ΣΧΟΛΗ ΕΠΙΣΤΗΜΩΝ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΤΜΗΜΑ ΛΟΓΙΣΤΙΚΗΣ ΚΑΙ ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΗΣ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΣΤΗ ΣΤΡΑΤΗΓΙΚΗ ΔΙΟΙΚΗΤΙΚΗ ΛΟΓΙΣΤΙΚΗ ΚΑΙ ΤΗ ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΗ ΔΙΟΙΚΗΣΗ

Διπλωματική Εργασία

Κρυπτονομίσματα και Διαχείριση Κινδύνου Κυβερνοχώρου

του

ΔΟΥΜΑ ΣΤΥΛΙΑΝΟΥ

Επιβλέπων Καθηγητής: ΛΙΒΑΝΗΣ ΕΥΣΤΡΑΤΙΟΣ

Υποβλήθηκε ως απαιτούμενο για την απόκτηση του Μεταπτυχιακού Διπλώματος στη

Στρατηγική Διοικητική Λογιστική και τη Χρηματοοικονομική Διοίκηση

Νοέμβριος 2019

ΠΕΡΙΛΗΨΗ

Η εκπόνηση της παρούσας διπλωματικής εργασίας στοχεύει στην ανάδειξη της τεχνολογίας που κρύβεται πίσω από τα κρυπτονομίσματα και στην ανάλυση των κινδύνων που έχουν παρουσιαστεί μέσα από αυτά.

Αρχικά θα γίνει μία ιστορική αναδρομή στην έννοια του χρήματος, μέχρι την εποχή των κρυπτονομισμάτων και στην συνέχεια θα αναλυθεί η λειτουργία της αλυσίδας των μπλοκ (blockchain). Έπειτα θα αναλυθεί το Bitcoin ως πρώτο κρυπτονόμισμα, καθώς θα γίνει αναφορά και στα υπόλοιπα δημοφιλή κρυπτονομίσματα προβάλλοντας τους λόγους για τους οποίους έχουν εδραιωθεί.

Επιπρόσθετα θα παρουσιαστούν οι κίνδυνοι κυβερνοχώρου που έχουν δημιουργηθεί μέσα από τα κρυπτονομίσματα, με αναλύσεις δύο περιπτώσεων με απάτες/κλοπές από γνωστές πλατφόρμες συναλλαγών.

Επιπλέον θα γίνει αναφορά στα κρυπτονομίσματα ως μέσο συναλλαγής για την νομιμοποίηση εσόδων από παράνομες δραστηριότητες, την εμπορία ναρκωτικών καθώς και τον εκβιασμό.

Τέλος θα προβληθούν τρόποι αντιμετώπισης των πιθανών κινδύνων που μπορεί να προκληθούν από συναλλαγές μέσω κρυπτονομισμάτων, προκειμένου να αποτραπούν πιθανές μελλοντικές απάτες.

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: Χρήμα, Κρυπτονομίσματα, Blockchain, Bitcoin, Ανταλλακτήριο

ABSTRACT

The aim of this paper is to highlight the technology hidden behind cryptocurrencies and the analysis of the risks that have been presented through them.

First, there will be a historical overview of the concept of money until the era of cryptocurrencies and then the functioning of the blockchain chain will be analyzed. Afterwards bitcoin will then be analyzed as the first cryptocurrency, with reference to the other popular cryptocurrencies outlining the reasons why they have been established.

In addition, cyber risks created through cryptocurrencies will be presented, with two case analysis of fraud / theft from known trading platforms.

Thereafter, cryptocurrencies will be mentioned as means of trading for money laundering, drug trafficking and extortion.

Finally, we will look at ways to deal with the potential risks that can be caused by cryptocurrency transactions in order to prevent possible future scams.

KEYWORDS: Money, Cryptocurrencies, Blockchain, Bitcoin, Exchange

Περιεχόμενα

1. ΕΙΣΑΓΩΓΗ

1.1. Εισαγωγικές παρατηρήσεις

Ο κοινός αποδεκτός ορισμός του χρήματος σύμφωνα με το Ευρετήριο Οικονομικών όρων είναι πως «Το χρήμα είναι το σύνολο των οικονομικών αξιών που οι άνθρωποι χρησιμοποιούν σε καθημερινή βάση για την αγορά αγαθών και υπηρεσιών και την αποπληρωμή δανείων».[1]

Σε μία σύγχρονη οικονομία τα είδη χρήματος που χρησιμοποιούνται είναι τα κέρματα, όπου είναι μεταλλικά νομίσματα χαμηλής αξίας που χρησιμοποιούνται για συναλλαγές μικρής αξίας, τα χαρτονομίσματα, τα οποία εκδίδει η Κεντρική Τράπεζα και η ποσότητά τους καθορίζεται με την εκάστοτε νομισματική πολιτική και οικονομικά κριτήρια της κάθε χώρας. Επιπρόσθετα υπάρχουν οι τραπεζικές επιταγές, όπου ο δικαιούχος λαμβάνει την επιταγή από την εμπορική τράπεζα με σκοπό να πληρώσει εκείνους με τους οποίους συναλλάσσεται καθώς επάνω στην επιταγή αναγράφεται το όνομα και η υπογραφή του δικαιούχου καθώς και το χρηματικό ποσό. Τέλος υπάρχουν και οι πιστωτικές κάρτες ή αλλιώς «πλαστικό χρήμα» με τις οποίες δίνεται η δυνατότητα στους καταναλωτές να κάνουν αγορές, τις οποίες θα εξοφλήσουν μετέπειτα στην τράπεζα, ενώ το συμβεβλημένο με την τράπεζα κατάστημα θα λάβει το ποσό άμεσα από τον τραπεζικό οργανισμό.[2]

Για την οικονομική οργάνωση μιας κοινωνίας απαραίτητες καθιστούνται οι βασικές λειτουργίες του χρήματος οι οποίες είναι:

i. Το χρήμα ως μέσο συναλλαγής, όπου οφείλεται ο μεγάλος καταμερισμός των έργων και η ανάπτυξη του εμπορίου.

---

[1] Ευρετήριο Οικονομικών όρων. (χ.χ) *Χρήμα (Money).* Ανακτήθηκε στις 15/6/2019 από τον ιστότοπο https://www.euretirio.com/xrima/.

[2] Λιανός Θ., Παπαβασιλείου Α. & Χατζηανδρέου Α. (8/2016). *Αρχές Οικονομικής Θεωρίας-Μικροοικονομία Μακροοικονομία*. Αθήνα: Ινστιτούτο Τεχνολογίας Υπολογιστών και Εκδόσεων – «ΔΙΟΦΑΝΤΟΣ»

ii. μονάδα μέτρησης της αξίας, η ζήτηση και η προσφορά διαμορφώνουν στην αγορά την τιμή ενός αγαθού σε χρηματικές μονάδες. Έτσι η αξία κάθε προϊόντος εκφράζεται σε χρηματικές μονάδες. Για παράδειγμα, η αξία ενός μικρού μπουκαλιού νερού είναι 0,5 ευρώ, ενός αναψυκτικού 2 ευρώ κτλ., το ευρώ δηλαδή γίνεται το μέτρο της απόλυτης αξίας των αγαθών**.** Μπορούμε επίσης με το χρήμα να προσδιορίσουμε την αξία ενός αγαθού σε σχέση με την αξία ενός άλλου, δηλαδή τη σχετική αξία των αγαθών.

iii. μέσο διατήρησης αξιών, εφόσον το χρήμα είναι μέτρο της απόλυτης αξίας των αγαθών, ο κάτοχος χρήματος μπορεί να διαθέτει τμηματικά μέρος των χρημάτων του για την αγορά αγαθών. Για παράδειγμα ένας παραγωγός σιτηρών σε μια οικονομία που δε χρησιμοποιεί χρήμα είναι υποχρεωμένος να διατηρεί σε αποθήκες την ετήσια παραγωγή του και να τη διαθέτει τμηματικά, ανταλλάσσοντάς την με άλλα αγαθά που έχει ανάγκη. Αν όμως γινόταν χρήση του χρήματος, ο ίδιος παραγωγός θα είχε τη δυνατότητα να πουλήσει ολόκληρη τη σοδιά του και να εισπράξει την αξία της σε χρήμα, το οποίο θα μπορούσε να δαπανά τμηματικά σε διαφορετικές χρονικές στιγμές για τις ανάγκες του. Έτσι το χρήμα γίνεται και μέσο διατήρησης αξιών.

1.2. Σκοπός και ερευνητικά ερωτήματα

Σκοπός της παρούσας διπλωματικής εργασίας είναι να δώσει την δυνατότητα στον αναγνώστη να κατανοήσει βασικές έννοιες των κρυπτονομισμάτων όπως, τι είναι τα κρυπτονομίσματα, πως δημιουργήθηκαν και εξελίχθηκαν, τον τρόπο λειτουργίας των κρυπτονομισμάτων, την τεχνολογία που κρύβεται πίσω από αυτά και ποια είναι αυτή την στιγμή τα κρυπτονομίσματα με την μεγαλύτερη κεφαλαιοποίηση. Στόχος όλης αυτής της ανάλυσης είναι να εξετάσουμε τους κινδύνους οι οποίοι υποβόσκουν με την χρήση των κρυπτονομισμάτων καθώς και αν το θεσμικό πλαίσιο γύρω από τα κρυπτονομίσματα είναι επαρκές.

Ερευνητικά ερωτήματα προκύπτουν και αφορούν λοιπόν, το κατά πόσο είναι ασφαλείς οι συναλλαγές κρυπτονομισμάτων μέσω ανταλλακτηρίων και αν τα κρυπτονομίσματα μπορούν να χρησιμοποιηθούν από τους χρήστες για παράνομες δραστηριότητες.

2. ΒΙΒΛΙΟΓΡΑΦΙΚΗ ΕΠΙΣΚΟΠΗΣΗ

Στην ενότητα αυτή θα γίνει μία ιστορική αναδρομή στο χρήμα και στην εξέλιξή του στο ψηφιακό νόμισμα. Μέσα από μία οικονομική και μία νομική σκοπιά θα αναφερθεί η έννοια του χρήματος, ώστε να γίνει αντιληπτή η διαφορά από τα ψηφιακά νομίσματα, από το παραστατικό και ηλεκτρονικό χρήμα.

2.1. Το Χρήμα

Το χρήμα από οικονομικής άποψης ακολουθεί τρείς βασικές λειτουργίες σύμφωνα με την οικονομική βιβλιογραφία. Αρχικά λειτουργεί ως μέσο ανταλλαγής αφού τα χρήματα χρησιμοποιούνται στο εμπόριο για να αποφευχθούν προβλήματα ενός ανταλλασσόμενου συστήματος. Δεύτερον, λειτουργεί ως αποθήκευση αξίας με την έννοια ότι τα χρήματα μπορούν να αποθηκευτούν και να ανακτηθούν στο μέλλον. Και τρίτον, το χρήμα λειτουργεί ως λογιστική μονάδα, τυποποιημένη δηλαδή αριθμητική μονάδα για τη μέτρηση της αξίας και του κόστους των αγαθών και των υπηρεσιών και των υποχρεώσεων και των περιουσιακών στοιχείων.[3]

Από νομικής πλευράς, χρήμα είναι οτιδήποτε χρησιμοποιείται για την ανταλλαγή αξίας στις συναλλαγές, ενώ ο όρος «νόμισμα» υποδηλώνει υποδιαιρέσεις χρημάτων όπως τα κέρματα και τα τραπεζογραμμάτια. Μπορούμε να πούμε πως νομικά το νόμισμα αναφέρεσαι στη συγκεκριμένη μορφή χρήματος που χρησιμοποιείται γενικά μέσα σε μία χώρα και λαμβάνοντας υπόψη το γεγονός ότι τα εικονικά νομίσματα

[3]ECB., (2015). *Virtual currency schemes –a further analysis*., Ανακτήθηκε στις 11/11/2019 από τον ιστότοπο: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf
BIS., (2015). *Digital currencies*., Ανακτήθηκε στις 11/11/2019 από τον ιστότοπο: https://www.bis.org/cpmi/publ/d137.pdf
Dabrowski,M.,Janikowsk, L.,(2018). *Virtual currencies and central banks monetary policy: challenges ahead*. Monetary Dialogue July 2018. IN-DEPTH ANALYSIS. Requested by the ECON committee., Ανακτήθηκε στις 11/11/2019 από τον ιστότοπο: http://www.europarl.europa.eu/cmsdata/149900/CASE_FINAL%20publication.pdf
Friedman H. David, *Χρήμα και Τραπεζική*., Ανακτήθηκε στις 18/11/2019 από τον ιστότοπο: https://static.eudoxus.gr/books/04/chapter-7304.pdf
Karl Marx (1999), «*Capital*», Progress Publishers.
F.S.Mishkin, (2000), «The Economics of Money, Banking and Financial markets».

δεν χρησιμοποιούνται ευρέως για την ανταλλαγή αξίας, δεν αποτελούν συνεπώς και νόμιμα νομίσματα. [4]

2.1.1. Ιστορική Εξέλιξη Χρήματος - Αντιπραγματισμός

Κατά την αρχαιότητα ξεκινά η δημιουργία του χρήματος, όχι με την σημερινή έννοια αλλά στηρίζονταν στον αντιπραγματισμό, υπερίσχυε δηλαδή η ανταλλακτική οικονομία. Η ανταλλακτική οικονομία λειτουργούσε χωρίς την ύπαρξη χρημάτων, αλλά με ανταλλαγή προϊόντων και υπηρεσιών που γινόταν μέσω διαπραγμάτευσης. Οι άνθρωποι δηλαδή στην αρχαιότητα, διαπραγματεύονταν την τιμή του προϊόντος που ήθελαν να ανταλλάξουν, ενώ ουσιαστικά η τιμή ήταν η ποσότητα του αγαθού με το οποίο γινόταν ανταλλαγή. Η ανταλλακτική οικονομία βασίζεται στην αρχή της αμοιβαιότητας. Οι ενδιαφερόμενοι δηλαδή που προβαίνουν στην ανταλλαγή αγαθών έχουν αμοιβαία θέληση να αποκτήσει ο ένας το αγαθού του άλλου, αφού συμφωνήσουν στην ποσότητα που πρέπει να ανταλλαχθεί από κάθε προϊόν έτσι ώστε η ανταλλαγή να είναι δίκαιη. Οι υποστηρικτές της ανταλλακτικής οικονομίας θεωρούν πως η αρχή της αμοιβαιότητας αποτελεί μία αίσθηση σύνδεσης μεταξύ τους αλλά και την αίσθηση ότι μαζί αποτελούν μία κοινωνία. Σημαντικό είναι να αναφέρουμε πως ενώ ο αντιπραγματισμός ήταν μία ενέργεια η οποία διαδραματιζόταν στην αρχαιότητα, άρχισε να υφίσταται και στις μέρες μας. Αυτό συμβαίνει λόγω των οικονομικών δυσκολιών που περνούν οι περισσότεροι λαοί καθώς να καταπολεμήσουν την οικονομική ανασφάλεια που έχει δημιουργηθεί. [5]

Όλο και περισσότερα προβλήματα βέβαια δημιουργούνται με το πέρασμα των χρόνων στις οικονομίες που λειτουργούσαν με τον αντιπραγματισμό. Ένα από τα βασικότερα προβλήματα ήταν η άμεση εύρεση ατόμου που είχε ένα αγαθό και ήθελε να το ανταλλάξει με ένα άλλο άτομο, με την προϋπόθεση να υπάρχει αμοιβαία θέληση

[4] ECB., (2015). *Virtual currency schemes –a further analysis*., Ανακτήθηκε στις 11/11/2019 από τον ιστότοπο: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf

[5] Margaret Rouse. (January, 2014) *Barter economy.* Ανακτήθηκε στις 26/6/2019 από τον ιστότοπο https://whatis.techtarget.com/definition/barter-economy

Hauhgh Matthew (2014), *Barter Economy.*, Ανακτήθηκε στις 18/11/2019 από τον ιστότοπο: https://whatis.techtarget.com/definition/barter-economy

και από τις δύο μεριές για να γίνει η ανταλλαγή. Ακόμη ένα βασικό πρόβλημα ήταν ο καθορισμός της αξίας των αγαθών που ανταλλάσσονταν.

2.1.2. Μέσο συναλλαγής- Χρήση Μετάλλων

Γύρω στην 3η χιλιετία π.Χ στην περιοχή της Μεσοποταμίας ξεκίνησε η χρήση μετάλλων ως μέσο συναλλαγής καθώς σιγά σιγά όλες οι κοινότητες συμφώνησαν στο γεγονός πως θα έπρεπε να έχουν ένα αγαθό με το οποίο θα αντάλλαζαν τα υπόλοιπα και έτσι άρχισαν να χρησιμοποιούν τα μέταλλα. Τα μέταλλα δεν χρησιμοποιούνταν μόνο ως σύμβολο συναλλαγής αλλά και αλλά και για μέτρηση της αξίας των προϊόντων και των υπηρεσιών που προσέφεραν. [6] Βάση επιγραφών που υπάρχουν εκείνη την εποχή, υπήρχαν διάφοροι νόμοι που τηρούσαν μεταξύ τους οι συναλλασσόμενοι. Έκαναν διάφορα συμβόλαια και πλήρωναν με βάση το ποσό του μετάλλου. Τα μέταλλα όπως ο χρυσός, ο χαλκός, ο άργυρος και το ασήμι χρησιμοποιούνταν σε ακατέργαστη μορφή καθώς και η αξία τους υπολογιζόταν με βάση το βάρος τους.

Στην Αρχαία Ελλάδα χρησιμοποιούσαν τα τάλαντα στις συναλλαγές τους.[7]

[6] Κανελλόπουλος Αθανάσιος (1996). *Σύγχρονες Οικονομικές Σκέψεις των Αρχαίων Ελλήνων*. Λιβάνης: Νέα Σύνορα.
Παπαδόπουλος Α. , (2002) , *Νομισματική Θεωρία και Πολιτική*, Ρέθυμνο.

[7] Δέσποινας Ευγενίδου, Ευαγγελίας Αποστόλου, Γιάννη Στόγια, Παναγιώτη Τσελέκα, Μαίρης Φουντουλή, Ευτέρπης Ράλλη, * Αλέξη Τότσικα**.** (χ.χ.) Το νόμισμα στον Αρχαίο Ελληνικό Κόσμο. *Αργολική Αρχειακή Βιβλιοθήκη Ιστορίας και πολιτισμού*. Ανακτήθηκε στις 26/6/2019 από τον ιστότοπο https://argolikivivliothiki.gr/tag/%CF%84%CE%BF-%CE%BD%CF%8C%CE%BC%CE%B9%CF%83%CE%BC%CE%B1-%CF%83%CF%84%CE%BF%CE%BD-%CE%B1%CF%81%CF%87%CE%B1%CE%AF%CE%BF-%CE%B5%CE%BB%CE%BB%CE%B7%CE%BD%CE%B9%CE%BA%CF%8C-%CE%BA%CF%8C%CF%83%CE%BC%CE%BF/

 [8]

Διάγραμμα 1: Τάλαρα

Αργότερα κατά τον 7ο αιώνα π.Χ άρχισαν να χρησιμοποιούν ένα σιδερένιο αντικείμενο για τις συναλλαγές του που ονομαζόταν Οβολός. [9]

Έπειτα από την χρήση των διάφορων μετάλλων που χρησιμοποιήθηκαν για τις συναλλαγές, οι αρχαίοι επινόησαν την χρήση μικρότερων μετάλλων δίνοντας το μήκος και το σχήμα που τους επέτρεπε την εύκολη μεταφορά τους. Τυποποίησαν έτσι διάφορα νομίσματα τα οποία ήταν σφραγισμένα από κάποιους υπεύθυνους, ενώ παράλληλα χάραζαν και την αξία του μετάλλου έτσι ώστε να μην είναι απαραίτητη η διαδικασία του ζυγίσματος. [10]

[8] Η εικόνα ανακτήθηκε στις 26/6/2019 από τον ιστότοπο https://www.google.com/search?q=%CF%84%CE%B1%CE%BB%CE%B1%CE%BD%CF%84%CE%B1+%CE%BD%CE%BF%CE%BC%CE%B9%CF%83%CE%BC%CE%B1%CF%84%CE%B1&source=lnms&tbm=isch&sa=X&ved=0ahUKEwix4PHV4IzjAhUs2aYKHeQsAHYQ_AUIECgB&biw=1351&bih=636#imgrc=Yh6kUS-DpvZOOM:

[9] Δέσποινας Ευγενίδου, Ευαγγελίας Αποστόλου, Γιάννη Στόγια, Παναγιώτη Τσελέκα, Μαίρης Φουντουλή, Ευτέρπης Ράλλη, * *Αλέξη Τότσικα***.** (χ.χ.) Το νόμισμα στον Αρχαίο Ελληνικό Κόσμο. *Αργολική Αρχειακή Βιβλιοθήκη Ιστορίας και πολιτισμού*. Ανακτήθηκε στις 26/6/2019 από τον ιστότοπο https://argolikivivliothiki.gr/tag/%CF%84%CE%BF-%CE%BD%CF%8C%CE%BC%CE%B9%CF%83%CE%BC%CE%B1-%CF%83%CF%84%CE%BF%CE%BD-%CE%B1%CF%81%CF%87%CE%B1%CE%AF%CE%BF-%CE%B5%CE%BB%CE%BB%CE%B7%CE%BD%CE%B9%CE%BA%CF%8C-%CE%BA%CF%8C%CF%83%CE%BC%CE%BF/

[10] Δέσποινας Ευγενίδου, Ευαγγελίας Αποστόλου, Γιάννη Στόγια, Παναγιώτη Τσελέκα, Μαίρης Φουντουλή, Ευτέρπης Ράλλη, * Αλέξη Τότσικα**.** (χ.χ.) Το νόμισμα στον Αρχαίο Ελληνικό Κόσμο. *Αργολική Αρχειακή Βιβλιοθήκη Ιστορίας και πολιτισμού*. Ανακτήθηκε στις 26/6/2019 από τον ιστότοπο https://argolikivivliothiki.gr/tag/%CF%84%CE%BF-%CE%BD%CF%8C%CE%BC%CE%B9%CF%83%CE%BC%CE%B1-%CF%83%CF%84%CE%BF%CE%BD-%CE%B1%CF%81%CF%87%CE%B1%CE%AF%CE%BF-%CE%B5%CE%BB%CE%BB%CE%B7%CE%BD%CE%B9%CE%BA%CF%8C-%CE%BA%CF%8C%CF%83%CE%BC%CE%BF/

[11]

Διάγραμμα 2: Οβολός

2.1.3. Δημιουργία Τραπεζών

Κατά τον 6ο αιώνα π.Χ χρονολογείται η πρώτη τράπεζα που άρχισε να λειτουργεί και να δραστηριοποιείται στον Ελλαδικό χώρο. Κύρια ευθύνη της πρώτης τράπεζας ήταν ο έλεγχος των διάφορων νομισμάτων που χρησιμοποιούσαν οι κοινωνίες. Αυτό συνέβαινε διότι πολλά νομίσματα τα οποία ο λαός χρησιμοποιούσε για τις συναλλαγές του δεν ήταν όμοια μεταξύ τους και έτσι δημιουργήθηκε η ανάγκη ενός οργανισμού ο οποίος θα ήταν σε θέση να αναλάβει τον έλεγχο της ποιότητας των νομισμάτων αυτών.[12] Εν συνεχεία, οι νεοσύστατες τράπεζες δημιουργούν τον τόκο με αποτέλεσμα οι τραπεζίτες να δίνουν τόκο σε όσους κατέθεταν τα χρήματά τους στις τράπεζες. Έτσι όλος και περισσότερος κόσμος άρχισε να καταθέτει τα χρήματά του στις τράπεζες, με απώτερο σκοπό να αυξήσει το ποσοστό των χρημάτων του. Με αυτόν τον τρόπο λοιπόν άρχισε να λειτουργεί και να υφίσταται μέχρι και σήμερα ο θεσμός της τράπεζας, βέβαια με διαφορετική μορφή από το ξεκίνημά της. Οι ιδιωτικές και οι δημόσιες καταθέσεις αργυρών αλλά και οι παραχωρήσεις αυτών σε μορφή δανείου ξεκίνησαν από τον 5ο

[11] Η εικόνα ανακτήθηκε στις 26/6/2019 από τον ιστότοπο https://www.google.com/search?q=%CE%BF%CE%B2%CE%BF%CE%BB%CE%BF%CF%82++%CE%BD%CE%BF%CE%BC%CE%B9%CF%83%CE%BC%CE%B1%CF%84%CE%B1&source=lnms&tbm=isch&sa=X&ved=0ahUKEwj39vOH3YzjAhUE7aYKHZVMBIYQ_AUIECgB&biw=1351&bih=587#imgrc=2GyIj1Ea8gny8M:

[12] Τιβέριος Μ.Δ. (20/6/ 1999; Δημοσιεύθηκε 24/11/2008). Τράπεζες και τοκογλύφοι στην Αρχαία Ελλάδα. *Το Βήμα.* Ανακτήθηκε στις 27/6/2019 από τον ιστότοπο https://www.tovima.gr/2008/11/24/opinions/trapezes-kai-tokoglyfoi-stin-arxaia-ellada/

αιώνα π.Χ. Επιπρόσθετα τότε ξεκίνησαν οι τραπεζίτες να διαχειρίζονται τις περιουσίες ανθρώπων που εμπιστεύονταν τα χρήματά τους σε αυτούς και άρχισαν να δίνουν εντολές για λογαριασμό τρίτων, γεγονός που γίνεται και σήμερα. [13]

2.2. Ιδιωτικό Χρήμα

2.2.1. Κρυπτονομίσματα, Εικονικό Και Ψηφιακό χρήμα

Για το ιδιωτικό χρήμα χρησιμοποιούνται οι ορολογίες κρυπτονομίσματα, εικονικό χρήμα και ψηφιακό χρήμα, χωρίς αυτό να σημαίνει ότι αυτές ταυτίζονται απαραίτητα. Εικονικό χρήμα ή αλλιώς VCs[14] είναι κάτι που χρησιμοποιείται ως μέσο συναλλαγής και υπάρχει μόνο στο διαδίκτυο χωρίς να ρυθμίζεται από κάποια κυβέρνηση.[15]Το ψηφιακό χρήμα είναι άυλο, δεν μπορεί να έχει φυσική παρουσία, η δημιουργία του βασίζεται μόνο σε αλγοριθμικές παραστάσεις και το απαραίτητο εργαλείο μέσω του οποίου οι ενδιαφερόμενοι μπορούν να κάνουν συναλλαγές με αυτού του είδους το χρήμα είναι ο ηλεκτρονικός υπολογιστής. Μέσω των ψηφιακών νομισμάτων μπορεί φυσικά να πραγματοποιηθεί αγορά αγαθών και υπηρεσιών και μπορούν να χρησιμοποιηθούν ποικιλοτρόπως για διασυνοριακές πληρωμές αρκεί ο κάτοχος αυτών των νομισμάτων να είναι συνδεδεμένος στο διαδίκτυο μέσω του ηλεκτρονικού υπολογιστή.

---

[13] Φίλιππας Ν. (30/5/2011). Οι Αρχαίοι Έλληνες και η Οικονομία. *Μύρτις*. . Ανακτήθηκε στις 27/6/2019 από τον ιστότοπο http://www.myrtis.gr/index.php?option=com_content&view=article&id=253&Itemid=315&lang=fr
Ένωση Ελληνικών Τραπεζών, (2003), «*Οι Τράπεζες μοχλός της ανάπτυξης*», ενημερωτικό έντυπο με ομιλία προέδρου Ε.Ε.Τ κα.Θ.Καρατζά.

[14] Schollmeir Rüdiger. "A Definition of Peer-to-Peer Networking for the Classification of Peer-to Peer Architectures and Applications" Munchen, 2002 Ανακτήθηκε στις 1/9/2019 από τον ιστότοπο https://www.researchgate.net/publication/3940901_A_Definition_of_Peer-to-Peer_Networking_for_the_Classification_of_Peer-to-Peer_Architectures_and_Applications, 8

[15] J.P. and G.T., *Virtual Currency: The Economist*, Ανακτήθηκε στις 6/7/2019 από τον ιστότοπο z

2.2.2. Ορισμός Κρυπτονομισμάτων (cryptocurrency)

Με βάση το oxford dictionary ως κρυπτονόμισμα ορίζεται ένα «ψηφιακό νόμισμα στο οποίο χρησιμοποιούνται τεχνικές κρυπτογράφησης (encryption techniques) για την ρύθμιση της παραγωγής μονάδων νομίσματος και την επαλήθευση της μεταφοράς κεφαλαίων που λειτουργεί ανεξάρτητα από μία κεντρική τράπεζα»[16]

3. Η ΤΕΧΝΟΛΟΓΙΑ ΠΙΣΩ ΑΠΟ ΤΑ ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΑ ΑΛΥΣΙΔΑ ΤΩΝ ΜΠΛΟΚ (BLOCKCHAIN)

3.1. Ορισμός Αλυσίδας Μπλοκ (Blockchain)

Ως Blockchain ορίζεται ένα αποκεντρωμένο συνεχές κατανεμημένο κατάστιχο στο οποίο καταγράφονται οι συναλλαγές. Μία βάση δεδομένων η οποία διαμοιράζεται από όλους τους κόμβους του δικτύου, ανανεώνεται από τους εξορυκτές(miners), παρακολουθείτε από τον καθένα και δεν ελέγχεται από κανέναν. Είναι σαν ένα τεράστιο δια δραστικό φύλλο στο οποίο μπορεί να έχει πρόσβαση ο καθένας και ανανεώνεται και επιβεβαιώνει ότι οι ψηφιακές συναλλαγές μεταφοράς κεφαλαίων είναι μοναδικές.[17]

[16] Lexico. *Cryptocurrency,* ανακτήθηκε στις 6/7/2019 από τον ιστότοπο https://www.lexico.com/en/definition/cryptocurrency
Πιτσικός Σπύρος, «*Τι είναι τα κρυπτονομίσματα και πώς επενδύει κανείς σε αυτά*», Ανακτήθηκε στις 16/11/2019 από ιστότοπο https://www.news.gr/oikonomia/article/919934/ti-ine-ta-kriptonomismata-ke-pos-ependii-kanis-se-afta.html
[17] Swan Melanie (2015)., *Blockchain: Blueprint for a new economy*., O' Reilly Media, Inc.

3.2. Δίκτυο «Peer to Peer»

Η τεχνολογία «blockchain» βασίζεται σε ένα «peer to peer» αρχιτεκτονικά δομημένο δίκτυο ως ένα στρώμα πάνω στο Διαδίκτυο. Η συγκεκριμένη μορφή δικτύου ξεχωρίζει από τα μέχρι σήμερα συστήματα δικτύου γιατί δεν υπάρχει ένας κεντρικός υπολογιστής (server) ο οποίος επιτρέπει την επικοινωνία του υπολογιστή με το δίκτυο. Αντ' αυτού η εμπιστοσύνη επιτυγχάνεται από τις αλληλεπιδράσεις των διαφόρων συμμετεχόντων στο δίκτυο (κόμβοι). Οι κόμβοι σε ένα τέτοιο δίκτυο στέλνουν και λαμβάνουν πακέτα την ίδια στιγμή. Τα δίκτυα «peer to peer» ονομάστηκαν έτσι λόγω του ότι οι συμμετέχοντες στο δίκτυο είναι ομότιμοι μεταξύ τους, «peer». Συνοψίζοντας, τα δίκτυα «peer to peer» είναι ανθεκτικά αποκεντρωμένα και ανοιχτά. Στο παρελθόν έχουμε δει επιτυχημένες μορφές «peer to peer» δικτύου, με το «Napster» ως πρωτοπόρο και τις εφαρμογές «Torrent» πιο πρόσφατα.[18]

3.3. Τρόπος Λειτουργίας Της Αλυσίδας Μπλοκ (Blockchain)

Η δομή δεδομένων της αλυσίδας των μπλοκ είναι μία ταξινομημένη, συνδεδεμένη προς τα πίσω (backlinked) λίστα των μπλοκ των συναλλαγών.[19] Η αλυσίδα των μπλοκ αποθηκεύεται ως ένα απλό αρχείο η μία απλή βάση δεδομένων. Τα δεδομένα αποθηκεύονται χρησιμοποιώντας την βάση δεδομένων LevelDB της Google. Τα μπλοκ της αλυσίδας έχουν τρία βασικά χαρακτηριστικά,

1. Την πληροφορία που θέλουμε να καταγράψουμε (συναλλαγή)
2. Τον μοναδικό αριθμό κατακερματισμού του προηγούμενου μπλοκ (previous block hash)
3. Την κρυπτογραφική περιστασιακή τιμή. (nonce)

Η πληροφορία η οποία θέλουμε να καταγράψουμε, κρυπτογραφείται με την χρήση του αλγόριθμου κρυπτογραφικού κατακερματισμού SHA256 στην κεφαλίδα του μπλοκ. Ο συγκεκριμένος αλγόριθμος έχει την ιδιότητα να παίρνει πληροφορίες

[16] Antonopoulos M. Andreas (2014), *Mastering Bitcoin*, United States of America: O'Reilly Media, Inc.
[19] Antonopoulos M. Andreas (2014), *Mastering Bitcoin*, United States of America: O'Reilly Media, Inc.

ανεξαρτήτου μεγέθους και να τις μετατρέπει σε μία σειρά από αριθμούς ή γράμματα συγκεκριμένου μεγέθους μοναδικού συνδυασμού (hash). Αυτή η ακολουθία με κάθε νέο μπλοκ που αναγράφει τον αριθμό κατακερματισμού του προηγούμενου μπλοκ (hash) δημιουργεί μία αλυσίδα μέχρι το 1ο μπλοκ που δημιουργήθηκε, το γνωστό ως μπλοκ γέννησης.

3.4. Αλγόριθμος Συναίνεσης (Consensus Algorithm) [20]

Ως αλγόριθμος συναίνεσης ορίζεται ο μηχανισμός μέσα από τον οποίο μία συναλλαγή επιβεβαιώνεται και προστίθεται στην αλυσίδα μπλοκ.

Υπάρχουν 4 βασικοί Αλγόριθμοι Συναίνεσης, ο αριθμός των οποίων αυξάνεται καθώς εξελίσσεται η τεχνολογία «blockchain» σε μία προσπάθεια να βρεθεί ο βέλτιστος μηχανισμός συναίνεσης.

1. Proof of Work (Pow)

   Είναι ο πρώτος μηχανισμός συναίνεσης που χρησιμοποιήθηκε στην τεχνολογία Blockchain, και πιο συγκεκριμένα αυτό έγινε μέσα από το Bitcoin. Ο συγκεκριμένος μηχανισμός είναι άμεσα συνδεδεμένος με την υπολογιστική δύναμη του εκάστοτε υπολογιστή. Οι εξορύκτες (miners) στο δίκτυο διαγωνίζονται μεταξύ τους στην επίλυση ενός αλγόριθμου. Αυτοί οι αλγόριθμοι είναι πολύ δύσκολο να λυθούν, αλλά πολύ εύκολο να επιβεβαιωθούν. Όταν ένας εξορύκτης βρει την λύση, θα την διαδώσει στο δίκτυο, και οι άλλοι εξορύκτες θα ελέγξουν αν επιβεβαιώνεται. Κατά την επιβεβαίωση ο εξορύκτης που βρήκε την λύση θα ανταμειφθεί για την εργασία του με μία συγκεκριμένη ποσότητα κρυπτονομίσματος.

   Εξόρυξη μπορούμε να κάνουμε χρησιμοποιώντας

   i. Τον Επεξεργαστή του Η/Υ (CPU)
   ii. Την κάρτα γραφικών του Η/Υ (GPU)
   iii. Εξειδικευμένες συσκευές εξόρυξης (ASIC)

[20] Binance Academy, «*What Is a Blockchain Consensus Algorithm?*» Ανακτήθηκε στις 20/7/2019 από τον ιστότοπο https://www.binance.vision/blockchain/what-is-a-blockchain-consensus-algorithm

Χαρακτηριστικά PoW

- Το δίκτυο θεωρείται ασφαλές λόγω της τεράστιας υπολογιστικής δύναμης που έχει παγκοσμίως.
- Χρειάζεται μεγάλο κεφάλαιο επένδυσης για την έναρξη εξόρυξης
- Οι εξορύκτες που ανταγωνίζονται μεταξύ τους χρησιμοποιούν μεγάλη ισχύ σε ηλεκτρικό ρεύμα

2. Proof of Stake (PoS)

   Σε αυτόν τον μηχανισμό συναίνεσης, θεωρείται ότι δεν γίνεται εξόρυξη των νέων μπλοκ αλλά σφυρηλάτηση. Το δίκτυο επιλέγει ένα κόμβο «node» ο οποίος θα είναι ο κόμβος που θα επιβεβαιώσει το επόμενο μπλοκ. Για να μπορέσει κάποιος να συμμετέχει στην διαδικασία της σφυρηλάτησης, πρέπει να δεσμεύσει κάποια, νομίσματα τα οποία κατέχει στο δίκτυο. Στην συνέχεια η επιλογή του κόμβου που θα σφυρηλατήσει το νέο μπλοκ γίνεται με ένα συνδυασμό κριτήριων όπως, η χρονική περίοδος που ο κόμβος αναμένει να κάνει σφυρηλάτηση του νέου μπλοκ, τυχαιοποίηση, και το πόσα νομίσματα έχει δεσμεύσει (όσο περισσότερα τόσες περισσότερες πιθανότητες). Σε αυτόν τον μηχανισμό συναίνεσης νέα νομίσματα δημιουργούνται ως κόστη συναλλαγής και δίνονται στον κόμβο που έκανε την σφυρηλάτηση. Για να χρησιμοποιηθεί ο μηχανισμός PoS σε κάποιο κρυπτονόμισμα, είτε το ίδιο ξεκινάει να λειτουργεί με τον αλγόριθμο PoW και στην συνέχεια αλλάζει, είτε ξεκινάει με την πώληση νομισμάτων τα οποία έχουν δημιουργηθεί πριν την έναρξη των συναλλαγών του κρυπτονομίσματος στο κοινό.

   Χαρακτηριστικά PoS

   - Σε αυτήν την μορφή η υπολογιστική δύναμη δεν παίζει κανένα ρόλο
   - Ο συγκεκριμένος μηχανισμός είναι αποδοτικός από άποψη ενέργειας

- Ενθαρρύνει του χρήστες να γίνουν κόμβοι και είναι ιδιαίτερα αποκεντρωμένο λόγω της τυχαιοποίησης που υπάρχει στην επιλογή του κόμβου

3. Delegated Proof of Stake (DPoS)

   Ο μηχανισμός συναίνεσης DPoS δημιουργήθηκε στο 2014 από τον «Daniel Larimer». Διατηρείται μέσω από ένα σύστημα εκλογών, όπου οι κάτοχοι των νομισμάτων ψηφίζουν έναν αντιπρόσωπο ο οποίος είναι υπεύθυνος να επιβεβαιώσει νέα μπλοκ. Θεωρείται από πολλούς ένας πιο αποδοτικός και δημοκρατικός τρόπος από την μέθοδο PoS. Οι αντιπρόσωποι μπορεί να είναι από 21-101 και ψηφίζονται από τους χρήστες του δικτύου που κατέχουν νομίσματα. Κάθε χρήστης έχει τόσες ψήφους όσες και τα νομίσματα που έχει. Νέα μπλοκ δημιουργούνται κάθε μερικά δευτερόλεπτα και κάθε αντιπρόσωπος έχει προκαθορισμένα μπλοκ που θα επιβεβαιώσει.

   Χαρακτηριστικά DPoS

   - Τα χαρακτηριστικά του μηχανισμού είναι ίδια με αυτού του PoS, ωστόσο ο μηχανισμός DPoS εισάγει ένα δημοκρατικό σύστημα ψηφοφορίας.
   - Ο μηχανισμός DPoS τείνει να είναι πιο γρήγορος ως προς τις συναλλαγές ανά δευτερόλεπτο.

4. Proof of Aythority (PoA)

   Ο μηχανισμός συναίνεσης PoA δημιουργήθηκε το 2017 από τον συνιδρυτή του γνωστού κρυπτονομίσματος «etherium» Gavin Wood και είναι ιδιαίτερα διαδεδομένος στα ιδιωτικά δίκτυα. Είναι ο τροποποιημένος μηχανισμός συναίνεσης «Proof of Stake». Η σημαντική διαφορά είναι ότι οι κόμβοι επιβεβαίωσης των μπλοκ είναι υποχρεωμένοι να ανακοινώσουν την πραγματική τους ταυτότητα, και να δεσμεύσουν την φήμη τους και όχι νομίσματα.

Χαρακτηριστικά

- Οι κόμβοι επιβεβαίωσης πρέπει να επικυρώσουν την πραγματική τους ταυτότητα
- Ο συγκεκριμένος μηχανισμός συναίνεσης αποκλείει την αποκέντρωση του δικτύου.
- Αποτελεί έναν ενδιαφέρον μηχανισμό συναίνεσης ο οποίος αντιτίθεται στην ιδεολογία και τον λόγο ύπαρξης των κρυπτονομισμάτων, αποτελεί όμως έναν μηχανισμό συναίνεσης ο οποίος ταιριάζει καλύτερα σε ιδιωτικά δίκτυα αλυσίδας μπλοκ.

3.5. Ασφάλεια Της Αλυσίδας Των Μπλοκ (Blockchain Security)

Οι αλυσίδες των μπλοκ διασφαλίζουν την ακεραιότητα τους μέσα από διάφορους μηχανισμούς που περιλαμβάνουν προηγμένες κρυπτογραφικές τεχνικές και μαθηματικά μοντέλα συμπεριφοράς και λήψης αποφάσεων. Η τεχνολογία «Blockchain» είναι ο θεμελιώδης λίθος των κρυπτονομισμάτων και είναι φτιαγμένη με τέτοιο τρόπο ώστε να είναι ασφαλής. Αυτό επιτυγχάνεται μέσα από πολλές δικλίδες ασφαλείας. Οι δύο σημαντικότερες είναι, ο μηχανισμός συναίνεσης που αναλύσαμε νωρίτερα και η ιδιότητα που έχει να είναι αμετάβλητη.[21]

Ο συνδυασμός των δύο παραπάνω χαρακτηριστικών παρέχουν την βάση για την ασφάλεια της αλυσίδας των μπλοκ. Καθώς ο αλγόριθμος συναίνεσης διασφαλίζει ότι όλοι οι κανόνες του συστήματος ακολουθούνται από τους χρήστες κατά την διαδικασία της εξέλιξης της αλυσίδας των μπλοκ, η ιδιότητα να μένει αμετάβλητη διασφαλίζει την ακεραιότητα των δεδομένων αφού με κάθε νέο μπλοκ οι συναλλαγές επιβεβαιώνονται.[22]

[21] Binance Academy, « *What Makes a Blockchain Secure?»* Ανακτήθηκε στις 24/8/2019 από τον ιστότοπο https://www.binance.vision/blockchain/what-makes-a-blockchain-secure

[22] Binance Academy, « *What Makes a Blockchain Secure?»* Ανακτήθηκε στις 24/8/2019 από τον ιστότοπο https://www.binance.vision/blockchain/what-makes-a-blockchain-secure

3.5.1. Κρυπτογραφία Στην Αλυσίδα Των Μπλοκ

Οι αλυσίδες των μπλοκ βασίζονται στην αρχιτεκτονική της κρυπτογραφίας για να επιτύχουν την ασφάλεια των δεδομένων. Ο αλγόριθμος κατακερματισμού είναι αυτός που χρησιμοποιείται και έχει την ιδιότητα να λαμβάνει δεδομένα ανεξαρτήτου μεγέθους και μας δίνει σαν αποτέλεσμα ένα προκαθορισμένο μέγεθος χαρακτήρων. Το σημείο κλειδί σε αυτήν την διαδικασία είναι ότι τα δεδομένα που λαμβάνονται υπόψιν είναι το αποτέλεσμα του αλγόριθμου κατακερματισμού του προηγούμενου μπλοκ και τα δεδομένα των συναλλαγών. Αν εισάγουμε τα ίδια δεδομένα, όσες φορές και αν χρησιμοποιήσουμε τον αλγόριθμο κατακερματισμού, πάντα θα λαμβάνουμε το ίδιο αποτέλεσμα. Έτσι, αν κάποιος προσπαθήσει να αλλάξει μία συναλλαγή, το αποτέλεσμα που θα λάβουμε από τον αλγόριθμο κατακερματισμού θα είναι εντελώς διαφορετικό. Κατ' επέκταση θα αλλάξει ο αριθμός κατακερματισμού όλων των επόμενων μπλοκ. Πρακτικά αυτή αλλαγή δεν επιβεβαιώνεται, γιατί όλοι οι κόμβοι του δικτύου, διατηρούν αντίγραφο της αλυσίδας μπλοκ και ως έγκυρη αλυσίδα θεωρείται η μεγαλύτερη. Αυτό διασφαλίζει ότι όλα τα μπλοκ της αλυσίδας μένουν αμετάβλητα και δεν μπορεί να γίνει αλλαγή σε κανένα προηγούμενο μπλοκ.

3.6. Επιθέσεις Στην Αλυσίδα Μπλοκ[23]

Η τεχνολογία «Blockchain» με τις ιδιότητες που έχει εξ 'ορισμού μοιάζει ως μία από τις βέλτιστες επιλογές σχετικά με την ασφάλεια. Σε αυτήν την νέα εποχή πραγμάτων, εμφανίζονται νέες επιθέσεις οι οποίες είναι πολύ εξελιγμένες και μπορούν να προκαλέσουν ανεπανόρθωτες ζημιές. Παρακάτω θα δούμε μερικές από αυτές.

[23] Abilash Soundararajan, 10 Blockchain and New Age Security Attacks You Should Know, Ανακτήθηκε στις 25/8/2019 από τον ιστότοπο: https://blogs.arubanetworks.com/solutions/10-blockchain-and-new-age-security-attacks-you-should-know/

3.6.1. Επιθέσεις Βασισμένες Στο Δίκτυο «Peer to Peer»

- Επίθεση «Eclipse»: Ένας κόμβος βασίζεται σε «Χ» αριθμό κόμβων για να συγκρίνει το αντίγραφο της αλυσίδας που έχει ο ίδιος. Αν αυτός ο κόμβος δεχτεί επίθεση και ο επιτιθέμενος καταφέρει να τον κάνει να βασίζεται σε «Ψ» κόμβους οι οποίοι έχουν μία «πειραγμένη» αλυσίδα, αυτή που έχει φτιάξει ο επιτιθέμενος, τότε θα κάνει τον κόμβο να αναγνωρίσει την νέα αλυσίδα ως έγκυρη.
- Επίθεση «Sybil»: Ο επιτιθέμενος θα προσθέσει στο δίκτυο έναν τεράστιο αριθμό από κόμβους με ψευδή ταυτότητες και θα προσπαθήσει να επηρεάσει το δίκτυο. Οι κόμβοι θα μοιάζουν ανεξάρτητοι μεταξύ τους, όμως στην πραγματικότητα θα λειτουργούν υπό την καθοδήγηση ενός ανθρώπου. Σε αυτήν την περίπτωση ο επιτιθέμενος φτιάχνει διακλαδώσεις στην αλυσίδα και προσπαθεί να διπλό ξοδέψει τα κρυπτονομίσματα τα οποία έχει.

3.6.2. Επιθέσεις Στον Μηχανισμό Συναίνεσης

- Επίθεση «Selfish mining»: Σε πολλές αλυσίδες μπλοκ θεωρείται ότι η μεγαλύτερη αλυσίδα είναι η έγκυρη. Κατά την συγκεκριμένη επίθεση ένας εξορύκτης (miner) προσπαθεί να μεγαλώσει την αλυσίδα μπλοκ χωρίς να την δημοσιεύει «stealth mode» και όταν καταφέρει να είναι μπροστά από το υπόλοιπο δίκτυο κατά δύο ή και παραπάνω μπλοκ τότε δημοσιεύει την δική του διακλάδωση η οποία γίνεται αποδεκτή από του άλλους κόμβους λόγω του ότι είναι η μεγαλύτερη. Ο τρόπος που εκμεταλλεύεται την προαναφερθείσα κατάσταση, είναι πολύ απλός. Ο ίδιος κάνει συναλλαγές στο δίκτυο λίγο πριν δημοσιεύσει την αλυσίδα των μπλοκ που έχει δημιουργήσει, και με την νέα αλυσίδα αναστρέφει τις συναλλαγές που μόλις έκανε.
- Επίθεση «Mining malware»: Κακόβουλο λογισμικό χρησιμοποιεί την υπολογιστική δύναμη του υπολογιστή του ανυποψίαστου θύματος για να κάνει εξόρυξη κρυπτονομισμάτων.

- Επίθεση «51%»: Αυτή η επίθεση είναι εφικτή όταν ένα πλήθος ανθρώπων κατέχει το 51% της υπολογιστικής δύναμης όλου του δικτύου. Αυτό είναι σχεδόν απίθανο να συμβεί σε μεγάλα δίκτυα, όμως σε μικρότερα δεν είναι κάτι που δεν έχουμε δει. Όταν συμβεί αυτό η ομάδα των ανθρώπων που κατέχει το 51% μπορεί να εμποδίσει συγκεκριμένες συναλλαγές, ή ακόμη και να αλλάξει πρόσφατες προηγούμενες συναλλαγές.
- Επίθεση «timejack»: Τα μπλοκ έχουν χρονοσφραγίδα. Σε συγκεκριμένες αλυσίδες μπλοκ όπως στην αλυσίδα «Bitcoin» η έννοια του χρόνου βασίζεται στον μέσο χρόνο που έχει το σύνολο των κόμβων του δικτύου. Παραδείγματος χάρη βασίζεσαι στον φίλο σου για να γνωρίζεις τι ώρα είναι. Ας υποθέσουμε ότι ο επιτιθέμενος καταφέρει να βάλει πολλούς κακόβουλους φίλους στην λίστα φίλων σου και στην συνέχεια παραποιεί την πληροφορία που έχουμε ως προς το τι ώρα είναι. Το πρώτο βήμα για την συγκεκριμένη επίθεση, είναι η επίθεση «eclipse» που αναφέραμε νωρίτερα. Στην συνέχεια ο κόμβος που δέχτηκε την επίθεση δεν θα επιβεβαιώσει κανένα μπλοκ από την πραγματική αλυσίδα αφού η σφραγίδα των νέων μπλοκ δεν θα συμβαδίζει χρονικά με την δική του αλυσίδα. Αυτό δίνει την ευκαιρία στον επιτιθέμενο να διπλό ξοδέψει ή να πραγματοποιήσει συναλλαγές με τον κόμβο που δέχτηκε την επίθεση μίας και οι συγκεκριμένες συναλλαγές δεν θα επιβεβαιωθούν ποτέ από το δίκτυο.
- Επίθεση «Finney»: Ο επιτιθέμενος κάνει εξόρυξη ενός μπλοκ με μία συναλλαγή που έχει κάνει ο ίδιος και δεν μεταδίδει το νέο μπλοκ στην αλυσίδα. Με αυτόν τον τρόπο έχει την ευκαιρία να διπλό ξοδέψει το ποσό. Ο επιτιθέμενος κάνει νέα συναλλαγή με το «θύμα». Αν το «θύμα» αποδεχτεί την νέα μη-επιβεβαιωμένη συναλλαγή μπορείς να του μεταβιβάσεις το ποσό του κρυπτονομίσματος που είχες ξοδέψει στην πρώτη συναλλαγή. Στην συνέχεια ο επιτιθέμενος δημοσιεύει το πρώτο μπλοκ το οποίο είχε κρατήσει κρυφό και περιλαμβάνει την έγκυρη συναλλαγή. Έτσι η δεύτερη συναλλαγή δεν πραγματοποιείται ποτέ.
- Επίθεση «race»: Αυτή η επίθεση είναι μία παραλλαγή της επίθεση «Finney». Στην συγκεκριμένη επίθεση ο επιτιθέμενος κάνει ταυτόχρονα δύο συναλλαγές. Η μία δημοσιεύεται στο δίκτυο ενώ η άλλη όχι. Είναι πολύ πιο εύκολο να επιτευχθεί η επίθεση, αν ο επιτιθέμενος είναι άμεσα συνδεδεμένος με τον κόμβο

του «θύματος». Αυτό δίνει την ψευδαίσθηση στο «θύμα» ότι η συναλλαγή του είναι η πρώτη, αλλά ποτέ δεν υποβάλλεται στην αλυσίδα μπλοκ.

4. ΔΗΜΟΦΙΛΗ ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΑ

4.1. Το bitcoin

4.1.1. Το bitcoin Και η Προέλευσή Του

Το bitcoin είναι ένα ψηφιακό νόμισμα που η δημιουργία του φέρεται να είναι το 2008 από κάποιον με το ψευδώνυμο Satoshi Nakamoto. Ο Nakamoto υποστηρίζεται πως είναι γένους αρσενικού, γεννημένος στις πέντε Απριλίου του 1975 και ζει στην Ιαπωνία. Με την εμφάνιση του ηλεκτρονικού νομίσματος το οποίο ήθελε να προωθήσει ο Nakamoto είχε την δυνατότητα να επικοινωνεί συνεχώς με τον κόσμο της τεχνολογίας. Μέσω μηνυμάτων που έχει ανταλλάξει με τον κόσμο που ήρθε σε επαφή μαζί του ο Nakamoto υποστηρίζει πως η αρχή της δημιουργίας του κώδικα του Bitcoin έγινε τον Μάιο του 2007 ενώ κατοχυρώθηκε στην σελίδα του bitcoin.org τον Αύγουστο του 2008. Αρχικά, ξεκίνησε αποστέλλοντας προσωπικά e-mails σε ανθρώπους που θεωρούσε πως θα έβρισκαν ενδιαφέρουσα την ιδέα του ενώ λίγο αργότερα, τον Οκτώβριο του 2008, δημοσίευσε στην ιστοσελίδα metzdowd.com, την έρευνά του για το νέο αυτό ψηφιακό νόμισμα με τίτλο «Bitcoin: A Peer-to-Peer Electronic Cash System». Εν συνεχεία κατέστησε το νέο κώδικα προσιτό για όλους μέσω του διαδικτύου και για τα επόμενα δύο χρόνια παρακολουθούσε τις εξελίξεις του bitcoin, δημοσιεύοντας σε διάφορες ηλεκτρονικές ιστοσελίδες συζητήσεων τις σκέψεις του απαντώντας παράλληλα και σε μηνύματα χρηστών οι οποίοι ήθελαν περισσότερες πληροφορίες για αυτή την καινοτομία, με απώτερο σκοπό να εξαλείψει τις τυχόν ανησυχίες τους. Για το προγραμματιστικό κομμάτι του κώδικα, έκανε διορθώσεις, έχοντάς τον πάντα στην επίβλεψή του ενώ είχε και συνεργασία και με άλλους προγραμματιστές που τον βοηθούσαν να επιλύσει ζητήματα που τυχόν προκύπταν.[24]

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

Η άποψη που υπερισχύει είναι ότι ο άνθρωπος με το ψευδώνυμο, Satoshi Nakamoto είναι άντρας και αυτό λόγω του ότι εκεί παραπέμπει το συγκεκριμένο ψευδώνυμο. Υπάρχει βεβαίως και η ιδέα πως μπορεί να είναι μία ομάδα ειδικών των υπολογιστών και κρυπτογράφων που ζούσαν στην Ευρώπη και στις ΗΠΑ, αλλά αυτό θεωρείται απίθανο από τους περισσότερους που έχουν δραστηριότητα σε αυτόν τον χώρο και αυτό γιατί αν εξετάσουμε το σύνολο των ηλεκτρονικών αλληλεπιδράσεων που υπάρχουν με το συγκεκριμένο ψευδώνυμο και σε συνδυασμό με τα δύο χρόνια που ο Satoshi Nakamoto αφιέρωσε για να απαντά σε ηλεκτρονικά μηνύματα και να διορθώνει τον κώδικα, είναι εξαιρετικά δύσκολο να μπορούν πολλοί άνθρωποι να μοιράζονται λογαριασμούς χρηστών και κωδικούς πρόσβασης και να απαντούν πάντα με παρόμοιο ύφος και φωνή χωρίς να έρχονται σε αντίθεση μεταξύ τους. Σαν εξήγηση λοιπόν, φαίνεται απλούστερη αυτό το τμήμα δραστηριότητας να έγινε μόνο από ένα άτομο, αφού είναι σαφές από τα γραπτά και από τις διορθώσεις στον κώδικα ότι το συγκεκριμένο άτομο είναι εξιδεικευμένο και αντιλαμβάνεται πλήρως τον κώδικα και τις πτυχές σχεδιασμού του Bitcoin. Εν κατακλείδι, ο Satoshi Nakamoto είναι σχεδόν βέβαιο ότι είχε δεχτεί βοήθεια από προγραμματιστές σχετικά με το αρχικό σχέδιο του Bitcoin, αφού μετά την προώθησή του παρατηρούμε ότι δίνει ιδιαίτερη αναφορά σε όλους όσους συνεισέφεραν. [25]

Με βάση την μελέτη του καθώς επίσης και από τις αναφορές του σε πρώιμες εκδόσεις της ιστοσελίδας bitcoin ο Satoshi Nakamoto φαίνεται πως είχε γνώσεις στα ιστορικά στοιχεία του ψηφιακού νομίσματος. Στην μελέτη του, γίνονται αναφορές σε βασικά θεωρήματα της κρυπτογραφίας και της θεωρίας των πιθανοτήτων, καθώς επίσης και στη θεωρία του blockchain. Επιπρόσθετα αναφέρει το hashcash, όπου το υπολογιστικό πάζλ του bitcoin είναι παρόμοιο με αυτό. Αναφέρεται επίσης στο b-money, μετά από προτροπή του Adam Beck, καθώς επίσης μετέπειτα και για το bit-gold, ενώ είχε έρθει πρώτα σε επαφή με τον Wei Dai (δημιουργό του b-money) ο οποίος του συνέστησε να μελετήσει το bit-gold, καθώς ανέφερε και για το σχέδιο του Hal Finney το οποίο κάνει λόγο για την επαναχρησιμοποίηση του του υπολογιστικού παζλ λύσεων. Ως εκ τούτου, όταν ο Satoshi Nakamoto ξεκίνησε να υλοποιεί το όραμά του και να γράφει τον κώδικά του είχε αρκετές πληροφορίες στην διάθεσή του για την κρυπτογραφία και τα πρώτα ψηφιακά νομίσματα. Η περιγραφή που πρότεινε ο ίδιος ο

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

Satoshi Nakamoto για το Bitcoin είναι «*το Bitcoin είναι μια εφαρμογή του σχεδίου b-money του Wei Dai για τους Cypherpunks το 1998 και της πρότασης του Nick Szabo για bit-gold*». Με αυτήν την περιγραφή το Bitcoin τοποθετείται από τον Satoshi Nakamoto ως επέκταση των δύο αυτών ιδεών ή ως μία εφαρμογή των δύο αυτών συστημάτων στις οποίες βασίστηκε και δόμησε το δικό του ψηφιακό νόμισμα.

4.1.2. Το bitcoin Και η Χρησιμότητά Του

Σύμφωνα με την άποψη του Satoshi Nakamoto το εμπόριο στο διαδίκτυο βασίζεται αποκλειστικά σε χρηματοπιστωτικά ιδρύματα τα οποία λειτουργούν ως αξιόπιστα τρίτα μέρη με κύριο σκοπό να επεξεργάζονται ηλεκτρονικές συναλλαγές. Ενώ το σύστημα λειτουργεί αρκετά καλά για τις περισσότερες συναλλαγές, εξακολουθεί να πάσχει από τις έμφυτες αδυναμίες του μοντέλου που βασίζεται στην εμπιστοσύνη. [26] Εξαιτίας αυτού ο ίδιος συνέστησε το bitcoin, έχοντας ως απώτερο σκοπό να εξαλείψει τις αδυναμίες του ηλεκτρονικού εμπορίου, παραθέτοντας το υψηλό κόστος των συναλλαγών μέσω του διαδικτύου, ιδιαίτερα κυρίως για τις συναλλαγές μικρής αξίας. Ο ίδιος στην μελέτη του αναφέρει «*Αυτό που χρειάζεται είναι ένα ηλεκτρονικό σύστημα πληρωμών βασισμένο στην κρυπτογραφική απόδειξη αντί της εμπιστοσύνης, επιτρέποντας σε δυο ενδιαφερόμενα μέρη να πραγματοποιούν συναλλαγές απευθείας μεταξύ τους χωρίς να χρειάζεται κάποιο αξιόπιστο τρίτο μέρος. Συναλλαγές που δεν είναι πρακτικά εφαρμόσιμες για να αντιστραφούν, θα προστατεύσουν τους πωλητές από την απάτη και οι συνήθεις μηχανισμοί μεσεγγύησης θα μπορούσαν εύκολα να εφαρμοστούν για την προστασία των αγοραστών. Σε αυτό το έγγραφο, προτείνουμε μια λύση στο πρόβλημα των διπλών δαπανών χρησιμοποιώντας μια διανεμημένη από ομοτίμους timestamp server για να παράγει υπολογιστική απόδειξη της χρονολογικής σειράς συναλλαγών. Το σύστημα είναι ασφαλές όσο οι ειλικρινείς κόμβοι ελέγχουν συλλογικά*

[26] Satoshi Nakamoto (2008), «*Bitcoin; A Peer-To-Peer Electronic Cash System*», ανακτήθηκε στις 1/9/2019 από τον ιστότοπο https://bitcoin.org/bitcoin.pdf

περισσότερη ισχύ CPU από οποιαδήποτε άλλη συνεργαζόμενη ομάδα κόμβων εισβολέα.»[27]

4.1.3. Το bitcoin Και η Δημοτικότητά Του

Τον Ιούνιο του 2011, με την υπόθεση Wikileaks, ήταν η πρώτη φορά που απασχόλησε περισσότερο το Bitcoin τα μέσα μαζικής ενημέρωσης. Το Wikileaks είναι ένας ιστότοπος που δημοσιεύει πληροφορίες και κυρίως διαρροές ειδήσεων και μυστικές πληροφορίες. Το Wikileaks το 2010, δημοσίευσε σειρά από μυστικά έγγραφα σχετικά με τον πόλεμο στο Αφγανιστάν, υπόθεση που κέντρισε την προσοχή των μέσων μαζικής ενημέρωσης και έβαλε τον συγκεκριμένο ιστότοπο σε αντιπαράθεση με την κυβέρνηση των Ηνωμένων Πολιτειών Αμερικής. Συνέπεια αυτού ήταν το Δεκέμβριο του 2010 ορισμένες τράπεζες και υπηρεσίες πληρωμών αρνήθηκαν να παράσχουν στο Wikileaks τις υπηρεσίες τους, προξενώντας δύσκολο έως και αδύνατο ο ιστότοπος να λάβει συνδρομές και δωρεές από τους υπερασπιστές του. Τότε, τον Ιούνιο του 2011, ο Julian Assange, ιδρυτής του Wikileaks, αποφάσισε να δέχεται δωρεές σε Bitcoin, δίνοντας έμφαση στην ευελιξία του νομίσματος, στην ανωνυμία που παρέχει και στην ανεξαρτησία του από τους παραδοσιακούς χρηματοπιστωτικούς φορείς. [28]

Τα μέσα μαζικής ενημέρωσης ασχολήθηκαν ξανά με το Bitcoin στα τέλη του 2013 διότι η τιμή του αυξήθηκε από τα κάτω 15 δολάρια στις αρχές του 2013 σε πάνω από 1.200 δολάρια στα τέλη Νοεμβρίου του 2013. Παράλληλα το Bitcoin κέρδισε το προβάδισμα στο ηλεκτρονικό εμπόριο με τρανό παράδειγμα την Baidu, κινέζικη μηχανή αναζήτησης που είναι πέμπτη πιο δημοφιλής μηχανή αναζήτησης στον κόσμο, που αποφάσισε τον Οκτώβριο του 2013 να ξεκινήσει να αποδέχεται του Bitcoin για το Jiasule, την εμπορική της υπηρεσία για τη βελτίωση της ασφάλειας και των επιδόσεων των ιστοσελίδων.[29]

---

[27] Satoshi Nakamoto (2008), «*Bitcoin; A Peer-To-Peer Electronic Cash System*», ανακτήθηκε στις 1/9/2019 από τον ιστότοπο https://bitcoin.org/bitcoin.pdf

[28] Halaburda Hanna, Sarvary Miklos (2016), *Beyond Bitcoin; The Economics of Digital Currencies*, Palgrave Macmillan

[29] Halaburda Hanna, Sarvary Miklos (2016), *Beyond Bitcoin; The Economics of Digital Currencies*, Palgrave Macmillan

4.1.4. Απόκτηση bitcoin

Η απόκτηση του Bitcoin μπορεί να γίνει με τρεις βασικούς τρόπους. Ο πρώτος τρόπους είναι πως κάποιος μπορεί να πληρωθεί με το Bitcoin για το προϊόν ή υπηρεσία που προσφέρει έχοντας βέβαια εγκατεστημένο το wallet του, όπου και θα σταλεί και το αντίτιμο που έχει ζητήσει. Πολύ σημαντικό είναι ακόμη να αναφερθεί πως ολοένα και περισσότερες εταιρίες αρχίζουν να δέχονται ως τρόπο πληρωμής τα κρυπτονομίσματα. Ένας δεύτερος τρόπος είναι η αγορά του Bitcoin μέσω των ανταλλακτηρίων ιστοσελίδων που υπάρχουν, όπως το coinbase. Στην συναλλαγή που πραγματοποιείται από μία τέτοια ιστοσελίδα, ο χρήστης θα πρέπει να έχει εγκατεστημένο ένα wallet σε μορφή application στο κινητό του, όπως για παράδειγμα το Copey, πραγματοποιώντας σε αυτήν ένα έμβασμα από κάποιο τραπεζικό λογαριασμό. Η αγορά γίνεται βάσει της τρέχουσας ισοτιμίας του Bitcoin με το νόμισμα που θέλει να ανταλλάξει ένας χρήστης και οφείλει κανείς να ενημερώνεται μέχρι την τελευταία στιγμή πριν προχωρήσει στην αγοραπωλησία, αφού η τιμή του μεταβάλλεται κάθε δευτερόλεπτο. Ο τρίτος τρόπος είναι μέσω της λεγόμενης «εξόρυξης» (mining). Το mining είναι διαδικασία όπου οι χρήστες λύνουν πολυσύνθετα μαθηματικά προβλήματα του συστήματος του Bitcoin και αμείβονται για την δουλειά τους με Bitcoin (την σημερινή εποχή με υποδιαιρέσεις του, λόγω αύξησης της τιμής του). Το Bitcoin mining στην πραγματικότητα προσθέτει νέα Bitcoins στην αγορά, βέβαια βάσει του ανοιχτού κώδικα που δημιούργησε ο Satoshi Nakamoto μέχρι και 21 εκατομμύρια Bitcoins μπορούν να δημιουργηθούν στη διάρκεια της ζωής τους.[30]

[30] *« Bitcoin: Μύθοι, Αλήθειες και μυστικά»* ανακτήθηκε στις 2/9/2019 από τον ιστότοπο http://longreads.news247.gr/bitcoin

4.1.5. Λειτουργία bitcoin

Το σύστημα Bitcoin ξεχωρίζει από τα μέχρι σήμερα τραπεζικά συστήματα λόγω του ότι βασίζεται σε ένα δίκτυο «peer to peer», δεν υπάρχει μία κεντρική αξιόπιστη αρχή για να ελέγχει και να επικυρώνει τις συναλλαγές οι οποίες πραγματοποιούνται. Αντ' αυτού η εμπιστοσύνη επιτυγχάνεται από τις αλληλεπιδράσεις των διαφόρων συμμετεχόντων στο δίκτυο.

Υπάρχουν 3 τρόποι για να συνδεθεί κάποιος με το δίκτυο και να κάνει συναλλαγές,

1. Full Client: Με αυτόν τον τρόπο ο χρήστης έχει τον απόλυτο έλεγχο αφού αποθηκεύει ο ίδιος όλο το ιστορικό των συναλλαγών, έχει δημιουργήσει και διαχειρίζεται το "πορτοφόλι" του και μπορεί να κάνει απευθείας συναλλαγές στο δίκτυο bitcoin χωρίς να υπάρχει κάποιος διαμεσολαβητής.
2. Light Client: Ο χρήσης αποθηκεύει το πορτοφόλι του, αλλά βασίζεται σε διακομιστές τρίτων για να έχει πρόσβαση στο δίκτυο και να κάνει συναλλαγές. Ο χρήστης δεν αποθηκεύει πλήρες αντίγραφο όλων των συναλλαγών, άρα πρέπει να εμπιστευτεί τους "διακομιστές τρίτων" για την επικύρωση της συναλλαγής.
3. Web Client: Ο χρήσης μέσω ενός προγράμματος περιηγητή μπορεί να εισέλθει στον λογαριασμό του και να κάνει συναλλαγές. Το πορτοφόλι του χρήστη είναι εξολοκλήρου αποθηκευμένο σε έναν «διακομιστή τρίτων»

Σε κάθε περίπτωση υπάρχουν πλεονεκτήματα και μειονεκτήματα. Η επιλογή του Client που θα χρησιμοποιηθεί αφορά τις προτιμήσεις του πελάτη.

4.1.5.1. Πορτοφόλι bitcoin (bitcoin wallet)

Το πορτοφόλι (bitcoin wallet) κάθε χρήστη είναι το εργαλείο του για να μπορεί να στέλνει και να λαμβάνει bitcoins. Ένα πορτοφόλι περιλαμβάνει το σύνολο των ιδιωτικών κλειδιών, τα οποία είναι απαραίτητα για την εκτέλεση καθεμίας συναλλαγής. Χρειάζεται μεγάλη προσοχή από τον χρήστη όσον αναφορά την ασφάλειά του, καθώς το πορτοφόλι (bitcoin wallet) έχει την αντίστοιχη αξία και σημασία με ένα συμβατικό πορτοφόλι με μετρητά. [31]

Υπάρχουν διάφορες μορφές πορτοφολιών και η διάκριση γίνεται με βάση τον τρόπο με τον οποίο θέλει ο κάθε χρήστης να έχει πρόσβαση στο πορτοφόλι του. Υπάρχουν τα πορτοφόλια όπου προσφέρονται για χρήση μέσω του ηλεκτρονικού υπολογιστή (desktop wallets) και απευθύνονται σε χρήστες που χρησιμοποιούν τα πιο διαδεδομένα λειτουργικά συστήματα όπως τα windows, mac και linux προσφέροντας υψηλά επίπεδα ασφαλείας και ταχύτητας συναλλαγών. Επιπλέον τα πορτοφόλια όπου προσφέρονται για χρήση μέσω κινητού και tablet (mobile wallets) και είναι πιο εύχρηστα από τα desktop wallets αφού έχεις την δυνατότητα χρήσης των Bitcoins συνεχώς. Υπάρχουν τα hardware wallets, πορτοφόλια υλισμικού, τα οποία είναι τα ασφαλέστερα πορτοφόλια από όλα τα υπόλοιπα καθώς είναι συσκευές ειδικά σχεδιασμένες να λειτουργούν ως πορτοφόλια μη έχοντας την δυνατότητα εγκατάστασης κάποιου επιπλέον λογισμικού στην συσκευή και σε περίπτωση καταστροφής ο χρήστης μπορεί να ανακτήσει τα κεφάλαιά του. Ακόμη μία μορφή πορτοφολιού αποτελούν τα online wallets τα οποία είναι και τα πιο ευάλωτα αφού ο χρήστης μπορεί να έχει πρόσβαση στα κεφάλαιά του από οπουδήποτε αρκεί να μπορεί να συνδεθεί στο διαδίκτυο, απειλούμενος συνεχώς από οποιανδήποτε κακόβουλη ενέργεια. [32]

[31] Bitcoin, *«Διασφαλίζοντας το πορτοφόλι σας»*, ανακτήθηκε στις 14/9/2019 από τον ιστότοπο https://bitcoin.org/el/secure-your-wallet#online

[32] Bitcoin, *«Επιλέξτε το Bitcoin πορτοφόλι σας»*, ανακτήθηκε στις 14/9/2019 από τον ιστότοπο https://bitcoin.org/el/choose-your-wallet?step=1

4.1.5.2. Ψηφιακά Κλειδιά Και Διευθύνσεις

Για να αποδείξει κάποιος ότι είναι κάτοχος Bitcoin απαραίτητο μέσο αποτελούν τα ψηφιακά κλειδιά, οι ψηφιακές υπογραφές και οι διευθύνσεις. Τα ψηφιακά κλειδιά δημιουργούνται από το πορτοφόλι του χρήστη και αποθηκεύονται σε αυτό. Αν στην συσκευή του ο χρήστης έχει εγκαταστήσει κάποιο λογισμικό, τα ψηφιακά κλειδιά αποθηκεύονται στη συσκευή του και εάν ο χρήστης χρησιμοποιεί κάποιο διαδικτυακό πορτοφόλι τα ψηφιακά κλειδιά αποθηκεύονται σε απομακρυσμένους διακομιστές.

Οποιαδήποτε συναλλαγή με bitcoin απαιτεί μια ψηφιακή υπογραφή ώστε η συναλλαγή να συμπεριληφθεί στην αλυσίδα των μπλοκ (Blockchain). Μέσω του ιδιωτικού κλειδιού του χρήστη δημιουργείται η ψηφιακή υπογραφή και πραγματοποιείται από το λογισμικό του πορτοφολιού του χρήστη.

Ένα πορτοφόλι (wallet) περιέχει ζεύγη κλειδιών καθένα από τα οποία αποτελείται από ένα δημόσιο και ένα ιδιωτικό κλειδί. Το ιδιωτικό κλειδί είναι ένας αριθμός τυχαία, συνήθως, δημιουργημένος. Από το ιδιωτικό κλειδί, χρησιμοποιούμε πολλαπλασιασμό ελλειπτικής καμπύλης, μία μονόδρομη κρυπτογραφική συνάρτηση για να δημιουργήσουμε ένα δημόσιο κλειδί.[33]

- Ιδιωτικό κλειδί: γνωστοποιείται στον χρήστη αφού δημιουργήσει το πορτοφόλι του. Αποτελεί το μοναδικό τρόπο να έχει ο χρήστης πρόσβαση στα κεφάλαιά του και είναι πολύ σημαντικό διότι μέσω αυτού δημιουργούνται οι ψηφιακές υπογραφές, οι οποίες απαιτούνται ώστε να αποδειχθεί η κυριότητα των κεφαλαίων που εμπεριέχονται σε οποιαδήποτε συναλλαγή. Το ιδιωτικό κλειδί πρέπει να διατηρείται κρυφό για την ασφάλεια του κάθε χρήστη.
- Δημόσιο κλειδί: δημοσιεύεται από τον εκάστοτε χρήστη που ξοδεύει bitcoin σε κάθε συναλλαγή που κάνει μαζί με μία υπογραφή (σε κάθε συναλλαγή εμφανίζεται διαφορετικό δημόσιο κλειδί το οποίο προκύπτει από το ιδιωτικό κλειδί). Μέσα από αυτήν την διαδικασία οι κόμβοι του δικτύου βλέπουν το κλειδί και επιβεβαιώνουν την συναλλαγή ως έγκυρη, επιβεβαιώνοντας ότι στο άτομο που κάνει την μεταφορά ανήκαν εκείνη τη στιγμή τα bitcoin.

[33] Antonopoulos M. Andreas (2014), *Mastering Bitcoin*, United States of America: O'Reilly Media, Inc.

- Διεύθυνση Bitcoin: αποτελείται από μία σειρά από 26 έως 35 αλφαριθμητικών χαρακτήρων, προκύπτει μέσω των δημόσιων κλειδιών και προορίζεται να διαμοιραστεί από τον κάτοχο σε χρήστες του δικτύου και γι' αυτό το λόγο συχνά αναφέρεται ως «δημόσια» διεύθυνση Bitcoin. Για να γίνει πληρωμή από ένα άτομο με bitcoin, η συναλλαγή μεταδίδεται στο δίκτυο μαζί με μία υπογραφή, το δημόσιο κλειδί του αποστολέα, που επίσης αποτελείται από αλφαριθμητικούς χαρακτήρες διαφόρου μήκους, και την προσωπική διεύθυνση του παραλήπτη. [34]

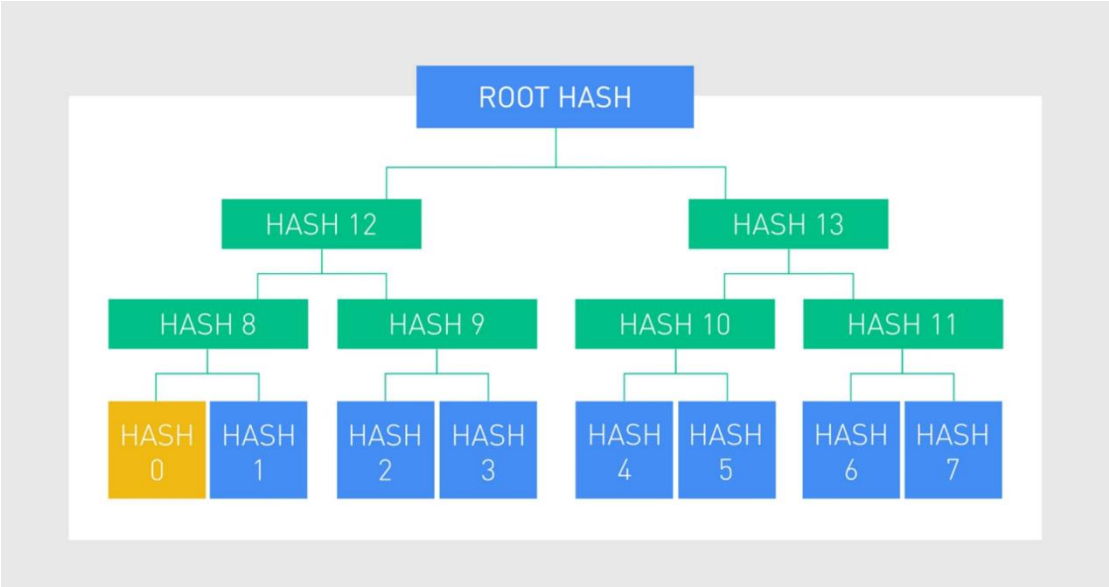
4.1.5.3. Εξόρυξη (Mining)

Εξόρυξη (mining) είναι αν όχι η πιο βασική, μία από τις πιο βασικές, διαδικασίες οι οποίες βοηθούν το δίκτυο bitcoin να είναι αποκεντρωμένο χωρίς να χρειάζεται κάποια κεντρική αρχή να ελέγχει το δίκτυο και τις συναλλαγές. Κατά την εξόρυξη (mining) οι συναλλαγές που πραγματοποιούνται επιβεβαιώνονται και προστίθενται στο δημόσιο βιβλίο συναλλαγών και κατ' επέκταση στην αλυσίδα των μπλοκ. Παράλληλα δημιουργούνται νέα νομίσματα τα οποία τα λαμβάνουν οι εξορύκτες (miners).

Εξορύκτης (miner) είναι ένας κόμβος του δικτύου ο οποίος συλλέγει συναλλαγές και δουλεύει για να τις οργανώσει και να τις κάνει μπλοκ στην αλυσίδα. Κάθε φορά που γίνεται μία συναλλαγή οι εξορύκτες βλέπουν την συναλλαγή στο δίκτυο και είναι δική τους δουλειά να επιβεβαιώσουν ότι είναι έγκυρη. Αφού ολοκληρωθεί η διαδικασία της επιβεβαίωσης η συναλλαγή προστίθεται στην προσωρινή μνήμη με όλες τις υπόλοιπες συναλλαγές που έχουν γίνει πρόσφατα με σκοπό να δημιουργηθεί ένα νέο μπλοκ. Για να φτάσουμε στο νέο μπλοκ, η πρώτη διαδικασία που υλοποιείται είναι η κρυπτογράφηση όλων των συναλλαγών στην πρόσφατη μνήμη. Ο εξορύκτης δημιουργεί μία συναλλαγή κατά την οποία λαμβάνει ο ίδιος την αμοιβή του δικτύου για την δημιουργία του νέου μπλοκ (coinbase transaction) και στην συνέχεια κρυπτογραφεί όλες τις συναλλαγές οι οποίες είναι στην προσωρινή μνήμη, με την χρήση του αλγόριθμου κατακερματισμού (hash). Αφού

[34] Halaburda Hanna, Sarvary Miklos (2016), *Beyond Bitcoin; The Economics of Digital Currencies*, Palgrave Macmillan

κρυπτογραφηθούν οι συναλλαγές στην συνέχεια οργανώνονται σε «Merkel Tree», ή «Hash Tree», δηλαδή οργανώνονται σε ζευγάρια και στην συνέχεια και χρησιμοποιείται εκ νέου ο αλγόριθμος κατακερματισμού (hash). Αυτό επαναλαμβάνεται μέχρι να φτάσουμε σε ένα και μοναδικό αποτέλεσμα (root hash).



Διάγραμμα 3: Σχηματική απεικόνιση του «Merkel Tree». [35]

Το μοναδικό αποτέλεσμα που βρήκαμε παραπάνω, μαζί με τον αριθμό κατακερματισμού του προηγούμενου μπλοκ και τον τυχαίο αριθμό «nonce» μπαίνουν στην κεφαλίδα του νέο μπλοκ. Στην συνέχεια χρησιμοποιείται εκ νέου ο αλγόριθμος κατακερματισμού στην κεφαλίδα του μπλοκ, ο οποίος μας δίνει έναν αριθμό ο οποίος πλέον ονομάζεται «αριθμός αναγνώρισης του μπλοκ». Ο «αριθμός αναγνώρισης του μπλοκ» πρέπει να είναι μικρότερος από μία συγκεκριμένη τιμή που έχει οριστεί από το πρωτόκολλο του δικτύου. Για να πετύχουν αυτήν την τιμή, οι εξορύκτες στο δίκτυο αλλάζουν τον τυχαίο αριθμό «nonce», και στην συνέχεια χρησιμοποιούν εκ νέου τον αλγόριθμο κατακερματισμού μέχρι κάποιος εξορύκτης να έχει έναν έγκυρο «αριθμό αναγνώρισης του μπλοκ». Μόλις ο εξορύκτης δημιουργήσει το νέο μπλοκ, θα το διαμοιράσει στο δίκτυο. Οι υπόλοιποι εξορύκτες θα δουν, θα επιβεβαιώσουν το νέο μπλοκ, θα το προσθέσουν στο αντίγραφο της αλυσίδας που κατέχουν οι ίδιοι και θα προχωρήσουν στην εξόρυξη του επόμενου μπλοκ. Σπάνια βέβαια, υπάρχει η περίπτωση δύο εξορύκτες να διαμοιράσουν ένα έγκυρο μπλοκ, την ίδια στιγμή. Σε αυτήν την περίπτωση δημιουργείται μία διακλάδωση στο δίκτυο της αλυσίδας μπλοκ γνωστό και

[35] Η εικόνα ανακτήθηκε από το βίντεο https://www.youtube.com/watch?v=2VtH-XAOjXw με τίτλο «what is cryptocurrency mining?» στις 27/10/2019

ως «Mining Fork» το οποίο θα αναλύσουμε αργότερα. Η πιθανότητα που έχει ένας κόμβος να δημιουργήσει το επόμενο μπλοκ και να λάβει την ανταμοιβή για αυτό, είναι άμεσα συνδεδεμένη με το ποσοστό της επεξεργαστικής δύναμης το οποίο κατέχει. Εξορύκτες με μικρή υπολογιστική δύναμη είναι σχεδόν αδύνατο να βρουν το επόμενο μπλοκ μόνοι τους. Γι' αυτόν τον λόγο δημιουργήθηκαν τα λεγόμενα «mining pools», τα οποία είναι δίκτυα μεταξύ εξορυκτών οι οποίοι ενώνουν την επεργαστική τους δύναμη, για την εύρεση του επόμενου μπλοκ και διαμοιράζονται τα κέρδη ανάλογα με το πόσο έχει προσφέρει ο καθένας στην δημιουργία αυτού του μπλοκ.

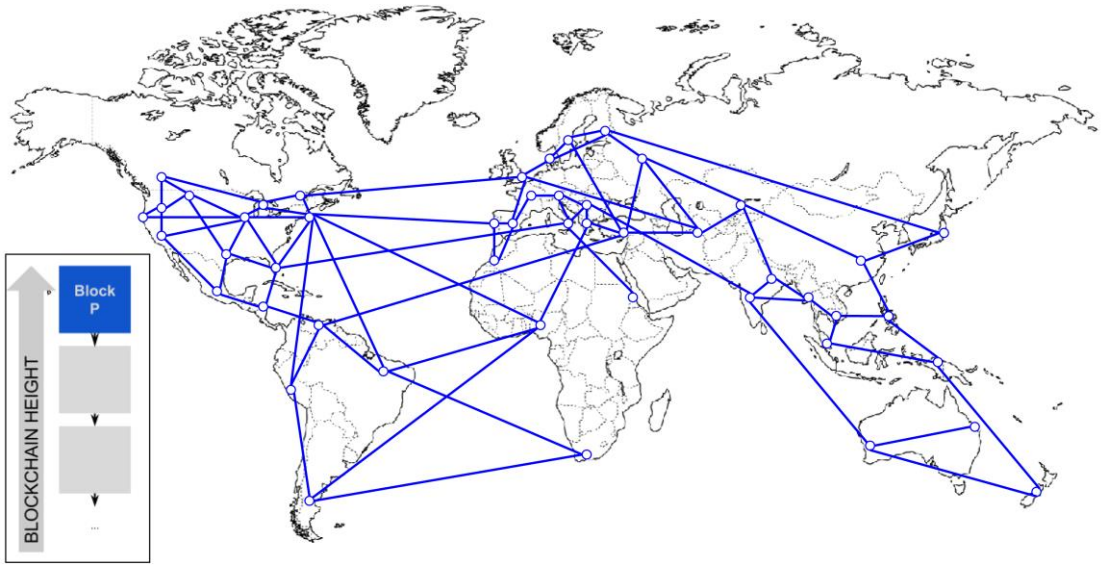
4.1.5.4. Διακλάδωση- Mining Forks[36]

Καθώς θα γίνεται εξόρυξη για τον σχηματισμό νέων μπλοκ, προσωρινά θα υπάρχουν πολλά νέα εν δυνάμει μπλοκ τα οποία ονομάζονται «παιδικά». Κάθε «παιδικό» μπλοκ θα έχει τον ίδιο αριθμό κατακερματισμού προηγούμενου μπλοκ, στο τέλος όμως μόνο ένα από τα «παιδικά» θα επιβεβαιωθεί και θα προστεθεί στην αλυσίδα των μπλοκ. Σπάνια μπορεί να λυθούν δύο μπλοκ ταυτόχρονα, και σε αυτήν την περίπτωση δημιουργείται μία διακλάδωση και το δίκτυο χωρίζεται σε δύο επιμέρους δίκτυα προσωρινά με σκοπό την επίλυση του νέου μπλοκ.

Κάθε κόμβος λαμβάνει και στέλνει πληροφορίες ταυτόχρονα, επειδή όμως η αλυσίδα των μπλοκ είναι αποκεντρωμένη, μπορεί διαφορετικά μπλοκ να φτάσουν σε διαφορετικό κόμβο. Κάθε κόμβος πάντα επιλέγει να κρατήσει προσωρινά την μεγαλύτερη αλυσίδα μπλοκ μέχρι που προστίθεται ένα νέο μπλοκ σε μία από τις διακλαδώσεις και έτσι τελικά επιλύεται η διακλάδωση.

[36] Antonopoulos M. Andreas (2014), Mastering Bitcoin, United States of America: O'Reilly Media, Inc.

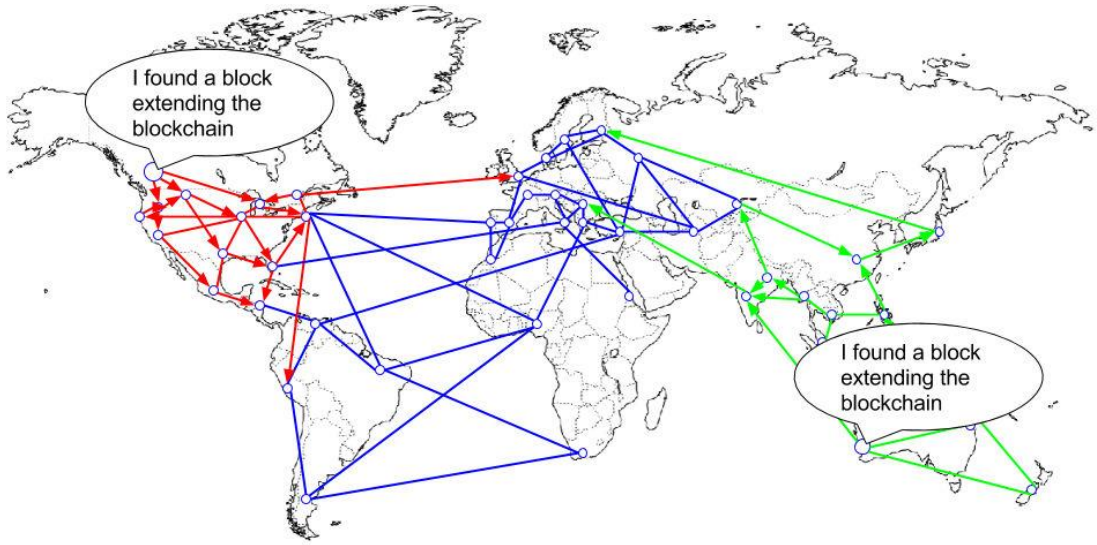
Παράδειγμα διακλάδωσης μπλοκ



Διάγραμμα 4: Αλυσίδα μπλοκ, ακριβώς πριν την διακλάδωση [37]

Παραπάνω βλέπουμε μία αλυσίδα μπλοκ πριν την διακλάδωση. Η διακλάδωση συμβαίνει όταν δύο εξορύκτες βρίσκουν την λύση για το αντίστοιχο μπλοκ, και ταυτόχρονα το διαδίδουν στους κόμβους του δικτύου οι οποίοι στην συνέχεια το αναμεταδίνουν στους υπόλοιπους κόμβους. Κάθε κόμβος που λαμβάνει το έγκυρο μπλοκ το ενσωματώνει στην αλυσίδα. Στην συνέχεια οι ίδιοι κόμβοι θα δουν το δεύτερο υποψήφιο μπλοκ, το οποίο έχει το ίδιο μητρικό και το προσθέτουν σε μία δευτερεύουσα αλυσίδα. Στο σημείο αυτό βλέπουμε ότι κάποιοι κόμβοι θα δουν το μπλοκ Α ως κύριο και κάποιοι άλλοι το μπλοκ Β.

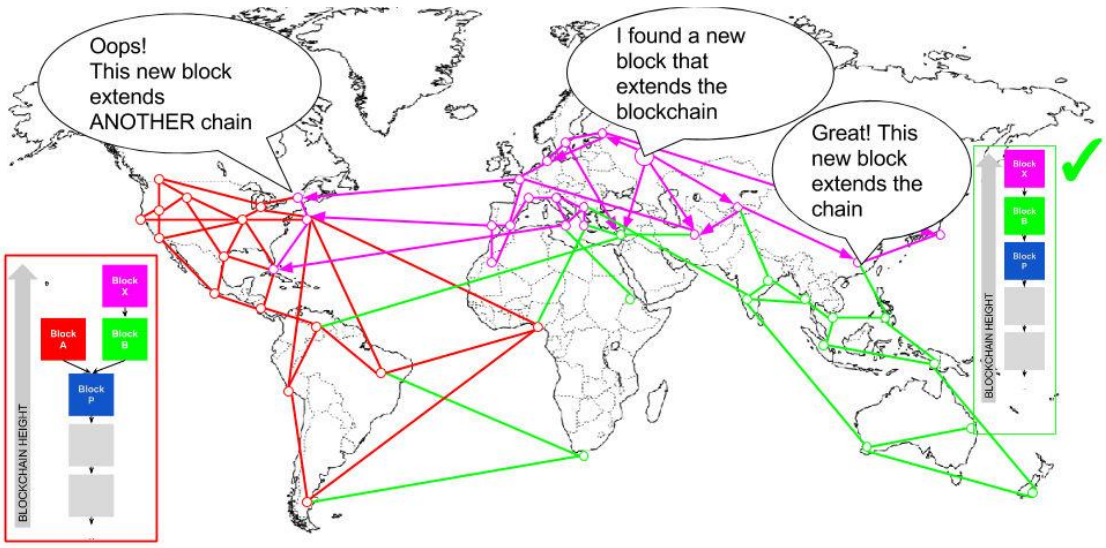
[37] Antonopoulos M. Andreas (2014), *Mastering Bitcoin*, United States of America: O'Reilly Media, Inc.



Διάγραμμα 5: Απεικόνιση της διακλάδωσης – ταυτόχρονη εξόρυξη δύο μπλοκ[38]

Σε αυτό το σημείο υπάρχουν δύο υποψήφια μπλοκ, το κόκκινο και το πράσινο. Τα δύο μπλοκ συμπεριλαμβάνουν ένα μεγάλο ποσοστό των ίδιων συναλλαγών, με ελάχιστες διαφορετικές συναλλαγές. Στο σημείο αυτό οι εξορύκτες που είδαν το κόκκινο μπλοκ ως πρώτο στην σειρά ξεκινούν να εργάζονται για την επίλυση του επόμενου μπλοκ χρησιμοποιώντας ως μητρικό το κόκκινο μπλοκ, και αντίστοιχα οι εξορύκτες που είδαν το πράσινο μπλοκ ως πρώτο στην σειρά, ξεκινούν να εργάζονται για την επίλυση του επόμενου μπλοκ χρησιμοποιώντας ως μητρικό το πράσινο μπλοκ. Ακόμα και αν το δίκτυο και η υπολογιστική δύναμη των εξορυκτών χωριστεί στην μέση μία ομάδα θα βρει την λύση για το επόμενο μπλοκ νωρίτερα από την άλλη. Για παράδειγμα αν οι εξορύκτες του πράσινου μπλοκ επιλύσουν ένα καινούριο «ροζ» μπλοκ το οποίο μεγαλώνει την αλυσίδα, αμέσως διαμοιράζουν το νέο μπλοκ και όλο το δίκτυο το βλέπει ως την πλέον έγκυρη αλυσίδα μπλοκ.

[38] Antonopoulos M. Andreas (2014), *Mastering Bitcoin*, United States of America: O'Reilly Media, Inc.



Διάγραμμα 6: Σημείο επίλυσης της διακλάδωσης[39]

Στο σημείο αυτό οι εξορύκτες ενημερώνουν τους κόμβους για το νέο μπλοκ και έγκυρη αλυσίδα θεωρείται η μεγαλύτερη, δηλαδή η αλυσίδα η οποία περιλαμβάνει το μπλοκ μπλε-πράσινο-ροζ. Οι κόμβοι που είχαν ως βασική αλυσίδα την μπλε-κόκκινη θα διορθώσουν την αλυσίδα των μπλοκ με την πλέον έγκυρη (μπλε-πράσινο-ροζ). Όσοι εξορύκτες δούλευαν στην επίλυση του επόμενου μπλοκ της αλυσίδας μπλε-κόκκινο θα σταματήσουν, γιατί το επόμενο μπλοκ θα είναι «ορφανό», δεν επιβεβαιώνεται, μιας και το μητρικό μπλοκ δεν είναι πλέον στην μεγαλύτερη αλυσίδα μπλοκ. Οι συναλλαγές του κόκκινου μπλοκ είναι στην αναμονή και θα επεξεργαστούν και θα προστεθούν στην εξόρυξη του επόμενου μπλοκ.

4.2. Alternative Coins (AltCoins)

Πέρα από τα Bitcoin, έχουν ξεκινήσει να εμφανίζονται και να εδραιώνονται στο χώρο της οικονομίας και της τεχνολογίας και νέα κρυπτονομίσματα τα οποία έχουν και τα δικά τους ιδιαίτερα χαρακτηριστικά. Βέβαια σε κάποιες περιπτώσεις τα καινούρια

[39] Antonopoulos M. Andreas (2014), *Mastering Bitcoin*, United States of America: O'Reilly Media, Inc.

κρυπτονομίσματα αποτελούν απλά μία απομίμηση και παραλλαγή των αρχικών ψηφιακών νομισμάτων χωρίς πραγματικές βελτιώσεις. [40]

Το σύνολο των νέων αυτών ανταγωνιστικών κρυπτονομισμάτων ονομάζεται AltCoins και η δημιουργία τους οφείλεται στην επιτυχία του Bitcoin αλλά και στην ανοικτή φύση του λογισμικού του, κατά την οποία πολλοί προγραμματιστές μπορούν να πειραματιστούν με τον κώδικα και να τον τροποποιήσουν. Αποτέλεσμα ήταν να δημιουργηθεί μια νέα ποικιλία κρυπτονομισμάτων με κύριο στόχο την βελτιστοποίηση του ήδη υπάρχων κώδικα και την προσθήκη νέων λειτουργιών και δυνατοτήτων, όπως οι ταχύτερες συναλλαγές και η μεγαλύτερη ανωνυμία.[41]Από έρευνες που έχουν γίνει προκύπτει πως το Bitcoin, είναι ένα από τα εκατοντάδες κρυπτονομίσματα που υπάρχουν στον κόσμο, αφού από τον Μάιο του 2018 πάνω από 1500 κρυπτονομίσματα έχουν τεθεί σε κυκλοφορία τα οποία μάλιστα είναι παραλλαγές ή βελτιώσεις του Bitcoin και βασίζεται σε πολύ μεγάλο βαθμό σε καινοτομίες και ιδέες που εισήγαγε αυτό.[42]

4.2.1. Ethereum

Ένα από τα κρυπτονομίσματα τα οποία θεωρείται το μέλλον από όλο τον κόσμο και αυτόν του διαδικτύου, είναι το Ethereum. Δημιουργήθηκε και κυκλοφόρησε το 2015 από τον Vitalik Buterin, ο οποίος κατάφερε το συγκεκριμένο κρυπτονόμισμα να λειτουργεί ως μία αποκεντρωμένη πλατφόρμα λογισμικού η οποία καθιστά δυνατή την κατασκευή smart contracts και τη δημιουργία και χρήση κατανεμημένων εφαρμογών (DApps) χωρίς διακοπές, ελέγχους, απάτες ή παρεμβολές από τρίτους. Το Ethereum

[40] Frankenfield,Jake(2018*), VirtualCurrency*, ανακτήθηκε στις 14/9/2019 από τον ιστότοπο: https://www.investopedia.com/terms/v/virtual-currency.asp

[41] Finley, Klint (2018)., *After 10 years, Bitcoin has changed everything and nothing*, ανακτήθηκε στις 14/9/2019 από τον ιστότοπο: https://www.wired.com/story/after-10-years-bitcoin-changed-everything-nothing/

[42] Frankenfield, Jake(2014). *Altcoin*. ανακτήθηκε στις 14/9/2019 από τον ιστότοπο: https://www.investopedia.com/terms/a/altcoin.asp

δηλώνεται πως «μπορεί να χρησιμοποιηθεί για την κωδικοποίηση, αποκέντρωση, ασφάλεια και εμπορία για σχεδόν οτιδήποτε».[43]

Ο όρος smart contracts ή αλλιώς έξυπνες συμβάσεις, προβάλει ένα νέο πρωτόκολλο το οποίο διευκολύνει ψηφιακά την επιβολή ή την επαλήθευση μιας διαπραγμάτευσης καθώς και την εκτέλεση μίας σύμβασης. Επιτρέπουν την εκτέλεση αξιόπιστων συναλλαγών χωρίς μεσολαβητές και καθιστούν συναλλαγές ανιχνεύσιμες, διαφανείς και μη αναστρέψιμες. [44]

Το Ethereum έχει επίσης το πλεονέκτημα να επιτρέπει την χρήση blockchain από άλλους προγραμματιστές για την κατασκευή αποκεντρωμένων εφαρμογών, γνωστές και ως Dapps.[45]Η γλώσσα προγραμματισμού του Ethereum ονομάζεται Solidity. Ωστόσο, για να αναπτυχθεί κάποια εφαρμογή και για να μπορέσει το δίκτυο να την φιλοξενήσει πρέπει να πληρωθεί ένα αντίτιμο είτε με κάποιο ανταλλακτικό νόμισμα, είτε με το νόμισμα του Ethereum το οποίο ονομάζεται ether.

Το ether μπορεί να χρησιμοποιηθεί ως κρυπτονόμισμα για ανταλλαγή ή για να εκτελέσει εφαρμογές στο εσωτερικό του δικτύου και για την αποκόμιση κέρδους από εργασίες. [46]Ενας προγραμματιστής εφαρμογών, θα πρέπει να πληρώνει τα τέλη φιλοξενίας της εφαρμογής του στο δίκτυο με ether, αλλά και η δική του πληρωμή θα πρέπει να γίνεται αντίστοιχα με το ίδιο κρυπτονόμισμα. Βέβαια η απόκτηση των ether νομισμάτων μπορεί να συμβεί ακόμη αν οι χρήστες συμμετέχουν σε διαδικασίες εξόρυξης και επαλήθευσης συναλλαγών, κατά τις οποίες ανταμείβονται για τους πόρους τους οποίους διαθέτουν στο δίκτυο με αποτέλεσμα να διατηρούν ευέλικτο και λειτουργικό το δίκτυο του Ethereum. [47]

---

[43] Bajpai, Prableen(2017). *The 10 most important cryptocurrencies other than Bitcoin.,* ανακτήθηκε στις 14/9/2019 από τον ιστότοπο: https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin/
Frankenfield, Jake(2016). *Ethereum*. ανακτήθηκε στις 14/9/2019 από τον ιστότοπο: https://www.investopedia.com/terms/e/ethereum.asp

[44] Shobhit, Seth(2018). *All about Ethereum*. ανακτήθηκε στις 14/9/2019 από τον ιστότοπο: https://www.investopedia.com/tech/all-about-ethereum/

[45] Bajpai, Prableen(2017). *The 10 most important cryptocurrencies other than Bitcoin.,* ανακτήθηκε στις 14/9/2019 από τον ιστότοπο: https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin/

[46] Frankenfield, Jake(2016). *Ethereum*. ανακτήθηκε στις 14/9/2019 από τον ιστότοπο: https://www.investopedia.com/terms/e/ethereum.asp

[47] Shobhit, Seth(2018). *All about Ethereum*. ανακτήθηκε στις 14/9/2019 από τον ιστότοπο: https://www.investopedia.com/tech/all-about-ethereum/

Το ether χρησιμοποιείται για να πληρώσει ο κάθε χρήστης την εκτέλεση μιας εφαρμογής ή ενός προγράμματος ανάλογα με την ενέργεια και τον χρόνο που απαιτείται για να εκτελεστεί αυτό. Η πληρωμή ενός ποσού για οποιαδήποτε ενέργεια πραγματοποιείται μέσα στο σύστημα και η απόκτηση ενός ether είναι πολύ πιο γρήγορη σε σύγκριση με την απόκτηση ενός bitcoin, διότι το ether αποκτάται σε χρονικό διάστημα 14 ή 15 δευτερολέπτων ενώ το bitcoin σε διάστημα 10 λεπτών, γεγονός το οποίο σημαίνει την κυκλοφορία περισσοτέρων ether νομισμάτων από ότι bitcoin.[48] Συγκεκριμένα, 18 εκατομμύρια ethers δημιουργούνται ετησίως με 5 ethers να δημιουργούνται περίπου κάθε 12 δευτερόλεπτα. Φαίνεται λοιπόν, πως οι κανόνες του Ethereum για την οικονομία είναι πιο ανοικτοί και δεν διαθέτουν όριο νομισμάτων που θα τεθούν σε κυκλοφορία.[49]

Το Ethereum δημιουργήθηκε για να προσφέρει στους χρήστες του την ευχέρεια να κατασκευάζουν αποκεντρωμένες εφαρμογές στο δίκτυό του. Πολλές επιχειρήσεις θέλουν να υλοποιήσουν τα σχέδιά τους μέσα στο δίκτυο του Ethereum και αξιοσημείωτη είναι η συνεργασία του Ethereum με τη Microsoft η οποία προσφέρει το Ethereum blockchain ως υπηρεσία στο Microsoft Azure (EBaaS) έτσι ώστε οι προγραμματιστές και οι χρήστες να έχουν την δυνατότητα με το πάτημα ενός κουμπιού ένα cloud- based blockchain προγραμματιστικό περιβάλλον.[50] Θεωρείται πως το Ethereum έχει δυνατότητα να χρησιμοποιηθεί σε αποκεντρωμένες οργανώσεις, χρηματιστηριακές αγορές, διαδικτυακά τυχερά παιχνίδια, στοιχήματα ακόμη και σε ασφαλιστικές βιομηχανίες. Το Ethereum ωστόσο αντιμετωπίζει και αυτό προβλήματα κλιμάκωσης, όπως και το Bitcoin, λόγω του μεγέθους της χωρητικότητας των συναλλαγών καθώς υπάρχουν και άλλες πλατφόρμες οι οποίες δημιουργούν παρόμοια τεχνολογία και είναι πιο απλές στην χρήση, γεγονός που ασκεί πίεση στο Ethereum.[51]

Οι Αποκεντρωμένες Αυτόνομες Οργανώσεις γνωστές και ως DAO, δημιουργήθηκαν με την χρήση του Ethereum και στόχος τους είναι η λειτουργία μιας

---

[48] Frankenfield, Jake(2016). *Ethereum*. ανακτήθηκε στις 14/9/2019 από τον ιστότοπο: https://www.investopedia.com/terms/e/ethereum.asp

[49] Hertig, Alyssa and Palmer, Daniel (2017). *What is ether?* ανακτήθηκε στις 14/9/2019 από τον ιστότοπο: https://www.coindesk.com/information/what-is-ether-ethereum-cryptocurrency

[50] Frankenfield, Jake(2016). *Ethereum*. ανακτήθηκε στις 14/9/2019 από τον ιστότοπο: https://www.investopedia.com/terms/e/ethereum.asp

[51] Bajpai, Prableen(2017). *The 10 most important cryptocurrencies other than Bitcoin.,* ανακτήθηκε στις 14/9/2019 από τον ιστότοπο: https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin/

εταιρίας χωρίς ηγέτες. Έτσι για να το επιτύχουν αυτό, χρησιμοποιούν έναν συνδυασμό smart contracts και αλλάζουν την δομή και τους κανόνες του Ethereum.[52] Το 2016, ένα έργο DAO με τίτλο «The DAO» συγκέντρωσε επιτυχώς 150 εκατομμύρια δολάρια μέσα από την πώληση smart contracts και τον Ιουνίου του ιδίου έτους μπήκε στο στόχαστρο ενός χάκερ ο οποίος κατάφερε να υποκλέψει το 1/3 των ethers τα οποία ισοδυναμούσαν εκείνο το διάστημα σε 50 εκατομμύρια δολάρια. Αν και ανακτήθηκαν ethers αντιστοιχίας 48 εκατομμύριων δολαρίων το πλήγμα ήταν τεράστιο τόσο για το DAO όσο και για το Ethereum του οποίου η συναλλαγματική αξία κατρακύλησε. Παρόλο που δεν υπήρχαν προβλήματα στο δίκτυο του Ethereum, μετά από αυτήν την επίθεση το Ethereum χωρίστηκε σε δυο κρυπτονομίσματα, στο Ethereum, όπως είναι γνωστό σήμερα με αλλαγές στην ασφάλεια για παρόμοιες τέτοιες επιθέσεις κακόβουλων λογισμικών και το Ethereum Classic. [53]

4.2.2. Ripple- XRP

Το ripple ή αλλιώς γνωστό και ως XRP είναι μία τεχνολογία η οποία διαθέτει δύο διαφορετικές ιδιότητες, η πρώτη ιδιότητά του είναι πως χρησιμοποιείται ως ψηφιακό νόμισμα με την ονομασία XRP και η άλλη ιδιότητά του είναι πως πρόκειται για ένα πρωτόκολλο πληρωμών για χρηματοπιστωτικές συναλλαγές.[54] Το συγκεκριμένο νομισματικό σύστημα δημιουργήθηκε και προορίζεται ώστε να χρησιμοποιηθεί σε πραγματικό χρόνο από τις τράπεζες και τους παρόχους πληρωμών για άμεσες διασυνοριακές πληρωμές, με χαμηλά τέλη και υψηλή ασφάλεια. Ξεκινώντας από το

---

[52] Shobhit, Seth(2018). *All about Ethereum*. ανακτήθηκε στις 14/9/2019 από τον ιστότοπο: https://www.investopedia.com/tech/all-about-ethereum/

[53] Μπάλας, Φώτης (2016). *Τα πιο σημαντικά, εναλλακτικά του Bitcoin, Ψηφιακά νομίσματα.,* ανακτήθηκε στις 14/9/2019 από τον ιστότοπο: https://www.pcsteps.gr/107937-%CF%88%CE%B7%CF%86%CE%B9%CE%B1%CE%BA%CE%AC-%CE%BD%CE%BF%CE%BC%CE%AF%CF%83%CE%BC%CE%B1%CF%84%CE%B1-%CE%B5%CE%BD%CE%B1%CE%BB%CE%BB%CE%B1%CE%BA%CF%84%CE%B9%CE%BA%CE%AC-%CF%84%CE%BF%CF%85-bitcoin/

[54] Μπάλας, Φώτης (2016). *Τα πιο σημαντικά, εναλλακτικά του Bitcoin, Ψηφιακά νομίσματα.,* ανακτήθηκε στις 14/9/2019 από τον ιστότοπο: https://www.pcsteps.gr/107937-%CF%88%CE%B7%CF%86%CE%B9%CE%B1%CE%BA%CE%AC-%CE%BD%CE%BF%CE%BC%CE%AF%CF%83%CE%BC%CE%B1%CF%84%CE%B1-%CE%B5%CE%BD%CE%B1%CE%BB%CE%BB%CE%B1%CE%BA%CF%84%CE%B9%CE%BA%CE%AC-%CF%84%CE%BF%CF%85-bitcoin/

2012, το Ripple *«επιτρέπει στις τράπεζες να διακανονίζουν διασυνοριακές πληρωμές σε πραγματικό χρόνο, με διαφάνεια και χαμηλό κόστος»*. [55]

Το Ripple κυκλοφόρησε το 2012 και δημιουργοί του είναι οι Chris Larsen και Jed McCalab. Η πιο διαδεδομένη ιδιότητά του φαίνεται να είναι αυτή του πρωτόκολλου ψηφιακής πληρωμής παρά του κρυπτονομίσματος. Το πρωτόκολλο ξεχωρίζει από το Bitcoin αλλά και από πολλά άλλα AltCoins διότι δεν λειτουργεί με αλγόριθμους Proof of Work ή Proof of Stake και δεν υποστηρίζει την διαδικασία της εξόρυξης ως τρόπο επιβεβαίωσης των συναλλαγών. [56]Το Ripple βασίζεται σε δίκτυα εμπιστοσύνης χρησιμοποιώντας έναν αλγόριθμο ομοφωνίας μεταξύ των μελών του δικτύου προκειμένου να επικυρωθούν τα υπόλοιπα των λογαριασμών και οι συναλλαγές του συστήματος. Με αυτόν τον τρόπο παρεμποδίζονται οι διπλές δαπάνες και επιτυγχάνεται η βελτίωση της ακεραιότητας του συστήματος.[57]

Το Ripple ως σύστημα πληρωμών λειτουργεί σε μία αποκεντρωμένη πλατφόρμα peer-to-peer ανοικτού κώδικα και επιτρέπει την μεταφορά χρημάτων σε οποιαδήποτε μορφή χωρίς να κάνει διακρίσεις μεταξύ παραστατικών νομισμάτων και κρυπτονομισμάτων. Με αυτόν τον τρόπο καθιστά ευκολότερη την ανταλλαγή οποιουδήποτε νομίσματος με άλλο νόμισμα. Οι συναλλαγές λοιπόν, επιτυγχάνονται στο συγκεκριμένο σύστημα με τρόπο τέτοιο όπου οι χρήστες διασυνδέονται με άλλους χρήστες τους οποίους εμπιστεύονται και μέσω της δημιουργίας αλυσίδων με τους έμπιστους χρήστες αποστέλλουν χρήματα για πληρωμές. Αυτές οι αλυσίδες δημιουργούνται χρησιμοποιώντας ως μέσο γνωστό ως Gateway το οποίο χρησιμεύει ως σύνδεσμος εμπιστοσύνης ανάμεσα στα δύο μέρη που επιθυμούν να πραγματοποιήσουν μία συναλλαγή και διαρκούν μέχρι τα χρήματα να φθάσουν στον

---

[55] Bajpai, Prableen(2017). *The 10 most important cryptocurrencies other than Bitcoin.,* ανακτήθηκε στις 14/9/2019 από τον ιστότοπο: https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin/

[56] Bajpai, Prableen(2017). *The 10 most important cryptocurrencies other than Bitcoin.,* ανακτήθηκε στις 14/9/2019 από τον ιστότοπο: https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin/

Μπάλας, Φώτης (2016). *Τα πιο σημαντικά, εναλλακτικά του Bitcoin, Ψηφιακά νομίσματα.,* ανακτήθηκε στις 14/9/2019 από τον ιστότοπο: https://www.pcsteps.gr/107937-%CF%88%CE%B7%CF%86%CE%B9%CE%B1%CE%BA%CE%AC-%CE%BD%CE%BF%CE%BC%CE%AF%CF%83%CE%BC%CE%B1%CF%84%CE%B1-%CE%B5%CE%BD%CE%B1%CE%BB%CE%BB%CE%B1%CE%BA%CF%84%CE%B9%CE%BA%CE%AC-%CF%84%CE%BF%CF%85-bitcoin/

[57] Wikoff, Shawn (2016). *The expert Shawn Wikoff talks about Electronic money.,* ανακτήθηκε στις 14/9/2019 από τον ιστότοπο: https://medium.com/@wikoff.shawn/the-expert-shawn-wikoff-talks-about-electronic-money-d01964dd669c

επιθυμητό παραλήπτη. Η ασφάλεια του δικτύου βέβαια είναι διαφορετική σε σχέση με τα άλλα κρυπτονομίσματα, αφού εδώ το ιστορικό συναλλαγών είναι δημόσιο και έτσι οι πληροφορίες παραμένουν ευάλωτες στο θέμα γνωστοποίησης και ταυτοποίησης των χρηστών.[58]

Το XRP στη σημερινή εποχή έχει πολλούς υποστηρικτές οι οποίοι πιστεύουν πως δεν πρέπει πλέον να θεωρείται αποκεντρωμένο κρυπτονόμισμα, αφού η ίδια η εταιρεία διαθέτει πάνω από το 50% όλων των XRP νομισμάτων και κατέχει ακόμη την πλειοψηφία των κόμβων επικύρωσης στο δίκτυο. [59] Τον Ιούνιο του 2017, ήταν το τρίτο μεγαλύτερο κρυπτονόμισμα με αξία 11,94 δισεκατομμύρια δολάρια μετά το Bitcoin που είχε 45,26 δισεκατομμύρια δολάρια και το Ethereum με αξία 31,53 δισεκατομμύρια δολάρια. Τον Οκτώβριο του 2018, είχε 20,07 δισεκατομμύρια δολάρια,[60]και στις αρχές του 2019 η τιμή του έπεσε στα 0,311 δολάρια Αμερικής. Το μόνο σίγουρο είναι πως το Ripple δεν μπορεί να μπει στην ίδια κατηγορία του Bitcoin και Ethereum και θα πρέπει να αποδείξει πως είναι αξιόπιστη πλατφόρμα για διεθνείς πληρωμές.[61]

[58] Reiff, Nathan (2017). *Could cryptocurrencies replace cash?.,* ανακτήθηκε στις 14/9/2019 από τον ιστότοπο:https://www.investopedia.com/news/could-cryptocurrencies-replace-cash-bitcoin-flippening/

[59]Dossis Luc, *The top 10 cryptos explained.,* ανακτήθηκε στις 14/9/2019 από τον ιστότοπο: https://blog.goodaudience.com/the-top-10-cryptos-explained-85cddbe4f281

[60] Bajpai, Prableen(2017). *The 10 most important cryptocurrencies other than Bitcoin.,* ανακτήθηκε στις 14/9/2019 από τον ιστότοπο: https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin/

[61] Dossis Luc, *The top 10 cryptos explained.,* ανακτήθηκε στις 14/9/2019 από τον ιστότοπο: https://blog.goodaudience.com/the-top-10-cryptos-explained-85cddbe4f281

5. ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΑ ΚΑΙ ΚΙΝΔΥΝΟΙ ΚΥΒΕΡΝΟΧΩΡΟΥ

Στα προηγούμενα κεφάλαια αναλύσαμε την λειτουργία των Κρυπτονομισμάτων σε μία προσπάθεια να γίνουν πλήρως κατανοητά. Στο παρών κεφάλαιο θα εστιάσουμε σε έναν πολύ σημαντικό παράγοντα, τους τεχνολογικούς κινδύνους που έρχονται με την χρήση των κρυπτονομισμάτων και θα δούμε τι μας έχει διδάξει η ιστορία.

5.1. Η Περίπτωση Της Quadriga CX (Key Man Risk)[62]

Το «ρίσκο του ατόμου κλειδί» αναφέρεται στο οικονομικό ρίσκο της συγκέντρωσης της δύναμης σε ένα μόνο άτομο στην κορυφή ενός οργανισμού. Παρακάτω θα δούμε πως και γιατί τα δίκτυα συναλλαγών κρυπτονομισμάτων μπορεί να επηρεαστούν από το «ρίσκο του ατόμου κλειδί», βλέποντας την περίπτωση της «Quadriga CX».

Το «ρίσκο του ατόμου κλειδί», είναι ένα πολύ ενδιαφέρον θέμα στον κλάδο των παραδοσιακών οικονομικών. Στην ουσία είναι η ανησυχία ότι η συγκέντρωση της δύναμης σε ένα μόνο άτομο στην κορυφή ενός οργανισμού ενδέχεται να βλάψει την κανονική λειτουργία του οργανισμού στην περίπτωση της μη-συνέχειας. Η μη-συνέχεια μπορεί να αναφέρεται στο θάνατο, αναπηρία, δυσλειτουργία, απόλυση, αλλαγή θέσης, ή κάποιας άλλης μορφής αλλαγή με το άτομο να απομακρύνεται από την θέση κλειδί του οργανισμού στον οποίο εργάζεται.

Μία τέτοια ανησυχία μπορεί να μην φαίνεται ότι ανήκει στον κόσμο των κρυπτονομισμάτων, επειδή αυτά τα εναλλακτικά νομισματικά μέσα βασίζονται στην τεχνολογία blockchain και χαρακτηρίζονται από μια αποκεντρωμένη, αμετάβλητη, τυφλής εμπιστοσύνης αρχιτεκτονική τουλάχιστον στην θεωρία. Στο παρόν κεφάλαιο θα δούμε την περίπτωση της QuadrigaCX, μίας εταιρίας συναλλαγών

[62] The Key Man Problem in Cryptocurrencies? Case of QuadrigaCX 5 th February, 2019, Usman W. Chohan, MBA, PhD

Κρυπτονομισμάτων, η οποία έχει υποστεί καταστροφικές δυσκολίες, εξαιτίας της απώλειας της πρόσβασης στα περιουσικά στοιχεία που κατέχει, μετά τον θάνατο του ιδρυτή της, Gerald Cotton.

Υπάρχουν τρεις άμεσοι περιορισμοί στην υπόθεση της QuadrigaCX.

1. Πρώτον η συγκεκριμένη υπόθεση είναι υπό εκδίκαση σε δικαστήριο του Halifax, ως εκ τούτου, η ταυτόχρονη εκδίκαση της υπόθεσης αποκλείει οριστικά σχόλια.

2. Υπάρχουν κερδοσκοπικοί ισχυρισμοί ότι έχει σχεδιαστεί μία απάτη εξόδου του ανταλλακτηρίου, κάτι το οποίο αυτό δεν θα αναλύσουμε στην παρούσα διπλωματική εργασία, εφόσον ο στόχος του παρόν κεφαλαίου είναι να τονίσει τα προβλήματα και του κίνδυνους κυβερνοχώρου που έχουν προκύψει με την ανάπτυξη των νέων τεχνολογιών των κρυπτονομισμάτων.

3. Η εξέταση του «προβλήματος του ανθρώπου κλειδί» δεν αφορά ακριβώς τα κρυπτονομίσαματα, αλλά τις δομές που διευκολύνουν τις συναλλαγές αυτών των μέσων, κοινώς αποκαλούμενα «ανταλλακτήρια», σύμφωνα με την ορολογία των παραδοσιακών οικονομικών. Τα «ανταλλακτήρια» λειτουργούν ως κόμβοι στο δίκτυο για την συναλλαγή κρυπτονομισμάτων μεταξύ πωλητών και αγοραστών. Σε αυτό το σημείο ο ανθρώπινος παράγοντας είναι κρίσιμης σημασίας και αυτό και εδώ θα επικεντρωθούμε στην συγκεκριμένη περίπτωση.

Τα κρυπτονομίσματα και η τεχνολογία πίσω από αυτά χαρακτηρίζονται από μία πολυπλοκότητα η οποία αποτρέπει τους «παραδοσιακούς επενδυτές», οι οποίοι προσπαθούν ακόμα και σήμερα να αντιμετωπίσουν έναν ήδη περίπλοκο τομέα, αυτή τη νέα κατηγορία στοιχείων ενεργητικού. Παρ’ όλα αυτά η τεχνολογία των κρυπτονομισμάτων έχει προκαλέσει ένα σημαντικό δημόσιο ενδιαφέρον, το οποίο μας έχει οδηγήσει στην αναζήτηση της χρησιμότητας της αλυσίδας blockchain σε παγκόσμιο επίπεδο. Παρόλο που η υπόσταση των κρυπτονομισμάτων δίεπεται από κάποιες βασικές αρχές,

- την αρχή της αποκέντρωσης
- της τυφλής εμπιστοσύνης

- της μη αναστρέψιμότητας
- της αυτονομίας

αρχές του «κρυπτοαναρχισμου», στην πράξη οι συναλλαγές των κρυπτονομισμάτων περιλαμβάνουν την εμπλοκή του ανθρώπινου παράγοντα στις λειτουργίες του «ανταλλακτηρίου». Αυτές οι συναλλαγές φέρουν αναμφίβολα το ανρθώπινο στοιχείο και είναι επιρρεπείς στο ανθρώπινο ρίσκο το οποίο χαρακτηρίζει την παραδοσιακή οικονομία, όπως το «ρίσκο του ατόμου κλειδί».

Η QuadrigaCX βοηθάει στην απεικόνιση του προβλήματος αυτού. Ιδρύθηκε το 2013 και ήταν το μεγαλύτερο ανταλλακτήριο του Καναδά μέχρι και τις αρχές του 2019. Ξεκίνησε σαν ένα τοπικό ανταλλακτήριο το οποίο πολύ σύντομα μεγάλωσε και ουσιαστικά ήταν υπεύθυνο για τη δημιουργία του δεύτερου Bitcoin ATM στο Βανκούβερ το οποίο δημιουργήθηκε τον Ιανουάριο του 2014. Η ταχεία επέκταση και η συνολική τάση αύξησης των τιμών των κρυπτονομισμάτων, έδωσαν στην Quadriga μία σημαντική θέση στο διεθνή χώρο των κρυπτονομισμάτων μέχρι το 2017. Εντούτοις η πορεία της είχε δυσκολίες παρόμοιες με άλλα ανταλλακτήρια ανά τον κόσμο όπως αυτό της «Mt Gox» στην Ιαπωνία το οποία εν κατακλείδι διαλύθηκε. Για παράδειγμα τον Ιούνιο του 2017 ένα σφάλμα σε ένα έξυπνο συμβόλαιο (smart contract), προκάλεσε την απώλεια δεκατεσσάρων εκατομμυρίων δολαρίων σε κρυπτονομίσματα Etherium. Στην συνέχεια το 2018 ακολούθησαν δυσκολίες, οι οποίες δεν επέτρεπαν στους πελάτες να λάβουν δολάρια σε αντάλλαγμα για τα κρυπτονομίσματα τα οποία είχαν στην κατοχή τους. Την δεδομένη στιγμή η Quadriga απέδωσε αυτό το πρόβλημα σε διαμάχες με τα παραδοσιακά χρηματοπιστωτικά ιδρύματα.

Στο κέντρο της ανόδου και της πτώσης της Quadriga βρισκόταν πάντα ο ιδρυτής της, Gerald Cotter, ο οποίος είχε χρησιμοποιήσει δραστικά μέτρα για την προστασία των κρυπτονομισμάτων με αποτέλεσμα να έχει μόνο ο ίδιος πρόσβαση σε αυτά. Το Δεκέμβριο του 2018 ανακοινώνεται ότι ο Gerald Cotter έχει χάσει την ζωή του μετά από επιπλοκές που σχετίζονται με την «νόσο του Crohn» κατά την διάρκεια ταξιδιού που πραγματοποιούσε στην Ινδία για την οικοδόμηση ενός ορφανοτροφείου. Ως ο «άνθρωπος κλειδί» πίσω από την QuadrigaCX μόνο ο ίδιος είχε πρόσβαση σε ολόκληρη την περιουσία του ανταλλακτηρίου. Από τον Ιανουάριο του 2019 το συνολικό ποσό φαίνεται να είναι αντίστοιχο των εκτατών ενενήντα εκατομμυρίων δολαρίων. Έχοντας προστατεύσει αυστηρά την πρόσβαση στο ενεργητικό των

κρυπτονομισμάτων, ο θάνατος του Cotter ανάγκασε το ανταλακτήριο να ζητήσει προστασία του πιστωτικού ιδρύματος δεδομένου ότι δεν μπορούσε να έχει πρόσβαση στην περιουσία για να επιστρέψει στου αντισυμβαλλόμενους τα ποσά τα οποία τους οφείλει. Έχουν γίνει καταγγελίες στις οποίες δεν μπορούμε να πάρουμε θέση, οι οποίες αναφέρουν ότι το ανταλλακτήριο δεν είχε τα υποκείμενα περιουσιακά στοιχεία για να εξοφλήσει τους αντισυμβαλλόμενους σε καμία περίπτωση. Δεδομένης της τεράστιας αξίας ισοδύναμου σε δολάρια των καταθέσεων, το «ρίσκο του ανθρώπου κλειδί» στην περίπτωση της QuadrigaCX παρουσιάζει σημαντικούς κινδύνους απώλειας στους αντισυμβαλλόμενους και δημιουργεί ένα κλίμα δυσπιστίας και δυσφήμισης στο αρκετά ριζοσπαστικό τομέα των κρυπτονομισμάτων.

Έτσι, σχετικά με τα κρυπτονομίσματα και την τεχνολογία που κρύβεται πίσω από αυτά, όσο αποκεντρωμένα και αν είναι, ακόμα και αν οι συναλλαγές είναι μη αναστρέψιμες και υπάρχει τυφλή εμπιστοσύνη στην τεχνολογία της αλυσίδας των μπλοκ, θα υπάρχει πάντα πανικός και έλλειψη εμπιστοσύνης και αυτό λόγω του ανθρώπινου παράγοντα ο οποίος βρίσκεται στο κέντρο της ανταλλαγής των κρυπτονομισμάτων. Επιπλέον,

Συνοψίζοντας η απόσπαση των κρυπτονομισμάτων από τον τρόπο λειτουργίας των παραδοσιακών χρηματοπιστωτικών οργανισμών είναι κάτι που ακόμα δεν έχουμε καταφέρει να επιτύχουμε. Το πρόβλημα εμφανίζεται με δύο τρόπους. Ο πρώτος αφορά την ανθρώπινη φύση, δηλαδή το «πρόβλημα του ατόμου κλειδί» , και ο δεύτερος, την ανάγκη να για διορθωτική δράση μέσω των παραδοσιακών ιδρυμάτων. Ως εκ τούτου, υπάρχει η ανάγκη να εξετάσουμε την φιλοσοφία των κρυπτονομισμάτων στην βάση της, διότι ενώ υιοθετούν υψηλά ιδεώδη αυτόνομης και εθελοντικής συμμετοχής από ενημερωμένους συμμετέχοντες σε ένα αποκεντρωμένο δίκτυο, στην πράξη, το δίκτυο δεν ανταποκρίνεται στην επίλυση των προβλημάτων που πλήττουν σοβαρά το νέο αυτό χρηματοπιστωτικό μοντέλο, τα οποία είναι τα ίδια προβλήματα που αντιμετωπίζουν οι παραδοσιακοί χρηματοπιστωτικοί οργανισμοί.

5.2. Η Μεγαλύτερη Ληστεία Bitcoin «Mt Gox Hack»[63]

[63] *« The History of the Mt Gox Hack: Bitcoin's Biggest Heist »* ανακτήθηκε στις 19/10/2019 από τον ιστότοπο http://longreads.news247.gr/bitcoinhttps://blockonomi.com/mt-gox-hack/

Το 2010 στην Ιαπωνία ιδρύθηκε το ανταλλακτήριο «Mt Gox» από τον Αμερικανό προγραμματιστή «Jed McCaleb», ο οποίος αργότερα δημιούργησε ένα από τα πιο επιτυχημένα κρυπτονομίσματα, το «Riple». Το όνομα του ανταλλακτηρίου «Mt Gox» είναι συντομογραφία του «Magic: The Gathering Online eXchange». Το ανταλλακτήριο αγοράστηκε από τον Γάλλο προγραμματιστή και υποστηρικτή του Bitcoin «Mark Karpelés» το 2011 και έκτοτε επεκτάθηκε πολύ γρήγορα καταφέρνοντας να γίνει το πιο δημοφιλές ανταλλακτήριο Bitcoin στον κόσμο. Τον Ιούνιου του 2011 το ανταλλακτήριο δέχθηκε επίθεση, η οποία κατά πάσα πιθανότητα πραγματοποιήθηκε από υπολογιστή ο οποίος είχε παραβιαστεί, και ανήκε σε έναν ελεγκτή της εταιρίας. Ο Hacker χρησιμοποίησε την πρόσβασή του στην πλατφόρμα για να αλλάξει την τιμή συναλλαγής των bitcoin σε ένα λεπτό και στην συνέχεια μετέφερε περίπου δύο χιλιάδες bitcoin στον λογαριασμό του, τα οποία αργότερα πουλήθηκαν. Επιπλέον υπολογίζεται ότι την στιγμή που τα bitcoin κόστιζαν ένα λεπτό αγοράστηκαν κατά προσέγγιση 650 bitcoin από πελάτες του ανταλλακτηρίου, τα οποία δεν επιστράφηκαν ποτέ στο ανταλλακτήριο. Ως αποτέλεσμα των παραπάνω το ανταλλακτήριο έλαβε δραστικά μέτρα, όπως να πάρει το μεγαλύτερο μέρος των bitcoin που είχε στην κατοχή του και να το αποθηκεύσει σε «cold wallet», δηλαδή σε συσκευές, ειδικά φτιαγμένες, για την αποθήκευση κρυπτονομισμάτων offline.

Παρά την παραβίαση της πλατφόρμας τον Ιούνιου του 2011, έως το 2013 το ανταλλακτήριο είχε εδραιωθεί ως το μεγαλύτερο ανταλλακτήριο bitcoin στον κόσμο.

Τον Μάιο του 2013 το ανταλλακτήριο «Coinlab» μήνησε το «Mt Gox», για παραβίαση συμβολαίου διεκδικώντας εβδομήντα πέντε εκατομμύρια δολάρια. Οι δύο εταιρίες είχαν υπογράψει ένα συμβόλαιο σύμφωνα με το οποίο το ανταλλακτήριο «Coinlab» θα αναλάμβανε να εξυπηρετεί όλους τους Αμερικανούς πελάτες του «Mt. Gox». Σύμφωνα με την μήνυση του «Coinlab» η συμφωνία δεν υλοποιήθηκε ποτέ λόγου ότι το ανταλλακτήριο «Mt. Gox» παραβίασε μία ρήτρα της σύμβασης. Επιπρόσθετα, το «Υπουργείο Εσωτερικής Ασφάλειας των ΗΠΑ» διερευνούσε ισχυρισμούς ότι μια θυγατρική του Mt. Gox που δραστηριοποιείται στις ΗΠΑ δεν είχε άδεια και ως εκ τούτου λειτουργούσε παράνομα. Το αποτέλεσμα της έρευνας ήταν να κατασχεθούν από την εταιρία περισσότερα από πέντε εκατομμύρια δολάρια από τους τραπεζικούς λογαριασμούς της. Μετά την ολοκλήρωση της έρευνας και την κατάσχεση του ποσού, το ανταλλακτήριο ανακοίνωσε προσωρινή αναστολή αναλήψεων σε Αμερικανικά Δολάρια. Παρόλο που αυτή η αναστολή κράτησε ονομαστικά μόνο για

ένα μήνα, πολλοί πελάτες αντιμετώπιζαν καθυστερήσεις έως και τρεις μήνες στην ανάληψη μετρητών από τους λογαριασμούς τους. Αυτές οι καθυστερήσεις στις αναλήψεις έστρεψαν τον κόσμο σε άλλα ανταλλακτήρια, με αποτέλεσμα το «Mt Gox» να χάσει την πρωτοκαθεδρία του και μέχρι το τέλος του 2013 να είναι πλέον η τρίτη σε μέγεθος πλατφόρμα συναλλαγής Bitcoin. Όπως αποδείχθηκε αυτό ήταν το μικρότερο πρόβλημα που αντιμετώπιζε το ανταλλακτήριο την δεδομένη χρονική στιγμή, καθώς αποδείχθηκε ότι για περισσότερο από δύο χρόνια δεχόταν παραβιάσεις χωρίς γίνει να αντιληπτό.

Στις επτά Φεβρουαρίου του 2014 το ανταλλακτήριο «Mt Gox» σταμάτησε όλες τις αναλήψεις Bitcoin, υποστηρίζοντας ότι απλώς παγώνει την δυνατότητα ανάληψης «Για να αποκτήσει μία καθαρή τεχνική όψη της πορείας των νομισμάτων στην πλατφόρμα». Μετά από μερικές βδομάδες αβεβαιότητας, στις είκοσι τέσσερις Φεβρουαρίου τους 2014, το ανταλλακτήριο σταμάτησε όλες τις συναλλαγές και η ιστοσελίδα του σταμάτησε να είναι προσβάσιμη. Την ίδια εβδομάδα διέρρευσε ένα εταιρικό έγγραφο το οποίο έγγραφε ότι οι χάκερ κατάφεραν να αποσπάσουν επτακόσιες σαράντα τέσσερις χιλιάδες, τετρακόσια οκτώ Bitcoin τα οποία ανήκαν σε πελάτες του ανταλλακτηρίου και επιπλέον εκατό χιλιάδες Bitcoin τα οποία ανήκαν στην εταιρία. Στις είκοσι οκτώ Φεβρουαρίου το ανταλλακτήριο υπέβαλε αίτηση για πτώχευση στην Ιαπωνία και δύο εβδομάδες αργότερα έκανε το ίδιο και στις ΗΠΑ. Μεταγενέστερες έρευνες έδειξαν ότι η παράνομη πρόσβαση στην περιουσία του ανταλλακτηρίου είχε επιτευχθεί από τον Σεπτέμβριο του 2011.

Ως αποτέλεσμα όλων των παραπάνω το ανταλλακτήριο λειτουργούσε ενώ τεχνικά ήταν αφερέγγυο για τουλάχιστον δύο χρόνια και είχε χάσει πρακτικά όλα τα κρυπτονομίσματα τα οποία κατείχε από τα μέσα του 2013. Πρόσθετα στοιχεία υποδεικνύουν ότι το ανταλλακτήριο είχε ήδη χάσει έως και ογδόντα χιλιάδες bitcoin από το ενεργητικό του, πριν ακόμα αναλάβει ο «Mark Karpeles» το 2011.

Αν και παραμένει ανοιχτή η υπόθεση και συνεχίζονται οι έρευνες σχετικά με τα γεγονότα, θεωρείται ότι τα περισσότερα bitcoin που κλάπηκαν από το «Mt Gox» πάρθηκαν από τα «Hot wallet». Η βασική διαφορά μεταξύ «Hot Wallet» και «Cold Wallet», είναι ότι τα πρώτα είναι συνδεδεμένα στο διαδίκτυο, ενώ τα δεύτερα όχι. Υπάρχουν διάφοροι λόγοι για τους οποίους χρησιμοποιούνται αυτοί οι δύο τύποι

πορτοφολιών, και είναι κάτι σύνηθες για τις πλατφόρμες να κρατούν και των δύο τύπων πορτοφόλια.

Πριν τον Σεπτέμβριο του 2011, το ανταλλακτήριο δεν είχε κρυπτογραφήσει τα ιδιωτικά κλειδιά των λογαριασμών που είχε, και το πιο πιθανό είναι να κλάπηκαν είτε από κάποια παραβίαση, είτε από κάποιον ο οποίος εργαζόταν στην εταιρία, μέσω ενός ηλεκτρονικού αρχείου «wallet.dat». Έκτοτε έχουν γίνει πολλές υποθέσεις σχετικά με το πώς πραγματοποιήθηκε η κλοπή, με την μέχρι στιγμής πιο έγκυρη να είναι η θεωρία του «Andrew Norry», σύμφωνα με την οποία οι επιτιθέμενοι απέκτησαν πρόσβαση στα ιδιωτικά κλειδιά, και πλέον ήταν σε θέση να μεταφέρουν σταδιακά τα bitcoin χωρίς να γίνουν αντιληπτοί, καθώς το σύστημα θεωρούσε ότι γίνεται μεταφορά των κεφαλαίων σε πιο ασφαλή λογαριασμούς.

Τον Μάρτιο του 2014 το ανταλλακτήριο ανέφερε στην ιστοσελίδα του ότι είχε ανακτήσει διακόσιες χιλιάδες bitcoin από πορτοφόλια που ήταν στην κατοχή του ανταλλακτηρίου και γίνονταν χρήση πριν το 2011. Τα συγκεκριμένα bitcoin παραμένουν κρατημένα για την μερική αποπληρωμή των πιστωτών, ενώ η εταιρία παραμένει σε πτώχευση υπό προστασία.

Ο «Mark Karpelés» συνελήφθη τον Αύγουστο του 2015 στην Ιαπωνία και κατηγορήθηκε για απάτη και υπεξαίρεση, αν και καμία από τις κατηγορίες δεν σχετίζεται άμεσα με την κλοπή. Ο ίδιος προφυλακίστηκε μέχρι τον Ιούλιο του 2016 όπου και αφέθηκε ελεύθερος με εγγύηση. Ο ίδιος έχει δηλώσει αθώος στις παραπάνω κατηγορίες και η δίκη συνεχίζεται ακόμη και σήμερα.

Τον Ιούλιο του 2017, ο «Alexander Vinnik», Ρώσσος στην καταγωγή, συνελήφθη από τις Αμερικανικές αρχές στην Ελλάδα, και κατηγορήθηκε ότι έπαιξε σημαντικό ρόλο στο ξέπλυμα χρήματος των κλοπιμαίων από το ανταλλακτήριο «Mt Gox». Επιπλέον ο Vinnik κατηγορήθηκε από τις ελληνικές αρχές για ξέπλυμα χρήματος bitcoin συνολικής αξίας τεσσάρων δισεκατομμυρίων ευρώ. Ο ίδιος φέρεται να συνδέεται με το γνωστό ανταλλακτήριο bitcoin «BTC-e» στο οποίο εισέβαλε το FBI στο πλαίσιο έρευνας που έγινε . Η ιστοσελίδα του «BTC-e» έχει τερματιστεί και πλέον είναι υπό την κυριότητα του FBI. Είναι η πρώτη φορά στην ιστορία, που η Αμερικανική Κυβέρνηση έχει κατασχέσει ξένο συνάλλαγμα σε ξένο έδαφος.

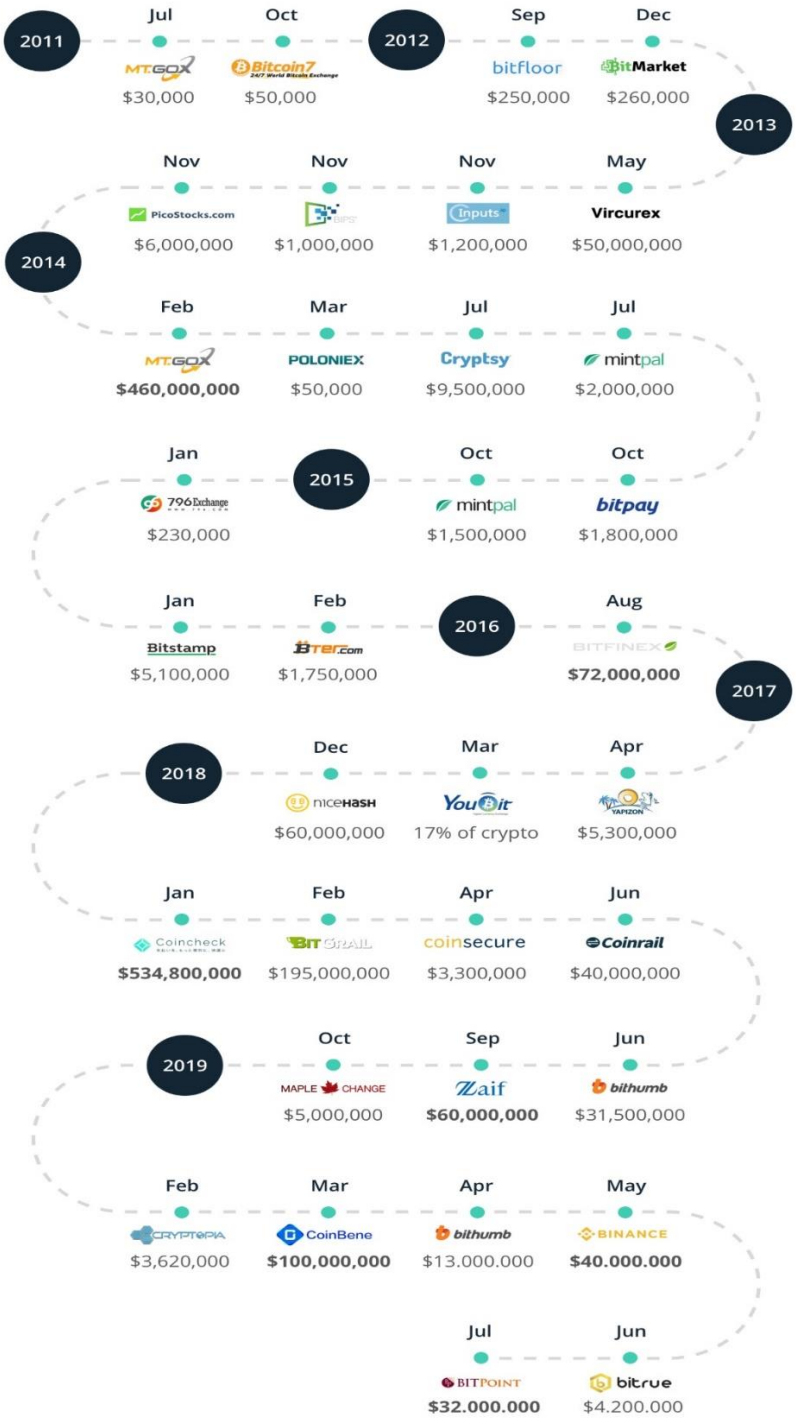
Σε έρευνες που έγιναν από την «Wizsec» μία ομάδα ειδικών ασφαλείας, εντοπίστηκε ότι ο «Alexander Vinnik», ήταν ο ιδιοκτήτης των πορτοφολιών στα οποία

είχαν μεταφερθεί τα κλεμμένα bitcoins του «Mt Gox» εκ των οποίων τα περισσότερα πωλήθηκαν στην πλατφόρμα του ανταλλακτηρίου «BTC-e»

Η δίκη συνεχίζεται, και τον Φεβρουάριο του 2019 μέσω του ιστότοπου «TechCrunch» ανακοινώθηκε ότι ένα κίνημα με το όνομα «GoxRising» εργάστηκε για να ακολουθηθεί μία εναλλακτική λύση στην πτώχευση για το ανταλλακτήριο. Η ιδέα πίσω από το κίνημα είναι απλή. Αντί να χρησιμοποιηθεί η νομοθεσία που αφορά την πτώχευση και να παραδοθούν τα εναπομείναντα περιουσιακά στοιχεία στους κατόχους της εταιρίας, το κίνημα ζήτησε να χρησιμοποιηθεί η νομοθεσία περί πολιτικής αποκατάστασης, ώστε να επιστραφούν τα κρυπτονομίσματα που έχει στην κατοχή του το ανταλλακτήριο στους πιστωτές του. Αναμένεται να δούμε τα αποτελέσματα της δίκης, καθώς και τις αλλαγές που θα επιφέρει στον τρόπο λειτουργίας των ανταλλακτηρίων. Αυτό που μας δίδαξε η υπόθεση του ανταλλακτηρίου «Mt Gox» είναι ότι πρέπει να υπάρχουν καλύτερες υποδομές σε περίπτωση που συμβεί το χειρότερο. Είναι παράλογο ακόμα και σήμερα μετά από πέντε χρόνια να υπάρχουν χρήστες του ανταλλακτηρίου οι οποίοι περιμένουν να λάβουν πίσω ένα μέρος των επενδύσεων που είχαν.

Παρόλο που το δίκτυο των κρυπτονομισμάτων είναι αποκεντρωμένο, τα ανταλλακτήρια που προσφέρουν τις καλύτερες τιμές και έχουν την μεγαλύτερη ρευστότητα δεν είναι αποκεντρωμένα. Οι χρήστες πρέπει να δηλώσουν τα στοιχεία τους και έτσι δεν μπορούν να υποστηρίξουν την πλήρη ανωνυμία, έχουν δηλαδή τον ρόλο του μεσάζοντα. Υπάρχουν αποκεντρωμένα ανταλλακτήρια, αλλά σε καμία περίπτωση δεν μπορούν να προσφέρουν την ευκολία και το «user interface» που έχουν τα μη αποκεντρωμένα ανταλλακτήρια.

Το πρόβλημα που πρέπει να λυθεί είναι το εξής. Όταν ένα ανταλλακτήριο αναλάβει την κυριότητα των κρυπτονομισμάτων από έναν χρήστη, είναι πιθανό να υπάρξει ένα αντίστοιχο σενάριο με αυτό που αναλύσαμε παραπάνω. Δεδομένου του είδους των νόμων που διέπουν την πτώχευση στο καθιερωμένο χρηματοπιστωτικό σύστημα, το μόνο σίγουρο είναι ότι η ίδια νομοθεσία δεν ταιριάζει στις λειτουργίες των ανταλλακτηρίων κρυπτονομισμάτων.



Διάγραμμα 7: Χρονική απεικόνιση κλοπών σε ανταλλακτήρια κρυπτονομισμάτων ανά τον κόσμο[64]

[64] Η εικόνα ανακτήθηκε στις 27/10 από τον ιστότοπο https://www.ledger.com/academy/crypto/hacks-timeline/

5.3. Κρυπτονομίσματα Και Παράνομες Δραστηριότητες[65]

Η αυξημένη ασφάλεια και η σχετική ανωνυμία που προσφέρουν τα κρυπτονομίσματα τα καταδεικνύει ως το κατάλληλο μέσο για την πραγματοποίηση παράνομων δραστηριοτήτων. Οι συνηθέστερες είναι πώληση ναρκωτικών ουσιών και όπλων, δολοφονίες, νομιμοποίηση εσόδων από παράνομες δραστηριότητες και κλοπή ταυτότητας. Αναφερόμαστε σε ένα στρώμα ανωνυμίας γιατί στην πραγματικότητα καμία συναλλαγή δεν είναι εντελώς ανώνυμη, και πάντα υπάρχει η πιθανότητα μία συναλλαγή η ένας λογαριασμός να συνδεθεί με την ταυτότητα του κατόχου.

5.3.1. Νομιμοποίηση Εσόδων Από Παράνομες Δραστηριότητες

Τα περισσότερα γνωστά ανταλλακτήρια, αυτά που έχουν την μεγαλύτερη ρευστότητα και τις καλύτερες τιμές, όπως και τα παραδοσιακά τραπεζικά ιδρύματα χρησιμοποιούν ένα σύστημα «Γνωριμίας με τον συναλλασσόμενο» ονομαζόμενο «KYC» (know you client) πράγμα που σημαίνει ότι κάθε λογαριασμός τακτοποιείται στα στοιχεία του χρήστη. Η νομιμοποίηση παράνομων εσόδων μέσω των κρυπτονομισμάτων γίνεται με τους παρακάτω τρόπους:

- Ανταλλακτήρια κρυπτονομισμάτων επιτρέπουν την αγοροπωλησία κρυπτονομισμάτων απλά με την χρήση μετρητών χωρίς κάποιον περεταίρω έλεγχο, με κόστος συνήθως μία προμήθεια 10%-15% της συνολικής αξίας, σε αντίθεση με τα εξουσιοδοτημένα ανταλλακτήρια που το ύψος της προμήθειας είναι 1%-2%. Η διαφορά είναι ότι ο συναλλασσόμενος με ένα κόστος 10%-15% έχει την δυνατότητα να μετατρέψει τα παράνομα χρήματα σε κρυπτονομίσματα και στην συνέχεια να εισαγάγει «καθαρά» μετρητά στο χρηματοπιστωτικό σύστημα.

[65]Dr. Nikolaos Theodorakis «The Use of Cryptocurrencies for Illicit Activities and Relevant Legislative Initiatives» ανακτήθηκε στις 27/10/2019 από τον ιστότοπο https://theartofcrime.gr/the-use-of-cryptocurrencies-for-illicit-activities-and-relevant-legislative-initiatives/

- Αυτόματες ταμειακές μηχανές (ATM) κρυπτονομισμάτων επιτρέπουν την αγορά κρυπτονομισμάτων με μετρητά χωρίς να απαιτείται από τον συναλλασσόμενο να δηλώσει κάποια πληροφορία. Τα «ATM» συνήθως κρατούν μία προμήθεια ύψους 10%-15%.
- «Υπηρεσίες πλυντηρίων» μέσω των οποίων το ποσό μεταφοράς, διαιρείται σε πολλά μικρότερα ποσά τα οποία στέλνονται ταυτόχρονα σε πολλούς λογαριασμούς και μετά από πολλές συναλλαγές καταλήγουν στον τελικό προορισμό που είναι ο λογαριασμός του χρήστη. Η διαδικασία αυτή ακολουθείτε ώστε η συναλλαγές να καταστούν λιγότερο αναγνωρίσιμες.
- Επίσης νομιμοποίηση παράνομων εσόδων μπορεί να γίνει μέσο διαμεσολαβητών που αγοράζουν αντικείμενα από δημοφιλείς ιστοσελίδες όπως είναι το «amazon» και το «ebay». Δεδομένου ότι αυτές οι πλατφόρμες δεν εφαρμόζουν προγράμματα γνωριμίας με τον συναλλασσόμενο, οι περισσότερες συναλλαγές δεν ελέγχονται.

5.3.2. Εμπορία Ναρκωτικών Μέσω Των Κρυπτονομισμάτων

Η εμπορία ναρκωτικών με χρήση κρυπτονομισμάτων, πραγματοποιείται σε σελίδες που προσφέρουν (σχετική) ανωνυμία. Για να επιτευχθεί αυτό, οι αγοροπωλησίες πραγματοποιούνται στο «σκοτεινό δίκτυο» γνωστό ως «dark web». Για να εισέλθει κάποιος στο «σκοτεινό δίκτυο» απαραίτητη προϋπόθεση είναι να χρησιμοποιήσει έναν συγκεκριμένο περιηγητή ο οποίος κάνει την περιήγηση ανώνυμη.

Το «σκοτεινό δίκτυο» έπαιξε μεγάλο ρόλο στην αύξηση της παράνομης διακίνησης ναρκωτικών ουσιών. Το 2011 δημιουργήθηκε το πρώτο ηλεκτρονικό κατάστημα πώλησης ναρκωτικών ουσιών, «SilkRoad» το οποίο έμοιαζε με μεγάλες ιστοσελίδες αγοροπωλησιών όπως είναι το «ebay» και το «amazon». Το ηλεκτρονικό κατάστημα λειτούργησε μέχρι το 2013, όταν το FBI συνέλαβε τον δημιουργό της ιστοσελίδας «Ross Ulbricht», ο οποίος καταδικάστηκε σε δις ισόβια κάθειρξη και επιπλέον σαράντα χρόνια, χωρίς την δυνατότητα αποφυλάκισης υπό όρους. Μετά την σύλληψη του δημιουργού δημιουργήθηκε το «SilkRoad 2.0» ως συνέχεια του αρχικού

καταστήματος το οποίο κατασχέθηκε το 2014. Ωστόσο στα μέσα του 2016 δημιουργήθηκε το «RoadSilk 3.0» και λειτουργεί ακόμα και τώρα.

Τα κρυπτονομίσματα προσφέρουν έναν νέο τρόπο συναλλαγής στους διακινητές παράνομων ουσιών ο οποίος δίνει την δυνατότητα αγοράς και πώλησης ενός προϊόντος χωρίς την φυσική επαφή. Τέλος ένας πωλητής έχει την δυνατότητα να δημιουργήσει ένα «αξιόπιστο» προφίλ, με βάση τις κριτικές των πελατών του.

5.3.3 Εκβιασμός Με Χρήση Των Κρυπτονομισμάτων

Τα τελευταία χρόνια τα περιστατικά εκβιασμών με χρήση κρυπτονομισμάτων έχουν αυξηθεί. Το «Crypto-ransomware» είναι ένα είδος επιβλαβούς προγράμματος που κρυπτογραφεί αρχεία που είναι αποθηκευμένα σε έναν υπολογιστή ή μία κινητή συσκευή για να εκβιάσει τον κάτοχο της συσκευής και να του αποσπάσει κάποιο χρηματικό ποσό συνήθως σε μορφή «bitcoin», ή κάποιο άλλο κρυπτονόμισμα. Σε αντίθεση με άλλους ιούς το «Crypto-ransomware» δεν είναι κρυμμένο, αντίθετα εμφανίζει μηνύματα στην οθόνη και χρησιμοποιεί το πλεονέκτημα του φόβου και του σοκ για να κάνει τον κάτοχο της συσκευής να πληρώσει τα λύτρα, τα οποία συνήθως ζητούνται σε μορφή «bitcoin» ή κάποιου άλλου κρυπτονομίσματος. Το 2015 πραγματοποιήθηκε μία τέτοιου είδους επίθεση σε τρεις ελληνικές τράπεζες από μία ομάδα εγκληματιών με το όνομα «Armada Collective». Στις οθόνες των υπολογιστών των τραπεζών εμφανίστηκε ένα μήνυμα το οποίο ζητούσε να καταβάλουν μεγάλα χρηματικά ποσά σε μορφή «bitcoin» με την απειλή πως αν δεν το κάνουν θα διαρρεύσουν δεδομένα και στοιχεία πελατών.

6. ΣΥΜΠΕΡΑΣΜΑΤΑ ΕΡΕΥΝΑΣ

Η χρήση των κρυπτονομισμάτων έχει αυξηθεί τα τελευταία χρόνια με ραγδαίους ρυθμούς. Τα κρυπτονομίσματα και η τεχνολογία που κρύβεται πίσω από αυτά, αποτελούν μία καινοτομία στον χώρο των συναλλαγών και όχι μόνο. Αυτό που συμπεραίνουμε είναι ότι καμία τεχνολογία δεν μπορεί να αποφέρει την πλήρη ασφάλεια, παρόλο που τα χαρακτηριστικά που διέπουν την αλυσίδα «blockchain» είναι μία αισιόδοξη προσέγγιση στην τομέα της ασφάλειας. Στην παρούσα διπλωματική εργασία εξετάσαμε δύο περιπτώσεις ανταλλακτηρίων κρυπτονομισμάτων, στις οποίες οι χρήστες δεν έχουν πλέον πρόσβαση στα κεφάλαια τους. Οι χρήστες πρέπει να προσέχουν ιδιαίτερα πριν να εμπιστευτούν τα κεφάλαια τους σε κάποιο ανταλλακτήριο. Ακόμα και αν το κάνουν προτείνεται να κρατούν το μεγαλύτερο μέρος των κρυπτονομισμάτων σε «Cold Wallet», δηλαδή πορτοφόλια τα οποία δεν είναι συνδεδεμένα με το διαδίκτυο. Η νομοθεσία των παραδοσιακών χρηματοπιστωτικών ιδρυμάτων και των μετοχών δεν επαρκεί για να εφαρμοστεί στις ιδιαιτερότητες των σύγχρονων κρυπτονομισμάτων. Επίσης εξετάσαμε τη χρήση κρυπτονομισμάτων για την διεξαγωγή παράνομων συναλλαγών και νομιμοποίηση παράνομων εσόδων. Κάθε χώρα έχει την δική της νομοθεσία σχετικά με τα μέτρα «KYC» (γνωριμία με τον συναλλασσόμενο) «AML» (καταπολέμηση του ξεπλύματος χρημάτων) «CFT» (καταπολέμηση της χρηματοδότησης της τρομοκρατίας), ωστόσο αυτοί οι νόμοι δεν συνοδεύονται από συγκεκριμένα πρότυπα επειδή οι ρυθμιστικές αρχές θέλουν τα χρηματοπιστωτικά ιδρύματα να κάνουν ότι μπορούν για να μειώσουν τους κινδύνους. Τα κρυπτονομίσματα είναι εδώ και θα μείνουν για μεγάλο χρονικό διάστημα, πράγμα που σημαίνει ότι η νομοθεσία και το ρυθμιστικό πλαίσιο που τα περιβάλει πρέπει να εξελιχθούν.

ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ

ΗΛΕΚΤΡΟΝΙΚΕΣ ΠΗΓΕΣ:

ΕΛΛΗΝΟΓΛΩΣΣΕΣ:

1. Ευρετήριο Οικονομικών όρων. (χ.χ) *Χρήμα (Money).* Ανακτήθηκε στις 15/6/2019 από τον ιστότοπο https://www.euretirio.com/xrima/.
2. Margaret Rouse. (January, 2014) *Barter economy.* Ανακτήθηκε στις 26/6/2019 από τον ιστότοπο https://whatis.techtarget.com/definition/barter-economy
3. Δέσποινας Ευγενίδου, Ευαγγελίας Αποστόλου, Γιάννη Στόγια, Παναγιώτη Τσελέκα, Μαίρης Φουντουλή, Ευτέρπης Ράλλη, * Αλέξη Τότσικα**.** (χ.χ.) Το νόμισμα στον Αρχαίο Ελληνικό Κόσμο. *Αργολική Αρχειακή Βιβλιοθήκη Ιστορίας και πολιτισμού*. Ανακτήθηκε στις 26/6/2019 από τον ιστότοπο https://argolikivivliothiki.gr/tag/%CF%84%CE%BF-%CE%BD%CF%8C%CE%BC%CE%B9%CF%83%CE%BC%CE%B1-%CF%83%CF%84%CE%BF%CE%BD-%CE%B1%CF%81%CF%87%CE%B1%CE%AF%CE%BF-%CE%B5%CE%BB%CE%BB%CE%B7%CE%BD%CE%B9%CE%BA%CF%8C-%CE%BA%CF%8C%CF%83%CE%BC%CE%BF/
4. Η εικόνα ανακτήθηκε στις 26/6/2019 από τον ιστότοπο https://www.google.com/search?q=%CF%84%CE%B1%CE%BB%CE%B1%CE%BD%CF%84%CE%B1+%CE%BD%CE%BF%CE%BC%CE%B9%CF%83%CE%BC%CE%B1%CF%84%CE%B1&source=lnms&tbm=isch&sa=X&ved=0ahUKEwix4PHV4IzjAhUs2aYKHeQsAHYQ_AUIECgB&biw=1351&bih=636#imgrc=Yh6kUS-DpvZOOM:
5. Η εικόνα ανακτήθηκε στις 26/6/2019 από τον ιστότοπο https://www.google.com/search?q=%CE%BF%CE%B2%CE%BF%CE%BB%CE%BF%CF%82++%CE%BD%CE%BF%CE%BC%CE%B9%CF%83%CE%BC%

CE%B1%CF%84%CE%B1&source=lnms&tbm=isch&sa=X&ved=0ahUKEwj39vOH3YzjAhUE7aYKHZVMBIYQ_AUIECgB&biw=1351&bih=587#imgrc=2GyIj1Ea8gny8M:

6. Μπάλας, Φώτης (2016). *Τα πιο σημαντικά, εναλλακτικά του Bitcoin, Ψηφιακά νομίσματα.,* ανακτήθηκε στις 14/9/2019 από τον ιστότοπο: https://www.pcsteps.gr/107937-%CF%88%CE%B7%CF%86%CE%B9%CE%B1%CE%BA%CE%AC-%CE%BD%CE%BF%CE%BC%CE%AF%CF%83%CE%BC%CE%B1%CF%84%CE%B1-%CE%B5%CE%BD%CE%B1%CE%BB%CE%BB%CE%B1%CE%BA%CF%84%CE%B9%CE%BA%CE%AC-%CF%84%CE%BF%CF%85-bitcoin/
7. Τιβέριος Μ.Δ. (20/6/ 1999; Δημοσιεύθηκε 24/11/2008). Τράπεζες και τοκογλύφοι στην Αρχαία Ελλάδα. *Το Βήμα.* Ανακτήθηκε στις 27/6/2019 από τον ιστότοπο https://www.tovima.gr/2008/11/24/opinions/trapezes-kai-tokoglyfoi-stin-arxaia-ellada/
8. Φίλιππας Ν. (30/5/2011). Οι Αρχαίοι Έλληνες και η Οικονομία. *Μύρτις.* . Ανακτήθηκε στις 27/6/2019 από τον ιστότοπο http://www.myrtis.gr/index.php?option=com_content&view=article&id=253&Itemid=315&lang=fr
9. Friedman H. David, *Χρήμα και Τραπεζική*., Ανακτήθηκε στις 18/11/2019 από τον ιστότοπο: https://static.eudoxus.gr/books/04/chapter-7304.pdf
10. *« Bitcoin: Μύθοι, Αλήθειες και μυστικά»* ανακτήθηκε στις 2/9/2019 από τον ιστότοπο http://longreads.news247.gr/bitcoin
11. Bitcoin, *«Διασφαλίζοντας το πορτοφόλι σας»*, ανακτήθηκε στις 14/9/2019 από τον ιστότοπο https://bitcoin.org/el/secure-your-wallet#online
12. Bitcoin, *«Επιλέξτε το Bitcoin πορτοφόλι σας»*, ανακτήθηκε στις 14/9/2019 από τον ιστότοπο https://bitcoin.org/el/choose-your-wallet?step=1

ΞΕΝΟΓΛΩΣΣΕΣ:

1. Abilash Soundararajan, 10 Blockchain and New Age Security Attacks You Should Know, Ανακτήθηκε στις 25/8/2019 από τον ιστότοπο: https://blogs.arubanetworks.com/solutions/10-blockchain-and-new-age-security-attacks-you-should-know/
2. Bajpai, Prableen(2017). *The 10 most important cryptocurrencies other than Bitcoin.*, ανακτήθηκε στις 14/9/2019 από τον ιστότοπο: https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin/
3. Binance Academy, «*What Is a Blockchain Consensus Algorithm?»* Ανακτήθηκε στις 20/7/2019 από τον ιστότοπο https://www.binance.vision/blockchain/what-is-a-blockchain-consensus-algorithm
4. Dossis Luc, *The top 10 cryptos explained.*, ανακτήθηκε στις 14/9/2019 από τον ιστότοπο: https://blog.goodaudience.com/the-top-10-cryptos-explained-85cddbe4f281
5. Dr. Nikolaos Theodorakis (2018) «The Use of Cryptocurrencies for Illicit Activities and Relevant Legislative Initiatives» ανακτήθηκε στις 27/10/2019 από τον ιστότοπο https://theartofcrime.gr/the-use-of-cryptocurrencies-for-illicit-activities-and-relevant-legislative-initiatives/
6. Finley, Klint (2018)., *After 10 years, Bitcoin has changed everything and nothing*, ανακτήθηκε στις 14/9/2019 από τον ιστότοπο: https://www.wired.com/story/after-10-years-bitcoin-changed-everything-nothing/
7. Frankenfield, Jake(2014). *Altcoin*. ανακτήθηκε στις 14/9/2019 από τον ιστότοπο: https://www.investopedia.com/terms/a/altcoin.asp
8. Frankenfield, Jake(2016). *Ethereum*. ανακτήθηκε στις 14/9/2019 από τον ιστότοπο: https://www.investopedia.com/terms/e/ethereum.asp
9. Frankenfield,Jake(2018*), VirtualCurrency*, ανακτήθηκε στις 14/9/2019 από τον ιστότοπο: https://www.investopedia.com/terms/v/virtual-currency.asp
10. Hauhgh Matthew (2014), *Barter Economy*., Ανακτήθηκε στις 18/11/2019 από τον ιστότοπο: https://whatis.techtarget.com/definition/barter-economy

11. Hertig, Alyssa and Palmer, Daniel (2017). *What is ether?* ανακτήθηκε στις 14/9/2019 από τον ιστότοπο: https://www.coindesk.com/information/what-is-ether-ethereum-cryptocurrency
12. Shobhit, Seth(2018). *All about Ethereum*. ανακτήθηκε στις 14/9/2019 από τον ιστότοπο: https://www.investopedia.com/tech/all-about-ethereum/
13. J.P. and G.T., *Virtual Currency: The Economist*, Ανακτήθηκε στις 6/7/2019 από τον ιστότοπο https://www.economist.com/babbage/2011/06/13/bits-and-bob
14. Lexico. *Cryptocurrency*, ανακτήθηκε στις 6/7/2019 από τον ιστότοπο https://www.lexico.com/en/definition/cryptocurrency
15. Satoshi Nakamoto (2008), «*Bitcoin; A Peer-To-Peer Electronic Cash System*», ανακτήθηκε στις 1/9/2019 από τον ιστότοπο https://bitcoin.org/bitcoin.pdf
16. Schollmeir Rüdiger. "A Definition of Peer-to-Peer Networking for the Classification of Peer-to Peer Architectures and Applications" Munchen, 2002 Ανακτήθηκε στις 1/9/2019 από τον ιστότοπο https://www.researchgate.net/publication/3940901_A_Definition_of_Peer-to-Peer_Networking_for_the_Classification_of_Peer-to-Peer_Architectures_and_Applications
17. Shobhit, Seth(2018). *All about Ethereum*. ανακτήθηκε στις 14/9/2019 από τον ιστότοπο: https://www.investopedia.com/tech/all-about-ethereum/
18. Reiff, Nathan (2017). *Could cryptocurrencies replace cash?.*, ανακτήθηκε στις 14/9/2019 από τον ιστότοπο:https://www.investopedia.com/news/could-cryptocurrencies-replace-cash-bitcoin-flippening/
19. Wikoff, Shawn (2016). *The expert Shawn Wikoff talks about Electronic money.*, ανακτήθηκε στις 14/9/2019 από τον ιστότοπο: https://medium.com/@wikoff.shawn/the-expert-shawn-wikoff-talks-about-electronic-money-d01964dd669c
20. *« The History of the Mt Gox Hack: Bitcoin's Biggest Heist »* ανακτήθηκε στις 19/10/2019 από τον ιστότοπο http://longreads.news247.gr/bitcoinhttps://blockonomi.com/mt-gox-hack/
21. Η εικόνα ανακτήθηκε από το βίντεο https://www.youtube.com/watch?v=2VtH-XAOjXw με τίτλο «what is cryptocurrency mining?» στις 27/10/2019

22. Η εικόνα ανακτήθηκε στις 27/10 από τον ιστότοπο https://www.ledger.com/academy/crypto/hacks-timeline/

ΒΙΒΛΙΑ:

ΕΛΛΗΝΟΓΛΩΣΣΑ:

1. Κανελλόπουλος Αθανάσιος (1996). *Σύγχρονες Οικονομικές Σκέψεις των Αρχαίων Ελλήνων*. Λιβάνης: Νέα Σύνορα.
2. Λιανός Θ., Παπαβασιλείου Α. & Χατζηανδρέου Α. (8/2016). *Αρχές Οικονομικής Θεωρίας- Μικροοικονομία Μακροοικονομία*. Αθήνα: Ινστιτούτο Τεχνολογίας Υπολογιστών και Εκδόσεων – «ΔΙΟΦΑΝΤΟΣ»

ΞΕΝΟΓΛΩΣΣΑ:

1. Antonopoulos M. Andreas (2014), *Mastering Bitcoin*, United States of America: O'Reilly Media, Inc.
2. Swan Melanie (2015)., *Blockchain: Blueprint for a new economy*., O' Reilly Media, Inc.
3. Halaburda Hanna, Sarvary Miklos (2016), *Beyond Bitcoin; The Economics of Digital Currencies*, Palgrave Macmillan
4. Narayanan Arvind, Bonneau Joseph, Felten Edward, Miller Andrew, Goldfeder Steven (2016), *Bitcoin and other Cryptocurrency Technologies*, Princeton University Press

ΑΡΘΡΑ ΣΕ ΕΠΙΣΤΗΜΟΝΙΚΑ ΠΕΡΙΟΔΙΚΑ:

ΞΕΝΟΓΛΩΣΣΑ:

1. F.S.Mishkin, (2000), «*The Economics of Money, Banking and Financial markets*».
2. The Key Man Problem in Cryptocurrencies? Case of QuadrigaCX 5 th February, 2019, Usman W. Chohan, MBA, PhD
3. Karl Marx (1999), «*Capital*», Progress Publishers.

ΕΛΛΗΝΟΓΛΩΣΣΑ:

1. Ένωση Ελληνικών Τραπεζών, (2003), «*Οι Τράπεζες μοχλός της ανάπτυξης*», ενημερωτικό έντυπο με ομιλία προέδρου Ε.Ε.Τ κα. Θ. Καρατζά.
2. Παπαδόπουλος Α. , (2002) , *Νομισματική Θεωρία και Πολιτική*, Ρέθυμνο.
3. Πιτσικός Σπύρος, «*Τι είναι τα κρυπτονομίσματα και πώς επενδύει κανείς σε αυτά*», Ανακτήθηκε στις 16/11/2019 από ιστότοπο https://www.news.gr/oikonomia/article/919934/ti-ine-ta-kriptonomismata-ke-pos-ependii-kanis-se-afta.html