

Τ.Ε.Ι. Δυτικής Ελλάδας
Τμήμα Μηχανικών Πληροφορικής Τ.Ε.



Μη ρυθμιζόμενα ψηφιακά νομίσματα

ΕΞΕΛΙΚΤΙΚΗ ΔΙΑΔΙΚΑΣΙΑ ΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ
ΝΟΜΙΣΜΑΤΩΝ ΚΑΙ ΕΞΟΡΥΞΗ ΤΟΥ BITCOIN

Αναστάσιος Αγγελάκης AM 1308
Δημητρίου Μαρία AM 1369

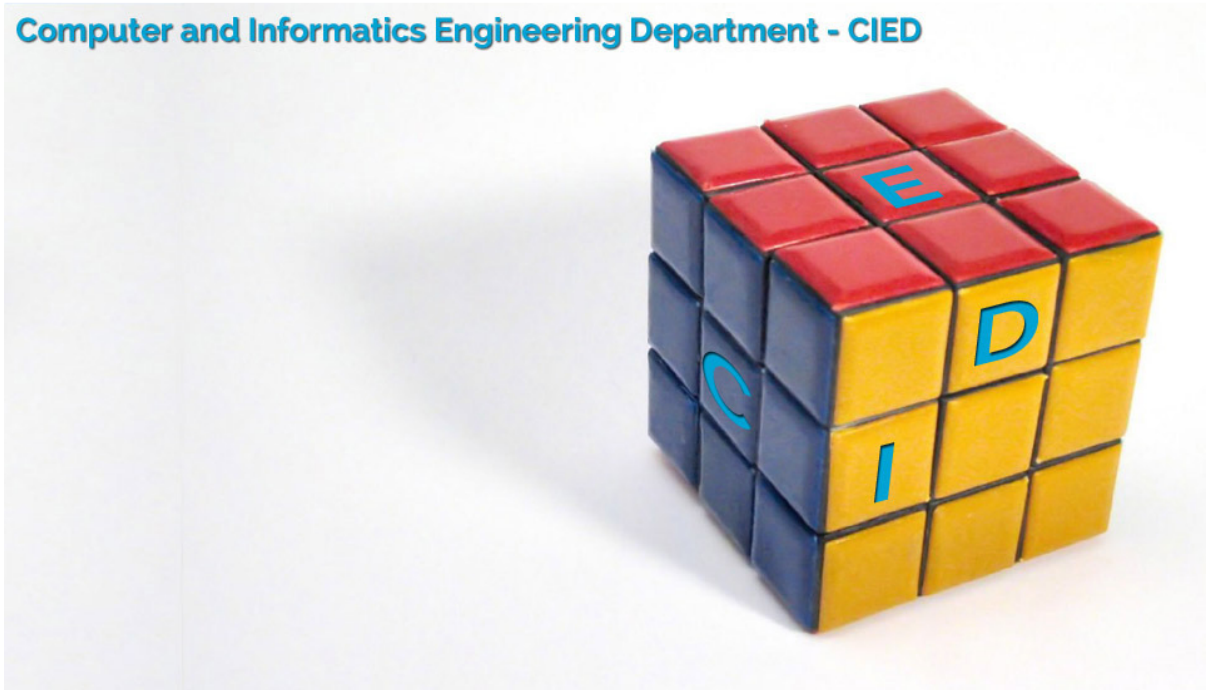
Επιβλέπωντας Καθηγητής: **Ασημακόπουλος Γεώργιος**

Μη ρυθμιζόμενα ψηφιακά νομίσματα

Τ.Ε.Ι. Δυτικής Ελλάδας

Τμήμα Μηχανικών Πληροφορικής Τ.Ε.

Computer and Informatics Engineering Department - CIED



Επιβλέπωντας Καθηγητής: **Ασημακόπουλος Γεώργιος**

Εισαγωγή

Σε αυτή την εργασία, η οποία υλοποιείται στα πλαίσια πτυχιακής εργασίας, θα ασχοληθούμε με τα ηλεκτρονικά νομίσματα. Θα περιγράψουμε το χρονικό διάστημα από τη δημιουργία τους, τη χρήση τους έως σήμερα, καθώς επίσης και τα προβλήματα που έχουν δημιουργηθεί. Θα αναφέρουμε κάποιες περιπτώσεις ψηφιακών νομισμάτων και στη συνέχεια θα αναλύσουμε την περίπτωση του bitcoin

Το bitcoin αποτελεί την πιο εξελιγμένη μορφή χρήματος. Σε αυτήν την εργασία λοιπόν θα κάνουμε μια ιστορική αναδρομή των ψηφιακών νομισμάτων και στη συνέχεια θα αναλύσουμε τα χαρακτηριστικά του bitcoin. Θα αναλύσουμε την εξόρυξη, τον τρόπο με τον οποίο αποθηκεύονται τα bitcoins που έχουμε στη διάθεσή μας. Επίσης θα αναφερθούμε σε κακόβουλες ενέργειες που έχουν παρατηρηθεί από την έναρξη του έως σήμερα.

Μη ρυθμιζόμενα ψηφιακά νομίσματα

Περιεχόμενα

Εισαγωγή	2
Κεφάλαιο 1	8
1.1 Περί νομισμάτων	8
1.1.1 Η προκερματική περίοδος.....	8
1.2.1 Τα πρώτα νομίσματα.....	9
1.1.2 Σήμερα	10
1.2 Ψηφιακά Νομίσματα.....	10
Κεφάλαιο 2	12
2.1 Μια σύντομη ιστορική αναδρομή.....	12
2.2 Εξειδικευμένη περιγραφή για το bitcoin	14
2.2.1 Τι είναι το bitcoin.....	14
2.2.2 Πώς λειτουργεί το Bitcoin	15
2.2.3 Πλεονεκτήματα του Bitcoin	15
2.2.4 Μειονεκτήματα του Bitcoin.....	17
2.2.5 Bitcoin και προστασία προσωπικών δεδομένων	17
2.2.6 Τι συμβαίνει όταν τα bitcoins χαθούν;	18
2.3 Νομικά ζητήματα.....	18
2.4 Εξόρυξη	19
2.4.1 Τι είναι η εξόρυξη του Bitcoin	19
2.4.2 Η λειτουργία της εξόρυξης	20
2.4.3 Δαπάνη ενέργειας για εξόρυξη	21
2.4.4 Συνάφεια μεταξύ εξόρυξης και ασφάλειας.....	21
2.4.5 Υλικό και Λογισμικό που χρησιμοποιείται για την εξόρυξη.....	22
2.4.6 Εξόρυξη με cloud.....	23
2.4.6.1 Τύποι εξόρυξης μέσω cloud.....	24

Μη ρυθμιζόμενα ψηφιακά νομίσματα

2.4.6.2 Ρίσκα και Ανταμοιβή	25
Κεφάλαιο 3ο	27
3.1 Πισίνες Εξόρυξης - Mining Pools.....	27
3.1.1 Διαδεδομένες πισίνες εξόρυξης	27
3.1.2 Συμβουλές για αρχάριους	29
3.1.3 Μέθοδοι διαμοιρασμού νομισμάτων	29
3.2 Ανταλλακτήρια Bitcoin	31
3.2.1 Λειτουργία των ανταλλακτηρίων	31
3.2.2 Γνωστά Ανταλλακτήρια.....	32
3.2.3 Εναλλακτικοί τρόποι ανταλλαγής.....	33
3.2.4 Κίνδυνοι και Προφυλάξεις	33
3.2.5 Ανταλλακτήρια κρυπτονομισμάτων	34
3.3 Φύλαξη bitcoins εκτός-δικτύου	35
3.3.1 Εταιρείες Φύλαξης Bicoins.....	35
3.3.2 Διασφαλίζοντας το πορτοφόλι σας.....	36
3.3.3 Online υπηρεσίες	37
3.3.4 Αντίγραφα ασφαλείας.....	38
3.3.4.1 Αντίγραφα ασφαλείας για ολόκληρο το πορτοφόλι σας.....	38
3.3.4.2 Κρυπτογράφηση των online αντίγραφων ασφαλείας	39
3.3.4.3 Πολλές και ασφαλείς τοποθεσίες.....	39
3.3.5 Συμβουλές για το πορτοφόλι σας.....	39
Κεφάλαιο 4 ^ο	41
4.1 Εξόρυξη με χρήση λογισμικού μέσω server	41
4.1.1 Εξυπηρετητής.....	42
4.2 Παραδείγματα Υλοποίησης	44
4.2.1 Προσπάθεια εξόρυξης με χρήση 3000 server - iDrive	44
4.2.2 Κόστος της εξόρυξης.....	45
4.2.3 Χρονικοί περιορισμοί	45

Μη ρυθμιζόμενα ψηφιακά νομίσματα

4.2.3 Αύξηση των εσόδων;	46
4.2.4 Η ασφάλεια και η εξόρυξη.....	46
4.4 Εξόρυξη με χρήση επεξεργαστή AMD.....	47
4.4.1 Βασικές Προϋποθέσεις	47
4.4.2 Εγκατάσταση και προετοιμασία	48
4.4.3 Απομακρυσμένη Διαχείριση.....	49
Κεφάλαιο 5 ^ο	51
5.1 Χρήσεις του Bitcoin.....	51
5.1.1 Η περίπτωση του εστιατορίου	52
5.1.2 Συναλλαγές στη μέση ανατολή.....	53
5.1.3 Η νομική εταιρία του Λονδίνου.....	53
5.1.4 Αφορολόγητο το Bitcoin στην Ευρώπη.....	53
5.1.5 Δάνεια σε Bitcoin;	54
5.1.6 Το πρώτο ATM για Bitcoin στην Ελλάδα	54
5.1.7 Αποπληρωμή εξαγωγών σε Bitcoin	54
5.2 Ισοτιμία	55
5.3 Bitcoin και Νόμοι	57
Επίλογος.....	69
Βιβλιογραφία	71

Μη ρυθμιζόμενα ψηφιακά νομίσματα

Κεφάλαιο 1

1.1 Περί νομισμάτων

1.1.1 Η προκερματική περίοδος

Ο άνθρωπος από την εμφάνισή του στον πλανήτη είχε ως κυρίαρχο μέλημα την εξεύρεση των απαραίτητων αγαθών για την επιβίωσή του. Αρχικά, πριν ακόμα οργανωθεί σε κοινωνίες, το μόνο του μέλημα ήταν το κυνήγι και η συλλογή καρπών. Όταν όμως οργανώθηκε στις πρώτες κοινωνίες, η επιβίωσή τους στηριζόταν στην αυτάρκεια των προϊόντων που παρήγαγαν. Με την εξέλιξη της κοινωνίας ο άνθρωπος διαπίστωσε πως ο επιμερισμός των εργασιών απέφερε μεγαλύτερη αποδοτικότητα και περίσσειμα αγαθών, τα οποία μπορούσε να τα ανταλλάξει με άλλα αγαθά που είτε έλειπαν ή ήταν αδύνατη η παραγωγή τους.

Έτσι γεννήθηκε το εμπόριο. Οι πρώτες συναλλαγές πραγματοποιούνταν με ανταλλαγές των ίδιων των προϊόντων. Η αξία αυτών καθοριζόταν από την σπανιότητά τους, την χρησιμότητά τους ή και από τη δυσκολία παραγωγής τους (Ξενοφών, 430-354 π.Χ., Πόροι 4, Οικονομικός Ι, 10). Η ανταλλαγή όμως των προϊόντων είχε το μειονέκτημα ότι πολλά προϊόντα αλλοιώνονται με το χρόνο, η παραγωγή των αγαθών, η οποία έχει διακυμάνσεις λόγω των καιρικών συνθηκών, δε συμπίπτει πάντα χρονικά με τις ανάγκες ανταλλαγής των προϊόντων. Ακόμα, οι έμποροι πρέπει να είναι κάτοχοι χρήσιμων αγαθών για την ανταλλαγή, ενώ το εμπόρευμα τους πρέπει να είναι ισάξιο με το ανταλλάξιμο προϊόν και κυρίως πρέπει όλοι οι συναλλασσόμενοι να αποδέχονται ένα κοινό μέτρο προσδιορισμού της αξίας των ανταλλασσόμενων προϊόντων.

Ήδη από το τέλος της 3^{ης} χιλιετίας π. Χ. [2] οι κάτοικοι της Μεσοποταμίας, και στη συνέχεια και άλλοι λαοί της Ανατολικής Μεσογείου, χρησιμοποίησαν ζυγισμένα μέταλλα ως μέσο ανταλλαγής και πληρωμής αντί για ζώα, δέρματα ζώων, κοχύλια ή ζυγισμένα σιτηρά που αντάλλαζαν πριν. Τα μέταλλα υπερίσχυσαν και υιοθετήθηκαν για τις συναλλαγές: αναλλοίωτα, με τη δυνατότητα να μπορούν να υποδιαιρεθούν χωρίς να μεταβάλλεται η δομή τους, μπορούσαν εύκολα να μεταφερθούν λόγω μικρού όγκου και να αποθησαυρισθούν χωρίς καμία δαπάνη συντήρησης και διατήρησης. Το μέταλλο χυτευόταν σε ράβδους ή πλίνθους, ενώ συχνά του έδιναν και τη μορφή σύρματος. Επειδή όμως η ακριβής ονομαστική αξία του μετάλλου δεν ήταν επίσημα εγγυημένη από κάποιον, η αξία του υπολογιζόταν με ζύγισμα σε κάθε πληρωμή. Έτσι εξαπλώθηκε η χρήση του ζυγού στην Αίγυπτο και τη Μεσοποταμία χάριν στη συνεχή ανάγκη ζυγίσεων. Αυτά τα ζυγισμένα μεταλλικά τεμάχια, ήταν οι πρόδρομοι του νομίσματος. Οι

Μη ρυθμιζόμενα ψηφιακά νομίσματα

συναλλαγές πραγματοποιούνται χάριν σε αυτό το εύχρηστο μέσον συναλλαγής. Κάθε προϊόν είχε μια εγγενή αξία που αντιστοιχούσε σε ένα συγκεκριμένο βάρος μετάλλου.



Εικόνα 1.1: Αρχαία νομίσματα.

1.2.1 Τα πρώτα νομίσματα

Οι αρχαίες πηγές δεν αναφέρονται σχετικά με τη χρονολογία επινόησης του νομίσματος, ούτε σχετικά με το άτομο ή το λαό που τα επινόησε. Ο Ηρόδοτος αναφέρει ότι οι Λυδοί, λαός κατ' εξοχήν εμπορικός (κάπηλοι), επινόησαν το νόμισμα. Το βασίλειο ήταν οικονομικά προηγμένο, με ισχυρή κεντρική εξουσία, που είχε αναπτύξει το εμπόριο και τη βιοτεχνία. Δεν είναι σίγουρο αν οι Λυδοί ή οι Ίωνες, οι Έλληνες έμποροι της Ιωνίας, ήταν αυτοί που έβαλαν το νόμισμα σε κυκλοφορία και διέδωσαν τη χρήση του γύρω στα 600 με 580 π. Χ. Ένας από τους πρώτους αποθησαυρισμούς που γνωρίζουμε, χρονολογείται γύρω στο 560 π. Χ.. Ο «θησαυρός» ανακαλύφθηκε στα θεμέλια του πρώτου ναού της Άρτεμης στην Έφεσο, περιλαμβάνει 24 νομίσματα από ήλεκτρο που αποδίδονται στη Λυδία και στις πόλεις της Μικράς Ασίας. Κατά συνέπεια μπορούμε να προβληματιζόμαστε ακατάπαυστα χωρίς να δώσουμε μια τελική απάντηση στο ερώτημα.

Το γεγονός είναι ότι το νόμισμα μετά την επινόηση του, διαδόθηκε, έγινε αποδεκτό και κυκλοφόρησε από τις πόλεις, τις φυλές, τις Αμφικτυονίες, τα Κοινά και τα ελληνικά βασίλεια. Η επινόηση του νομίσματος πηγάζει από τις ανάγκες των εμπορικών συναλλαγών, όμως

Μη ρυθμιζόμενα ψηφιακά νομίσματα

αναμφίβολα τα πολιτικά και στρατιωτικά του πλεονεκτήματα δεν παραγνωρίστηκαν. Η αποδοχή και η διάδοσή του προκύπτουν από μία καινοφανή πολιτικοκοινωνική δομή που δεν απαντάται παρά μόνον στον ελληνικό κόσμο. Δεν είναι τυχαίο ότι ο Αριστοτέλης στο έργο του περί Ηθικής Νικομάχου εξηγεί ότι η υιοθέτηση του νομίσματος από την πόλη εξυπηρετεί την εύρυθμη λειτουργία της, και τις ανταλλαγές υπηρεσιών σχετικών με τη δημόσια ζωή, όπως η αγορά από την πόλη σιτηρών ή υλικών για τις δημόσιες κατασκευές, ή πληρωμές των υπαλλήλων και των εργατών, η ανακατανομή του πλεονάσματος στους πολίτες, η είσπραξη φόρων, ενοικίων, η μισθοδοσία και η πληρωμή των μισθοφόρων.

Τα χάρτινα χρήματα ή τραπεζογραμμάτια χρησιμοποιήθηκαν για πρώτη φορά στην Κίνα, κατά τη διάρκεια της Δυναστείας των Σονγκ. Αυτά τα τραπεζογραμμάτια, γνωστά ως "Jiaozhi" εξελίχθηκαν από χρεόγραφο που είχαν χρησιμοποιηθεί από τον 7ο αιώνα μ.Χ., ωστόσο, δεν είχαν σταματήσει τη χρήση των νομισμάτων ουσιαστικής αξίας. Στην Ευρώπη τα πρώτα τραπεζογραμμάτια εξεδόθησαν από τη Stockholms Banco το 1661 και χρησιμοποιήθηκαν παράλληλα με κέρματα.

1.1.2 Σήμερα

Ερχόμενοι στη σημερινή εποχή δεν έχει νόημα άμεσα η έννοια του νομίσματος. Υπάγεται σε μια γενικότερη έννοια, την έννοια του χρήματος. Τι είναι όμως το χρήμα; Σήμερα ο ορισμός του τι είναι χρήμα σε μια οικονομία είναι πολύ συγκεκριμένος: Χρήμα είναι το σύνολο των κερμάτων, τραπεζογραμματίων και καταθέσεων. [3] Οτιδήποτε άλλο εκτός από αυτά τα τρία δεν είναι χρήμα. Ο όρος τραπεζογραμμάτιο είναι συνώνυμος με τον όρο χαρτονόμισμα. Το σύνολο κερμάτων και χαρτονομισμάτων ονομάζεται σύνολο νομισματικής κυκλοφορίας.

Το Χρήμα επιτελεί τις τρεις ακόλουθες βασικές λειτουργίες:

1. Αποτελεί γενικά αποδεκτό μέσο συναλλαγών – ανταλλαγής.
2. Μέτρο υπολογισμού των οικονομικών αξιών.
3. Τέλος, διασφαλίζει την αγοραστική δύναμη του κατόχου του.

1.2 Ψηφιακά Νομίσματα

Μη ρυθμιζόμενα ψηφιακά νομίσματα

Η μορφή του χρήματος σήμερα, πέρα από την χάρτινη ή μεταλλική μορφή του, μπορεί να πάρει και τη μορφή του πλαστικού χρήματος (με τη μορφή κάρτας - πίστωση συναλλαγών σε υπάρχοντες λογαριασμούς καταθέσεων) καθώς και πιο πρόσφατα και τη μορφή του ηλεκτρονικού - ψηφιακού νομίσματος.

Τα ψηφιακά νομίσματα είναι μια μορφή χρήματος που στηρίζεται στην κρυπτογραφία. Για αυτό το λόγο το σύνολο των συναλλαγματικών σε ψηφιακή μορφή διεθνώς αποκαλείται "κρυπτονόμισμα" ή "cryptocurrency" στη διεθνή ορολογία. Τα κρυπτονομίσματα παράγονται συλλογικά από ολόκληρο το σύστημα των χρηστών. Ο ρυθμός και η ποσότητα καθορίζονται κατά τη δημιουργία του εκάστοτε συστήματος και οι κανόνες του είναι δημοσίως γνωστοί, κοινώς αποδεκτοί και σχεδόν αδύνατο να αλλάξουν, σε αντίθεση με τα κεντρικά οικονομικά συστήματα, όπου η ροή και η παραγωγή του χρήματος ελέγχεται από κυβερνήσεις και τραπεζικά διοικητικά συμβούλια. Ωστόσο, παρά τη δύναμή τους, ούτε οι κυβερνήσεις ούτε και οι τράπεζες μπορούν να παράγουν κρυπτοσυναλλάγματα και ως εκ τούτου, τα κρυπτογραφημένα νομίσματα θεωρούνται μια μορφή "αποκεντρωμένου" χρήματος που δεν ελέγχεται από κανέναν και δεν υπόκειται σε κανένα οικονομικό σύστημα. Ο κάθε μεμονωμένος χρήστης είναι υπεύθυνος για τη δημιουργία - εξόρυξη και φύλαξη των ψηφιακών του νομισμάτων. Οι συναλλαγές πραγματοποιούνται μεταξύ χρηστών απευθείας (peer to peer - p2p), βάση ενός κοινού αποδεκτού συστήματος. Το στοιχειώδες σύστημα πάνω στο οποίο στηρίζονται πλέον τα περισσότερα κρυπτονομίσματα βασίζεται στο σύστημα που δημιούργησε ο Satoshi Nakamoto το 2007. [4]

Μέχρι τον Οκτώβριο του 2015, εκατοντάδες ψηφιακά νομίσματα "κυκλοφορούν" στο χώρο του διαδικτύου, το καθένα με το δικό του καπέλο, όσον αφορά το μέγιστο αριθμό νομισμάτων που μπορούν να παραχθούν. Το μέγιστο, το οποίο ορίζεται από το κάθε νόμισμα, μιμείται την σπανιότητα και την αξία του των πολύτιμων μετάλων για την αποφυγή του υπερπληθωρισμού. [5] Τα πιο πολλά στηρίζονται ή είναι παράγωγα του δημοφιλέστερου μέχρι σήμερα ψηφιακού νομίσματος, το bitcoin. [6]

Η ασφάλεια των συναλλαγών βασίζεται στην αμοιβαία εμπιστοσύνη μεταξύ εξορυκτών και στην ειλικρινή προσπάθεια αυτών να διατηρήσουν την καθολικότητα του νομίσματός τους, καθώς όλοι έχουν το οικονομικό κίνητρο της μη απαξίωσης των νομισμάτων τους.

Κεφάλαιο 2

2.1 Μια σύντομη ιστορική αναδρομή

Το BitCoin σαν ιδέα ξεκίνησε το 2007 [7], όταν ο Satoshi Nakamoto ξεκίνησε την επεξεργασία ενός project για τη δημιουργία ενός νέου ηλεκτρονικού συναλλαγματικού μέσου. Το BitCoin. Εικάζεται ότι το όνομα Nakamoto δεν είναι το όνομα ενός μόνο ατόμου αλλά ένα συλλογικό ψευδώνυμο ενός ή περισσότερων ατόμων.

Στις 15 Αυγούστου το 2008, κατοχυρώνεται μια νέα πατέντα[8] από τους Neal Kin, Vladimir Oksman, και Charles Bry για μια εφαρμογή κρυπτογράφησης. Τα χαρακτηριστικά της πατέντας αυτής μοιάζουν με τα χαρακτηριστικά του BitCoin, όπως αυτά φάνηκαν στη συνέχεια, αλλά και οι τρεις αρνούνται οποιαδήποτε σχέση με τον Satoshi Nakamoto, τον υποτιθέμενο δημιουργό του BitCoin. Μερικές μέρες μετά, κατοχυρώνεται στο anonymousspeech.com (μια ιστοσελίδα που επιτρέπει την ανώνυμη κατοχύρωση ονομάτων στο χώρο του διαδικτύου) η ιστοσελίδα με όνομα bitcoin.org. Το BitCoin γεννιέται.



Εικόνα 2.1: Το λογότυπο του bitcoin

Το Bitcoin είναι μια μονάδα μέτρησης ανταλλακτικής αξίας, που φυσικά έχει και υποδιαιρέσεις τις οποίες παραθέτουμε παρακάτω.

- 1 dBTC το οποίο ισούται με 1 δέκατο του Bitcoin
- 1 cBTC το οποίο ισούται με 1 εκατοστό του Bitcoin (όπως για παράδειγμα τα εκατοστά του μέτρου)
- 1 mBTC το οποίο ισούται με 1 χιλιοστό του Bitcoin (όπως για παράδειγμα τα χιλιοστά του μέτρου)
- 1 μBTC το οποίο ισούται με 1 εκατομμυριοστό του Bitcoin

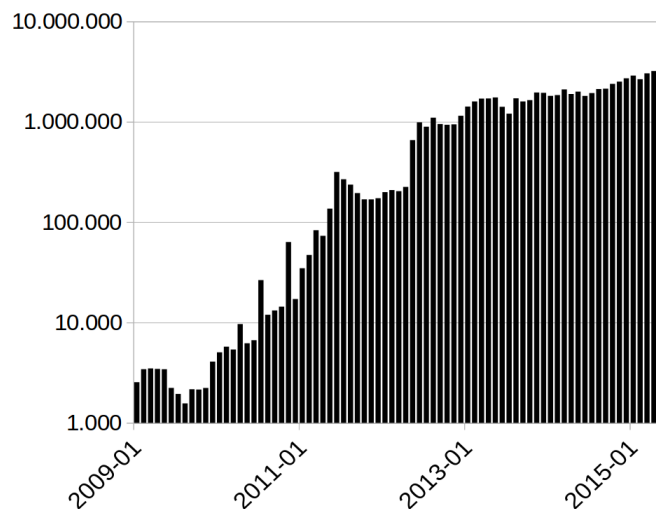
Τον Οκτώβριο του ίδιου έτους δημοσιεύεται το επίσημο paper [9] του Satoshi Nakamoto με τίτλο " Bitcoin: A Peer-to-Peer Electronic Cash System" στην ιστοσελίδα bitcoin.org, για να

Μη ρυθμιζόμενα ψηφιακά νομίσματα

καταχωρηθεί ένα μήνα μετά και η εφαρμογή στο SourceForge.net, μια κοινότητα ανάπτυξης και διανομής λογισμικού ανοικτού κώδικα. Στη συνέχεια το λογισμικό αρχίζει και διατίθεται υπό την άδεια MIT, που όπως φαίνεται από το όνομά της η άδεια αυτή έχει την καταγωγή της από το γνωστό Ινστιτούτο τεχνολογίας της Μασαχουσέτης.

Το πρώτο BitCoin ή το Genesis Block δημιουργείται στις 3 Ιανουαρίου του 2009, και η πρώτη συναλλαγή πραγματοποιήθηκε μερικές μέρες μετά (12 Ιανουαρίου). Τον Οκτώβριο του 2009 έχουμε την καθιέρωση της πρώτης συναλλαγματικής αξίας για το BitCoin, η οποία είναι ίση με $US\$1 = 1,309.03 \text{ BTC}$, ισότητα η οποία συμπεριλαμβάνει και το κόστος του ρεύματος που χρησιμοποιεί ένας υπολογιστής για να εξορύξει BitCoins.

Από την πρώτη συναλλαγή με το νέο νόμισμα το 2009 [10] έως σήμερα, το bitcoin βλέπει τη δημοτικότητά του να ανεβαίνει κατακόρυφα. Οι μηνιαίες συναλλαγές εκτοξεύονται με μεγάλους ρυθμούς, και όπως παρουσιάζεται και στο σχήμα 3, το 2015 φαίνεται να ξεπερνάει τις 1,5 εκατομμύρια μηνιαίες συναλλαγές. Το νέο αυτό νόμισμα ξεκίνησε να είναι αποδεκτό κυρίως από μη κερδοσκοπικούς οργανισμούς ως μορφή δωρεάς – υποστήριξης, για παράδειγμα στη Wikileaks κ.α.. Στη συνέχεια και με την πάροδο του χρόνου, το bitcoin γίνεται κοινώς αποδεκτό σε πολλές συναλλαγές. Όπως θα δούμε σε επόμενο κεφάλαιο, υπήρξαν πολλές προσφυγές ως προς τη νομιμότητά και την εγκυρότητα, αυτό όμως δεν εμπόδισε τις συναλλαγές μεταξύ ιδιωτών μιας και το bitcoin είναι τελείως ανεξάρτητο και δεν ελέγχεται από καμία απολύτως αρχή ή τραπεζικό ίδρυμα.



Εικόνα 2.2: Οι μηνιαίες συναλλαγές με το bitcoin από την πρώτη εξόρυξη μέχρι τον Ιανουάριο του 2015
- Image from Wikimedia Commons, the free media repository (λογαριθμική κλίμακα)

Μη ρυθμιζόμενα ψηφιακά νομίσματα

Φυσικά, ένα από τα αποτελέσματα της δημοτικότητάς του, ήταν η αύξηση της ισοτιμίας του ως προς τα άλλα νομίσματα, αναγνωριζόμενο κατά κάποιο ως ένα πραγματικό νόμισμα. Το ιστορικό υψηλό του bitcoin ήταν στα 1.124,73 US\$ το Νοέμβριο του 2013 (περίπου 970 ευρώ την ίδια εποχή).



Εικόνα 2.3: Η τιμή του bitcoin το Νοέμβριο του 2013 έφτασε τα 1.124,76 US\$, από τα 13,36 US\$ στις αρχές του ίδιου χρόνου. Η τιμή του σταδιακά ξαναέπεσε και πλέον κυμαίνεται σταθερά στα 200-300 US\$ - Image from Wikimedia Commons, the free media repository (ημιλογαριθμική κλίμακα)

Ανάμεσα στις πολλές αιτίες που οδήγησαν σε αυτή την ξέφρενη άνοδο ήταν και η Ευρωπαϊκή κρίση χρέους και ιδιαίτερα η κυπριακή χρηματοπιστωτική κρίση του 2012-13 και οι δηλώσεις του FinCEN (Financial Crimes Enforcement Network) βελτίωσαν την νομική υπόσταση του νομίσματος σε μια περίοδο που το διαδίκτυο έπαιξε μεγάλο ρόλο στην ενημέρωση.

2.2 Εξειδικευμένη περιγραφή για το bitcoin

2.2.1 Τι είναι το bitcoin

Το Bitcoin είναι ένα συναινετικό δίκτυο που παρέχει τη δυνατότητα ενός νέου συστήματος πληρωμών και μιας εντελώς ψηφιακής μορφής χρημάτων. [11] Είναι το πρώτο αποκεντρωμένο δίκτυο πληρωμής μεταξύ ομότιμων (peer-to-peer) που λειτουργεί από τους χρήστες του χωρίς κεντρική αρχή ή μεσάζοντες. Από τη σκοπιά του χρήστη, το Bitcoin θα

Μη ρυθμιζόμενα ψηφιακά νομίσματα

μπορούσε να χαρακτηριστεί ως τα *μετρητά χρήματα του Διαδικτύου*. Το Bitcoin μπορεί επίσης να θεωρηθεί ως το πιο περίφημο λογιστικό σύστημα τριπλής καταχώρησης που υπάρχει.

Κανείς δεν είναι ιδιοκτήτης του δικτύου Bitcoin όπως ακριβώς συμβαίνει και με την τεχνολογία πίσω από το e-mail. Το Bitcoin ελέγχεται, παράλληλα, από όλους τους χρήστες Bitcoin σε όλο τον κόσμο. Ενώ οι προγραμματιστές στην ουσία είναι αυτοί που συμβάλλουν στη βελτίωση του λογισμικού, δεν μπορούν να εξαναγκάσουν καμία αλλαγή στο πρωτόκολλο Bitcoin, διότι όλοι οι χρήστες έχουν την ελευθερία να επιλέξουν την έκδοση του λογισμικού που θα χρησιμοποιούν. Για να διατηρηθεί η συμβατότητα, όλοι οι χρήστες πρέπει να χρησιμοποιούν το λογισμικό που υπακούει στους ίδιους κανόνες. Για να επιτευχθεί η σωστή λειτουργία του Bitcoin απαιτείται η πλήρης συναίνεση μεταξύ όλων των χρηστών. Ως εκ τούτου, δίνεται ένα ισχυρό κίνητρο σε όλους τους χρήστες και τους προγραμματιστές για να προστατεύουν αυτήν την γενική συναίνεση.

2.2.2 Πώς λειτουργεί το Bitcoin

Από τη μεριά του χρήστη, το Bitcoin δεν είναι τίποτα περισσότερο από μια εφαρμογή κινητού τηλεφώνου ή υπολογιστή η οποία παρέχει ένα προσωπικό πορτοφόλι Bitcoin και επιτρέπει στο χρήστη να στέλνει και να λαμβάνει bitcoins μέσω αυτού. Έτσι λειτουργεί το Bitcoin για τους περισσότερους χρήστες.

Στο παρασκήνιο, το δίκτυο Bitcoin μοιράζεται ένα δημόσιο λογιστικό βιβλίο (ledger) που ονομάζεται "block chain" (αλυσίδα των μπλοκ). Αυτό το βιβλίο περιέχει κάθε συναλλαγή που έχει ποτέ επεξεργαστεί από το δίκτυο, επιτρέποντας στον υπολογιστή του χρήστη να εξακριβώνει την εγκυρότητα της κάθε συναλλαγής. Η αυθεντικότητα της κάθε συναλλαγής προστατεύεται από ψηφιακές υπογραφές που αντιστοιχούν στις διευθύνσεις αποστολής, επιτρέποντας σε όλους τους χρήστες να έχουν πλήρη έλεγχο κατά την αποστολή bitcoins από τις δικές τους διευθύνσεις Bitcoin. Επιπλέον, ο καθένας μπορεί να επεξεργαστεί συναλλαγές που χρησιμοποιούν την υπολογιστική ισχύ εξειδικευμένου υλικού (hardware) και να κερδίσει μια ανταμοιβή σε bitcoins για την υπηρεσία αυτή. Αυτό συχνά ονομάζεται εξόρυξη (mining).

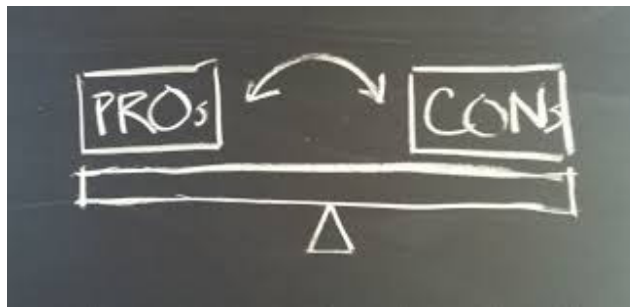
2.2.3 Πλεονεκτήματα του Bitcoin

- *Ελευθερία πληρωμών* - Είναι δυνατό να στείλετε και να λάβετε οποιοδήποτε χρηματικό ποσό αμέσως, οπουδήποτε στον κόσμο, οποιαδήποτε στιγμή. Χωρίς αργίες. Χωρίς σύνορα.

Μη ρυθμιζόμενα ψηφιακά νομίσματα

Χωρίς επιβαλλόμενα όρια. Το Bitcoin επιτρέπει στους χρήστες του να έχουν τον πλήρη έλεγχο των χρημάτων τους.

- *Πολύ χαμηλά τέλη* - Προς το παρόν, οι πληρωμές με Bitcoin γίνονται είτε με μηδενικά είτε με εξαιρετικά χαμηλά τέλη. Οι χρήστες μπορεί να συμπεριλάβουν τέλη στις συναλλαγές τους προκειμένου να έχουν προτεραιότητα στην διεκπεραίωση, κάτι που έχει ως αποτελέσματα την γρηγορότερη επικύρωση των συναλλαγών από το δίκτυο. Επιπροσθέτως, οι επεξεργαστές για εμπόρους υπάρχουν για να τους βοηθήσουν στην επεξεργασία πληρωμών, μετατρέποντας τα bitcoins σε πιστωτικό χρήμα και καταθέτοντας τα κεφάλαια απευθείας στον τραπεζικό λογαριασμό των εμπόρων καθημερινά. Καθώς αυτές οι υπηρεσίες βασίζονται στο Bitcoin, μπορούν να προσφέρονται με πολύ χαμηλότερα τέλη σε σχέση με την PayPal ή δίκτυα πιστωτικών καρτών.



Εικόνα 2.4: Πλεονεκτήματα και Μειονεκτήματα της χρήσης του Bitcoin.

- *Λιγότεροι κίνδυνοι για τους εμπόρους* - Οι συναλλαγές με Bitcoin είναι ασφαλείς, μη αναστρέψιμες και δεν περιέχουν προσωπικές πληροφορίες ή ευαίσθητα προσωπικά δεδομένα των πελατών. Αυτό προστατεύει τους εμπόρους από ζημιές που προκαλούνται από απάτες ή δόλιους αντιλογισμούς χρέωσης (chargebacks) και δεν υπάρχει ανάγκη για συμβατότητα με PCI. Οι έμποροι μπορούν εύκολα να επεκταθούν σε νέες αγορές όπου είτε οι πιστωτικές κάρτες δεν είναι διαθέσιμες, είτε τα ποσοστά απάτης είναι απαράδεκτα υψηλά. Τα αποτελέσματα σε καθαρό κέρδος είναι χαμηλότερα τέλη, μεγαλύτερες αγορές και λιγότερα διοικητικά κόστη.
- *Ασφάλεια και έλεγχος* - Οι χρήστες του Bitcoin έχουν πλήρη έλεγχο των συναλλαγών τους. Είναι ανέφικτο για τους εμπόρους να επιβάλλουν ανεπιθύμητες ή απαρατήρητες χρεώσεις όπως μπορεί να συμβεί με άλλες μεθόδους πληρωμής. Οι πληρωμές με Bitcoin μπορούν να διεξαχθούν χωρίς να συνδέονται προσωπικές πληροφορίες με την συναλλαγή. Αυτό προσφέρει ισχυρή προστασία κατά της κλοπής ταυτότητας. Οι χρήστες του Bitcoin μπορούν επίσης να προστατέψουν τα χρήματά τους με αντίγραφα ασφαλείας και κρυπτογράφηση.

Μη ρυθμιζόμενα ψηφιακά νομίσματα

- *Διαφανής και ουδέτερος* - Όλες οι πληροφορίες που αφορούν τον εφοδιασμό του Bitcoin με χρήματα είναι άμεσα διαθέσιμες στην αλυσίδα των μπλοκ (block chain) για τον οποιονδήποτε να τις επιβεβαιώσει και να τις χρησιμοποιήσει σε πραγματικό χρόνο. Κανένα άτομο ή οργανισμός δεν μπορεί να ελέγξει ή να πλαστογραφήσει το πρωτόκολλο του Bitcoin διότι είναι κρυπτογραφικά ασφαλές. Αυτό επιτρέπει στον πυρήνα του Bitcoin να είναι αξιόπιστος αφού είναι απόλυτα ουδέτερος, διαφανής και προβλέψιμος. [12]

2.2.4 Μειονεκτήματα του Bitcoin

- *Βαθμός αποδοχής* - Πολλοί άνθρωποι δεν είναι ακόμα ενήμεροι για το Bitcoin. Καθημερινά, περισσότερες επιχειρήσεις δέχονται τα bitcoins γιατί θέλουν τα πλεονεκτήματα κάνοντας χρήση του αλλά η λίστα παραμένει μικρή και ακόμα χρειάζεται να μεγαλώσει έτσι ώστε να επωφεληθούμε από τα αποτελέσματα δικτύου.
- *Αστάθεια* - Η συνολική αξία των bitcoins σε κυκλοφορία και ο αριθμός των επιχειρήσεων που χρησιμοποιούν το Bitcoin είναι ακόμα πολύ μικρός σε σύγκριση με αυτό που θα μπορούσε να είναι. Συνεπώς, σχετικά μικρά γεγονότα, συναλλαγές, ή επιχειρηματικές δραστηριότητες μπορούν να επηρεάσουν σημαντικά την τιμή. Θεωρητικά, η αστάθεια αυτή θα μειωθεί καθώς οι αγορές Bitcoin και η τεχνολογία ωριμάζουν. Ποτέ στο παρελθόν δεν έχει δει ο κόσμος ένα νεοσύστατο νόμισμα, οπότε είναι πραγματικά δύσκολο (και συναρπαστικό να φανταστούμε το πώς θα εξελιχθεί.
- *Συνεχής εξέλιξη* - Το λογισμικό του Bitcoin είναι ακόμα σε έκδοση beta με πολλά ημιτελή χαρακτηριστικά σε ενεργή εξέλιξη. Καινούρια εργαλεία, λειτουργίες και υπηρεσίες εξελίσσονται για να κάνουν το Bitcoin πιο ασφαλές και προσβάσιμο στις μάζες. Μερικές από αυτές δεν είναι ακόμα έτοιμες για όλους. Οι περισσότερες επιχειρήσεις Bitcoin είναι νέες και δεν προσφέρουν ασφάλεια ακόμα. Γενικότερα, το Bitcoin είναι ακόμα σε διαδικασία ωρίμανσης.

2.2.5 Bitcoin και προστασία προσωπικών δεδομένων

Το Bitcoin είναι σχεδιασμένο ώστε να επιτρέπει στους χρήστες του να στέλνουν και να λαμβάνουν πληρωμές με ένα αποδεκτό επίπεδο προστασίας προσωπικών δεδομένων όπως γίνεται και σε οποιαδήποτε άλλη μορφή χρημάτων. [13] Από την άλλη πλευρά όμως, το Bitcoin δεν είναι ανώνυμο και δεν μπορεί να προσφέρει το ίδιο επίπεδο προστασίας προσωπικών

Μη ρυθμιζόμενα ψηφιακά νομίσματα

δεδομένων όπως με τα μετρητά. Η χρήση του Bitcoin αφήνει εκτεταμένα δημόσια αρχεία. Υπάρχουν διάφοροι μηχανισμοί ικανοί να προστατέψουν τα προσωπικά δεδομένα των χρηστών και φυσικά όλες αυτές οι διαδικασίες είναι υπό εξέλιξη. Ωστόσο, χρειάζεται ακόμα δουλειά που πρέπει να γίνει πριν οι λειτουργίες αυτές χρησιμοποιούνται σωστά από τους περισσότερους χρήστες του Bitcoin.

Όπως είναι αναμενόμενο έχουν διατυπωθεί κάποιες ανησυχίες ότι οι ιδιωτικές συναλλαγές με Bitcoin θα μπορούσαν να χρησιμοποιηθούν για παράνομους σκοπούς. Ωστόσο, αξίζει να σημειωθεί ότι το Bitcoin θα υπόκειται αναμφίβολα σε παρόμοιους κανονισμούς με αυτούς που ήδη εφαρμόζονται στα υπάρχοντα χρηματοοικονομικά συστήματα. Το Bitcoin δεν μπορεί να είναι πιο ανώνυμο από τα μετρητά και η πιθανότητα να εμποδίζει την διεξαγωγή εγκληματολογικών ερευνών είναι μικρή. Επιπροσθέτως, το Bitcoin είναι σχεδιασμένο επίσης για να αποτρέπει ένα μεγάλο φάσμα οικονομικών εγκλημάτων.

2.2.6 Τι συμβαίνει όταν τα bitcoins χαθούν;

Στην περίπτωση που ένας χρήστης χάσει το πορτοφόλι του, έχει ως αποτέλεσμα τα χρήματα να βγαίνουν εκτός κυκλοφορίας. Τα χαμένα bitcoins παραμένουν ακόμα στην αλυσίδα των μπλοκ (block chain) ακριβώς όπως και όλα τα άλλα bitcoins. Ωστόσο, τα χαμένα bitcoins παραμένουν ανενεργά για πάντα διότι δεν υπάρχει η δυνατότητα για κάποιον να βρει το ιδιωτικό κλειδί – ή τα ιδιωτικά κλειδιά - που θα τους επιτρέψουν να ξοδευτούν ξανά. Εξαιτίας του νόμου προσφοράς και ζήτησης, όταν υπάρχουν λιγότερα bitcoins διαθέσιμα, τα εναπομείναντα θα έχουν μεγαλύτερη ζήτηση και αυτό έχει ως αποτέλεσμα να την αύξηση της αξίας τους για αντιστάθμισμα.

2.3 Νομικά ζητήματα

Βάσει όσων γνωρίζουμε, το Bitcoin δεν έχει καταστεί παράνομο από την νομοθεσία στις περισσότερες δικαιοδοσίες. Ωστόσο, μερικές δικαιοδοσίες (όπως η Αργεντινή και η Ρωσία) περιορίζουν αυστηρά ή απαγορεύουν ξένα νομίσματα. Άλλες δικαιοδοσίες (όπως η Ταϊλάνδη) μπορεί να περιορίζουν την αδειοδότηση σε συγκεκριμένους φορείς όπως τα ανταλλακτήρια Bitcoin.

Μη ρυθμιζόμενα ψηφιακά νομίσματα

Οι ρυθμιστικές αρχές από διάφορες δικαιοδοσίες λαμβάνουν μέτρα για να παρέχουν σε ιδιώτες και επιχειρήσεις κανόνες για το πώς θα ενσωματώσουν αυτή τη νέα τεχνολογία με το επίσημο, ρυθμιζόμενο χρηματοοικονομικό σύστημα. Αναφέρουμε ως παράδειγμα, το Δίκτυο Δίωξης Οικονομικών Εγκλημάτων (FinCEN), μια υπηρεσία του Υπουργείου Οικονομικών των ΗΠΑ, το οποίο εξέδωσε κατευθυντήριες γραμμές μη δεσμευτικού χαρακτήρα για το πώς χαρακτηρίζει ορισμένες δραστηριότητες που σχετίζονται με εικονικά συναλλάγματα.

Θα αναλύσουμε τα περί νομοθεσίας, αναλυτικά ανά χώρα στο 5^ο κεφάλαιο της εργασίας.

2.4 Εξόρυξη

2.4.1 Τι είναι η εξόρυξη του Bitcoin



Εικόνα 2.5: Εξόρυξη του Bitcoin.

Η εξόρυξη (mining) [14] είναι η διαδικασία δαπάνης υπολογιστικής ισχύος ώστε να πραγματοποιείται η επεξεργασία των συναλλαγών, να ασφαλιστεί το δίκτυο και για να παραμείνουν όλοι στο σύστημα συγχρονισμένοι.

Μπορούμε να το θεωρήσουμε ως το κέντρο δεδομένων του Bitcoin με εξαίρεση ότι έχει σχεδιαστεί για να είναι πλήρως αποκεντρωμένο, με εξορύκτες που λειτουργούν σε όλες τις χώρες και κανένας δεν έχει τη δυνατότητα να ασκεί έλεγχο πάνω στο δίκτυο. Αυτή η μέθοδος αναφέρεται ως εξόρυξη του Bitcoin (mining) εμπνευσμένο από την εξόρυξη χρυσού, καθώς είναι ένας προσωρινός μηχανισμός που χρησιμοποιείται στην έκδοση νέων bitcoins. Ωστόσο, σε αντίθεση με την εξόρυξη χρυσού, η εξόρυξη Bitcoin παρέχει μια ανταμοιβή σε αντάλλαγμα των χρήσιμων υπηρεσιών που απαιτούνται για να λειτουργήσει ένα ασφαλές δίκτυο πληρωμών. Η εξόρυξη θα απαιτείται ακόμα και μετά την έκδοση του τελευταίου bitcoin.

2.4.2 Η λειτουργία της εξόρυξης

Ο καθένας μπορεί να γίνει εξορύκτης Bitcoin (miner) τρέχοντας το λογισμικό με εξειδικευμένο υλικό (hardware). Το λογισμικό εξόρυξης αφουγκράζεται τις μεταδόσεις συναλλαγών μέσω του δικτύου μεταξύ ομότιμων (peer-to-peer) και εκτελεί τις κατάλληλες εργασίες για να επεξεργαστεί και να επιβεβαιώσει τις συναλλαγές αυτές. Οι εξορύκτες Bitcoin εκτελούν αυτή την εργασία διότι μπορούν να κερδίσουν τέλη συναλλαγής που πληρώνονται από τους χρήστες για ταχύτερη επεξεργασία μιας συναλλαγής και πρόσφατα δημιουργηθέντα bitcoins που έλαβαν σάρκα και οστά σύμφωνα με μια σύνθετη φόρμουλα.

Για να επιβεβαιωθούν οι νέες συναλλαγές, αυτές πρέπει να συμπεριληφθούν σε ένα μπλοκ (block) μαζί με μια μαθηματική απόδειξη εργασίας. Δεν είναι εύκολο να παράγουμε τέτοιες αποδείξεις διότι δεν υπάρχει κανένας τρόπος δημιουργίας τους παρά μόνο δοκιμάζοντας δισεκατομμύρια υπολογισμούς το δευτερόλεπτο. Αυτό απαιτεί οι εξορύκτες να εκτελούν αυτούς τους υπολογισμούς πριν τα μπλοκ (blocks) γίνουν αποδεκτά από το δίκτυο και πριν αυτοί λάβουν μια αμοιβή. Όσο περισσότεροι χρήστες συμμετέχουν στην εξόρυξη, η δυσκολία εξεύρεσης έγκυρων μπλοκ αυξάνεται αυτόματα από το δίκτυο για να διασφαλίσει ότι ο μέσος χρόνος για να βρεθεί ένα μπλοκ παραμένει ίσος με 10 λεπτά. Αυτό έχει ως συνέπεια, η εξόρυξη γίνεται μια πολύ ανταγωνιστική επιχείρηση όπου κανένας ιδιώτης εξορύκτης δεν μπορεί να ελέγξει τι περιλαμβάνεται εντός της αλυσίδας των μπλοκ (block chain).

Η απόδειξη εργασίας είναι επίσης σχεδιασμένη να εξαρτάται από το προηγούμενο μπλοκ (block) για να επιβάλλει μια χρονολογική σειρά στην αλυσίδα των μπλοκ (block chain). Αυτό καθιστά εκθετικά δύσκολη την αντιστροφή των προηγούμενων συναλλαγών διότι απαιτεί επαναυπολογισμό των αποδείξεων εργασίας όλων των ακόλουθων μπλοκ (block). Όταν δύο μπλοκ βρίσκονται ταυτόχρονα, οι εξορύκτες εργάζονται πάνω στο πρώτο μπλοκ που λαμβάνουν και αλλάζουν σε μεγαλύτερες αλυσίδες των μπλοκ μόλις βρεθεί το επόμενο μπλοκ. Αυτό έχει ως αποτέλεσμα η εξόρυξη να είναι ασφαλής και να διατηρείται μια παγκόσμια γενική συναίνεση που βασίζεται στην επεξεργαστική ισχύ.

Οι εξορύκτες Bitcoin δεν είναι μπορούν ούτε να εξαπατήσουν αυξάνοντας την δική τους ανταμοιβή, ούτε να επεξεργαστούν δόλιες συναλλαγές οι οποίες θα μπορούσαν να αλλοιώσουν το δίκτυο του Bitcoin διότι όλοι οι κόμβοι Bitcoin θα απέρριπταν οποιοδήποτε μπλοκ (block) περιέχει άκυρα δεδομένα σύμφωνα με τους κανόνες του πρωτόκολλου του Bitcoin. Συνεπώς, το δίκτυο παραμένει ασφαλές ακόμα και αν όλοι οι εξορύκτες Bitcoin δεν είναι έμπιστοι.

2.4.3 Δαπάνη ενέργειας για εξόρυξη

Όπως και κάθε άλλη υπηρεσία πληρωμής, η χρήση του Bitcoin συνεπάγεται κόστη επεξεργασίας. Οι υπηρεσίες που είναι αναγκαίες για την λειτουργία των ευρύτατα διαδεδομένων τρεχόντων νομισματικών οικονομικών συστημάτων, όπως είναι οι τράπεζες, οι πιστωτικές κάρτες και τα θωρακισμένα οχήματα επίσης καταναλώνουν πολλή ενέργεια. Παρόλο που σε αντίθεση με το Bitcoin, η συνολική ενεργειακή τους κατανάλωση δεν είναι διαφανής και δεν μπορεί να μετρηθεί τόσο εύκολα.

Η εξόρυξη Bitcoin (mining) έχει σχεδιαστεί για να τελειοποιηθεί περισσότερο με την πάροδο του χρόνου με χρήση εξειδικευμένου υλικού (hardware) που καταναλώνει λιγότερη ενέργεια και τα λειτουργικά κόστη εξόρυξης θα πρέπει να συνεχίσουν να είναι αναλογικά με την ζήτηση. Όταν η εξόρυξη Bitcoin γίνει πολύ ανταγωνιστική και λιγότερο επικερδής, μερικοί εξορύκτες επιλέγουν να τερματίσουν τις δραστηριότητές τους. Επιπροσθέτως, όλη η ενέργεια που δαπανάται για την εξόρυξη, τελικά μετασχηματίζεται σε θερμότητα και οι πιο κερδοφόροι εξορύκτες θα είναι εκείνοι που αξιοποιούν αυτή τη θερμότητα για καλή χρήση. Ένα βέλτιστο αποδοτικό δίκτυο εξόρυξης είναι αυτό που δεν καταναλώνει στην πραγματικότητα επιπλέον ενέργεια. Ενώ αυτό είναι το ιδανικό, τα οικονομικά της εξόρυξης είναι τέτοια που οι εξορύκτες σε ατομικό επίπεδο υπερβάλλουν εαυτόν προς αυτή την κατεύθυνση.

2.4.4 Συνάφεια μεταξύ εξόρυξης και ασφάλειας

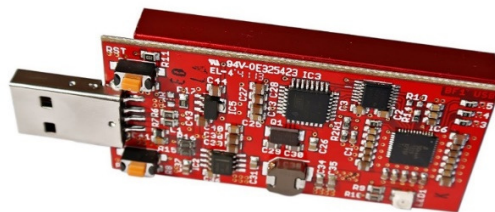
Η εξόρυξη (mining) δημιουργεί το ισοδύναμο μιας ανταγωνιστικής λοταρίας η οποία καθιστά δύσκολο για τον καθένα να προσθέτει διαδοχικά νέα μπλοκ σε μια αλυσίδα των μπλοκ (block chain). Αυτό προστατεύει την ουδετερότητα του δικτύου αποτρέποντας οποιοδήποτε άτομο από το να αποκτήσει εξουσία για να μπλοκάρει συγκεκριμένες συναλλαγές. Αυτό επίσης αποτρέπει οποιοδήποτε άτομο από το να αντικαταστήσει τμήματα της αλυσίδας των μπλοκ (block chain) ώστε να μειώσουν τις δικές τους δαπάνες πράγμα το οποίο θα μπορούσε να χρησιμοποιηθεί στην εξαπάτηση άλλων χρηστών. Η εξόρυξη καθιστά εκθετικά πιο δύσκολο να αντιστραφεί μια προηγούμενη συναλλαγή αφού απαιτείται η επανεγγραφή όλων των μπλοκ (blocks) που ακολουθούν την συναλλαγή αυτή.

Μη ρυθμιζόμενα ψηφιακά νομίσματα

2.4.5 Υλικό και Λογισμικό που χρησιμοποιείται για την εξόρυξη

Κατά τις πρώτες ημέρες του Bitcoin, ο καθένας μπορούσε να βρει ένα καινούριο μπλοκ (block) χρησιμοποιώντας την κεντρική μονάδα επεξεργασίας (CPU) του υπολογιστή του. Καθώς όλο και περισσότεροι άνθρωποι ξεκίνησαν εξόρυξη, η δυσκολία εξεύρεσης νέων μπλοκ αυξήθηκε κατά πολύ στο σημείο που η μόνη αποδοτική από πλευράς κόστους μέθοδος σήμερα είναι η χρήση εξειδικευμένου υλικού (hardware).

Όπως αναφέραμε και νωρίτερα αρχικά η εξόρυξη πραγματοποιούνταν σε επεξεργαστές προσωπικών υπολογιστών, όμως δεν επαρκούσε η απόδοση τους. Στη συνέχεια χρησιμοποιήθηκε η GPU, επεξεργαστική μονάδα γραφικών, η οποία ήταν πολύ πιο αποδοτική, 50 με 100 φορές πιο γρήγορη από την CPU. Κατά τη διάρκεια του 2011, δημιουργήθηκε εξειδικευμένο υλικό για την εξόρυξη το οποίο αύξησε ακόμα περισσότερο την απόδοση της εξόρυξης. Η πρώτη γενιά τέτοιων εξειδικευμένων συσκευών ήταν FPGAs (Field-Programmable Gate Arrays) επεξεργαστές οι οποίοι εφαρμόζονταν σε υπολογιστές με USB σύνδεση. Με τη χρήση των FPGAs εκτός από καλύτερη απόδοση, καταφέραμε να μειώσουμε την ενέργεια που καταναλώνεται.



Εικόνα 2.6: Εξειδικευμένο FPGA για την εξόρυξη Bitcoin.

Σήμερα μιλάμε για ASIC Application-specific integrated circuit εξορύκτες, οι οποίοι έχουν λάβει ενεργό ρόλο στην εξόρυξη. Αυτά τα κυκλώματα πραγματοποιούν εξόρυξη με πολύ μεγαλύτερη απόδοση και με το μικρότερη δυνατή κατανάλωση. Πολλές εταιρείες έχουν κάνει την είσοδό τους στην εξόρυξη bitcoin.

Μη ρυθμιζόμενα ψηφιακά νομίσματα



Εικόνα 2.7: ASIC εξορύκτης bitcoin.

2.4.6 Εξόρυξη με cloud

Εκτός λοιπόν από τις μεθόδους εξόρυξης που έχουμε αναφέρει και νωρίτερα, η εξόρυξη με cloud αποτελεί μια εναλλακτική λύση για όποιον χρήστη δεν επιθυμεί να επενδύσει σε υλικό για τη διαδικασία της εξόρυξης. Το cloud mining επιτυγχάνεται με το διαμοιρασμό υπολογιστικής ισχύος από απομακρυσμένα κέντρα, τα οποία συμβάλλουν στην εξόρυξη. Προφανώς βέβαια, αν και φαίνεται ως μια πολύ καλή λύση για τους χρήστες, εμπεριέχει και πολλά ρίσκα.

Θα ξεκινήσουμε αναφέροντας τα πλεονεκτήματα του cloud mining. Δεν απαιτείται από μέρους του χρήστη καμία εμπλοκή του με υπολογιστή όσον αφορά την εξόρυξη. Επίσης, δεν χρειάζεται να αγοράσει κανείς επιπλέον υλικό για να πραγματοποιήσει την εξόρυξη. Ένα επίσης σοβαρό πρόβλημα που αντιμετωπίζουν οι χρήστες οι οποίοι αποφασίζουν να πραγματοποιήσουν εξόρυξη στο σπίτι, είναι ότι απαιτείται ένα αρκετά ισχυρό σύστημα ψύξης για το σύστημα που πραγματοποιεί την εξόρυξη. Είτε χρησιμοποιείτε server είτε χρησιμοποιείτε ένα εξειδικευμένο FPGA. Άρα, με υλοποίηση της εξόρυξης μέσω cloud, μειώνεται σε μεγάλο βαθμό το κόστος που προκύπτει από την κατανάλωση ρεύματος, είτε η εξόρυξη πραγματοποιείται στο σπίτι, είτε σε επαγγελματικό χώρο του χρήστη. Ακόμη, ο χρήστης δεν χρειάζεται να προβληματίζεται για το πώς θα διαχειριστεί το υλικό που τυχόν έχει αγοράσει, όταν η εξόρυξη δεν είναι πλέον αποδοτική.

Βέβαια, όπως είναι φυσικό υπάρχουν και μειονεκτήματα δεδομένου ότι παρεμβάλλονται στη διαδικασία και τρίτοι παράγοντες. Το πρώτο και ίσως από τα σημαντικότερα μειονεκτήματα, είναι ότι το κέρδος δεν είναι το ίδιο καθώς οι διαχειριστές του cloud, χρειάζονται κάποια αμοιβή. Δεν μπορεί ο χρήστης να έχει την ίδια ευελιξία και τον έλεγχο σε

Μη ρυθμιζόμενα ψηφιακά νομίσματα

σχέση με την υλοποίηση της εξόρυξης σε πρώτο επίπεδο από τον ίδιο. Σε ένα άλλο επίπεδο δίνεται η δυνατότητα σε ένα ενδιαμέσο χρήστη να πραγματοποιήσει κακοβουλίες. Επίσης, τα επίπεδα της διαφάνειας δεν μπορούν να αλλοιωθούν. Τέλος, όσον αφορά τους εξαρτημένους από τον υπολογιστές δεν θα έχουν τη χαρά να ζήσουν την εξόρυξη σε όλο της το μεγαλείο. [15]

Στη συνέχεια θα αναφέρουμε και θα αναλύσουμε τους διάφορους τύπους εξόρυξης μέσω cloud.

2.4.6.1 Τύποι εξόρυξης μέσω cloud

Σε γενικές γραμμές υπάρχουν τρεις τύποι εξόρυξης μέσω cloud, οι οποίοι είναι και διαθέσιμοι, έως σήμερα βέβαια που υλοποιείται η συγγραφή αυτής της διπλωματικής εργασίας.

- **Εξόρυξη μέσω Hosted:** Ουσιαστικά μιλάμε για την ενοικίαση μιας μηχανής εξόρυξης η οποία διαχειρίζεται από τον πάροχο.
- **Εικονική διαχείριση της εξόρυξης:** Ο χρήστης δημιουργεί μια εικονική μηχανή και στη συνέχεια εγκαθιστά λογισμικό το οποίο πραγματοποιεί το mining.
- **Ενοικίαση hashing ισχύος:** Αποτελεί την πιο διαδεδομένη μέθοδο και ουσιαστικά ο χρήστης νοικιάζει hashing ισχύ χωρίς να υπάρχει κάποια εικονική μηχανή ή κάποιο υπολογιστικό σύστημα.

Βέβαια, θα πρέπει να αναφέρουμε και μια αναλυτική αναφορά του κέρδους το οποίο προσφέρει αυτή η μέθοδος. Οι διαδικτυακές υπηρεσίες που προσφέρονται στο χρήστη, αναφέρονται σε κέρδος το οποίο αποδίδεται, υλοποιώντας ο χρήστης την εξόρυξη μόνος του, είτε μέσω χρήσης υλικού ειδικού σκοπού, είτε μέσω λογισμικού για αυτόν τον σκοπό. Στην απόδοση κερδών δεν αναφέρονται περιπτώσεις εξόρυξης μέσω cloud, και όπως είναι φυσικό οι εμπλεκόμενοι καθορίζουν πολλές φορές τα ποσοστά απόδοσης.



Εικόνα 2.8: Ηλεκτρονικές «αριθμομηχανές».

Οι ηλεκτρονικές αυτές «αριθμομηχανές» σας δίνουν παρ' όλα αυτά τη δυνατότητα να κάνετε μερικούς βασικούς υπολογισμούς. Κάποιες από τις συχνά ζητούμενες πληροφορίες είναι η αναφορά του κόστους του ρεύματος για την εξόρυξη, καθώς επίσης και το κόστος που απαιτείτε για την αγορά εξειδικευμένου υλικού.

Ακόμη σας ζητείτε να δώσετε πληροφορίες για τρέχοντα κόστη ή και για επενδύσεις που έχουν γίνει κατά τη διάρκεια της εξόρυξης. Βέβαια, δεδομένου ότι, στην περίπτωση της εξόρυξης μέσω cloud, δεν πληρώνει ο χρήστης το κόστος ισχύος, μπορεί να χρησιμοποιηθεί το κόστος ενοικίου για αυτό το πεδίο.

Σε περίπτωση που δεν έχετε ακόμα αποφασίσει τον τρόπο με τον οποίο θέλετε να πραγματοποιήσετε την εξόρυξη, μπορείτε να συγκρίνετε, από διάφορες αναφορές που είναι διαθέσιμες στο διαδίκτυο, αυτήν που εσείς θεωρείτε πιο επικερδή.

Το θέμα του κέρδους είναι πολύ σημαντικό, αλλά εκτός αυτού έχουμε και πολλά άλλα θέματα τα οποία θα πρέπει να αναλύσουμε πριν αποφασίσετε τη μέθοδο την οποία θα ακολουθήσετε για την εξόρυξη.

2.4.6.2 Ρίσκα και Ανταμοιβή

Το bitcoin ανήκει στην κατηγορία της κρύπτο-οικονομίας, [16]οπότε η εξόρυξη κρύβει πολλούς κινδύνους και ρίσκα. Στη συνέχεια θα αναφέρουμε μερικά βασικά σημεία κλειδιά τα οποία θα σας βοηθήσουν να αποφασίσετε με ποιον τρόπο θα υλοποιήσετε την εξόρυξη.

Κάνοντας τους υπολογισμούς θα παρατηρήσετε ότι η εξόρυξη μέσω cloud μπορεί να σας αποφέρει κέρδη για τους πρώτους μήνες αλλά στη συνέχεια θα έχετε απώλειες όσο η εξόρυξη έχει μεγαλύτερες απαιτήσεις τόσο το κέρδος μειώνετε. Ένας τρόπος για να μειώσετε την απώλεια, είναι να επενδύσετε εκ νέου τα κέρδη ώστε να αυξήσετε τον ρυθμό του hashing. Όπως καταλαβαίνετε αυτό είναι αρκετά ριψοκίνδυνο.

Μη ρυθμιζόμενα ψηφιακά νομίσματα

Όπως αναφέραμε και νωρίτερα, το ρίσκο της απάτης και της κακής διαχείρισης είναι υψηλό στην εξόρυξη μέσω cloud, για να μπορεί να επιτευχθεί ανταγωνιστικό ρυθμός εξόρυξης, αλλά μπορεί να αποφέρει υψηλά κέρδη.



Εικόνα 2.9: Ρίσκα και ανταμοιβή.

Οι χρήστες, λοιπόν, που σκοπεύουν να ασχοληθούν με την εξόρυξη μέσω cloud, θα πρέπει να γνωρίζουν τα ρίσκα και να είναι σε θέση να αναλάβουν την ευθύνη σε περίπτωση αποτυχίας, και φυσικά να μην επενδύει κανείς περισσότερα από όσο είναι διαθέσιμος να χάσει.

Κεφάλαιο 3ο

3.1 Πισίνες Εξόρυξης - Mining Pools

Οι δυσκολίες όσον αφορά την εξόρυξη έγιναν αισθητές από το 2014. Σε αυτό συνέβαλε η άφιξη στις εργασίες της εξόρυξης εξειδικευμένων συσκευών, ASIC, με αποτέλεσμα να παραγκωνιστεί εντελώς η παραγωγή Bitcoin από προσωπικούς ηλεκτρονικούς υπολογιστές, οι οποίοι ούτως ή άλλως κατανάλωναν πολύ περισσότερη ενέργεια με πολύ χαμηλότερη παραγωγικότητα.



Εικόνα 3.1: Bitcoin Miner.

Η εξόρυξη λειτουργεί με δύο διαφορετικούς τρόπους. Οι εξορύκτες μπορούν να λειτουργούν είτε ως ομάδα, είτε ο καθένας μεμονωμένα για την ανακάλυψη ενός block. Σε περίπτωση συνεργασίας, θα πρέπει φυσικά η διαδικασία να ακολουθεί εγκεκριμένο προγραμματισμό και να είναι συντονισμένοι οι συνεργασία. Η συνεργασία κατά την εξόρυξη είναι συνήθης πρακτική καθώς η εξόρυξη είναι μια πολύ απαιτητική και χρονοβόρα διαδικασία. Το αποτέλεσμα της εξόρυξης μοιράζεται σε όσους έλαβαν μέρος στην εξόρυξη και ο καθένας λαμβάνει το ανάλογο της προσπάθειας που κατέβαλλε.

3.1.1 Διαδοσμένες πισίνες εξόρυξης

Οι πιο διαδοσμένες mining pools που χρησιμοποιούνται σήμερα αναφέρονται παρακάτω και δίνουμε κάποια στοιχεία για την καθεμία περίπτωση.

DeepBit: [17] Είναι μία «πισίνα» η οποία αποτελεί πλέον παρελθόν με τελευταία καταγραφή σε επίπεδο εξόρυξης το 2013. Η τελευταία αναφορά που έχουμε από τον χρήστη και ιδρυτή της πλατφόρμας είναι το 2014. Αποτελούσε μια από τις πιο σημαντικές πλατφόρμες εξόρυξης με ποσοστά έως και 50% στην παγκόσμια αγορά και εγγυόταν άμεση πληρωμή των



Εικόνα 3.2 Λογότυπο της DeepBit.

Μη ρυθμιζόμενα ψηφιακά νομίσματα

συμμετεχόντων. Ενώ ανακοινώθηκε από την εταιρεία η πρόθεση για χρήση ASIC τεχνολογίας, το πρότζεκτ τελικά ακυρώθηκε χωρίς επιπλέον πληροφόρηση για τις αιτίες.

BitcoinCZ: [18] Αποτελεί μια ενεργή πλατφόρμα εξόρυξης με servers στην Αμερική, την Ευρώπη και την Ασία. Έγινε, αρχικά, γνωστή με την ονομασία slush. Έχει στο ενεργητικό της πολλές διακρίσεις και οι χρήστες της αυξάνονται



Εικόνα 3.3: Λογότυπο της BitcoinCZ.

καθημερινά. Εγγυάται στους χρήστες της υψηλού επιπέδου υπηρεσίες και γρήγορες πληρωμές.

OzCoin: [19] Είναι μία ενεργή πλατφόρμα όπως και η προηγούμενη, με διαρκώς εξελισσόμενη τεχνολογία και αναβαθμίσεις. Υπόσχεται στους χρήστες της χαμηλής διακύμανσης εξόρυξη, αυστηρή αναλογία στη διαμοίραση των ποσών με σταθερό μέγεθος πισίνας και τη μέθοδο διπλών γεωμετρικών μεταβλητών.



Εικόνα 3.4 Λογότυπο της OzCoin.

EclipseMC: [20] Αποτελεί μια εκλεκτική πλατφόρμα η οποία είναι σχεδιασμένη για τα βέλτιστα αποτελέσματα. Διαθέτει servers σε Ευρώπη και Αμερική.



Εικόνα 3.5 Λογότυπο της EclipseMC.

BitMinter: [21] Είναι μια από τις παλιές πλατφόρμες στο χώρο της εξόρυξης αφού λειτουργεί από το 2011 και διαθέτει χρήστες από την έναρξή της.



Εικόνα 3.6: Λογότυπο της BitMinter.

Μη ρυθμιζόμενα ψηφιακά νομίσματα

P2Pool: [22] Λειτουργεί και αυτή από 2011 και εγγυάται στους χρήστες της διασφάλιση των προσωπικών τους στοιχείων κατά τις συναλλαγές τους.



Εικόνα 3.7: Λογότυπο της P2Pool.

3.1.2 Συμβουλές για αρχάριους

Η εξόρυξη Bitcoin αποτελεί μια νέα και πολλά υποσχόμενη διαδικασία για μελλοντικούς χρήστες. Θα πρέπει όμως να έχετε υπόψη σας ορισμένα πράγματα πριν αποφασίσετε να ασχοληθείτε με την εξόρυξη Bitcoin. Θα πρέπει να ενημερωθεί κανείς για τη διαδικασία της εξόρυξης ώστε να επιβεβαιώσει ότι τον ενδιαφέρει πραγματικά να ασχοληθεί και όχι επειδή αποτελεί μια δημοφιλή και μοντέρνα ενασχόληση.

3.1.3 Μέθοδοι διαμοιρασμού νομισμάτων

Οι τρόποι με τους οποίους οι πλατφόρμες εξόρυξης πραγματοποιούν το διαμοιρασμό των νομισμάτων ποικίλουν και βασίζονται στη τρόπο με τον οποίο δημιουργείται ένα μπλοκ, με βάση τους συμμετέχοντες στη δημιουργία του. Οι πιο διαδεδομένοι παρουσιάζονται παρακάτω και ακολουθεί μια σύντομη περιγραφή για καθέναν από αυτούς. [9] [23]

PPS – Pay per share: Αποτελεί τον πιο κοινό τρόπο υπολογισμού του διαμοιρασμού. Κάθε χρήστης που έχει συμμετάσχει στην εξόρυξη ανταμείβεται με συγκεκριμένο αριθμό νομισμάτων, συνήθως της τάξης λίγων χιλιοστών του Bitcoin.

SMPPS – Shared Maximum Pay Per Share: Ακολουθεί την ίδια λογική με το PPS αλλά σε αυτήν την περίπτωση η πλατφόρμα εξόρυξης δεν αποδίδει ποτέ παραπάνω νομίσματα από αυτά που εξορύχθηκαν.

ESMPPS – Equalized Shared Maximum Pay Per Share: Ακολουθεί την ίδια λογική με SMPPS αλλά με πιο δίκαιη λογική.

Μη ρυθμιζόμενα ψηφιακά νομίσματα

RSMPPS – Recent Shared Maximum Pay Per Share: Έχει την ίδια λογική με το SMPPS, αλλά δίνεται προτεραιότητα πληρωμής στους «εξορύκτες» που έχουν εισέλθει στο σύστημα πιο πρόσφατα.

CPPSRB – Capped Pay Per Share with Recent Backpay: Ίδια περίπτωση με το PPS αλλά διαθέτει όριο το οποίο υπολογίζεται από τις πρόσφατες αναδρομικές αποδοχές της πλατφόρμας.

Score: Η αμοιβή στους χρήστες πραγματοποιείται με βάση το score τους. Κάθε πρόσφατο μερίδιο έχει μεγαλύτερο σκορ από κάποιο παλαιότερο. Όσο παλαιότερο είναι το μερίδιο τόσο μικρότερο το σκορ του. Χρησιμοποιώντας αυτό το σύστημα, ένας χρήστης που θα σταματήσει την εξόρυξη στην πλατφόρμα, το score του θα πέσει πολύ γρήγορα και παράλληλα και η αμοιβή του.

PPLNS – Pay Per Last N Shares: Το ποσό των νομισμάτων υπολογίζεται, σε αυτήν την περίπτωση, με βάση τα N μερίδια, στα οποία συνεισφέρει ο χρήστης. Δεν είναι απαραίτητο ο εξορύκτης να συνεισφέρει σε ένα μόνο μπλοκ. Με αυτόν τον τρόπο αποφεύγουμε το φαινόμενο του pool hopping κατά το οποίο κάποιοι εξορύκτες εξορύσσουν με στρατηγική σε διάφορες «πισίνες», με απώτερο σκοπό να αυξήσουν το εισόδημα τους, σε βάρος άλλων εξορυκτών.

Prop: Μόλις βρεθεί το μπλοκ όλοι αμείβονται ανάλογα με τα πόσα μερίδια έχει συνεισφέρει ο καθένας.

DGM - Double Geometric Method. Θα μπορούσε να χαρακτηριστεί ως ένα υβρίδιο μεταξύ της PPLNS και της μεθόδου Γεωμετρικής ανταμοιβής. Ο χρήστης λαμβάνει ένα τμήμα των απολαβών ανά τακτά χρονικά διαστήματα και το επιστρέφει αργότερα ώστε να ομαλοποιηθούν οι πληρωμές.

Σε περίπτωση που κάποιος χρήστης ξεκινά την εξόρυξη για πρώτη φορά είναι πολύ πιο εύκολο να ξεκινήσει από μια PPS πισίνα, στην οποία θα έχει συγκεκριμένες απολαβές, ανάλογες του μεριδίου που παρέχει. Οι ήδη εξοικειωμένοι χρήστες μπορούν να αποφασίσουν μελετώντας και τις υπόλοιπες περιπτώσεις πριν αποφασίσουν το είδος.

Μη ρυθμιζόμενα ψηφιακά νομίσματα

Pool Είδος πλατφόρμας	PPS	SMPP S	ESMPP S	RSMPP S	CPPSR B	Score	PPLN S	Prop	DGM
DeepBit	X							X	
Slush						X			
OzCoin	X								X
EclipseMC	X								X
BitMinter							X		
P2Pool							X		

Πίνακας 3.1: Οι μέθοδοι που χρησιμοποιούνται από τις "πισίνες" εξόρυξης.

3.2 Ανταλλακτήρια Bitcoin

3.2.1 Λειτουργία των ανταλλακτηρίων

Τα ανταλλακτήρια Bitcoin επιτελούν ακριβώς την ίδια διαδικασία με τα ανταλλακτήρια νομισμάτων όπως τα ξέραμε μέχρι σήμερα. Μετατρέπουν τα συμβατικά χρήματα, δολάρια, ευρώ, σε ηλεκτρονικά νομίσματα, Bitcoin, Ietcoin κ.α.. Αρχικά θα πρέπει να δημιουργήσουμε έναν προσωπικό λογαριασμό και στη συνέχεια να πιστώσουμε ένα ποσό, συμβατικού νομίσματος, σε αυτόν, μέσω τραπεζικής συναλλαγής. Με τα χρήματα αυτά μπορούμε σι συνέχεια να αγοράσουμε Bitcoins. Στη συνέχεια μπορούμε να διαχειριστούμε τα Bitcoins με οποίο τρόπο επιθυμεί ο κάθε χρήστης.

Ανάλογη λογική πραγματοποιείται και κατά την αντίθετη διαδικασία, τη μετατροπή δηλαδή του ψηφιακού νομίσματος σε κάποιο συμβατικό νόμισμα. Θα πρέπει αρχικά τα Bitcoin να αποσταλούν στο ανταλλακτήριο και να πιστωθούν στο λογαριασμό του χρήστη. Στη συνέχεια μπορούμε να τα πουλήσουμε και να πιστωθεί στο λογαριασμό μας το ανάλογο ποσό. Τέλος, τα χρήματα μεταφέρονται στον τραπεζικό λογαριασμό.

Στη συνέχεια αυτού του κεφαλαίου θα αναφέρουμε μερικά γνωστά ανταλλακτήρια και θα δώσουμε βασικές πληροφορίες για καθένα από αυτά.

3.2.2 Γνωστά Ανταλλακτήρια

Τα πιο διαδεδομένα ανταλλακτήρια στα οποία οι χρήστες μπορούν να αγοράσουν ή να πωλήσουν Bitcoin παρουσιάζονται στην παρακάτω λίστα:



Εικόνα 3.8: Λογότυπο της BTCGreece.

Το **BTCGreece** [24] είναι το πρώτο ελληνικό ανταλλακτήριο, το οποίο συνεργάζεται με ελληνικές τράπεζες. Οι ανταλλαγές μικρών ποσών μπορούν να πραγματοποιηθούν με διατήρηση της ανωνυμίας του χρήστη, κάτι το οποίο δεν ισχύει για μεγαλύτερα ποσά.

Το **Bitcoin Central** είναι ένα ανταλλακτήριο στο οποίο μπορούν να πραγματοποιηθούν συναλλαγές από και προς ευρώ. Σε αντίθεση με το προηγούμενο, για να γίνει χρήση των υπηρεσιών του απαιτούνται δικαιολογητικά ταυτοπροσωπίας, όπως η ταυτότητα του χρήστη, αλλά και τα στοιχεία του λογαριασμού που θα συμμετάσχει στη διαδικασία ανταλλαγής.

Ένα ακόμη γνωστό ανταλλακτήριο είναι το Bitcoin.de, το οποίο επιτρέπει απευθείας αγοροπωλησίες, διασφαλίζοντας τις συναλλαγές μεταξύ των χρηστών. Για την χρήση των υπηρεσιών της η εταιρεία έχει χρέωση 1% επί της συναλλαγής. Το ποσό αυτό καταβάλλεται ισομερώς τόσο από τον αγοραστή όσο και από τον πωλητή. Υποστηρίζει Liberty Reserve και Τραπεζικές συναλλαγές.



Εικόνα 3.9: Λογότυπο της BitStamp.

Τέλος, το **BitStamp** [25], είναι ένα πιο «δίκαιο» ανταλλακτήριο αφού πραγματοποιεί χρεώσεις ανάλογες του όγκου των μηνιαίων συναλλαγών που πραγματοποιεί ο χρήστης. Για

Μη ρυθμιζόμενα ψηφιακά νομίσματα

μηνιαίες συναλλαγές έως 500 δολάρια, η χρέωση είναι 0,5%, ενώ για μηνιαίες συναλλαγές που υπερβαίνουν τις 150.000 δολάρια η χρέωση είναι 0,2%.



Εικόνα 3.9: Λογότυπο της Kraken.

Το **Kraken** [26] είναι ένα πιο ευέλικτο ανταλλακτήριο αφού επιτρέπει συναλλαγές με περισσότερα χαρακτηριστικά. Παρέχει δυνατότητα για εντολές Market, Limit, Stop limit, Take profit, Stop loss, Take profit limit, κ.α. Ανταλλάσσει μεταξύ Ευρώ, Δολάριο, Bitcoin, Litecoin, Dogecoin, Ripple και Namecoin.

Θα αναφέρουμε τέλος το Intersango, το οποίο είναι πλέον ένα ανενεργό ανταλλακτήριο. Υποστήριζε συναλλαγές με ευρώ, δολάρια, λίρες Αγγλίας κ.α.. Οι συναλλαγές πραγματοποιούνταν μέσω κατάθεσης σε τραπεζικό λογαριασμό. Οι χρεώσεις γίνονταν ως εξής: 0,35% για τον εξορύκτη και 0,95% για τον αγοραστή. • Το συγκεκριμένο ανταλλακτήριο δεν δέχεται πλέον νέες εγγραφές.

3.2.3 Εναλλακτικοί τρόποι ανταλλαγής

Μια ακόμη πολύ χρήσιμη υπηρεσία που επιτρέπει στους υποψήφιους αγοραστές την αγορά Bitcoin είναι η GetBitcoin. Με χρήση αυτής της υπηρεσίας η διαδικασία της συναλλαγής μπορεί να γίνει πιο εύκολη, ανάλογα με τον τρόπο που θα επιλέξει κάποιος να πραγματοποιήσει την ανταλλαγή, με χρήση, για παράδειγμα, Linden Dollars, κουπόνια ή Moneygram. Αν ο χρήστης επιθυμεί να πραγματοποιήσει τη συναλλαγή με μετρητά μπορεί να το κάνει μέσω της υπηρεσίας LocalBitcoins.

3.2.4 Κίνδυνοι και Προφυλάξεις

Όπως συμβαίνει στις καθημερινές συναλλαγές μας, έτσι και κατά τις συναλλαγές με Bitcoin, υπάρχει έλεγχος των στοιχείων των χρηστών. Αν μπορούμε στην διαδικασία εξόρυξης Bitcoin και στη συνέχεια αποφασίσουμε να τα ανταλλάξουμε με συμβατικά χρήματα, τότε θα

Μη ρυθμιζόμενα ψηφιακά νομίσματα

κληθούμε να αποδείξουμε με ποιο τρόπο έγινε η εκροή του ποσού αυτού, το γνωστό σε όλους μας, πόθεν έσχες.

Ένα ακόμα στοιχείο που πολλοί από τους αρχάριους στη διαδικασία της εξόρυξης δεν γνωρίζουν, είναι πως οι τραπεζικές συναλλαγές μεταξύ της τράπεζας και του ανταλλακτηρίου δεν είναι άμεσες. Υπάρχει πιθανότητα να διαρκέσουν ακόμα και κάποιες μέρες. Ένα επίσης ιδιαίτερο σημείο, άξιον προσοχής, είναι η μέθοδος με την οποία θα επιλέξουν οι χρήστες αφού κάποιες έχουν υψηλή χρέωση.

Μετά από την αλλαγή της νομοθεσίας, η οποία πολλές φορές δυστυχώς ακολουθεί των εξελίξεων, τα περισσότερα ανταλλακτήρια πλέον πραγματοποιούν ταυτοποίηση των στοιχείων των χρηστών τους. Για να μπορέσουν οι χρήστες πολλές φορές να πραγματοποιούν συναλλαγές χωρίς κάποιο ανώτατο όριο συναλλαγών, θα πρέπει να γίνει πιστοποίηση των στοιχείων των χρηστών αποστέλλοντας στο ανταλλακτήριο ηλεκτρονικά στοιχεία ταυτοποίησης, όπως αντίγραφο της ταυτότητας ή του διαβατηρίου τους. Σε πιο εξειδικευμένες περιπτώσεις απαιτείται και αντίγραφο λογαριασμού κοινής ωφέλειας για την ενίσχυση της ταυτοποίησης τους. Τέλος, για να γίνει οποιαδήποτε συναλλαγή μεταξύ του ανταλλακτηρίου και του τραπεζικού λογαριασμού, θα πρέπει τα στοιχεία του χρήστη να αναφέρονται και στον τραπεζικό λογαριασμό. Σε διαφορετική περίπτωση ενδέχεται να υπάρξουν προβλήματα κατά την καταβολή των ποσών. [27] [28]

3.2.5 Ανταλλακτήρια κρυπτονομισμάτων

Όπως είναι γνωστό εκτός από το Bitcoin σήμερα κυκλοφορούν και πολλά άλλα νομίσματα τα οποία βασίζονται στην κρυπτογραφία, όπως το Bitcoin. Βασίζονται και αυτά στην ίδια λογική, όπως περιγράψαμε και στο πρώτο κεφάλαιο, δεν έχουν υλική υπόσταση, είναι ψηφιακά, παράγονται με χρήση blockchain κτλ.. Η διαφορά τους είναι στην εξειδικευμένη παραμετροποίηση καθενός από αυτά, τη συχνότητα εξόρυξης κάθε μπλοκ, την ποσότητα των νομισμάτων που έχει κάθε μπλοκ, πόσα νομίσματα κυκλοφορούν στην αφορά κ.α.. Για να πραγματοποιήσει κάποιος ανταλλαγή Bitcoin με κάποιο άλλο κρυπτονόμισμα θα πρέπει λοιπόν να απευθυνθεί στα ανταλλακτήρια κρυπτονομισμάτων.

3.3 Φύλαξη bitcoins εκτός-δικτύου

Ένα σοβαρό θέμα που καλούνται να αντιμετωπίσουν οι χρήστες Bitcoin είναι οι ασφαλής φύλαξη των κρυπτονομισμάτων τους. Είναι περισσότερο επιθυμητό τα Bitcoins να αποθηκεύονται εκτός υπολογιστή ώστε να μειωθεί ο κίνδυνος απώλειας από ιούς ή σφάλματα που μπορεί να προκύψουν τόσο στο υλικό όσο και στο λογισμικό του υπολογιστή. Προφανώς, οι χρήστες αναζητούν λύσεις ώστε να αποφύγουν την απώλεια των χρημάτων τους.

3.3.1 Εταιρείες Φύλαξης Bicoins

Μια εταιρεία η οποία ασχολείται με τη φύλαξη πολύτιμων λίθων είναι η GoldMoney Group, η οποία εδρεύει στη Βρετανία, αποφάσισε και προχώρησε στην ίδρυση του Natagio. Το Natagio είναι μια θυγατρική της εταιρεία η οποία προσφέρει στους πελάτες της αποθήκευση των Bicoins τους εκτός δικτύου, με προσωπικό κλειδί διεύθυνσης. Το κλειδί του κάθε χρήστη κρυπτογραφείται και αποθηκεύεται σε συσκευές αποθήκευσης οι οποίες τοποθετούνται σε ασφαλή χρηματοκιβώτια. Η επιτυχία GoldMoney Group η οποία οφείλεται στην εμπιστοσύνη των πελατών της περνά σήμερα πλέον σε άλλα επίπεδα.

Το μεγαλύτερο κέρδος σε κύρος της εταιρείας είναι η δυνατότητα αποθήκευσης των Bitcoins εκτός δικτύου, και φυσικά η πολυετείς της φήμη σε θέματα φύλαξης. Η εταιρεία επιπλέον δίνει στους πελάτες της τη δυνατότητα να έχουν απομακρυσμένη πρόσβαση στα Bitcoins, με χρήση, φυσικά, two-factor authentication. Η χρήση της υπηρεσίας αυτής δεν έχει επιπλέον χρέωση. [13]



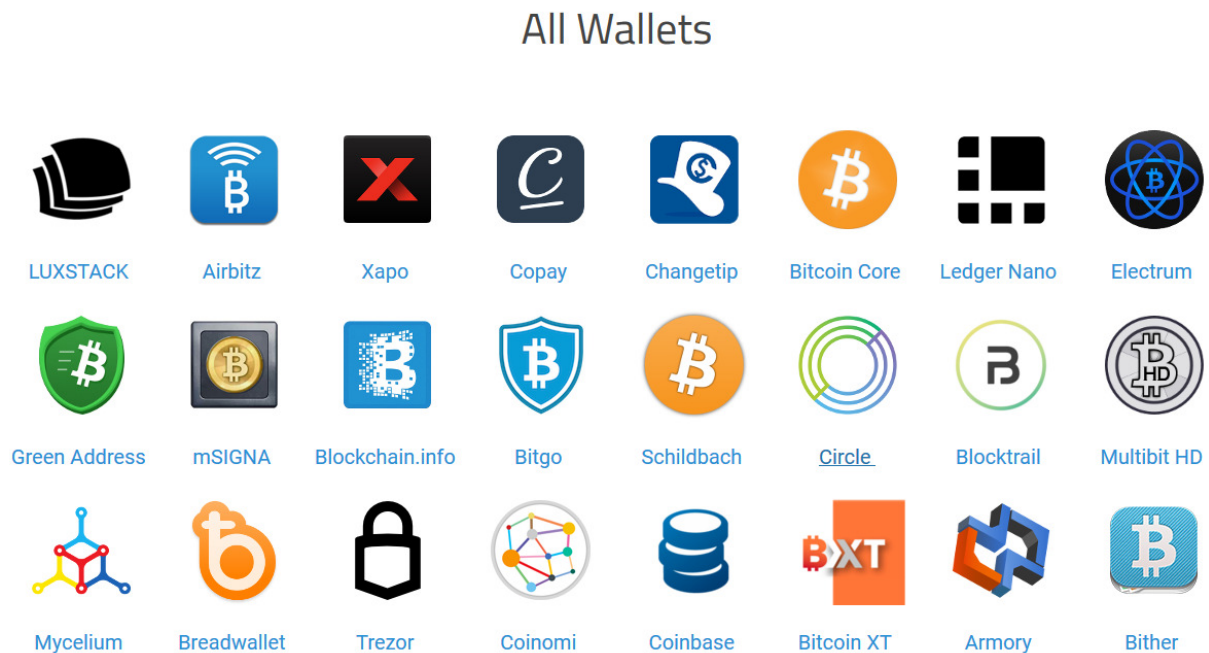
Εικόνα 3.10: Εκτός δικτύου αποθήκευση των bitcoins.

Μια ακόμη εταιρεία η οποία δίνει τη δυνατότητα φύλαξης Bitcoin εκτός δικτύου είναι η Elliptic Vault. Τα Bitcoins αποθηκεύονται σε κρυπτογραφημένα αρχεία, τα οποία αποθηκεύονται σε διασφαλισμένες τοποθεσίες. Το ιδιαίτερο και ταυτόχρονα αποκλειστικό της συγκεκριμένης υπηρεσίας είναι ότι η Lloyd's του Λονδίνου εγγυάται την αξία των αποθηκευμένων bitcoins. Προφανώς η παραπάνω υπηρεσία απαιτεί κάποια επιπλέον χρέωση, ανάλογα με το ποσό των bitcoins τα οποία θέλει να διασφαλίσει

3.3.2 Διασφαλίζοντας το πορτοφόλι σας

Όπως και στην πραγματική ζωή, το πορτοφόλι σας πρέπει να είναι ασφαλισμένο. Με το Bitcoin σας δίνετε η δυνατότητα να μεταφέρετε ποσά οπουδήποτε με πολύ εύκολο τρόπο και σας επιτρέπει να έχετε τον έλεγχο των χρημάτων σας. Τέτοιες σπουδαίες δυνατότητες συνήθως συνοδεύονται και από ανησυχίες όσον αφορά την ασφάλεια των μεταφορών. Ταυτόχρονα, το Bitcoin μπορεί να παρέχει πολύ υψηλά επίπεδα ασφάλειας αν χρησιμοποιείται σωστά. Να θυμάστε πάντα ότι είναι δική σας ευθύνη να υιοθετήσετε τις σωστές πρακτικές προκειμένου να προστατεύσετε τα χρήματά σας.

Μη ρυθμιζόμενα ψηφιακά νομίσματα



Εικόνα 3.11: Λογότυπα εταιριών Bitcoin πορτοφολιών.

3.3.3 Online υπηρεσίες

Οι υπηρεσίες φύλαξης εντός δικτύου μπορεί να αποτελούν μια καλή και αρκετά εύχρηστη επιλογή για τη φύλαξη των Bitcoin σας αλλά απαιτείται και από μέρος μεγάλη προσοχή κατά την χρήση τους. Τέτοια τέλεια χαρακτηριστικά όμως, συνοδεύονται επίσης από μεγάλες έγνοιες σχετικές με την ασφάλεια. Δυστυχώς στο παρελθόν έχουμε αρκετά παραδείγματα διαρροών ασφαλείας, οπότε απαιτείται επιφυλακτική στάση από μέρος σας. Οι υπηρεσίες φύλαξης εντός δικτύου δεν μπορούν να προσφέρουν στο χρήστη την ασφάλεια που παρέχετε από μια τράπεζα αποθήκευσης συμβατικού χρήματος. Αυτό μας οδηγεί στο συμπέρασμα ότι τα πορτοφόλια εντός δικτύου δεν αποτελούν τον καλύτερο τρόπο φύλαξης των Bitcoin και ο χρήστης θα ήταν καλύτερο να αναζητήσει διαφορετικούς τρόπους φύλαξης. Αλλά, αν επιλέξετε τελικά τα πορτοφόλια εντός δικτύου, μια καλή συμβουλή θα ήταν να γίνει χρήση ελέγχου δύο παραγόντων.

Σε γενικές γραμμές τα εντός δικτύου πορτοφόλια είναι αποτελούν μια έξυπνη λύση για τη φύλαξη μικρών ποσών. Όπως και στην καθημερινή μας ζωή θα επιλέγαμε ένα υλικό πορτοφόλι για τη μεταφορά, για παράδειγμα 500 ευρώ, με την ίδια λογική θα επιλέγαμε ένα

Μη ρυθμιζόμενα ψηφιακά νομίσματα

online πορτοφόλι για τα Bitcoins μας. Ποσά, δηλαδή που χρησιμοποιούνται για καθημερινές χρήσεις και η διασφάλιση των μεγαλύτερων ποσών μπορεί να γίνεται με άλλους τρόπους.

Τέλος, όπως θα παρουσιάσουμε και στη συνέχεια παρέχεται η δυνατότητα να κρατάτε αντίγραφα ασφαλείας για το πορτοφόλι σας ώστε να διασφαλίσετε τα ποσά σας. [29]

3.3.4 Αντίγραφα ασφαλείας

Μια συμβουλή που δίνεται από τους έμπειρους χρήστες είναι η δημιουργία ηλεκτρονικών αντιγράφων ασφαλείας για το πορτοφόλι σας. Μην ξεχνάμε ότι η δημιουργία αντιγράφων ασφαλείας, σε ευρύτερο επίπεδο είναι μια συνήθης τεχνική για τους έμπειρους χρήστες ηλεκτρονικών συσκευών, το γνωστό σε όλους μας backup. Αποθηκεύοντας τα αντίγραφα ασφαλείας, δίνεται η δυνατότητα να αποφύγουμε απώλειες που μπορεί να οφείλονται σε οποιαδήποτε βλάβη του υπολογιστή ή σε ανθρώπινα λάθη. Μια κλασική ιστορία που κυκλοφορεί στον κόσμο των χρηστών του Bitcoin είναι η περίπτωση ενός χρήστη ο οποίος έχασε ένα αρκετά μεγάλο ποσό για έκανε διαμόρφωση στο σκληρό δίσκο που αποθήκευε τα Bitcoins του.

Εκτός βέβαια, από προσωπικά σας λάθη η δημιουργία αντιγράφων ασφαλείας σας εξασφαλίζει σε περίπτωση κακόβουλων ενεργειών. Έχετε με αυτόν τον τρόπο τη δυνατότητα να ανακτήσετε το πορτοφόλι σας σε περίπτωση που κλαπεί ο υπολογιστής σας ή το κινητό σας τηλέφωνο, με την προϋπόθεση βέβαια το πορτοφόλι σας να είναι κρυπτογραφημένο.

3.3.4.1 Αντίγραφα ασφαλείας για ολόκληρο το πορτοφόλι σας

Ο τρόπος με τον οποίο λειτουργούν τα πορτοφόλια δεν είναι κοινός. Μερικά κρατούν πολλά κρυφά ιδιωτικά κλειδιά. Με το να διατηρούνται αντίγραφα ασφαλείας των ιδιωτικών κλειδιών, τα οποία δείχνουν στις ορατές διευθύνσεις Bitcoin, δεν είναι απαραίτητο να μπορεί να γίνει ανάκτηση όλου του ποσού που διαφυλάσσεται στο πορτοφόλι σας. Υπάρχει πιθανότητα ένα μεγάλο μέρος του ποσού να χαθεί.

Μη ρυθμιζόμενα ψηφιακά νομίσματα

3.3.4.2 Κρυπτογράφηση των online αντίγραφων ασφαλείας

Σε αυτήν την εργασία θα χρησιμοποιήσουμε πολλούς παραλληλισμούς με καθημερινές υπηρεσίες γιατί δυστυχώς τα Bitcoin εμπίπτουν στα προβλήματα των ηλεκτρονικών συσκευών και στα προβλήματα που δημιουργούνται με τις υπηρεσίες εντός δικτύου. Δημιουργώντας αντίγραφα ασφαλείας τα οποία αποθηκεύονται εντός δικτύου, τα κάνει αυτομάτως ευάλωτα σε κλοπή. Όπως ακριβώς συμβαίνει και με έναν προσωπικό υπολογιστή ο οποίος είναι συνδεδεμένος στο διαδίκτυο, άρα ευάλωτος σε κακόβουλες ενέργειες. Άρα, κρυπτογραφώντας τα αντίγραφα ασφαλείας που βρίσκονται online, πρακτικά δημιουργούμε μια επιπλέον δικλείδα ασφαλείας. [30]

3.3.4.3 Πολλές και ασφαλείς τοποθεσίες

Το να αποθηκεύετε τα κλειδιά ασφαλείας σας σε ένα σημείο τα κάνει πιο ευάλωτα. Η συμβουλή μας λοιπόν είναι να χρησιμοποιείτε πολλά και καλό θα ήταν, διαφορετικού είδους σημεία αποθήκευσης. Με αυτόν τον τρόπο γίνεται πολύ πιο δύσκολος ο εντοπισμός και ο συνδυασμός τους, εξασφαλίζοντας έτσι τα ποσά σας. Μπορείτε να κάνετε χρήση διαφορετικών μέσων όπως κλειδιά USB, CDs ή ακόμα και την παραδοσιακή μέθοδο του χαρτιού.

3.3.5 Συμβουλές για το πορτοφόλι σας

Διατήρηση αντίγραφων ασφαλείας του πορτοφολιού σας ανά τακτά χρονικά διαστήματα. Με το να έχετε πρόσφατα αντίγραφα ασφαλείας με ανανεωμένες τις πληροφορίες για τις διευθύνσεις των Bitcoin σας είναι μια καλή πρακτική για να αποφύγετε απώλειες. Βέβαια, όλες αυτές οι εφαρμογές θα καταλήξουν να χρησιμοποιούν πορτοφόλια τα οποία χρειάζονται αντίγραφο ασφαλείας μόνο μια φορά.

Όταν μιλάμε για κρυπτογράφηση του πορτοφολιού σας στο κινητό σας επιτρέπει να ορίσετε έναν κωδικό πρόσβασης για οποιονδήποτε προσπαθήσει να κάνει ανάληψη οποιουδήποτε κεφαλαίου. Με αυτόν τον τρόπο προστατεύεστε από οποιονδήποτε προσπαθήσει να αποσπάσει από εσάς ποσά. Ένα πρόβλημα από το οποίο δεν προστατεύεστε είναι από υλικό ή λογισμικό καταγραφής πληκτρολογήσεων.

Μη ρυθμιζόμενα ψηφιακά νομίσματα

Ένα πρόβλημα που ίσως αντιμετωπίσουν οι νέοι χρήστες, είναι πως θα πρέπει να έχουν ένα κωδικό ασφαλείας τον οποίο θα πρέπει να απομνημονεύσουν. Σε αντίθεση με τις τράπεζες, οι επιλογές ανάκτησης κωδικού με το Bitcoin είναι πολύ περιορισμένες. Πρακτικά, όσο τρομακτικό και αν ακούγεται θα πρέπει κανείς να είναι σε θέση να θυμάται των κωδικό πρόσβασής, ακόμα και αν έχει πολύ καιρό να τον χρησιμοποιήσει. Καλό θα ήταν λοιπόν να διατηρείται αποθηκευμένος και σε κάποιο ασφαλές σημείο, κατά προτίμηση όχι σε ηλεκτρονικό μέσο αποθήκευσης.

Κάτι το οποίο ίσως φαίνεται περιττό να αναφερθεί, αλλά στις μέρες είναι απαραίτητο είναι η επιλογή του κωδικού σας. Ακριβώς επειδή δεν δίνεται η δυνατότητα της αλλαγής με ευκολία, θα πρέπει ο κωδικός να είναι αρκετά ισχυρός. Μόνο αριθμοί η ακόμα και λίγα γράμματα δεν προσδίδουν αρκετή ασφάλεια στον κωδικό σας. Μια καλή πρακτική θα ήταν να χρησιμοποιήσετε κάποιο λογισμικό παραγωγής κωδικών ώστε να είστε σίγουροι για την ασφάλεια των Bitcoin σας.

Ένα πορτοφόλι εκτός σύνδεσης, επίσης γνωστό ως αποθήκευση υπό ψύξη (cold storage), είναι στο μέσο που σας παρέχει ακόμη υψηλότερα επίπεδα ασφάλειας για τις αποταμιεύσεις. Συνδυάζει την αποθήκευση ενός πορτοφολιού σε ασφαλές μέρος το οποίο δεν είναι συνδεδεμένο με το δίκτυο. Όταν γίνει σωστά, μπορεί να παρέχει μια πολύ καλή ασφάλεια έναντι στα κενά ασφαλείας των υπολογιστών.

Φυσικά χρησιμοποιώντας ένα offline πορτοφόλι και συνδυάζοντάς το με αντίγραφα ασφαλείας και κρυπτογράφηση αποτελεί μια ακόμη πιο ισχυρή πρακτική. Στη συνέχεια σας παρέχουμε μερικά παραδείγματα offline πορτοφολιών.

Κεφάλαιο 4^ο

4.1 Εξόρυξη με χρήση λογισμικού μέσω server

Η αρχική ιδέα για την υλοποίηση της διπλωματικής εργασίας ήταν, η υλοποίηση της εξόρυξης για ένα χρονικό διάστημα με χρήση του κατάλληλου λογισμικού στο server της σχολής. Αυτό που χρειαζόμασταν είναι οι κωδικοί ώστε να έχουμε πρόσβαση σε ένα τμήμα του server, server rack, ώστε να εγκαταστήσουμε το λογισμικό μας και να ξεκινήσουμε την εξόρυξη.

Δυστυχώς επειδή δεν μας δόθηκε ευκαιρία να πάρουμε τους κατάλληλους κωδικούς και να έχουμε τα αποτελέσματα που επιθυμούμε, θα περιγράψουμε σε θεωρητικό επίπεδο την διαδικασία που έπρεπε να ακολουθηθεί και θα αναφέρουμε μερικά υπαρκτά παραδείγματα υλοποίησης. Τα παραδείγματα αυτά θα μας βοηθήσουν να έχουμε μια πιο σωστή άποψη για την απόδοση των τεχνικών που χρησιμοποιήθηκαν αλλά και τα προβλήματα που δημιουργήθηκαν κατά την υλοποίηση.



Εικόνα 4.1: Server ο οποίος χρησιμοποιείται για την εξόρυξη bitcoin.

Μη ρυθμιζόμενα ψηφιακά νομίσματα

Η διαδικασία που θα ακολουθούσαμε θα περιγραφεί στην παρακάτω ενότητα. Αρχικά θα πρέπει να αναλύσουμε τα χαρακτηριστικά του server. Ο server που χρησιμοποιούμε τρέχει με λειτουργικό Linux. Άρα θα χρειαστούμε κάποιο λογισμικό για Linux συστήματα. Τα λοιπά χαρακτηριστικά είναι τα εξής: Χαρακτηριστικά. Στη συνέχεια θα αναφέρουμε μερικά τέτοια παραδείγματα λογισμικού τα οποία θα μπορούσαμε να εφαρμόσουμε στο server [1].

- Το easyminer: είναι ένα GUI για εξόρυξη το οποίο είναι κατάλληλο για λειτουργικά συστήματα Windows, Linux και Android. Οι σημερινές εκδόσεις του προγράμματος είναι το EasyMiner v1.5A και EasyMiner v1.5B. Επίσης, υπάρχει και λογισμικό για FPGA. Ανήκει στην Butterflylabs η οποία είναι προσφέρει λογισμικό και για άλλες εφαρμογές.
- Phoenix Miner: πρόκειται για ένα λογισμικό το οποίο έχει τη δυνατότητα να δουλεύει με μνήμη η λειτουργεί με μεγαλύτερο κύκλο ρολογιού έως και τα 300 Mhz και 32 δυαδικά ψηφία μέγεθος.

Επίσης υπάρχουν και άλλες παραδείγματα τέτοιων προγραμμάτων τα οποία μπορούμε να χρησιμοποιήσουμε με βάση το λειτουργικό σύστημα που χρησιμοποιούμε και τον τρόπο με τον οποίο θέλουμε να πραγματοποιήσουμε την εξόρυξη.

4.1.1 Εξυπηρετητής

Ο Εξυπηρετητής ή διακομιστής [29], στην αγγλική ορολογία server, είναι το υλικό ή λογισμικό το οποίο συμμετέχει στην παροχή διάφορων υπηρεσιών. Η δουλειά που επιτελεί ο εξυπηρετητής είναι να δουλεύει πάνω στις αιτήσεις άλλων προγραμμάτων, τα οποία αποκαλούνται πελάτες, ή χρησιμοποιώντας την αγγλική ορολογία clients, τα οποία τρέχουν στον ίδιο υπολογιστή ή σε κάποιο άλλο υπολογιστή ο οποίος είναι συνδεδεμένος μέσω δικτύου με τον εξυπηρετητή. Στην ουσία όταν ένα υπολογιστικό σύστημα χρησιμοποιείται όλη την ημέρα για να υλοποιεί αυτές τις εργασίες, μπορεί να καλείται εξυπηρετητής. Με τον όρο πελάτης, μπορεί να αποκαλείται είτε το υλικό είτε το λογισμικό το οποίο βρίσκεται σε επικοινωνία με τον εξυπηρετητή. Ο πελάτης στέλνει αιτήματα στον εξυπηρετητή και αναμένει την απάντησή του.

Επειδή δεν χρειάζεται να αναφέρουμε πιο εξειδικευμένα χαρακτηριστικά του εξυπηρετητή, γιατί δεν αποτελεί θέμα αυτής της διπλωματικής εργασίας, θα περιοριστούμε στην περιγραφή των βασικών χαρακτηριστικών του υλικού, ώστε να έχουμε ένα μέτρο σύγκρισης του κόστους της εξόρυξης.

Η λειτουργία των υπολογιστών που επιτελούν το ρόλο του εξυπηρετητή, είναι καθημερινή και χωρίς διακοπές. Αυτός, όπως είναι λογικό, οδηγεί τους κατασκευαστές

Μη ρυθμιζόμενα ψηφιακά νομίσματα

υπολογιστών να δίνουν ιδιαίτερη έμφαση στην κατασκευή των εξυπηρετητών, τα οποία όπως είναι λογικό αυξάνουν το κόστος κατασκευής συγκριτικά με έναν υπολογιστή οικιακής χρήσης. Στη συνέχεια θα δώσουμε κάποια χαρακτηριστικά των υπολογιστικών συστημάτων τα οποία λειτουργούν ως εξυπηρετητές.

Τρία είναι τα βασικά χαρακτηριστικά ενός εξυπηρετητή, η μητρική πλακέτα, το κουτί και ο σκληρός δίσκος του. Το καθένα από αυτά έχει τα εξής χαρακτηριστικά τα οποία αναλύονται στη συνέχεια.



Η μητρική πλακέτα του εξυπηρετητή έχει ενσωματωμένο σύστημα RAID¹ και απαιτείται η αντοχή σε υψηλές θερμοκρασίες. Επίσης περιέχεται ενσωματωμένη κάρτα οθόνης, για να έχετε τη δυνατότητα χειρισμού του εξυπηρετητή. Τα στοιχεία μνήμης είναι πιο αραιά τοποθετημένα για να δίνεται η δυνατότητα σωστής ψύξης του συστήματος.

Ακόμη, δεν υπάρχουν πολλές ρυθμίσεις επέκτασης και φυσικά υπάρχουν πολύ περισσότερες ενδείξεις των λειτουργιών για να μπορεί ο χρήστης να έχει πλήρη έλεγχο. Τέλος, μπορείτε να χρησιμοποιήσετε μνήμη ECC².

Εικόνα 4.6: Εικόνα εξυπηρετητή.

Το κουτί στο οποίο τοποθετείτε είναι διαφορετικό από τα κλασικά tower των οικιακών συσκευών. Είναι πολύ πιο βαριά, με ειδικό κλείδωμα. Οι ψυκτικοί μηχανισμοί είναι πολύ πιο αποδοτικοί γιατί οι απαιτήσεις του συστήματος είναι πολύ περισσότερες. Επίσης, κάποια ειδικά κουτιά μπορούν να ενσωματωθούν σε racks.

Ένα ακόμη βασικό στοιχείο είναι οι σκληροί δίσκοι του συστήματος. Τα δύο στοιχεία των δίσκων είναι ο μεγαλύτερος χρόνος ζωής καθώς επίσης ότι δίνεται η δυνατότητα αποσύνδεσης τους ενώ βρίσκονται σε λειτουργία.

Βέβαια για να υπολογίσουμε το συνολικό κόστος της εξόρυξης θα πρέπει να λάβουμε υπόψιν και το κόστος του ρεύματος το οποίο θα καταναλωθεί. Μπορεί στη συγκεκριμένη περίπτωση ο server να ανήκει στο τμήμα, αλλά η υπολογιστική ισχύς που καταναλώνεται κατά

¹ Redundant Array of Inexpensive Disks: είναι μια τεχνολογία εικονικής αποθήκευσης δεδομένων.

² Error Correcting Code: κώδικας διόρθωσης λαθών σε RAM.

Μη ρυθμιζόμενα ψηφιακά νομίσματα

την εξόρυξη αυξάνει το ρεύμα το οποίο καταναλώνεται. Δυστυχώς όπως αναφέραμε και νωρίτερα δεν μας δόθηκε η ευκαιρία να υλοποιήσουμε την εξόρυξη οπότε δεν είμαστε σε θέση να σας παραθέσουμε ακριβή στοιχεία.

4.2 Παραδείγματα Υλοποίησης

Στη συνέχεια αυτού του κεφαλαίο θα παρουσιάσουμε κάποια παραδείγματα εξόρυξης τα οποία υλοποιήθηκαν στο παρελθόν, τα προβλήματα που αντιμετώπισαν και τα αποτελέσματα που έβγαλαν.

4.2.1 Προσπάθεια εξόρυξης με χρήση 3000 server - iDrive

Διαβάζοντας αυτό το παράδειγμα εξ αρχής μας δημιουργήθηκε μεγάλη περιέργεια γιατί ο τίτλος του άρθρου ήταν άκρως δελεαστική. Παραθέτουμε τον ακριβή τίτλο και τη μετάφρασή σου «iDrive Attempted To Mine Bitcoin with 3000 Servers - That was a Mistake» [30] σε Ελληνικά «iDrive μια απόπειρα εξόρυξης με 3000 servers – Αυτό ήταν μεγάλο λάθος».



Εικόνα 4.3: Τμήμα της αρχικής σελίδας της εταιρείας iDrive.

Η iDrive είναι μια εταιρεία που προσπάθησε να κάνει εξόρυξη με χρήση 3000 server.

Η εταιρεία η οποία φροντίζει για όλες σας τις ανάγκες σε θέμα αποθήκευσης και διατήρησης εφεδρικών αρχείων, αποφάσισε να κάνει μια προσπάθεια εξόρυξης Bitcoin.

Ο Βασικός λόγος ήταν πως ήθελαν να δοκιμαστούν σε ένα πεδίο το οποίο θεωρούσαν ανεκμετάλλευτη ροή εσόδων. Το αποτέλεσμα ήταν αξιόλογη συλλογή πληροφοριών την οποία μοιράστηκαν στο τηλεοπτικό δίκτυο CNN.

Έτσι αποφάσισαν να πραγματοποιήσουν ένα τεστ εξόρυξης. Γνωρίζοντας βέβαια ότι κατά τη διάρκεια της περιόδου δεν θα έχουν απώλειες και έτσι αποφάσισαν να χρησιμοποιούν

Μη ρυθμιζόμενα ψηφιακά νομίσματα

την μη χρήσιμη χωρητικότητα των server για άλλους σκοπούς. Μια εξειδικευμένη ομάδα μηχανικών της εταιρείας έτρεξαν ένα τεστ για μια εβδομάδα ώστε να καταλήξουν στο αν μπορούσαν να ασχοληθούν με την εξόρυξη Bitcoin. Κατέληξαν σε κάποια συμπεράσματα τα οποία μοιράστηκαν με το κοινό και σας τα παραθέτουμε στη συνέχεια.

4.2.2 Κόστος της εξόρυξης

Παρ όλο που εταιρεία IDrive έχει στην κατοχή της 3000 server αποφάσισε να χρησιμοποιήσει μόνο τους 600 από αυτούς, καθένας από τους οποίους με τετραπύρηνο επεξεργαστή σε συχνότητα 2.8 GHz. Η μελέτη τους βασίστηκε σε ένα χρόνο τεστ και για αυτό το χρονικό διάστημα οι επεξεργαστές λειτουργούν σε καθημερινή βάση 24 ώρες την ημέρα με την δυσκολία η εξόρυξη να αυξάνεται γραμμικά. Θεώρησαν επίσης ότι το να δουλεύουν τους επεξεργαστές τους σε καθημερινή βάση με πλήρη ισχύ, δεν θα δημιουργούνταν επιπλέον έξοδα στην εταιρεία. Συνήθως οι server του δουλεύουν σε 5% ισχύ σε μη απαιτητικές περιόδους. Η διαφορά λοιπόν έγκειται στο γεγονός ότι οι server θα έπρεπε να λειτουργούν συνεχώς στο 100%. Έτσι, θα αυξανόταν η χρήση ηλεκτρικού ρεύματος με αποτέλεσμα την αύξηση του κόστους. Ένα επίσης σημαντικό πρόβλημα είναι ο φόρτος ο οποίος συνέβαλλε και στη γρηγορότερη φθορά των server, το οποίο φυσικά σε μια εταιρεία μεταφράζεται ως κόστος. Τέλος, το να υπερβούν την επιτρεπόμενη κατανάλωση ισχύος θα ήταν ένα σοβαρό πρόβλημα, γιατί θα είχε ως αποτέλεσμα την απενεργοποίηση των server τους.

4.2.3 Χρονικοί περιορισμοί

Μια βασική ανακάλυψη είναι ότι παρατήρησαν, όσο παράδοξο και αν φαίνεται αυτό, πως όσοι περισσότεροι ανακατεύονταν στην εξόρυξη τόσο μειωνόταν η απόδοση για τη δημιουργία ενός bitcoin. Ακόμα και στην περίπτωση που ανάμειξη περισσότερων είναι απαραίτητη, γιατί η κρυπτογραφία γίνεται πιο απαιτητική. Τέλος, παρατήρησαν πως ήταν άσκοπο να σπαταλούν χρόνο μελετώντας τις λεπτομέρειες της διαδικασίας εξόρυξης, θα μπορούσαν να τον αξιοποιήσουν για εστιάζοντας στις δικές τους λειτουργίες.

4.2.3 Αύξηση των εσόδων;

Όπως είναι ήδη γνωστό, η τιμή του bitcoin δεν είναι σταθερή και βασίζεται τις προσαγωγές της αγοράς. Η εταιρεία θεώρησε το ROI³ ως εντελώς απρόβλεπτο, επίσης το ποσό που δόθηκε στους miners ήταν πολύ μεγάλο με τη λογική ότι θα μπορούσε να μειωθεί με την πάροδο του χρόνου, όσο δηλαδή απαιτείται για να είναι η παροχές σε ελεγχόμενο επίπεδο. Όσο λοιπόν η ROI σημειώνει πτωτική τάση, η ενέργεια, οι διαδικασίες, η πολυπλοκότητα και ο χρόνος που απαιτούνταν αυξανόταν. Μετά από ένα προϋπολογισμό της εταιρείας, το να πραγματοποιήσουν εξόρυξη για ένα χρόνο θα τους απέφερε περίπου 0,43 Bitcoin, με κέρδος βασισμένο στις τιμές εκείνης της περιόδου, που ανέρχεται στα \$275.08.

4.2.4 Η ασφάλεια και η εξόρυξη

Οι servers στην εταιρεία δεν είναι βελτιστοποιημένοι ή ρυθμισμένοι για να χρησιμοποιηθούν σε εξόρυξη. Δεν είναι τόσο απλή υπόθεση η εφαρμογή ενός λογισμικού στο server για την εξόρυξη, θα πρέπει να εγκατασταθεί ένας «Bitcoin daemon» σε καθέναν από αυτούς. Ξεκινώντας τη διαδικασία της εξόρυξης και επαναλειτουργώντας την υποδομή που είχαν κλείσει προηγουμένως, ώστε να επιτρέψουν στο δίκτυο του Bitcoin την επικοινωνία με τους server τους. Συχνά πραγματοποιούνται έλεγχοι ασφαλείας ώστε να επιβεβαιώσουν ότι δεν υπάρχουν ανοιχτές περιοχές που δεν πρέπει να είναι ανοικτές. Ανοίγοντας το δίκτυο τους για κάτι μη ουσιώδες όπως το Bitcoin, θεωρήθηκε από τους υπευθύνους ως ένα όχι και τόσο απαραίτητο ρίσκο. Χαρακτηριστική είναι και η απάντηση του Matthew Harvey. «Μην το κάνετε. Χρειαζόμαστε εξειδικευμένο υλικό για να έχουμε αποδοτική εξόρυξη και να παράγουμε αληθινή ROI.» Παραθέτουμε την ακριβή απάντηση του: “Don’t do it. You need custom machines to effectively mine bitcoins and generate a real ROI.”

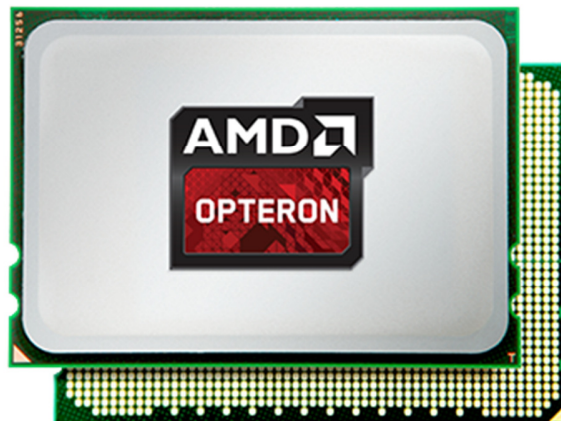
Τέλος, η iDrive ισχυρίζεται ότι πήρε πολλές γνώσεις για την εξόρυξη του Bitcoin, αλλά σε καμία περίπτωση τα πλεονεκτήματα δεν υπερτερούν των μειονεκτημάτων, ώστε να τους δώσει έναυσμα να ασχοληθούν με την εξόρυξη.

³ Return on investment, είναι πρακτικά το κέρδος του επενδυτή το οποίο αποκτάται από μια επένδυση ποσού σε κάποια εταιρεία ή εφαρμογή.

4.4 Εξόρυξη με χρήση επεξεργαστή AMD

4.4.1 Βασικές Προϋποθέσεις

Θα αναλύσουμε σε αυτό το σημείο τα προαπαιτούμενα, τα οποία πρέπει να διευθετήσουμε ώστε να ξεκινήσουμε την εξόρυξη. Το πρώτο και βασικό σημείο είναι να διαθέτουμε μια διεύθυνση bitcoin στην οποία θα αποστέλλουμε τα bitcoin που παράγονται κατά την εξόρυξη. Η διεύθυνση αυτή μπορεί να χρησιμοποιηθεί και για τις μελλοντικές σας συναλλαγές. Επίσης θα χρειαστείτε έναν πελάτη, client, με τον οποίο θα πραγματοποιείτε συναλλαγές και να παρακολουθείτε το υπόλοιπό σας. Ιδιαίτερη προσοχή χρειάζεται στο γεγονός του ότι κάθε φορά που μεταφορτώνεται η βάση με τις συναλλαγές σας, θα παρατηρείτε μεγάλη καθυστέρηση, ιδιαίτερα την πρώτη φορά. Στην περίπτωση που περιγράφουμε χρησιμοποιήθηκε ο bitcoin-qt, είναι από τους πρώτους client που γράφτηκαν και είναι διαθέσιμος μόνο σε Ubuntu. Για περισσότερες πληροφορίες μπορείτε να μεταβείτε στη σελίδα του bitcoin-qt.



Εικόνα 4.4: Ο επεξεργαστής Opteron της AMD για χρήση σε εξυπηρετήτες.

Θα δώσουμε στη συνέχεια μερικές βασικές προδιαγραφές των στοιχείων που χρησιμοποιήθηκαν στο συγκεκριμένο παράδειγμα. [31]

- Η AMD APP Technology είναι το επεξεργαστικό σύστημα που χρησιμοποιήσαμε.
- AMD APP Software Development Kit είναι το περιβάλλον ανάπτυξης εφαρμογών της εταιρείας κατασκευής.

Μη ρυθμιζόμενα ψηφιακά νομίσματα

- Το OpenCL είναι το ανοιχτό πρότυπο προγραμματισμού συστημάτων με ετερογενείς. Όταν λέμε ετερογένειες εννοούμε συνήθως το συνδυασμό GPU⁴ και CPU. Με αυτόν τον τρόπο μπορούμε να χρησιμοποιήσουμε την αποδοτικότητα μιας GPU για υπολογισμούς που υλοποιούνται κατά την εξόρυξη. Οι πιο πρόσφατες εκδόσεις του Catalyst υλοποιούν το opencl.

4.4.2 Εγκατάσταση και προετοιμασία

Ο οδηγός Catalyst περιέχει υποστήριξη, αλλά ο προγραμματιστής για να συντάξει και να μεταγλωττίσει ένα πρόγραμμα θα χρειαστεί κάποια έκδοση του AMD-APP-SDK. Την συγκεκριμένη έκδοση που θα χρειαστείτε θα την βρείτε στην ιστοσελίδα της εταιρείας. Οπότε, θα πρέπει να γνωρίζουμε την έκδοση του catalyst που αντιστοιχεί στην έκδοση του fg1rx οδηγού μας. Θα πρέπει να χρησιμοποιήσετε την εντολή `$ dmesg | grep fg1rx`, η οποία θα σας δώσει την έκδοση του fg1rx. Ένας άλλος τρόπος είναι να ανοίξετε το catalyst control center. Επειδή το να αναφέρουμε επιπλέον πληροφορίες ξεφεύγει από το σκοπό αυτής της εργασίας, αν θέλετε περισσότερες πληροφορίες μπορείτε να διαβάσετε το αρχείο README και να δείτε αναλυτικά τα βήματα εγκατάστασης.

Δυο απαραίτητα στοιχεία τα οποία θα χρειαστείτε είναι:

- pyopencl: βιβλιοθήκη της Python τη χρήση opencl κώδικα.
- miner: Υπάρχουν πολλοί εξορύκτες που μπορείτε να χρησιμοποιήσετε. Στα πλαίσια της εργασίας που αναφέρουμε χρησιμοποιήθηκε ο roclbm.
- Επίσης απαιτήθηκε και η χρήση του git γιατί δεν υπάρχει πακέτο στα επίσημα αποθετήρια.

Το θέμα που προέκυψε όσον αφορά τη χρήση του miner, ο οποίος είναι single setup με 5870 και ο amd sempron 140, οπότε απαιτείται μια ισχυρή ΚΜΕ. Η ΚΜΕ που χρησιμοποιήθηκε είχε κατά μέσο όρο 330MHash/s. Οι απαιτήσεις που είχαν καθοριστεί από την εταιρεία ήταν στα 390MHash/s. Επίσης η θερμοκρασία της κάρτας διπλασιάζεται από κατά τη διάρκεια της εξόρυξης, ένα θέμα που απαιτεί λύση. Αυτό σημαίνει πως θα πρέπει να έχουμε συνεχή έλεγχο της θερμοκρασίας, για να μην αντιμετωπίσουμε προβλήματα κατά την εξόρυξη.

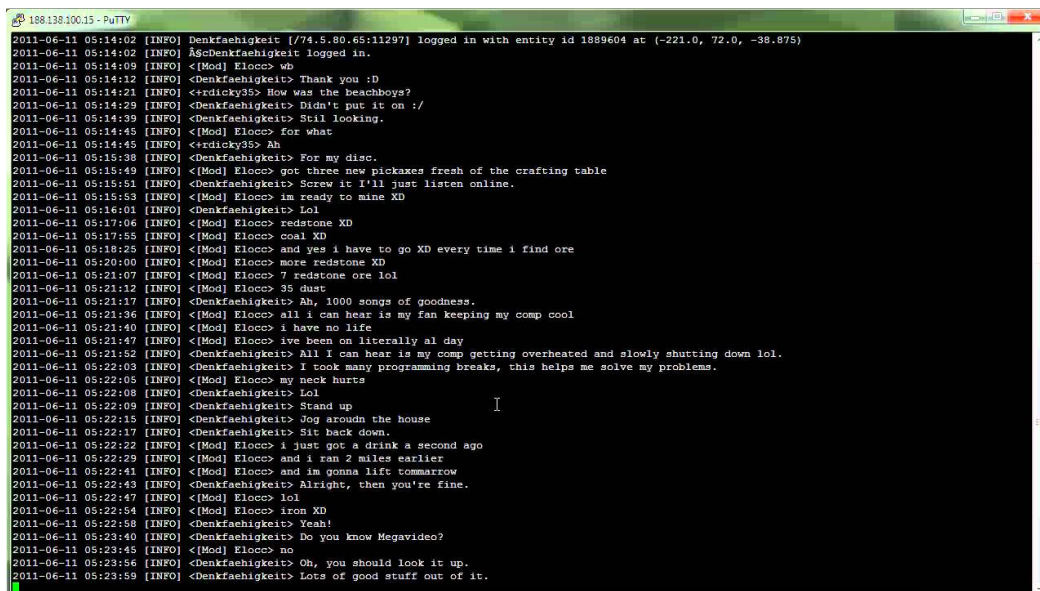
⁴ Graphics Processing Unit: Ο επεξεργαστής της κάρτας γραφικών, που ονομάζεται μονάδα επεξεργασίας γραφικών και ακολουθεί την ίδια λογική με τον επεξεργαστή ενός υπολογιστή.

Μη ρυθμιζόμενα ψηφιακά νομίσματα

4.4.3 Απομακρυσμένη Διαχείριση

Στην ιδανική περίπτωση θα επιθυμούσαμε να έχουμε τη δυνατότητα απομακρυσμένης διαχείρισης στα εξής πεδία:

- Να πραγματοποιούμε έναρξη και λήξη των Miners.
- Να παρακολουθούμε την αποδοτικότητα των Miners.
- Να ελέγχουμε τη μνήμη και την ταχύτητα του συστήματος.
- Να ελέγχουμε τη θερμοκρασία του συστήματος.
- Να παρακολουθούμε και να μπορούμε να επέμβουμε στην ταχύτητα των ψυκτικών μέσων.



```
188.138.100.15 - PuTTY
2011-06-11 05:14:02 [INFO] Denkfaehigkeit [/74.5.80.65:11297] logged in with entity id 1889604 at (-221.0, 72.0, -38.875)
2011-06-11 05:14:02 [INFO] ÅSDenkfaehigkeit logged in.
2011-06-11 05:14:09 [INFO] <Mod Elococ> wo
2011-06-11 05:14:12 [INFO] <Denkfaehigkeit> Thank you :D
2011-06-11 05:14:21 [INFO] <+rdicky95> How was the beachboys?
2011-06-11 05:14:29 [INFO] <Denkfaehigkeit> Didn't put it on :/
2011-06-11 05:14:39 [INFO] <Denkfaehigkeit> Still looking.
2011-06-11 05:14:45 [INFO] <Mod Elococ> for what
2011-06-11 05:14:45 [INFO] <+rdicky95> Ah
2011-06-11 05:15:38 [INFO] <Denkfaehigkeit> For my disc.
2011-06-11 05:15:49 [INFO] <Mod Elococ> got three new pickaxes fresh of the crafting table
2011-06-11 05:15:51 [INFO] <Denkfaehigkeit> Screw it I'll just listen online.
2011-06-11 05:15:53 [INFO] <Mod Elococ> im ready to mine XD
2011-06-11 05:16:01 [INFO] <Denkfaehigkeit> Lol
2011-06-11 05:17:06 [INFO] <Mod Elococ> redstone XD
2011-06-11 05:17:55 [INFO] <Mod Elococ> coal XD
2011-06-11 05:18:25 [INFO] <Mod Elococ> and yes i have to go XD every time i find ore
2011-06-11 05:20:00 [INFO] <Mod Elococ> more redstone XD
2011-06-11 05:21:07 [INFO] <Mod Elococ> 7 redstone ore lol
2011-06-11 05:21:12 [INFO] <Mod Elococ> 35 dust
2011-06-11 05:21:17 [INFO] <Denkfaehigkeit> Ah, 1000 songs of goodness.
2011-06-11 05:21:36 [INFO] <Mod Elococ> all i can hear is my fan keeping my comp cool
2011-06-11 05:21:40 [INFO] <Mod Elococ> i have no life
2011-06-11 05:21:47 [INFO] <Mod Elococ> ive been on literally al day
2011-06-11 05:21:52 [INFO] <Denkfaehigkeit> All I can hear is my comp getting overheated and slowly shutting down lol.
2011-06-11 05:22:03 [INFO] <Denkfaehigkeit> I took many programming breaks, this helps me solve my problems.
2011-06-11 05:22:05 [INFO] <Mod Elococ> my neck hurts
2011-06-11 05:22:08 [INFO] <Denkfaehigkeit> Lol
2011-06-11 05:22:09 [INFO] <Denkfaehigkeit> Stand up
2011-06-11 05:22:15 [INFO] <Denkfaehigkeit> Jog around the house
2011-06-11 05:22:17 [INFO] <Denkfaehigkeit> Sit back down.
2011-06-11 05:22:22 [INFO] <Mod Elococ> i just got a drink a second ago
2011-06-11 05:22:29 [INFO] <Mod Elococ> and i ran 2 miles earlier
2011-06-11 05:22:41 [INFO] <Mod Elococ> and im gonna lift tomorrow
2011-06-11 05:22:43 [INFO] <Denkfaehigkeit> Alright, then you're fine.
2011-06-11 05:22:47 [INFO] <Mod Elococ> lol
2011-06-11 05:22:54 [INFO] <Mod Elococ> ikon XD
2011-06-11 05:22:58 [INFO] <Denkfaehigkeit> Yeah!
2011-06-11 05:23:40 [INFO] <Denkfaehigkeit> Do you know Megavideo?
2011-06-11 05:23:45 [INFO] <Mod Elococ> no
2011-06-11 05:23:56 [INFO] <Denkfaehigkeit> Oh, you should look it up.
2011-06-11 05:23:59 [INFO] <Denkfaehigkeit> Lots of good stuff out of it.
```

Εικόνα 4.4: Περιβάλλον server με χρήση εντολών Linux.

Ο miner δεν απαιτεί περιφερειακές συσκευές εισόδου – εξόδου, αλλά μόνο μια κάρτα δικτύου. Οι μέθοδοι με τις οποίες μπορούμε να διαχειριστούμε το miner είναι με το πληκτρολόγιο *vinu* ή με χρήση *κοινής επιφάνειας εργασίας*. Όσον αφορά τις ρυθμίσεις του server που πρέπει να διαχειριστούμε κατά τη διάρκεια της εξόρυξης οι βασικές είναι:

- Η δυνατότητα σε άλλους χρήστες να ελέγχουν την επιφάνεια εργασίας.
- Αίτηση επιβεβαίωσης κάθε φορά που υπάρχει πρόσβαση στο σύστημα.
- Αίτηση κωδικού επιβεβαίωσης κατά την είσοδο.

Μη ρυθμιζόμενα ψηφιακά νομίσματα

Η σύνδεση με απομακρυσμένο εξορύκτη μπορεί να γίνει και χωρίς γραφικό περιβάλλον με τη χρήση εντολών. Όπως είναι λογικό αυτό απαιτεί και κάποιες επιπλέον γνώσεις. Τέλος, σε αυτό το παράδειγμα θα αναφέρουμε και το κόστος σε ρεύμα το οποίο αναφέρει ο χρήστης. Αν ο miner καταναλώνει 400W τότε μιλάμε για 0.4KWH επί 24 ώρες, άρα 9.6 KWH.

Κεφάλαιο 5^ο

Σε αυτό το κεφάλαιο θα ασχοληθούμε με δύο βασικά και δυναμικά θέματα που αφορούν το Bitcoin. Το πρώτο είναι οι εφαρμογές και συναλλαγές στις οποίες μπορεί το Bitcoin να χρησιμοποιηθεί ως μέσω συναλλαγής. Δεύτερον, και εξίσου σημαντικό, είναι τα νομικά θέματα που ισχύουν και συνεχώς διαμορφώνονται σε σχέση με τις συναλλαγές αλλά και τη νομιμότητα απόκτησης των κρυπτονομισμάτων. [32]

5.1 Χρήσεις του Bitcoin

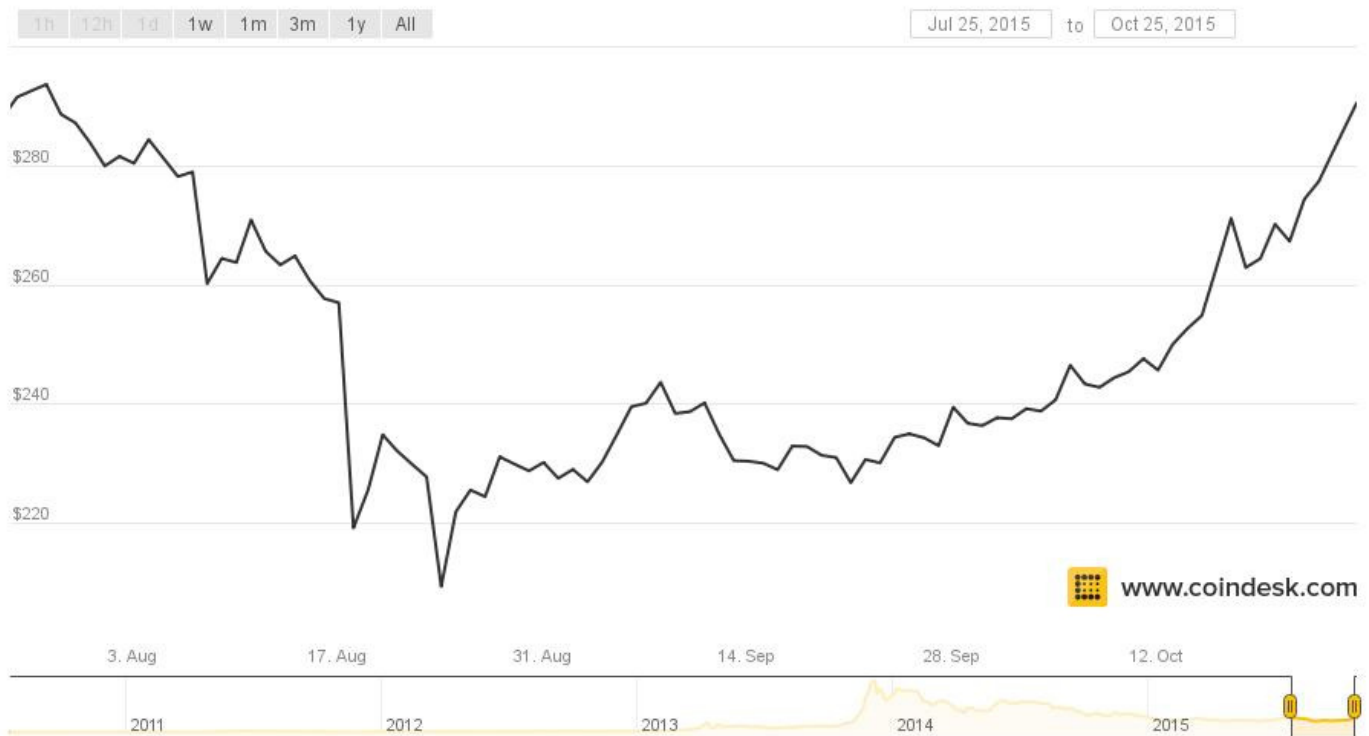
Όπως αναφέραμε στην αρχή αυτού του κεφαλαίου, σε αυτό το εδάφιο θα ασχοληθούμε με τις συναλλαγές οι οποίες μπορούν να πραγματοποιηθούν, χρησιμοποιώντας ως νόμισμα συναλλαγής το Bitcoin. Αυτό βέβαια αποτελεί ένα πολύ δυναμικό πεδίο, το οποίο, χωρίς καμία δόση υπερβολής, αλλάζει ακόμη και τη διάρκεια συγγραφής αυτής της διπλωματικής εργασίας. Αυτό είναι και το πιο δύσκολο κομμάτι για την συγγραφή της.

Το Bitcoin αρχικά χρησιμοποιούνταν σε ελάχιστες εφαρμογές. Σήμερα όλο και περισσότερες επιχειρήσεις και οργανισμοί υιοθετούν το Bitcoin ως εναλλακτικό τρόπο πληρωμής. Αυτή βεβαίως δεν είναι μια απλή διαδικασία αφού θα πρέπει να θεσμοθετηθεί κατάλληλο νομικό πλαίσιο που να επιτρέπει και να προστατεύει τόσο τους πελάτες όσο και τις επιχειρήσεις. Μην ξεχνάμε πως το Bitcoin δεν σταθερή τιμή, με αποτέλεσμα μια συναλλαγή να μπορεί να υπερτιμηθεί ή υποτιμηθεί. Για να δώσουμε ουσία σε αυτά που προαναφέραμε θα παραθέσουμε ένα γράφημα με τις διακυμάνσεις του Bitcoin το τελευταίο τρίμηνο⁵, έως τις 24 Οκτωβρίου 2015. Παρατηρούμε ότι το Bitcoin έχει ασταθή συμπεριφορά η οποία επηρεάζεται τα πολιτικά και οικονομικά δρώμενα παγκοσμίως.

Τον τελευταίο καιρό όλο και περισσότερα, διεθνή μέσα μαζικής επικοινωνίας ασχολούνται με τα νέα του Bitcoin. Στη συνέχεια θα αναφέρουμε κάποια επιλεγμένα άρθρα από τον τύπο τα οποία αναφέρονται σε επιχειρήσεις και οργανισμούς και τις συναλλαγές τους με Bitcoin.

⁵ Πηγή του γραφήματος είναι η ιστοσελίδα <http://www.coindesk.com/price/>.

Μη ρυθμιζόμενα ψηφιακά νομίσματα



Εικόνα 5.1: Η διακύμανση του Bitcoin το τελευταίο τρίμηνο.

5.1.1 Η περίπτωση του εστιατορίου

Πρόσφατα, για την ακρίβεια στα μέσα Οκτώβρη, ένα εστιατόριο στο San Diego κοινοποίησε την απόφαση του ιδιοκτήτη του να δέχεται ως τρόπο πληρωμής τα Bitcoin για τις υπηρεσίες που προσφέρει το κατάστημά του. Όπως αναφέρει ο ιδιοκτήτης, το έκανε ώστε το θέμα να πάρει έκταση και να προσελκύσει κόσμο. Ο κόσμος το δέχτηκε με χαρά και όπως φάνηκε πέτυχε το σκοπό του. Ένα χαρακτηριστικά παράδειγμα marketing λοιπόν, χρησιμοποιώντας το Bitcoin. Παραθέτουμε και τα ακριβή λόγια του ιδιοκτήτη, κύριου Torres, στο CCN⁶. «I wanted to get a little exposure and have people trickle in, you want to go slow and take it easy and make sure things are right. So far, so good, people seem to be enjoying it.». Το άρθρο βγήκε στη δημοσιότητα τον Οκτώβριο του 2015.

⁶ Financial Bitcoin & Cryptocurrency News

5.1.2 Συναλλαγές στη μέση ανατολή

Η startup εταιρία BitOasis επεκτείνει πλέον τις συναλλαγές στη μέση Ανατολή, είναι ο τίτλος του άρθρου της CoinDesk. Η εταιρία έχει πλέον συναλλαγές με το Κουβέιτ, το Μπαχρέιν και το Κατάρ και επιθυμεί να ξεκινήσει την εξόρυξη στις χώρες αυτές. Ο κ. Doubin, ιδρυτής της εταιρίας, ανέφερε πως οι πελάτες πλέον φτάνουν τους 20.000. Η συνεργασία τους είναι τόσο με μικρές όσο και μεγαλύτερες επιχειρήσεις οι οποίες επιθυμούν να πραγματοποιήσουν συναλλαγές με το Bitcoin.

5.1.3 Η νομική εταιρία του Λονδίνου

Μια Τεξανή εταιρία, η οποία ιδρύθηκε πρόσφατα, ζήτησε από μια νομική εταιρία να ανταλλάξει τα συμβόλαιά της με αυτόματα «έξυπνα συμβόλαια», τα οποία θα βρίσκονται ένα επίπεδο παραπάνω από την αλυσίδα του Bitcoin. Ο συνέταιρος της εταιρίας ανέφερε ότι η εταιρία εδώ και καιρό προσπαθεί να βρει εναλλακτικούς τρόπους επίλυσης του θέματος αυτού από το 2013. Παραθέτουμε και τα ακριβή λόγια που χρησιμοποίησε « We envisage smart contracts being revolutionary in litigation across the world. This is just the beginning of a game-changing implementation and execution of contracts. Ultimately, the technology is now in place for any contract to be a smart contract. »

5.1.4 Αφορολόγητο το Bitcoin στην Ευρώπη

Το θέμα που έχει προκύψει αφορά την φορολόγηση του Bitcoin. Δεν είναι κάτι απλό και πρόσφατα τέθηκε θέμα στο Ευρωπαϊκό δικαστήριο, το οποίο αφορούσε τη μετατροπή κρυπτονομισμάτων σε άλλα συμβατικά νομίσματα. Το θέμα αυτό ξεκίνησε με την αντιπαράθεση που δημιουργήθηκε μεταξύ των Daniel Hedqvist, ο οποίος είναι Bitcoin Forum Operator, με τις οικονομικές αρχές της Σουηδίας, σχετικά με τη διακίνηση και τη φορολογία των κρυπτονομισμάτων. Η απόφαση του Δικαστηρίου η εξής: «η μετατροπή αυτή αποτελεί μία μορφή οικονομικής υπηρεσίας η οποία δεν μπορεί να αλλοιωθεί, διότι θα παραβιάσει μία από τις κατευθυντήριες αρχές πάνω στις οποίες βασίζεται το Bitcoin.» Έτσι τα ανταλλακτικά μπορούν να μεταβιβάζουν κρυπτονομίσματα σε συμβατικά νομίσματα χωρίς την καταβολή ειδικού φόρου.

5.1.5 Δάνεια σε Bitcoin;

Μια ακόμα δικαστική απόφαση αφορά την είδηση που θα αναφέρουμε. Η ιστορία αυτή προέκυψε στις ΗΠΑ μεταξύ του ενάγοντα Daniel Kaminski de Souza, ο οποίος δάνεισε στον εναγόμενο Dennis Kerley, το ποσό των 11,95 BTC. Την ημέρα που έγινε η δoσοληψία η αξία σε συμβατικό νόμισμα, στην περίπτωση αυτή δολάρια, ήταν περίπου \$10.000.



Εικόνα 5.2: Δικαστική διαμάχη λόγω Bitcoin.

Η συμφωνία για την αποπληρωμή του ποσού δεν τηρήθηκε και όπως είναι αναμενόμενο η υπόθεση κατέληξε στο δικαστήριο. Αρχικά, το δικαστήριο αποφάσισε ως ποσό αποπληρωμής τα 64,74381250 BTC, μετά από 91 μέρες καθυστερημένης αποπληρωμής, οπότε και ασκήθηκε αγωγή εκ μέρους του συνηγόρου υπεράσπισης. Τελικά, την 5^η Ιουλίου του τρέχοντος έτους, ο εναγόμενος κρίθηκε να πληρώσει το ποσό των \$67.591, ποσό που αφορά το δάνειο που πήρε.

5.1.6 Το πρώτο ATM για Bitcoin στην Ελλάδα

Το πρώτο ATM, είναι γεγονός και λειτουργεί στην Αθήνα. Αποτελεί ένα χαρακτηριστικά παράδειγμα της δημοτικότητας του Bitcoin. Μέχρι σήμερα, 129 ελληνικές εταιρείες έχουν ανοίξει λογαριασμό στην πλατφόρμα ώστε να μπορούν να δέχονται συναλλαγές με Bitcoins. Η εταιρία που το λάνσαρε, bitcoinsgreece, είναι πολύ ικανοποιημένη από την αποδοχή του κόσμου και σκοπεύει άμεσα την τοποθέτηση και άλλων ATM στην Αθήνα αλλά και σε άλλες πόλεις της Ελλάδας.

5.1.7 Αποπληρωμή εξαγωγών σε Bitcoin

Στην περίπτωση αυτή, η οποία αφορά την Ελλάδα και το σοβαρό θέμα συναλλαγών με το εξωτερικό το καλοκαίρι του 2015, έχουμε την πληρωμή εξαγωγών με Bitcoin. Η προσέγγιση αυτή έχει δοθεί από μία Ιρλανδική εταιρία, με όνομα Spartan Route, η οποία προτίθεται να

Μη ρυθμιζόμενα ψηφιακά νομίσματα

παίζει τον ενδιάμεσο στις συναλλαγές με εξαγόμενα προϊόντα. Με αυτόν τον τρόπο οι Ελληνικές εταιρίες εξάγουν τα προϊόντα τους και αμείβονται με Bitcoin τα οποία, προς το παρόν τουλάχιστον, δεν υπόκεινται στους περιορισμούς συναλλαγών όπως τα συμβατικά νομίσματα, παρά των περιορισμό των κεφαλαίων που είχαν εφαρμοστεί. Έχουμε λοιπόν μια ακόμη επεμβατική χρήση του Bitcoin η οποία έδωσε λύση σε ένα οικονομικό πρόβλημα που είχε δημιουργηθεί.

Δεν είναι τυχαίο ότι αναφέραμε τις πληρωμές, εν μέσω καθεστώτος κεφαλαιακών περιορισμών, στους οποίους δεν υπόκεινται τα κρυπτογραφημένα νομίσματα. Στη συνέχεια λοιπόν, θα αναφέρουμε το νομικό καθεστώς ισχύει, αλλά συνεχώς διαμορφώνεται, στις περισσότερες χώρες οι οποίες υποστηρίζουν συναλλαγές με Bitcoin.

5.2 Ισοτιμία

Σε αυτό το σημείο θα αναλύσουμε ένα ουσιαστικό χαρακτηριστικό του bitcoin, το οποίο το διαφοροποιεί από τα συμβατικά νομίσματα και επηρεάζει ουσιαστικά την ισοτιμία του. Το bitcoin είναι ένα εξωτραπεζικό νόμισμα και οι παράγοντες που επηρεάζουν την ισοτιμία του δεν μπορούν να καθοριστούν ώστε να έχουμε ένα εύρος τιμών στο οποίο να ανήκει. Προτού όμως μιλήσουμε για τα προβλήματα που μπορεί να προκαλέσει αυτή η ιδιότητα του, θα αναλύσουμε κάποιους οικονομικούς όρους, όπως την ισοτιμία και πως καθορίζεται.

	Μεταβλητότητα	Τάση	Προηγ. Εβδομάδα	Τρέχοντα Δεδομένα	Σύστημα DailyFX
EURUSD	22.22%	↓	3.39%	Trend	Trend
USDCHE	13.33%	↑	98.41%	Trend	Trend
NZDUSD	9.52%	↔	66.67%	Range/Trend	Range/Trend
USDCAD	3.08%	↔	41.94%	Range	Range
AUDUSD	7.81%	↔	71.43%	Trend/Range	Trend/Range
GBPUSD	18.75%	↔	35.94%	Trend	Trend
USDJPY	1.64%	↓	10.53%	Range/Trend	Trend
EURCAD	1.56%	↓	3.08%	Trend	Trend
EURCHF	30.65%	↓	18.60%		
EURGBP	12.70%	↓	1.59%	Trend	Trend
GBPCHF	16.36%	↑	100.00%	Trend	Trend
AUDJPY	11.11%	↔	57.81%	Range/Trend	Trend
EURJPY	33.85%	↓	1.61%	Trend	Trend
CADJPY	1.72%	↔	39.06%	Range/Trend	Trend
CHFJPY	35.94%	↓	1.54%	Trend	Trend
EURAUD	4.76%	↓	3.13%	Trend	Trend
GBPJPY	31.15%	↓	12.31%	Trend	Trend
NZDJPY	11.11%	↔	51.56%	Range/Trend	Trend

Εικόνα 5.3: Ταμπλό ονομαστικών συναλλαγματικών ισοτιμιών σε ανταλλακτήριο συναλλάγματος στην Ταϊλάνδη (πηγή Google images)

οργανισμών όπως για παράδειγμα το Διεθνές Νομισματικό Ταμείο. [33]

Μη ρυθμιζόμενα ψηφιακά νομίσματα

Στη οικονομία, όπως ορίζεται σήμερα, ο όρος ισοτιμία που χρησιμοποιείται κυρίως στις εμπορικές συναλλαγές, όπου χρησιμοποιούνται διαφορετικά νομίσματα, αφορά τιμές προϊόντων, συναλλάγματος, την αγοραστική δύναμη ενός νομίσματος και τέλος του μισθούς των κατοίκων μιας χώρας. Η αξία του κάθε νομίσματος αποτελεί συνάρτηση της οικονομικής ισχύος της κάθε χώρας καθώς και της νομισματικής πολιτικής που ακολουθεί η Κεντρική τράπεζα της εκάστοτε χώρας ή με παρέμβαση διεθνών οργανισμών όπως για παράδειγμα το Διεθνές Νομισματικό Ταμείο.

Ένας τομέας στον οποίο είναι βασική η ισοτιμία, είναι οι διεθνής συναλλαγές στις οποίες απαιτείται η ανταλλαγή νομισμάτων, και ουσιαστικά η τιμή τους καθορίζει την αγοραστική του δύναμη, η οποία καλείται συναλλαγματική ισοτιμία. Οι οικονομικές, κοινωνικές και πολιτικές συνθήκες μπορούν να επηρεάσουν τη συναλλαγματική ισοτιμία ενός νομίσματος. Χαρακτηριστικό παράδειγμα η ισοτιμία του ευρώ έναντι του δολαρίου σε περιόδους που είτε στην Ηνωμένες πολιτείες, είτε στην Ευρώπη κοινωνικοπολιτικές αλλαγές επηρεάζουν τη μεταξύ του ισοτιμία. Όμως υπάρχει ένα άνω και κάτω όριο στην τιμή του κάθε νομίσματος.

Η ουσιαστική διαφορά του bitcoin έναντι των προαναφερθέντων είναι ότι και η τιμή του bitcoin επηρεάζεται από κοινωνικοπολιτικούς παράγοντες, αλλά επηρεάζεται και από παράγοντες αγοράς και ζήτησης εκ μέρους των χρηστών του. Επίσης, η τιμή του έχει παρουσιάσει σε βραχύβια περίοδο, τεράστιες αυξομειώσεις. Το 2013 η τιμή του bitcoin άγγιζε τα 1000 δολάρια κάνοντας πολλούς κατόχους εκατομμυριούχους, για μικρό χρονικό διάστημα. Το τελευταίο εξάμηνο η αγοραστική αξία του bitcoin κυμαίνεται από 280 έως 350 δολάρια. Ποιος ήταν ο λόγος λοιπόν που έχουμε τόσο μεγάλες διακυμάνσεις;

Κατά την εμφάνισή του bitcoin το ευρύ κοινό δεν γνώριζε την ύπαρξή και φυσικά δεν είναι τυχαίο πως και η ταυτότητα του εμπνευστή του, Shatoshi Nakamoto, ακολουθείται ακόμα και σήμερα από διάφορους μύθους που αφορούν την ύπαρξη του. Πώς λοιπόν σήμερα ασχολούνται όλο και περισσότεροι χρήστες με την εξόρυξη bitcoin;

Ένας λόγος για τον οποίο ξεκίνησαν οι πρώτοι χρήστες την εξόρυξη ήταν η περιέργεια για το νέο και άγνωστο αυτό αντικείμενο. Αυτός ήταν ένας παράγοντας που επηρέασε στην αύξηση της αγοραστικής αξίας του bitcoin και την εκτόξευσε σε μικρό χρονικό διάστημα. Ακόμα και σήμερα διάφοροι λόγοι οδηγούν νέους χρήστες στην ενασχόληση με την εξόρυξη, όπως η αγορά συγκεκριμένων προϊόντων, η κερδοσκοπία, ή ακόμα και η μείωση της αγοραστικής αξίας του συμβατικού νομίσματος. Όλοι αυτοί οι λόγοι συμβάλλουν στην αύξηση της ζήτησης.

Μη ρυθμιζόμενα ψηφιακά νομίσματα

Η προσφορά του από την άλλη, μπορεί να σχετίζεται με τις αρνητικές προσδοκίες για την πορεία της τιμής του bitcoin, την επιθυμία καθαρού κέρδους για όσους τα παράγουν, τα καταστήματα τα οποία δέχονται ψηφιακά νομίσματα και προβαίνουν άμεσα στην ανταλλαγή τους, με την ρευστοποίησή τους για αποπληρωμή υποχρεώσεων των χρηστών, ή την μετατροπή τους για αγορά προϊόντων σε καταστήματα που δεν δέχονται Bitcoin. [34]

Όπως είναι λογικό, η αστάθεια στην ισοτιμία του bitcoin, αλλά και όλων των ψηφιακών νομισμάτων, αποτελεί ανασταλτικό παράγοντα για πολλούς χρήστες ή ενδιαφερόμενους, οι οποίοι το σκέφτονται να σπαταλήσουν χρόνο και χρήμα για την εξόρυξη. Η κατάσταση αυτή οδηγεί τους κακοπροαίρετους να αποκαλούν το bitcoin μια «φούσκα», τονίζοντας την αστάθεια που το χαρακτηρίζει. Δυστυχώς ακόμα, δεν μπορούμε να πάρουμε θέση και να σας δώσουμε μια απάντηση για το αν θα κερδίσετε ή θα χάσετε από την εξόρυξη bitcoin, καθώς το νομικό πλαίσιο το οποίο μπορεί να σας προστατέψει βρίσκεται ακόμη υπό εξέλιξη.

Όλα όσα αναφέρθηκαν παραπάνω αποτελούν παράγοντες για τους οποίους, οι πιο συντηρητικοί δεν «παρασύρθηκαν» στην εξόρυξη, φοβούμενοι την απώλεια κέρδους. Όμως οι χρήστες του bitcoin συνεχώς αυξάνονται προσδίδοντας μια επιπλέον σταθερότητα στην τιμή του, και δίνοντας του χώρο να εξελιχθεί.

5.3 Bitcoin και Νόμοι

Δεν είναι η πρώτη φορά που η επιστήμη της νομικής έπεται των εξελίξεων. Στις περισσότερες περιπτώσεις ψηφιακών αλμάτων το νομικό πλαίσιο διαμορφώνεται κατόπιν εορτής με αποτέλεσμα να επικρατεί «αναρχία», έως ότου θεσμοθετηθούν οι απαραίτητοι περιορισμοί. Οι περισσότερες χώρες έχουν διαμορφώσει ένα πολιτικό πλαίσιο, το οποίο φυσικά διαμορφώνεται και εξελίσσεται.

Στη συνέχεια παραθέτουμε έναν πίνακα με την ισχύουσα, προς στιγμήν, νομοθεσία για την κάθε χώρα. [14] [35]



Αργεντινή

Το Bitcoin σύμφωνα με το Εθνικό Ίδρυμα της Αργεντινής θεωρείται χρήμα, αλλά δεν μπορεί να θεωρηθεί εθνικό νόμισμα, υπό τη νομική έννοια.

Μη ρυθμιζόμενα ψηφιακά νομίσματα



Αυστραλία

Το 2013, σε συνέντευξη του Προέδρου της Τράπεζας Αποθεμάτων της Αυστραλίας ειπώθηκε ότι: *Κανείς δεν μπορεί να αποδιεί τον κόσμο να πραγματοποιεί τις συναλλαγές του με κάποιο εναλλακτικό οικονομικό μέσο σε οποιοδήποτε κατάσταση, αν είναι κοινώς αποδεκτό και από τις δύο πλευρές. Δεν υπάρχει κάποιος νόμος που να το απαγορεύει, δεδομένου ότι υπάρχουν ανταγωνιστικές οικονομίες.* Τα ακριβή του λόγια παρατίθενται: «There would be nothing to stop people in this country deciding to transact in some other currency in a shop if they wanted to. There's no law against that, so we do have competing currencies».



Μπαγκλαντές

Στο Μπαγκλαντές δεν επιτρέπεται απολύτως καμία συναλλαγή με Bitcoin. Για την ακρίβεια οποιοσδήποτε πραγματοποιήσει μια τέτοιου είδους συναλλαγή απειλείται με φυλάκιση, δεδομένου ότι οι νόμοι της χώρας για τις παράνομες χρηματικές συναλλαγές είναι αυστηροί. Ο νόμος αυτός ψηφίστηκε το Σεπτέμβριο του 2014 και τα ακριβή λόγια του Προέδρου της εθνικής τράπεζας της χώρας ήταν τα εξής «anybody caught using the virtual currency could be jailed under the country's strict anti-money laundering laws».



Βέλγιο

Ο πρόεδρος οικονομικών της χώρας ανέφερε πως δεν θεωρείται απαραίτητο να αναμειχθεί η κυβέρνηση στο σύστημα λειτουργίας του Bitcoin, τη δεδομένη χρονική περίοδο.



Βολιβία


Η εθνική τράπεζα της χώρας δεν δέχεται οποιαδήποτε συναλλαγή με κρυπτονομίσματα.







Βραζιλία

Οι συναλλαγές με Bitcoin πραγματοποιούνται, νομικά βέβαια βρίσκονται ακόμα υπό συζήτηση, τόσο μέσω πληρωμών με κινητά συστήματα ή με ηλεκτρονικές εξαργυρώσεις.

Μη ρυθμιζόμενα ψηφιακά νομίσματα

 Βουλγαρία	Το Bitcoin βρίσκεται υπό ρυθμιζόμενο νόμο ο οποίος συζητά θέματα πληρωμών και υπηρεσίες πληρωμών.
 Καναδάς	Το θέμα ρυθμίζεται κάτω από προϋποθέσεις που προσπαθούν να προστατέψουν την οικονομία της χώρας από ξέπλυμα χρήματος, και νόμοι που αφορούν θέματα τρομοκρατικών ενεργειών σε οικονομικό επίπεδο.
 Χιλή	Δεν έχει θεσμοθετηθεί νομοθετικό πλαίσιο για το Bitcoin στη συγκεκριμένη χώρα.
 Κίνα (PRC)	Ενώ οι ιδιώτες έχουν τη δυνατότητα να συντηρούν και να εμπορεύονται Bitcoin στην Κίνα, οι κανονισμοί απαγορεύουν σε εταιρίες που ασχολούνται με οικονομικά, όπως για παράδειγμα τράπεζες, να κάνουν οποιοσδήποτε συναλλαγές.
 Κολομβία	Το Μάρτη του 2014 συντάχθηκε εγκύκλιος στην οποία αναφέρεται ότι η χρήση Bitcoin δεν είναι ρυθμισμένη στη χώρα.
 Κροατία	Το Δεκέμβριο του 2013, διεξήχθη συζήτηση, σύμφωνα με πληροφορίες, στην εθνική τράπεζα της χώρας, για την κυκλοφορία ψηφιακών νομισμάτων, η οποία κατέληξε στο ότι το Bitcoin δεν είναι παράνομο στη χώρα.
 Δημοκρατία της Ρωσίας	Δεν απαιτείται πιστοποίηση για εμπορία Bitcoin στη χώρα αυτή και η εθνική τράπεζα της χώρας δεν μπορεί να απαιτήσει κάτι τέτοιο.
 Κύπρος	Δεν έχει θεσμοθετηθεί νομοθετικό πλαίσιο για το Bitcoin στη συγκεκριμένη χώρα.

Μη ρυθμιζόμενα ψηφιακά νομίσματα

 Δανία	Το Bitcoin δεν θεωρείτε εθνικό νόμισμα, και ως εκ τούτου δεν μπορεί να ρυθμίσει τη χρήση του.
 Εκουαδόρ	Η κυβέρνηση του Εκουαδόρ απαγόρευσε το Bitcoin και τα υπόλοιπα ψηφιακά νομίσματα.
 Εσθονία	Η χρήση του Bitcoin δεν είναι ρυθμισμένη στην Εσθονία και δεν μπορεί να περιοριστεί από την κυβέρνηση.
 Ευρωπαϊκή Ένωση	Κατά τη συγγραφή αυτού του άρθρου δεν υπήρχε κάποια συγκεκριμένη θεσμοθέτηση για το Bitcoin. Πρόσφατα όμως το Bitcoin αναγνωρίστηκε ως το Ευρωπαϊκό Δικαστήριο αποφάσισε πως η μετατροπή από και προς Bitcoin δεν θα φορολογείται.
 Φιλανδία	Η Φιλανδική Κυβέρνηση εξέδωσε πρόσφατα οδηγίες για την φορολόγηση εικονικών νομισμάτων, συμπεριλαμβανομένου και του Bitcoin.
 Γαλλία	Δεν έχει θεσμοθετηθεί νομοθετικό πλαίσιο για το Bitcoin στη συγκεκριμένη χώρα.
G7	Το 2013 το οικονομικό επιτελείο της G7 εξέδωσε την ακόλουθη δήλωση, ως κατευθυντήρια γραμμή που μπορεί να εφαρμοστεί σε επιχειρήσεις που ασχολούνται με τη χρήση Bitcoin και άλλων νομισμάτων, «υπηρεσίες πληρωμών που βασίζονται στο Internet που επιτρέπουν τη χρηματοδότηση τρίτων μερών από ανώνυμες πηγές μπορεί να αντιμετωπίζουν αυξημένο κίνδυνο, χρήματα εσόδων από παράνομες δραστηριότητες ή χρηματοδότησης της τρομοκρατίας.

Μη ρυθμιζόμενα ψηφιακά νομίσματα



Γερμανία

Σύμφωνα με ανακοίνωση που εξέδωσε για το Bitcoin η Ομοσπονδιακή Οικονομική Εποπτική Αρχή στις 19 Δεκεμβρίου 2013, το Bitcoin είναι νομικά δεσμευμένα χρηματοοικονομικά μέσα που εμπίπτουν στην κατηγορία των λογιστικών μονάδων και υπόκεινται στους ανάλογους νόμους του Γερμανικού Δικαίου.



Ελλάδα

Δεν έχει θεσμοθετηθεί νομοθετικό πλαίσιο για το Bitcoin στη συγκεκριμένη χώρα.



Χονγκ-Κονγκ

Στις 8 Ιανουαρίου 2014 ο υπουργός Οικονομικών Υπηρεσιών και το Υπουργείο Οικονομικών απευθύνθηκε στον Συμβούλιο Legislative δηλώνοντας ότι «το Χονγκ Κονγκ προς το παρόν δεν έχει νομοθεσία που να ρυθμίζουν άμεσα θέματα για το Bitcoin και τα άλλα εικονικά νομίσματα παρόμοιου είδους. Ωστόσο, οι υφιστάμενοι νόμοι, όπως το Organised and Serious Crimes διάταγμα, προβλέπουν κυρώσεις κατά παρανόμων ενεργειών που αφορούν Bitcoins, όπως απάτη ή ζέπλυμα χρήματος.



Ισλανδία

Σύμφωνα με τη γνώμη του 2014 από την Κεντρική Τράπεζα της Ισλανδίας: Δεν υπάρχει άδεια για να αγοραστεί ξένο νόμισμα από τα χρηματοπιστωτικά ιδρύματα στην Ισλανδία ή τη μεταφορά σε ξένο νόμισμα κατά μήκος των συνόρων με βάση τις συναλλαγές με το εικονικό νόμισμα. Για το λόγο αυτό και μόνο, οι συναλλαγές με εικονικό νόμισμα υπόκεινται σε περιορισμούς στην Ισλανδία. Αυτό δεν σταματάει επιχειρήσεις στην Ισλανδία από την εξόρυξη Bitcoin.



Ινδία

Στις 28 Δεκεμβρίου 2013, ο Υποδιοικητής της Κεντρικής Τράπεζας της Ινδίας, KK Chakrabarty, δήλωσε ότι η Κεντρική Τράπεζα της Ινδίας δεν είχε σχέδια για τη ρύθμιση Bitcoin.

Μη ρυθμιζόμενα ψηφιακά νομίσματα


Ινδονησία

Στις 6 Φεβρουαρίου 2014, η Τράπεζα της Ινδονησίας εξέδωσε δελτίο Τύπου που σχετίζονται με το Bitcoin δηλώνοντας «Κατά την άποψη του νόμου αριθ 7 Έτος 2012, σχετικά με το νόμισμα και το νόμο αριθ 23 Έτος 1999, η οποία έχει τροποποιηθεί αρκετές φορές, η τελευταία με το νόμο αριθ 6 έτος 2009, η Τράπεζα της Ινδονησίας αναφέρει ότι το Bitcoin και τα άλλα εικονικά νόμισμα δεν είναι το νόμισμα ή νομικό μέσο πληρωμής στην Ινδονησία.


Ιρλανδία

Η Κεντρική Τράπεζα της Ιρλανδίας αναφέρθηκε στη συνέλευση της Ιρλανδίας δηλώνοντας ότι δεν ασκεί ρύθμιση στις συναλλαγές με Bitcoin.


Ισραήλ

Δεν έχει θεσμοθετηθεί νομοθετικό πλαίσιο για το Bitcoin στη συγκεκριμένη χώρα έως τις 23 Δεκεμβρίου 2015.


Ιταλία

Στην Ιταλία δεν υπάρχει ρύθμιση για συναλλαγές από μεμονωμένους ιδιώτες.


Ιαπωνία

Δεν έχει θεσμοθετηθεί νομοθετικό πλαίσιο για το Bitcoin στη συγκεκριμένη χώρα.


Ιορδανία

Η κυβέρνηση της Ιορδανίας έχει εκδώσει μια προειδοποίηση αποθαρρύνοντας τη χρήση Bitcoin και άλλων παρόμοιων συστημάτων.


Κιργιζία

Τον Ιούλιο του 2014, η δήλωση της Εθνικής Τράπεζας της Δημοκρατίας της Κιργισίας κατέστησε σαφές ότι η χρήση των εικονικών νομισμάτων, ιδίως Bitcoin, ως μέσο πληρωμής στη Δημοκρατία της Κιργισίας θα αποτελέσει παραβίαση του νόμου τους κράτους.

Μη ρυθμιζόμενα ψηφιακά νομίσματα

	Η κυβέρνηση της Ιορδανίας έχει εκδώσει μια προειδοποίηση αποθαρρύνοντας τη χρήση Bitcoin και άλλων παρόμοιων συστημάτων.
Λίβανο	
	Η εθνική τράπεζα της Λιθουανίας εξέδωσε προειδοποίηση τη 31η Ιανουαρίου 2014 ότι Bitcoin δεν αναγνωρίζεται ως νόμιμο χρήμα και ότι οι χρήστες Bitcoin θα πρέπει να γνωρίζουν τους υψηλούς κινδύνους που έρχονται με τη χρήση του.
Λιθουανία	
	Η Επιτροπή Εποπτείας του Χρηματοοικονομικού Τομέα έχει εκδώσει μια ανακοίνωση στο Φεβρουάριο του 2014 με την οποία αναγνωρίζει την ιδιότητα του νομίσματος του Bitcoin και των άλλων κρυπτονομισμάτων. Η πρώτη άδεια για Bitcoin εκδόθηκε τον Οκτώβριο του 2015, και η κυβέρνηση στηρίζει ενεργά αυτή η εξέλιξη.
Λουξεμβούργο	
	Δεν έχει θεσμοθετηθεί νομοθετικό πλαίσιο για το Bitcoin στη συγκεκριμένη χώρα.
Μαλαισία	
	Δεν έχει θεσμοθετηθεί νομοθετικό πλαίσιο για το Bitcoin στη συγκεκριμένη χώρα.
Μάλτα	
	Η Τράπεζα Αποθεμάτων της Νέας Ζηλανδίας αναφέρει: "Μη τραπεζικά ιδρύματα δεν χρειάζονται την έγκρισή μας για τα καθεστώτα που σχετίζονται με την αποθήκευση ή τη μεταφορά αξιών, όπως το Bitcoin, εφ' όσον δεν συνεπάγονται την έκδοση της υλικής κυκλοφορίας νομισμάτων, χαρτονομίσματα και κέρματα.
Νέα Ζηλανδία	
	Δεν έχει θεσμοθετηθεί νομοθετικό πλαίσιο για το Bitcoin στη συγκεκριμένη χώρα.
Ολλανδία	

Μη ρυθμιζόμενα ψηφιακά νομίσματα



Νικαράγουα

Η χώρα, σύμφωνα με ανακοίνωση αποδέχεται τις συναλλαγές με Bitcoin.



Νορβηγία

Η νορβηγική Φορολογική Διοίκηση έχει εκδώσει μια δήλωση ότι bitcoins θα πρέπει να αντιμετωπίζονται ως ιδιοκτησία κεφαλαίου για λόγους φορολογικής φύσεως.



Φιλιππίνες

Στις 6 Μαρτίου 2014, η Κεντρικά Τράπεζα των Φιλιππίνων, BSP, εξέδωσε μια δήλωση σχετικά με τους κινδύνους που συνδέονται με την εμπορία και τη χρήση του Bitcoin. Bitcoin ανταλλαγές δεν ρυθμίζονται από το BSP αυτή τη στιγμή.



Πολωνία

Δεν έχει θεσμοθετηθεί νομοθετικό πλαίσιο για το Bitcoin στη συγκεκριμένη χώρα.



Πορτογαλία

Δεν έχει θεσμοθετηθεί νομοθετικό πλαίσιο για το Bitcoin στη συγκεκριμένη χώρα.



Ρωσία

Από τον Ιανουάριο του 2015, ένα νομοσχέδιο που απαγορεύει ρητά τη χρήση ή κατοχή Bitcoins δεν υπάρχει στη Ρωσία, αν και φαίνεται ένα πως μια δεδομένη απαγόρευση κατέχει τη θέση του. Το CNBC ανέφερε ότι Bitcoin ήταν παράνομο στη Ρωσία έως το Δεκέμβριο του 2014, και διάφορες ρωσικές αρχές και οργανισμοί έχουν μιλήσει ή λάβει μέτρα κατά του Bitcoin. Στις αρχές του 2015, ο ρυθμιστής των μέσων ενημέρωσης της Ρωσίας μπλοκάρει αρκετές ιστοσελίδες που σχετίζονται με Bitcoin, το 2015 ένα ρωσικό κρατικό μέσο μαζικής ενημέρωσης ανέφερε ότι "Η Κεντρική Τράπεζα είπε ότι η χρήση του Bitcoin ήταν παράνομη σύμφωνα με νομοθεσία της Ρωσικής Ομοσπονδίας". Το Φεβρουάριο του 2014 στο Γραφείο του ρωσικού Γενικού Εισαγγελέα υπήρχε εισήγηση που όπως αναφέρεται έγραφε: «Διαδικτυακά νομίσματα συμπεριλαμβανομένων των πιο γνωστών, όπως το Bitcoin, είναι υποκατάστατα χρήματος και δεν μπορεί να χρησιμοποιούνται από φυσικά ή

Μη ρυθμιζόμενα ψηφιακά νομίσματα

νομικά πρόσωπα.»



Σιγκαπούρη

Τον Δεκέμβριο του 2013, η Νομισματική Αρχή της Σιγκαπούρης φέρεται να δήλωσε ότι «στις επιχειρήσεις που είτε αποδέχονται τα Bitcoins είτε όχι, σε αντάλλαγμα για τα αγαθά και τις υπηρεσίες τους, θεωρείται μια εμπορική απόφαση στην οποία το MAS δεν παρεμβαίνει».



Σλοβακία

Η Εθνική Τράπεζα της Σλοβακίας (NBS), δήλωσε ότι τα Bitcoin δεν έχουν τα νομικά χαρακτηριστικά ενός νομίσματος, και ως εκ τούτου δεν εμπίπτει υπό εθνικό έλεγχο.



Σλοβενία

Στις 23 Δεκεμβρίου του 2013, το Υπουργείο Οικονομικών της Δημοκρατίας της Σλοβενίας εξέδωσε επίσημη γνώμη σχετικά με την θέση του έναντι του Bitcoin και άλλων εικονικών νομισμάτων σε απάντηση ενός αιτήματος από τη Φορολογική Διοίκηση της Δημοκρατίας της Σλοβενίας. Η γνωμοδότηση αναφέρει ότι το Bitcoin δεν είναι νομισματικό μέσο σλοβενικού δικαίου ούτε θεωρείτε χρηματοπιστωτικό μέσο.



Βόρεια Κορέα

Αν και δεν είναι παράνομο στη χώρα, οι αρχές της Κορέας θα ασκήσουν δίωξη για παράνομη δραστηριότητα σε οποιονδήποτε σχετίζεται με το Bitcoin. Έχουν ήδη απαγγελλεί κατηγορίες, τουλάχιστον σε ένα άτομο για την αγορά φαρμάκων με Bitcoin.



Ισπανία

Δεν έχει θεσμοθετηθεί νομοθετικό πλαίσιο για το Bitcoin στη συγκεκριμένη χώρα.



Σουηδία

Η Σουηδική Φορολογική Υπηρεσία έχει εκδώσει προδικαστική απόφαση περί Φόρου Προστιθέμενης Αξίας (ΦΠΑ) επί των Bitcoins, δηλώνοντας ότι το εμπόριο Bitcoins δεν υπόκειται σε σουηδικό ΦΠΑ, αλλά, αντιθέτως, με την επιφύλαξη των κανονισμών της Οικονομικής Εποπτικής Αρχής αντιμετωπίζονται ως νόμισμα. Στην απόφαση αυτή έχει ασκηθεί έφεση από την σουηδική φορολογική υπηρεσία.

Μη ρυθμιζόμενα ψηφιακά νομίσματα



Σουηδία

Οι Bitcoin επιχειρήσεις στην Ελβετία υπόκεινται σε νομιμοποίηση εσόδων από παράνομες δραστηριότητες και τους κανονισμούς σε ορισμένες περιπτώσεις που κάποιος μπορεί να χρειαστεί να λάβει τραπεζική άδεια



Ταϊβάν

Τα ATM για Bitcoin έχουν απαγορευτεί στην Ταϊβάν αν και μέσα από μια περίπλοκη διαδικασία, τα Bitcoins μπορούν να αγοραστούν σε μερικά καταστήματα, όπως τα περίπτερα που πωλούν επίσης εισιτήρια τρένων και θα τους επιτρέψει να πληρώνουν τους λογαριασμούς.



Ταϊλάνδη

Η Τράπεζα της Ταϊλάνδης κήρυξε το Bitcoin παράνομο το 2013, αλλά ορισμένες εταιρείες Bitcoin έχουν τη δυνατότητα να αποκτήσουν άδειες για τις επιχειρήσεις τους. Μια άρνηση άδειας εκκίνησης άσκησης επιχειρηματικής δραστηριότητας, έφερε τον υποψήφιο επιχειρηματία να δηλώσει «η αγορά και η πώληση Bitcoins, ή η χρήση Bitcoins για να αγοράσει ή να πωλήσει κανείς αγαθά και υπηρεσίες, και τη μεταφορά Bitcoins μέσα και έξω από την Ταϊλάνδη, πρακτικά σήμερα θεωρούνται όλες παράνομες»



Τουρκία

Δεν έχει θεσμοθετηθεί νομοθετικό πλαίσιο για το Bitcoin στη συγκεκριμένη χώρα.



Ηνωμένο Βασίλειο

Η κυβέρνηση του Ηνωμένου Βασιλείου έχει δηλώσει ότι το Bitcoin είναι χωρίς καθορισμένες αρχές.



Ηνωμένες

Το Υπουργείο Οικονομικών των ΗΠΑ κατατάσσει το Bitcoin ως μετατρέψιμο αποκεντρωμένο εικονικό νόμισμα το 2013.

Μη ρυθμιζόμενα ψηφιακά νομίσματα

Πολιτείες	
	Βιετνάμ
	Παρόλο που η εμπορία σε Bitcoin είναι παράνομη σε αυτή τη χώρα, σύμφωνα με μια δήλωση που κυκλοφόρησε από την κρατική τράπεζα του Βιετνάμ, τον Φεβρουάριο του 2014, αλλά και μέχρι τώρα συναλλαγές σε Bitcoin στο Βιετνάμ εξακολουθούν να είναι νόμιμες και δεν περιορίζονται από το νόμο. Δύο μεγάλες αγορές Bitcoin στο Βιετνάμ η VBTC και η Bitcoin Βιετνάμ επιτελούν αυτή τη στιγμή εργασία χωρίς κανένα απολύτως πρόβλημα.

Πίνακας 5.1: Η ισχύουσα νομοθεσία για τα κρυπτονομίσματα, πηγή Wikipedia.

Ως ένα γενικό σχόλιο το οποίο παρατηρείται μελετώντας τη νομοθεσία ανά χώρα, είναι ότι η νομοθεσία είναι αρκετά ρευστή και αρκετές ανεπτυγμένες χώρες δεν έχουν ακόμα κάποιο νομοθετικό πλαίσιο. Από την άλλη μεριά οι συντηρητικές χώρες απλά απαγορεύουν οποιαδήποτε χρήση του.

Δεν αποτελεί καθόλου απλή υπόθεση η θεσμοθέτηση νόμων για το Bitcoin, καθώς αποτελεί μια αρκετά νεαρή «δημιουργία» και το κάθε κράτος θα πρέπει να λάβει μέτρα τα οποία θα προστατεύουν τους πολίτες από κακόβουλες ενέργειες, αλλά και το ίδιο το κράτος από επιχειρήσεις η μεμονωμένους χρήστες οι οποίοι έχουν ως σκοπό τη μετακίνηση η διαχείριση χρημάτων τα οποία έχουν αποκτηθεί με παράνομο τρόπο.

Όπως παραθέσαμε και νωρίτερα, υπάρχουν αρκετά παραδείγματα πολιτών οι οποίοι κινήθηκαν δικαστικά για να δικαιωθούν, γιατί είχαν πρόβλημα με τη χρήση η ανταλλαγή Bitcoin.

Μη ρυθμιζόμενα ψηφιακά νομίσματα

Επίλογος

Ο σκοπός μας σε αυτή τη διπλωματική ήτα η μελέτη ενός κρυπτονομίσματος, ονόματι Bitcoin. Αρχικός σκοπός ήταν η ολοκλήρωση της διαδικασίας υλοποιώντας και εξόρυξη του Bitcoin χρησιμοποιώντας κατάλληλο λογισμικό και αξιοποιώντας την υπολογιστική ισχύ του server του τμήματος. Δυστυχώς τελικά δεν μπορέσαμε να φτάσουμε σε αυτό το βήμα, οπότε περιοριστήκαμε στην μελέτη του Bitcoin. [36]

Ασχοληθήκαμε με θέματα που αφορούσαν τη γενική περιγραφή, την εξόρυξη, τις εφαρμογές, τα νομικά θέματα και κάποιες ήδη υλοποιημένες εφαρμογές. Η συγγραφή μας έδωσε κίνητρο να ασχοληθούμε με ένα άκρως επίκαιρο και δυναμικό θέμα, το οποίο προσελκύει καθημερινά όλο και περισσότερους ενδιαφερόμενους.

Είναι λοιπόν σίγουρο ότι στο μέλλον έχουμε να παρατηρήσουμε πολλές αλλαγές όσον αφορά τον τρόπο υλοποίησης των συναλλαγών μας.

Μη ρυθμιζόμενα ψηφιακά νομίσματα

Βιβλιογραφία

- [1] A. Antonopoulos, *Mastering Bitcoin*. O'Reilly Media, 2015.
- [2] E. Παπαευθυμίου, “Σύντομη αναδρομή στην ιστορία του νομίσματος και της αρχαίας οικονομίας.” http://e-domisi.gr/index.php?option=com_content&view=article&id=708:2011-05-29-16-29-48&catid=93:2010-09-14-08-07-10&Itemid=116. [Accessed: 09-Nov-2015].
- [3] S. F. R. Dornbusch, “Η Κεντρική Τράπεζα, το χρήμα και οι πιστώσεις,” 1990. .
- [4] “Bitcoin-block-signing History,” 2014. <http://blockchain.info>.
- [5] J. Matonis, “How Cryptocurrencies Could Upend Banks’ Monetary Role,” 2013. <http://www.americanbanker.com/bankthink/how-cryptocurrencies-could-upend-banks-monetary-role-1057597-1.html>.
- [6] “Listing of active coins,” 2014. <http://cryptocoincharts.info/>.
- [7] Shatoshi Nakamoto, “No Title,” 2007. historyofbitcoin.org.
- [8] “Wikipedia,” 2015. https://en.wikipedia.org/wiki/Satoshi_Nakamoto#Dorian_Nakamoto.
- [9] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” *Consulted*, pp. 1–9, 2008.
- [10] “Blockexplorer,” 2015. <https://blockexplorer.com/>.
- [11] Γ. ΓΕΩΡΓΙΟΣ and Μ. ΑΓΓΕΛΟΣ, “‘Bitcoin’ TO NEO ΝΟΜΙΣΜΑ;,” p. 81, 2014.
- [12] “Bitcoin Community,” 2015. <http://www.bitcoincommunity.gr/index.php/el/>.
- [13] J. Weinstein and P. Murck, “Bitcoin: Virtual Currency , Real Risks ... and Real Opportunities,” 2014.
- [14] European Parliament Reserach Service, “Bitcoin Market , economics and regulation,” pp. 1–9, 2014.
- [15] “CoinDesk,” 2015. https://www.google.gr/search?q=cloud+mining&ie=utf-8&oe=utf-8&gws_rd=cr&ei=P8NBVqWYG4q8ygOH4KrQDw.

Μη ρυθμιζόμενα ψηφιακά νομίσματα

- [16] I. Alqassem and D. Svetinovic, “Towards reference architecture for cryptocurrencies: Bitcoin architectural analysis,” *Proc. - 2014 IEEE Int. Conf. Internet Things, iThings 2014, 2014 IEEE Int. Conf. Green Comput. Commun. GreenCom 2014 2014 IEEE Int. Conf. Cyber-Physical-Social Comput. CPS 20*, no. iThings, pp. 436–443, 2014.
- [17] “Wikipedia - DeepBit,” 2011. <https://en.bitcoin.it/wiki/DeepBit>.
- [18] “BitcoinCZ,” 2010.
- [19] “Ozcoin,” 2011. <http://ozco.in/>.
- [20] “EclipseMC,” 2012. <https://eclipsemc.com/>.
- [21] “BitMinter,” 2011. <https://bitminter.com/>.
- [22] “P2Pool,” 2015. <http://p2pool.org/>.
- [23] “Wikipedia - Bitcoin,” 2011. <https://el.wikipedia.org/wiki/Bitcoin>.
- [24] “BTCGreece,” 2014. <https://www.btcgreece.com/>.
- [25] “Bit Stamp,” 2012. <https://www.bitstamp.net/>.
- [26] J. Powell, “Kraken,” 2013. <https://www.bitstamp.net/>.
- [27] J. Bonneau, J. A. Kroll, and E. W. Felten, “Research Perspectives and Challenges for Bitcoin and Cryptocurrencies.”
- [28] J. (Stanford U. Bonneau, A. (University of M. Miller, J. (Concordia U. Clark, A. (Princeton U. Narayanan, J. (Princeton U. Kroll, and E. (Princeton U. Felten, “SoK : Research Perspectives and Challenges for Bitcoin and Cryptocurrencies,” 2015.
- [29] “Wikipedia - Server,” 2012. <https://el.wikipedia.org/wiki/%CE%95%CE%BE%CF%85%CF%80%CE%B7%CF%81%CE%B5%CF%84%CE%B7%CF%84%CE%AE%CF%82>.
- [30] J. CAMPANELLA, “No Title,” 2014.
- [31] “How to Set Up a Bitcoin Miner,” 2013. .

Μη ρυθμιζόμενα ψηφιακά νομίσματα

- [32] S. Barber, X. Boyen, E. Shi, and E. Uzun, “Bitter to better - How to make bitcoin a better currency,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 7397 LNCS, pp. 399–414, 2012.
- [33] “Ισοτιμία.”
[https://el.wikipedia.org/wiki/%CE%99%CF%83%CE%BF%CF%84%CE%B9%CE%BC%CE%AF%CE%B1_\(%CE%BF%CE%B9%CE%BA%CE%BF%CE%BD%CE%BF%CE%BC%CE%AF%CE%B1\)](https://el.wikipedia.org/wiki/%CE%99%CF%83%CE%BF%CF%84%CE%B9%CE%BC%CE%AF%CE%B1_(%CE%BF%CE%B9%CE%BA%CE%BF%CE%BD%CE%BF%CE%BC%CE%AF%CE%B1)).
- [34] “Bitcoin Και Συναλλαγματικές Ισοτιμίες.” <http://www.bitcoin-gr.org/?p=3319>.
- [35] “Wikipedia - Legality of bitcoin by country,” 2015.
https://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country.
- [36] S. Challenges and M. A. Zahid, “Bitcoins : and Future of This Currency,” p. 5, 2014.