ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ
ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ & ΗΛΕΚΤΡΟΝΙΚΩΝ ΜΗΧΑΝΙΚΩΝ

Διπλωματική Εργασία

ΝΕΑ ΕΡΓΑΛΕΙΑ ΚΑΙ ΕΞΕΛΙΞΕΙΣ ΣΤΙΣ ΣΥΝΑΛΛΑΚΤΙΚΕΣ ΣΥΝΗΘΕΙΕΣ ΤΩΝ ΠΟΛΙΤΩΝ

Φοιτητής: Μπιτζής Μάριος
ΑΜ: 46365

Επιβλέπων Καθηγητής: ΠΑΤΣΗΣ ΓΕΩΡΓΙΟΣ

ΑΘΗΝΑ-ΑΙΓΑΛΕΩ ΙΟΥΛΙΟΣ 2022

UNIVERSITY OF WEST ATTICA
FACULTY OF ENGINEERING
DEPARTMENT OF ELECTRICAL & ELECTRONICS ENGINEERING

Diploma Thesis

NEW TOOLS AND DEVELOPMENTS IN CITIZEN'S TRADING HABITS

Student: BITZIS MARIOS
Registration Number: 46365

Supervisor

PROFESSOR: PATSIS GEORGIOS

ATHENS-EGALEO, JULY 2022

Η Διπλωματική Εργασία έγινε αποδεκτή και βαθμολογήθηκε από την εξής τριμελή επιτροπή:

Γεώργιος Πάτσης, Καθηγητής	Ευάγγελος Βαλαμόντες Καθηγητής	Διονύσης Κανδρής Καθηγητής
Digitally signed by GEORGIOS PATSIS Date: 2022.07.18 11:28:54 +03'00' (Υπογραφή)	Evangelos Valamontes Digitally signed by Evangelos Valamontes Date: 2022.07.18 23:09:28 +03'00' (Υπογραφή)	Dionisis Kandris Digitally signed by Dionisis Kandris Date: 2022.07.18 11:45:37 +03'00' (Υπογραφή)

ΔΗΛΩΣΗ ΠΕΡΙ ΠΝΕΥΜΑΤΙΚΩΝ ΔΙΚΑΙΩΜΑΤΩΝ ΚΑΙ ΛΟΓΟΚΛΟΠΗΣ

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, δηλώνω ενυπόγραφα ότι η παρούσα εργασία προετοιμάστηκε και ολοκληρώθηκε από εμένα αποκλειστικά και ότι είμαι ο αποκλειστικός συγγραφέας του κειμένου της.

Η εργασία μου δεν προσβάλλει οποιασδήποτε μορφής δικαιώματα πνευματικής ιδιοκτησίας, προσωπικότητας ή προσωπικών δεδομένων τρίτων, δεν περιέχει έργα/εισφορές τρίτων για τα οποία απαιτείται άδεια των δημιουργών/δικαιούχων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής ή λογοκλοπής.

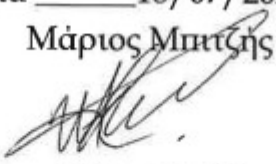
Κάθε βοήθεια που έλαβα για την ολοκλήρωση της εργασίας είναι αναγνωρισμένη και αναφέρεται λεπτομερώς στο κείμενό της. Ειδικότερα, έχω αναφέρει ευδιάκριτα μέσα στο κείμενο και με την κατάλληλη παραπομπή όλες τις πηγές δεδομένων, κώδικα προγραμματισμού Η/Υ, απόψεων, θέσεων και προτάσεων, ιδεών και λεκτικών αναφορών που χρησιμοποιήθηκαν, είτε κατά κυριολεξία είτε βάσει επιστημονικής παράφρασης, και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη

περιγραφή. Επιπλέον, όλες οι πηγές που χρησιμοποιήθηκαν περιορίζονται στις βιβλιογραφικές αναφορές και μόνον και πληρούν τους κανόνες της επιστημονικής παράθεσης κατά τα διεθνή πρότυπα.

Τέλος δηλώνω ενυπόγραφα ότι αναλαμβάνω πλήρως, ατομικά και προσωπικά, όλες τις νομικές και διοικητικές συνέπειες στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της είναι προϊόν λογοκλοπής.

Ημερομηνία _____18/07/2022_____

Μάριος Μπιτζής



(Υπογραφή)

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να εκφράσω τις θερμές ευχαριστίες μου στον καθηγητή και επιβλέποντα της Διπλωματικής μου κύριο Γεώργιο Πάτση για την στήριξη, την παρότρυνση, την καθοδήγηση και τις παρατηρήσεις του επι της οργάνωσης, του περιεχομένου και της δομής της παρούσας εργασίας. Τέλος, θέλω να ευχαριστήσω από καρδίας την οικογένεια μου, τους φίλους μου, τους συνεργάτες μου και την προϊστάμενη μου για την υπομονή, την ενθάρρυνση αλλά και την στήριξη τους όλο αυτόν τον χρόνο.

Περίληψη

Η πρώτη αναφορά ενός προϊόντος που ονομάζεται bitcoin ήταν τον Αύγουστο του 2008, όταν δυο προγραμματιστές που χρησιμοποίησαν τα ονόματα Satoshi Nakamoto και Martti Malmi κατέγραψαν έναν νέο τομέα, το bitcoin.org. Τον Οκτώβριο του ιδίου έτους ο Nakamoto δημοσίευσε ένα έγγραφο, το οποίο ονομάστηκε Λευκή Βίβλος με θέμα ένα ηλεκτρονικό σύστημα μετρητών peer-to-peer. Στόχος της εργασίας είναι η πλήρης κατανόηση του ψηφιακού νομίσματος αλλά και η ανάλυση των δυνατοτήτων που δημιουργούνται μέσα από αυτό. Στο πλαίσιο της εργασίας, το ερευνητικό σχέδιο περιλαμβάνει ανάλυση του περιβάλλοντος των κρυπτονομισμάτων και των υπηρεσιών που μέσω αυτών παρουσιάζονται και οι διάφοροι μέθοδοι αποθήκευσης και υλοποίησης στρατηγικής. Επιπλέον στην εργασία εμπεριέχεται η παρουσίαση και η ανάλυση του ερωτηματολογίου που είχε αποδέκτες ανθρώπους διάφορων ηλικιών και ξεχωριστών επαγγελματικών ενδιαφερόντων.

Λέξεις – κλειδιά

Κρυπτονόμισμα, bitcoin, blockchain, εξόρυξη, συναλλαγές, πορτοφόλι, blowfish, cipher block chaining

Abstract

The first mention of a product called bitcoin was in August 2008, when two developers using the name Satoshi Nakamoto and Martti Malmi patented a new domain, bitcoin.org. In October of that year, Nakamoto published a paper called the White Paper on an electronic peer-to-peer cash system. The aim of the work is the full understanding of the digital currency but also the analysis of the possibilities created through it. As part of the work, the research project includes an analysis of the environment of cryptocurrencies and the services through which the various methods of storage and implementation are presented. In addition, the work includes the presentation and analysis of the questionnaire that was addressed to people of different ages and different professional interests.

Keywords

Transactions, Wallet, Mining, Bitcoin, Blockchain, Cryptocurrency

Περιεχόμενα

Κατάλογος Διαγραμμάτων

Κατάλογος Εικόνων

Αλφαβητικό Ευρετήριο

Ledger: Αρχείο υπολογιστή για την καταγραφή οικονομικών συναλλαγών

Peer-to-peer: Λειτουργικό σύστημα που επιτρέπει σε κάθε άτομο να αλληλοεπιδρά άμεσα με τα υπόλοιπα

MIT / X11: Άδεια λογισμικού

Cold storage: Τρόπος αποθήκευσης που χρησιμοποιείται για πορτοφόλια εκτός σύνδεσης.

Hackable: Δυνατότητα ηλεκτρονικής εισβολής ή πρόσβασης χωρίς άδεια

Txid: Κατακερματισμός συναλλαγών

Hash: Δείκτης μέτρησης κατακερματισμού

Hash rate: Ποσοστό κατακερματισμού

Mining: Εξόρυξη

Blockchain: Δημόσιο αρχείο συναλλαγών Bitcoin

Btc: Κοινή μονάδα που χρησιμοποιείται για τον προσδιορισμό ενός bitcoin

Private Key: Μυστικό κομμάτι των δεδομένων που αποδεικνύει το δικαίωμα σας να περάσετε bitcoins από ένα συγκεκριμένο πορτοφόλι

Wallet: Πορτοφόλι Bitcoin είναι αντίστοιχο ενός φυσικού πορτοφολιού στο δίκτυο bitcoin.

Blowfish: Συμμετρικός αλγόριθμος κρυπτογράφησης που χρησιμοποιεί το ίδιο μυστικό κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση.

Cipher block chaining: Τρόπος λειτουργίας για ένα μπλοκ αποκρυπτογράφησης.

Feistel cipher: Συμμετρική δομή που χρησιμοποιείται για την κατασκευή blockchain.

Indicators: Τεχνικοί Δείκτες (SMA, EMA, RSI,)

Pair: Εμπορεύσιμο ζεύγος, συνήθως σε μορφή **Base/Quote (XRP/USDT)**

Limit Order: Οριακές Εντολές που εκτελούνται στην καθορισμένη τιμή ορίου ή καλύτερη.

Market Order: Εγγυημένη πληρωμή, ενδέχεται να μετακινηθεί η τιμή ανάλογα με το μέγεθος της παραγγελίας.

ΕΙΣΑΓΩΓΗ

Ως κρυπτονόμισμα ορίζεται ένα αποκεντρωμένο σύστημα χωρίς κεντρική εξουσία, το οποίο χρησιμοποιεί κρυπτογραφία για τον έλεγχο κάθε συναλλαγής. Όλες οι συναλλαγές αποθηκεύονται ψηφιακά και καταγράφονται στο λογισμικό σύστημα των κρυπτονομισμάτων. Η έννοια του κρυπτονομίσματος αναδύθηκε πρώτη φορά το 2009 καθώς το bitcoin έγινε το πρώτο αποκεντρωμένο κρυπτονόμισμα.

Τα τελευταία χρονιά, το bitcoin και άλλες μορφές ψηφιακών νομισμάτων αναπτύσσονται μανιωδώς στην οικονομία ,θέτοντας έτσι τον καθένα από εμάς να αναρωτιέται το προφίλ και τις δυνατότητες, θετικές ή αρνητικές, αυτού του ψηφιακού νομίσματος. Στην δραματικά εξελισσόμενη περίοδο στην οποία ζούμε και δραστηριοποιούμαστε, όλες μας οι σταθερές επαναξιολογούνται, εξελίσσονται ή καταρρίπτονται. Στο πλαίσιο αυτό ετούτη η εργασία πραγματεύεται μια από τις μεγαλύτερες σύγχρονες προκλήσεις, την ριζική διαφοροποίηση της λειτουργίας του τρόπου με τον οποίο συναλλασσόμαστε. Μια νέα δυναμική αναδεικνύεται, που ο χρόνος μόνο θα δείξει αν θα εξελιχθεί ή θα απορριφθεί, στην οποία τα φυσικά χρήματα ή και οι τράπεζες, τουλάχιστον με την μορφή που τα ξέρουμε, δεν θα υπάρχουν. Το τραπεζικό σύστημα που στην τρέχουσα έκφραση του λειτουργεί περί τα 500 χρονιά καλείται να προσαρμοστεί ή να αποτελέσει είδος προς εξαφάνιση .

Οι κύριοι στόχοι ετούτης της εργασίας δεν είναι μόνο η κατανόηση ενός «ξένου» νομίσματος που βρίσκεται μόνο σε ηλεκτρονική μορφή και έχει ξεκινήσει να απασχολεί από τους απλούς ανθρώπους μέχρι και ολόκληρες κυβερνήσεις αλλά η προσπάθεια του κάθε χρήστη που θα ξεκινήσει την διαδικασία της εξόρυξης και την ολοκληρωμένη λειτουργία όλου του συστήματος που κρύβεται πίσω από αυτό που λέμε κρυπτονόμισμα.

Μετα την εισαγωγή, το ερευνητικό σχέδιο εξελίσσεται ως εξής :

Στο Κεφάλαιο 1 παρουσιάζεται η οπτική του χρήματος.

Στο Κεφάλαιο 2 αναλύεται η έννοια του ψηφιακού χρήματος.

Στο Κεφάλαιο 3 αναλύεται το περιβάλλον των υπηρεσιών του bitcoin.

Στο Κεφάλαιο 4 παρουσιάζονται οι μέθοδοι απόκτησης του bitcoin.

Στο Κεφάλαιο 5 παρουσιάζονται οι μέθοδοι αποθήκευσης του bitcoin.

Στο Κεφάλαιο 6 παρουσιάζονται οι τρόποι συναλλαγών του bitcoin.

Στο Κεφάλαιο 7 αναλύεται το σύστημα της εξόρυξης.

Στο Κεφάλαιο 8 παρουσιάζεται αναλυτικά η στρατηγική κέρδους του bitcoin μέσω ενός αλγορίθμου χαρτογράφησης.

Το ερευνητικό σχέδιο ολοκληρώνεται στο Κεφάλαιο 9, με την παρουσίαση και την ανάλυση της ερευνάς που πραγματοποιήθηκε.

ΚΕΦΑΛΑΙΟ 1ο : Η Οπτική του Χρήματος

Το χρήμα είναι οποιοδήποτε αντικείμενο που χρησιμοποιείται από μια κοινωνία ως υποκατάστατο αξίας, μέσο ανταλλαγής και μονάδα υπολογισμού. Η αξία των χρημάτων προκύπτει κατά ένα μέρος από την χρησιμότητα του ως μέσο ανταλλαγής εντούτοις εξαρτάται από την αναγνώριση της αγοραστικής του αξίας, επομένως αυτές οι δυο πτυχές των χρημάτων είναι αλληλεξαρτώμενες. Η έννοια του χρήματος άρχισε να εξελίσσεται ακόμα περισσότερο όταν οι άνθρωποι αποφάσισαν να αντικαταστήσουν τα κοχύλια και να χρησιμοποιούν τα μέταλλα ως μέσο ανταλλαγής τους . Η αρχή για την δημιουργία των πρώτων νομισμάτων ήταν πριν 2600 χρόνια στην περιοχή της Μικράς Ασίας. Με την ανάπτυξη του εμπορίου η ανάγκη για περισσότερα χρήματα ως ανταλλακτικό μέσο αυξήθηκε έτσι οι τράπεζες και οι κυβερνήσεις αρχίσαν να εκδίδουν χαρτονομίσματα. (Χρήμα, 2020) Τα πρώτα χαρτονομίσματα εκδοθήκαν το 900 μ.Χ. στην Κίνα , για να φτάσουμε μέχρι την σημερινή εποχή οπού το 1995 δημιουργείται το ηλεκτρονικό χρήμα. Στην σημερινή εποχή έχουμε διάφορες μορφές του χρήματος καθώς με την πάροδο του χρόνου και την εξέλιξη της τεχνολογίας οι απαιτήσεις της κοινωνίας ανάγκασαν να δημιουργηθούν και αλλά είδη χρήματος με σκοπό την διευκόλυνση των συναλλαγών μας. Αναλυτικά τα είδη του χρήματος είναι :

1. **Μεταλλικό χρήμα & χαρτονόμισμα**: Είναι η κοινή μορφή χρήματος τα γνωστά μας κέρματα - νομίσματα που χρησιμοποιούμε με χαρακτηριστικό ότι δεν αλλοιώνονται εύκολα, είναι ομοιογενή και διαιρετά. Τα χαρτονομίσματα επίσης χρησιμοποιούνται πολύ και εκδίδονται από τράπεζες. Και οι δυο μορφές ανήκουν στο παραστατικό χρήμα, δηλαδή η αναγραφόμενη αξία αντιστοιχεί σε τιμή μεγαλύτερη από την αξία του υλικού που το αποτελεί.

2. Πιστωτικό Χρήμα: Το πιστωτικό χρήμα έχει δυο μορφές την επιταγή και την συναλλαγματική επιταγή. Η επιταγή ουσιαστικά είναι μια εντολή σε μια τράπεζα για την εξαργύρωση του ποσού που αναγράφετε πάνω της με την προϋπόθεση ότι το ποσό είναι διαθέσιμο στον τραπεζικό λογαριασμό. Η συναλλαγματική επιταγή είναι μια υπόσχεση πληρωμής στο μέλλον την συγκεκριμένη ημερομηνία.

3. Πιστωτικές Κάρτες: Είναι το "πλαστικό χρήμα", δηλαδή οι κλασσικές κάρτες που εκδίδονται από τις τράπεζες και χρησιμοποιούνται για την αγορά προϊόντων.

4. Ψηφιακό Χρήμα: Είναι η πιο σύγχρονη κατά σειρά μορφή χρήματος καθώς μπήκε στις ζωές μας τα τελευταία χρόνια. Τα κρυπτονομίσματα είναι εικονικά χρήματα που δημιουργούνται από μαθηματικούς αλγορίθμους και έχουν πολλά πλεονεκτήματα λόγω της ανεξαρτησίας που διαθέτουν. Μερικά από τα πιο γνωστά ψηφιακά νομίσματα είναι τα εξής : bitcoin, Ripple, Litecoin, altcoin. (money, 2020)

ΚΕΦΑΛΑΙΟ 2ο : Η Έννοια του Ψηφιακού Νομίσματος

Η έννοια του ψηφιακού νομίσματος ξεκίνησε το έτος 1998 σαν μια ιδέα του Wei Dai που δημοσιεύτηκε στην λίστα αλληλογραφίας Cypherpunks, όπου αναφερόταν στην ιδέα ενός νέου χρήματος που χρησιμοποιούσε κρυπτογραφία για να ελέγξει τις συναλλαγές και αυτός ήταν ο λόγος που ονομάστηκε μετέπειτα κρυπτονόμισμα. Μετά από δέκα χρόνια , το 2008 , ο Satoshi Nakamoto δημοσιεύει στην ίδια λίστα αλληλογραφίας ένα έγγραφο το οποίο το ονόμασε «A Peer-to-Peer Electronic Cash System». Μετά από αυτή την δημοσίευση, το κρυπτονόμισμα 'Bitcoin' έχει πάρει μια υπερβολικά ανοδική πορεία μέσα στα χρόνια, η οποία βέβαια είχε πολλά σκαμπανεβάσματα μέχρι σήμερα στην χρηματιστηριακή του πορεία. Ένα τρανό παράδειγμα ήταν το 2009 που ένα προγραμματιστικό σφάλμα επέτρεψε την δημιουργία απεριορίστων bitcoins και αυτό είχε σαν αποτέλεσμα να το εκμεταλλευτούν κάποιοι κακόβουλοι hackers και να κλέψουν κάποια από αυτά τα bitcoins. Εκτός από το Bitcoin, μέσα στα χρόνια, δημιουργήθηκαν και άλλα κρυπτονομίσματα τα οποία είναι τα εξής :

RIPPLE

Αποτελεί το μοναδικό κρυπτονόμισμα που δεν βασίζεται στην τεχνολογία Blockchain , αλλά σε ένα διεθνές συναινετικό βιβλίο. Το πρωτόκολλο Ripple χρησιμοποιείται από θεσμικούς φορείς , όπως οι μεγάλες τράπεζες και οι επιχειρήσεις παροχής υπηρεσιών χρήματος .

LITECOIN

Το LITECOIN ξεκίνησε το 2011 και θεωρείται ως άμεσα ανταγωνιστικό του Bitcoin. Πρόκειται για λογισμικό κρυπτογράφησης ανοιχτού κώδικα που εκχωρείται υπό την άδεια MIT / X11. Η δημιουργία και η μεταφορά νομισμάτων βασίζεται σε κρυπτογραφικό πρωτόκολλο ανοιχτής πηγής και δεν διαχειρίζεται από καμία κεντρική αρχή.

DASH

Πρόκειται για κρυπτονόμισμα που βασίζεται στην προστασία του ιδιωτικού απορρήτου. Οι ανταλλαγές DASH κατανέμονται μεταξύ των miners και των πελατών με το 10% των εσόδων να διατίθενται στην χρηματοδότηση της ανάπτυξης του κρυπτονομίσματος. (econinfosec, 2020)

Εικόνα 1:Η δημιουργία του 1ου Ψηφιακού Νομίσματος

Πηγή : Ιδία Επεξεργασία

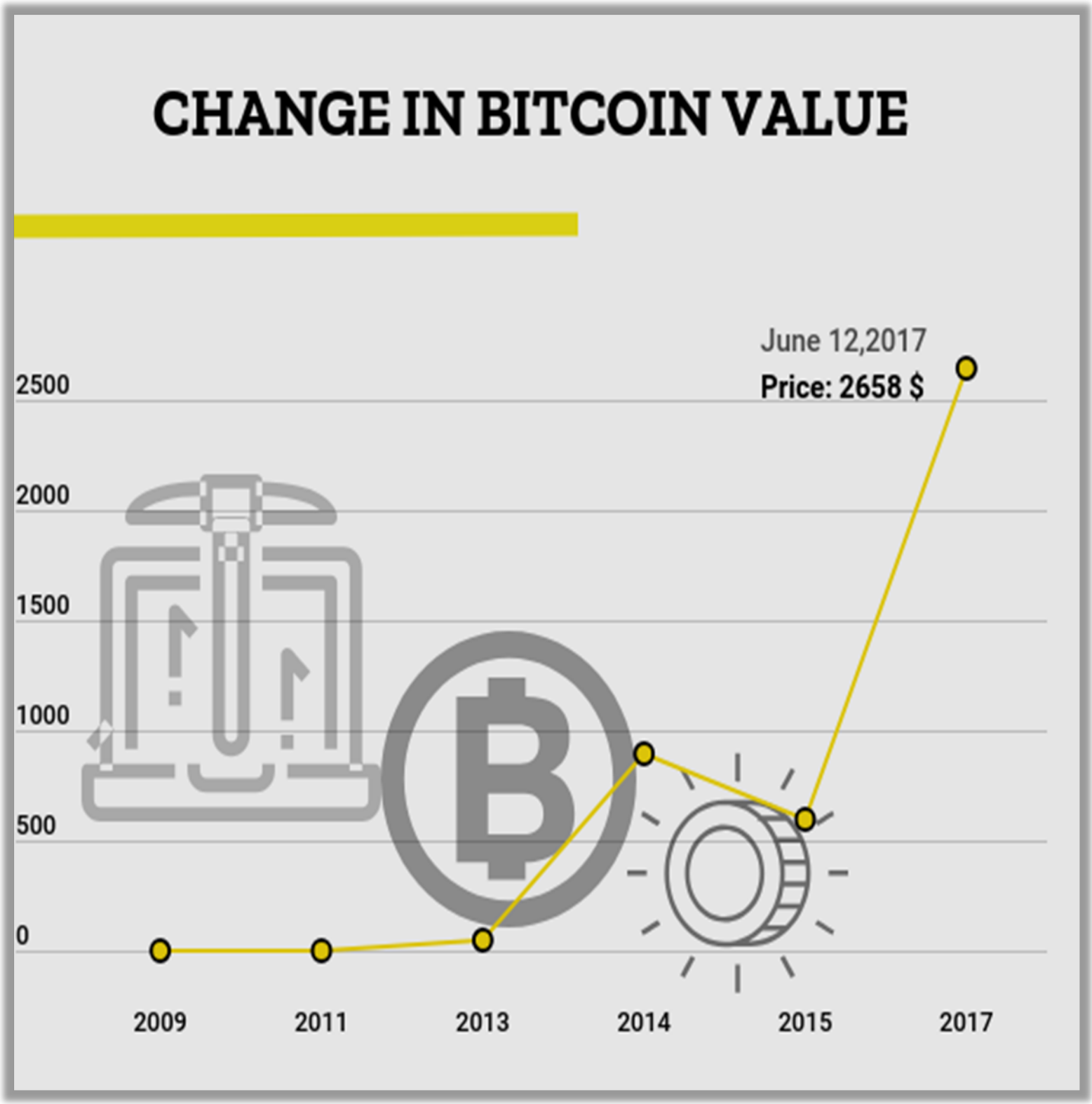
Χρονικά θα αναφέρουμε κάποια από τα σημαντικότερα γεγονότα (με την βοήθεια εικόνων) που έχουν καταγραφεί από την δημιουργία του bitcoin έως σήμερα:

Εικόνα 2:Η Ιστορία του Bitcoin

Πηγή : Ιδία Επεξεργασία

2.1 Ο στόχος του Bitcoin

Το ψηφιακό κρυπτονόμισμα είναι ένας εικονικός τρόπος συναλλαγής, με αλλά λόγια ένα νομισματικό σύστημα. Τα βασικά του στοιχεία είναι ότι προσφέρει σταθερότητα, ανωνυμία και ασφάλεια. Για να πραγματοποιηθεί αυτό, το σύστημα λειτουργεί με δυο παράγοντες: τις δημόσιες καταχωρήσεις και την κρυπτογράφηση. Οι δημόσιες καταχωρήσεις αποθηκεύονται σε έναν κατάλογο και οποιοσδήποτε μπορεί να δει αναλυτικά τα στοιχεία των συναλλαγών. Επιπλέον η κρυπτογραφία είναι επιστήμη των μεθόδων κρυπτογράφησης των δεδομένων και δυο στόχοι για την χρησιμοποίηση της. Ο πιο σημαντικός είναι να αποστέλλονται μηνύματα με ασφάλεια, εμπιστοσύνη και ανωνυμία. Ο δεύτερος στόχος είναι για την επίλυση πολλών ποικίλων προβλημάτων στον τομέα της αυθεντικότητας, ασφάλειας και εγκυρότητας των δεδομένων. Το κρυπτονόμισμα θα λέγαμε ότι αποτελείται από τεχνολογίες και θεωρίες που είχαν ειπωθεί όλα αυτά τα χρόνια πολύ πριν την δημιουργία του. Ο κύριος σκοπός του είναι η ανάπτυξη ενός συστήματος εικονικού χαρτονομίσματος το οποίο θα έχει την ικανότητα να αντέχει σε διάφορες «εξωτερικές» επιθέσεις, να προσδίδει ασφάλεια και πάνω από όλα νομιμότητα και αξιοπιστία. Πριν την δημιουργία του κρυπτονομίσματος είχαν γίνει πολλές προσπάθειες ενός τέτοιου νομίσματος, το οποίο θα αποτελούνταν από κρυπτογραφικά πρωτοκολλά αλλά η πρώτη επιτυχημένη προσπάθεια έγινε όπως προαναφέρθηκε το 2008 από τον Satoshi Nakamoto με την δημιουργία του bitcoin. Ταυτόχρονα δημιουργήθηκαν και άλλα κρυπτονομίσματα, τα διασημότερα εκ των οποίων ήταν το Litecoin, dogecoin, ripple και altcoins, τα οποία ουσιαστικά ήταν αντίγραφα του bitcoin με κάποιες τροποποιήσεις ή διαφορετικά με κάποια τεχνολογικά πλεονεκτήματα τα οποία τα καθιστούσαν ξεχωριστά σε διαφορετικούς τομείς.



Εικόνα 3:Η χρηματιστηριακή αξία του bitcoin μέσα στα χρόνια
Πηγή : Ιδία Επεξεργασία

ΚΕΦΑΛΑΙΟ 3 : Το Περιβάλλον των υπηρεσιών του Bitcoin

Το Bitcoin είναι ένα αποκεντρωμένο ψηφιακό σύστημα χρήματος που χρησιμοποιεί peer-to-peer συνδέσεις μαζί με ψηφιακές υπογραφές και κρυπτογράφηση, καθώς δεν υπάρχει κάποιος server ή κάποιο σημείο ελέγχου, για να δημιουργήσει ουσιαστικά μια οικονομία. Τα bitcoin παράγονται με μια διαδικασία που ονομάζεται εξόρυξη, στην οποία δίνεται στον υπολογιστή ένα περίπλοκο μαθηματικό πρόβλημα για να λυθεί και ο κωδικός είναι ένας 64 ψηφίων αριθμός. Αν ο υπολογιστής καταφέρει και λύσει τον αλγόριθμο αυτόν, τότε ο χρήστης θα είναι κάτοχος ενός καινούργιου μπλοκ(block) με 13 bitcoin.

Το δίκτυο αυτομάτως προσαρμόζει την δυσκολία της εξόρυξης ώστε τα 13 bitcoin να δημιουργούνται περίπου κάθε δέκα λεπτά. Επιπλέον υπάρχει ένας προκαθορισμένος αριθμός bitcoin που πρόκειται να δημιουργηθεί στο σύστημα και υπολογίζεται στα 21 εκατομμύρια. Έτσι γίνεται αντιληπτό ότι η διαδικασία εξόρυξης είναι αναγκαστική με σκοπό την απόκτηση bitcoins, καθότι δεν είναι δυνατή η απλή «τύπωση» χρημάτων. Λόγω της ανωνυμίας του Bitcoin και των άλλων κρυπτονομισμάτων, τα ψηφιακά νομίσματα συγκρίνονται πολλές φορές με τα μετρητά.

Εν αντιθέση με τα μετρητά, τα κρυπτονομίσματα χρησιμοποιούνται ως μέθοδος ηλεκτρονικής πληρωμής και αποτελούν κύριους ανταγωνιστές των πιστωτικών καρτών και του PayPal. Στην ουσία, τα κρυπτονομίσματα αποτελούν εικονικά αγαθά που έχουν τα χαρακτηριστικά του χρήματος, προσφέροντας μια λογιστική μονάδα και ένα μέσο ανταλλαγής. Οι τρέχουσες εξελίξεις και ο ανταγωνισμός στο πλαίσιο του οικοσυστήματος του Bitcoin, μπορεί να έχει σημαντικό αντίκτυπο στην μελλοντική επιτυχία αυτής της τεχνολογίας. Μολονότι η δημοτικότητα του Bitcoin έχει αυξηθεί, υπάρχουν ακόμα πολλά αναπάντητα ερωτήματα όσον αφορά την βιωσιμότητα των κρυπτονομίσματος και τις δυνατότητες αυτής της ανατρεπτικής τεχνολογίας. (CoinDesk, 2020)

Τα στάδια ανάπτυξης ενός bitcoin αποτελούνται από την κωδικοποίηση, την εύρεση χρηστών και την αύξηση της δημοτικότητας.

- **Κωδικοποίηση**

Οι χρήστες που διαθέτουν μια στοιχειώδη κατανόηση της κωδικοποίησης, είναι εξαιρετικά εύκολο να δημιουργήσουν την δική τους μορφή κρυπτογράφησης. Σε πιο προχωρημένο επίπεδο, οι προγραμματιστές μπορούν να κάνουν τροποποιήσεις στον κώδικα που αλλάζει την λειτουργία του νομίσματος που επιθυμούν. Ωστόσο, ακόμα και για τους χρήστες που δεν γνωρίζουν ή δεν κατανοούν σε βάθος την κωδικοποίηση, υπάρχουν ορισμένες διαθέσιμες υπηρεσίες που επιτρέπουν την δημιουργία κρυπτονομίσματος έναντι αμοιβής.

- **Εύρεση Χρηστών**

Η ανάπτυξη ενός κρυπτονομίσματος είναι εύκολη, άλλα η εξεύρεση δικτύου χρηστών είναι σαφώς μια πολύ πιο δύσκολη διαδικασία. Το κρυπτονόμισμα βασίζεται σε μια αποκεντρωμένη βάση δεδομένων, η οποία με την σειρά της βασίζεται στον έλεγχο και την εγγύηση της ακεραιότητας των δεδομένων. Αρά γίνεται αντιληπτό πως όχι μόνο απαιτείται ένα μεγάλο δίκτυο χρηστών, άλλα αυτό το δίκτυο θα πρέπει να είναι αξιόπιστο και να διαθέτει τα καταλληλά μέσα επεξεργασίας για να διασφαλιστεί το γεγονός ότι όλες οι συναλλαγές πραγματοποιούνται σωστά. Οι περισσότεροι νέοι τύποι κρυπτονομίσματος δημιουργούνται στην βάση της λύσης ενός προβλήματος που σχετίζεται με τα παραδοσιακά νομίσματα. Παρόλα αυτά, αν υπάρχει ανεπαρκής ικανότητα επεξεργασίας για να διευκολυνθεί το σύνολο των συναλλαγών του δικτύου, η κρυπτογράφηση μπορεί να μην πραγματοποιηθεί ποτέ με επιτυχία. Στην ουσία, προκειμένου ένας τύπος νομίσματος να κερδίσει την ευρύτερη προσοχή των χρηστών του οικοσυστήματος Blockchain, πρέπει οι μεταφορές νομισμάτων να γίνονται γρηγορά και με ασφαλή τρόπο.

Διαφορετικά, οι χρήστες μπορούν απλά να βρουν έναν άλλο τύπο ψηφιακού νομίσματος προς χρήση.

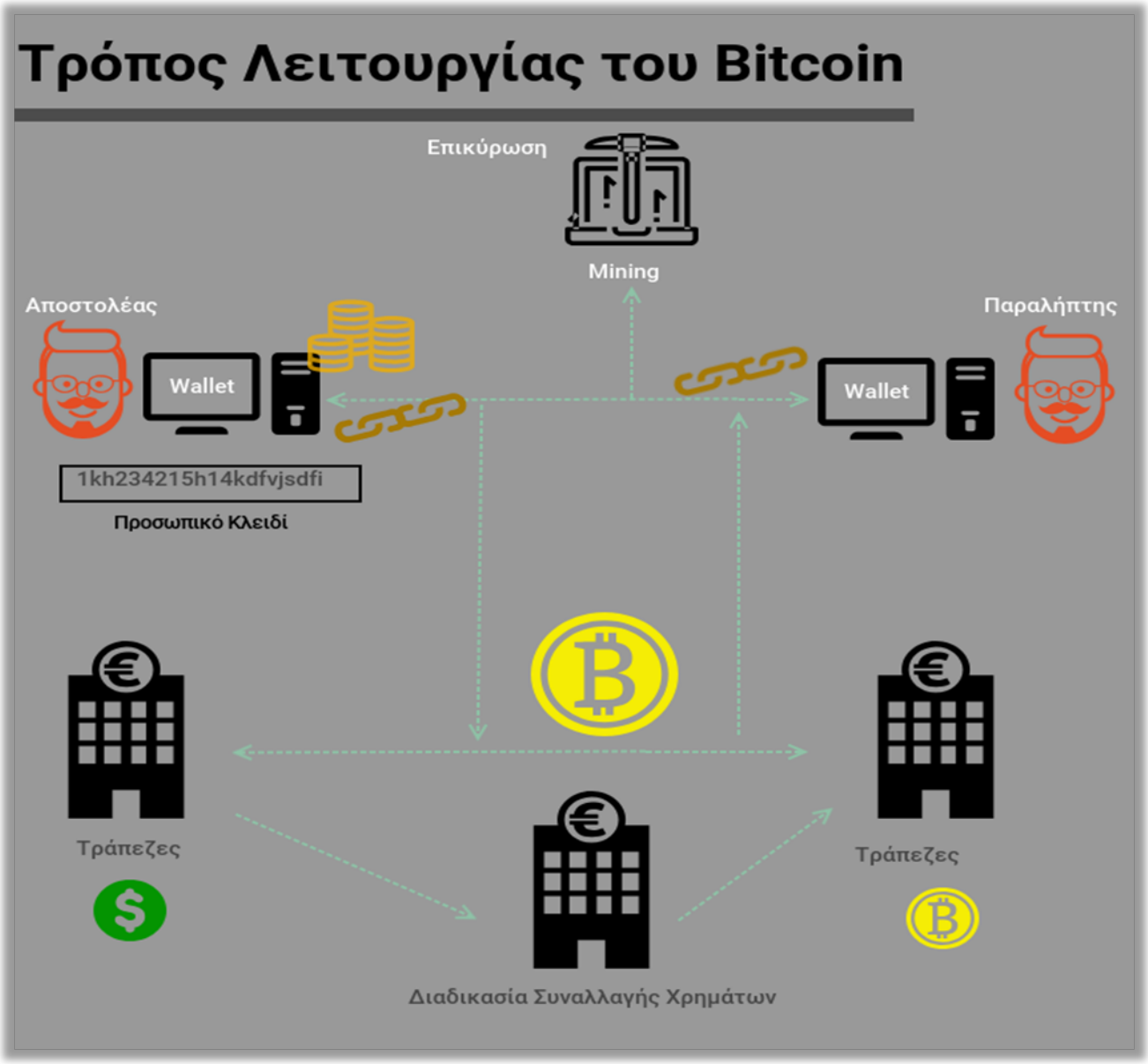
- **Αύξηση Δημοτικότητας**

Το τελευταίο βήμα για την ανάπτυξη και την εκκίνηση κυκλοφορίας ενός κρυπτονομίσματος, είναι να κερδίσει δημοτικότητα. Οι προγραμματιστές κρυπτονομίσματος θέλουν τα νομίσματα τους να φτάσουν σε όσο το δυνατόν περισσοτέρους ανθρώπους διότι με τον τρόπο αυτόν αυξάνεται και η αξία τους.

Το bitcoin δίνει την δυνατότητα στους χρήστες να κάνουν μια ηλεκτρονική συναλλαγή χρημάτων τόσο εύκολα όσο να στέλνουν ένα e-mail. Για να σταλούν τα χρήματα χρησιμοποιείται μια εφαρμογή που ονομάζεται «wallet», στο οποίο μπορούν να γράψουν ένα ποσό και να το στείλουν στον λογαριασμό ενός άλλου χρήστη. Η συναλλαγή γίνεται άμεσα και ο χρήστης που παραλαμβάνει το ποσό ειδοποιείται κατευθείαν. Σε βασικό επίπεδο, το bitcoin είναι ένα ψηφιακό αρχείο το οποίο μέσα του περιέχει ονόματα και λογαριασμούς, έτσι οποίος θέλει να κάνει μια συναλλαγή χρήματων απλά τροποποιεί το αρχείο αυτό (block). Κάθε φορά που πατάει ένας χρήστης το κουμπί της αποστολής, το ηλεκτρονικό πορτοφόλι στέλνει μήνυμα στο δίκτυο του bitcoin περιγράφοντας πώς το αρχείο πρέπει να αλλάξει, συμπεριλαμβάνοντας τον αριθμό των λογαριασμών του αποστολέα και του παραλήπτη όπως και το ποσό που θα μεταφερθεί.

Η ψηφιακή υπογραφή εξυπηρετεί τον ίδιο σκοπό όπως μιας κανονικής υπογραφής τυπωμένης πάνω σε ένα έγγραφο , αλλά φυσικά είναι βασισμένη σε πολλά περισσότερα στοιχεία. Η τεχνολογία της κρυπτογράφησης χρησιμοποιείται με πολύ εμφατικό τρόπο για να «κρύψει» μηνύματα αλλά έχει αναπροσαρμοστεί για να αποδεικνύει την ταυτότητα του χρήστη. Κάθε αριθμός λογαριασμού bitcoin έχει ένα συ σχετιζόμενο κλειδί (private key) που μόνο ο κάτοχός του γνωρίζει, και

χρησιμοποιείται για να δημιουργήσει ψηφιακές υπογραφές κρυπτογραφώντας τα μηνύματα της συναλλαγής. Στη συνέχεια ο παραλήπτης αποκρυπτογραφεί τα μηνύματα της συναλλαγής. Έπειτα, ο παραλήπτης αποκρυπτογραφεί τα μηνύματα αυτά και έτσι μπορεί να επιβεβαιωθεί ότι είναι ο πραγματικός αποστολέας. Επίσης αυτές οι υπογραφές δεν μπορούν να αντιγράφουν σαν τις κανονικές γιατί είναι ξεχωριστές και μοναδικές για κάθε συναλλαγή. (Bitcoin, 2020)



Εικόνα 4:Απεικόνιση λειτουργίας μιας συναλλαγής
Πηγή : Ιδία Επεξεργασία

Οπότε οι ηλεκτρονικές υπογραφές δεσμεύουν τις συναλλαγές με σκοπό να μην γίνονται μετατροπές στο ψηφιακό αρχείο αλλά ταυτόχρονα εγγυόνται ότι οποίος θέλει μπορεί να ελέγξει αυτές τις υπογραφές. Ένας κύριος στόχος του bitcoin είναι να προσφέρει ένα αποκεντρωμένο σύστημα, δηλαδή καμία εταιρία ή οποιαδήποτε κυβέρνηση να μην μπορεί να το ελέγξει. Αρά όταν κάποιος στέλνει χρήματα, ένα μήνυμα συναλλαγής φτάνει σε όλους όσους θέλουν να βοηθήσουν στην διατήρηση του γενικού ψηφιακού αρχείου (ledger/blockchain – αρχείο καταγραφής συναλλαγών) δηλαδή στους «miners». Κάθε «miner» κρατά ένα προσωπικό αντίγραφο του ψηφιακού αρχείου ή αλλιώς ledger και το ενημερώνει οπότε παραλαμβάνει ένα μήνυμα με μια νέα συναλλαγή , με την προϋπόθεση όμως ότι έχει έγκυρη ψηφιακή υπογραφή.

Όμως με τόσα πολλά ψηφιακά αρχεία σκορπισμένα σε όλον τον κόσμο είναι φυσικό να υπάρχει μια σχετική καθυστέρηση στο δίκτυο που ενδεχομένως να οδηγεί σε διαφορές μεταξύ τους. Αυτό αποτελεί ένα σημαντικό πρόβλημα διότι πρέπει να υπάρχει η ιδιά ενημέρωση παντού. Έτσι λοιπόν τα άτομα που βοηθάνε στην συντήρηση αυτού του αρχείου προσπαθούν να λύσουν ένα ειδικό puzzle που είναι βασισμένο στην έκδοση του ledger τους. Όποιος καταφέρει και το λύσει πρώτος ανακοινώνει την λύση και οι υπόλοιποι ενημερώνουν το ledger τους στην συγκεκριμένη έκδοση. Όσα περισσότερα άτομα δουλεύουν πάνω στην ίδια έκδοση τόσο πιο γρηγορά θα βρουν την λύση. Αυτή η διαδικασία είναι συνεχής καθώς οι συναλλαγές γίνονται σε μεγάλη συχνότητα.

3.1 Blockchain Technology

Μετα την εμφάνιση του Bitcoin έχουν εισαχθεί περίπου 1.500 αναδυόμενα εναλλακτικά κρυπτονομίσματα στην κυκλοφορία με την προοπτική εφαρμογής σε τομείς πέρα από τις νομισματικές συναλλαγές . Τα 600 από αυτά τα νέα κρυπτονομίσματα αποτελούν αντικείμενο ενεργού διαπραγμάτευσης σήμερα. Όλα τα κρυπτονομίσματα μοιράζονται την υποκείμενη τεχνολογία Blockchain και το μηχανισμό ανταμοιβής , αλλά συνήθως αναπτύσσονται σε απομονωμένα δίκτυα συναλλαγών. Πολλά από αυτά είναι κλώνοι του Bitcoin , αν και με διαφορετικές παραμέτρους όπως προμήθειες, χρόνους επικύρωσης συναλλαγών κλπ. , ενώ αλλά έχουν προκύψει από πιο σημαντικές καινοτομίες της υποκείμενης τεχνολογίας Blockchain (Franco, 2020).

Τα περισσότερα οικοσυστήματα Blockchain έχουν ένα σταθερό αριθμό Bitcoin που μπορούν να παράγουν στην βάση ενός αποπληθωριστικού οικονομικού μοντέλου καθώς η τιμή Bitcoin αυξάνεται εγγενώς λόγω της περιορισμένης προσφοράς. Τα Bitcoin μπορούν επίσης να δημιουργηθούν μόνο σε ένα συγκεκριμένο ποσοστό, το οποίο καθορίζεται μαθηματικά από την κρυπτογράφηση το οικοσυστήματος για την πρόληψη της υπερπροσφοράς (Franco, 2020). Αυτές οι προσεγγίσεις οδηγούν σε μια οικονομία κόστους των οικοσυστημάτων Blockchain μέσω χαμηλότερων τελών συναλλαγών (Tu, 2020). Ακόμα , τα κρυπτονομίσματα έχουν ένα σημαντικά χαμηλότερο κόστος από τα παραδοσιακά νομίσματα από άποψη οικονομικού, περιβαλλοντικού και κοινωνικοοικονομικού κόστους (Antonopoulos, 2020).

Τα κρυπτονομίσματα χρησιμοποιούνται σήμερα ως μέσο ανταλλαγής καθημερινών πληρωμών, δηλαδή για τον πρωταρχικό λόγο για τον οποίο εισήχθη το Bitcoin, αλλά και για κερδοσκοπία . Άλλες χρήσεις περιλαμβάνουν τη μη δαπανηρή διασυνοριακή μεταφορά χρήματων παρόλο που η έλλειψη ρυθμιστικής αρχής και η ανεξαρτησία των

κρυπτονομισμάτων καθιστούν την αγορά μοναδική και την τιμή τους εξαιρετικά ασταθή. Το μοντέλο σχεδιασμού των κρυπτονομισμάτων έχει αποδυναμώσει το μοντέλο των παραδοσιακών χρηματοπιστωτικών ιδρυμάτων με την προσθήκη νέων δυνατοτήτων προς υιοθέτηση από ατομικούς χρήστες και οργανισμούς , ως ακολούθους:

I. Διευκόλυνση νομισματικών και νομικών συναλλαγών χωρίς τα τρίτα μέρη.

II. Μεταφορά χρήματων με πιο ασφαλή ή εντελώς ανώνυμο τρόπο, ο οποίος προστατεύει τα προσωπικά δεδομένα των χρηστών.

III. Πρόσβαση σε τραπεζικές υπηρεσίες και το παγκόσμιο χρηματοπιστωτικό σύστημα με οποιαδήποτε συσκευή που συνδέεται με το διαδίκτυο, βελτιώνοντας την ποιότητα ζωής των χρηστών.

IV. Αποφυγή σημαντικών αμοιβών συναλλαγών, όπως εκείνων που χρεώνονται από εταιρίες πιστωτικών καρτών και επεξεργαστές κεντρικών πληρωμών.

V. Μείωση του κίνδυνου πληθωρισμού.

Όσον αφορά το αντίκτυπο στον τραπεζικό τομέα , τα κρυπτονομίσματα έχουν δημιουργήσει μια τεχνολογική επανάσταση παρόμοια με εκείνη του διαδικτύου. Πάρα το γεγονός ότι το Bitcoin πρωτοεμφανίστηκε το 2009, δεν έλαβε μεγάλη προσοχή πριν το 2014, οπότε και η τεχνολογία άρχισε να χρησιμοποιείται ευρέως στα χρηματοοικονομικά προϊόντα.

Από το 2014 έως και σήμερα, η τεχνολογία Blockchain αποτελεί κύριο θέμα συζήτησης σε πολλές χρηματοοικονομικές επιχειρήσεις λόγω του αποκεντρωμένου μοντέλου με το οποίο λειτουργεί και το οποίο αναμένεται να γίνει μια σημαντική λειτουργία για τις επιχειρήσεις που δραστηριοποιούνται στην επένδυση κρυπτονομισμάτων. Αυτό συμβαίνει διότι το Blockchain είναι μια νέα μορφή νομικής διάρθρωσης, στην οποία

η διαχείριση και ο έλεγχος διεξάγονται μέσω έξυπνων συμβάσεων και αυτοεξυπηρετούμενων συμφωνιών για την επένδυση σε ψηφιακά νομίσματα. Ωστόσο, ο αριθμός των εφαρμογών Blockchain αυξάνεται και επεκτείνεται περαιτέρω από τον τομέα των κρυπτονομισμάτων σε βιομηχανίες.

Από την άλλη πλευρά , πάρα την αυξανομένη δημοτικότητα και την ευρεία διάδοση, οι υπάρχουσες πλατφόρμες αξιολόγησης των ψηφιακών νομισμάτων περιορίζονται σε μικρό αριθμό υπηρεσιών και προϊόντων. Ωστόσο , η χρήση αυτών των πλατφορμών συνδέεται άμεσα με διάφορες εφαρμογές , τις οποίες οι πελάτες πρέπει να «τρέχουν» περιοδικά για να είναι σε θέση να πραγματοποιούν συναλλαγές , ανταλλαγές χρήματων , συλλογή ή επένδυση. Αυτό επιβάλλει την παροχή φιλικών προς τον χρήστη προϊόντων και υπηρεσιών, όπως η πλατφόρμα ενιαίας εξυπηρέτησης. Παρακάτω παρατίθεται ο πίνακας SWOT του κρυπτονομίσματος , με σκοπό την συνοπτική περιγραφή τόσο των δυνατών και των αδύνατων σημείων του κρυπτονομίσματος, όσο και των ευκαιριών και απειλών του που αναδύονται στο σύγχρονο περιβάλλον.

Δυνατά Σημεία	**Αδύναμα Σημεία**
• **<u>Προστασία προσωπικών δεδομένων</u>** Οι αγορές Bitcoin είναι ανώνυμες. Αυτό σημαίνει ότι δεν μπορούν να συνδεθούν τα προσωπικά στοιχεία με τις συναλλαγές. Τα Bitcoin αποθηκεύονται σε ψηφιακό πορτοφόλι, το οποίο περιέχει μόνο το ιδιωτικό κλειδί της κάθε διεύθυνσης Bitcoin που κάποιος έχει στην κατοχή του. Με τον τρόπο αυτό αποτρέπεται η	• **<u>Επεκτασιμότητα</u>** Το οικοσύστημα Blockchain χρησιμοποιεί την απόδειξη εργασίας(proof-of-work) και κάθε συναλλαγή πρέπει να επικυρωθεί πριν την επεξεργασία της. Αυτό έχει αρνητική επίπτωση στον αριθμό των συναλλαγών που μπορούν να γίνουν. Η PayPal επεξεργάστηκε 7,6 δισεκατομμύρια

κλοπή ταυτότητας .

- **<u>Αποκέντρωση</u>**

Η αποκέντρωση είναι ένα από τα μεγαλύτερα πλεονεκτήματα του Bitcoin καθώς δεν απαιτείται διαμεσολαβητής για την ολοκλήρωση μιας συναλλαγής. Κυβερνήσεις , τράπεζες και οικονομικοί μεσάζοντες δεν μπορούν να παρέμβουν στις συναλλαγές χρηστών καθώς η τεχνολογία Blockchain είναι ομότιμο σύστημα. Συνεπώς, οι χρήστες Bitcoin έχουν μεγαλύτερη ελευθέρια από τα συμβατικά νομίσματα , τα οποία ελέγχονται από τρίτους .

- **<u>Τέλη συναλλαγής</u>**

Επειδή το νόμισμα είναι αποκεντρωμένο και ελέγχεται μόνο από τους χρήστες δεν υπάρχουν αμοιβές τρίτων ή φόροι για συναλλαγές . Το Bitcoin μπορεί, ωστόσο να μετατραπεί σε συμβατικό νόμισμα έναντι αμοιβής περίπου 1%. Λόγω του κίνητρου των miners να δημιουργήσουν νέα κρυπτονομίσματα , το κόστος εξόρυξης είναι δωρεάν και οι τράπεζες χρεώνουν μόνο το λειτουργικό κόστος της συναλλαγής .

συναλλαγές το 2017 το οποίο αντιστοιχεί σε περίπου 20 εκατομμύρια συναλλαγές ημερησίως. Το Bitcoin δεν μπορεί να ανταγωνιστεί τους αριθμούς αυτούς. Ο μεγαλύτερος ημερήσιος αριθμός συναλλαγών με Bitcoin ήταν περίπου 490.000 και πραγματοποιήθηκε στις 14 Δεκέμβριου 2017.

- **<u>Δυσκολία Κατανόησης</u>**

Παρόλο που το Bitcoin είναι το πιο γνωστό κρυπτονόμισμα, εξακολουθούν να υπάρχουν μεγάλες ομάδες ανθρώπων που δεν γνωρίζουν το ψηφιακό νόμισμα και την λειτουργικότητα του. Είναι αρκετά δύσκολο να εφαρμοστεί η χρήση ενός νομίσματος όταν ένας μεγάλος αριθμός ανθρώπων δεν το γνωρίζει καν. Το Bitcoin είναι πιο περίπλοκο από το σημερινό νομισματικό σύστημα και οι περισσότεροι άνθρωποι θέλουν να καταλάβουν πώς λειτουργεί πριν αρχίσουν να το χρησιμοποιούν . Για τον λόγο αυτό, είναι απίθανο νέοι χρήστες να προβούν σε σημαντικές συναλλαγές συμβατικών νομισμάτων με το Bitcoin . Αυτός είναι ένας από τους πιο βασικούς λογούς για τους οποίους το Bitcoin δεν αντιμετωπίζεται ως νόμισμα , αλλά ως μια κερδοσκοπική επένδυση.

- **Προστασία κατά της απάτης χρέωσης**

Όταν ένα καταναλωτής κάνει online αγορά με πιστωτική κάρτα , μπορεί να ζητήσει την επιστροφή χρήματων από την τράπεζα έκδοσης μετά την παραλαβή των αγορασθέντων αγαθών ή υπηρεσιών. Εφόσον εγκριθεί η αίτηση , ο καταναλωτής λαμβάνει την επιστροφή των χρήματων του και η οικονομική συναλλαγή ακυρώνεται με αντιστροφή χρεών. Ωστόσο, ο έμπορος έχει ήδη παραδώσει τα αγαθά ή τις υπηρεσίες, χωρίς να λαμβάνει πληρωμή. Αυτή η διαδικασία, γνωστή ως «απάτη χρέωσης», δεν μπορεί να γίνει με το bitcoin. Συνεπώς , οι έμποροι προστατεύονται και οι καταναλωτές ξέρουν τι ξοδεύουν.

- **Ασυλία στον πληθωρισμό**

Οι οικονομολόγοι χρησιμοποιούν τον ορό «πληθωρισμό» για να δηλώσουν μια συνεχιζόμενη αύξηση στο γενικό επίπεδο των τιμών. Ο πληθωρισμός συνεπάγεται σε συνεχή πτώση του συνόλου της αγοραστικής δύναμης της νομισματικής μονάδας όταν ο βαθμός στον οποίο η ονομαστική προσφορά αυξάνεται ταχύτερα από την πραγματική ζήτηση (White, 2008). Επειδή το Bitcoin είναι αποκεντρωμένο, η προσφορά είναι περιορισμένη. Συνεπώς , η αγοραστική δύναμη του Bitcoin δεν μειώνεται

- **Μεταβλητότητα**

Η μεταβλητότητα του Bitcoin είναι ένας από τους λογούς που οι άνθρωποι φοβούνται να επενδύσουν μεγάλα χρηματικά ποσά στο νόμισμα.

- **Κατανάλωση Ενέργειας**

Το ενεργειακό κόστος μιας συναλλαγής Bitcoin είναι σημαντικά μεγαλύτερο από οποιοδήποτε συμβατικό νόμισμα (851 κιλοβατώρες έναντι 169). Επιπλέον , το σύστημα δεν μοιάζει να είναι φιλικό προς το περιβάλλον καθώς παράγει υψηλό αποτύπωμα άνθρακα, επειδή οι περισσότερες από τις δραστηριότητες εξόρυξης διεξάγονται στην Κίνα, που τροφοδοτείται κυρίως από σταθμούς ηλεκτροπαραγωγής με καύση άνθρακα.

όσο αυξάνεται η προσφορά του Bitcoin.	
Ευκαιρίες	**Απειλές**
• **<u>Οικονομική Κρίση</u>** Σε περίπτωση οικονομικής κρίσης , οι άνθρωποι ενδέχεται να χάσουν την πιστή τους στο τρέχον νομισματικό σύστημα και να αρχίσουν να αναζητούν εναλλακτικές λύσεις . Αυτό σημαίνει ότι , ενδεχομένως , κάποιοι επενδυτές να εστιάσουν στα πλεονεκτήματα του Bitcoin και να είναι περισσότερο δεκτικοί στα κρυπτονομίσματα . Επίσης οι κυβερνήσεις ξεκινούν σταδιακά να προτείνουν την χρήση ψηφιακού νομίσματος για την μη μετάδοση του ιού COVID-19 . • **<u>Αυξημένα Ποσοστά Πληθωρισμού</u>** Δεδομένου ότι το Bitcoin δεν επηρεάζεται από τον πληθωρισμό, η αύξηση του πληθωρισμού θα μπορούσε να σημαίνει ότι οι άνθρωποι θα ενδιαφερθούν περισσότερο να επενδύσουν ή να κρατήσουν το Bitcoin στο ψηφιακό τους	• **<u>Ρυθμιστικό Πλαίσιο</u>** Οι ισχύοντες νόμοι και κανονισμοί δεν λαμβάνουν υπόψη τεχνολογίες όπως το Bitcoin , επομένως η διαδικασία ρύθμισης θα είναι σύνθετη . Πάρα το γεγονός ότι η έλλειψη ρύθμισης αποτελεί πόλο έλξης για τους χρήστες, εντούτοις , η ανωνυμία και η αποκέντρωση του Bitcoin έχει οδηγήσει στην χρήση του για εγκληματικές δραστηριότητες. Αυτός είναι ο λόγος για τον οποίον πολλές κυβερνήσεις αν τον κόσμο προσπαθούν να καθιερώσουν σαφείς κανονισμούς σχετικά με την χρήση του Bitcoin και την έννομη συμπεριφορά. Για παράδειγμα , στο Παγκόσμιο Οικονομικό Φόρουμ στο Νταβός , πολλοί ηγέτες του κόσμου φάνηκαν να συμφωνούν ότι η εφαρμογή ρυθμιστικού πλαισίου θα πρέπει να ληφθεί σοβαρά ώστε να αποτρέπεται η χρήση του Bitcoin για παράνομες δραστηριότητες. Κάποια παραδείγματα

πορτοφόλι, προκειμένου να εξασφαλίσουν ότι τα χρήματα τους δεν θα χάσουν την αξία τους .

- **<u>Επίπτωση Δικτύου</u>**

Η επίπτωση δικτύου είναι το φαινόμενο κατά το οποίο αυξάνεται ο αριθμός των ατόμων ή των συμμετεχόντων στην αξία ενός αγαθού ή μιας υπηρεσίας . Συνεπώς όσο περισσότεροι άνθρωποι αρχίζουν να χρησιμοποιούν το Bitcoin , τόσο θα αυξηθεί η αξία του με την προοπτική να γίνει ευρύτερα αποδεκτό ως μέσο ανταλλαγής και να προκύψουν περισσότερες υπηρεσίες που να συνδέονται με το κρυπτονόμισμα.

ρύθμισης των κρυπτονομισμάτων αφορούν σε εμβάσματα , συναλλαγματικές ισοτιμίες , θέματα δανειοδότησης , ξέπλυμα χρήματος και χρηματοδότηση της τρομοκρατίας και ελάφρυνση φορολογίας .

- **<u>Σύνδεση με εγκληματικές δραστηριότητες</u>**

Το Bitcoin έχει συνδεθεί με εγκληματικές δραστηριότητες , δεδομένου ότι καμία συναλλαγή δεν συνδέεται με προσωπικές πληροφορίες. Ως εκ τούτου , το Bitcoin χρησιμοποιείται ευρέως για παράνομες αγοραπωλησίες , ξέπλυμα χρήματος και χρηματοδότηση της τρομοκρατίας (Bitcoin, 2020).Περαιτέρω λόγοι είναι οι εξής:

- Το σύστημα επιτρέπει την μεταφορά χρημάτων από οπουδήποτε , οποτεδήποτε και σε οποιοδήποτε ποσό. Αυτό σημαίνει ότι ένας τρομοκράτης στην χωρά Α μπορεί να ξεκινήσει μια συναλλαγή μέσω διαδικτύου για να μετατρέψει το εθνικό νόμισμα της χωράς Β μέσω εικονικής συναλλαγής νομισμάτων στην χωρά Γ και μεταφορά του

	εικονικού νομίσματος σε ένα ψηφιακό πορτοφόλι στην χωρά Δ. • Το σύστημα μπορεί να πραγματοποιεί γρηγορά τις μεταφορες, μέσα σε δευτερόλεπτα. • Είναι δύσκολο για τις αρχές κάθε χωράς να παρακολουθούν τις συναλλαγές. • Το σύστημα δεν απαιτεί προχωρημένες τεχνικές γνώσεις.

Γενικότερα, η τεχνολογία Blockchain μπορεί να οδηγήσει σε ένα ριζικά διαφορετικό ανταγωνιστικό μέλλον στην χρηματοπιστωτική βιομηχανία, όχι μόνο λόγω της τεράστιας εξοικονόμησης κόστους , αλλά και την υψηλότερη διαφάνεια στις συναλλαγές, γεγονός πολύ θετικό από άποψη ελέγχου και κανονιστικής σκοπιάς. Επιπλέον, η εμφάνιση του Blockchain και του Bitcoin είναι τόσο επαναστατική η οποία θα έχει σαν αποτέλεσμα την εκτόξευσή του σε χρήση κατά 69,0% μέχρι το 2021 (econinfosec, 2020).

ΚΕΦΑΛΑΙΟ 4 : Μέθοδοι Απόκτησης Bitcoin

Οποιοσδήποτε το επιθυμεί μπορεί να γίνει κάτοχος Bitcoin με διάφορους τρόπους όπως ανταλλακτήρια ή απευθείας από άλλους ανθρώπους , όπως και φυσικά από την διαδικασία της εξόρυξης. Ο τρόπος πληρωμής είναι ποικίλος από μετρητά έως πιστωτικές κάρτες και ο πιο διαδεδομένος είναι μέσω ανταλλακτηρίων . Αυτό που κάνει εντύπωση είναι ότι δεν είναι εύκολο να αγοράσει κάποιος bitcoin μέσω κάρτας PayPal, αναλόγως με τους κανονισμούς της χωράς που διαμένει και αυτό συμβαίνει διότι τέτοιες συναλλαγές μπορούν να ακυρωθούν από τον χρήστη και να αντιστρέφει το μισό της συναλλαγής . Επομένως , αυτή η μέθοδος πληρωμής αποφεύγεται επειδή πολύ απλά δεν μπορεί να αποδειχθεί η συναλλαγή. Τα Μεγαλύτερα ανταλλακτήρια είναι το bit stamp , batch – e , kraken , bitfinex , okcoin , btc. Η πιο δημοφιλής ανταλλακτική υπηρεσία όμως είναι το coin base, που έχει την δυνατότητα να συναλλάξει ευρώ ή δολάρια για bitcoin , όπως επίσης και το circle το οποίο είναι διαθέσιμο για κινητά τηλεφωνά. Άλλα διάσημα πορτοφόλια που κάνουν την ιδιά δουλειά είναι το Conjar , και το Unocoin. Εμβαθύνοντας στους τρόπους απόκτησης των νομισμάτων παρατηρούνται και άλλοι μέθοδοι απόκτησης με μηδαμινή ή καθόλου χρηματική επιβάρυνση και αναφέρονται παρακάτω . (Coinmarketcap, 2020)

- **ΑΠΟΚΤΗΣΗ ΜΕΣΩ ΙΣΤΟΣΕΛΙΔΩΝ**

Υπάρχουν πολλές ιστοσελίδες που μπορείς να κερδίσεις bitcoin. Η λογική αυτή είναι ότι μπορεί κάποιος να επισκεφτεί μια ιστοσελίδα και μόνο με μία μικρή εξερεύνηση να κερδίσει ένα μικρό ποσό , κυρίως λόγω των διαφημίσεων. Όταν κερδίζεις bitcoin μέσω αυτών των διαφημιστικών

ιστοσελίδων , ουσιαστικά ανταμείβεσαι για τον χρόνο που προσδίδεις. Μερικές από αυτές τις ιστοσελίδες είναι οι εξής :

- Bitvisitor

Αποκτάς bitcoin απλώς βλέποντας βίντεο σε ιστοσελίδες. Κάθε βίντεο που προβάλλεται έχει διάρκεια περίπου πέντε λεπτών και η πληρωμή του χρήστη ανέρχεται περίπου σε 0.00012 btc ανά ώρα. Επίσης δεν χρειάζεται να έχεις κάνει εγγραφή στην ιστοσελίδα , απλά να έχεις την διεύθυνση του bitcoin λογαριασμού σου.

- Coin Worker

Προσφέρει bitcoin μετά από την ολοκλήρωση αναλυτικών survey ή διάφορων tasks . Απαιτείται λογαριασμός για αυτήν την ιστοσελίδα και είναι πιο αποδοτικό από την προηγουμένη επιλογή.

- Freedigitalmoney.com

Μέσω αυτής της ιστοσελίδας αποκτώνται bitcoin δίνοντας βραβεία για αγορές που έχουν γίνει με bitcoin. Για να αποκτήσεις πρόσβαση σε αυτήν την ιστοσελίδα δεν χρειάζεται να έχεις κάποιον λογαριασμό.

- Bitfortip

Απαντώντας σε ερωτήσεις σε διαφορά forum έχεις την δυνατότητα να αποκτήσεις bitcoin. Είναι αποδοτικός τρόπος που φέρνει κοντά τους χρήστες για ένα θέμα που τους ενδιαφέρει.

- **ΑΠΟΚΤΗΣΗ ΜΕΣΩ ΧΡΗΜΑΤΙΣΤΗΡΙΑΚΗΣ ΜΕΤΟΧΗΣ**

Αυτή η μέθοδος ουσιαστικά δεν είναι πολύ κερδοφόρα και ταυτόχρονα είναι αρκετά περιπλοκή. Ένα παράδειγμα αυτής της μεθόδου είναι όταν

κάποιος βρίσκει την ευκαιρία να αγοράσει ένα απόκτημα σε ένα μέρος για μια συγκεκριμένη τιμή και το πουλάει αμέσως κάπου αλλού για καλύτερη τιμή. Φυσικά υπάρχουν διαφορά ρίσκα και σε ένα γενικό πλαίσιο δεν είναι και τόσο εύκολο να ανταλλάξεις κάτι σε μια πιο κερδοφόρα τιμή . Ένα τέτοιο διαδικτυακό μέρος που υπάρχουν τέτοιες ευκαιρίες είναι το Bitcoin Stack Exchange. Ειδάλλως , μπορεί κάποιος να κάνει υποθέσεις ότι η τιμή των bitcoin θα ανεβεί και να περιμένει την κατάλληλη χρονική στιγμή που θα πουλήσει ή θα τα ανταλλάξει όποτε θεωρεί αυτός ότι θα βγάλει κάποιο κέρδος από αυτό . (Bitcoin.fr, 2020)

- **ΑΠΟΚΤΗΣΗ ΜΕΣΩ ΤΥΧΑΙΟΠΑΙΓΝΙΑΣ**

Δεν είναι η κατάλληλη επιλογή για να αποκτήσει κάποιος bitcoin αλλά πρέπει να αναφερθεί καθώς το δίκτυο είναι γεμάτο από σελίδες τυχερών παίγνιων, οι οποίες έχουν ως προεπιλογή τη χρήση κρυπτονομίσματος

ΚΕΦΑΛΑΙΟ 5 : Μέθοδος Αποθήκευσης Bitcoin

Παρόμοιο με έναν αριθμό τραπεζικού λογαριασμού, το πορτοφόλι συνοδεύεται από μια διεύθυνση πορτοφολιού που εμφανίζεται σε μια αναζήτηση καθολικού και κοινοποιείται σε άλλους με σκοπό την πραγματοποίηση συναλλαγών. Αυτή η διεύθυνση, η οποία είναι μια πιο σύντομη, πιο εύχρηστη έκδοση του δημοσίου κλειδιού, αποτελείται από 35 στοιχεία π.χ.: 1AZ1p1Ep5QGefi2DMPTfTL5SL.mv7DIvdAb. Τα κλειδιά χρησιμοποιούνται για να επαληθεύσουν ότι ο χρήστης είναι κάτοχος του προαναφερθέντος δημοσίου κλειδιού και έχει την δυνατότητα να αποσυνδεθεί από τις συναλλαγές . Ορισμένα πορτοφόλια δημιουργούν μια ασφαλή φράση σπόρου, δηλαδή ένα σύνολο λέξεων που θα επιτρέψουν στον χρήστη να ξεκλειδώσει το πορτοφόλι του εάν χάσει το δημόσιο κλειδί. Συνήθως είναι συνετό, η φράση αυτή να εκτυπώνεται και να φυλάσσεται σε ασφαλές μέρος .(Investopedia, 2020)

Πηγή: Shutterstock

Η αλήθεια είναι ότι το πορτοφόλι bitcoin είναι παρόμοιο με το φυσικό πορτοφόλι. Εάν χάσει κάποιος τα ιδιωτικά κλειδιά στο πορτοφόλι , πιθανότατα θα χάσει το νόμισμα σε αυτό για πάντα. Το πορτοφόλι δημιουργεί ένα κύριο αρχείο οπού αποθηκεύονται τα δημοσιά και ιδιωτικά κλειδιά . Σε αυτό το αρχείο πρέπει να δημιουργηθεί αντίγραφο ασφάλειας σε περίπτωση που το αρχικό αρχείο χαθεί ή καταστραφεί. Διαφορετικά , κινδυνεύει να χάσει ο χρήστης την πρόσβαση στα χρήματα του. Μπορεί κάποιος να αποθηκεύσει τα προσωπικά κλειδιά του στον υπολογιστή, την κινητή συσκευή , σε ένα φυσικό υλικό αποθήκευσης ή ακόμα και σε ένα κομμάτι χαρτί .

Είναι σημαντικό να διατηρούνται τα ιδιωτικά κλειδιά ασφαλή δημιουργώντας αντίγραφα ασφάλειας τόσο στο διαδίκτυο όσο και εκτός σύνδεσης. Το πορτοφόλι δεν βρίσκεται σε καμία συσκευή . Το ίδιο το πορτοφόλι βρίσκεται στο blockchain του Bitcoin όπως ακριβώς η τραπεζική εφαρμογή δεν «κρατάει» πραγματικά τα μετρητά στον λογαριασμό.

Ενώ οι εφαρμογές πορτοφολιών λειτουργούν καλά και είναι σχετικά ασφαλείς , η ασφαλέστερη επιλογή είναι ένα πορτοφόλι υλικού που διατηρείται εκτός σύνδεσης , σε ασφαλές μέρος . Τα πιο δημοφιλή πορτοφόλια υλικού χρησιμοποιούν ειδικά επίπεδα ασφάλειας για να διασφαλίσουν ότι τα κλειδιά δεν θα κλαπούν και το bitcoin του χρήστη είναι ασφαλές . Αλλά για άλλη μια φορά , εάν χαθεί το πορτοφόλι υλικού , τα bitcoin που περιέχονται μέσα θα χαθούν εκτός εάν έχει διατηρηθεί αξιόπιστο αντίγραφο ασφάλειας των κλειδιών. Η λιγότερο ασφαλής επιλογή είναι ένα διαδικτυακό πορτοφόλι , δηλαδή η αποθήκευση του bitcoin σε συναλλαγή . Αυτό συμβαίνει επειδή τα κλειδιά κρατούνται σε τρίτο μέρος .Για πολλούς , τα διαδικτυακά πορτοφόλια ανταλλαγής είναι τα πιο ευκολά στην ρύθμιση και την χρήση , παρουσιάζοντας μια πολύ οικεία επιλογή : ευκολία έναντι ασφάλειας. Πολλοί σοβαροί επενδυτές

bitcoin χρησιμοποιούν μια υβριδική προσέγγιση: Διατηρούν ένα πυρήνα, μακροπρόθεσμο ποσό bitcoin εκτός σύνδεσης στο λεγόμενο «κρύο χώρο αποθήκευσης» διατηρώντας παράλληλα ένα ισοζύγιο δαπανών σε ένα λογαριασμό κινητού. Ανάλογα με την στρατηγική του bitcoin κάθε χρήστη και την προθυμία του να αποκτήσει τεχνική βοήθεια , διατίθενται διάφοροι τύποι πορτοφολιών bitcoin. (Coinmarketcap.com, 2020)

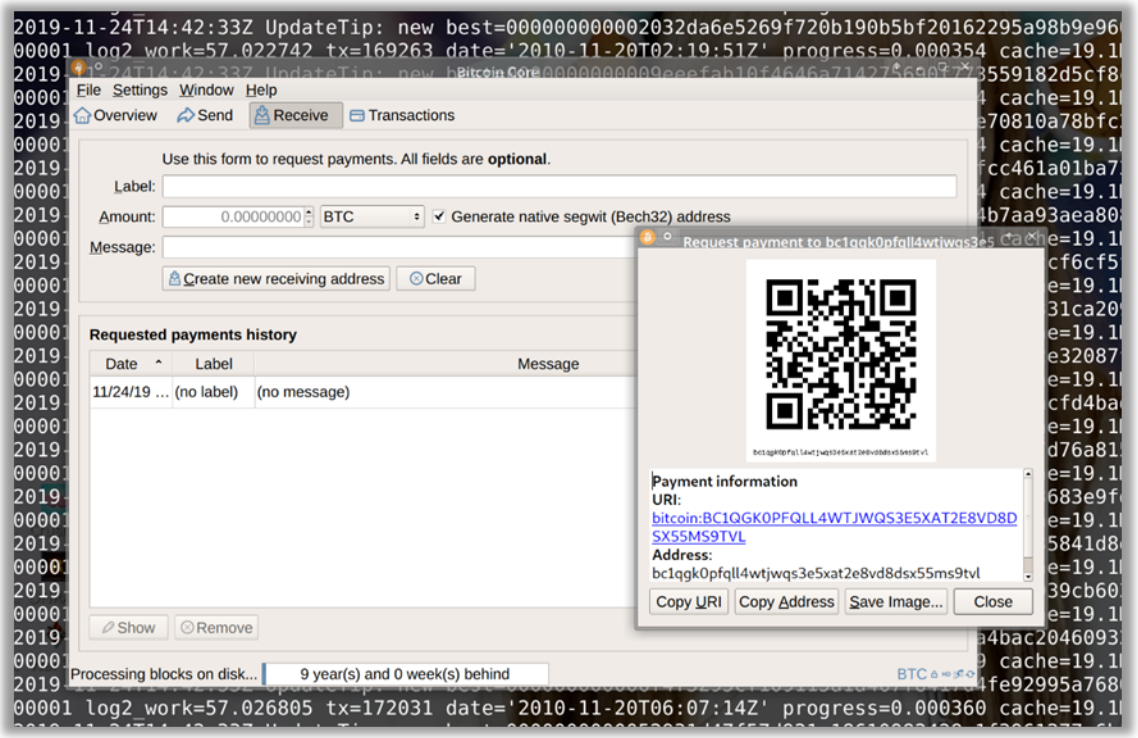
Εικόνα 5:Δομή πορτοφολιού Cloud
Πηγή: Shutterstock

Τα **πορτοφόλια Cloud** υπάρχουν στο διαδίκτυο και τα κλειδιά συνήθως αποθηκεύονται σε ένα απομακρυσμένο διακομιστή που εκτελείται από τρίτο μέρος. Τα πορτοφόλια που βασίζονται σε σύννεφο τείνουν να έχουν μια πιο φιλική προς τον χρήστη διεπαφή, αλλά ο χρήστης πρέπει να εμπιστεύεται ένα τρίτο μέρος με τα ιδιωτικά κλειδιά του , γεγονός που καθιστά τα χρήματα του πιο ευαίσθητα σε κλοπή. Μερικά παραδείγματα αυτού του τύπου πορτοφολιού είναι το Coinbase, Blockchain και το Lumiwallet . Τα περισσότερα κρυπτονομίσματα , συμπεριλαμβανομένου του bitcoin , έχουν τα δικά τους εγγενή πορτοφόλια . Ορισμένα

προσφέρουν πρόσθετες δυνατότητες ασφάλειας , όπως αποθήκευση εκτός σύνδεσης (Coinbase ,Xapo) . Με τα ιδιωτικά κλειδιά αποθηκευμένα σε έναν διακομιστή , πρέπει ο χρήστης να εμπιστευτεί τα μετρά ασφάλειας του κεντρικού υπολογιστή και επίσης να πιστεύει ότι ο κεντρικός υπολογιστής δεν θα εξαφανιστεί με τα χρήματα ή θα κλείσει και θα αρνηθεί την πρόσβαση στον χρήστη.

Τα **πορτοφόλια υπολογιστή** έχουν εγκατεστημένο τον αρχικό και βασικό bitcoin client(bitcoin core) , το οποίο τρέχει στον υπολογιστή ένα πορτοφόλι που πιθανόν ο χρήστης να μην το γνωρίζει. Επιπροσθέτως , για έμπιστη συναλλαγή στο δίκτυο, αυτό το λογισμικό σου επιτρέπει να δημιουργήσεις μια διεύθυνση bitcoin για αποστολή και παραλαβή των ψηφιακών νομισμάτων, όπως και την αποθήκευση του ιδιωτικού κλειδιού για την διεύθυνση αυτή. Το μειονέκτημα είναι ότι ο κάθε χρήστης είναι υπεύθυνος για την ασφάλεια των κλειδιών του. Τα πορτοφόλια λογισμικού απαιτούν επίσης μεγαλύτερες προφυλάξεις ασφάλειας. Εάν ο υπολογιστής παραβιαστεί ή κλαπεί , ο κλέφτης μπορεί να πάρει ένα αντίγραφο του πορτοφολιού του χρήστη και του bitcoin του. Μολονότι ο χρήστης μπορεί να κατεβάσει ένα πρωτότυπο Bitcoin Core (το οποίο αποθηκεύει ένα καθολικό όλων των συναλλαγών από το 2009 και καταλαμβάνει πολύ χώρο), τα περισσότερα πορτοφόλια που χρησιμοποιούνται σήμερα είναι πορτοφόλια ελαφριά ή πορτοφόλια SPV (Απλοποιημένη επαλήθευση πληρωμής) τα οποία δεν χρειάζεται να γίνει λήψη του αρχείου απλά να συγχρονιστεί. Το Electrum είναι ένα γνωστό πορτοφόλι Bitcoin για επιτραπέζιους υπολογιστές SPV που προσφέρει επίσης «ψυκτική αποθήκευση» μια εντελώς εκτός σύνδεσης επιλογή για επιπλέον ασφάλεια. Το Exodus μπορεί να παρακολουθεί πολλά στοιχεία με ένα εξελιγμένο περιβάλλον εργασίας χρήστη. Ορισμένα όπως το JaxxLiberty, μπορούν να διατηρήσουν ένα ευρύ φάσμα ψηφιακών στοιχείων και μερικά όπως το Copay προσφέρουν την δυνατότητα οικιών λογαριασμών. Πριν από την

λήψη οποιασδήποτε εφαρμογής , πρέπει να γίνει επιβεβαίωση ότι κατεβαίνει ένα νόμιμο αντίγραφο ενός πραγματικού πορτοφολιού. Μερικοί σκιεροί προγραμματιστές δημιουργούν κλώνους από διάφορους ιστότοπους κρυπτογράφησης και προσφέρουν δωρεάν λήψεις , οδηγώντας σε πιθανότητα παραβίασης. (CoinDesk, 2020)



Εικόνα 6:bitcoin core wallet
Πηγή: Shutterstock

Τα πορτοφόλια υπολογιστή είναι όλα πολύ χρήσιμα και αξιόπιστα , αλλά δεν βοηθάνε πολύ όταν ένας χρήστης βρίσκεται σε εξωτερικό χώρο προσπαθώντας να πραγματοποιήσει μια συναλλαγή σε κάποιο κατάστημα . Σε αυτήν την περίπτωση τα mobile wallets εμφανίζονται χρήσιμα. Τρέχουν σαν μια εφαρμογή στο κινητό , μπορώντας να αποθηκεύουν τα ιδιωτικά κλειδιά της bitcoin διεύθυνσης , δίνοντας την δυνατότητα να γίνει κάποια αγορά κατευθείαν από το κινητό γρηγορά και ευκολά . Ένα άλλο κοινο χαρακτηριστικό των mobile wallets είναι ότι δεν είναι πλήρεις bitcoin clients. Ένας πλήρης bitcoin client πρέπει να κατεβάσει ολόκληρο το block chain που δεν σταματάει να μεγαλώνει και έχει χωρητικότητα

πολλά gigabits , επομένως ένα κινητό δεν θα μπορούσε να αποθηκεύσει ολόκληρο το block chain καθώς θα εμφανίζονται προβλήματα στην χωρητικότητα και την λειτουργικότητα του . Για τον λόγο αυτό είναι σχεδιασμένα για απλοποιημένη επαλήθευση πληρωμής . Κατεβάζουν ένα πολύ μικρό σύνολο της block chain αλυσίδας βασιζόμενα σε άλλους έμπιστους κόμβους του δικτύου για να σιγουρευτούν ότι έχουν τις σωστές πληροφορίες . Όλα τα διαδικτυακά πορτοφόλια και τα περισσότερα από τα επιτραπέζια που αναφέρονται παραπάνω έχουν εκδόσεις για κινητά , ενώ αλλά όπως το Abram , Edge και το Bread , δημιουργήθηκαν με γνώμονα τα κινητά .

Εικόνα 7:Trezor Hardware Wallet
Πηγή: Shutterstock

Τα **πορτοφόλια υλικού** είναι μικρές συσκευές που συνδέονται στον Ιστό μόνο για την πραγματοποίηση συναλλαγών bitcoin . Είναι πιο ασφαλείς επειδή είναι γενικά εκτός σύνδεσης και επομένως δεν είναι hackable . Μπορούν , ωστόσο , να κλαπούν ή να χαθούν , μαζί με τα bitcoin που

ανήκουν στα αποθηκευμένα ιδιωτικά κλειδιά , επομένως συνίσταται να δημιουργούνται αντίγραφα ασφάλειας των κλειδιών.

Μερικοί μεγάλοι επενδυτές διατηρούν τα πορτοφόλια υλικού σε ασφαλείς τοποθεσίες ,όπως θησαυροφυλάκια τράπεζων . Τα Trezor , Keep Key και Ledger είναι αξιοσημείωτα παραδείγματα.

Αυτή η συσκευή απευθύνεται στους χρήστες του bitcoin που θέλουν να έχουν ένα σημαντικό αριθμό νομισμάτων , αλλά δεν θέλουν να εξαρτώνται από τρίτους για τις υπηρεσίες αποθήκευσης του bitcoin που υπάρχουν , καθώς και τις μη πρακτικές μορφές του cold storage ή αλλιώς «κρύο χώρο αποθήκευσης» .(Duffield, 2020)

Εικόνα 8: Ledger Hardware Wallet
Πηγή: Shutterstock

Τα **χάρτινα πορτοφόλια** είναι ίσως πιο απλά από όλα τα πορτοφόλια που προαναφέρθηκαν. Τα πορτοφόλια χαρτιού είναι κομμάτια χαρτιού που περιέχουν τα ιδιωτικά και δημοσιά κλειδιά μιας διεύθυνσης bitcoin. Ιδανικό για την μακροπρόθεσμη αποθήκευση bitcoin (φυσικά από το νερό και την φωτιά) ή για την παροχή του bitcoin ως δώρου , αυτά τα

πορτοφόλια είναι πιο ασφαλή καθώς δεν είναι συνδεδεμένα σε δίκτυο, παρόλα αυτά είναι και τα πιο ευκολά να χαθούν . Με υπηρεσίες όπως το Wallet Generator , μπορεί ευκολά κάποιος να δημιουργήσει μια νέα διεύθυνση και να εκτυπώσει το πορτοφόλι στον εκτυπωτή του. Όταν είναι έτοιμος ο χρήστης να συμπληρώσει το χαρτοφυλάκιο χαρτιού , απλά στέλνει bitcoin σε αυτήν την διεύθυνση και στην συνέχεια αποθηκεύεται με ασφάλεια.

Όποια και να είναι η επιλογή που θέλει ο χρήστης , φροντίζει να δημιουργεί αντίγραφα ασφαλείας για τα πάντα και να τα αποθηκεύει στον προσωπικό του χώρο . Τα χάρτινα πορτοφόλια θεωρούνται μια από τις πιο διάσημες , εύκολες και φθηνότερες επιλογές για να κρατάς τα bitcoin ασφαλή. Ουσιαστικά δημιουργείται μια διεύθυνση bitcoin όπως και μια εικόνα που περιέχει δυο κωδικούς : ο ένας είναι η δημοσιά διεύθυνση που χρησιμοποιείς για να παραλάβεις bitcoin και ο άλλος είναι το ιδιωτικό κλειδί.

Εικόνα 9:Bitcoin Encrypted Paper Wallet
Πηγή : Shutterstock

ΚΕΦΑΛΑΙΟ 6: Τρόποι Συναλλαγών Bitcoin

Η χρήση του bitcoin μεγαλώνει μέρα με την μέρα καθώς βλέπουμε αυξανομένη δραστηριότητα στις συναλλαγές από τα μέσα κυρίως του 2014, όπου πολλά καταστήματα αρχίσαν να δέχονται τα bitcoin ως μέσο πληρωμής με αποτέλεσμα μέχρι σήμερα να βλέπουμε τεράστια αποδοχή . Όπως αναφέραμε το bitcoin ουσιαστικά είναι ψηφιακό νόμισμα και η χρησιμότητα του δεν διαφέρει από την παραδοσιακή οικονομία καθώς πραγματοποιούνται συναλλαγές – μεταφορές χρήματων . Όμως αυτό που κάνει ιδιαίτερο το bitcoin αντιστοίχως το κάνει και πιο δύσκολο στην κατανόηση όλων των λειτουργιών του καθώς πολλοί άνθρωποι δεν ξέρουν τι μπορούν να αγοράσουν , σε ποιες τοποθεσίες αλλά και άλλους τρόπους που μπορούν να χρησιμοποιήσουν τα bitcoin. Τα σημεία που κάποιος χρήστης bitcoin μπορεί να απευθυνθεί για κάποια αγορά είναι :

- Αγορές από καταστήματα που δέχονται άμεσα τα bitcoin.
- Ειδικές παροχές που το bitcoin είναι αποδεκτό σε μεγαλύτερο βαθμό.
- Να απευθυνθεί απευθείας σε διάφορους εμπόρους που δέχονται ως μέσο συναλλαγής τα bitcoin για τα προϊόντα ή τις υπηρεσίες που προσφέρουν.
- Να αποκτήσει κάποια κάρτα δώρου (που περιλαμβάνει bitcoin) δίνοντας την δυνατότητα να χρησιμοποιηθεί κάνοντας αγορές από εμπόρους που ακόμα δεν δέχονται άμεσες συναλλαγές με το bitcoin .

Το πιο βασικό σημείο για να πραγματοποιηθεί μια αγορά είναι τα καταστήματα που χωρίζονται σε online(με σύνδεση) και offline(χωρίς σύνδεση).

Τα online καταστήματα ουσιαστικά είναι ιστοσελίδες στο διαδίκτυο που δέχονται άμεσες πληρωμές με το bitcoin. Για να αγοράσει κάποιος από μια τέτοια ιστοσελίδα πρέπει να ακολουθήσει κάποια βήματα. Αρχικά πρέπει

να αντιγράψει την bitcoin διεύθυνση του ηλεκτρονικού καταστήματος, στην συνέχεια θα πρέπει να στείλει το ποσό που κοστίζει το συγκεκριμένο προϊόν από το ηλεκτρονικό πορτοφόλι του στην διεύθυνση αυτήν , και τέλος θα πραγματοποιηθεί η πληρωμή που κατά κύριο λόγο γίνεται στην ιστοσελίδα. Μερικά από αυτά τα καταστήματα παρέχουν QR κωδικό για πληρωμές μέσω κινητού τηλεφώνου . Στην περίπτωση που μια ιστοσελίδα – κατάστημα δεν δέχεται coins μπορεί να χρησιμοποιηθεί η κάρτα δώρο που θα γίνει αποδεκτή από μεταπωλητές που λαμβάνουν bitcoin . Δηλαδή τα χρήματα που έδωσε ένας χρήστης για την κάρτα αυτή μπορούν να χρησιμοποιηθούν για την αγορά των προϊόντων του καταστήματος . Μια από τις πιο δημοφιλείς κάρτες δώρου είναι η "gift" καθώς είναι αποδεκτή από πολλά καταστήματα. (Antonopoulos, 2020)

Τα offline καταστήματα είναι ουσιαστικά τα κοινά καταστήματα που κάνουμε τις αγορές μας και ποικίλουν σε είδη από ρούχα , οικοδομικά υλικά , εστιατόρια και καφετέριες . Αυτό όμως που είναι άξιο προσοχής είναι ότι ο μεγαλύτερος αριθμός καταστημάτων που δέχονται bitcoin προσφέρουν ποτά και τρόφιμα . Για την διευκόλυνση ενός κάτοχου bitcoin μπορεί απλά να χρησιμοποιηθεί ένας ηλεκτρονικός χάρτης που ονομάζεται coin map , εκεί που μπορεί να δει ανάλογα με την περιοχή που βρίσκονται τα καταστήματα που δέχονται πληρωμές με bitcoin . Ένα πολύ σημαντικό στοιχείο ή αλλιώς χαρακτηριστικό του bitcoin είναι ότι χρησιμεύει και στην απόκτηση αγαθών ή υπηρεσιών που αγοράζονται μόνο με αυτό χωρίς το παραδοσιακό χρήμα. Επομένως δημιουργήθηκαν κάποιες τοποθεσίες , υπηρεσίες που μπορείς να πληρώσεις μόνο με αυτό . Κάποιες από αυτές μπορεί να είναι τυχερά παιχνίδια . Τα πολύ γνωστά ηλεκτρονικά καζίνο που η πρόσβαση σε αυτά γίνεται μόνο με την διεύθυνση ip που δέχονται bitcoin ή κάποιο άλλο κρυπτονόμισμα. Επιπλέον υπάρχουν και κάποιες εταιρίες όπως η Amagi metals που

ασχολούνται συγκεκριμένα με την αγορά και την πώληση χρυσού με bitcoin. (Tu, 2020)

Υπάρχουν τρεις βασικές μεταβλητές σε οποιαδήποτε συναλλαγή bitcoin: ποσό, είσοδος και έξοδος. Μια είσοδος είναι η διεύθυνση από την οποία αποστέλλονται τα χρήματα και μια έξοδος είναι η διεύθυνση που λαμβάνει τα χρήματα. Δεδομένου ότι ένα πορτοφόλι μπορεί να περιέχει πολλές διευθύνσεις εισόδου, ο χρήστης μπορεί να στείλει χρήματα από μια ή περισσότερες εισόδους σε μια ή περισσότερες εξόδους. Επίσης, υπάρχει ένα τμήμα αποθήκευσης δεδομένων σε κάθε συναλλαγή, ένα είδος σημείωσης, που επιτρέπει να καταγράφει αμετάβλητα δεδομένα στο blockchain. Αυτό σημαίνει ότι το πορτοφόλι συνήθως καταλήγει σε πολλές διευθύνσεις για να κάνει μελλοντικές συναλλαγές. Για να πραγματοποιηθεί μια αγορά και να αποθηκευτεί, όπως έχει αναφερθεί σε προηγούμενα κεφάλαια, χρειάζονται τα ιδιωτικά και δημοσιά κλειδιά με σκοπό την πραγματοποίηση της συναλλαγής.

Για να γίνει αυτό , τοποθετείται το ιδιωτικό κλειδί , το ποσό των bitcoin που θέλει να στείλει ο χρήστης και την διεύθυνση εξόδου στο λογισμικό bitcoin στον υπολογιστή ή στο smartphone. Στην συνέχεια, το πρόγραμμα δημιουργεί μια υπογραφή από το ιδιωτικό κλειδί του χρήστη για να ανακοινωθεί αυτήν την συναλλαγή στο δίκτυο για επικύρωση. Το δίκτυο πρέπει να επιβεβαιώσει ότι ο χρήστης είναι κάτοχος του bitcoin που μεταφέρεται κα ότι δεν τα έχει ξοδέψει ελέγχοντας όλες τις προηγούμενες συναλλαγές που είναι δημοσιές στο καθολικό . Μόλις το πρόγραμμα bitcoin επιβεβαιώσει ότι πράγματι το ιδιωτικό κλειδί του χρήστη αντιστοιχεί στο παρεχόμενο δημόσιο κλειδί , η συναλλαγή επιβεβαιώνεται.

Αυτή η συναλλαγή περιλαμβάνεται τώρα σε ένα μπλοκ που συνδέεται με το προηγούμενο μπλοκ για προσθήκη στο blockchain . Κάθε συναλλαγή στο blockchain συνδέεται με ένα μοναδικό αναγνωριστικό που ονομάζεται

κατακερματισμός συναλλαγών (txid), το οποίο μοιάζει με μια συμβολοσειρά τυχαίων γραμμάτων και αριθμών 64 χαρακτήρων. Ο χρόνος που απαιτείται για την επιβεβαίωση μιας συναλλαγής ποικίλλει, οπουδήποτε από λίγα λεπτά έως μερικές μέρες , με βάση την επισκεψιμότητα στο blockchain και το μέγεθος της συναλλαγής σας . Μεγαλύτερες συναλλαγές με υψηλοτέρα τέλη τείνουν να επικυρώνονται από τους ανθρακωρύχους γρηγορότερα από τις μικρότερες . Μόλις επιβεβαιωθεί , καταγράφεται αμετάβλητα για πάντα . Στο bitcoin , κάθε block είναι σχεδιασμένο να έχει μέγεθος 1 Mb . Αυτό σημαίνει πως όταν συγκεντρωθούν αρκετές συναλλαγές ώστε το συνολικό τους μέγεθος να είναι 1 Mb , τότε το block θα κλείσει . Κάθε block περιέχει πάνω από 2.000 συναλλαγές . Κάθε συναλλαγή που καταγράφεται στο block επηρεάζει τον τελικό αριθμό που χρειάζεται στο mining για να κλείσει το block . Υπάρχει μεγάλος φόβος γύρω από το bitcoin οι άνθρωποι δεν το εμπιστεύονται γιατί δεν το γνωρίζουν , όμως πλέον στα τελευταία χρόνια οι συναλλαγές είναι πιο αξιόπιστες και πιο αποτελεσματικές σε σχέση με τις άλλες .

Το σημαντικό είναι ότι ανεξαρτήτως τοποθεσία σε όλον τον κόσμο οι συναλλαγές γίνονται άμεσα με χαμηλό κόστος αποστολής που ανέρχεται στα 0.001 btc ή χωρίς καμία χρέωση σε μερικές περιπτώσεις . Πρέπει όμως να κατανοήσουμε αρχικά ότι δεν υπάρχουν τα bitcoin ούτε μπορούν να αποθηκευτούν σε κάποιο σκληρό δίσκο . Μπορούμε να λεμέ ότι είμαστε κάτοχοι bitcoin αλλά όταν κοιτάμε σε μια διεύθυνση btc βλέπουμε ότι δεν υπάρχουν ψηφιακά νομίσματα που αποθηκεύονται εκεί . Αντιθέτως υπάρχουν συναλλαγές αναμεσά σε διαφορετικές διευθύνσεις με λογαριασμούς που αυξομειώνονται . Κάθε συναλλαγή που πραγματοποιήθηκε έχει καταγραφή σε έναν δημόσιο αρχείο .

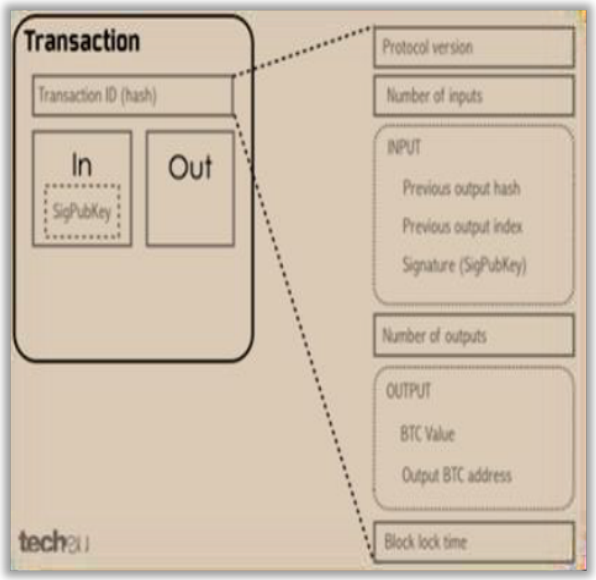
Οι συναλλαγές στέλνονται και λαμβάνονται μέσω του ηλεκτρονικού πορτοφολιού και όλοι στο δίκτυο του (bitcoin) γνωρίζουν την οποιαδήποτε συναλλαγή και τις λεπτομέρειες της. Υποθέτοντας ότι έχουμε δυο χρήστες

Α και Β και θέλουμε να πραγματοποιηθεί μια συναλλαγή. Αν ο χρήστης Α θέλει να στείλει bitcoin στον χρήστη Β τότε θα έχουμε τρία σημαντικά κομμάτια πληροφορίας αναμεσά στους δυο χρήστες:

- INPUT (εισαγωγή): Είναι η διεύθυνση bitcoin που χρησιμοποιήθηκε για να σταλούν τα νομίσματα στον χρήστη Α (δεν έχει σημασία από που τα έλαβε ο χρήστης Α)

- AMOUNT (ποσό): Αυτό είναι το ποσό που ο χρήστης Α στέλνει στον χρήστη Β.

- OUTPUT (εξαγωγή): Είναι η bitcoin διεύθυνση του χρήστη Β. Έτσι λοιπόν για να στείλει bitcoin χρειάζεσαι δυο πράγματα, μια διεύθυνση bitcoin και ένα ιδιωτικό κλειδί. Μια διεύθυνση bitcoin παράγεται τυχαία και είναι μια απλή ακολουθία από γράμματα και αριθμούς . Το ίδιο είναι και το ιδιωτικό κλειδί , απλά αντιθέτως με την διεύθυνση bitcoin είναι κρυφό. Σκεφτείτε ότι η διεύθυνση bitcoin είναι ένα ασφαλές γυάλινο κουτί , όλοι μπορούν να δουν μέσα του και ξέρουν επομένως τι περιέχει αυτό το κουτί αλλά κάνεις δεν μπορεί να το ανοίξει αν δεν έχει το ιδιωτικό κλειδί(private key). Έτσι λοιπόν όταν ο χρήστης Α θέλει να στείλει στον Β χρησιμοποιεί το ιδιωτικό του κλειδί για να στείλει ένα μήνυμα με την μεταβλητή INPUT(δηλαδή την πηγή συναλλαγής των νομισμάτων , το ποσό amount και το output). Στην συνέχεια στέλνει τα στοιχεία από το ηλεκτρονικό πορτοφόλι του στο ευρύτερο δίκτυο που εκεί οι ανθρακωρύχοι επικυρώνουν την συναλλαγή τοποθετώντας την σε ένα block .(Coinmarketcap, 2020)



Εικόνα 10:Μέθοδος Transaction

Πηγή : Shutterstock

ΚΕΦΑΛΑΙΟ 7:Το Σύστημα της Εξόρυξης(MINING)

Παρόμοια με την εξόρυξη χρυσού , τα bitcoin υπάρχουν στο σχεδιασμό του πρωτοκόλλου , όπως και ο χρυσός που υπάρχει υπόγεια και δεν έχει ακόμα σκαφτεί. Το πρωτόκολλο bitcoin ορίζει ότι θα υπάρξουν 21 εκατομμύρια bitcoin σε κάποιο σημείο . Αυτό που κάνουν οι ανθρακωρύχοι είναι να τους φέρουν στο φως , λίγα κάθε φορά . Μόλις οι ανθρακωρύχοι ολοκληρώσουν την εξόρυξη όλων αυτών των νομισμάτων , δεν θα υπάρξουν περισσότερα νομίσματα , εκτός εάν αλλάξει το πρωτόκολλο bitcoin για να επιτρέψει μεγαλύτερη προσφορά.

Οι ανθρακωρύχοι πληρώνονται σε τέλη συναλλαγής για την δημιουργία μπλοκ επικυρωμένων συναλλαγών και την συμπερίληψη τους στο blockchain. Για να γίνει κατανοητό πώς λειτουργεί η εξόρυξη bitcoin , θα χρησιμοποιήσουμε σαν παράδειγμα τους κόμβους. Ένας κόμβος είναι ένας ισχυρός υπολογιστής που τρέχει το λογισμικό bitcoin και επικυρώνει πλήρως τις συναλλαγές και τα μπλοκ . Δεδομένου ότι το δίκτυο bitcoin είναι αποκεντρωμένο , αυτοί οι κομβόι είναι συλλογικά υπεύθυνοι για την επιβεβαίωση των εκκρεμών συναλλαγών .

Ο καθένας μπορεί να εκτελέσει έναν κόμβο απλά κατεβάζοντας ένα δωρεάν λογισμικό bitcoin. Το μειονέκτημα είναι ότι καταναλώνει ενέργεια και χώρο αποθήκευσης (το δίκτυο την στιγμή της γραφής παίρνει εκατοντάδες gigabyte δεδομένων). Οι κομβόι διαδίδουν συναλλαγές bitcoin στο δίκτυο. Ένας κόμβος θα στείλει πληροφορίες σε μερικούς κόμβους που γνωρίζει, ο οποίος θα μεταδώσει τις πληροφορίες σε κόμβους που γνωρίζουν κ.λπ.. Με αυτόν τον τρόπο, η εκκρεμούσα συναλλαγή καταλήγει να μετακινείται σε όλο το δίκτυο αρκετά γρήγορα.

Ορισμένοι κομβόι είναι κομβόι εξόρυξης, οι οποίοι συνήθως αναφέρονται ως «ανθρακωρύχοι». Τα κομμάτια στα οποία εκκρεμούν συναλλαγές σε μπλοκ προστίθενται στο blockchain. Αυτό γίνεται με την επίλυση ενός

σύνθετου μαθηματικού παζλ που αποτελεί μέρος του προγράμματος bitcoin και συμπεριλαμβανομένης της απάντησης στο μπλοκ . Το παζλ που χρειάζεται επίλυση, αφορά στην εξεύρεση ενός αριθμού ο οποίος όταν συνδυάζεται με τα δεδομένα στο μπλοκ και διέρχεται μια συνάρτηση κατακερματισμού -η οποία μετατρέπει τα δεδομένα εισόδου οποιουδήποτε μεγέθους, σε δεδομένα εξόδου σταθερού μεγέθους-, παράγει ένα αποτέλεσμα που βρίσκεται εντός ενός συγκεκριμένου εύρους .(Bitcoin Dedicated Servers, 2020)

Εικόνα 11:Απεικόνιση Συστήματος Εξόρυξης
Πηγή Coindesk

Για τους λάτρεις των trivia , αυτός ο αριθμός ονομάζεται ‘nonce’ , που είναι συντομογραφία του «number used once» . Στο blockchain , το nonce είναι ένας ακέραιος αριθμός μεταξύ του 0 και 4.294.967.296.

Η συνάρτηση κατακερματισμού καθιστά αδύνατο να προβλεφθεί ποια θα είναι η έξοδος. Έτσι οι ανθρακωρύχοι προσπαθούν να μαντέψουν τον μυστικό αριθμό χρησιμοποιώντας την εφαρμογή της συνάρτησης

κατακερματισμού στο συνδυασμό αυτό ο οποίος ξεκινά με ένα αριθμό μηδενικών. Δεν υπάρχει τρόπος να μαθευτεί ποιος αριθμός θα λειτουργήσει, γιατί δυο συνεχόμενοι ακέραιοι αριθμοί θα δώσουν εξαιρετικά διαφορικά αποτέλεσμα. Επιπλέον , μπορεί να υπάρχουν αρκετοί τρόποι που παράγουν το επιθυμητό αποτέλεσμα ή μπορεί να μην υπάρχουν και καθόλου. Έτσι οι ανθρακωρύχοι στην περίπτωση αυτή, συνεχίζουν να προσπαθούν αλλά με διαφορετική διαμόρφωση μπλοκ. Η δυσκολία του υπολογισμού (ο απαιτούμενος αριθμός μηδενικών στην αρχή της συμβολοσειράς κατακερματισμού) προσαρμόζεται συχνά, έτσι ώστε να απαιτείται κατά μέσο ορό περίπου δέκα λεπτά για την επεξεργασία ενός μπλοκ. Το χρονικό διάστημα που οι προγραμματιστές bitcoin θεωρούν απαραίτητο για μια σταθερή και φθίνουσα ροή νέων νομισμάτων είναι δέκα λεπτά και αναμένεται κάποια ότι στη διάρκεια του έτους 2140 να επιτευχθεί ο μέγιστος αριθμός των 21 εκατομμυρίων.

Ο πρώτος ανθρακωρύχος που έχει σαν αποτέλεσμα κατακερματισμού εντός της επιθυμητής περιοχής ανακοινώνει την νίκη του στο υπόλοιπο δίκτυο . Όλοι οι άλλοι ανθρακωρύχοι σταματούν αμέσως να δουλεύουν σε αυτό το μπλοκ και αρχίζουν να προσπαθούν να καταλάβουν τον μυστήριο αριθμό για τον επόμενο. Ως ανταμοιβή για την δουλειά του , ο νικητής ανθρακωρύχος παίρνει κάποιο νέο bitcoin . Την στιγμή της γραφής , η επιβράβευση είναι 6,25 btc ανα μπλοκ , η οποία αξίζει περίπου 56.000$ τον Ιούνιο του 2020. Ωστόσο, δεν είναι τόσο ευχάριστη συμφωνία όσο ακούγεται. Υπάρχουν πολλοί κόμβοι εξόρυξης που ανταγωνίζονται για αυτήν την ανταμοιβή, και όσο περισσότερη υπολογιστική ισχύς υπάρχει και όσοι περισσότεροι υπολογισμοί μπορούν να εκτελεστούν από έναν χρήστη, τόσο πιο κερδοφόρο είναι. Επίσης το κόστος της εξόρυξης είναι σημαντικό, όχι μόνο λόγω του ισχυρού υλικού που απαιτείται, αλλά και λόγω των μεγάλων ποσοτήτων ηλεκτρικής ενέργειας που καταναλώνουν αυτοί οι επεξεργαστές. (CoinDesk, 2020)

Ο αριθμός των bitcoin που απονέμονται ως ανταμοιβή για την επίλυση του παζλ θα μειωθεί . Αυτήν την χρονική στιγμή είναι στα 6,25 btc, αλλά κάθε τέσσερα χρονιά θα μειώνεται στα μισά (το επόμενο αναμένεται το 2024). Η αξία του bitcoin σε σχέση με το κόστος ηλεκτρικής ενέργειας και υλικού θα μπορούσε να αυξηθεί τα επόμενα χρονιά για να αντισταθμίσει εν μέρει αυτήν την μείωση , αλλά δεν είναι βέβαιο.

Πώς μπορεί να δημιουργηθεί ένα υλικό εξόρυξης bitcoin και να αρχίσει να δημιουργεί ο χρήστης ψηφιακά νομίσματα; Το πρώτο πράγμα που θα πρέπει να γίνει είναι να αποφασίσει ο χρήστης για το υλικό. Ο ρυθμός κατακερματισμού είναι ο αριθμός των υπολογισμών που μπορεί να εκτελεί το υλικό κάθε δευτερόλεπτο καθώς προσπαθεί να σπάσει το μαθηματικό πρόβλημα που επιγράφθηκε παραπάνω. Τα ποσοστά κατακερματισμού μετρώντας σε megahash, gigahash και terahashes ανά δευτερόλεπτο. Όσο υψηλότερο είναι το ποσοστό κατακερματισμού(σε σύγκριση με τον τρέχοντα μέσο όρο κατακερματισμού) , τόσο πιθανότερο είναι να επιλυθεί ένα μπλοκ συναλλαγών. (CoinDesk, 2020)

Εικόνα 12 :Επαγγελματική Μονάδα Εξορυξης Bitcoin
Πηγή Coindesk

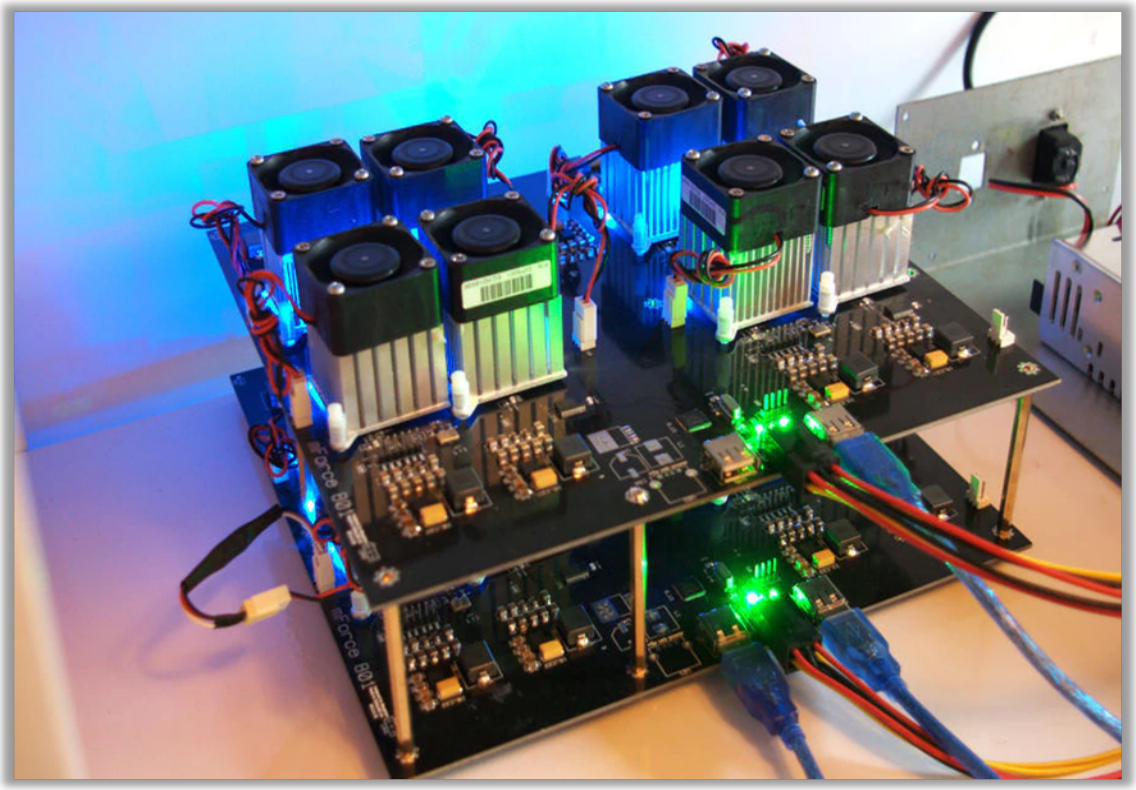
Η σελίδα σύγκρισης υλικού εξόρυξης του bitcoin wiki είναι ένα καλό μέρος για να βρει κάθε χρήστης ακατάλληλες πληροφορίες σχετικά με τα ποσοστά κατακερματισμού για διαφορετικό υλικό. Όταν επιλεχθεί ένα υλικό , αξίζει να παρατηρηθεί η κατανάλωση ενέργειας της συσκευής. Όλη αυτή η υπολογιστική δύναμη καταναλώνει ηλεκτρισμό και αυτό έχει σαν αποτέλεσμα να κοστίζει χρήματα . Για να υπολογίσει ένα χρήστης πόσους κατακερματισμούς παίρνει για κάθε watt ηλεκτρικής ενέργειας που χρησιμοποιείται, πρέπει να γίνει διαίρεση του αριθμού του κατακερματισμού με τον αριθμό των watt.

Για παράδειγμα, εάν ένας χρήστης διαθέτει συσκευή 500 GH/sec και καταναλώνει 400 watt , τότε παίρνει 1,25 GH/sec ανά watt . Σε ορισμένες περιπτώσεις θα χρησιμοποιείται ο υπολογιστής του χρήστη για να εκτελείται το υλικό εξόρυξης . Ο υπολογιστής έχει το δικό του ηλεκτρικό ρεύμα πάνω από το υλικό εξόρυξης και θα πρέπει να ληφθεί υπόψη στον υπολογισμό που θα γίνει.

Υπάρχουν τρεις κυρίες κατηγορίες υλικού για τους ανθρακωρύχους bitcoin: GPU, FPGA και ASIC. Για να μπορέσει κάποιος να δημιουργήσει bitcoin χρειάζεται επεξεργαστική ισχύ. Αρχικά η εξόρυξη πραγματοποιούνταν με την χρήση CPU (κεντρικός επεξεργαστής) ενός υπολογιστή. Όμως στην συνέχεια αποδείχθηκε ότι ο GPU (επεξεργαστής γραφικών) είναι πολύ πιο γρήγορος και αποτελεσματικός. Το μόνο μειονέκτημα αυτού του τρόπο εξόρυξης ήταν ότι παρότι οι κάρτες γραφικών έχουν την δυνατότητα να παράγουν εκατομμύρια hashes (κρυπτογραφικές συναρτήσεις κατακερματισμού του μαθηματικού αλγορίθμου που χρησιμοποιούνται για την επαλήθευση των συναλλαγών και συμβολίζουν την ταχύτητα της εξόρυξης) χρησιμοποιούν μεγάλα ποσά ενέργειας έχοντας ως συνέπεια μεγάλη παραγωγή θερμότητας που φυσικά οδηγεί στην ύπαρξη προβλημάτων τροφοδότησης και ψύξης τους. Επομένως η ανεύρεση νέων τροπών για mining ήταν μονόδρομος για αυτό

τον λόγο υπήρξε η κατασκευή των FPGA και ASIC συσκευών καθώς η εξόρυξη GPU είναι σε μεγάλο βαθμό νεκρή αυτές τις ημέρες λόγω της δυσκολίας εξόρυξης bitcoin η οποία έχει επιταχυνθεί τόσο πολύ με την απελευθέρωση της εξορυκτικής δύναμης ASIC που οι κάρτες γραφικών δεν μπορούν να τις ανταγωνιστούν.

Το **Field Programmable Gate Array (FPGA)** είναι ένα ολοκληρωμένο κύκλωμα σχεδιασμένο να διαμορφώνεται μετά την κατασκευή. Αυτό επιτρέπει σε έναν κατασκευαστή υλικού εξόρυξης να αγοράσει τις μάρκες σε όγκο και στην συνέχεια να τις προσαρμόσει για εξόρυξη bitcoin πριν τις τοποθετήσει στον δικό τους εξοπλισμό. Επειδή είναι προσαρμοσμένα για εξόρυξη, προσφέρουν βελτιώσεις απόδοσης έναντι των CPU & GPU . Είναι συσκευές στο μέγεθος μιας αστρονομικής ταυτότητας που μπορούν να αναπαράγουν εκατομμύρια hashes/δευτερόλεπτο χρησιμοποιώντας προγραμματιζόμενους επεξεργαστές .(array, 2020)



Εικόνα 13: Σύστημα Εξόρυξης FPGA

Πηγή : Coindesk

Τα **ειδικά ολοκληρωμένα κυκλώματα εφαρμογών (ASIC)** έχουν σχεδιαστεί ειδικά για να κάνουν μόνο ένα πράγμα : να κάνουν εξόρυξη bitcoin σε ταχύτητες συντριβής , με σχετικά μικρή χαμηλή κατανάλωση ενέργειας . Επειδή αυτές οι μάρκες πρέπει να σχεδιαστούν ειδικά για αυτό το έργο και στην συνέχεια να κατασκευαστούν , είναι ακριβές και χρονοβόρα στην παραγωγή , αλλά οι ταχύτητες τους είναι εκπληκτικές . Κατά την στιγμή της γραφής , οι μονάδες πωλούν με ταχύτητες οπουδήποτε από 5-500 GH/sec (αν και στην πραγματικότητα η μεταφορά ορισμένων από αυτά είναι πολύ δύσκολη). Οι προμηθευτές υπόσχονται ήδη ASIC συσκευές με πολύ περισσότερη ισχύ που θα επεκτείνονται σε 2 TH/sec.

Μια από τις άλλες βασικές παραμέτρους εδώ είναι η δυσκολία δικτύου. Αυτή η μέτρηση καθορίζει ποσό δύσκολο είναι να επιλυθεί ένα μπλοκ συναλλαγών και ποικίλλει ανάλογα με τον ρυθμό κατακερματισμού του δικτύου. Η δυσκολία είναι πιθανό να αυξηθεί σημαντικά καθώς οι συσκευές ASIC κυκλοφορούν στην αγορά, οπότε ίσως αξίζει να αυξήσει ο χρήστης την μέτρηση στην αριθμομηχανή για να δει πως θα είναι η απόδοση της επένδυσης. Μόλις επιλεχθεί το υλικό, θα πρέπει να γίνουν και κάποια πράγματα παραπάνω. Ανάλογα με τον εξοπλισμό που θα επιλεγεί, θα χρειαστεί να εκτελεστεί λογισμικό που θα χρησιμοποιήσει ο χρήστης. Συνήθως όταν χρησιμοποιείται GPU και FPGA, θα χρειαστεί ένας κεντρικός υπολογιστής που εκτελεί δυο πράγματα: τον τυπικό πελάτη bitcoin και το λογισμικό εξόρυξης.

Ο τυπικός πελάτης bitcoin συνδέει τον υπολογιστή στο δίκτυο και το επιτρέπει να αλληλοεπιδρά με τους πελάτες bitcoin, να προωθεί συναλλαγές και να παρακολουθεί την αλυσίδα μπλοκ. Θα χρειαστεί λίγος χρόνος για να κατεβάσει ολόκληρη την αλυσίδα μπλοκ bitcoin για να

ξεκινήσει. Ο πελάτης bitcoin μεταδίδει αποτελεσματικά πληροφορίες μεταξύ του miner και του δικτύου bitcoin.

Το λογισμικό εξόρυξης bitcoin είναι αυτό που καθοδηγεί το υλικό να κάνει την σκληρή δουλειά , περνώντας από μπλοκ συναλλαγών για να το λύσει . Υπάρχει μια ποικιλία από αυτά διαθέσιμα , ανάλογα με το λειτουργικό σύστημα . Είναι διαθέσιμα για Windows, Mac OS X και άλλα. Μπορεί επίσης να χρειαστεί ένα λογισμικό εξόρυξης και για τον ανθρακωρύχο ASIC.

Ένας έξυπνος προγραμματιστής παρήγαγε ακόμη και ένα λειτουργικό σύστημα εξόρυξης που έχει σχεδιαστεί και λειτουργεί στο Raspberry Pi, έναν υπολογιστή Linux με μέγεθος πιστωτικής κάρτας χαμηλού κόστους, σχεδιασμένος να καταναλώνει πολύ μικρές ποσότητες ενέργειας. Αυτό θα μπορούσε να χρησιμοποιηθεί για την τροφοδοσία ενός ASIC που συνδέεται με USB. (circuit)

Εικόνα 14:ASIC mining system
Πηγή: Coindesk

Τα **mining pools** είναι η διαδικτυακή μέθοδος εργασίας οπού πολλοί ανθρακωρύχοι εργάζονται προς τον ίδιο σκοπό δηλαδή την ανεύρεση του μπλοκ . Συγκεκριμένα είναι μια μέθοδος συνεργασίας που είναι αναγκαία γιατί πολύ απλά ένας χρήστης σε ατομικό επίπεδο θα έπρεπε να διαθέσει πολύ περισσότερο χρόνο. Επίσης τα bitcoin που ανακαλύπτονται από τα συγκεκριμένα μπλοκ δίνονται σε όλους τους χρήστες που συμμετείχαν αναλόγως με την αντίστοιχη προσπάθεια που κατέβαλαν δηλαδή την επεξεργαστική ισχύ.

Τα πιο διάσημα mining pools είναι:

- **Ant pool**: Είναι μια από τις μεγαλύτερες εταιρίες bitcoin στην Κίνα που ελέγχει το 30% των hash rate όλου του δικτύου.
- **BTCC**: Έχει στην επιρροή της το 15% hash rate του δικτύου.
- **Slush pool**: Διευθύνεται από τα satoshi tabs και έχει έδρα στην Τσεχία. Ο έλεγχος της ανέρχεται στα 7% hash rate του δικτύου.
- **F2POOl**: Είναι η δεύτερη μεγαλύτερη mining pool εταιρία που υπάρχει ελέγχοντας το 25% hash rate του δικτύου όμως το γραφικό του περιβάλλον υποστηρίζει μόνο την κινέζικη γλώσσα.
- **ELIGIUS**: Ήταν η πρώτη mining pool εταιρία που είχε δημιουργηθεί και σήμερα ελέγχει κάτι λιγότερο από το 1% hash rate του δικτύου.
- **BTMINER**: Όπως και η ELIGIUS πλέον ελέγχει κάτι λιγότερο από το 1%.
- **KanockPOOL**: Δημιουργήθηκε το 2014 και σήμερα ελέγχει το 3% hash rate.

Εικόνα 15:Κτίριο Στέγασης Mining Pool Εταιρίας
Πηγή: Coindesk

7.1 Υλοποίηση της Εξόρυξης

Το bitcoin έχει εισέλθει στην παγκόσμια οικονομία και έχει αποκτήσει μεγάλη δύναμη. Η ιδιότητα του χρυσού που διαθέτει αλλά και η ανεξαρτητοποίηση του από τα αλλά νομίσματα το καθιστά πολύτιμο αλλά ταυτόχρονα δύσκολο στην παραγωγή του καθώς αυτό συσχετίζεται με τον προκαθορισμένο αριθμό παραγωγής του. Όπως έχει αναφερθεί σε προηγούμενο κεφάλαιο, η παραγωγή των bitcoin γίνεται με την διαδικασία της εξόρυξης, κατά την οποία ένας μαθηματικός αλγόριθμος διανέμεται σε χρήστες του bitcoin και η λύση του οδηγεί σε ανεύρεση νέων μπλοκ με ανταμοιβή. **Το hardware που απαιτείται είναι οι επεξεργαστές και οι κάρτες γραφικών για «βασική» εξόρυξη ενώ οι διάφορες συσκευές εξόρυξης (FPGA, ASIC) χρησιμοποιούνται για μεγαλύτερο κέρδος.** Συνοπτικά μπορεί κάποιος να έχει κέρδος από το προσωπικό του υπολογιστή αλλά και να επενδύσει στις προαναφερόμενες συσκευές για να υπάρχει μηνιαίο εισόδημα. Πολλοί ανθρακωρύχοι επενδύουν σε ακριβές συσκευές ASIC με κόστος άνω των 500 ευρώ για να έχουν μεγάλη απόδοση και ταχύτητα εξόρυξης. (Icmec, 2020)

Θεωρώντας ότι η εξόρυξη αποτελεί ένα θέμα ιδιαίτερα ενδιαφέρον, ο μελετητής αυτής της διπλωματικής θα προχωρήσει στην αναφορά κάποιων βημάτων που μπορούν να ακολουθηθούν από τους ενδιαφερόμενους δυνητικούς “miners” με σκοπό την εξόρυξη κρυπτονομίσματος με απλά μέσα (π.χ. τον ήδη υπάρχον υπολογιστή).

Στην παρούσα διαδικασία καμία επιπλέον συσκευή δεν θα χρησιμοποιηθεί και δεν υπάρχει κάποιο κόστος ούτε σε software ούτε σε hardware εκτός βέβαια από έναν προσωπικό υπολογιστή μέσης τιμής ή κάποια πλατφόρμα. Ο σκοπός είναι η χαρτογράφηση του τρόπου εξόρυξης από τον προσωπικό υπολογιστή .

Η ταχύτητα εξόρυξης του bitcoin είναι άμεσα συσχετιζόμενη με το hardware που χρησιμοποιείται. Ένα υπολογιστής που θεωρείται «καλός» είναι πιο αποδοτικός στο hash rate (ο αριθμός των τυχαίων συνδυασμών που πραγματοποιείται το δευτερόλεπτο από μια υπολογιστική συσκευή). Αυτό ισχύει και για την κάρτα γραφικών, δεν σημαίνει όμως ότι ένα παλιό σύστημα που μπορεί να διαθέτει κάποιος στο σπίτι του δεν είναι ικανό να προσφέρει κέρδος. Έτσι το hardware του υπολογιστή που χρησιμοποιήθηκε από τον μελετητή έχει φυσιολογικό εύρος τιμών για έναν επιτραπέζιο υπολογιστή που αποκτήθηκε το 2018 έναντι των 700 ευρώ. Παρακάτω δίνεται αναλυτικά η λίστα των προϊόντων αλλά και το κόστος:

HARDWARE	**ΠΡΟΙΟΝ**	**ΤΙΜΗ /€**
ΕΠΕΞΕΡΓΑΣΤΗΣ	INTEL i3 6300K	**180**
ΚΑΡΤΑ ΓΡΑΦΙΚΩΝ	SAPPHIRE RX 570	**290**
ΜΝΗΜΗ RAM	CORSAIR 32GB	**180**
ΤΡΟΦΟΔΟΤΙΚΟ	CORSAIR 500W	**70**
ΣΚΛΗΡΟΣ ΔΙΣΚΟΣ	SAMSUNG M.2 250GB	**140**
ΛΕΙΤΟΥΡΓΙΚΟ ΣΥΣΤΗΜΑ	WINDOWS 10 PRO	**-**

Ο επεξεργαστής και η κάρτα γραφικών είναι τα κύρια στοιχεία που διαμορφώνουν την ταχύτητα της εξόρυξης . Εκτός από τον παράγοντα της απόδοσης πρέπει να υπολογιστεί ο παράγοντας το κόστους. Για τον συγκεκριμένο λόγο πρέπει να δώσουμε έμφαση στο τροφοδοτικό του υπολογιστή. Ένα τροφοδοτικό πολλών watt μπορεί να καταναλώσει περισσότερο ηλεκτρικό ρεύμα άρα περισσότερα έξοδα από τα κέρδη της εξόρυξης. Επίσης παίζει ρολό και η τιμή του bitcoin που είναι ανάλογη με τα κέρδη, δηλαδή όσο αυξάνεται η χρηματιστηριακή τιμή του τόσο αυξάνεται το χρηματικό ποσό που θα λάβει ο χρήστης.

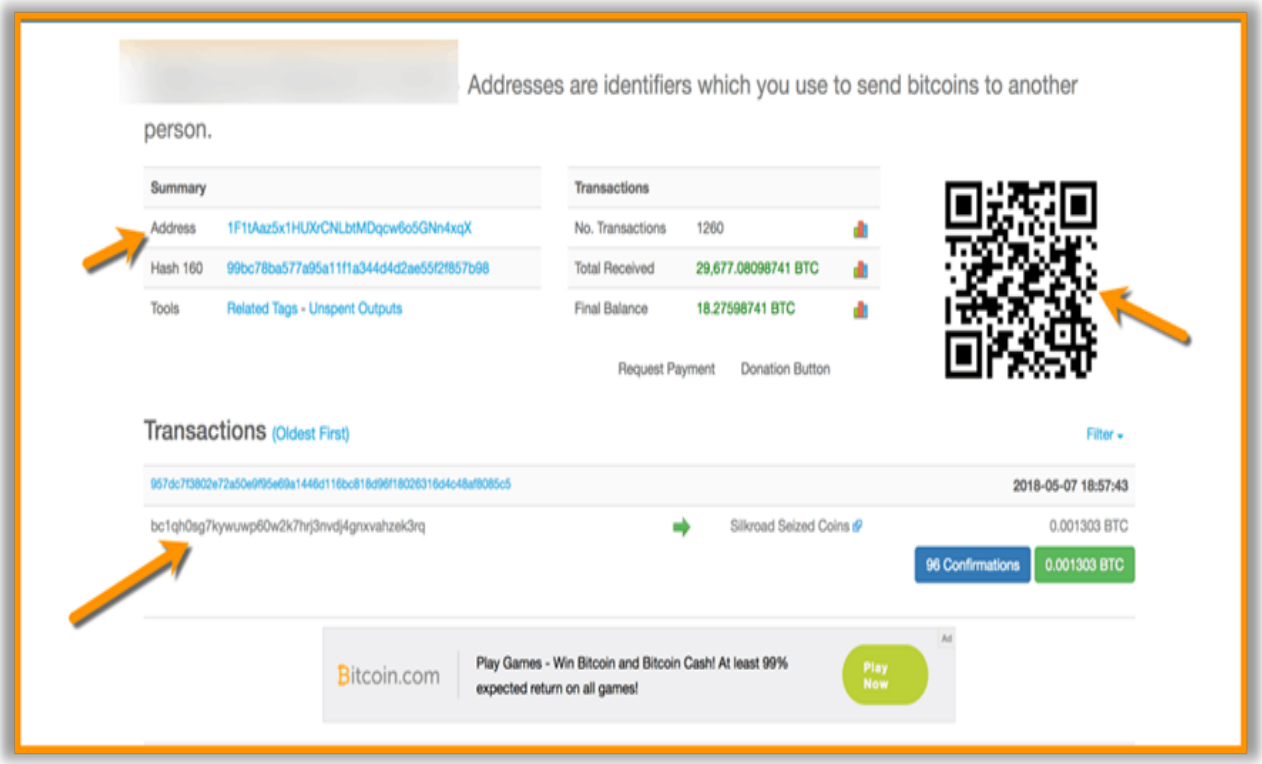
Όσο σημαντικό είναι το hardware άλλο τόσο σημαντικό είναι και το software καθώς παρομοιάζεται με τον «οδηγό» της διαδικασίας, δηλαδή το πρόγραμμα mining που εκτελεί την διαδικασία της εξόρυξης. Υπάρχουν διαφορά προγράμματα εξόρυξης ανάλογα με το λειτουργικό σύστημα που διαθέτει κάθε χρήστης. Στην παρούσα εργασία χρησιμοποιήθηκε το σύστημα «BLOC GUI MINER» το οποίο υποστηρίζεται και από windows αλλά και από MacOS. Ο συγκεκριμένος miner μπορεί να χρησιμοποιηθεί για την παραγωγή και άλλων ψηφιακών νομισμάτων.

Εικόνα 16:BLOC GUI MINER

Πηγή: medium

Η εκκίνηση του miner πραγματοποιείται πολύ εύκολα με το πάτημα ενός κουμπιού αλλά είναι απαραίτητο να οριστούν κάποιες επιλογές που θα κάνουν την διαδικασία πολύ πιο ευέλικτη. Αρχικά η σημαντική παράμετρος που πρέπει να ρυθμιστεί στο πρόγραμμα είναι η διεύθυνση του ηλεκτρονικού πορτοφολιού που διαθέτει ο χρήστης με στόχο να αποσταλούν τα κέρδη μετά την εξόρυξη . Αυτό συμπληρώνεται ευκολά στην σελίδα Payout Address όπως φαίνεται στην παρακάτω εικόνα , στην

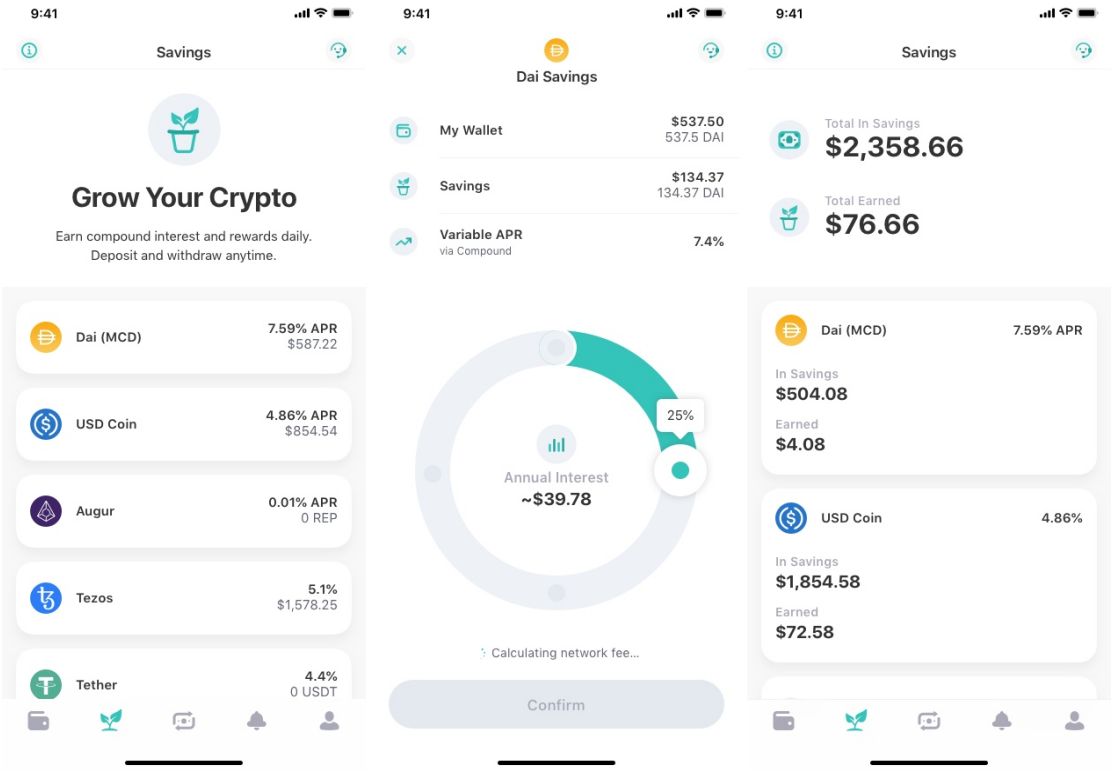
οποία δημιουργείται και ο κωδικός QR από τον οποίο σκανάροντας το έχει ως αποτέλεσμα την ταχύτητα και την ασφάλεια .



Εικόνα 17::Bitcoin Payout Address
Πηγή: medium

Στην συνέχεια η mining pool είναι εξίσου σημαντική για την διαδικασία της εξόρυξης και του κέρδους που θα αποκομίσει, καθώς μια μεγάλη pool είναι πιο αποτελεσματική από μια μικρότερη .

Στόχος της εργασίας αυτής ήταν να βοηθήσει τους αναγνώστες να κατανοήσουν τον τρόπο παραγωγής bitcoin με σχεδόν μηδαμινό κόστος χωρίς επιπλέον εξοπλισμό μέσω μιας εικονικής διαδικασίας από την αρχή έως την ολοκλήρωση της. Για αυτό τον λόγο χρησιμοποιήθηκε ένας μέσης τιμής επιτραπέζιος υπολογιστής. Σχεδόν όλες οι mining pool έχουν κάποιο payout και αυτό γιατί θέλουν να διασφαλίσουν την λειτουργία τους . Το payout είναι το όριο ή το ποσό που πρέπει να φτάσει κάποιος χρήστης κατά την διαδικασία της εξόρυξης, ώστε να σταλούν τα κέρδη από την mining pool στο ηλεκτρονικό πορτοφόλι.



Εικόνα 18: Bitcoin e-wallet

Πηγή: medium

ΚΕΦΑΛΑΙΟ 8:Πλανο Κατασκευής ASIC Συσκευής

Μέσα από τα προηγούμενα κεφάλαια έγινε μια προσπάθεια κατανόησης και λειτουργίας του ψηφιακού νομίσματος μέσω της εικονικής διαδικασίας στην οποία χρησιμοποιήσαμε έναν υπολογιστή για να μπορέσουμε να ανταπεξέλθουμε σε όσα μας ζητάει η μέθοδος της εξόρυξης . Παρόλα αυτά το πλάνο της συγκεκριμένης εργασίας είναι να δώσει την δυνατότητα σε οποιονδήποτε χρήστη, είτε αυτός είναι αρχάριος (newbie) είτε είναι προχωρημένος(professional), να δημιουργήσει την δικιά του ξεχωριστή συσκευή εξόρυξης, η οποία θα χρησιμοποιείται για έναν και μόνο σκοπό, την παραγωγή bitcoin. Η συσκευή που θα προταθεί μπορεί να την αγοράσει η πλειοψηφία των αναγνωστών καθώς κοστίζει ολοκληρωμένη περίπου 100-150€. Για να "στήσουμε" αυτήν την συσκευή δεν χρειάζεται ο χρήστης να έχει εξειδικευμένες τεχνικές γνώσεις αρκεί να ακολουθήσει όλα τα βήματα που θα παρουσιαστούν παρακάτω με υπομονή και σχολαστικότητα. Θα αναπτυχθούν δυο κεφάλαια στα οποία θα παρουσιάζεται τόσο η «hardware» διαδικασία όσο και η υλοποίηση του «software».

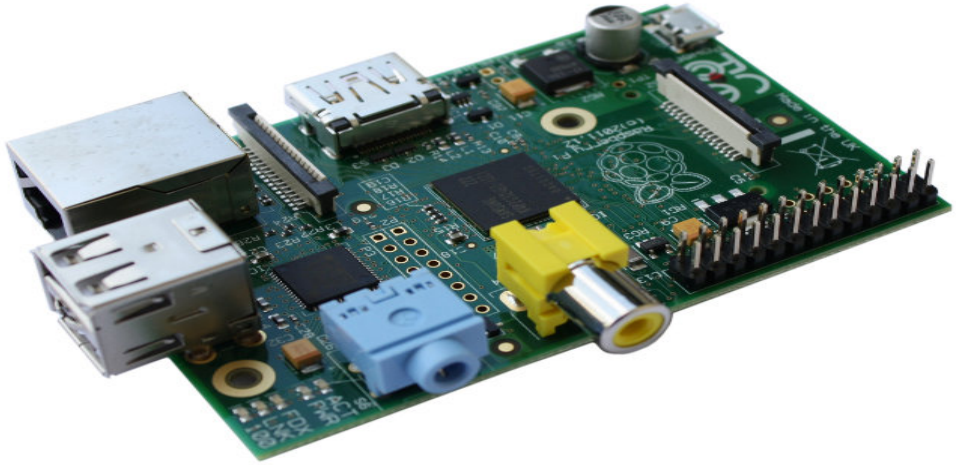
8.1 Τμήμα Υλοποίησης Hardware

Τα πρώτα βήματα που θα χρειαστεί να κανουμε για να ξεκινησει η διαδικασια υλοποιησης, είναι η αγορα του εξοπλισμου. Παρακατω θα αναφερθει μια λιστα πραγματων που θα χρησιμοοιησουμε σε αυτην την εργασία.

ΠΡΟΙΟΝ	**ΤΙΜΗ**
6 port USB hub	60€
Raspberry pi v.2	25€
Sd card (over 4GB)	20€
USB fan	10€
USB ASIC block miner	20€
PC case for Raspberry pi	10€

Το μέγεθος του Raspberry Pi v.2 είναι σε μέγεθος παρόμοιο με μια κάρτα τραπέζης και αυτό μας εξυπηρετεί από χωροταξικής εννοίας. Η συγκεκριμένη συσκευή μπορεί να λειτουργήσει ξεχωριστά από έναν υπολογιστή, γιατί πολύ απλά μπορεί να εκτελέσει ακριβώς τις ιδίες διαδικασίες με έναν κλασσικό υπολογιστή. Μια από τις δυνατότητες αυτής της συσκευής είναι ότι μπορεί να τροφοδοτηθεί ακόμα και από Usb καλώδιο, με αποτέλεσμα η συσκευή να θεωρείται μετακινήσιμη σε οποιοδήποτε χώρο αρκεί να βρίσκεται συνδεδεμένο σε ένα μεγάλο χωρητικότητας power bank άνω των 20.000mAh και να έχουμε συνδέσει πάνω στην συσκευή ένα Usb WIFI, διότι δίχως δίκτυο σταματάει αυτόματα η διαδικασια της εξόρυξης. Για λογούς ασφάλειας θα χρησιμοποιηθεί ένα κουτί προστασίας για τυχόν φθορές πάνω στην πλακέτα. Ότι αφορά το υπόλοιπο σύστημα, η κάρτα μνήμης Sd θα λειτουργήσει ως μέσο αποθήκευσης του λειτουργικού συστήματος που θα μπουτάρουμε στο Raspberry Pi. Αφού ολοκληρώσουμε την διαδικασία σεταρίσματος του λειτουργικού συστήματος, το μόνο που μας απομένει ένα μέσο στο οποίο θα λειτουργεί μέσα ένα πρόγραμμα εξόρυξης των bitcoin. Αυτό πραγματοποιείται με ένα Usb basic block miner που παράγει 345 megahashes/sec, το οποίο έχει την μορφή ενός κλασσικού Usb stick και βέβαια υπάρχει η δυνατότητα να χρησιμοποιηθούν περισσότερα από ένα

στικάκια τέτοιου τύπου. Στην εργασία χρησιμοποιούνται 6 τέτοια Usb, τα οποία αποδίδουν συνολικά περίπου 2 gigahashes/sec. Για να τροφοδοτηθούν όλα τα στικάκια, θα τα τοποθετήσουμε στο Usb hub που έχει αγορασθεί πάνω στο οποίο θα εισάγουμε και ένα fan το οποίο θα κρατάει τις θερμοκρασίες του συστήματος στο επιτρεπτό οροί. Τελειώνοντας, μετα την ολοκλήρωση όλων των σημείων, θα πρέπει να συνδέσουμε το καλώδιο δικτύου για να περάσουμε στο κομμάτι υλοποιησης του software.

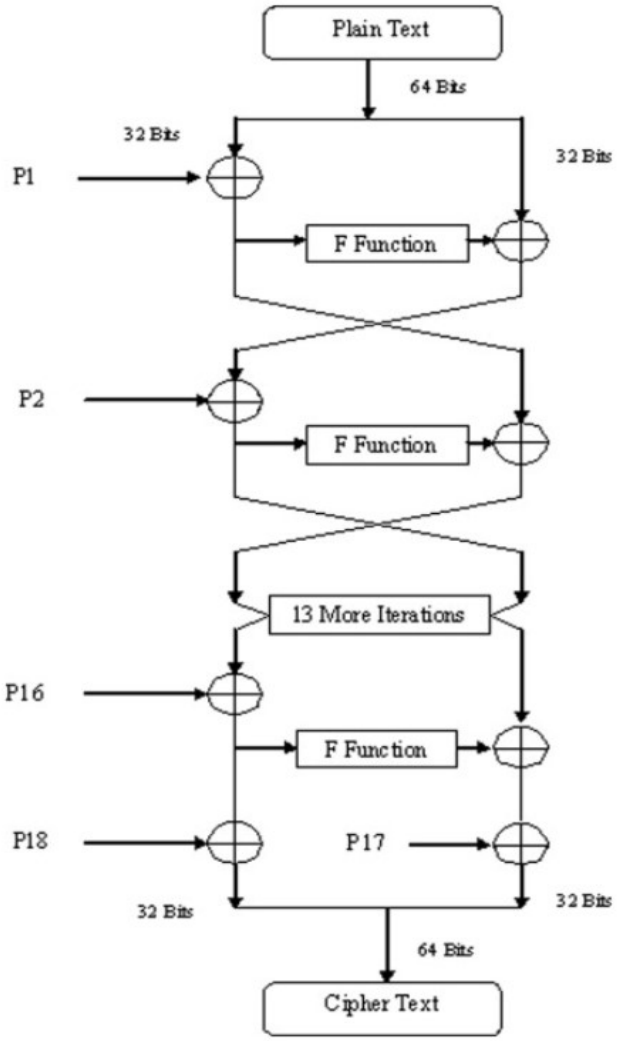


Εικόνα 19:Raspberry Pi v.2

Εικόνα 20:Usb Asic miner

8.2 Τμήμα Υλοποίησης Εφαρμογής ASIC του Αλγορίθμου Κρυπτογράφησης

Ο απώτερος στόχος της έρευνας που παρουσιάζεται σε αυτό το κεφάλαιο είναι η ανάπτυξη ενός αλγορίθμου κρυπτογράφησης χαμηλής ισχύος, υψηλής απόδοσης, σε πραγματικό χρόνο, αξιόπιστο και ασφαλές, ο οποίος μπορεί να επιτευχθεί μέσω υλοποιήσεων υλικού και να αποφέρει ένα κέρδος μέσω αυτής της διαδικασίας. Το Blowfish έχει μέγεθος μπλοκ 64 bit και μεταβλητό μήκος κλειδιού από 32 έως 448 bit. Είναι ένα κρυπτογράφημα Feistel 16 στροφών το οποίο αποτελείται από P-Boxes(κουτιά μετάθεσης), S-Boxes(πλαίσια αντικατάστασης) και XOR.



Εικόνα 21: Ο Αλγόριθμος Blowfish

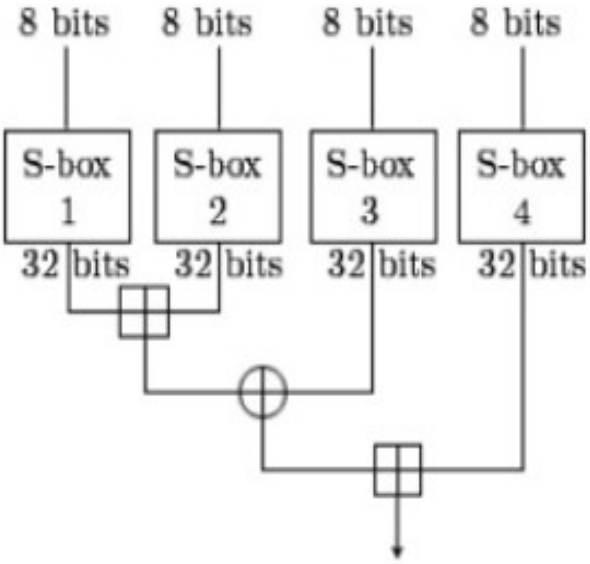
Πηγή : Science direct

Ένα μπλοκ 64 bit χωρίζεται σε δυο ίσα μισά μέρη : L και R. Στη συνέχεια, ορίζεται η Cipher Block όταν οι έξοδοι L και R του γύρου προσδιορίζονται από L και R του προηγούμενου.

$$L_i = L_{i-1}$$

$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i),$$

Όπου K_i είναι το δευτερεύον κλειδί που χρησιμοποιείται στον πρώτο γύρο και το F είναι συγκεκριμένο για τον συγκεκριμένο αλγόριθμο. Το κύριο χαρακτηριστικό αυτής της κατασκευής είναι ότι είναι αναστρέψιμη, δηλαδή το ίδιο δίκτυο (με τα κλειδιά πρόσβασης με αντίστροφη σειρά) χρησιμοποιείται τόσο για κρυπτογράφηση όσο και για αποκρυπτογράφηση.



Εικόνα 22:Η συνάρτηση Feistel του Blowfish

Πηγή : Science direct

Για να κρυπτογραφηθούν μεγάλες σειρές δεδομένων χρησιμοποιώντας το Blowfish, το μήνυμα θα χαραχθεί σε μπλοκ των 64-bit έτσι ώστε να κρυπτογραφηθεί κάθε μπλοκ και να αποθηκεύσει τα δεδομένα.

Το κύριο πλεονέκτημα του αλγορίθμου Blowfish είναι το πολύπλοκο πρόγραμμα κλειδιών του. Τα βήματα για την δημιουργία του είναι τα εξής :

- Αρχικοποιείται πρώτα ο πίνακας P και μετα τα τέσσερα S – πλαίσια με δεκαεξαδικά ψηφία π.
- *XOR* P_1 με τα πρώτα 32 bit του κλειδιού, *XOR* P_2 με τα δεύτερα 32 bit του κλειδιού και ούτω καθεξής για όλα τα bit του κλειδιού*(έως* P_{18} *)*.
- Γίνεται κρυπτογράφηση της συμβολοσειράς all zero με τον αλγόριθμο Blowfish, χρησιμοποιώντας τα κλειδί που περιγράφονται στα δυο πρώτα βήματα.
- Γίνεται αντικατάσταση των P_1, P_2 με την έξοδο του προηγούμενου βήματος.
- Γίνεται κρυπτογράφηση της εξόδου του.
- Χρησιμοποιείται ο αλγόριθμος Blowfish με τα τροποποιημένα κλειδιά.
- Γίνεται αντικατάσταση των P_3, P_4 με την έξοδο της κρυπτογράφησης.
- Συνεχίζεται η διαδικασια, αντικαθιστώντας όλα τα στοιχεία του πίνακα *P* και στην συνέχεια και τα τέσσερα S-Box με την σειρά, με την έξοδο του συνεχώς μεταβαλλόμενου αλγορίθμου.

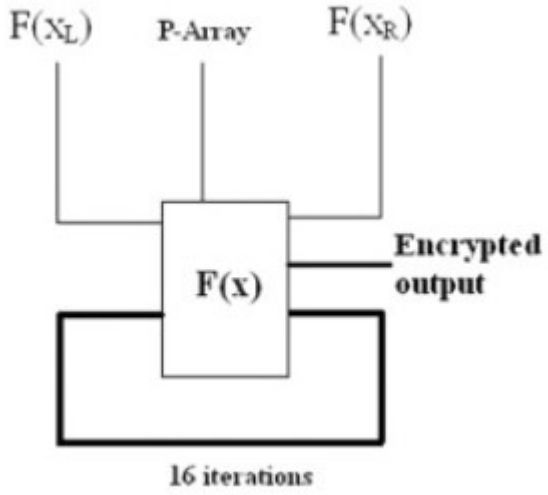
Ο προτεινόμενος αλγόριθμος θα δοκιμαστεί σε ένα FPGA. Αφού ληφθεί το ικανοποιημένο αποτέλεσμα, ο αλγόριθμος ακολουθεί το πρωτότυπο της τεχνολογίας των 130nm. Για ένα σχέδιο ASIC με ελάχιστη επιφάνεια πυριτίου, ακολουθείται η προσέγγιση από κάτω προς τα πάνω. Το πρωτότυπο τσιπ crypto – blowfish συντίθεται σε ένα Xilinx FPGA

χρησιμοποιώντας τεχνολογία VIRTEX. Για το προσαρμοσμένο σχεδιασμό IC, χρησιμοποιούνται διάφορα εργαλεία Synopsys με τεχνολογία συμπληρωματικού ημιαγωγού μεταλλικού οξειδίου (CMOS) 130nm. Το πρωτότυπο κρυπτό – τσιπ καταναλώνει ισχύ 7,3mW συμπεριλαμβανομένης της ισχύος μεταγωγής, βραχυκυκλώματος και διαρροής όταν λειτουργεί σε τροφοδοσία 1,0 V και συχνότητα 167 MHz. Το τσιπ δίνει απόδοση 2670 Mbps για την κρυπτογράφηση και 2642 Mbps για αποκρυπτογράφηση.

8.2.1 Εφαρμογη και Συγκριση Αποδοσης προσαρμοσμενου ASIC

Υπάρχουν δυο βασικά παραδείγματα για την εφαρμογή Blowfish. Ο πρώτος είναι ένας καθαρός συνδυασμός ή πλήρως διοχετευμένος πυρήνας. Αυτός ο σωληνωτός πυρήνας είναι ένας απλός τρόπος που χρησιμοποιεί σύγχρονο έλεγχο. Αυτό το είδος υλοποιησης απαιτεί την αντιγραφή και των 16 γύρων στον αλγόριθμο για 16 φορές καθώς και οι 16 γύροι εκτελούνται ταυτόχρονα. Ως εκ τούτου, τα κουτιά P – S πρέπει να είναι έτοιμα να επεξεργαστούν τα απαιτούμενα δεδομένα όποτε είναι απαραίτητο. Σύνολο θηρών μνήμης 32 bit η καθεμιά έχει διευθύνσεις 8 bit για τα S – box και 18 θύρες μνήμης με διευθύνσεις 5 bit για το P – box. Τ ο κύριο πλεονέκτημα αυτής της υλοποιησης είναι ότι κάθε λειτουργία μπορεί να πραγματοποιηθεί σε έναν κύκλο και η προετοιμασία ενός νέου κλειδιού μπορεί να γίνει απλά με λιγότερους κύκλους. Η συγκεκριμένη υλοποίηση της μείωσης της κατεχομένης περιοχής στοχεύει στην μείωση του αριθμού των σταδίων με αγωγό. Η προηγουμένη υλοποίηση θα καταλαμβάνει περισσότερο χώρο στο τσιπ, αυξάνοντας παράλληλα την απόδοση. Όταν ο αλγόριθμος απαιτεί λιγότερη περιοχή και περισσότερες διεκπεραιώσεις, πρέπει να γίνουν ορισμένες θυσίες για να επιτευχθούν οι απαιτούμενες προδιάγραφες.

Αντι για ένα τεράστιο αριθμό μητρώων που απαιτούνται μια ανατροφοδότηση σε κάθε γύρο. Αυτό σημαίνει ότι 4 θύρες μνήμης για 4 S – box και 1 θύρα μνήμης για P – array, δηλαδή 5 θύρες μνήμης στο σύνολο τους, όπως και στην προηγούμενη υλοποίηση που απαιτούνταν 1042 θύρες μνήμης. Ως εκ τούτου, η αρχιτεκτονική Crypt στο υλικό απαιτείται μόνο μια φορά, δηλαδή για ένα μόνο γύρο ταυτόχρονα η συνάρτηση F (X L) πρέπει να υπάρχει μόνο μια φορά όπως στο παρακάτω σχήμα.

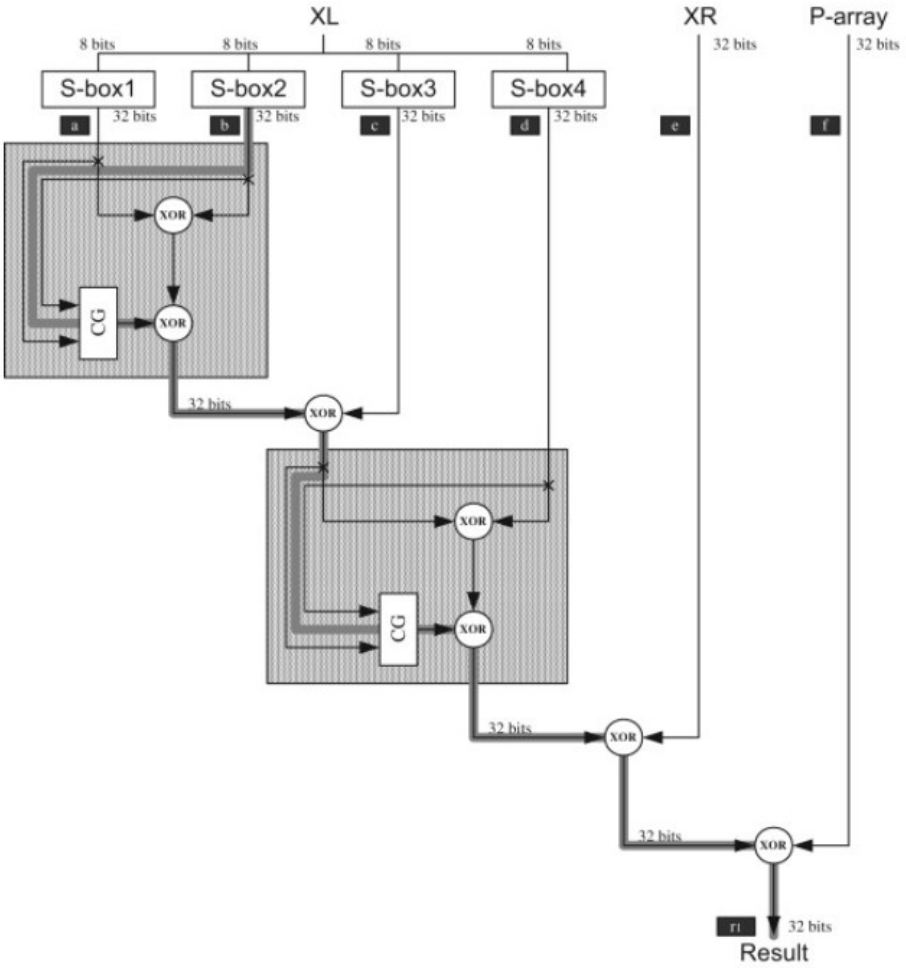


Εικόνα 23: Επαναληπτική Υλοποίηση Αλγορίθμου

Το κύριο πλεονέκτημα αυτής της μεθοδολογίας είναι ότι απαιτεί λιγότερο χώρο σε σύγκριση με προηγούμενες υλοποιήσεις. Το μειονέκτημα είναι ότι μπορεί να τρέξει κάτω από 16 κύκλους για κάθε μπλοκ δεδομένων και χρειάζεται περισσότερος αριθμός κύκλων για να αρχικοποιήσει το κλειδί, καθώς τα S - boxes και ο πίνακας P υλοποιούνται συγχρονισμένα. Η άλλη βελτιστοποίηση που πραγματοποιείται σε αυτόν τον σχεδιασμό είναι η ταχύτητα της λειτουργίας Feistel.

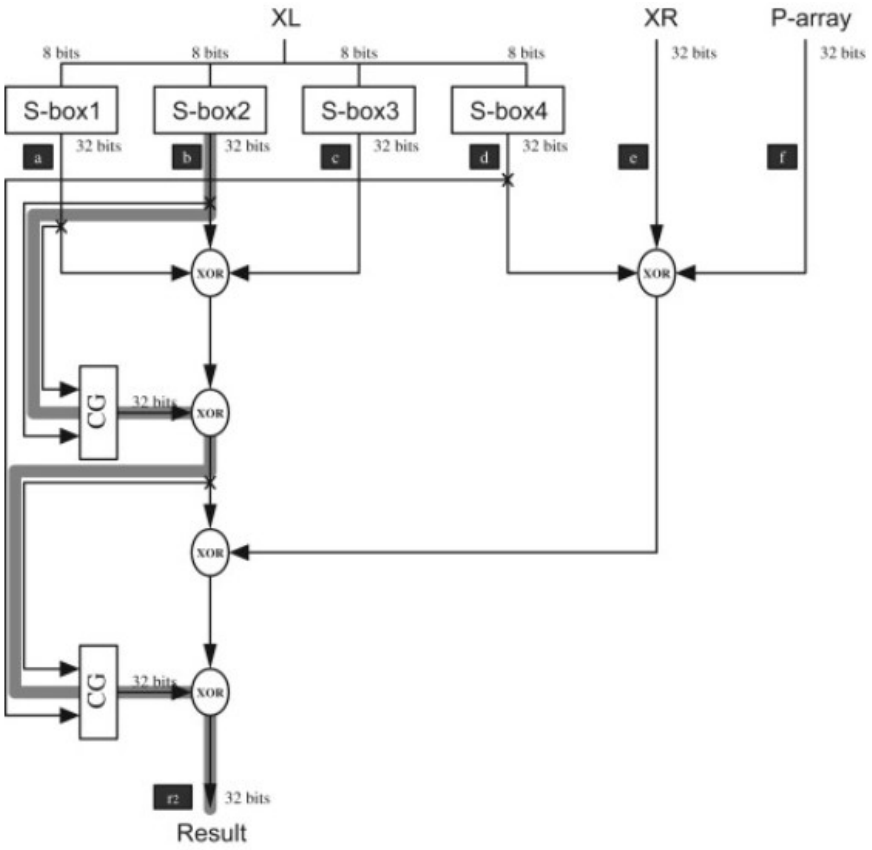
Η μέθοδος επαναπρογραμματισμού χειριστή χρησιμοποιείται για την επιτάχυνση της συνάρτησης F (X L). Στο παρακάτω σχήμα φαίνεται ότι το αρχικό DFG του σώματος βρόχου μετα την αντικατάσταση της λειτουργίας προσθήκης με την συνάρτηση CG και XOR. Κατά τον υπολογισμό του «$s=a+b$», το i-ο bit του s ισούται με (a_i x ή b_i x ή c_i), όπου c_i είναι η

μεταφορά του *i*- ου bit. Οι τελεστές περιλαμβάνουν μόνο γεννήτριες και XOR, επομένως η μέθοδος επαναπρογραμματισμού χειριστή χρησιμοποιείται για τη μείωση της καθυστέρησης της κρίσιμης διαδρομής.



Εικόνα 24: DFG του σώματος βρόχου

Στο επόμενο σχήμα διατυπώνεται το αποτέλεσμα του επαναπρογραμματισμού του χειριστή. Η σκοτεινή γραμμή σε αυτά τα σχήματα δείχνει την κρίσιμη διαδρομή. Η αρχική καθυστέρηση κρίσιμης διαδρομής είναι δυο καθυστερήσεις CG συν πέντε καθυστερήσεις XOR. Μετα τον επαναπρογραμματισμό, η καθυστέρηση κρίσιμης διαδρομής μειώνεται σε δυο καθυστερήσεις CG συν δυο καθυστερήσεις XOR. Τρεις καθυστερήσεις CG συν δυο καθυστερήσεις XOR. Τρεις καθυστερήσεις XOR 2 εισόδων είναι κρυφές.



Εικόνα 25: DFG μετα τον επαναπρογραμματισμό

Ακολουθεί μια σπονδυλωτή ροή σχεδίασης από πάνω προς τα κάτω κατά την εκτέλεση του αρχιτεκτονικού σχεδιασμού και της προσομοίωσης και την δημιουργία πρωτοτύπων FPGA. Λογικά και δομικά χωρίζει μια αρχιτεκτονική ενότητα σε πολλές ενότητες. Στην συνέχεια, αυτές οι μονάδες ελέγχονται και επαληθεύονται ξεχωριστά μέσω προσομοίωσης και σύνθεσης της γλώσσας περιγραφής υλικού VHSIC (VHDL) και της γλώσσας μεταφοράς καταχώρηση (RTL). Μόλις οι επιμέρους μονάδες δοκιμαστούν και επαληθευτούν ότι είναι λειτουργικά σωστές, συρράπτονται μεταξύ τους.

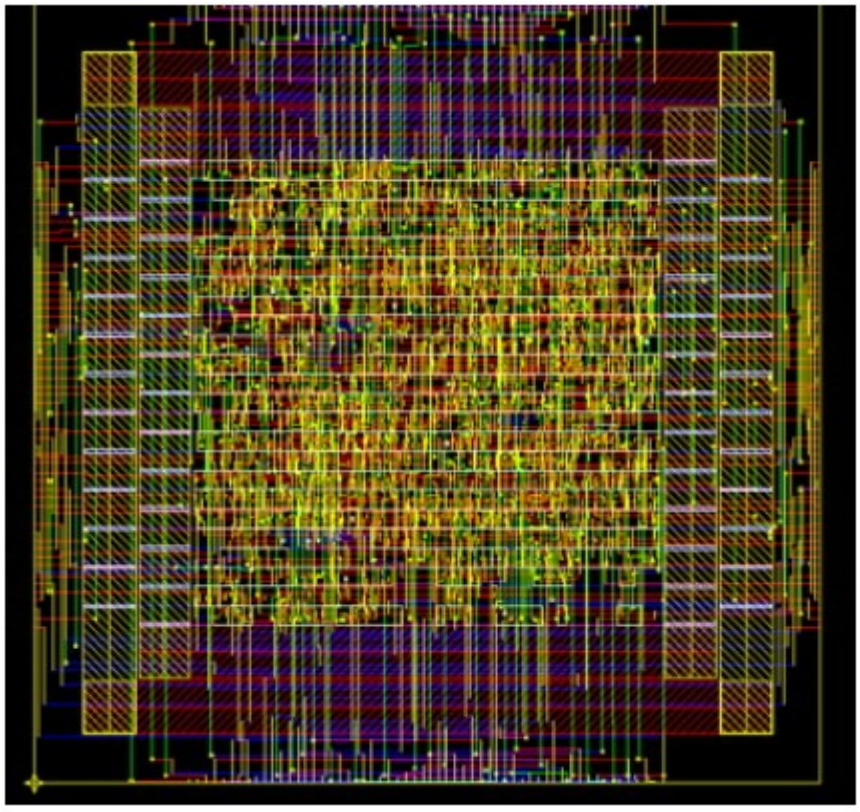
Με βάση την παραπάνω προσέγγιση, ο αλγόριθμος κρυπτογράφησης χωρίζεται σε δυο ενότητες : κρυπτογράφηση και αποκρυπτογράφηση. Όλη η μοντελοποιήση και ο σχεδιασμός εκτελούνται με χρήση VHDL. Η σύνθεση του τσιπ πραγματοποιείται στο εργαλείο Xilinx VIRTEX – II. Οι προσομοιώσεις πραγματοποιούνται χρησιμοποιώντας Modelsim.

Μεμονωμένα RTL λαμβάνονται μετα την σύνθεση του σχεδίου VHDL. Η προσομοίωση χρονισμού πραγματοποιείται επίσης για να επαληθευτεί η λειτουργική ορθότητα του σχεδιασμού. Ωστόσο, το διάγραμμα RTL δεν περιλαμβάνεται εδώ για συντομία.

Εικόνα 26: Προσέγγιση Σχεδιασμού βάσει FPGA

Στην συγκεκριμένη ενότητα θα αναφερθεί μια προσαρμοσμένη σχεδίαση IC της προτεινόμενης αρχιτεκτονικής. Στο παρακάτω σχήμα θα διατυπωθεί μια προσέγγιση αρθρωτού σχεδιασμού για την δημιουργία της διάταξης του πλήρους τσιπ, στο οποίο ο λογικός σχεδιασμός είναι από πάνω προς τα κάτω και ο φυσικός σχεδιασμός είναι από κάτω προς τα πάνω. Ο στόχος είναι να χρησιμοποιείται μια προσαρμοσμένη διάταξη για την κατασκευή ολόκληρου του τσιπ με ελάχιστο πυρίτιο.

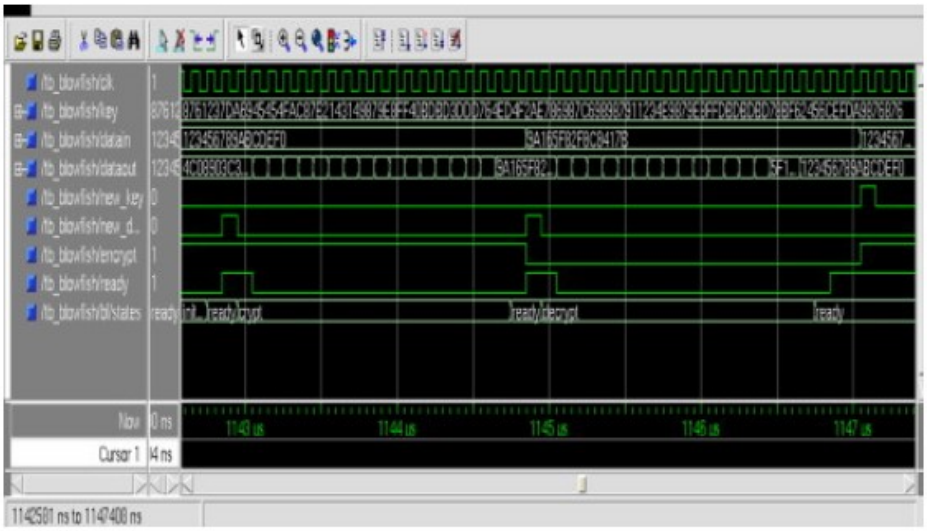
Ακολουθώντας μια ιεραρχική προσέγγιση, δημιουργείται η διάταξη διάφορων πόρων όπως αθροιστές, πολλαπλασιαστές κ.λπ. Αυτή η προσέγγιση ακολουθείται από ιεραρχική δημιουργία της διάταξης για τις μονάδες κρυπτογράφησης και αποκρυπτογράφησης. Τέλος, μόλις δημιουργηθεί η πλήρης διάταξη τσιπ, εκτελείται η εξαγωγή παρασιτικών και ανάλυση ισχύος.



Εικόνα 27: Διάταξη Πλήρους Τσιπ Κρυπτογράφησης

Οι πιο σημαντικές παράμετροι για την αξιολόγηση μιας δεδομένης υλοποιησης είναι η απόδοση, το απαιτούμενο υλικό και η κατανάλωση ενέργειας του τσιπ. Ο προτεινόμενος αλγόριθμος είναι πρωτότυπος σε τσιπ ASIC 130nm. Κάθε μεμονωμένη μονάδα στο τσιπ δοκιμάζεται ξεχωριστά με το εργαλείο VCS στο Synopsys και ο πλήρης αλγόριθμος blowfish προσομοιώνεται με VCS. Για τον έλεγχο χρησιμοποιούνται τυχαία διανύσματα. Η λειτουργικότητα και η καθυστέρηση κάθε ενότητας επαληθεύονται με την βοήθεια κυματομορφών προσομοίωσης.

Το 12345678ABCDEF είναι αυτό με το οποίο εμφανίζεται η κρυπτογράφηση και η αποκρυπτογράφηση στην κυματομορφή. Η τελική εφαρμογή κρυπτογράφησης blowfish μπορεί να εκτελέσει κρυπτογράφηση και αποκρυπτογράφηση μπλοκ κρυπτογράφησης σε μόνο 18 και 19 κύκλους, αντίστοιχα, όπως φαίνεται στο παρακάτω σχήμα.

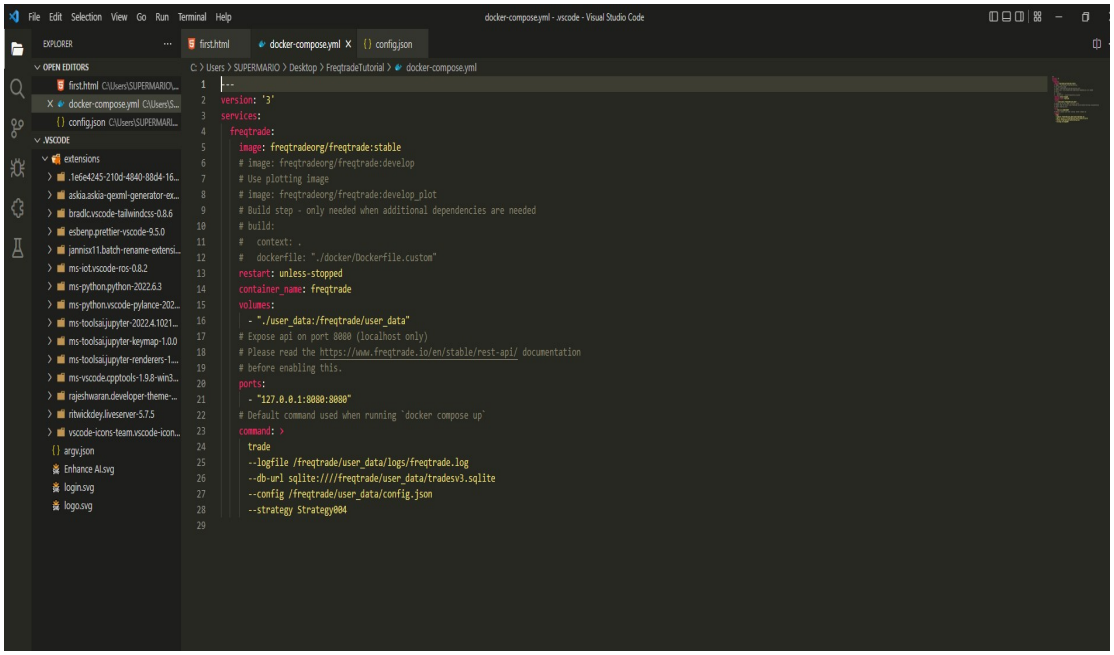


Εικόνα 28:Κρυπτογράφηση και Αποκρυπτογράφηση Δοκιμαστικού Φορέα

8.2.2 Υλοποιήση Στρατηγικής Κέρδους Κρυπτονομισμάτων

Σε αυτήν την ενότητα παρουσιάζονται αναλυτικά όλες οι διαδικασίες και οι παράμετροι για να υλοποιηθεί μια στρατηγική κέρδους στον τομέα των κρυπτονομισμάτων . Στην αρχή του κεφαλαίου γίνεται μια αναφορά για τον τρόπο εγκατάστασης και τα βήματα που πρέπει να ακολουθηθούν για την σωστή εκτέλεση του προγράμματος. Έπειτα, ο αλγόριθμος που θα υλοποιήσει αυτήν την διαδικασία εμπεριέχει μέσα μια συγκεκριμένη τροποποίηση που μας δίνει την δυνατότητα μέσω μιας λειτουργίας να δείξει την αποτελεσματικότητα του προγράμματος χρησιμοποιώντας εικονικά (virtual) χρήματα. Τέλος, μέσω μιας γραφικής παράστασης, θα αναλυθεί η χαρτογράφηση του αλγορίθμου και θα γίνει επεξήγηση της.

Ξεκινώντας την υλοποίηση της εργασίας, θα εγκατασταθεί στον υπολογιστή, μια εφαρμογή που ονομάζεται Docker και μέσω αυτού θα τρέξει ο αλγόριθμος για να δημιουργηθεί ένα bot, το οποίο είναι κάτι σαν πρόγραμμα που επιτελεί ένα συγκεκριμένο έργο με αυτοματοποιημένο τρόπο, χωρίς να χρειαστεί ανθρώπινη παρέμβαση. Ύστερα από την δημιουργία του χαρτογραφημένου διακομιστή, θα δημιουργηθεί μια στρατηγική κέρδους που θα αναλυθεί στην επόμενη παράγραφο.



Εικόνα 29: Δημιουργία Docker μέσω Visual Studio Code

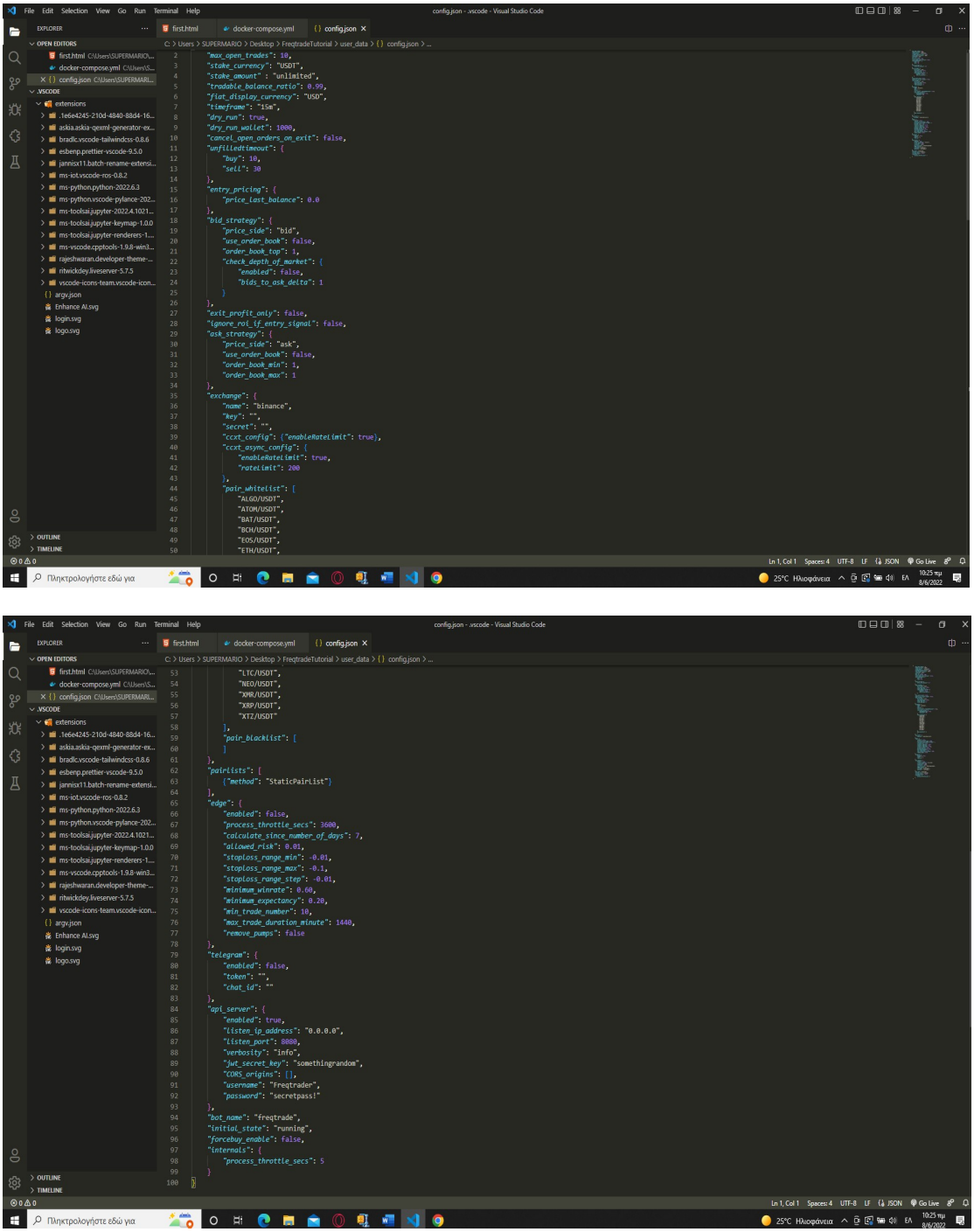
Πηγή : Ιδία Επεξεργασία

Η εκκίνηση του freqtrade σε ξηρή ή ζωντανή λειτουργία, θα ξεκινήσει το bot μαζί με τον βρόχο επανάληψης. Από προεπιλογή, ο βρόχος εκτελείται κάθε λίγα δευτερόλεπτα (internals.process_throttle_secs) και κάνει τις εξής διαδικασίες με την ακόλουθη σειρά:

- Λαμβάνει ανοιχτές συναλλαγές.
- Υπολογίζει την τρέχουσα λιστα εμπορεύσιμων ζευγών.
- Γίνεται λήψη δεδομένων για την λίστα ζευγών.
- Επανάκτηση Στρατηγικής Κλήσης.
- Αναλύει την στρατηγική ανά ζευγάρι.
- Ελέγχει τα στρατηγικά όρια για ανοιχτές συναλλαγές.
- Επανάκτηση στρατηγικής για ανοιχτές εντολές εισόδου – εξόδου.
- Επαλήθευση των υπαρχόντων θέσεων.

- Λαμβάνει υπόψιν το stoploss, την απόδοση επένδυσης και το σήμα εξόδου.

- Καθορίζει την τιμή εξόδου με βάση την ρύθμιση των παραμέτρων.

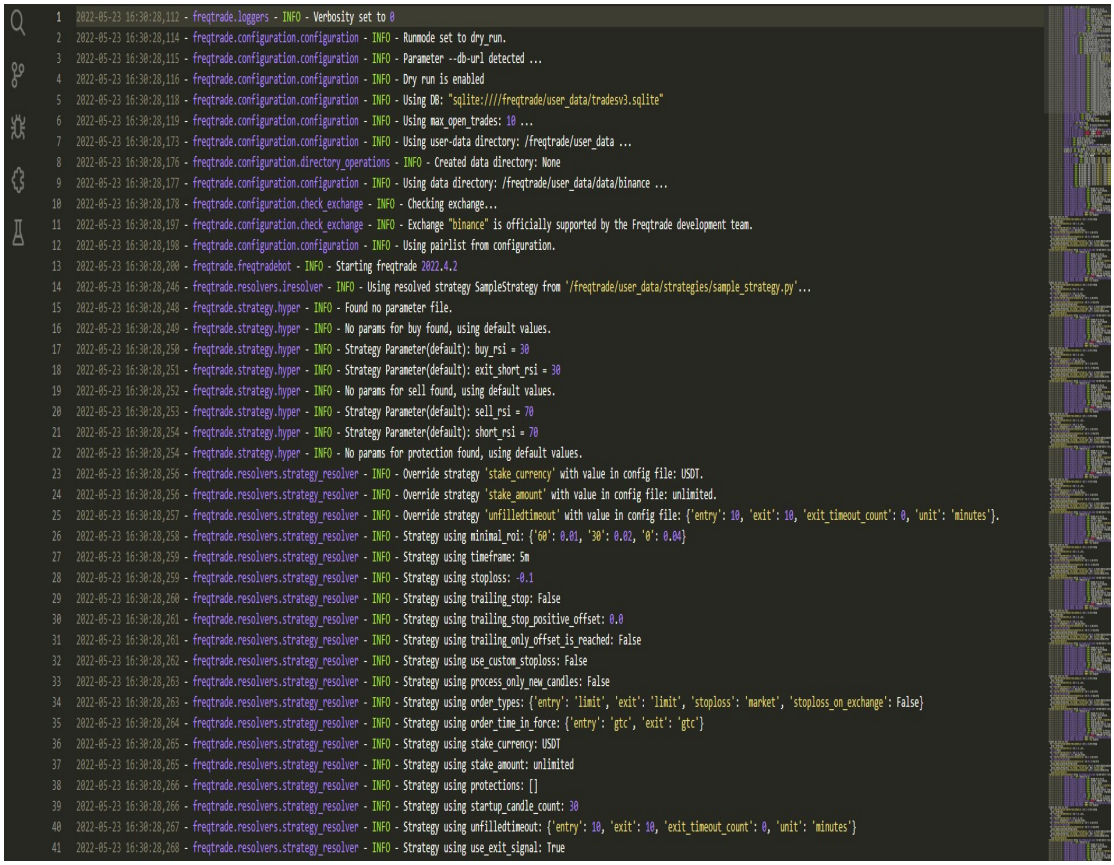


Εικόνα 30: Πλάνο Στρατηγικής μέσω Visual Studio Code

Πηγή : Ιδία Επεξεργασία

Στην συνέχεια της εργασίας, ενεργοποιούμε την διαδικασία του back testing, το οποίο κάνει ένα μέρος των προηγουμένων ενεργειών, καθώς οι περισσότερες από τις συναλλαγές είναι πλήρως προσομοιωμένες. Ταυτόχρονα καλείται και η λειτουργία της μελλοντικής εκπλήρωσης η οποία χρησιμοποιεί στρατηγική επανάκτηση για να επιτευχθεί η επιθυμητή μόχλευση. Για να μην προκύψει πρόβλημα εντός του κώδικα, πρέπει να προσδιοριστεί το μέγεθος του πονταρίσματος και να ελεγχθούν οι προσαρμογές θέσης για ανοιχτές συναλλαγές εάν είναι ενεργοποιημένες. Μια από τις τελευταίες ρυθμίσεις που θα χρειαστεί να υλοποιηθούν είναι μέσω του αρχείου διαμόρφωσης Freqrtade. Το bot χρησιμοποιεί ένα σύνολο παραμέτρων διαμόρφωσης κατά τη λειτουργία του που όλες μαζί συμμορφώνονται με την διαμόρφωσή του, το οποίο γίνεται μέσω της διαμόρφωσης του αρχείου που προαναφέρθηκε.

Από προεπιλογή, το bot φορτώνει την διαμόρφωση από το config.json αρχείο που βρίσκεται στο τρέχον κατάλογο εργασίας. Σε περίπτωση που χρησιμοποιηθεί η μέθοδος της γρήγορης εκκίνησης για την εγκατάσταση του bot, το σενάριο εγκατάστασης θα πρέπει να έχει ήδη δημιουργήσει το προεπιλεγμένο αρχείο διαμόρφωσης. Εάν δεν έχει δημιουργηθεί το προεπιλεγμένο αρχείο διαμόρφωσης, συνίσταται να χρησιμοποιηθεί το freqtrade new-config για την δημιουργία ενός βασικού αρχείου διαμόρφωσης. Επιπρόσθετα το bot επικυρώνει την σύνταξη του αρχείου διαμόρφωσης κατά την εκκίνηση και θα προειδοποιήσει σε τυχόν σφάλματα κατά την επεξεργασία του. Τελειώνοντας, η τελευταία παράμετρος διαμόρφωσης που ονομάζεται stop-loss είναι η απώλεια ως αναλογία που θα πρέπει να προκαλέσει μια πώληση. Αυτή η παράμετρος είναι προαιρετική καθώς περιλαμβάνει χρεώσεις.



Εικόνα 31: Παραμετροποιήσεις Στρατηγικής μέσω Visual Studio Code

Πηγή : Ιδία Επεξεργασία

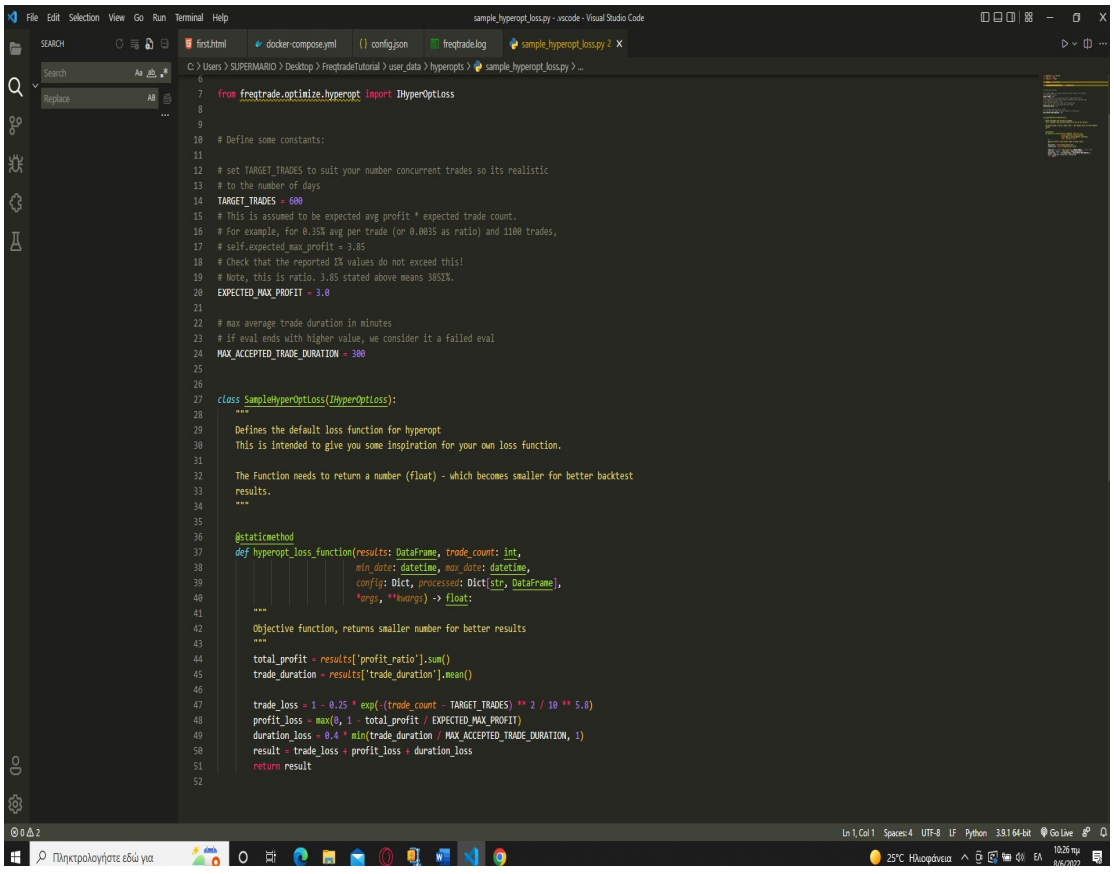
Με την ολοκλήρωσή της θα πρέπει να ελέγξουμε όλες τις παραμέτρους του αλγορίθμου να είναι σωστές, ώστε να ξεκινησει η λειτουργία του μέσω της εφαρμογής Docker. Ταυτόχρονα, μέσω του αλγορίθμου, χρησιμοποιούμε μια λειτουργία που ονομάζεται sandbox, η οποία χρησιμοποιεί εικονικά χρήματα για να δείξει την αποτελεσματικότητα της στρατηγικής χωρίς πιθανότητα απώλειας χρημάτων. Επιπλέον, μέσω της αλληλουχίας των προγραμμάτων, θα εγκατασταθεί και ένα plot machine που δείχνει κατά την διάρκεια της ημέρας διάφορες αλλαγές στην καθημερινή χαρτογράφηση με την χρήση δεικτών διαφορετικού χρώματος όπως:

1. Μείωση – Αύξηση τιμής νομίσματος
2. Διάρκεια Τιμής
3. Σταθερότητα Νομίσματος

4. Χρηματιστηριακό Σημείο Κλειδώματος

Κύριος σκοπός της υλοποίησής της στρατηγικής αυτής, δεν είναι τόσο το κέρδος, όσο η ισορροπία μεταξύ του πρώτου και σταθερότητας των συναλλαγών ώστε να αποφευχθεί η πιθανότητα να χαθεί μέρος των χρήματων στις συναλλαγές.

Μια ακόμα λειτουργία του συγκεκριμένου κώδικα είναι το hyperopt. Η συγκεκριμένη λειτουργία χρησιμοποιεί ένα μοντέλο μηχανικής εκμάθησης για να προσαρμόσει τις παραμέτρους της στρατηγικής, ωστόσο, αυτές οι τιμές θα μπορούσαν να καταστούν μη συμβατές με την πάροδο του χρόνου. Ιδανικά, οι τιμές αυτές, θα πρέπει να προσαρμόζονται ανάλογα με την αγορά.

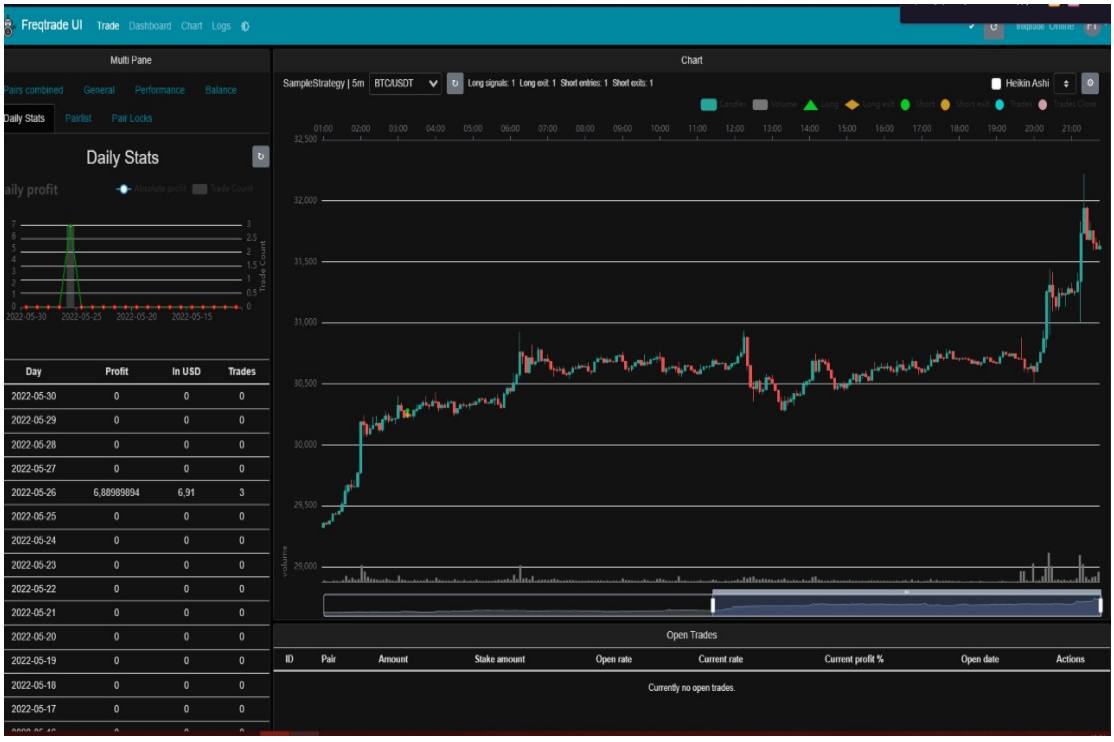


Εικόνα 32: Λειτουργία Hyperopt μέσω Visual Studio Code

Πηγή : Ιδία Επεξεργασία

Η παρακάτω γραφική παράσταση που προκύπτει σαν αποτέλεσμα αφού τρέξουμε τον αλγόριθμο στο πρόγραμμα της Microsoft : Visual Studio Code θα έχει τα ακόλουθα στοιχεία :

- **Πράσινα Τρίγωνα**: Σήματα αγοράς κατά την διάρκεια της στρατηγικής.
- **Κόκκινα Τρίγωνα**: Σήματα πώλησης από την στρατηγική(Κάθε σήμα πώλησης δεν τερματίζει μια συναλλαγή)
- **Κυανοί Κύκλοι**: Σημεία εισόδου στο εμπόριο.
- **Κόκκινα Τετράγωνα**: Σημεία εξόδου εμπορίου για επικερδείς συναλλαγές.
- Ενδείξεις με τιμές που καθορίζονται με indicators1 που αντιστοιχούν σε διάφορες κλίμακες (π.χ. : SMA/EMA)
- Όγκος (Ραβδογραμμα στο κάτω μέρος του κύριου γραφήματος)
- Ενδείξεις με τιμές που καθορίζονται με indicators2 που αντιστοιχούν σε διάφορες κλίμακες (π.χ. MACD, RSI) κάτω από τις γραμμές έντασης.



Εικόνα 33:Χαρτογράφηση Αποτελεσμάτων μέσω Freqtrade

Πηγή : Ιδία Επεξεργασία

ΚΕΦΑΛΑΙΟ 9: Έρευνα Κατανόησης & Λειτουργίας του Bitcoin

9.1 Ερευνητικό Σχέδιο

Η μεθοδολογία του ερευνητικού σχεδίου προβλέπει την συλλογή πρωτογενών δεδομένων με την μέθοδο των ερωτηματολογίων . Η μέθοδος αυτή επιλέχθηκε διότι επιτρέπει την συλλογή πρωτογενών δεδομένων με έγκαιρο και άμεσο τρόπο, επιτρέποντας την ανάλυση δεδομένων σε πραγματικό χρόνο. Η εξέλιξη της τεχνολογίας επιτρέπει την συλλογή ποσοτικών δεδομένων με μηδενικό κόστος , διευκολύνεται έτσι η ταχεία επεξεργασία και παρουσίαση των αποτελεσμάτων της ερευνάς. Επιπλέον, ακόμη και αν δεν υπάρχει ιστορικό στατιστικής ή επιστημονικής ερευνάς σχετικά με το ερευνητικό πρόβλημα , είναι εφικτό να διερευνηθούν οι τάσεις που προκύπτουν από την ανάλυση των ερωτηματολογίων και να δημιουργηθούν σημεία αναφοράς για μελλοντική ερευνά. Τέλος , τα ερωτηματολόγια μπορούν να διανεμηθούν σε μεγάλες ή μικρές ομάδες και να περιλαμβάνουν ανοιχτές ερωτήσεις ή ερωτήσεις πολλαπλών επίλογων , επιτρέποντας στον ερευνητή να συλλεγεί τις σχετικές πληροφορίες και να παρέχει αξιόπιστα αποτελέσματα.

Από την άλλη πλευρά , λόγω της ανωνυμίας , οι συμμετέχοντες ενδέχεται να μην παρέχουν αξιόπιστες απαντήσεις , επηρεάζοντας έτσι το ερευνητικό αποτέλεσμα. Τέλος , οι ερωτηθέντες μπορούν να παραλείψουν ερωτήσεις ή να κατανοήσουν κάτι διαφορετικό από αυτό που ζητά η ερώτηση , επηρεάζοντας έτσι την εγκυρότητα των δεδομένων. Η διανομή του ερωτηματολογίου διήρκησε 2 μήνες από τον Οκτώβριο μέχρι και τον Δεκέμβριο του 2020 και περιλάμβανε 16 ερωτήσεις οι οποίες αφορούσαν έμμεσα αλλά και άμεσα τα κρυπτονομίσματα και έπειτα πραγματοποιήθηκε η καταγραφή και η μελέτη των αποτελεσμάτων.

Η μελέτη που διενεργήθηκε πραγματοποιήθηκε δημιουργώντας ένα ηλεκτρονικό ερωτηματολόγιο προσαρμοσμένο στις σύγχρονες απαιτήσεις

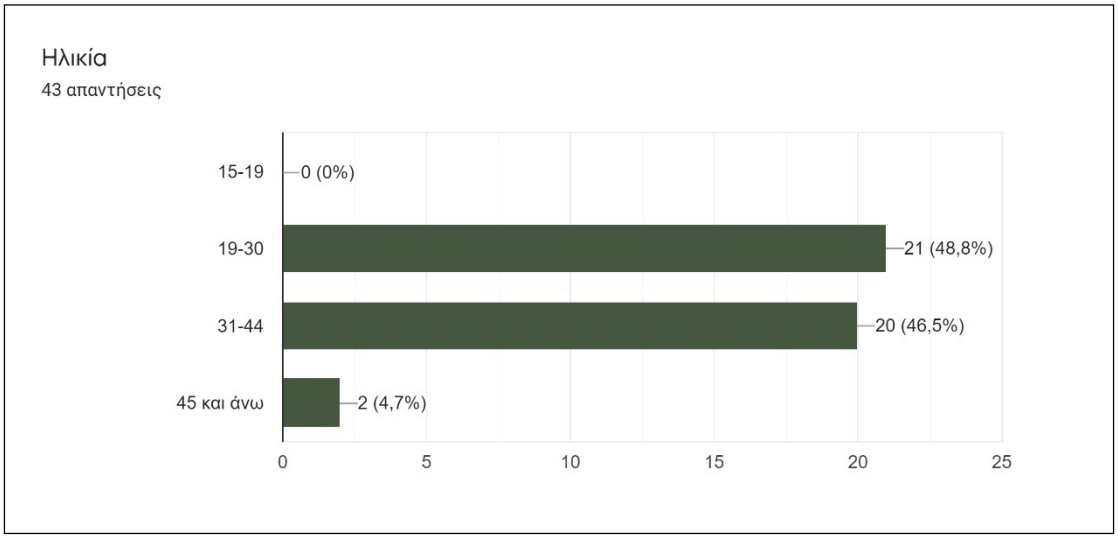
σχετικά με την αποφυγή των άμεσων επαφών λόγω COVID – 19, και διανεμήθηκε ηλεκτρονικά. Το ερωτηματολόγιο αυτό για λόγους περεταίρω διευκόλυνσης, προετοιμάστηκε και προσαρμόστηκε σε web περιβάλλον και είναι διαθέσιμο ηλεκτρονικά στην παρακάτω ηλεκτρονική διεύθυνση:

https://forms.gle/24jdEeAeg6vGwJG67

Το ερωτηματολόγιο είναι προσβάσιμο προς συμπλήρωση από κάθε ενδιαφερόμενο. Με τον τρόπο αυτό η διαδικασία επιταχύνεται και η αποτύπωση των αποτελεσμάτων είναι άμεση διαθέσιμη. Στο Παράρτημα επισυνάπτεται το ερωτηματολόγιο που προετοιμάσθηκε και χρησιμοποιήθηκε.

9.2 Αποτελέσματα Ερωτηματολογίου

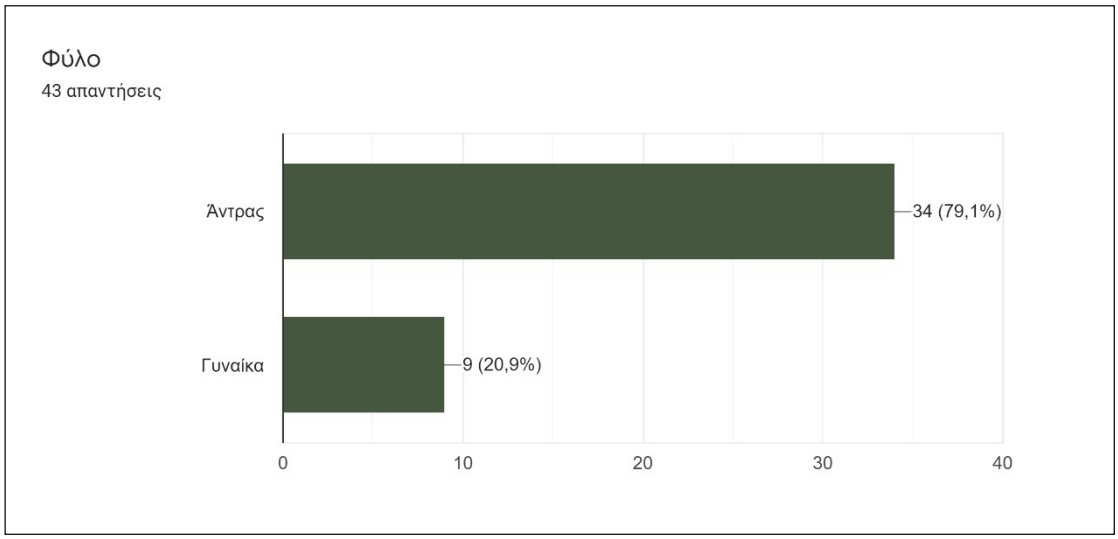
Από τους 43 συμμετέχοντες, τα 34 άτομα (79,1%) είναι άνδρες και 9 άτομα (20,9%) είναι γυναίκες. (Διάγραμμα 1)



Διάγραμμα 1:Κατάταξη ατόμων ανα Φύλο
Πηγή: Ερωτηματολόγια

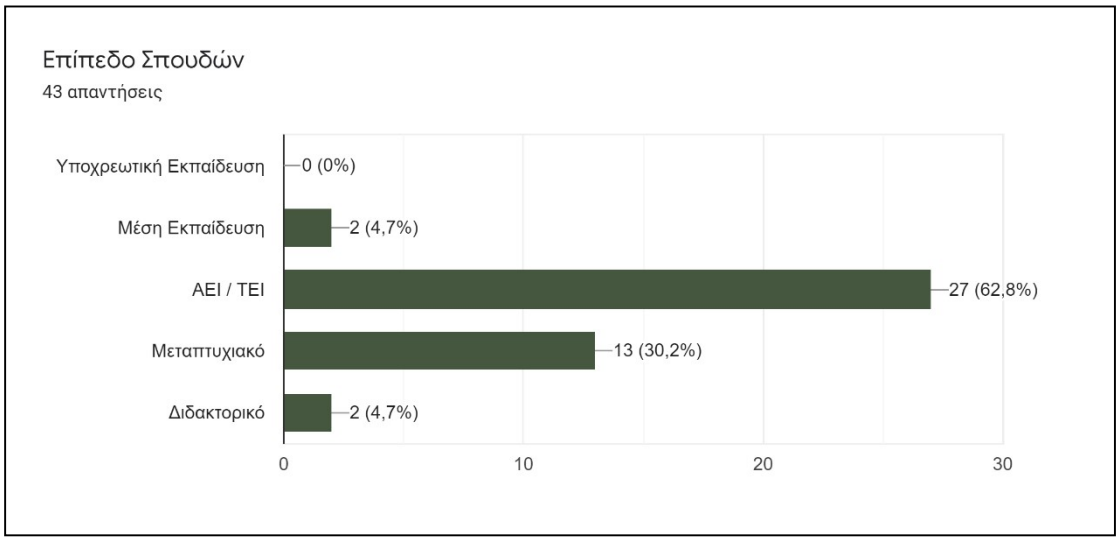
Τα 21 άτομα (48,8%) είναι από 19 έως 30 ετών , 20 άτομα (46,5%) είναι μεταξύ 31-44 ετών , 2 άτομα(4,7%) είναι από 45 και άνω , ενώ στις ηλικίες μεταξύ 15-19 δεν υπήρχε κανένα άτομο .

Οι συμμετέχοντες του ερωτηματολογίου κατανέμονται σχετικά ισόποσα στις ηλικίες μεταξύ 19 – 30 και 31 – 44 με ποσοστά 48,8% και 46,5% αντίστοιχα. Μόλις 2 άτομα ανήκουν στην ηλικιακή κατηγορία 45 και άνω (ήτοι, το 4,7%), ενώ κανένας συμμετέχοντας δεν ανήκει στην κατηγορία 15 – 19.



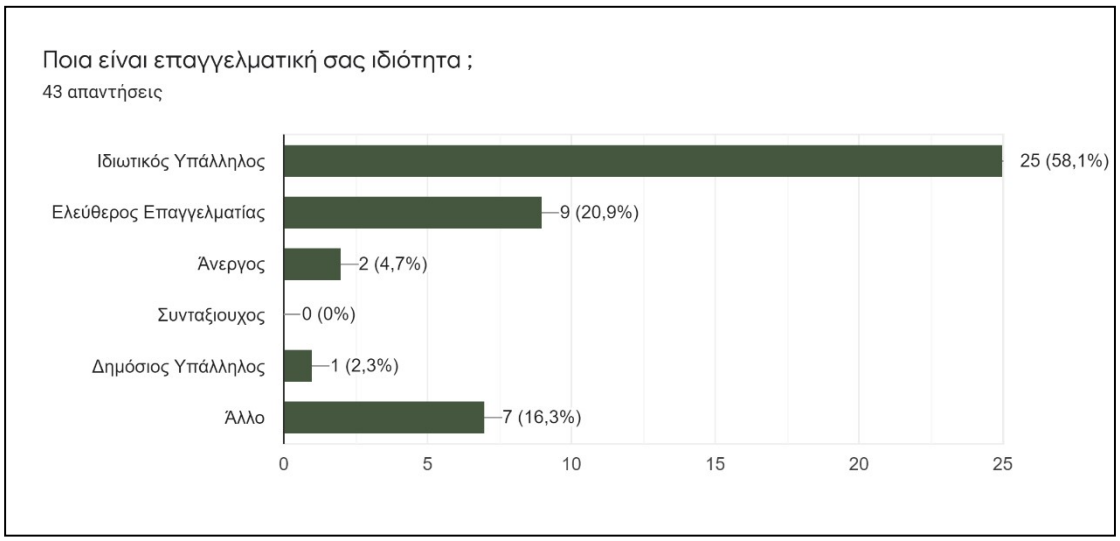
Διάγραμμα 2: Κατάταξη ατόμων ανα ηλικία
Πηγή: Ερωτηματολόγια

Αναφορικά με την εκπαίδευση , 27 άτομα (62,8%) είναι πτυχιούχοι ΑΕΙ / ΤΕΙ , 13 άτομα (30,2%) είναι κάτοχοι μεταπτυχιακού , 2 άτομα (4,7%) είναι κάτοχοι διδακτορικού , και 2 άτομα (4,7%) είναι απόφοιτοι λυκείου . (Διάγραμμα 3).



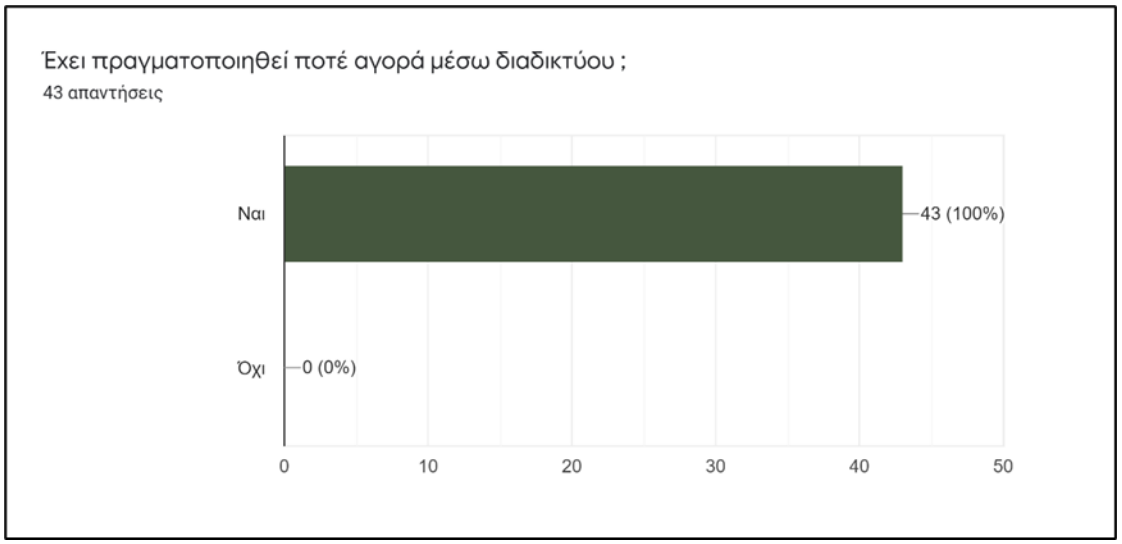
Διάγραμμα 3:Κατάταξη ατόμων κατά επίπεδο σπουδών
Πηγή: Ερωτηματολόγια

Από τους 43 συμμετέχοντες, 25 άτομα (58,1%) εργάζονται ως ιδιωτικοί υπάλληλοι , 9 άτομα (20,9%) είναι ελεύθεροι επαγγελματίες , 7 άτομα(16,3%) δήλωσαν άλλη επαγγελματική απασχόληση, 1 άτομο (2,3%) εργάζεται ως δημόσιος υπάλληλος και 2 άτομα (4,7%) είναι άνεργα (Διάγραμμα 4).



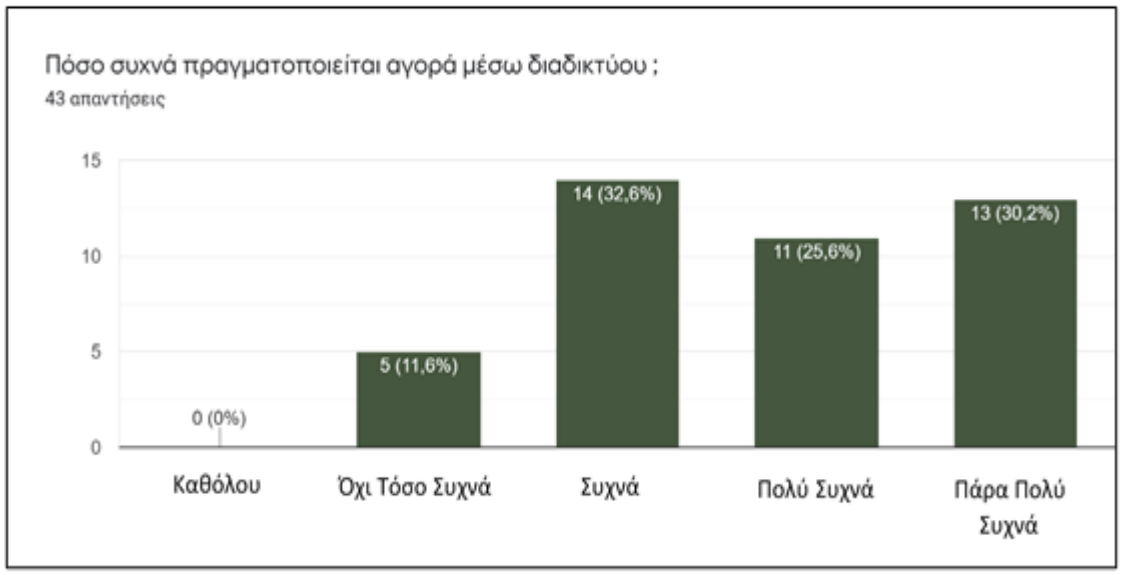
Διάγραμμα 4:Κατάταξη ατόμων ανα επάγγελμα
Πηγή Ερωτηματολόγια

Για το εάν έχει πραγματοποιηθεί κάποια αγορά μέσω διαδικτύου , και τα 43 άτομα απάντησαν θετικά δηλαδή το 100% (Διάγραμμα 5).



Διάγραμμα 5:Αγορά μέσω Διαδικτύου
Πηγή: Ερωτηματολόγια

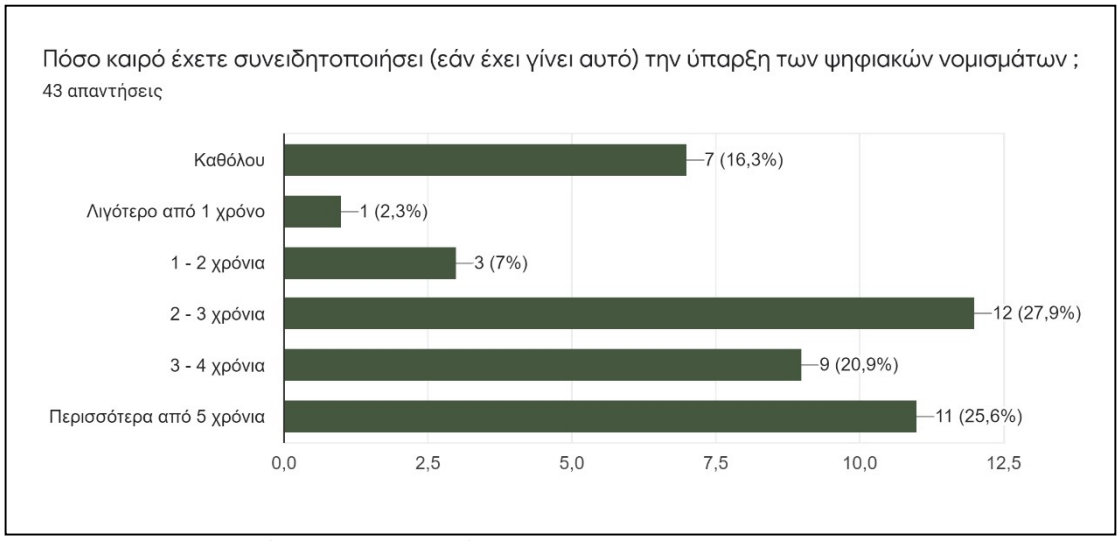
Στην ερώτηση ποσό συχνά πραγματοποιούνται αγορές μέσω διαδικτύου , 14 άτομα (32,6%) απάντησαν συχνά, 13 άτομα (30,2%) απάντησαν πάρα πολύ συχνά, 11 άτομα (25,6%) απάντησαν πολύ συχνά ενώ 5 άτομα (11,6%) απάντησαν όχι τόσο συχνά (Διάγραμμα 6).



Διάγραμμα 6:Ποσοστό συχνότητας αγοράς μέσω Διαδικτύου

Πηγή Ερωτηματολόγια

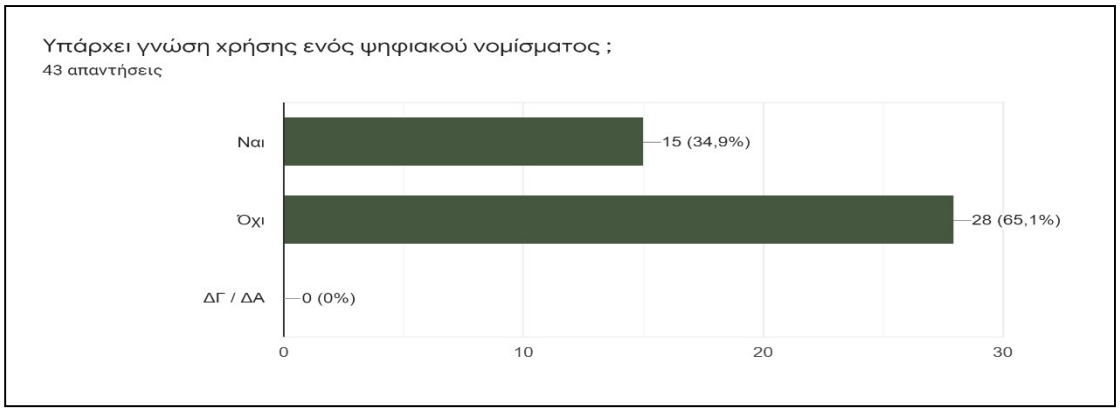
Όσον αφορά την ερώτηση σχετικά με την επίγνωση της ύπαρξης ψηφιακών νομισμάτων, 12 άτομα (27,9%) έχουν συνειδητοποιήσει την ύπαρξη των ψηφιακών νομισμάτων εδώ και 2-3 χρόνια, 11 άτομα (25,6 %) γνωρίζουν κάποιο ψηφιακό νόμισμα περισσότερα από 5 χρόνια, 9 άτομα (20,9%) εδώ και 3-4 χρόνια, 7 άτομα (16,3%) δεν γνωρίζουν καθόλου κάποιο ψηφιακό νόμισμα, 3 άτομα (7%) έχουν γνώση κάποιου ψηφιακού νομίσματος εδώ και 1-2 χρόνια ενώ 1 άτομο γνωρίζει λιγότερο από 1 χρόνο την ύπαρξη κάποιου ψηφιακού νομίσματος . (Διάγραμμα 7). Είναι σημαντικό να αναφερθεί ότι το μεγαλύτερο ποσοστό των συμμετεχόντων (ήτοι το 83,7%) γνωρίζει την ύπαρξη των ψηφιακών νομισμάτων ενώ μόλις το 16,3% δεν γνωρίζει κάποιο ψηφιακό νόμισμα.



Διάγραμμα 7:Κατάταξη γνώσης ύπαρξης ψηφιακού νομίσματος

Πηγή: Ερωτηματολόγια

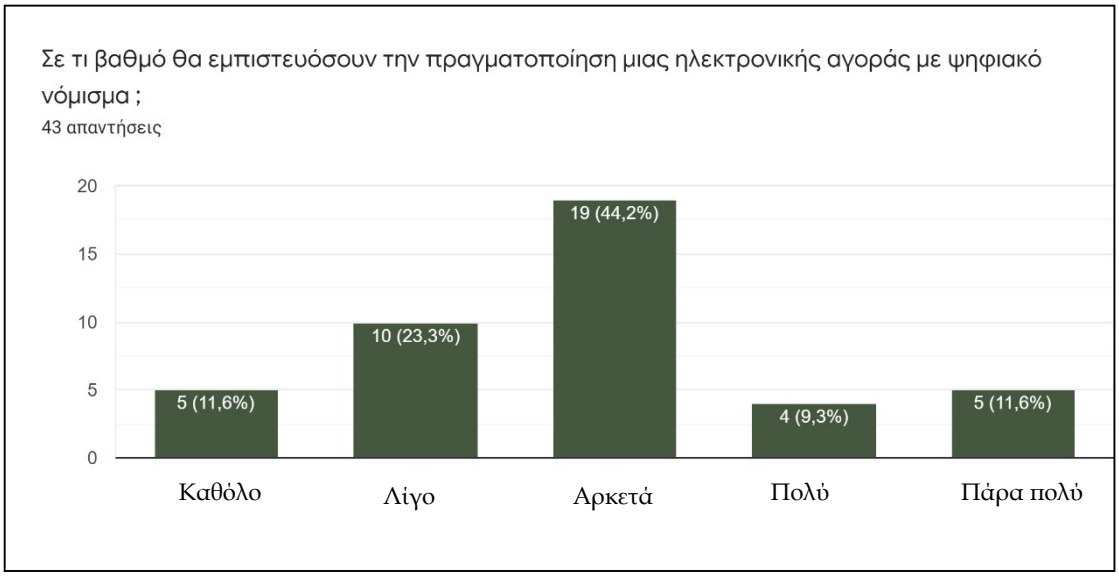
Στην ερώτηση αν υπάρχει γνώση χρήσης ενός ψηφιακού νομίσματος , 28 άτομα (65,1%) απάντησαν πως δεν γνωρίζουν ενώ 15 άτομα (34,9%) απάντησαν ότι έχουν γνώση χρήσης ενός ψηφιακού νομίσματος (Διάγραμμα 8).



Διάγραμμα 8: Γνώση Χρήσης ενός Ψηφιακού Νομίσματος

Πηγή : Ερωτηματολόγια

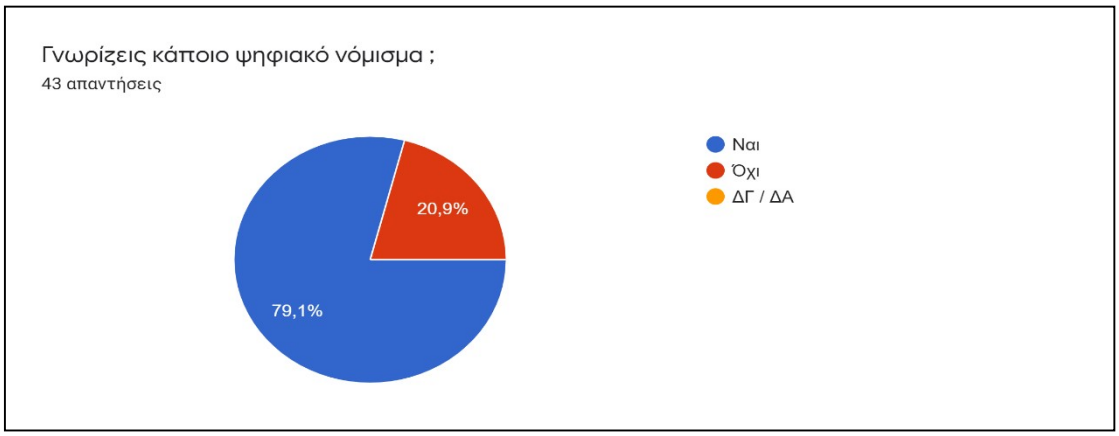
Όσον αφορά την εμπιστοσύνη στη χρήση ενός ψηφιακού νομίσματος για ηλεκτρονική αγορά, 19 άτομα (44,2%) θα εμπιστεύονταν αρκετά ένα ψηφιακό νόμισμα για να πραγματοποιήσει μια ηλεκτρονική αγορά , 10 άτομα (23,3%) θα εμπιστεύονταν λίγο αυτήν την διαδικασία , 5 άτομα (11,6%) δεν θα το εμπιστεύονταν καθόλου ενώ από την άλλη πλευρά 4 άτομα (9,3%) και 5 άτομα (11,6%) θα εμπιστεύονταν πολύ και πάρα πολύ αντίστοιχα αυτήν την διαδικασία . (Διάγραμμα 9)



Διάγραμμα 9:Κατάταξη Εμπιστοσύνης μιας ηλεκτρονικής αγοράς με ψηφιακό νόμισμα

Πηγή Ερωτηματολόγια

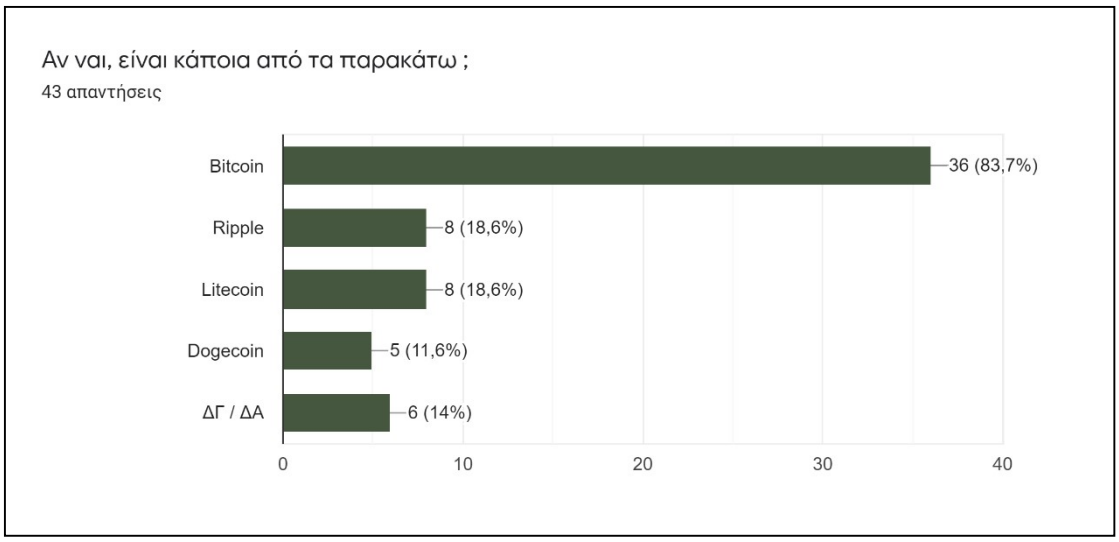
Όσον αφορά την γνώση κάποιου συγκεκριμένου κρυπτονομίσματος, το μεγαλύτερο ποσοστό, ήτοι το 79,1% γνωρίζει κάποιο ψηφιακό νόμισμα, ενώ μόλις το 20,9% δεν γνωρίζει κάποια ονομασία ψηφιακού νομίσματος (Διάγραμμα 10).



Διάγραμμα 10: Κατάταξη Γνώσης Ψηφιακού Νομίσματος

Πηγή : Ερωτηματολόγια

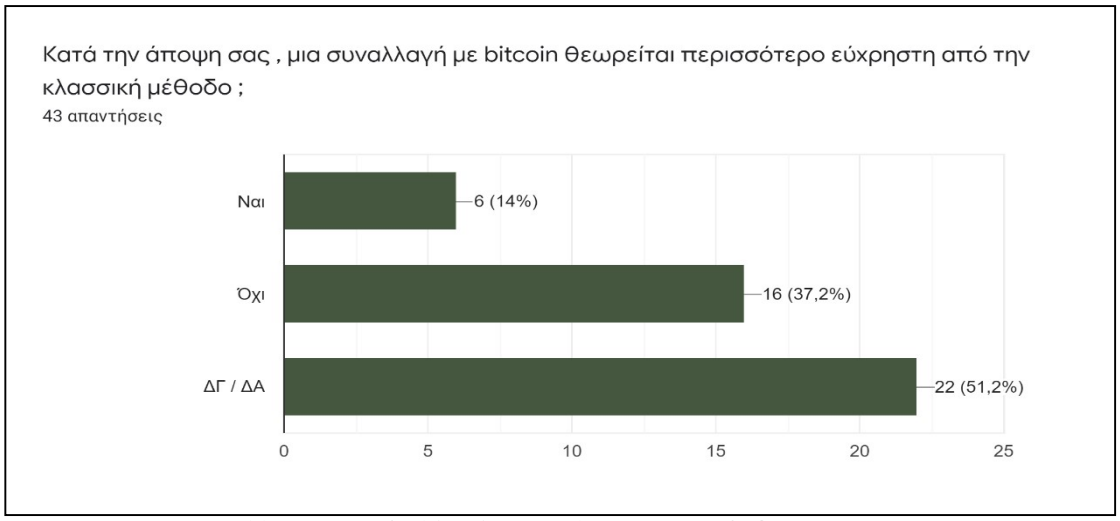
Όσον αφορά τη συγκεκριμένη γνώση κρυπτονομίσματος, 36 άτομα (83,7%) γνωρίζουν το ψηφιακό νόμισμα Bitcoin, το οποίο το καθιστά το πιο δημοφιλές ανάμεσα στους ερωτηθέντες. Ενώ 8 άτομα (18,6%) γνωρίζουν το Ripple και αντίστοιχα το Litecoin , 5 άτομα (11,6%) το Dogecoin και 6 άτομα (14%) δεν γνώριζαν κανένα (Διάγραμμα 11).



Διάγραμμα 11:Ψηφιακά Νομίσματα

Πηγή : Ερωτηματολόγια

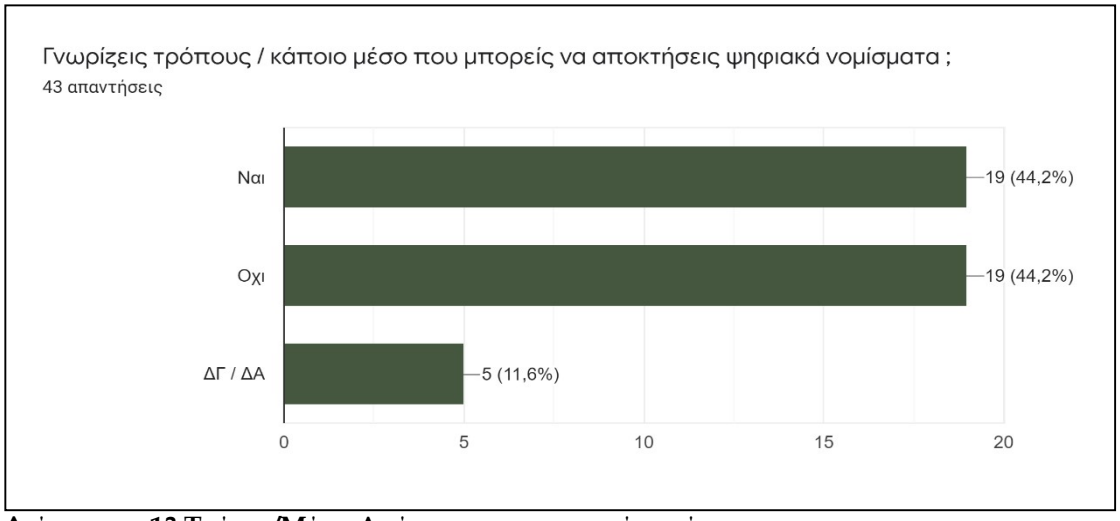
Στην υποκειμενική ερώτηση περί ευκολίας χρήσης του κρυπτονομίσματος, 22 άτομα (51,2%) δεν γνωρίζουν, 16 άτομα (37,2%) δεν πιστεύουν ότι μια συναλλαγή με bitcoin θεωρείται περισσότερο εύχρηστη από την κλασσική μέθοδο ενώ 6 άτομα (14%) πιστεύουν το αντίθετο(Διάγραμμα 12).



Διάγραμμα 12:Συναλλαγή μεταξύ bitcoin και κλασσικής μεθόδου

Πηγή : Ερωτηματολόγια

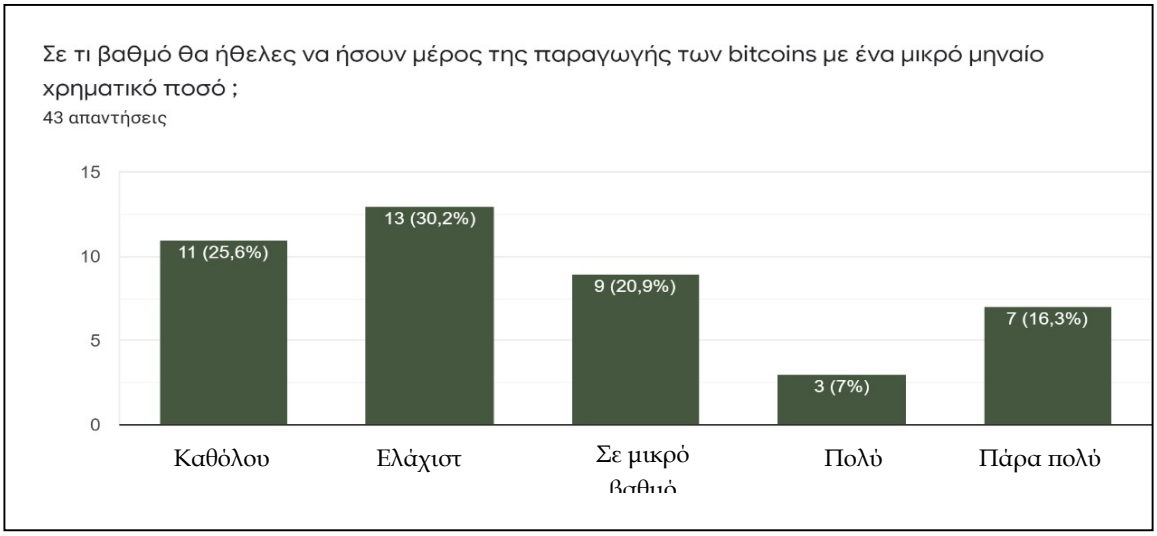
Στην ερώτηση αν γνωρίζουν κάποιους τρόπους/μέσο που μπορεί κάποιος να αποκτήσει ένα ψηφιακό νόμισμα 19 άτομα (44,2%) απάντησαν ναι και αντίστοιχα άλλοι 19 όχι, ενώ 5 άτομα (11,6%) δεν γνώριζαν κάποιο τρόπο/μέσο (Διάγραμμα 13).



Διάγραμμα 13:Τρόποι/Μέσα Απόκτησης ψηφιακού νομίσματος

Πηγή : Ερωτηματολόγια

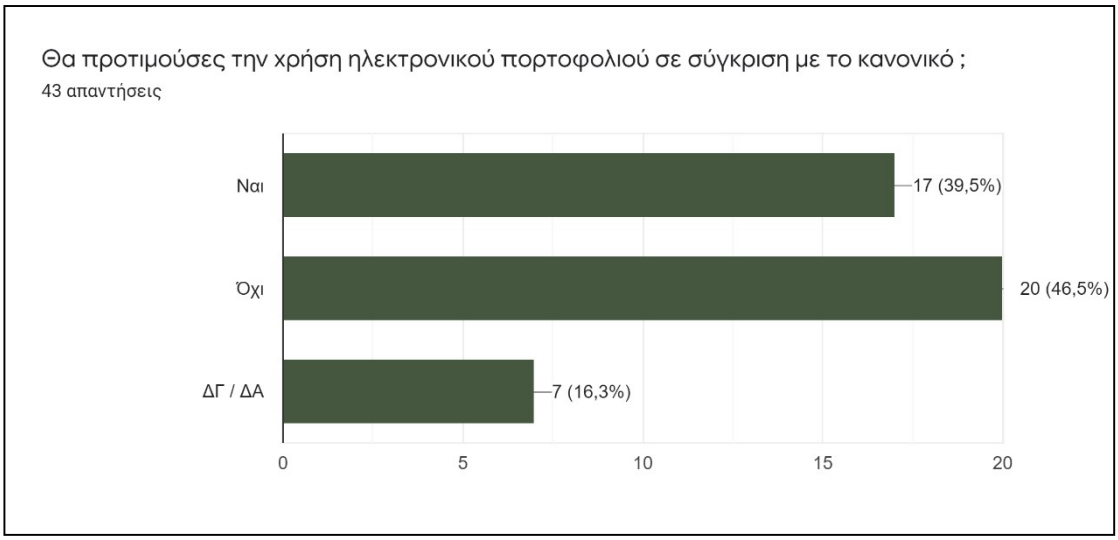
13 άτομα (30,2%) θα ήθελαν ελάχιστα να είναι μέρος της παραγωγής των bitcoins , 11 άτομα (25,6%) δεν θα ήθελαν καθόλου , 9 άτομα (20,9%) θα ήθελαν να συμμετέχουν σε ένα μικρό βαθμό , ενώ 7 άτομα (16,3%) και 3 άτομα (7%) θα ήθελαν πάρα πολύ και πολύ αντίστοιχα.(Διάγραμμα 14).



Διάγραμμα 14:Βαθμός Συμμετοχής στην Παραγωγή Bitcoin

Πηγή : Ερωτηματολόγια

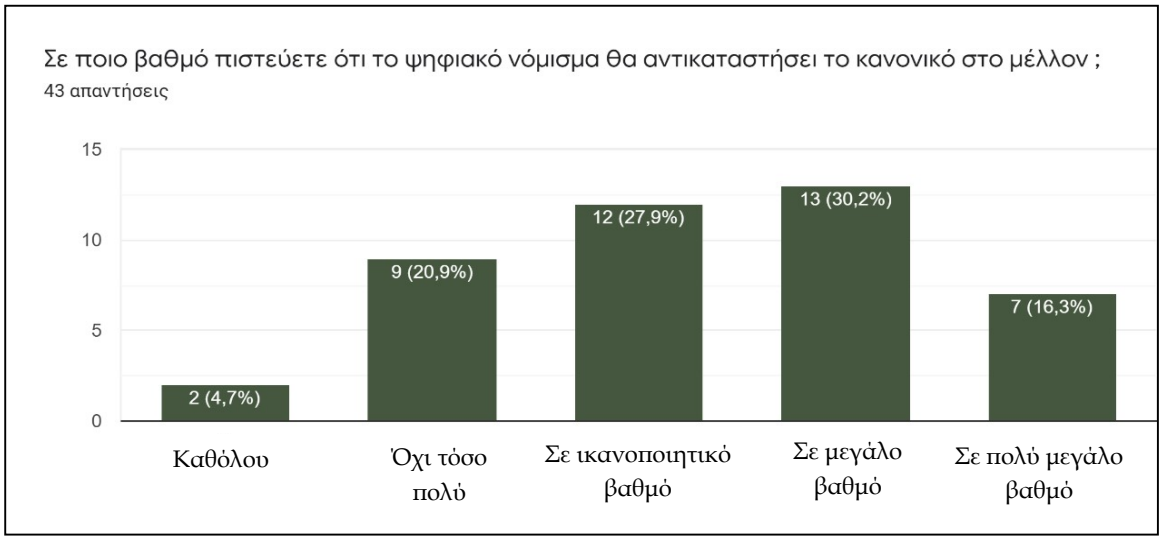
Στην προτίμηση χρήσης ηλεκτρονικού πορτοφολιού σε σύγκριση με το κανονικό , 20 άτομα (46,5%) δεν θα το προτιμούσαν , 17 άτομα (39,5%) θα το προτιμούσαν ενώ 7 άτομα (16,3%) δεν απαντούν στο συγκεκριμένο ερώτημα (Διάγραμμα 15).



Διάγραμμα 15:Προτίμηση ηλεκτρονικού ή κανονικού πορτοφολιού

Πηγή : Ερωτηματολόγια

13 άτομα (30,2%) πιστεύουν σε μεγάλο βαθμό ότι το ψηφιακό νόμισμα θα αντικαταστήσει το κανονικό, 12 άτομα (27,9%) το πιστεύουν σε ικανοποιητικό βαθμό , 7 άτομα (16,3%) το πιστεύουν σε πολύ μεγάλο βαθμό , 9 άτομα (20,9%) δεν το πιστεύουν τόσο πολύ ενώ 2 άτομα (4,7%) δεν το πιστεύουν καθόλου (Διάγραμμα 16) .



Διάγραμμα 16:Αντικατάσταση κανονικού χρήματος με το ψηφιακό

Πηγή : Ερωτηματολόγια

ΣΥΜΠΕΡΑΣΜΑΤΑ

Έχουν περάσει δώδεκα χρόνια από την παραγωγή του πρώτου bitcoin από τον άγνωστης ταυτότητας Satochi Nakamoto . Το πρώτο κρυπτονόμισμα στην ιστορία, ξεκίνησε χωρίς να αξίζει απολύτως τίποτα , έγινε μέσο ανταλλαγής για εμπόρους ναρκωτικών , έφτασε να έχει ισοτιμία 20.000 δολαρίων για να χάσει υστέρα τα 4/5 της αξίας του , και άνοιξε τον δρόμο για περισσότερα από 1.600 κρυπτονομίσματα .Τον τελευταίο καιρό έχει επιστρέψει πάλι στην ανοδική πορεία του και καταλαβαίνουμε σιγά σιγά πως γίνεται κομμάτι της ζωής μας το κρυπτονόμισμα . Η έννοια του ψηφιακού νομίσματος και του bitcoin φοβίζει αρκετά τους πιο πολλούς ανθρώπους . Γενικά όμως το bitcoin παρέχει πολλές διευκολύνσεις στις συναλλαγές και υπερτερεί σε σύγκριση με την παραδοσιακή οικονομία έχοντας ταχύτητα και ευκολία .

Υπάρχουν βέβαια και τα μειονεκτήματα που το καθιστούν ακόμα και σήμερα ασταθές όπως η μη αντιστρεψιμότητα των συναλλαγών και η απώλεια του λογαριασμού του χρήστη. Αυτό που έχει όμως μεγάλη σημασία δεν είναι ούτε τα πλεονεκτήματα ούτε τα μειονεκτήματα αλλά ότι το bitcoin στην συγκεκριμένη χρονική στιγμή έχει φτάσει στα 36.000 δολάρια και αυτό το καθιστά ως το πιο δυνατό και το πιο αποδοτικό νόμισμα αυτήν την στιγμή στον κόσμο . Παρόλα αυτά η μη αποδοχή του συγκεκριμένου νομίσματος είναι και ο λόγος που δεν κυριαρχεί ακόμα στην παγκόσμια αγορά .

Πολλοί άνθρωποι , όπως είδαμε και μέσα από το ερωτηματολόγιο , δεν γνωρίζουν την ψηφιακή οικονομία και έχουν μια πολύ μικρή γνώση του κρυπτονομίσματος, και όσοι γνωρίζουν κάποια πράγματα φοβούνται ακόμα να το εμπιστευτούν γιατί προτιμούν να έχουν τα χρήματα τους στα χεριά τους και όχι σε εικονικές πλατφόρμες. Είναι σημαντικό βέβαια να αναφερθεί το γεγονός ότι το ερωτηματολόγιο που διανεμήθηκε ηλεκτρονικά, συμπληρώθηκε από κατοίκους της Ελλάδας, μίας χώρας που

γενικά αντιμετωπίζει με καχυποψία τις ηλεκτρονικές συναλλαγές και τη χρήση τεχνολογιών αιχμής. Αυτό μπορεί να έγκειται στον παραδοσιακό χαρακτήρα της αλλά και στη νωχελικότητα με την οποία χρησιμοποιεί τα ηλεκτρονικά μέσα. Είναι σημαντικό να αναφερθεί ότι ήδη το «πλαστικό χρήμα» άργησε να εγκατασταθεί στη χώρα και να χρησιμοποιηθεί ευρέως, σε σχέση με άλλες ευρωπαϊκές και μη χώρες. Ίσως αυτή τη στιγμή η Ελλάδα να είναι σε μια πιο ώριμη φάση για την κατανόηση και τη χρήση του κρυπτονομίσματος αλλά απομένουν πολλές ακόμη ενέργειες για την ευρεία και ίσως καθολική χρήση του. Είναι σημαντικό να επισημανθεί ότι με την σωστή προστασία και με τις σωστές ενέργειες του κάθε χρήστη, είναι απολυτά ασφαλές για κάθε χρήστη να χρησιμοποιήσει το κρυπτονόμισμα. Ποτέ όμως θα είναι έτοιμη η πλειοψηφία των ανθρώπων να δεχτεί και να κάνει το ψηφιακό νόμισμα καθημερινότητα του;

Βιβλιογραφία – Αναφορές - Διαδικτυακές Πηγές

Antonopoulos, A. M., 2020. *Mastering bitcoin.* s.l.:s.n.

Taylor & Francis. 2022. *Bitcoins as an investment or speculative vehicle? A first look*. [online] Available at: https://doi.org/10.1080/13504851.2014.916379

BCH, B. E. |. B. |. E. |., 2020. *Blockchain.com.* [Ηλεκτρονικό]
Available at: https://www.blockchain.com/explorer

Borri, N., 2022. *Conditional Tail-Risk in Cryptocurrency Markets.*

Bitcoin.fr, 2020. [Ηλεκτρονικό]
Available at:
https://bitcoin.fr/public/divers/docs/Estimation_de_la_durabilite_et_du_cout_du_reseau_Bitcoin.pdf

Bitcoin.org, 2020. [Ηλεκτρονικό]
Available at: https://bitcoin.org/bitcoin.pdf

Bitcoin[Timeline], B. H.: T. c. h. o., 2020. *Bitcoin History: The complete history of Bitcoin[Timeline].* [Ηλεκτρονικό]
Available at: http://historyofbitcoin.org/
[Πρόσβαση 2020].

Bitcoin, M. -. T. ε. σ. τ., 2020. *https://bitcoinx.gr/mining/.* [Ηλεκτρονικό]
Available at: https://bitcoinx.gr/mining/

chain, W.-B., 2020. *En.bitcoin.it.* [Ηλεκτρονικό]
Available at: https://en.bitcoin.it/wiki/Block_chain

circuit, A.-s. i., χ.χ. *En.wikipedia.org.* [Ηλεκτρονικό]
Available at: https://en.wikipedia.org/wiki/Application-specific_integrated_circuit

CoinDesk, B. 1. -., 2020. *CoinDesk.* [Ηλεκτρονικό]
Available at: https://www.coindesk.com/learn/bitcoin-101/get-started-mining-pools

CoinDesk, B. 1. -., 2020. *CoinDesk.* [Ηλεκτρονικό]
Available at: https://www.coindesk.com/learn/bitcoin-101/how-do-bitcoin-transactions-work

CoinDesk, B. 1. -., 2020. *CoinDesk.* [Ηλεκτρονικό]
Available at: https://www.coindesk.com/learn/bitcoin-101/how-to-store-your-bitcoins

Coinmarketcap.com, 2020. *How to Keep Your Crypto Safe | CoinMarketCap.* [Ηλεκτρονικό]
Available at: https://coinmarketcap.com/alexandria/article/how-to-keep-your-crypto-safe

Coinmarketcap, 2020. *How to Mine Bitcoin | CoinMarketCap.* [Ηλεκτρονικό]
Available at: https://coinmarketcap.com/alexandria/article/how-to-mine-bitcoin

Duffield, E., 2020. *Darkcoin: Peer to Peer Crypto Currency with Anonymous Blockchain Transactions and an Improved Proof of Work System.* [Ηλεκτρονικό]
Available at: https://www.semanticscholar.org/paper/Darkcoin-%3A-Peer-to-Peer-Crypto-Currency-with-and-an-Duffield-Hagan/b05da03086ac0b24d316bc604b25c9859df34339?p2df

econinfosec, 2020. *Weis2019.econinfosec.org.* [Ηλεκτρονικό]
Available at: https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_30.pdf

Franco, P., 2020. *Understanding Bitcoin: Cryptography, Engineering, and Economics.* s.l.: John Wiley & Sons Inc.

Name, 2020. *Icmec.org.* [Ηλεκτρονικό]
Available at: https://www.icmec.org/wp-content/uploads/2017/05/ICMEC-FCACPCryptocurrencyPaperFINAL5-17.pdf

Investopedia, 2020. *What are the Safest Ways to Store Bitcoin?.* [Ηλεκτρονικό]
Available at: https://www.investopedia.com/news/bitcoin-safe-storage-cold-wallet/

money, H. o., 2020. *En.wikipedia.org.* [Ηλεκτρονικό]
Available at: https://en.wikipedia.org/wiki/History_of_money

Money, T. B. B. M. P. F. M., 2020. *Bitcoinmining.com.* [Ηλεκτρονικό]
Available at: https://www.bitcoinmining.com/bitcoin-mining-pools/

Tu, A., 2020. *Cryptocurrency.*

Wiki, C. o. m. p. -. B., 2020. *En.bitcoin.it.* [Ηλεκτρονικό]
Available at: https://en.bitcoin.it/wiki/Comparison_of_mining_pools

Wikipedia, 2020. *History of bitcoin,*

Χρήμα, 2020. *El.wikipedia.org.* [Ηλεκτρονικό]
Available at:
https://el.wikipedia.org/wiki/%CE%A7%CF%81%CE%AE%CE%BC%CE%B1

Παράρτημα Α

ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ ΚΑΤΑΝΟΗΣΗΣ ΚΑΙ ΛΕΙΤΟΥΡΓΙΑΣ ΕΝΟΣ ΨΗΦΙΑΚΟΥ ΝΟΜΙΣΜΑΤΟΣ

Αυτό το ερωτηματολόγιο αποσκοπεί στην κατανόηση του κατά ποσό τα κρυπτονομίσματα υπάρχουν στην καθημερινή ζωή ενός ανθρώπου και σε ποιον βαθμό έχει κατανοήσει κάποιος την ύπαρξη και την λειτουργία του. Απαντώντας στις ακόλουθες ερωτήσεις , κάθε άτομο θα συμβάλλει σε ένα ερευνητικό έργο που αφορά το κρυπτονόμισμα. Καμία από τις πληροφορίες που θα παραχωρηθούν δεν θα χρησιμοποιηθεί ενάντια στην τρέχουσα απασχόληση κάθε ατόμου. Το ερωτηματολόγιο θα χρησιμοποιηθεί εξολοκλήρου για ερευνητικούς σκοπούς .

1. Φύλο

[ ] Άντρας

[ ] Γυναίκα

2. Ηλικία

[ ] 15-19

[ ] 19-30

[ ] 31-44

[ ] 45 και άνω

3. Επίπεδο Σπουδών

[ ] Υποχρεωτική Εκπαίδευση

[ ] Μέση Εκπαίδευση

[ ] ΑΕΙ / ΤΕΙ

[ ] Μεταπτυχιακό

[ ] Διδακτορικό

4. Ποια είναι η επαγγελματική σας ιδιότητα ;

[ ] Ιδιωτικός Υπάλληλος

[ ] Ελεύθερος Επαγγελματίας

[ ] Άνεργος

[ ] Συνταξιούχος

[ ] Δημόσιος Υπάλληλος

[ ] Άλλο

5. Έχει πραγματοποιηθεί ποτέ αγορά μέσω διαδικτύου ;

[ ] Ναι

[ ] Όχι

6. Ποσό συχνά πραγματοποιείται αγορά μέσω διαδικτύου ;

Πολύ σπάνια 1 [ ]

2 [ ]

3 [ ]

4 [ ]

Πολύ συχνά 5 [ ]

7. Ποσό καιρό έχετε συνειδητοποιήσει (εάν έχει γίνει αυτό) την ύπαρξη των ψηφιακών νομισμάτων ;

[ ] Καθόλου

[ ] Λιγότερο από 1 χρόνο

[ ] 1 – 2 χρόνια

[ ] 2 – 3 χρόνια

[ ] 3 – 4 χρόνια

[ ] Περισσότερα από 5 χρόνια

8. Υπάρχει γνώση χρήσης ενός ψηφιακού νομίσματος ;

[ ] Ναι

[ ] Όχι

[ ] ΔΓ / ΔΑ

9. Σε τι βαθμό θα εμπιστευόσουν την πραγματοποίηση μιας ηλεκτρονικής αγοράς με ψηφιακό νόμισμα ;

Καθόλου 1 [ ]

2 [ ]

3 [ ]

4 [ ]

Πάρα πολύ 5 [ ]

10. Γνωρίζεις κάποιο ψηφιακό νόμισμα ;

[ ] Ναι

[ ] Όχι

[ ] ΔΓ / ΔΑ

11. Αν ναι, είναι κάποια από τα παρακάτω ;

[] Bitcoin

[] Ripple

[] Litecoin

[] Dogecoin

[] ΔΓ / ΔΑ

12. Κατά την άποψη σας , μια συναλλαγή με bitcoin θεωρείται περισσότερο εύχρηστη από την κλασσική μέθοδο ;

[ ] Ναι

[ ] Όχι

[ ] ΔΓ / ΔΑ

13. Γνωρίζεις τρόπους / κάποιο μέσο που μπορείς να αποκτήσεις ψηφιακά νομίσματα ;

[ ] Ναι

[ ] Όχι

[ ] ΔΓ / ΔΑ

14. Σε τι βαθμό θα ήθελες να είσαι μέρος της παραγωγής των bitcoin με ένα μικρό μηνιαίο χρηματικό ποσό ;

Καθόλου 1 [ ]

2 [ ]

3 [ ]

4 [ ]

Πάρα πολύ 5 [ ]

15. Θα προτιμούσες την χρήση ηλεκτρονικού πορτοφολιού σε σύγκριση με το κανονικό ;

[ ] Ναι

[ ] Όχι

[ ] ΔΓ / ΔΑ

16. Σε ποιο βαθμό πιστεύετε ότι το ψηφιακό νόμισμα θα αντικαταστήσει το κανονικό στο μέλλον ;

Καθόλου 1 [ ]

2 [ ]

3 [ ]

4 [ ]

Πάρα πολύ 5 [ ]