν είναι δύσκολο να εντοπιστούν, αλλά μπορεί, αν δεν αποφευχθούν, να κοστίσουν πάρα πολύ. Μία από τις μεγαλύτερες ‘’κόκκινες σημαίες’’ είναι η υπόσχεση επίτευξης μη ρεαλιστικών κερδών.



Εικόνα 4.4 μια δόλια Bitcoin-flipping ιστοσελίδα στο Instagram και η αναφερόμενη διεύθυνση URL που επισκέπτονται τα υποψήφια θύματα (πηγή: www.zerofox.com**)**

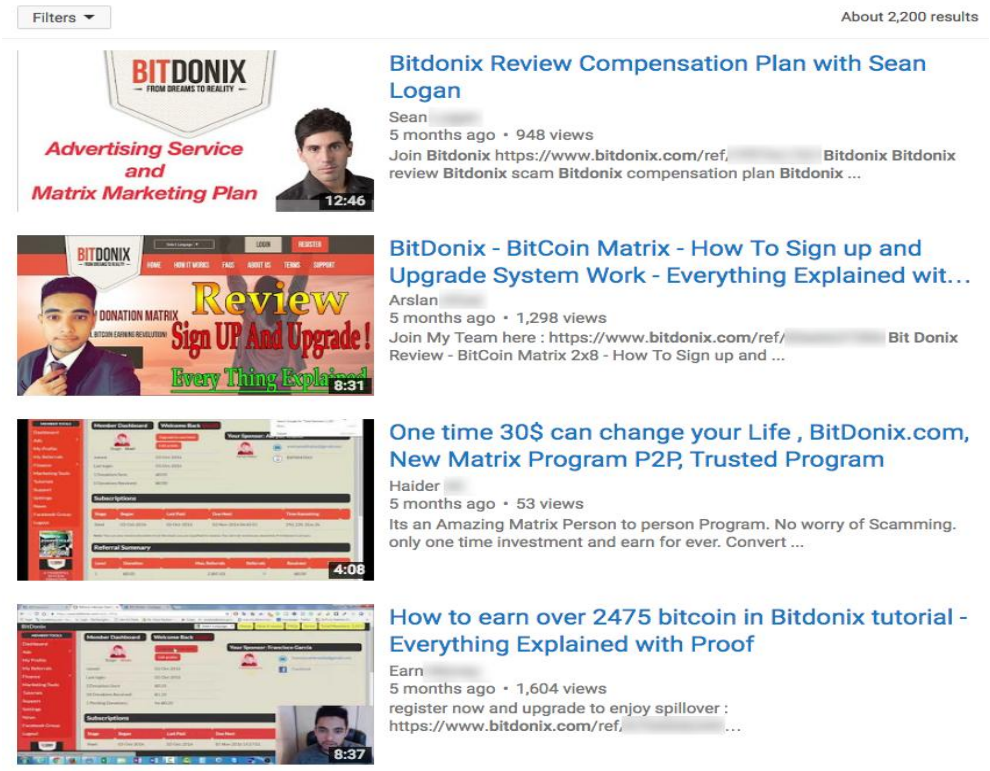
Αυτές οι απάτες δεν είναι δύσκολο να εντοπιστούν, αλλά μπορεί, αν δεν αποφευχθούν, να κοστίσουν πάρα πολύ. Μία από τις μεγαλύτερες ‘’κόκκινες σημαίες’’ είναι η υπόσχεση

επίτευξης μη ρεαλιστικών κερδών. Πρόκειται για ανταλλαγές που υπόσχονται μεγάλες εκπτώσεις για τις συναλλαγές σε bitcoin και χρησιμοποιούν αυτή τη στρατηγική για να προσελκύσουν τα ανυποψίαστα θύματα τους

4.3.4 Το πολυεπίπεδο μάρκετινγκ (η έννοια της πυραμίδας)

Ακόμη και στις ψηφιακές σφαίρες, πολλές αναρτήσεις σε ιστοσελίδες αναφέρονται σε συστήματα μάρκετινγκ πολλαπλών επιπέδων που προσφέρουν στους αφελείς επενδυτές άριστες «ευκαιρίες» για συνεχώς αυξανόμενα κέρδη σε bitcoin.

Το πολυεπίπεδο μάρκετινγκ (Multi Level Marketing) είναι μια στρατηγική μάρκετινγκ για την πώληση προϊόντων ή υπηρεσιών όπου τα έσοδα της εταιρείας MLM προέρχονται από μη μισθωτό εργατικό δυναμικό που πωλεί τα προϊόντα / υπηρεσίες της εταιρείας, ενώ τα κέρδη των πωλητών αυτού του τύπου προέρχονται από ένα σύστημα αποζημίωσης. Τα MLM, όπως είναι γνωστά, βασίζονται στην προσφορά γρήγορων επιστροφών, αλλά στην πραγματικότητα περιλαμβάνουν τη λήψη όλο και περισσότερων χρημάτων με την υπόσχεση ακόμα μεγαλύτερων κερδών. Στην εικόνα παρουσιάζονται κάποιες μορφές προώθησης των τεχνικών αυτών.



Εικόνα 4.5 παραπλανητικά βίντεο στο you Tube (πηγή: www.zerofox.com)

Αν και δεν είναι τελείως παράνομα, αυτά τα γκρίζα από τη πλευρά της νομιμότητας σχέδια, μια χαμηλή αρχική επένδυση μπορεί να πολλαπλασιαστεί με την εγγραφή πρόσθετων μελών χρησιμοποιώντας συνδέσμους παραπομπής. Στη συνέχεια, τα νέα μέλη ενθαρρύνονται να κάνουν το ίδιο, και αυτό επαναλαμβάνεται συνεχώς, έτσι ώστε σε μικρό διάστημα πολλές δεκάδες ατόμων έχουν προσχωρήσει στο σχέδιο. Σε μεταγενέστερο χρονικό σημείο, η αρχική απάτη εμφανίζεται καθώς η πυραμίδα που δημιουργήθηκε καταρρέει.

4.3.5 Οι ψεύτικες ICO [1]

Ένα από τα καλύτερα αποτελέσματα της έκρηξης κρυπτογράφησης ήταν η άνοδος της αρχικής προσφοράς νομισμάτων (Initial Coin Offering) ως ένας τρόπος για τις εταιρείες για να αντλήσουν κεφάλαια. Με χιλιάδες νέες εταιρείες υποστηριζόμενες από τη blockchain που ξεκινάνε στην αγορά με μοναδικές ιδέες και συναρπαστικά έργα, οι χρήστες μπορούν τώρα να υποστηρίξουν εύκολα τις επιχειρήσεις που τους ενδιαφέρουν. Ωστόσο, αυτή η τεράστια έκρηξη ευκαιριών ICO έχει αναπόφευκτα εμφανίσει στο προσκήνιο και το φάσμα της απάτης.

Υπάρχουν διάφοροι τρόποι με τους οποίους οι απατεώνες μπορούν να αποσπάσουν σημαντικές ποσότητες bitcoins από τους επενδυτές. Μια δημοφιλής μέθοδος απάτης περιλαμβάνει τη δημιουργία ψεύτικων ιστότοπων που μοιάζουν με τους ICO και καθοδηγούν τους χρήστες ώστε να καταθέτουν κέρματα σε ένα προδιαγραμμένο πορτοφόλι. Άλλες φορές, οι ίδιες οι ICO είναι υπεύθυνες για την απάτη που γίνεται. Η Centra Tech, για παράδειγμα, είναι μια επιχείρηση blockchain υποστηριζόμενη από πολλές διασημότητες και σήμερα έχει εναχθεί στις ΗΠΑ. Η εταιρεία κατηγορείται ότι εμφανίζει ψεύτικα μέλη της ομάδας, παραπλανητικούς επενδυτές και ψέματα για τα προϊόντα της. Ο καλύτερος τρόπος για να αποφύγει κάποιος αυτές τις απάτες είναι μια στενή έρευνα που περιλαμβάνει τη προσεκτική ανάγνωση των όρων και την αναζήτηση των χαρακτηριστικών της επενδυτικής ομάδας.

4.3.6 Προτάσεις για σχήματα εξόρυξης (cloud mining)

Η εξόρυξη είναι ο μόνος τρόπος για να δημιουργηθούν νέα bitcoins χωρίς την αγορά ή την ανταλλαγή τους, αλλά έχει πλέον γίνει μια απίστευτα δαπανηρή σε πόρους δραστηριότητα. Λόγω του μοναδικού τρόπου εξόρυξης νέων κερμάτων, απαιτούνται

[1] Μια αρχική προσφορά νομισμάτων (ICO), είναι ένας τύπος δημόσιας εγγραφής μιας ομάδας από κρυπτοχρήστες, με στόχο την άντληση κεφαλαίων

τεράστιες ποσότητες ωρών επεξεργασίας και υπολογιστικής ισχύος, και συνεπώς χρήματα, για την εξόρυξη ενός νέου κρυπτονομίσματος. Στο cloud mining, οι κάτοχοι ‘’πορτοφολιών’’ με bitcoins πολλές φορές ενώνουν τις δυνάμεις τους για να νοικιάσουν ακόμη πιο ισχυρούς υπολογιστές για την εξόρυξη bitcoins, οι οποίοι πρέπει να είναι ισχυροί και ταχύτατοι ταυτόχρονα για να λύσουν τους κρυπτογραφικούς αλγόριθμους κατακερματισμού που είναι απαραίτητοι για την δημιουργία νέων bitcoins.

Ωστόσο, πολλές εταιρείες προσφέρουν σε τακτικούς χρήστες τη δυνατότητα να νοικιάσουν, σε μια καθορισμένη τιμή, κάποιο χώρο αποθήκευσης σελίδων εφαρμογών για την εξόρυξη κρυπτονομισμάτων σε έναν διακομιστή.

Ορισμένες εταιρείες προσφέρουν ‘’συμβόλαια διάρκειας ζωής’’, τα οποία διατηρούν το ίδιο κόστος και υποτίθεται ότι προσφέρουν εξαιρετικές αποδόσεις. Ωστόσο, καθώς η δυσκολία της εξόρυξης αυξάνεται, η ίδια επένδυση θα επιστρέφει όλο και μικρότερες παντανοιβές κάθε φορά. Επιπλέον, ορισμένες εταιρείες αναφέρουν εντυπωσιακούς ισχυρισμούς σχετικά με τις αποδόσεις τους χωρίς να είναι διαφανείς σχετικά με το πραγματικό κόστος και τη τάση για μειούμενες αποδόσεις. Άλλες απλά λειτουργούν ως προγράμματα Ponzi (πυραμίδες) που μπορεί να οδηγήσουν σε τεράστιες απώλειες.

Στη συνέχεια αναφέρουμε ένα χρήσιμο παράδειγμα για το πώς μπορεί να στηθεί μια απάτη.

4.3.7 Η περίπτωση της OneCoin

Μία αρκετά γνωστή στο χώρο των κρυπτονομισμάτων εταιρεία που έχει επανειλημμένα συζητηθεί το τελευταίο διάστημα για παρατυπίες και ίσως και απάτες με τη μορφή σχηματισμού πυραμίδας συναλλαγών είναι η OneCoin, οι ιδιοκτήτες της οποίας εμπλέκονταν στο παρελθόν και σε πολλές άλλες ύποπτες επιχειρήσεις της ίδιας μορφής, ως σχήματα Ponzi .

Η εταιρεία προσέφερε στους επενδυτές ογκώδη κέρδη, ακόμα και πολυτελή αγαθά και προνόμια αν ενδιαφέρονταν να πληρώσουν περισσότερα από μια αρχική συμμετοχή. Σύμφωνα με την OneCoin, η κύρια δραστηριότητα της είναι η πώληση εκπαιδευτικού υλικού για συναλλαγές σε ψηφιακές κυρίως πλατφόρμες. Τα μέλη μπορούν να αγοράσουν εκπαιδευτικά πακέτα αξίας από 100 ευρώ έως 118.000 ευρώ. Κάθε πακέτο περιλαμβάνει τη χορήγηση ανάλογης ποσότητας "tokens" τα οποία μπορούν να χρησιμοποιηθούν για την εξόρυξη OneCoins. Το OneCoin είναι δυνατόν να εξορύσσεται από διακομιστές σε δύο τοποθεσίες στη Βουλγαρία και στο Χονγκ Κονγκ. Δεν υπάρχει

τρόπος να ανταλλαγούν τα OneCoins με οποιοδήποτε άλλο νόμισμα και ο μόνος τρόπος ανταλλαγής τους σε οποιοδήποτε άλλο νόμισμα ήταν το OneCoin Exchange, το xcoinx, μια εσωτερική αγορά για τα μέλη που είχαν όμως επενδύσει περισσότερο από ένα απλό ποσό εκκίνησης. Αυτή η υπηρεσία τερματίστηκε χωρίς προειδοποίηση τον Ιανουάριο του 2017. Όμως, και όταν λειτουργούσε, τα OneCoins μπορούσαν να ανταλλάσσονται μόνο με ευρώ, τα οποία τοποθετούνταν σε ένα εικονικό πορτοφόλι από το οποίο θα μπορούσαν να μεταφερθούν στο λογαριασμό του κατόχου OneCoins. Η αγορά xcoinx είχε όρια ημερήσιας πώλησης ανάλογα με τα χρήματα που είχε επενδύσει ο πωλητής, γεγονός που περιόριζε σημαντικά το ποσό των OneCoins που θα μπορούσαν να ανταλλάσσονται. Ωστόσο, υπάρχουν λίγες πληροφορίες σχετικά με την εταιρεία εκτός της δικής τους ιστοσελίδας, και οι αρχές σε πολλές χώρες του κόσμου έχουν ασκήσει πολλές και σοβαρές κατηγορίες εναντίον της (www.en.wikipedia.org) ενώ το τελευταίο διάστημα σε πολλές χώρες διεθνώς, έχει ξεκινήσει μια προσπάθεια να διερευνηθούν πλήρως οι δραστηριότητες της OneCoin, που η Ιντερπόλ ονομάζει "κεντρικό σύστημα πυραμίδας κρυπτονομισμάτων" ενώ στη πραγματικότητα δεν έχει τίποτα το κοινό με αυτά. Σύμφωνα με δημοσιεύματα των ΜΜΕ, τρία εκατομμύρια άνθρωποι ενδέχεται να έχουν εξαπατηθεί από την εταιρεία που δραστηριοποιείται σε τέσσερις ηπείρους (www.news.bitcoin.com)

Κεφάλαιο 5ο

Τα ψηφιακά νομίσματα στην Ελλάδα

5.1 Η κατάσταση στην Ελλάδα

Η Ελλάδα, ενώ πάντοτε αφουγκραζόταν έντονα τη τεχνολογική πρωτοπορία, δεν ακολουθούσε ποτέ έγκαιρα τις εφαρμογές αυτής στη καθημερινή πρακτική. Χαρακτηριστικό παράδειγμα είναι η χρήση των ηλεκτρονικών καρτών για τις καθημερινές δαπάνες, όπου ακόμα και σήμερα που άρχισε να υπάρχει μια αυξημένη τάση χρησιμοποίησης τους, εξαιτίας των περιορισμών διακίνησης κεφαλαίων και των φορολογικών δεσμεύσεων, να βρισκόμαστε πολύ πίσω από τον μέσο Ευρωπαϊκό όρο. Το ίδιο συμβαίνει και με την αποδοχή του e-banking ή τις αγορές από το Διαδίκτυο.

Ανάλογη είναι και η εικόνα που επικρατεί στις αγορές των ψηφιακών νομισμάτων. Τα ψηφιακά νομίσματα έρχονται να αντικαταστήσουν την παραδοσιακή μορφή χρημάτων που κυκλοφορούν αλλά στην Ελλάδα έχουμε ακόμα μεγάλο περιθώριο για ανάπτυξη. Αν και βρίσκεται ακόμη σε νηπιακή μορφή η αγορά ψηφιακών νομισμάτων στην Ελλάδα αναμένεται να έχει εκρηκτική ανάπτυξη γρήγορα καθώς το λανθάνον χαρακτηριστικό του τζόγου που ενυπάρχει σε αυτά σε συνδυασμό με τη σημερινή αποφυγή του Έλληνα για την αποταμίευση μέσω τραπεζών. Άλλωστε η χρήση των πλαστικών καρτών διευκολύνει το πέρασμα αυτό από τη μια μορφή συναλλαγών στην άλλη με τα ψηφιακά νομίσματα.

Τα ψηφιακά νομίσματα ανταλλάσσονται απευθείας με βασικά στοιχεία την αμεσότητα και την ταχύτητα και αποκτούν αξία με βάση τον φορέα έκδοσης αυτών και τους στόχους της δημιουργίας τους.

Η επένδυση σε ψηφιακά νομίσματα με πρώτο βέβαια το πιο γνωστό από αυτά, το bitcoin, έχει αρχίσει να απασχολεί όλο και περισσότερους Έλληνες, ειδικά μετά την επιβολή των περιορισμών στη διακίνηση κεφαλαίων και τις όλο και περισσότερες φορολογικές ενοχλήσεις και σκέψεις για φορολόγηση της περιουσίας που ακούγονται τελευταία. Στην Ελλάδα ήδη έχουν εμφανισθεί τα πρώτα καταστήματα, φυσικά και ηλεκτρονικά, τα οποία έχουν υιοθετήσει το Bitcoin ως μέθοδο πληρωμής.

Η πραγματικότητα όμως είναι ότι, οι περισσότεροι που ασχολούνται με τα ηλεκτρονικά νομίσματα αυτή τη περίοδο, δεν το κάνουν για να εκμεταλλευτούν τα πλεονεκτήματα του ως ένας εναλλακτικός τρόπος συναλλαγών, αλλά τα χρησιμοποιούν ως επενδυτικές πλατφόρμες για κερδοσκοπικούς λόγους.

Αν και βέβαια είναι φανερό ότι άλλο είναι οι συναλλαγές σε ψηφιακά νομίσματα και άλλο η επένδυση σε ψηφιακά, όπου κάποιος προσπαθεί να επωφεληθεί από τις διαφορές τιμών των ψηφιακών νομισμάτων και τις μεγάλες διακυμάνσεις που αυτές παρουσιάζουν.

5.2 Η κατάσταση στην Ελλάδα σήμερα

Αν και δεν είναι εύκολο να προσδιορίσουμε ποιος είναι ο ακριβής αριθμός όσων έχουν bitcoin στην Ελλάδα , αφού δεν απαιτούνται στοιχεία ταυτότητας για την απόκτησή του, φαίνεται ότι οι Έλληνες που το χρησιμοποιούν για τις συναλλαγές τους είναι λιγότεροι από 3000. Από αυτούς οι περισσότεροι χρησιμοποιούν τα bitcoins για επένδυση και είναι ενδιαφέροντα τα διάφορα σκεπτικά που αναπτύσσονται στα διάφορα site τα αφιερωμένα στα κρυπτονομίσματα. Αναφέρουμε μερικά από αυτά

"Είναι πολύ βολικό για τις πληρωμές αφού γίνονται άμεσα χωρίς τη μεσολάβηση τράπεζας και σε οποιαδήποτε χώρα του κόσμου"

"αν απαγορευθεί κάποτε, θα αποκτήσει ακόμη φανατικότερους οπαδούς και μεγαλύτερη αξία"

"Το ψηφιακό συνάλλαγμα θα δημιουργήσει πιο αποτελεσματικές υπηρεσίες και θα λειτουργήσει ως μηχανισμός για την εξάπλωση των οικονομικών υπηρεσιών σε τομείς του κόσμου που δεν έχουν μεγάλη τραπεζική υποστήριξη"

Παρά το γεγονός ότι το bitcoin στην Ελλάδα δεν είναι αρκετά διαδεδομένο, ιδίως στο χώρο των εμπορικών και ψηφιακών καταστημάτων, αυτό δεν έχει αποτρέψει κάποιους να το δέχονται ως μέσο συναλλαγής για τις προσφερόμενες υπηρεσίες και προϊόντα που διαθέτουν.

Όσο αυξάνεται η διάδοση του ψηφιακού νομίσματος στην Ελλάδα τόσο θα αυξάνει ο σημερινός περιορισμένος αριθμός καταστημάτων που δέχονται το bitcoin. Στοιχεία για τα καταστήματα που δέχονται ψηφιακά νομίσματα μπορεί κάποιος να βρεί στο παγκόσμιος χάρτης εμπορικής αποδοχής του Bitcoin Coinmap .Τα καταστήματα που αναφέρονται είναι λίγα αλλά αυτό δεν σημαίνει ότι συνεχώς δεν προστίθενται και νέα. Είναι ενδιαφέρον να παρατηρήσει κανείς ότι υπάρχουν κάθε κατηγορίας επιχειρήσεις και όχι για παράδειγμα επιχειρήσεις στο τομέα της τεχνολογίας ή των Η/Υ όπως θα φαινόταν και πιο φυσικό. Ενδεικτικά αναφέρονται μερικές από αυτές (οι πρωτοπόρες το 2015)

Kernel IT Solutions (εταιρεία δημιουργίας λογισμικού), **Carena Bar-Restaurant** (βρίσκεται στην Κεφαλονιά), **Web-Toner** (παραγωγή και ανακύκλωση toner & μελανιών με έδρα τον Ασπρόπυργο), **NetStudio** (εταιρεία δημιουργία ιστοσελίδων), **VoiceSolutions** (εταιρεία τηλεφωνικών εγκαταστάσεων και συστημάτων επικοινωνίας**), Κ.Τ.Ε.Ο Ισταίας**, **Akrotiri Rooms-Restaurant** (ενοικιαζόμενα δωμάτια στην Μάνη), **Great Alexander** (ξενοδοχείο στη Πλάκα Λιτοχώρου**),** **Datalive** (εταιρεία πληροφορικής & ανάλυσης δεδομένων).

Στο παράρτημα Α' υπάρχει η πλήρης λίστα με τις επιχειρήσεις εκείνες που δέχονται bitcoins στο τέλος του 2017. Μια σύγκριση με τη λίστα του 2015 μας δείχνει ότι μέσα σε δύο χρόνια ο αριθμός των επιχειρήσεων που αναφέρονται εικοσαπλασιάσθηκε.

Όπως φαίνεται το προφίλ αυτών που ασχολούνται με τα ψηφιακά νομίσματα είναι κυρίως νέα σε ηλικία άτομα τα οποία είναι εξοικειωμένα με την τεχνολογία και το Διαδίκτυο και μπορούν να αντιληφθούν τη νέα ψηφιακή πραγματικότητα χωρίς όμως κατ' ανάγκη να την έχουν σπουδάσει. Αυτό είναι ιδιαίτερα αισθητό σε όσους συναλλάσσονται με bitcoins. Σε όσους όμως χρησιμοποιούν το χώρο των ψηφιακών νομισμάτων για επενδυτικό σκοπό υπάρχουν και άτομα μεγάλης ηλικίας που δεν διστάζουν να δοκιμάσουν τον κλάδο των ψηφιακών νομισμάτων ποντάροντας στις υψηλές αποδόσεις που υπάρχουν. Για το λόγο αυτό αναμένεται να αυξάνει η ζήτηση όσο οι αποδόσεις του bitcoin αυξάνονται και δεν είναι απίθανο να δημιουργηθεί μια μόδα ανάλογη με εκείνη στα τέλη της δεκαετίας του 90 με το Χρηματιστήριο.

Ήδη έχουν αρχίσει να εμφανίζονται τα πρώτα ATM για bitcoins. Το πρώτο από αυτά τοποθετήθηκε το 2015 στο Μενίδι Αττικής από την bitcoinsgreece.com που είναι μέχρι

σήμερα μεγαλύτερη Ελληνική πλατφόρμα συναλλαγών ψηφιακών νομισμάτων. Μέχρι σήμερα ATMS έχουν εγκατασταθεί σε διάφορα σημεία στην Αθήνα και τη Θεσσαλονίκη, το Ηράκλειο, και τη Λάρισα. Κάποια από αυτά εκτελούν πλήρεις συναλλαγές, δηλαδή πουλούν και αγοράζουν bitcoins. Κάποια άλλα μόνο πουλάνε. Είναι η πιο άμεση μέθοδος συναλλαγών αλλά δεν είναι η μόνη.

Εικόνα 5.1 το bitcoin ATM που εγκατέστησε η Bcash στη Λάρισα (πηγή: www.coinatmradar.com)

Αυτή τη στιγμή βρίσκεται στο τελικό στάδιο η διαδικασία εγκατάστασης 1.000 ATM για bitcoin στην Ελλάδα, τα οποία στην πλειονότητα θα υποστηρίζονται από το ήδη υπάρχον δίκτυο των χρηματοπιστωτικών ιδρυμάτων.

Μπορεί κάποιος να κάνει συναλλαγές και σε ανταλλακτήρια ψηφιακών νομισμάτων σε όλο τον κόσμο μέσα από τραπεζικά εμβάσματα ή σε συγκεκριμένα ανταλλακτήρια που αποδέχονται τις συναλλαγές μέσω καρτών.

Έχει δε εμφανισθεί και η BTC Greece που είναι η πρώτη εταιρεία-μεσάζοντας στην Ελλάδα, της οποίας οι δραστηριότητες αφορούν τη δημιουργία συνδέσμων που θα προωθούν τις διαδικασίες αγοράς και πώλησης του ηλεκτρονικού νομίσματος, bitcoin. Η εταιρεία δηλαδή φροντίζει να φέρνει σε επαφή το χρήστη που θέλει να αγοράσει με εκείνον που θέλει να πουλήσει και απευθύνεται κυρίως σε μικρομεσαίες επιχειρήσεις.

5.3 Τα προβλήματα που αντιμετωπίζει το bitcoin στην Ελλάδα

Ένας από τους ειδικούς που ασχολούνται με το bitcoin είναι Έλληνας και σε πρόσφατη ομιλία του δήλωσε ότι "το bitcoin δεν είναι ακόμα έτοιμο για την Ελλάδα"(Αντωνόπουλος, 2015). Αν αντιστρέψουμε τη πρόταση μπορούμε να πούμε ότι και ''η Ελλάδα δεν είναι έτοιμη για το bitcoin''. Ποια από τις δύο προτάσεις είναι η σωστή ή μήπως και οι δύο είναι αλήθεια;

Ο χαμηλός αριθμός συναλλαγών που υποστηρίζει σήμερα το bitcoin εμποδίζει τη καθιέρωση του ως επίσημο νόμισμα συναλλαγών σε κάθε χώρα και επομένως αυτό ισχύει και στην Ελλάδα. Με 7 μόνο συναλλαγές το λεπτό δεν καλύπτονται ούτε στοιχειωδώς οι ανάγκες για τις χιλιάδες συναλλαγές που γίνονται. Παράλληλα η αξία του διακρίνεται από πολύ μεγάλη μεταβλητότητα και όχι μόνο σε μεγάλα χρονικά διαστήματα αλλά και μέσα στην ίδια την ημέρα. Αν δεί λοιπόν κάποιος ένα προϊόν σε μια τιμή το πρωϊ ώσπου να πάει το μεσημέρι να το αγοράσει μπορεί να το δεί σε μια τιμή διαφορετική κατά 10-15% . Το ίδιο μπορεί να συμβεί και σε κάποιον που παραγγέλνει κάτι στο εξωτερικό και η ισοτιμία δολαρίου/ bitcoin μεταβάλλεται πάνω από 10% ώσπου να συμφωνηθεί η συναλλαγή. Τέλος θα πρέπει να ξεφύγει το bitcoin από τις αυστηρά online διαδικασίες για να μπορούν να εκτελούνται και offline συναλλαγές οι οποίες είναι και οι περισσότερες στην καθημερινότητα του καταναλωτή.

Όμως είπαμε και η Ελλάδα δεν είναι έτοιμη για το bitcoin. Τα μεγαλύτερα προβλήματα που αντιμετωπίζει το bitcoin στην πιο μαζική υιοθέτηση του από το κοινό στην Ελλάδα είναι τα εξής:

Υπάρχει έλλειψη τόσο χρηστών, όσο και εμπόρων. Η ύπαρξη και των δύο πλευρών είναι απαραίτητη για να υπάρξει το απαιτούμενο "network effect" για την ανάπτυξη οποιασδήποτε τεχνολογίας ευρείας χρήσης, ιδιαίτερα στον οικονομικό τομέα που διακινούνται χρήματα. Στην Ελλάδα είμαστε ακόμη πολύ μακριά από τη στιγμή που θα έχει σχηματισθεί αυτή η ''κρίσιμη μάζα''.

Δεν υπάρχει ακόμη η κατάλληλα προσαρμοσμένη νομοθεσία. Αντίθετα υπάρχει μια σειρά από αντιφατικές νομοθετικές ρυθμίσεις που δεν ξεκαθαρίζουν για το τι ακριβώς είναι υποχρεωμένοι όσοι συναλλάσσονται σε bitcoins να ακολουθούν. Σε μια μελέτη του το νομικό γραφείο Γιαννιτσή (2014) αναφέρει κάποιες από τις αντιφατικές θεωρήσεις που υπάρχουν.

Σύμφωνα λοιπόν με τα άρθρα 3 και 8 του ν. 3606/07 αν το Bitcoin είναι χρηματοπιστωτικό μέσο, απαγορεύεται η εκτέλεση δραστηριοτήτων όπως η λήψη και

διαβίβαση εντολών, οι συναλλαγές αγοράς/πώλησης σε Bitcoins, καθώς και η φύλαξη και διοικητική διαχείριση Bitcoins για λογαριασμό πελατών από μη αδειοδοτημένες προς τούτο εταιρείες. 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’’ τότε δεν εμπίπτει στον ν. 3606/07 αλλά αν χαρακτηριστεί ως κινητή αξία, αυτή θα πρέπει να είναι δεκτική διαπραγμάτευσης στην κεφαλαιαγορά, κάτι που με δεδομένη την αρχιτεκτονική δομή της αγοράς των κρυπτονομισμάτων σαφώς δεν ισχύει.

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, καθώς δεν εκτελούν συναλλαγές καταθέσεων, χορήγησης δανείων ή έκδοση εγγυητικών επιστολών. Δεν είναι όμως ούτε και ιδρύματα 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 δεν εκδίδουν μέσα πληρωμής.

Στην πραγματικότητα καθώς το σύστημα είναι αποκεντρωμένο τα ψηφιακά νομίσματα εκδίδονται από το οποίο δεν ανήκει σε κανένα πρόσωπο και καταβάλλονται στους καταχωρητές ως αμοιβή. Ενδεικτικό είναι το γεγονός ότι αυτοί δεν ελέγχουν καν τη διαδικασία δημιουργίας νέων Bitcoins.

Αυτές είναι κάποιες από τις αρκετές νομοθετικές αντιφάσεις που υπάρχουν και χρειάζονται ξεκαθάρισμα.

Υπάρχει έλλειψη του αναγκαίου ρυθμιστικού πλαισίου για τα κρυπτονομίσματα.

Οι χώρες, η μια μετά την άλλη, προσαρμόζουν τη νομοθεσία τους και μαζί με αυτήν και το κανονιστικό πλαίσιο που έχει διαμορφωθεί ώστε να υπάρχει διαύγεια στις συναλλαγές. Τελευταία στη σειρά, η Σιγκαπούρη αποφάσισε τη ρύθμιση των αγορών κρυπτονομισμάτων με σκοπό την αποτροπή χρηματοδότησης της τρομοκρατίας και του

ξεπλύματος μαύρου χρήματος.

Προς το παρόν στην Ελλάδα δεν υφίσταται κανένα απολύτως ειδικό ρυθμιστικό πλαίσιο των αγορών ψηφιακών νομισμάτων και δεν έχουν εκφέρει καμία άποψη όλες οι

αρμόδιες ελληνικές αρχές (Τράπεζα της Ελλάδος, Επιτροπή Κεφαλαιαγοράς) (Παρασκευόπουλος- Κόλιας, 2014).

Δεν υπάρχει η απαραίτητη υποδομή τόσο από τη πλευρά του εξοπλισμού όσο και από τη πλευρά της εξοικείωσης των Ελλήνων.

Είδαμε προηγουμένως ότι μόλις το 2015 εγκαταστάθηκε στην Ελλάδα το πρώτο ATM για bitcoins και πάνω από το 85% των συναλλαγών γίνεται ακόμη από ανταλλακτήρια στο εξωτερικό. Για να υιοθετήσει μια χώρα όπως η Ελλάδα το Bitcoin ως νόμισμα χρειάζεται να υπάρχει η απαραίτητη υποδομή αποδοχής του αλλά αυτό δεν είναι αρκετό. Χρειάζεται να εξοικειωθούν οι χρήστες με τη τεχνολογία που κρύβεται πίσω από τα ψηφιακά νομίσματα και με έννοιες όπως η τεχνολογία Blockchain, το ηλεκτρονικό πορτοφόλι, τα κλειδιά κρυπτογράφησης, κ.λπ. και για όλα αυτά θα χρειασθεί χρόνο.

Οι προϋποθέσεις αυτές θα απαιτήσουν οπωσδήποτε ένα αρκετά μεγάλο χρονικό διάστημα, το οποίο μπορέι να μεγαλώσει ή να μειωθεί ανάλογα με το πώς θα διαμορφωθεί η εικόνα του Bitcoin μέσα στη κοινωνία. Όσο πληθαίνουν οι θετικές αναφορές το Bitcoin θα κερδίζει έδαφος, ενώ οι αρνητικές εικόνες (αναφορές, ειδήσεις, απάτες) θα απομακρύνουν τους Έλληνες από αυτό.

5.4. Τα πρώτα Ελληνικά κρυπτονομίσματα

Το Hellenic Coin (HNC)

Το πρώτο Ελληνικό Κρυπτονόμισμα, με το όνομα Hellenic Coin (HNC) δημιουργήθηκε το 2015 και η διαπραγμάτευσή του στη διεθνή αγορά των Κρυπτονομισμάτων ξεκίνησε στις 21 Ιουλίου 2015 με κωδικό αναγνώρισης HNC (Hellenic Coin). Κάθε χρήστης Hellenic Coin (HNC) διαθέτει ένα δημόσιο κλειδί (Public key), καθώς και ένα ιδιωτικό (Private key), το οποίο λειτουργεί σαν μυστικός κωδικός (www.helleniccoin.com) . Στηρίζεται στις ίδιες υπολογιστικές αρχές όπως και το Litecoin.

Το Hellenic Coin (HNC), είναι ένα ψηφιακό περιουσιακό στοιχείο ‘’σχεδιασμένο να λειτουργεί ως μέσο ανταλλαγής με κρυπτογράφηση, έτσι ώστε να εξασφαλίζει την ασφάλεια των συναλλαγών και να ελέγχει τη δημιουργία πρόσθετων μονάδων του νομίσματος’’. Αυτή τη στιγμή η διαπραγμάτευση του γίνεται μέσα από τη διεθνή πλατφόρμα συναλλαγών “Livecoin” (www.livecoin.net), μέσω της οποίας ο κάθε ενδιαφερόμενος μπορεί να ανοίξει και να ενεργοποιήσει το ηλεκτρονικό του πορτοφόλι

αγοράζοντας το HNC. Ο στόχος είναι μέσα στο 2018 το Hellenic Coin να τοποθετηθεί και σε άλλα τέσσερα ανταλλακτήρια κρυπτονομισμάτων και να καθιερωθεί ως ένα διεθνές κρυπτονόμισμα το οποίο θα γίνει αποδεκτό μέσο συναλλαγής από 15.000 Ηλεκτρονικά Καταστήματα παγκοσμίως.

Ο ρόλος του ως Ελληνικό κρυπτονόμισμα αναμένεται να είναι εξίσου σημαντικός, ιδιαίτερα στον κλάδο του - ταχέως αναπτυσσόμενου - Ελληνικού Τουρισμού: Ελληνικές Τουριστικές Ξενοδοχειακές Μονάδες έχουν ήδη ξεκινήσει τη σύνδεσή τους με το Hellenic Coin (HNC), αποδεχόμενες οι κρατήσεις και οι πληρωμές τους να πραγματοποιούνται αποκλειστικά (όταν είναι με Coin) με χρήση του Hellenic Coin (HNC).

Το Hellenic Coin (HNC), όπως και τα άλλα κρυπτονομίσματα, διαπραγματεύεται 365 ημέρες και καθ΄ όλο το εικοσιτετράωρο μέσα από τη διεθνή πλατφόρμα συναλλαγών "Livecoin" (www.livecoin.net), μέσω της οποίας ο κάθε ενδιαφερόμενος μπορεί να ανοίξει και να ενεργοποιήσει το ηλεκτρονικό του πορτοφόλι αγοράζοντας το κρυπτονόμισμα Hellenic Coin (HNC) για όλες τις εμπορικές συναλλαγές τους καθώς και για τις επενδυτικές του δραστηριότητες, ενώ είναι προγραμματισμένο να τοποθετηθεί και σε άλλα τέσσερα(4) ανταλλακτήρια κρυπτονομισμάτων μέχρι το τέλος του 2017.

Ο κύριος τομέας εφαρμογής του Hellenic Coin είναι ο τομέας των τουριστικών υπηρεσιών στον οποίο η Ελλάδα έχει μεγάλη έκθεση και ήδη υπάρχουν δύο ξενοδοχειακές μονάδες Ξενοδοχειακές Μονάδες έχουν ήδη ξεκινήσει τη σύνδεσή τους με το Hellenic Coin (HNC), αποδεχόμενες οι κρατήσεις και οι πληρωμές τους να πραγματοποιούνται αποκλειστικά με χρήση του Hellenic Coin (HNC).

Το Oceanus coin

Ο τομέας της ναυτιλίας δεν είναι εύκολο να ανταποκριθεί στις σύγχρονες τεχνολογικές προκλήσεις και την ταχύτητα που αυτές μεταβάλλονται Το Oceanus coin βασίζεται στις δυνατότητες που δημιουργούνται από την χρήση των Smart Contracts στην τεχνολογία του Ethereum και δημιουργήθηκε για να συμμετάσχει στη ριζική αναδιάρθρωση του τομέα της ναυτιλίας και όχι για να προσφέρει μια μερική λύση. Μερικές από τις δραστηριότητες που συμμετέχει είναι:

- Η δημιουργία πλατφόρμας διευκόλυνσης συναλλαγών για μεταφορά φορτίων μέσω πλοίων

- Η δημιουργία εκπαιδευτικών προγραμμάτων σε όλους τους κλάδους της ναυτιλίας σε συνεργασία με πανεπιστημιακά και εκπαιδευτικά ιδρύματα
- Ο σταδιακός εκσυγχρονισμός των Bill of Landing σε ψηφιακά

Η επένδυση σε καινοτόμες startup επιχειρήσεις που ασχολούνται με τους τομείς της ναυτιλίας, διαχείρισης λιμένων και μεταφορών.

Το ψηφιακό νόμισμα Oceanus έχει τη δυνατότητα να ανταλλαχθεί με άλλα ψηφιακά νομίσματα σε πλατφόρμες ανταλλαγής, να εξαργυρωθεί άμεσα για υπηρεσίες που θα προσφέρουν οι νεοφυείς επιχειρήσεις και να χρησιμοποιηθούν για τις πληρωμές διδάκτρων σε προγράμματα τριτοβάθμιας εκπαίδευσης που αφορούν τις ναυτιλιακές σπουδές.

Το κρυπτονόμισμα Gene

Το πρώτο κρυπτονόμισμα ελληνικής εμπνεύσεως έχει πλέον ξεκινήσει τη πορεία του καθώς η εταιρεία ParkGene, μια εταιρεία που διαχειρίζεται θέσεις παρκαρίσματος δημιούργησε το token Gene φτιαγμένο πάνω στη τεχνολογία που βασίζονται στο Ethereum Blockchain και βασισμένο στην ιδέα ‘’AirBnB για Parking’’, το οποίο ξεκίνησε να διατίθεται στην αγορά.

Στόχος της εταιρείας είναι η διάθεση 1 δισ. genes, συνολικής αξίας 100 εκατ. δολ. ΗΠΑ (1 gene = 0,1 δολ. ΗΠΑ), με στόχο τη δημιουργία της Airbnb των θέσεων στάθμευσης αυτοκινήτων. Στον επόμενο πίνακα φαίνονται οι λεπτομέρειες από τη κίνηση αυτή.

Εικόνα 5.2 οι πληροφορίες για την ICO της ParkGene (πηγή: εφημερίδα Καθημερινή)

Από τα τέλη Δεκεμβρίου του 2017 που ξεκίνησαν οι διαδικασίες υλοποίησης της ICO μέχρι το τέλος Μαρτίου 2018 η ParkGene κατάφερε να συγκεντρώσει 125 εκατ. tokens, με τιμή 0,1 δολ./token, αν και ο αρχικός στόχος ήταν 35 εκ. δολάρια USD. Με τα κεφάλαια αυτά, η εταιρεία θα εξελίξει και θα προωθήσει την εφαρμογή ParkGene και το δικό της κρυπτονόμισμα, του οποίου η συνολική διάθεση θα περιλάβει ένα δισεκατομμύριο μονάδες.

Όπως φαίνεται και από τον πίνακα το 40% θα παραμείνει στο ParkGene Future Fund, με στόχο την συνεχή εξέλιξη του κρυπτονομίσματος, το 10% (100 εκατ. genes) θα πάρουν οι ιδρυτές της εταιρείας, ένα επιπλέον 10% οι σύμβουλοί της, ένα 5% οι υποστηρικτές (bounty) της ιδέας του κρυπτονομίσματος και το υπόλοιπο 35% θα διατεθεί στο ευρύ κοινό. Οι τελευταίοι μπορούν να αποκτήσουν το gene πληρώνοντας είτε σε εθνικά νομίσματα, π.χ. ευρώ, δολάρια κ.λπ., είτε σε κρυπτονομίσματα, όπως είναι το bitcoin, το ethercoin κ.ά.(Μανδραβέλης, 2018)

Με τα genes κάποιος θα μπορεί να μισθώνει θέσεις πάρκινγκ. Η σύλληψη της ιδέας βασίζεται στο ότι καθένας που φεύγει για να εργαστεί απελευθερώνει μία θέση στάθμευσης, η οποία μπορεί να χρησιμεύσει σε κάποιον που επισκέπτεται την περιοχή γύρω από το σπίτι του. Οι δύο αυτοί θα μπορούν να συναλλάσσονται μεταξύ τους, αφήνοντας στην ParkGene το 10% της τιμής. Όσοι διαθέτουν τη θέση πάρκινγκ θα κερδίζουν το 50% της αξίας παρκαρίσματος στη περιοχή. Επομένως, όποιος τη νοικιάζει θα έχει όφελος το 50%, ενώ όφελος 40% θα έχει και όποιος τη διαθέτει αφού θα πρέπει να δώσει το 10% στην ParkGene.

Το στοίχημα, όπως και σε κάθε άλλο κρυπτονόμισμα που διατίθεται μέσω ICO, βρίσκεται πίσω από την επιτυχία της εμπορευματοποίησης της ιδέας. Αν η ιδέα που προβάλλεται γίνει αποδεκτή από το ευρύ κοινό τότε η αξία του κρυπτονομίσματος θα αυξηθεί καθώς θα υπάρχει ζήτηση από όλους αυτούς που θα το χρησιμοποιούν. Όσοι λοιπόν θα κατέχουν genes θα γίνουν πλούσιοι. Αν η ιδέα δεν διαδοθεί δεν θα έχει πετύχει και στη περίπτωση αυτή τα genes που θα κατέχουν οι χρήστες θα είναι άχρηστα.

Το σχέδιο προβλέπει ακόμη ότι, μέχρι το τέλος του έτους, η εφαρμογή ParkGene θα είναι διαθέσιμη σε 20 γλώσσες σε όλο τον πλανήτη και ότι στο τέλος του 2019 θα έχει 15 εκατ. χρήστες των υπηρεσιών ParkGene. Επίσης, στην 5ετία, η εταιρεία θα έχει έσοδα 35 εκατ. δολ. ετησίως.

Συμπεράσματα

Η έννοια του χρήματος ως μέσο ανταλλαγής είναι παρούσα στη παγκόσμια ιστορία από το ξεκίνημα της ιστορίας του ανθρώπινου γένους. Οι διάφορες μορφές χρήματος εξελίσσονται παράλληλα με τις διάφορες ιστορικές καταστάσεις και τις ανθρώπινες δραστηριότητες. Με τη πάροδο των αιώνων φθάσαμε στη σημερινή εποχή και μετά το ηλεκτρονικό χρήμα έφθασε σήμερα η εποχή που εμφανίσθηκε το ψηφιακό χρήμα, του οποίου η πιο γνωστή έκφραση είναι το bitcoin.

Η ευκολία και τα οφέλη που προσφέρει η νέα μορφή συναλλαγής είναι σημαντικά. Ο καταναλωτής είναι πιο ασφαλής κατά την διενέργεια των συναλλαγών του, καθώς δεν έχει πάνω του χρήματα σε ρευστό κι έτσι δεν διατρέχει τον κίνδυνο να τα χάσει. Η κρυπτογράφηση έχει αυξήσει την ασφάλεια που υπάρχει κατά τις διαδικτυακές συναλλαγές. Η αποκέντρωση των χρηματικών συναλλαγών υπόσχεται αυξημένες ταχύτητες διεκπεραίωσης και χαμηλότερο κόστος.

Θα περίμενε κανείς πως η λογική αντίδραση που θα προκαλούσε μια τέτοια εξέλιξη θα ήταν από τη μια πλευρά ικανοποίηση για τη δυναμική που φέρνει το bitcoin στον τομέα των χρηματοπιστωτικών συναλλαγών, ενδιαφέρον για τη ευκαιρία μεγαλύτερων αποδόσεων, αλλά ταυτόχρονα και επιφυλακτικότητα για τη μελλοντική του εξέλιξη, καθώς είναι ακόμη κάτι που δεν έχει δοκιμασθεί επαρκώς παρά το γεγονός ότι τυχόν αδυναμίες που προέκυψαν μέχρι σήμερα ξεπεράστηκαν επιτυχώς.

Τα βασικά χαρακτηριστικά του bitcoin, όπως ο αποκεντρωμένος χαρακτήρας, η ασφαλής και ανεπηρέαστη καταγραφή των συναλλαγών που γίνονται και η απλή και ευέλικτη χρήση του ψηφιακού νομίσματος συντελούν στο να προσδώσουν δυναμική σε αυτό.

Όμως άλλο είναι η υιοθέτηση του ψηφιακού νομίσματος στις συναλλαγές και άλλο η επένδυση για να ασχοληθεί κάποιος με το mining, επένδυση που σίγουρα δεν αξίζει να γίνει.

Τα ψηφιακά νομίσματα είναι για την ώρα ένα σύστημα που βρίσκεται στα πρώτα στάδια της ζωής του, έχει ακόμη κενά ασφαλείας που εύκολα, όπως φαίνεται, μπορούν να εκμεταλλευθούν οι χάκερς, υπάρχει πάντοτε η περίπτωση αποτυχίας μιας startup που βασίζεται σε αυτά και τίποτα δεν μας εγγυάται ότι η τιμή τους δεν θα ξεφουσκώσει.

Η γνώση και η κατανόηση της λειτουργίας των ψηφιακών νομισμάτων θα βοηθήσει στο να αξιολογήσουμε καλύτερα τα προβλήματα που μπορεί να δημιουργηθούν από τη χρησιμοποίηση τους και ως εκ τούτου να μπορέσουμε να καταλάβουμε πληρέστερα τις ανάγκες πρόληψης στις οποίες πρέπει να εστιάσουμε

Τα κρυπτονομίσματα προσφέρουν έναν τρομακτικό αριθμό δυνατοτήτων τις οποίες ούτε τις φανταζόμασταν πριν μία δεκαετία ή ακόμα και πριν από 5 χρόνια. Ο ρυθμός ανάπτυξης είναι μεγάλος σε επίπεδο λογισμικού και καινοτομιών αλλά σίγουρα όχι τόσο μεγάλος όσο σε επίπεδο αποδοχής από τον κόσμο.

Στην Ελλάδα, όπως και αλλού, ο κόσμος έχει μάθει να θεωρεί το χρήμα σαν κάτι που συνδέεται με τη λειτουργία του κράτους και ως εκ τούτου είναι επιφυλακτικός απέναντι σε κάτι που διαφέρει ριζικά με αυτό. Η επιφυλακτικότητα όμως του Έλληνα ισορροπείται από την έμφυτη τάση του για τζόγο και για το λόγο αυτό έχει αρχίσει και στην Ελλάδα να υπάρχει μια κινητικότητα γύρω από τα ψηφιακά νομίσματα και το bitcoin.

Όμως στη τάση για περαιτέρω ενίσχυση της δυναμικής ένας από τους σημαντικότερους προβληματισμούς που οδηγούν σε αναστολή της είναι ότι λόγω της απουσίας ελέγχου αποτελεί ένα άκρως ελκυστικό μέσο για παράνομες συναλλαγές και ηλεκτρονική νομιμοποίηση εσόδων από παράνομες δραστηριότητες. Επίσης, αυξάνει το ρίσκο για κακόβουλη πρόσβαση στον υπολογιστή, με σκοπό την κλοπή των χρημάτων, όπως μαρτυρούν μια σειρά από σχετικές αναφορές.

Η εργασία μας οδηγεί στο συμπέρασμα ότι πιο πολύ και από το σκεπτικό που οδηγεί στην υιοθέτηση ή όχι των ψηφιακών νομισμάτων πιο μεγάλη σημασία έχει να πιστέψει μια χώρα στα ευρύτερα οφέλη της τεχνολογίας blockchain στην οποία στηρίζεται το bitcoin. Η τεχνολογία πίσω από το ψηφιακό νόμισμα Bitcoin μπορεί να μεταμορφώσει τον τρόπο που συναλλασσόμαστε, ανταλλάζουμε δεδομένα και στοιχεία, ώστε τα πάντα να γίνονται χωρίς μεσάζοντες. Το δίλημμα για τις τράπεζες είναι μεγάλο καθώς θα πρέπει να επιλέξουν αν θα πολεμήσουν την απειλή ή αν θα αξιοποιήσουν την ευκαιρία. Η χώρα όμως γενικότερα πρέπει να χρησιμοποιήσει τη τεχνολογία αυτή για την γενικότερη διακυβέρνηση της π.χ κτηματολόγιο στο blockchain, συμβόλαια στο blockchain, ενεργειακά δίκτυα, κ.α.

Βιβλιογραφικές αναφορές

Ελληνικές

Αποστολίδου Κυριακή, (2008). *Εφαρμογές της κρυπτογραφίας*. Διπλωματική εργασία, ΤΕΙ Δυτ. Μακεδονίας, Κοζάνη 2008.

Κετιτζιάν Στάθης, (2017*). Το πρώτο ελληνικό ψηφιακό νόμισμα είναι εδώ*, (online), 05 Σεπτεμβρίου 2017 δημοσιεύθηκε στο epixeiro.gr. http://www.epixeiro.gr/article/60408

Κορδώνης Στράτος, (20170*. Bitcoin: Το ψηφιακό σας πορτοφόλι*, (online), 15 Δεκεμβρίου 2017 δημοσιεύθηκε στο unboxholics. https://unboxholics.com/stories/27944-bitcoin-to-psifiako-sas-portofoli

Κυρίτσης Άγγελος, (2016). *Κρυπτογράφηση Δεδομένων – Τι είναι και Πώς Λειτουργεί,* (online),δημοσιεύθηκε την 21/01/2016 στο PCsteps. https://www.pcsteps.gr/16634-%ce%ba%cf%81%cf%85%cf%80%cf%84%ce%bf%ce%b3%cf%81%ce%ac%cf%86%ce%b7%cf%83%ce%b7

Μαρτίνο Ιωαν, (2017*). BITCOIN Ο απόλυτος οδηγός*. Εκδότης ο Φανταστικός Κόσμος, 2015

Μαυρέλη Κωνσταντίνα, (2015). *Το ψηφιακό νόμισμα Bitcoin*. Πτυχιακή εργασία ΑΤΕΙ Κρήτης, Ηράκλειο 2015

Μπαλάς Φώτης, (2017). *Τι είναι το Ethereum: Όλα Όσα Πρέπει να Ξέρετε,* (online),δημοσιεύθηκε την 20/06/2017 στο PCsteps. https://www.pcsteps.gr/199177-%CF%84%CE%B9-%CE%B5%CE%AF%CE%BD%CE%B1%CE%B9-%CF%84%CE%BF-ethereum

Μωράτης Γιώργος, (2017). *Ripple ένα κρυπτονόμισμα με ιδιαιτερότητες,* (online),07 Σεπτεμβρίου 2017 δημοσιεύθηκε στο Capital. http://www.capital.gr/me-apopsi/3237758/pera-apo-to-bitcoin-ripple-ena-kruptonomisma-me-idiaiterotites

Ξαρχάκου Αναστασία, (2017). Το ψηφιακό νόμισμα: η θεωρητική,οικονομική και τεχνολογική προσέγγιση του. Διπλωματική εργασία, Πανεπιστήμιο Μακεδονίας, Οκτώβριος 2017.

Παπαϊωάννου Γιάννης, (2017). *Blockchain: Η επόμενη τεχνολογική επανάσταση,* δημοσιεύθηκε 24.11.2017 στο lifo.gr, http://www.lifo.gr/articles/technology_articles/170283

Πανσεληνά Έρη, (2018). *Οσα πρέπει να γνωρίζετε για το bitcoin σε 7 ερωτήσεις,* (online), 23 Ιανουαρίου 2018, δημοσιεύθηκε στο http://www.news247.gr/oikonomia/osa-prepei-na-gnorizete-gia-to-bitcoin-se-7-erotiseis.6573327.html

Παρασκευόπουλος-Κόλιας Χρήστος, (2014). *Οικονομικές, Τεχνικές και Νομικές όψεις του bitcoin*. Legal Insight, http://yiannatsis.gr/download/bitcoin%20gr.pdf

Φυτιλής Γιάννης, (2017*), Τι είναι το Blockchain και πώς κάνει ασφαλή τα Ψηφιακά Νομίσματα*, (online), 07 Σεπτεμβρίου 2017 δημοσιεύθηκε την 27/07/2017 στο

https://www.pcsteps.gr/214154-%CF%84%CE%B9-%CE%B5%CE%AF%CE%BD%CE%B1%CE%B9-%CF%84%CE%BF-blockchain-%CF%88%CE%B7%CF%86%CE%B9%CE%B1%CE%BA%CE%AC-%CE%BD%CE%BF%CE%BC%CE%AF%CF%83%CE%BC%CE%B1%CF%84%CE%B1/

Ξένες

Ahamad Shaik Shakeel, Nair Madhusoodhnan, Vargese Biju, (2013). *A Survey on Crypto Currencies*. Association of Computer Electronics and Electrical Engineers, Proceedings of International Conference on Advances in Computer Sciences, 2013

Ametrano Ferdinando M., (2016). Hayek Money: *The Cryptocurrency Price Stability Solution*, (online),13 August 2016, SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2425270

Antonopoulos Andreas, (2014). *Mastering Bitcoin: Unlocking Digital Cryptocurrencies* O'Reilly Media; 1 edition (December 20, 2014)

Damiani Jesse, (2017). *6 Possible Explanations Why Bitcoin and Cryptocurrency Prices Dropped,* (online) Forbes, December 22, 2017. Διαβάστηκε από: https://www.forbes.com/sites/jessedamiani/2017/12/22/6-possible-explanations-why-bitcoin-and-cryptocurrency-prices-dropped-so-low-yesterday/#110ff84e3e2e

Dannen Chris, (2017). *Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners*. Apress 1st ed. Edition (March 18, 2017)

Fernando Jason, (2018). *Bitcoin Vs. Litecoin: What's the Difference*? (online) Investopedia, updated February 15, 2018. https://www.investopedia.com/articles/investing/042015/bitcoin-vs-litecoin-whats-difference.asp

Franco Pedro, (2014). *Understanding Bitcoin: Cryptography, Engineering, and Economics.* The Wiley Finance Series, Wiley; 1 edition (November 24, 2014)

Grinberg R., (2011). *Bitcoin: An Innovative Alternative Digital Currency*. Hastings Science & Technology Law Journal 4

Huth Michael, (2009). *Symmetric Key Cryptography*. Network Security Presentations, October 2009.

Ivaschenko, A.I., (2016*). Using Cryptocurrency in the Activities of Ukrainian Small and Medium Enterprises in order to improve their investment attractiveness*. Problems of economy, (3), p. 267-273.

Mayer Jakob, (2018). *The history of Ethereum,* (online), published January 3,2018 at Jaxenter. https://jaxenter.com/history-ethereum-140143.html

McFarlane Greg, (2017). *What Is Litecoin And How Does It Work?* (online) Investopedia, updated December 22, 2017. https://www.investopedia.com/articles/investing/040515/what-litecoin-and-how-does-it-work.asp

Miteva-Kacarski Emilija, Bunjaku Flamur and Bunjaku Flamur, (2017). *Cryptocurrencies Advantages and Disadvantages*. University Goce Delcev

Murphy Edward V., Murphy Maureen M., SeitzingerMichael V., (2015). *Bitcoin: Questions, Answers, and Analysis of Legal Issues*. Congressional Research Service, October 13, 2015.

Narayanan Arvind, Bonneau Joseph, Felten Edward, Miller Andrew and Goldfeder Steven, (2016*). Bitcoin and Cryptocurrency Technologies*. Princeton University Press

Peterson Thad & Van Wezel Ron, (2016). *The Evolution of Digital and Mobile Wallets*. Mahindra Comviva, August 2016)

Pryzmont Piotr, (2016). *An empirical study of how Bitcoin related incidents impact its price volatility*. Master of Business Administration, National College of Ireland, August 2016.

Stark Harold, (2017). *From here to where? Bitcoin and the future of Cryptocurrency,* (online) Forbes, April 21, 2017. Διαβάστηκε από:

https://www.forbes.com/sites/haroldstark/2017/04/21/from-here-to-where-bitcoin-and-the-future-of-cryptocurrency/#73a255ec4367

Taylor, Michael Bedford, (2013). *Bitcoin and the age of bespoke silicon*. Proceedings of the 2013 International Conference on Compilers, Architectures and Synthesis for Embedded Systems. Piscataway, NJ

Torpey Kyle, (2017). *Comparing Bitcoin and Other Cryptocurrencies by 'Market Cap' Can Be Very Misleading,* (online) Forbes, December 29, 2017. Διαβάστηκε από: https://www.forbes.com/sites/ktorpey/2017/12/29/comparing-bitcoin-and-other-cryptocurrencies-by-market-cap-can-be-very-misleading/#3950d1a92509

Tymoigne (2015). *Do Cryptocurrencies Such as Bitcoin Have a Future*? No: As a Currency, Bitcoin Violates All the Rules of Finance. Wall street journal – Eastern edition, 265(49)

Wiatr, M., (2014). *Bitcoin as a Modern Financial Instrument*. Digital Repository of Polessky State University (2014)

Wood Gavin, (2015). Ethereum: *A Secure Decentralised Generalised Transaction Ledger*. Yellow paper

Στο Διαδίκτυο

https://en.wikipedia.org/wiki/Ripple_(payment_protocol)

https://mightyfoxblog.files.wordpress.com/2017/06/understanding-ethereum.pdf

https://github.com/ethereum/wiki/wiki/White-Paper#ethereum-accounts

https://cointelegraph.com/ethereum-for-beginners/what-is-ethereum

http://fortune.com/2017/07/25/bitcoin-ethereum-cryptocurrency-predictions/

http://www.helleniccoin.com

https://cointelegraph.com/explained/proof-of-work-explained

Παραρτήματα

Παράρτημα Α’ Οι επιχειρήσεις που δέχονται σήμερα bitcoins στην Ελλάδα

Name	Category	Location
Bitrefill	Top up prepaid Wind, Vodafone, Cosmote and CYTA phones	Online
The Cube	Coworking space	Athens,
My Sunshine	Maternity and baby products	Athens
KEEN Organic Living	Children's apparel	Athens,
Aggelos Tavern	Tavern	Haidari,
Bike Lounge	Bicycle shop	Marousi,
Tsourapa Furniture	Furniture	Athens,
Feel Your Home	Household items	Athens,
Omega Gaming Center	Gaming center	Alimos,
daskaloi.gr	Education masketplace	Athens,
Yampouranis and Yampouranis	Lawyers	Athens,
Ioannis Igglezakis	Lawyer	Thessaloniki,
Tic Tac	Data recovery	Elliniko, Attica,

Northwind	Data recovery	Thessaloniki, and Athens,
Ratio Legal Services	Legal Services	Thessaloniki, Macedonia,
MultiCopter	Drones	Haidari
Tetradio	Bookshop	Athens
Biofire	Bioethanol fireplaces	Athens,
Casa del Bambino	Children's Clothing Store	Athens, Attica, Greece
Sousourades	Women's clothes	Athens, Attica, Greece
Hiotis	Fire extinguishers	Nea Ionia, Attica, Greec

Clinical laboratory Pegklis Evangelos	Clinical laboratory	Kalyvia Thorikou, Attica,
Priona Resort	Rooms to rent	Skotina, Pieria,
Villa Pergola - Andros	Villas to rent	Andros, Cyclades,
Paros Paradise Villas	Villas to rent	Paros, Cyclades,
Savvas Sandals	Leather sandals worthshop	Rhodes, Greece
Lord Underware	Underware manufacturer	Katerini, Pieria,
PetWorkz	Pet shop	Voula, Attica,
Anik Snacks	Zante foodstuff	Agia Paraskevi,
Innoview	Web sites, e-shops, mobile apps	Αττική,
Pointer.gr	Web hosting and domain name provider	Thessaloniki,
E64.gr	Web development	Thessaloniki, Macedonia, Greece
Papaki.gr	Web hosting and domain provider	Heraklion, Crete,
Miniweb	Internet services	Ierapetra, Crete,

Alda Shop	Gift shop	Rethymno, Crete,
Imam Baildi	Gift shop	Rethymno, Crete, Greece
Irinaios Roustas	Insurance agent, e.roystas@yahoo.gr, 6977562156	Porto Rafti, Attica,
Dimitris Dimitriou	Accountant	Volos, Magnisia,
Stampa Stampa	Print decorated garmets and accessories	Volos, Magnisia, Greece
Komitini online	Portal	Komotini, Rodopi,
Gee	Coffee and breakfast	Komotini, Rodopi,
Easy.gr	Telephony, Web hosting and domain provider	Athens, Attica,
Digitech4all.eu	Computer and cellphone shop	Athens, Attica,
Skytech	Computer shop	Athens, Attica,
allVoIP	VoIP Telephony	Neo Iraklio, Attica,
Computer Lab	Computer shop	Nikaia, Attica,
HostChefs	Website Design & Hosting	Volos, Greece
Advanced Computing	IT solutions	Thessaloniki and Halkidiki, Greece
Hotwater	Plumbing, heating, air conditioning, natural gas	Aegaleo, Attica,
Digifort	Home security	Athens, Attica, Greece
Fit.gr	Food supplements	Athens, Attica,
Meat Pro	School for Butchers	Athens, Attica,
Sign New Media Advertising	Outdoor Advertising, Signs and Brochures, 21	Athens, Attica,
Mybrand Shoes	Shoe Shop	Petroupoli, Attica,
3DMagic	3D Printing	Ilion, Attica,
Pharmacy128	Pharmacy	Thessaloniki, Macedonia,

Ergobyte	Software and Website Development	Thessaloniki, Macedonia,
Athera	Geospatial Information	Thessaloniki, Macedonia,
Carnet	Car accessories	Thessaloniki, Macedonia,
Movement and Function	Physiotherapy center	Thessaloniki, Macedonia,
SOFTWeb	Internet and mobile app services	Thessaloniki, Macedonia, Greece
ELTA shop at Pagkrati	Post Office	Athens, Attica,
Hersonissos Pharmacy	Pharmacy	Hersonissos, Heraklion, Crete,
Nostos	Restaurant	Agia Marina, Chania, Crete,
KAOL Energy Solutions	Energy systems	Zante, Greece
Kimioni Pharmacy	Pharmacy	Elliniko, Attica, Greece
Vrana Pharmacy and e-farmacy.gr	Pharmacy and online pharmacy	Elliniko, Attica,
Green Grow	Hydroponic products	Glyfada, Attica,
Galinos.gr	Pharmaceutical drug guide	Thessaloniki, Macedonia, Greece
Oral & Maxillofacial Medicine & Surgery Center	Oral & Maxillofacial Surgery - Oral Medicine - Oral Implantology	Agia Paraskevi, Attica,
Dr Aias-Theodoros Papastavrou	Ear Nose Throat doctor	Athens, Attica,
Medical Dent	Dentist	Athens, Attica,
Teddywear	Children's apparel and shoes	Thessaloniki, Macedonia, Greece
Directshop	Computer eshop	Ioannina, Epirus,
Dimitrios Ntaras	Photography and videography	Ioannina, Epirus, Greece

Uniphone	Mobile phone shop	Arta, Epirus,
WebToner	Printer ink and toner	Aspropyrgos, Attica, Greece
OK Anytime Market Agia Paraskevi	Mini super market. Franchise page	Agia Paraskevi, Attica,
Lennon Eco-gastrobar	Cafe	Patras, Greece
Pytheas Group	Sand blasting specialists	Patras, Greece
Apela	Lakonia business guide and photography services	Sparta, Greece
Ap. Th. Kyritsi Pharmacy	Pharmacy	Karditsa, Greece
DeltaHacker	Greek e-magazine for computers and hacking	Thessaloniki, Macedonia, Greece
Pistacia Natura	Cosmetics based on pistachio oil (accepts Bitcoin in-store only)	Aegina, Greece
EKIVOLOS	Car roadworthiness certification	Istiaia, Evia,
Englouvi's Lentils	Lentil farmer	Englouvi, Lefkada,
Chronostore	Wrist watch store	Corfu,
Here Comes The Paint TShirt Printing	TShirt Printing	Attica, Greece
Cardia Cafe	Coffee shop	Athens, Attica,
Extravagant coiffure	Coiffure	Nea Erythrea, Attica, Greece
Alexandros Hair Salon	Hair salon	Athens, Attica,
Oranje Beach Bar	Beach Bar	Almyros, Magnisia,
Fitness Tempo	Gym	Trikala, Thessaly,
Apartments	Short term lets. Contact gale5ole@gmail.com	Thessaloniki, Trikala,
Win2	Civil Engineers	Panorama, Macedonia,

Nikodimos El. Stavridis Law Office	Law Office	Serres, Macedonia, Greece
SafeWallet	RFID-safe wallets	Veria, Macedonia,
Kosmodiahirisi Saplatera Vasiliki	Building management	Kilkis, Macedonia, Greece
Aqua Mare	Fish Spa	Nafplio, Argolis,
The Project Garments	Mens fashion	Neo Iraklio, Attica,
Stavros Poulikarakos	Electrical shop tel. 2104815981	Piraeus, Attica, Greece
Vinos	Wine bar restaurent	Mykonos, Greece
KLOSTI	Gift shop	Online, Greece
SNIF	Web directory	Online, Greece
University of Nicosia	University	Nicosia, Cyprus
Expedia	Hotels	International
Gyft	US gift cards (Amazon.com, eBay, Hotels.com, ...)	International
eGifter	US gift cards (Skype, Amazon.com, eBay, Hotels.com, ...)	International
GiftOff	European gift cards (Amazon.co.uk, Skype, Spotify, Google Play, ...)	International