ΔΙΕΘΝΕΣ ΠΑΝΕΠΙΣΤΗΜΙΟ ΕΛΛΑΔΟΣ

ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΑΣ ΚΑΙ ΔΙΟΙΚΗΣΗΣ

ΤΜΗΜΑ ΛΟΓΙΣΤΙΚΗΣ ΚΑΙ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΤΟ ΨΗΦΙΑΚΟ ΝΟΜΙΣΜΑ ΣΤΟΝ ΣΥΓΧΡΟΝΟ ΚΟΣΜΟ: ΤΟ ΠΡΩΙΜΟ ΙΣΤΟΡΙΚΟ ΤΟΥ BIT-COIN ΚΑΙ ΟΙ ΣΥΓΧΡΟΝΕΣ ΕΦΑΡΜΟΓΕΣ ΤΟΥ

Προπτυχιακή Διπλωματική Εργασία

Του

Ηλία Ταγγίρη

Που υποβάλλεται στο καθηγητικό σώμα του Διεθνούς Πανεπιστημίου Ελλάδος για την μερική εκπλήρωση των υποχρεώσεων απόκτησης του τίτλου σπουδών του τμήματος Λογιστικής και Πληροφοριακών Συστημάτων

Θεσσαλονίκη

Σεπτέμβριος, 2019

ΔΙΕΘΝΕΣ ΠΑΝΕΠΙΣΤΗΜΙΟ ΕΛΛΑΔΟΣ

ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΑΣ ΚΑΙ ΔΙΟΙΚΗΣΗΣ

ΤΜΗΜΑ ΛΟΓΙΣΤΙΚΗΣ ΚΑΙ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΤΟ ΨΗΦΙΑΚΟ ΝΟΜΙΣΜΑ ΣΤΟΝ ΣΥΓΧΡΟΝΟ ΚΟΣΜΟ: ΤΟ ΠΡΩΙΜΟ ΙΣΤΟΡΙΚΟ ΤΟΥ BIT-COIN ΚΑΙ ΟΙ ΣΥΓΧΡΟΝΕΣ ΕΦΑΡΜΟΓΕΣ ΤΟΥ

Προπτυχιακή Διπλωματική Εργασία

Του

Ηλία Ταγγίρη

Που υποβάλλεται στο καθηγητικό σώμα του Διεθνούς Πανεπιστημίου Ελλάδος για την μερική εκπλήρωση των υποχρεώσεων απόκτησης του τίτλου σπουδών του τμήματος Λογιστικής και Πληροφοριακών Συστημάτων

Θεσσαλονίκη

Σεπτέμβριος, 2019

ΔΙΕΘΝΕΣ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΟΝΙΚΗΣ

ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΑΣ ΚΑΙ ΔΙΟΙΚΗΣΗΣ

ΤΜΗΜΑ ΛΟΓΙΣΤΙΚΗΣ ΚΑΙ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΤΟ ΨΗΦΙΑΚΟ ΝΟΜΙΣΜΑ ΣΤΟΝ ΣΥΓΧΡΟΝΟ ΚΟΣΜΟ: ΤΟ ΠΡΩΙΜΟ ΙΣΤΟΡΙΚΟ ΤΟΥ BIT-COIN ΚΑΙ ΟΙ ΣΥΓΧΡΟΝΕΣ ΕΦΑΡΜΟΓΕΣ ΤΟΥ

Προπτυχιακή Διπλωματική Εργασία

Του

Ηλία Ταγγίρη

Που υποβάλλεται στο καθηγητικό σώμα του Διεθνούς Πανεπιστημίου Ελλάδος για την μερική εκπλήρωση των υποχρεώσεων απόκτησης του τίτλου σπουδών του τμήματος Λογιστικής και Πληροφοριακών Συστημάτων

Εγκεκριμένο από το Καθηγητικό σώμα:

Επιβλέπων καθηγητής: Ευστάθιος Κύρκος Υπογραφή: . . . . . .

Μέλος: . . . . . Υπογραφή: . . . . . .

Μέλος: . . . . . Υπογραφή: . . . . . .

Θεσσαλονίκη

Σεπτέμβριος, 2019

ΠΕΡΙΛΗΨΗ

Ηλίας Ταγγίρης: Το ψηφιακό νόμισμα στον σύγχρονο κόσμο: Το πρώιμο ιστορικό του Bit-coin και οι σύγχρονες εφαρμογές του.

Η εργασία εκπονήθηκε υπό την επίβλεψη του κ. Ευσταθίου Κύρκου, καθηγητή του τμήματος Λογιστικής και Πληροφοριακών Συστημάτων του Διεθνούς Πανεπιστημίου Ελλάδος.

Η παρούσα εργασία εστίασε στο πρόσφατα εφαρμοσμένο ψηφιακό νόμισμα του bit-coin, από την πρώτη εμφάνιση της ιδέας ενός πλήρως αποκεντρωμένου κρυπτογραφημένου συστήματος πληρωμών το 1982 από τον David Lee Chaum, έως την επιτυχή εφαρμογή της το 2008 από μία ομάδα προγραμματιστών, κρυμμένων πίσω από το διαδικτυακό ψευδώνυμο Satoshi Nakamoto, έως σήμερα. Βασισμένος σε έναν μεγάλο αριθμό άρθρων, βιβλιογραφικών αλλά και ειδησεογραφικών προκειμένου να παρακολουθήσω την πορεία και απήχησή του, παρακάτω θα αναφερθώ στην εμφάνιση της ιδέας του bitcoin αλλά και στην μετά-από-χρόνια επιτυχή εφαρμογή της. Η ακόλουθη εργασία περιγράφει την φύση του ψηφιακού νομίσματος του bit-coin αλλά και τον τρόπο με τον οποίο αυτό χρησιμοποιείται. Στα κεφάλαια που ακολουθούν θα αναλυθούν οι μέθοδοι αλλά και τα κριτήρια απόκτησης του ψηφιακού νομίσματος, ο τρόπος με τον οποίο πραγματοποιούνται οι συναλλαγές με αυτό, οι κίνδυνοι που ελλοχεύουν και το απειλούν αλλά και προτάσεις προσωπικής ασφάλειας, και τέλος η απήχησή του στον κόσμο και ο ρυθμός με τον οποίο υιοθετείται από όλο και περισσότερους χρήστες.

ABSTRACT

Ilias Tangiris: The digital coin in the modern world: The early history of Bit-coin and its modern applications.

This paper was carried out under the supervision of Mr. Efstathios Kykros, professor of Accounting and Data-Processing Systems at the International Hellenic University.

This work is focused on the recently-implemented digital currency of Bit-coin, since the first appearance of the idea of a fully decentralized encrypted payment system in 1982 by David Lee Chaum, until its successful implementation in 2008 by a group of developers whose identity is concealed, aside the pseudonym Satoshi Nakamoto, to date. Based on a large number of bibliographic and news articles in order to follow its course and impact, I will refer to the idea of bitcoin and its post-successful implementation. The following paper describes the nature of the digital coin of bit-coin and how it can be used. The following chapters will analyze the methods and criteria for acquiring the digital currency, the way in which transactions are completed, the underlying and threatening risks but also personal security proposals, and finally its impact on the world and the rate at which it is adopted by more and more users.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΕΙΣΑΓΩΓΗ

Ο άνθρωπος από την αρχαιότητα αντιμετώπισε την ανάγκη να βρει ένα κοινό μέσο συναλλαγής προκειμένου να έχει την δυνατότητα να παρέχει είτε να του παρέχονται υπηρεσίες και προϊόντα, λαμβάνοντας είτε προσφέροντας την αντίστοιχη ανταμοιβή. Περίπου 100.000 χρόνια πριν συναντάται η γνωστή σε όλους "ανταλλαγή προϊόντων", σύμφωνα με την οποία οι πληρωμές πραγματοποιούνταν σε είδος. Με διακριτές τις ατέλειες αυτής της μεθόδου, με ίσως σημαντικότερη την αδυναμία υποδιαιρετικότητας, δεν άργησε να εμφανισθεί η ιδέα ενός κοινά αποδεκτού νομίσματος που θα έδινε την λύση σε κάθε είδους συναλλαγή. Περίπου το 3.000 π. Χ. στην Μεσοποταμία, όστρακα και κοχύλια χρησιμοποιήθηκαν ως μέσο συναλλαγής, ενώ αργότερα, το 700 π. Χ. ο σίδηρος και στην συνέχεια ο χρυσός χρησιμοποιήθηκαν για να κατασκευαστούν τα πρώτα νομίσματα από τον Λύδιο βασιλιά Κροίσο. Το χειροπιαστό αυτό νόμισμα επικράτησε μέχρι και σήμερα και εξελίχθηκε, παίρνοντας την μορφή της Δραχμής, του Ευρώ, του Δολαρίου, του Φράγκου αλλά και άλλων που χρησιμοποιούνται σήμερα κατά μήκος όλου του κόσμου, με τη μορφή των νομισμάτων αλλά και των χαρτονομισμάτων. Με την ανάπτυξη της τεχνολογίας, νέες μέθοδοι πληρωμών έκαναν την εμφάνισή τους στον κόσμο των συναλλαγών με το πλαστικό χρήμα να κάνει το πρώτο βήμα στις ΗΠΑ το 1920 με την μορφή μιας ηλεκτρονικής κάρτας πληρωμών. Χρεωστικές, πιστωτικές και προπληρωμένες κάρτες γνώρισαν τεράστια επιτυχία τα επόμενα χρόνια λόγω της φορητότητας, πρακτικότητας αλλά και ασφάλειας που αυτές παρέχουν. Από την ανταλλαγή προϊόντων, στο υλικό χρήμα, και από τον χρυσό στο πλαστικό χρήμα των ηλεκτρονικών καρτών. Στην ακόλουθη εργασία θα μιλήσουμε για τον επόμενο και πιο σύγχρονο τρόπο πληρωμών, ο οποίος παρά την εμφάνισή του από τον 20ό κιόλας αιώνα μονάχα ως θεωρητική ιδέα, τέθηκε σε εφαρμογή την τελευταία δεκαετία και όντας λειτουργικός, γνώρισε τεράστια επιτυχία. Αναφερόμαστε στο νέο ψηφιακό και κρυπτογραφημένο νόμισμα του bit-coin. Παρά την εμφάνιση περισσοτέρων ψηφιακών νομισμάτων, το bit-coin ήταν το πρώτο λειτουργικό νόμισμα του είδους του και το πιο επιτυχημένο μέχρι σήμερα.

1. ΜΙΑ ΝΕΑ ΜΕΘΟΔΟΣ ΠΛΗΡΩΜΩΝ: Η ΥΛΟΠΟΙΗΣΗ ΑΛΛΑ ΚΑΙ Η ΕΦΑΡΜΟΓΗ ΤΗΣ

1.1 Ιστορική αναδρομή

"Το εμπόριο στο Διαδίκτυο βασίζεται σχεδόν αποκλειστικά σε χρηματοπιστωτικούς φορείς που λειτουργούν ως αξιόπιστα τρίτα μέρη για να επεξεργάζονται τις ηλεκτρονικές πληρωμές. Ενώ το σύστημα λειτουργεί αρκετά καλά για τις περισσότερες συναλλαγές, εξακολουθεί να πάσχει από τις εγγενείς αδυναμίες του μοντέλου που βασίζεται στην εμπιστοσύνη. Μη αναστρέψιμες συναλλαγές δεν είναι πραγματικά δυνατές, δεδομένου ότι τα χρηματοπιστωτικά ιδρύματα δεν μπορούν να αποφύγουν τη διαμεσολάβηση διαφορών. Το κόστος της διαμεσολάβησης αυξάνει το κόστος συναλλαγής, περιορίζει το ελάχιστο μέγεθος πρακτικής συναλλαγής και διακόπτει τη δυνατότητα για μικρές απλές συναλλαγές. Ένα ορισμένο ποσοστό απάτης είναι αναπόφευκτο. Αυτό το κόστος και η αβεβαιότητα πληρωμών μπορεί να αποφευχθεί αυτοπροσώπως χρησιμοποιώντας φυσικό νόμισμα, αλλά δεν υπάρχει μηχανισμός για την πραγματοποίηση πληρωμών μέσω ενός καναλιού επικοινωνιών. 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 κάποιος αξιόπιστος τρίτος."

-Satoshi Nakamoto

Η παραπάνω ιδέα διατυπώθηκε και δημοσιεύθηκε τον Οκτώβριο του 2008 από μία ομάδα προγραμματιστών, πίσω από το όνομα Satoshi Nakamoto. Η έννοια του κρυπτονομίσματος είχε κάνει την εμφάνισή της ακόμα πιο παλιά, και στρέφουμε τα βλέμματα στον David Lee Chaum, γεννημένο το 1955, Αμερικανό επιστήμονα πληροφορικής και κρυπτογράφο ο οποίος πρώτος μίλησε επίσημα για την πιθανή επιτυχία και σπουδαιότητα που μπορούσε να προσφέρει ένα ψηφιακό κρυπτογραφημένο νόμισμα μέσα από την εργασία του με τίτλο Blind Signatures For Untraceable Payments που δημοσιεύθηκε το 1982. Παρόλο που το επιτυχημένο σχέδιο του bitcoin που βλέπουμε σήμερα εξακολουθεί να εξελίσσεται, την εποχή εκείνη, λίγοι ήταν οι άνθρωποι που είχαν ασχοληθεί σε βάθος με την τεχνολογία και λειτουργία του δικτύου των ηλεκτρονικών υπολογιστών πλην του Chaum. Λέγεται πως μόνο μια χούφτα ανθρώπων μπορούσαν να κατανοήσουν την ιδέα του, και παρόλο που η ιστορία δείχνει πως -αν δεν ήταν σπουδαία- τουλάχιστον είχε προοπτικές, παρέμεινε στο παρασκήνιο για μερικά ακόμα χρόνια.

Η ιδέα του ψηφιακού νομίσματος αναζωπυρώθηκε ξανά το 1998 από τον Wei Dai, ικανό προγραμματιστή που ασχολήθηκε με την ηλεκτρονική κρυπτογραφία πριν συλλάβει την ιδέα του εναλλακτικού αυτού νομίσματος. Με την βοήθεια των συνεργατών του Adam Back και Harold Thomas Finney, επίσης προγραμματιστών και κρυπτογράφων, ο Wei Dai, παρόλο που δεν ολοκλήρωσε το σχέδιο του, εισήγαγε μία νέα πρωτοποριακή ιδέα στον κόσμο των ηλεκτρονικών υπολογιστών, η οποία ήταν θέμα χρόνου να ανθίσει. Εκατοντάδες ακόμα έγγραφα δημοσιεύθηκαν έκτοτε θίγοντας αυτό το ζήτημα, δραματική όμως εξέλιξη στην ιστορία αυτή σημειώθηκε το 2008, το έργο έγινε πραγματικότητα με την υπογραφή "Satoshi Nakamoto".

Ακόμα και σήμερα, παραμένει μυστήριο το ποιος πραγματικά κρύβεται πίσω από το όνομα Satoshi Nakamoto. Είναι επίσης άγνωστο το εάν με την έννοια αυτή αναφερόμαστε σε ένα άτομο, ή σε μία ομάδα προγραμματιστών, και το αν αυτό αποτελεί πραγματικό όνομα ή κάποιου είδους ψευδώνυμο. Σε ένα διαδικτυακό προφίλ ωστόσο με όνομα "Nakamoto", ο διαχειριστής του ισχυρίστηκε πως αποτελεί κάτοικο της Ιαπωνίας. Το μόνο που ξέρουμε για τον Nakamoto, είναι πως είχε τις απαραίτητες γνώσεις για να κάνει το ψηφιακό νόμισμα πραγματικότητα. Μάλιστα, σε ένα άρθρο που δημοσιεύθηκε το 2011 με τίτλο "Bitcoin, what took ye so long?", ο προγραμματιστής Nick Szabo δηλώνει πως αρχικά πίστευε πως μόνο εκείνος, ο Wei Dai και ο Harold Finney έδειχναν να γοητεύονται από την ιδέα αυτή, μέχρι που το 2008, προ εκπλήξεως, ήρθε σε επαφή μαζί τους ο Nakamoto, πρόθυμος να υλοποιήσει το έργο. Και απ'ότι φαίνεται τα κατάφερε. Τον Οκτώβριο του 2008, ο Nakamoto δημοσίευσε ένα άρθρο με τίτλο Bitcoin: A Peer-to-Peer Electronic Cash System στην ιστοσελίδα SourceForge (η οποία επιτρέπει την αποθήκευση κώδικα σε αυτήν, την διάγνωση λαθών αλλά και την δημοσίευσή του στους υπόλοιπους επισκέπτες), αναλύοντας μέσα σε αυτό το έργο του. Παρά την ανοδική πορεία του bitcoin, διατηρείται η πεποίθηση πως η ομάδα αυτή ήταν "πλαστή" καθώς το όνομα τους δεν ακούστηκε ξανά από τον Απρίλιο του 2011.

Σχεδόν αμέσως εγείρεται το ερώτημα της υπόστασης του bitcoin και του τι πραγματικά αποτελεί. Πρόκειται για ένα μέσο συναλλαγής, μα όχι για χρήμα το οποίο διαχειρίζεται μια τράπεζα ή κάποιος άλλος φορέας. Το Bitcoin είναι απόλυτα ψηφιακό και άυλο, και απλοϊκά θα λέγαμε πως αποτελεί μία πληροφορία, κρυμμένη μέσα στο υπολογιστικό δίκτυο (Nakamoto, 2008). Αυτού του είδους οι πληροφορίες είναι πεπερασμένες και βρίσκονται διασκορπισμένες στο διαδίκτυο, και οι χρήστες, ξοδεύουν υπολογιστική ισχύ προκειμένου να "αναζητήσουν" και να "εντοπίσουν" αυτές τις πληροφορίες. Στη συνέχεια οι χρήστες έχουν τη δυνατότητα να ανταλλάσουν τα bitcoin μεταξύ τους. Αυτό σημαίνει πως το bitcoin αποτελεί ένα μέσο συναλλαγής, καθώς ο κάθε χρήστης "Α" μπορεί να παρέχει προϊόντα ή υπηρεσίες στον χρήστη "Β", και αυτός αντίστοιχα να αμείβει τον "Α" με bitcoin.

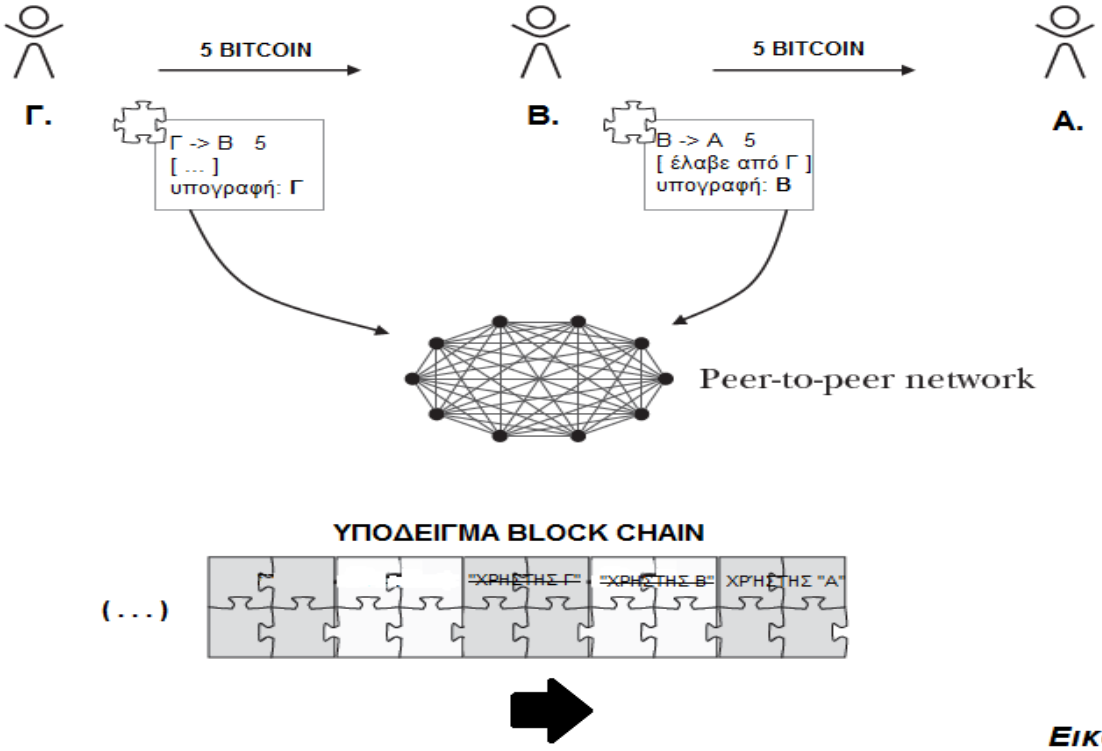
Ο Benjamin Wallace (2011) σχολιάζει το πρώιμο ιστορικό του bitcoin και δηλώνει ότι ο Nakamoto εξόρυξε και εισήγαγε τις πρώτες 50 μονάδες σε κυκλοφορία το 2009, κυρίως για να αποδείξει τη μέθοδο σε μια ομάδα διαδικτυακών παρατηρητών. Η κυκλοφορία του bitcoin πραγματοποιήθηκε αρχικά ανάμεσα σε εθελοντές και λάτρεις του κόσμου των υπολογιστών. Το ενδιαφέρον αυξήθηκε στο σημείο που το bitcoin άρχισε να κινείται το 2010 στην ιαπωνική εταιρία συναλλαγών bitcoin ονόματι Mt. Gox, η οποία είχε αρχικά δημιουργηθεί ως πλατφόρμα ανταλλαγής καρτών συναλλαγών από το παιχνίδι φαντασίας Magic. Την πρώτη ημέρα διαπραγμάτευσης στο Mt. Gox, 20 bitcoin άλλαξαν χέρια σε τιμή 4.951 σεντς, για συνολική αξία ελαφρώς μικρότερη από ένα δολάριο ΗΠΑ. Η πρώτη αγορά αγαθών και υπηρεσιών με bitcoin λέγεται από τον Wallace (2011) και άλλες πηγές πως αφορούσε δύο πίτσες με κόστος 10.000 bitcoin το 2009. Η επιχείρηση δεν δεχόταν άμεσα bitcoin, και αντίθετα ένας διαμεσολαβητής συμφώνησε να πουλήσει τις πίτσες χρησιμοποιώντας μια πιστωτική κάρτα και να δεχθεί τα bitcoin, σημερινής αξίας σχεδόν 50 εκατομμυρίων δολαρίων.

1.2 Η λειτουργία του Bitcoin

Το λογισμικό του bitcoin βασίζεται σε ένα Peer-to-Peer δίκτυο και μπορεί να ληφθεί δωρεάν από την σελίδα https://bitcoin.org/en/choose-your-wallet. Η έννοια του Peer-to-Peer αναφέρεται σε εκείνη την σχέση που αφορά μονάχα τα δύο ενδιαφερόμενα μέλη της συναλλαγής (αποστολέας και παραλήπτης) και δεν απαιτεί την ύπαρξη ενός τρίτου έμπιστου προσώπου, όπως μία τράπεζα, για την ολοκλήρωση μιας συναλλαγής. Άλλωστε η ιδέα του bitcoin σχηματίστηκε έχοντας στο στόχαστρο μια δυνατή συναλλαγή που βασίζεται σε ένα κρυπτογραφημένο σύστημα και όχι στην εμπιστοσύνη (Nakamoto, 2008). Το λογισμικό αυτό περιλαμβάνει μία μικρή λίστα από ορισμένα χαρακτηριστικά που επιτρέπουν και διευκολύνουν την χρήση του. Αρχικά, δημιουργεί ένα ψηφιακό "πορτοφόλι" για τον χρήστη, μέσα από το οποίο εκείνος μπορεί να διαχειρίζεται τα bitcoin του, χωρίς να είναι απαραίτητο να χρησιμοποιήσει το πραγματικό του όνομα ή κάποιο άλλο επίσημο έγγραφο ή πληροφορία για την ταυτοποίησή του. Με αυτό τον τρόπο δημιουργεί ένα διαδικτυακό προφίλ για τον χρήστη, για τη χρήση του οποίου είναι απαραίτητη η δυνατότητα σύνδεσης στο διαδίκτυο, και του παρέχει πρόσβαση στην "αλυσίδα συναλλαγών", γνωστή ως "block chain", ή οποία αποτελεί το ιστορικό όλων των συναλλαγών bitcoin.

Τα bitcoin εμφανίζονται ως συναλλαγές, και καθώς είναι εικονικά, δεν είναι εκφραστικά σωστό να πούμε πως κάποιος χρήστης (Α) έχει στην κατοχή του παράδειγμα 5 bitcoin. Αντιθέτως, ο Α συμμετέχει σε μία δημόσια συναλλαγή, που όπως είπαμε αποθηκεύεται στο block chain, η οποία δείχνει πως ο Α έχει λάβει τα 5 αυτά bitcoin από τον Β σε μία συγκεκριμένη χρονική στιγμή στο παρελθόν. Αντίστοιχα, ο Α, πριν λάβει τα bitcoin από τον Β, μπορούσε να δει και να επαληθεύσει πως ο Β είχε αυτά τα 5 bitcoin διαθέσιμα, καθώς τα έλαβε πρώτος από τον Γ, και πως τα bitcoin αυτά, δεν έχουν χρησιμοποιηθεί σε άλλη συναλλαγή. Αυτήν ακριβώς την μνήμη των κινήσεων όλων των bitcoin παρουσιάζει το block chain, στο οποίο μπορεί κανείς να δει όλες τις συναλλαγές που έγιναν με ένα συγκεκριμένο ή περισσότερα bitcoin, αναδρομικά, από την αρχή της δημιουργίας τους.

Το γεγονός αυτό σημαίνει πως ελέγχοντας την αλυσίδα, ο Α, μπορεί να αντιληφθεί πως τα bitcoin που έλαβε από τον Β, ανήκαν παλιά στον Γ, χωρίς όμως αυτό να δίνει καμία άλλη πληροφορία για τον Β ή τον Γ (ή και τους προηγούμενους κατόχους του bitcoin) πέραν του δημόσιου ονόματος τους, ενώ παράλληλα μπορεί να επαληθεύσει την εγκυρότητα της συναλλαγής και να μην αποτελέσει θύμα απάτης (εικόνα 1).



Εικόνα 1

Σκίτσο 1

Το bitcoin βασίζεται σε δύο βασικές τεχνολογίες κρυπτογράφησης: στην κρυπτογράφηση του δημόσιου-ιδιωτικού κλειδιού για την αποθήκευση των bitcoin, και στην επικύρωση των συναλλαγών. Η πρώτη επιτρέπει στους χρήστες να δημιουργήσουν ένα δημόσιο κλειδί, το οποίο είναι συσχετισμένο με ένα ιδιωτικό. Το πρώτο, είναι εμφανές σε όλους τους χρήστες, σε αντίθεση με το δεύτερο. Είναι δυνατό δηλαδή να αποσταλούν κρυπτογραφημένα μηνύματα έχοντας "δεσμεύσει" το δημόσιο κλειδί, και για την αποκρυπτογράφησή τους απαιτείται το αντίστοιχο ιδιωτικό, διασφαλίζοντας έτσι πως μόνο ο συγκεκριμένος χρήστης ή αλλιώς ο επιθυμητός παραλήπτης θα μπορεί να διαβάσει το μήνυμα. Με ακριβώς τον αντίστροφο τρόπο, ένας χρήστης έχει τη δυνατότητα να κρυπτογραφήσει ένα μήνυμα με το ιδιωτικό του κλειδί. Αυτό το μήνυμα είναι δυνατό να αποκρυπτογραφηθεί με το δημόσιό του κλειδί, το οποίο είναι ορατό σε όλους τους χρήστες. Με αυτόν τον τρόπο επιβεβαιώνεται η αυθεντικότητα και η εγκυρότητα του μηνύματος, για παράδειγμα στην μεταφορά bitcoin όπου επιβεβαιώνεται τόσο ο παραλήπτης όσο και ο αποστολέας.

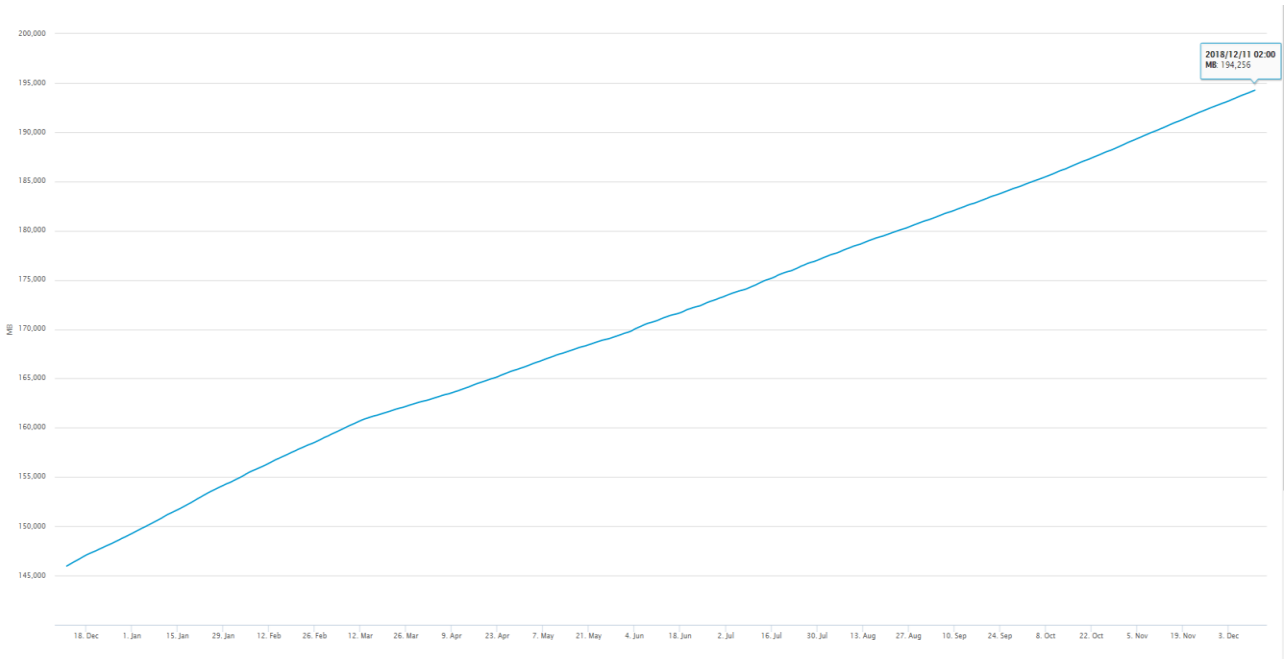
Μπορούμε να παρομοιάσουμε τις έννοιες του δημοσίου και ιδιωτικού κλειδιού, με αυτές του "username" και του "password" αντίστοιχα. Αυτό σημαίνει πως το δημόσιο κλειδί είναι η διαδικτυακή ταυτότητα του χρήστη, η πληροφορία εκείνη που απαιτείται για να τον εντοπίσει κάποιος άλλος χρήστης και να του στείλει τα bitcoin, ενώ το ιδιωτικό κλειδί εκείνο που προσφέρει την δυνατότητα της διαχείρισης των bitcoin του συγκεκριμένου χρήστη. Μπορούμε να συσχετίσουμε την περίπτωση αυτή με μία διεύθυνση ηλεκτρονικού ταχυδρομείου. Αυτή αποτελείται από ένα username και ένα password. Το username μας είναι ορατό σε όλους τους χρήστες καθώς είναι απαραίτητο για να μπορέσει κάποιος να επικοινωνήσει μαζί μας, και αυτή είναι η αποκλειστική λειτουργία του δημοσίου κλειδιού, γι'αυτό και είναι ορατό σε όλους. Το password μας από την άλλη, ή αλλιώς το ιδιωτικό μας κλειδί παρέχει την δυνατότητα να διαβάσει κάποιος όλα τα e-mail μας και να προωθήσει πληροφορίες, και για τον αντίστοιχο λόγο είναι ιδιωτικό και αυστηρά προσωπικό.

Εάν υποθέσουμε ότι ο Γ θέλει να στείλει 5 bitcoin στον Β, θα ακολουθήσει την εξής διαδικασία: θα δημοσιεύσει ένα μήνυμα στο δίκτυο συναλλαγών του bitcoin, στο οποίο θα συμπεριλάβει τις εξής πληροφορίες: θα ενημερώνει πως θα μεταφέρει 5 από τα bitcoin του στον Β, ενώ παράλληλα θα επισυνάψει μια συντόμευση για την συναλλαγή στο block chain κατά την οποία έλαβε τα bitcoin αυτά στο παρελθόν από τον προηγούμενο κάτοχο. Έπειτα, θα κρυπτογραφήσει ένα μέρος του μηνύματος αυτού με το ιδιωτικό του κλειδί, ώστε η κοινότητα του bitcoin να μπορεί να επαληθεύσει την ταυτότητά του ανοίγοντας το μήνυμα με το δημόσιό του κλειδί. Με τη σειρά του ο Β, όταν στείλει τα 5 bitcoin στον Α, θα κρυπτογραφήσει το μήνυμα με το ιδιωτικό του κλειδί, θα συμπεριλάβει την "αναφορά" στην απόκτηση των 5 bitcoin αυτών από τον Γ, και το υπόλοιπο δίκτυο θα μπορεί να επιβεβαιώσει την εγκυρότητα του μηνύματος, πάλι με το εμφανές σε όλους δημόσιό του κλειδί.

Κάθε νέα συναλλαγή λοιπόν δημοσιεύεται στο δίκτυο και στη συνέχεια ομαδοποιείται μαζί με άλλες δημιουργώντας ένα “block of transactions”, η αλλιώς έναν νέο κρίκο ο οποίος πρόκειται να ενταχθεί στην αλυσίδα. Για να σιγουρευτεί πως δεν εισάγεται στην αλυσίδα μια μη-επιβεβαιωμένη συναλλαγή, η αλυσίδα ελέγχει και συγκρίνει τον εαυτό της με ένα πρόσφατο αντίγραφό της, και καθώς νέα κομμάτια (blocks) εισάγονται στην αλυσίδα ανά περίπου δέκα λεπτά (Nakamoto, 2008), κάθε χρήστης μπορεί να επιβεβαιώσει ανά πάσα στιγμή εάν μια συναλλαγή πραγματοποιήθηκε ή όχι.

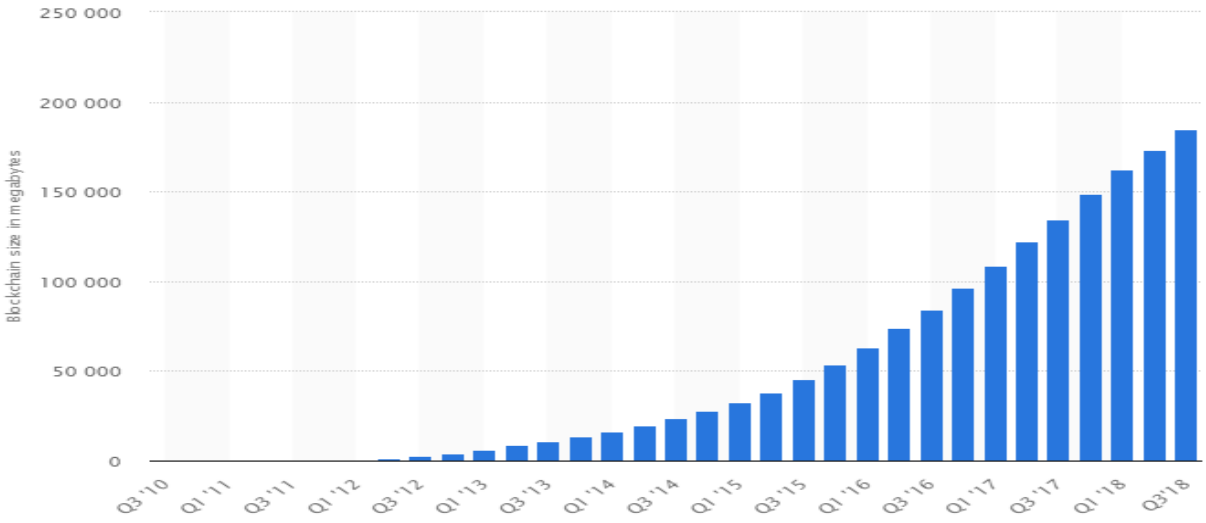
Τόσο για την χρήση για συναλλαγές, όσο και για την επαλήθευση των ήδη υπαρχουσών, απαραίτητη είναι η πρόσβαση του χρήστη στο block chain. Η σύνδεσή του πραγματοποιείται με την βοήθεια των “ψηφιακών πορτοφολιών” (digital wallets) τα οποία περιλαμβάνουν λογαριασμούς χρηστών, αποθηκευμένες συναλλαγές και ιδιωτικά κλειδιά. Υπάρχουν και πιο εξειδικευμένα λογισμικά που χρησιμοποιούνται σήμερα εξυπηρετώντας τον σκοπό του πορτοφολιού, όπως το Armory, το Electrum και το Hive. Ωστόσο πολλοί χρήστες δεν βρίσκουν την μέθοδο αυτή ιδιαίτερα ελκυστική καθώς το λογισμικό είναι δύσκολο να εγκατασταθεί και έχει αρκετές τεχνικές απαιτήσεις, όπως την αποθήκευση ολόκληρου του block chain, το οποίο έχει μέγεθος 189,703125 GB (11/12/2018). Παρόλο που η αποθήκευσή του δεν είναι απαραίτητη, η ορθή λειτουργία του συστήματος βασίζεται σε αυτήν.

Το μέγεθος του block chain σε MB το τελευταίο έτος:



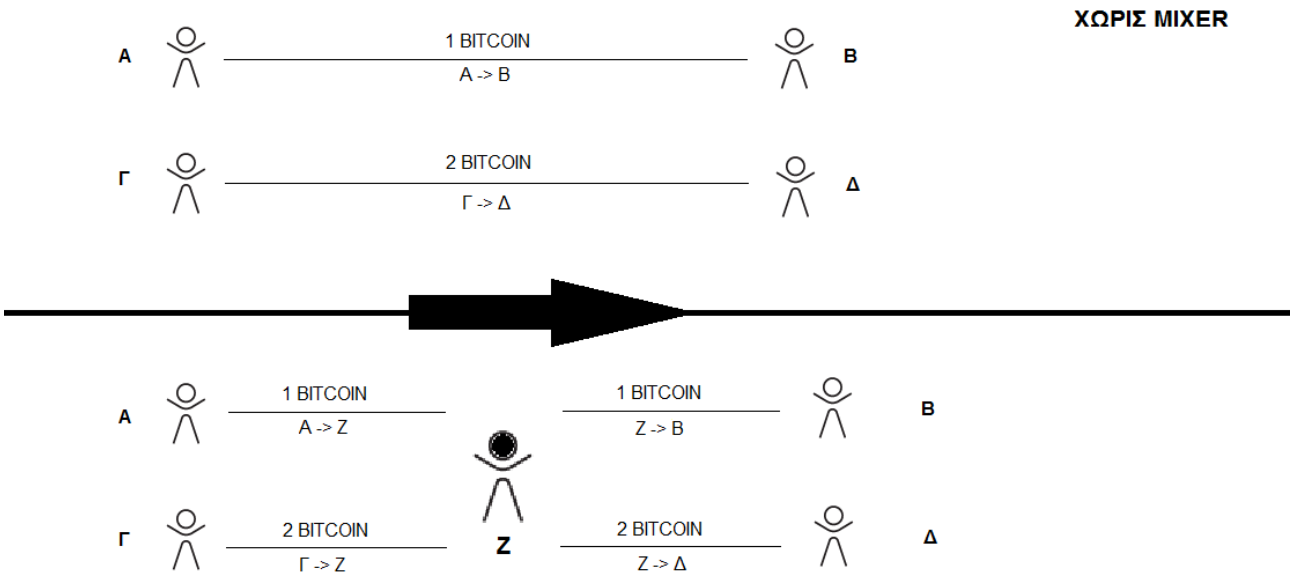
Πηγή: https://www.blockchain.com/charts

το μέγεθος του block chain σε MB από την αρχή της δημιουργίας του:



Πηγή: https://www.blockchain.com/charts

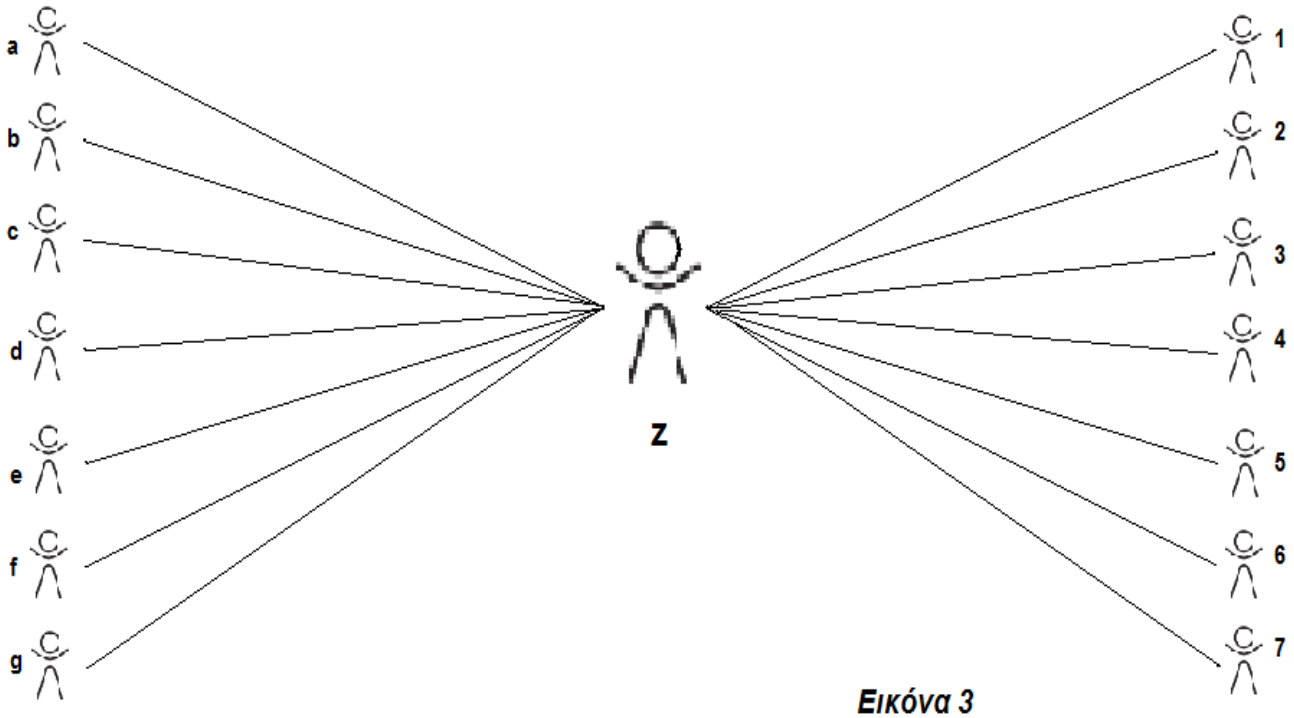
Όπως αναφέρθηκε προηγουμένως, κάθε συναλλαγή στο δίκτυο του bitcoin είναι ανώνυμη καθώς ο κάθε χρήστης "κρύβεται" πίσω από το δημόσιό του κλειδί. Στο block chain καταχωρείται η κάθε συναλλαγή με τα δημόσια κλειδιά των δύο μερών που συμμετείχαν, εμφανίζοντας μονάχα το ψευδώνυμο του καθενός. Παρόλο που είναι αδύνατον να γίνει γνωστή η ταυτότητα του χρήστη, είναι δυνατόν, χρησιμοποιώντας το ψευδώνυμο αυτό, να ανατρέξει κανείς στο block chain και να εντοπίσει όλες τις συναλλαγές που έγιναν από και προς το συγκεκριμένο χρήστη περιμένοντας για μίαν αδυναμία του συστήματος για την ταυτοποίησή του. Προκειμένου να επιτευχθεί η μέγιστη δυνατή ανωνυμία, εντοπίζουμε πλέον στο δίκτυο του bitcoin τα mixers. Οι εταιρείες που παρέχουν υπηρεσίες mixer, με ίσως πιο δημοφιλείς τις BestMixer, PrivCoin, Bitcoin Blender, CryptoMixer και Bitcoin Fog αντιμετωπίζουν αυτή την αδυναμία, παίρνοντας ένα σύνολο συναλλαγών και διεκπεραιώνοντάς τες οι ίδιες για να "χαθούν" τα βήματα των bitcoin από τους χρήστες στο block chain. Αυτό συμβαίνει ως εξής: Ας υποθέσουμε ότι ο Α θέλει να μεταφέρει ένα (1) Bitcoin στον Β, και ο Γ θέλει αντίστοιχα να μεταφέρει δύο (2) bitcoin στον Δ. Εάν οι συναλλαγές οποιουδήποτε από αυτούς τους τέσσερις παρακολουθούνται, θα είναι εμφανή στην αλυσίδα τα βήματα των συναλλαγών των χρηστών. Εάν ωστόσο τοποθετήσουμε στη μέση έναν μεσάζοντα ο οποίος λαμβάνει τα bitcoin τόσο από τον Α όσο και από τον Γ, και στη συνέχεια τα μεταφέρει ο ίδιος στον Β και Δ, θα είναι άγνωστη η πηγή προέλευσης και αδύνατο να συσχετιστεί ο Α με τον Γ και ο Β με τον Δ.



Εικόνα 2

Σκίτσο 2

Στην δεύτερη περίπτωση, ο Ζ αναλαμβάνει να μεταφέρει τα bitcoin στους ίδιους παραλήπτες, και παρόλο που το αποτέλεσμα είναι οπτικά το ίδιο, ένας παρατηρητής θα μπορούσε να αντιληφθεί πως ο Β έλαβε 1 bitcoin μέσω ενός mixer, μα δεν θα μπορούσε να ξέρει εάν αυτό προέρχεται από τον Α ή τον Γ (εικόνα 2). Με ακριβώς τον ίδιο τρόπο θα ήταν αδύνατο να αντιληφθεί εάν το bitcoin του Α προοριζόταν για τον Β ή τον Δ. Η μέθοδος αυτή είναι αποτελεσματική και ακόμα πιο σύνθετη, εάν σκεφτούμε πως ο Ζ αναλαμβάνει την μεταφορά από πολλούς περισσότερους από δυο αποστολείς/παραλήπτες (εικόνα 3).



Εικόνα 3

Σκίτσο 3

Ακόμα και με αυτή τη μέθοδο θα έλεγε κανείς πως υπάρχει ένα μικρό ψεγάδι, μιαν αδυναμία που θα μπορούσε πάλι να ωφελήσει έναν εξωτερικό παρατηρητή. Στο παραπάνω σχήμα, εάν ο Α μεταφέρει 4 bitcoin στον Z, μέσω το οποίου αυτά μεταφερθούν σε έναν χρήστη από την απέναντι ομάδα, ο παρατηρητής θα αρκούσε να ελέγξει τις παραλαβές τους ώστε να διαπιστώσει ποιος από αυτούς έλαβε το αντίστοιχο ποσό, μιας και οι πιθανότητες για συναλλαγές των ίδιων ποσών δεν είναι ιδιαίτερα πιθανές. Ανοικτό είναι ωστόσο το ενδεχόμενο, ο Α να μεταφέρει 4 bitcoin στον Z, εκ των οποίων τα 3 προορίζονται για το No.6 και το τελευταίο 1 για το No.7 . Σε μιαν αγορά όπου ακόμα περισσότεροι χρήστες συναλλάσσονται μέσω ενός mixer, αυτού του είδους οι διανομές είναι ακόμα περισσότερες και παρέχουν μιαν απόλυτη λύση στο παραπάνω ζήτημα, φέρνοντας τυχόν κακόβουλες σκοπιμότητες ενός τρίτου σε αδιέξοδο. Ή χρήση του mixer στις συναλλαγές, κοστολογείται με ποσοστά 1% έως και 3% επί του ποσού της μεταφοράς.

1.3 Digital Wallets

Το ψηφιακό πορτοφόλι αποτελεί ένα προϊόν λογισμικού μέσα από το οποίο διαχειριζόμαστε τα bitcoin μας. Το κάθε πορτοφόλι αποθηκεύει το δημόσιο και το ιδιωτικό κλειδί του χρήστη, τις πληροφορίες δηλαδή που χρειάζονται για να έχει αυτός πρόσβαση στα ψηφιακά του νομίσματα. Με την πάροδο του χρόνου, εμφανίστηκαν πολλά πορτοφόλια που λειτουργούν με αντίστοιχο τρόπο, ανταποκρινόμενα όμως απόλυτα στις πιο συγκεκριμένες πλέον ανάγκες του χρήστη, δίνοντας λύση σε ερωτήματα, τυχόν δυσλειτουργίες, πρακτικά ζητήματα και θέματα ασφαλείας. Το πλήθος των πορτοφολιών, έχουμε τη δυνατότητα να το χωρίσουμε σε δύο ευρείες κατηγορίες: Hot Storage και αντίστοιχα Cold Storage (Antonopoulos, 2015).

Η έννοια του Hot Storage αναφέρεται σε εκείνα τα πορτοφόλια τα οποία είναι διαρκώς συνδεδεμένα με το διαδίκτυο. Τα πορτοφόλια αυτά που χωρίζονται με τη σειρά τους σε τέσσερις διακριτές ομάδες, παρέχουν στον χρήστη τη δυνατότητα γρήγορης και άμεσης πρόσβασης στα ψηφιακά του νομίσματα προσφέροντας τη δυνατότητα πρόσβασης ακόμα και από διαφορετικές συσκευές. Ωστόσο, τα πορτοφόλια αυτά, παρά τις ευκολίες που παρέχουν, είναι επίσης επικίνδυνα και σε έναν σχετικά υψηλό βαθμό εκτεθειμένα σε επιθέσεις hacking (Antonopoulos, 2015).

A. Web / Cloud Wallets

Τα πορτοφόλια αυτά είναι αποθηκευμένα στο διαδίκτυο και προσφέρουν ταχύτατη πρόσβαση από τον χρήστη, ακόμα και από διαφορετικές συσκευές. Αντιμετωπίζουν ωστόσο το ρίσκο του εκτεθειμένου ιδιωτικού κλειδιού, το οποίο είναι ευάλωτο σε κυβερνοεπιθέσεις καθώς είναι αποθηκευμένο επίσης στο διαδικτυακό μας προφίλ.

B. Desktop Wallets

Αυτά με τη σειρά τους, λειτουργούν με την χρήση προγραμμάτων που εγκαθιστώνται στον σταθερό ή φορητό μας υπολογιστή. Πρόσβαση σε αυτά έχουμε απευθείας από την αντίστοιχη συσκευή καθώς τα κλειδιά μας αποθηκεύονται στον σκληρό δίσκο της. Τα πορτοφόλια αυτά παρόλο που είναι πολύ ασφαλέστερα από τα προηγούμενα, είναι επίσης δυνατό να παραβιαστούν από malware και άλλο κακόβουλο λογισμικό που ελλοχεύει στο διαδίκτυο. Καθώς το πορτοφόλι είναι αποθηκευμένο στον σκληρό μας δίσκο, απώλεια, αλλοίωση ή καταστροφή του θα επιφέρει επίσης απώλειά του. Χαρακτηριστικά παραδείγματα τέτοιων πορτοφολιών είναι τα Exodus και Jaxx.

C. Mobile Wallets

Τα Mobile Wallets λειτουργούν με τον ίδιο τρόπο με τα Desktop Wallets, και υποστηρίζονται από Android και iOS φορητές συσκευές που βασίζονται στην αντίστοιχη εφαρμογή που αποθηκεύει το πορτοφόλι στην μνήμη της συσκευής. Μάλιστα σε αυτές τις περιπτώσεις, η εφαρμογή είναι αρκετά πιο ελαφριά καθώς αποθηκεύει μόνο ένα μέρος του Block Chain και όχι ολόκληρη την αλυσίδα. Οι κίνδυνοι είναι αντίστοιχα διαδικτυακοί κυρίως, και η ακεραιότητα της συσκευής. Χαρακτηριστικά ονόματα ορισμένων Mobile Wallets, είναι τα Breadwallet και Electrum.

D. Multi-signature Wallets

Όπως μαρτυρά και το όνομά τους, τα πορτοφόλια αυτά απαιτούν περισσότερες υπογραφές για να πραγματοποιήσουν μια συναλλαγή και λειτουργούν όπως ένας λογαριασμός τραπέζης με πολλούς δικαιούχους. Ο καθένας τους έχει πρόσβαση στο λογαριασμό, όπως και στη δικιά μας περίπτωση υπάρχει ένας αριθμός κλειδιών που παρέχουν πρόσβαση στο πορτοφόλι. Αυτά τα πορτοφόλια είναι λιγότερο πρακτικά μα πιο ασφαλή καθώς δημιουργούν μια δικλείδα ασφαλείας σε περίπτωση απώλειας του κλειδιού μας.

Στην δεύτερη μεγάλη κατηγορία των ψηφιακών πορτοφολιών έχουμε το Cold Storage. Η βασική διαφορά του από το Hot Storage, είναι πως σε αυτή την περίπτωση δεν είναι απαραίτητη η σύνδεση στο διαδίκτυο για την αποθήκευση ψηφιακών νομισμάτων. Στο Cold Storage μειώνεται η πρακτικότητα για συχνές συναλλαγές μα αυξάνεται η ασφάλεια δραστικά (Antonopoulos, 2015). Εδώ συνήθως αποθηκεύονται τα ψηφιακά νομίσματα τα οποία θα διατηρηθούν για ένα χρονικό διάστημα και δεν χρησιμοποιούνται τακτικά. Οι κίνδυνοι είναι και εδώ υπαρκτοί, μα διαφορετικοί και περιορισμένοι κυρίως στο ανθρώπινο λάθος

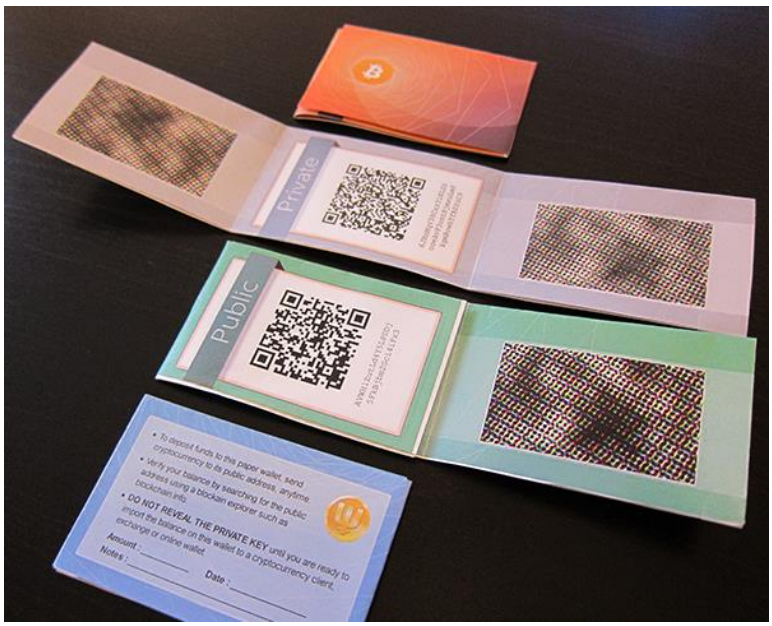
A. Hardware Wallets

Αναφερόμαστε πλέον σε συσκευές που εξυπηρετούν τον ρόλο του off-line πορτοφολιού, με χαρακτηριστικότερο παράδειγμα το USB stick, το οποίο έχει αποθηκευμένα στη μνήμη του τα bitcoin και με τη σύνδεση του στον υπολογιστή και παρέχοντας πρόσβαση στο διαδίκτυο, έχουμε τη δυνατότητα να τα χρησιμοποιήσουμε. Μεγαλύτερος κίνδυνος σε αυτά είναι η ακεραιότητα της συσκευής. Το Ledger Nano S και το Trezor αποτελούν δύο διάσημα Hardware Wallets.

Πηγή: https://www.buybitcoinworldwide.com/wallets/ledger-nano-s/

B. Paper Wallets

Ίσως ο πιο απλοϊκός και ασφαλέστερος τύπος πορτοφολιού. Μέσω προγραμμάτων έχουμε τη δυνατότητα να δημιουργήσουμε το δικό μας QR code το οποίο δημιουργείται τυχαία και αντιστοιχεί με το ιδιωτικό και δημόσιο μας κλειδί. Μια σελίδα χαρτί λοιπόν αποτελεί το κλειδί για την πρόσβαση στο ψηφιακό μας πορτοφόλι, παρόλα αυτά πρόκειται για μια εκτεθειμένη σελίδα χαρτιού στο περιβάλλον και είναι δυνατό να αλλοιωθεί ή καταστραφεί.



Πηγή: https://walletgenerator.net/

Ο μεγαλύτερος κίνδυνος της ακεραιότητας του πορτοφολιού μας βρίσκεται στο διαδίκτυο. Προκειμένου να διαχειριστούμε τα bitcoin μας είναι απαραίτητο να συνδεθούμε σε αυτό. Αυτό σημαίνει πως τα βασισμένα στο cold-storage πορτοφόλια είναι και αυτά πιθανό να παραβιαστούν το συγκεκριμένο εκείνο χρονικό διάστημα που τα χρησιμοποιούμε μα ο χρόνος αυτός είναι περιορισμένος σε σχέση με την συνεχή σύνδεση των hot-storage και για αυτό θεωρούνται πολύ πιο ασφαλή (Antonopoulos, 2015).

1.4 Ηλεκτρονικές Συναλλαγματικές Αγορές

Τα ψηφιακά πορτοφόλια είναι απολύτως λειτουργικά και ποικίλουν για να ανταποκριθούν στις διαφορετικές ανάγκες των χρηστών. Ο καθένας διαχειρίζεται τα Bitcoin του μέσα από το πορτοφόλι του και έχει τη δυνατότητα να τα στείλει σε κάποιον άλλο χρήστη ή αντίστοιχα να τα λάβει ανώνυμα, πίσω από το δημόσιο κλειδί του, ενώ μπορεί να βασιστεί στο block chain, το οποίο επιβεβαιώνει την εγκυρότητα της ύπαρξης του bitcoin, της προέλευσής του και στην συνέχεια της μεταφοράς του (Nakamoto, 2008). Όταν όμως κάποιος θέλει να αγοράσει ή να πουλήσει τα bitcoin του και όχι απλά να τα μεταφέρει η διαδικασία γίνεται λίγο πιο σύνθετη και απαιτεί την ύπαρξη ενός μεσάζοντα ο οποίος θα αναλάβει τον ρόλο του χρηματιστή. Την ευκαιρία αυτή άδραξαν πολλές εταιρείες που πλέον διαχειρίζονται διαδικτυακά αυτού του είδους τις συναλλαγές. Ηλεκτρονικά λοιπόν, μέσω αυτής της πλατφόρμας συναλλαγών, ο χρήστης έχει τη δυνατότητα να πουλήσει τα bitcoin του σε άλλους χρήστες ή να αγοράσει μερικά από άλλους. Οι σελίδες αυτές λειτουργούν με τον αντίστοιχο τρόπο του χρηματιστηρίου. Απαραίτητη ωστόσο για την σύνδεση σε αυτές τις ηλεκτρονικές αγορές, είναι η χρήση ορισμένων προσωπικών στοιχείων του χρήστη. Αυτά εξακολουθούν να παραμένουν κρυφά από τρίτους μα είναι απαραίτητα για την ταυτοποίησή του και για την ολοκλήρωση των συναλλαγών που πρόκειται να πραγματοποιήσει.

Οι αγορές και οι πωλήσεις στις περισσότερες ηλεκτρονικές συναλλαγματικές αγορές είναι δυνατόν να πραγματοποιηθούν με τρεις διαφορετικούς τρόπους:

Α. Ο χρήστης συνδέει έναν τραπεζικό του λογαριασμό με την ηλεκτρονική αγορά, στον οποίο βασίζονται οι συναλλαγές που θα πραγματοποιήσει. Σε αυτή την περίπτωση, οι συναλλαγές ολοκληρώνονται μέσα σε 4 με 5 ημέρες, ωστόσο η τιμή της συναλλαγής παραμένει σταθερή παρά την διακύμανση στην τιμή του ψηφιακού νομίσματος. Η αξία δηλαδή είναι ίδια με εκείνη την τιμή, όπως αυτή ορίστηκε στον χρόνο της συναλλαγής και όχι στον χρόνο της ολοκλήρωσής της.

Β. Ο χρήστης έχει τη δυνατότητα να συνδέσει την χρεωστική ή πιστωτική κάρτα του με την Ηλεκτρονική Αγορά προκειμένου τα χρήματα να κινούνται από και προς την συγκεκριμένη κάρτα. Πολλές από τις ήδη υπάρχουσες Ηλεκτρονικές Αγορές ωστόσο υποστηρίζουν μονάχα κάρτες MasterCard και Visa.

Γ. Ο χρήστης έχει τη δυνατότητα να διατηρήσει ένα ποσό της επιλογής του δεσμευμένο στον λογαριασμό του στην ηλεκτρονική αγορά προκειμένου να το χρησιμοποιήσει άμεσα στην επόμενη συναλλαγή του. Το ποσό αυτό είναι δυνατό να "τραβηχτεί" ανά πάσα στιγμή με τους παραπάνω δύο τρόπους.

Αυτή είναι μια διαδικασία που πραγματοποιείται από τις ηλεκτρονικές αγορές. Έχοντας συνδέσει έναν τραπεζικό λογαριασμό ή μία κάρτα, ο κάθε χρήστης έχει την δυνατότητα να συναλλάσσεται με την πλατφόρμα αυτή και να πουλάει ή να αγοράζει bitcoin για το αντίστοιχο χρηματικό ποσό. Γνωστές σελίδες που αναλαμβάνουν αυτόν τον ρόλο είναι οι CoinBase, Hive, Kraken, Cex.10, ShapeShift, CoinMama, Poloniex, CoinStamp και Bisq. Η κάθε ηλεκτρονική αγορά θέτει ποσοστά τόκων για τις υπηρεσίες που προσφέρει καθώς κατακρατείται το 1% με 4% του ποσού της συναλλαγής. Το ποσοστό αυτό εξαρτάται από το ποσό αλλά και το είδος της συναλλαγής και συνήθως είναι μεγαλύτερο όταν επιθυμείται η πώληση έναντι της αγοράς bitcoin. Όταν ο χρήστης Α πουλάει ένα bitcoin στην ηλεκτρονική αγορά, λαμβάνει ως αντάλλαγμα την τότε αξία του Bitcoin σε Ευρώ ή δολάρια, μείον ένα μικρό ποσό που αποτελεί τον τόκο της συναλλαγής. Η ίδια η αγορά στην συνέχεια, αναζητά έναν πιθανό αγοραστή του bitcoin αυτού, προσφέροντάς το για μίαν αξία λίγο μεγαλύτερη της πραγματικής της καθώς υπολογίζεται και πάλι ο τόκος (εικόνα 4).

Εικόνα 4

Σκίτσο 4

Οι Ηλεκτρονικές Αγορές εκτελούν αυτή την διαδικασία ασταμάτητα από την αρχή της δημιουργίας τους, καθώς την ίδια στιγμή που ο χρήστης πουλάει το bitcoin του στην αγορά, αυτή αρχίζει να αναζητά αγοραστές. Το κέρδος της πλατφόρμας για την παροχή αυτών των υπηρεσιών πηγάζει από δύο διαφορετικούς παράγοντες, τους τόκους και την πιθανή άνοδο στην αξία του νομίσματος:

Α. Η τιμή των bitcoin διαμορφώνεται με βάση την ζήτησή του, και αυτό έχει ως αποτέλεσμα την συνεχή διακύμανσή της. Εάν η Ηλεκτρονική αγορά προλάβει να αγοράσει και έπειτα να πουλήσει ένα Bitcoin για την ίδια ακριβώς αξία, τότε το κέρδος της εντοπίζεται στον τόκο που κράτησε τόσο από τον πωλητή όσο και από τον αγοραστή. Παρόλο που το ποσό αυτό είναι μικρό αρκεί να λάβουμε υπόψιν το πλήθος των συναλλαγών που πραγματοποιούν καθημερινά αυτές οι εταιρείες.

Β. Υπάρχει ωστόσο και ένας δεύτερος παράγοντας κερδοφορίας, ο οποίος αν και δεν είναι απόλυτα ασφαλής ή αξιόπιστος, έχει την προοπτική να εκτοξεύσει τα κέρδη αυτών των εταιρειών, ή ακόμα και ιδιωτών που έχουν την δυνατότητα να πάρουν το ρίσκο. Αυτό συναντάται σε εκτιμήσεις μιας πιθανής αύξησης της τιμής των bitcoin στην αγορά, καθώς σε ένα τέτοιο σενάριο το κέρδος θα βρίσκεται στην διαφορά στην τότε με την τώρα αξία του. Η μέθοδος αυτή όμως μπορεί να στραφεί και εναντίον του χρήστη ή της αγοράς, εάν εξετάσουμε ένα αντίθετο σενάριο στο οποίο η τιμή του bitcoin πέσει κατακόρυφα.

Για να αντιμετωπίσουν τέτοιες καταστάσεις με απρόβλεπτες και μεγάλες μεταβολές στην τιμή του κρυπτονομίσματος, πολλές εταιρείες Αγορών υιοθετούν μία ενδιάμεση πρακτική λύση. Δεν πωλούν τα bitcoin, μα προχωρούν σε μίαν διαδικασία δανεισμού με χρονικό περιορισμό. Αυτό σημαίνει, πως ο χρήστης Α, θα αγοράσει από την πλατφόρμα Ζ ένα bitcoin και θα έχει τη δυνατότητα να το διαχειρίζεται για παράδειγμα για δέκα (10) ημερολογιακές ημέρες. Με το πέρας των δέκα ημερών, το bitcoin αυτό θα πωληθεί αυτόματα στην εταιρεία και ο χρήστης θα λάβει την τότε αξία του, είτε αυτή είναι μεγαλύτερη, είτε είναι μικρότερη (συνυπολογίζεται και ο αντίστοιχος τόκος). Με άλλα λόγια ο χρήστης έχει στην διάθεσή του δέκα μέρες για να εκμεταλλευτεί το bitcoin, και μπορεί να το πουλήσει και νωρίτερα από τις δέκα ημέρες, εάν αυτό τον συμφέρει. Εάν το bitcoin επιστραφεί στην εταιρεία πριν τις δέκα ημέρες, το χρονικό περιθώριο δεν επηρεάζει πλέον τον χρήστη, και αυτός αντίστοιχα μπορεί να προβεί σε έναν νέο "δανεισμό". Εάν όμως για οποιονδήποτε λόγο ο χρήστης κρατήσει το bitcoin, για παράδειγμα επειδή παρατηρεί μια πτώση στην τιμή του, σε δέκα ημέρες, αυτό αυτόματα θα επιστρέψει στην εταιρεία. Με την μέθοδο αυτή οι Ηλεκτρονικές Αγορές προστατεύουν τον εαυτό τους από τυχόν ραγδαίες πτώσεις στην τιμή των κρυπτονομισμάτων.

2. ΔΙΑΔΙΚΤΥΑΚΟΙ ΚΙΝΔΥΝΟΙ, ΠΡΟΤΑΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΝΟΜΙΚΗ ΥΠΟΣΤΑΣΗ ΤΟΥ ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΟΣ

2.1 Ασφάλεια και Κίνδυνοι

Παρόλο που το bitcoin αλλά και άλλα γνωστά ψηφιακά νομίσματα είναι ιδιαίτερα πρακτικά και υποστηρίζεται από πολλούς οικονομολόγους (Wallace, 2011; Hurlburt & Bojanova, 2011) πως είναι δυνατό να αντικαταστήσουν το σημερινό χρήμα, σύμφωνα με τον Reuben Grinberg (2011) το μεγαλύτερο μέρος του πληθυσμού δεν είναι διατεθειμένο να στραφεί προς αυτά. Ο Grinberg υποστηρίζει πως αυτή η απόρριψη πηγάζει ως επί το πλείστον από πιθανές φοβίες για το νόμισμα αυτό, που προκύπτουν από την άγνοια και την έλλειψη τεχνογνωσίας. Πολλοί άνθρωποι υποστηρίζουν πως είναι πιο ασφαλές να διαχειρίζονται τα χρήματα μέσα στο πραγματικό τους πορτοφόλι παρά διαδικτυακώς, θεωρώντας πως οτιδήποτε βρίσκεται στο διαδίκτυο είναι σε μεγάλο βαθμό εκτεθειμένο σε κακοπροαίρετους χρήστες και κυβερνοεπιθέσεις. Η άποψη αυτή είναι εν μέρει σωστή, και για αυτό θα αναλύσουμε τους κινδύνους που ελλοχεύουν στο διαδίκτυο και υπονομεύουν και απειλούν το ψηφιακό νόμισμα.

Όπως υποστηρίζουν οι George F. Hurlburt και Irena Bojanova (2011), ένα από τα θετικά του bitcoin είναι η μη-αναστρέψιμες συναλλαγές. Μεταφορές bitcoin δεν είναι δυνατό να "παγώσουν", να διατηρηθούν σε αναμονή ή να ακυρωθούν. Αυτό ωστόσο υπό συνθήκες μπορεί να χρησιμοποιηθεί εναντίον μας, από κακόβουλους χρήστες που επιδιώκουν να αποκτήσουν τα bitcoin μας. Αυτό σημαίνει πως εάν το ψηφιακό μας πορτοφόλι παραβιαστεί και μεταφερθούν τα bitcoin μας σε κάποιον άλλο χρήστη, ο μόνος τρόπος να ανακτήσουμε αυτά τα bitcoin, είναι να μας τα στείλει πίσω ο νέος κάτοχος οικειοθελώς. Το ίδιο συμβαίνει και με τυχόν λάθη που πραγματοποιήσουμε εμείς χρησιμοποιώντας το πορτοφόλι μας. Εάν θέλουμε να στείλουμε τα bitcoin μας στον χρήστη Α, θα χρειαστεί να εισάγουμε το δημόσιο κλειδί του για να ολοκληρωθεί η μεταφορά. Εάν πληκτρολογήσουμε λάθος το κλειδί του, θα καταλήξουμε να στείλουμε τα bitcoin μας σε κάποιον άλλο χρήστη Β. Από εκεί και πέρα η τύχη των bitcoin βρίσκεται στα χέρια του Β ο οποίος έχει τον αποκλειστικό λόγο πάνω σε αυτά και παρόλο που μπορούμε να επικοινωνήσουμε μαζί του και να τον ενημερώσουμε για το λάθος μας, εκείνος θα αποφασίσει για το εάν φερθεί τίμια (Hurlburt &. Bojanova, 2011). Σε έναν αριθμό ανώνυμων δημοσίων δηλώσεων έχει διατυπωθεί πως τέτοιου είδους λάθη, μετά από επικοινωνία με τον παραλήπτη, έχουν διορθωθεί με την συνεργασία του και την μεταφορά των bitcoin πίσω στον αρχικό κάτοχο μα

κάτι τέτοιο δεν είναι δυνατό να αποδειχθεί και δεν αποτελεί αξιόπιστη λύση σε αυτό το πρόβλημα.

Όπως κατέστη σαφές παραπάνω, όλοι οι κίνδυνοι απώλειας των ψηφιακών μας νομισμάτων πηγάζουν από την ακεραιότητα του πορτοφολιού μας. Όπως είδαμε το κάθε πορτοφόλι αποτελείται από ένα δημόσιο κλειδί που θα μπορούσαμε να παρομοιάσουμε με το username μας στο δίκτυο, και από ένα ιδιωτικό, το αντίστοιχο password. Εάν κάποιος τρίτος αποκτήσει πρόσβαση στο password μας τότε έχει τον πλήρη έλεγχο των ψηφιακών νομισμάτων μας (Nakamoto, 2008; Kaplanov, 2012). Ορισμένα πορτοφόλια όπως αναλύθηκε σε προηγούμενο κεφάλαιο διατηρούνται ηλεκτρονικά στο διαδίκτυο, έχοντας αποθηκευμένο το δημόσιο και ιδιωτικό μας κλειδί. Σύμφωνα με τους Eskandari S., Barreray D., Stobertz E. και Clark J. (2015), τα πορτοφόλια αυτά, παρόλο που είναι πιο πρακτικά, είναι περισσότερο επίφοβα και πιο επικίνδυνα καθώς βρίσκονται διαρκώς εκτεθειμένα και απειλούνται από κακοπροαίρετους χρήστες και κακόβουλα προγράμματα που επιδιώκουν να αποκτήσουν πρόσβαση σε αυτά. Τα off-line wallets από την άλλη, κρατάνε το πορτοφόλι μας αποθηκευμένο στον σκληρό μας δίσκο, σε ένα USB stick ή ακόμα τυπωμένο και σε χαρτί. Τα πορτοφόλια αυτά είναι πιο ασφαλή από πλευράς κυβερνοεπίθεσης, μα απειλούνται από άλλους κινδύνους όπως φυσική φθορά και απώλεια λόγω καταστροφής ή ακόμα και κλοπής του αντικειμένου.

2.2 Η ακεραιότητα του συστήματος

Οι παραπάνω κίνδυνοι αφορούν τους χρήστες σε προσωπικό επίπεδο και κινδύνους που στοχεύουν τους ίδιους. Ας δούμε όμως τι συμβαίνει όταν κάποιος στοχοποιεί το ίδιο το σύστημα. Ο κάθε χρήστης με την απαραίτητη τεχνογνωσία έχει την δυνατότητα να "αλλοιώσει" το δίκτυο του bitcoin. Όπως υποστηρίζει ο Kaplanov N. (2012), μπορεί να εμφανίσει στο blockchain bitcoin στο δημόσιο κλειδί του ή να εμφανίσει μεταφορές από τους υπόλοιπους χρήστες προς αυτόν. Αυτή η απάτη παρόλο που μοιάζει απλή είναι σχεδόν αδύνατο να πραγματοποιηθεί για τους ακόλουθους λόγους. Καταρχάς, ο χρήστης που επιθυμεί να εμφανίσει ένα bitcoin στο όνομά του θα πρέπει να αλλοιώσει ολόκληρη την αλυσίδα συναλλαγών και να παρουσιάσει όλες τις κινήσεις του bitcoin, από την αρχή της δημιουργίας του μέχρι και σήμερα. Κάτι τέτοιο γίνεται διαρκώς πιο δύσκολο λόγω της εκθετικής πορείας του μεγέθους την αλυσίδας. Μα αυτό δεν είναι το κύριο εμπόδιο που θα αντιμετωπίσει. Σύμφωνα με τον Rainer Bohme και τους συνεργάτες του (2015), η αλυσίδα, πριν προσθέσει ένα block συναλλαγών, επαληθεύει την εγκυρότητά της συγκρίνοντας τον εαυτό της με ένα πρόσφατο αντίγραφο του εαυτού της, το οποίο βρίσκεται διασκορπισμένο σε όλους τους χρήστες της. Με άλλα λόγια, ο χρήστης θα

αλλοιώσει την δική του αλυσίδα, μα αυτή θα "ελέγξει" όλες τις υπόλοιπες αλυσίδες των υπολοίπων χρηστών, θα εντοπίσει την απόκλιση και θα την απορρίψει. Αυτό σημαίνει πως ο χρήστης, για να "ξεγελάσει" το σύστημα θα πρέπει να αλλοιώσει ολόκληρη την δική του αλυσίδα, αλλά και την αλυσίδα όλων των υπολοίπων εντός δέκα λεπτών, προτού προστεθεί το επόμενο block και η αλυσίδα απορρίψει τις μειοψηφικές αποκλίσεις.

Η αλυσίδα ελέγχει τον εαυτό της και θεωρεί ορθό το πλειοψηφικό αντίγραφό της, ακόμα και εάν αυτό έχει αλλοιωθεί. Αυτό σημαίνει πως εάν ο χρήστης καταφέρει να αλλοιώσει το 51% των αλυσίδων από όλους τους χρήστες, το σύστημα αποδέχεται αυτό το 51% ως το πλέον ορθό και σωστό και απορρίπτει το υπόλοιπο 49% (Barber, Boyen, Shi, & Uzen, 2012; Bohme et. Al., 2015). Για να λυγίσει λοιπόν το σύστημα ο χρήστης πρέπει να ασκήσει κακόβουλη υπολογιστική δύναμη μεγαλύτερη από την θεμιτή που ασκούν οι υπόλοιποι χρήστες. Αρκεί να φανταστούμε έναν αγώνα δύναμης όπου από την μία μεριά έχουμε τους "καλούς" χρήστες που τραβούν ένα σκοινί προς το μέρος τους. Για να σπάσει το σύστημα κάποιος, πρέπει να καταφέρει να τραβήξει το σκοινί από την άλλη μεριά ασκώντας μεγαλύτερη δύναμη.

2.3 Η ασφάλεια των συναλλαγματικών αγορών

Η χρήση του bitcoin γίνεται ανώνυμα μέσω του πορτοφολιού. Έχουμε την δυνατότητα να μεταφέρουμε και να λαμβάνουμε bitcoin δίχως να δίνουμε πληροφορίες σε τρίτους για στοιχεία της ταυτότητάς μας και με την βοήθεια των mixer κάνουμε αδύνατο τον συσχετισμό μας με μία ή περισσότερες συναλλαγές σε τυχόν εξωτερικούς παρατηρητές (Bohme et Al., 2012). Όταν όμως θέλουμε να αγοράσουμε ή να πουλήσουμε bitcoin, θα χρειαστεί να συνδεθούμε σε μία από τις αγορές που υπάρχουν, η οποία αναλαμβάνει τον ρόλο του μεσάζοντα. Η χρήση της ωστόσο απαιτεί ορισμένα στοιχεία για την εξακρίβωση της εγκυρότητας των πληροφοριών που δίνουμε. Τα στοιχεία που απαιτούνται δεν είναι απαραίτητα αυτά της ταυτότητάς μας (Kaplanov, 2012). Μα αρκεί να σκεφτούμε το εξής: εάν πουλήσουμε ένα bitcoin και λάβουμε το αντίστοιχο αντίτιμο σε χρήματα, είναι δυνατό, τουλάχιστον όσον αφορά άτομα του στενού μας κύκλου, ο παραλήπτης να μας παραδώσει προσωπικά τα χρήματα.

Πιο πρακτικό ωστόσο είναι τα χρήματα αυτά να μεταφερθούν σε τραπεζικό λογαριασμό της επιλογής μας ή σε κάποια κάρτα τραπέζης, και πιο ασφαλές εννοείται όταν το άτομο με το οποίο συναλλασσόμαστε μας είναι άγνωστο. Αυτό σημαίνει πως η σύνδεση μας στην αγορά απαιτεί τον συσχετισμό μας με έναν τραπεζικό λογαριασμό ή μία κάρτα από τα οποία θα γίνονται και οι συναλλαγές μας. Ο

τραπεζικός αυτός λογαριασμός ωστόσο δεν είναι πλέον τόσο δύσκολο να εντοπιστεί και να ανακαλυφθεί ο κάτοχός του, οπότε το προνόμιο της ανωνυμίας είναι και αυτό εκτεθειμένο.

Εάν χρησιμοποιούμε τις αγορές αυτές και πραγματοποιούμε τις συναλλαγές μας από εκεί, είναι ευνόητο πως η ασφάλειά μας συνάδει με την ασφάλεια της αγοράς, ή οποία λόγω της πληθώρας των συναλλαγών που εξυπηρετεί στοχοποιείται πιο συχνά. Αυτό σημαίνει πως μια "διαρροή" στην ασφάλεια της αγοράς που χρησιμοποιούμε θέτει σε κίνδυνο το ψηφιακό μας πορτοφόλι (Bohme et. Al., 2015). Τα bitcoin μας κατά την χρήση μιας ηλεκτρονικής αγοράς αποθηκεύονται σε πορτοφόλια της ίδιας της αγοράς. Εάν τα πορτοφόλια αυτά εκτεθούν, τότε είναι πιθανό να χάσουμε τα bitcoin μας τόσο εμείς, όσο και οι υπόλοιποι χρήστες της αγοράς αυτής.

Για να πραγματοποιηθεί μια συναλλαγή με χρήματα απαραίτητος είναι ο τρίτος, ο οποίος θα συγχρονίσει τον αγοραστή και τον πωλητή κρατώντας ένα μικρό μερίδιο για τον εαυτό του για τις υπηρεσίες του. Οι αγορές αυτές εξυπηρετούν ένα τεράστιο πλήθος συναλλαγών και διαχειρίζονται έναν τεράστιο αριθμό Bitcoin για τους χρήστες τους και για αυτό αποτελούν συχνότερο στόχο κυβερνοεπιθέσεων. Ακολουθούν πέντε χαρακτηριστικές επιθέσεις hacking στην ιστορία του bitcoin, βασισμένες στο ειδησεογραφικό άρθρο του Sudhir Khatwani, όπως αυτό δημοσιεύθηκε στην ιστοσελίδα https://www.coinsutra.com :

1) Mt. Gox

Η εταιρεία συναλλαγών bitcoin Mt. Gox με έδρα την Ιαπωνία λειτουργούσε από το 2010 και αποτελούσε την μεγαλύτερη συναλλαγματική αγορά εκείνη την εποχή. Η εταιρεία αυτή βρέθηκε στο στόχαστρο hackers όχι μία, αλλά δύο φορές. Η πρώτη πραγματοποιήθηκε τον Ιούνιο του 2011 όταν 2.609 Bitcoin μεταφέρθηκαν από την Mt. Gox σε άγνωστο σε αυτήν πορτοφόλι. Αυτό οδήγησε την Mt. Gox σε προσωρινή διακοπή της λειτουργίας της που διήρκησε αρκετές ημέρες, μα επέστρεψε και πάλι στην αγορά καταφέρνοντας να ανακτήσει προοδευτικά την εμπιστοσύνη των χρηστών της. Η δεύτερη επίθεση πραγματοποιήθηκε το 2014. Την περίοδο εκείνη, η Mt Gox διαχειριζόταν περίπου το 70% των συναλλαγών Bitcoin παγκοσμίως. Η δεύτερη αυτή επίθεση έδωσε τέλος στην λειτουργία της Mt Gox καθώς αυτή την φορά το ποσό ήταν αστρονομικό. Περισσότερα από 750.000 Bitcoin κλάπηκαν, τότε αξίας περίπου 350 εκατομμυρίων δολαρίων οδηγώντας την εταιρεία αυτή σε χρεοκοπία. Οι επενδυτές έχασαν τα πάντα και δεν αποζημιώθηκαν ποτέ.

Πηγή: https://www.reuters.com/article/us-bitcoin-mtgox-insight-idUSBREA1R06C20140228

2) BitFloor

Άλλη μία συναλλαγματική εταιρεία που δέχθηκε επίθεση τον Σεπτέμβριο του 2012. Hackers κατάφεραν να αποκτήσουν πρόσβαση σε ιδιωτικά κλειδιά που δεν είχαν κρυπτογραφηθεί και είχαν αποθηκευτεί διαδικτυακά ως backup, τραβώντας έτσι 24.000 bitcoin. Η απώλεια ήταν σχετικά μικρή και η BitFloor κατάφερε να αποζημιώσει τους χρήστες της, ωστόσο έκλεισε μετά από απόφαση του ιδρυτή της Roman Shtylman, ο οποίος δήλωσε δημόσια το εξής:

"I am sorry to announce that due to circumstances outside of our control BitFloor must cease all trading operations indefinitely. Unfortunately, our US bank account is scheduled to be closed and we can no longer provide the same level of USD deposits and withdrawals ans we have in the past. As such, I have made the decision to halt operations and return all funds. Over the next days we will be working with all clients to ensure that everyone receives their funds. Please be patient as we process your request."

Roman Shtylman

"Με λύπη ανακοινώνω πως λόγω συνθηκών πέραν των δυνατοτήτων μας, η BitFloor πρέπει να διακόψει όλες τις συναλλαγές της οριστικά. Δυστυχώς, ο τραπεζικός μας λογαριασμός πρόκειται να κλείσει και δεν έχουμε πια την δυνατότητα να εξυπηρετούμε τις ίδιες ποσότητες αναλήψεων και καταθέσεων όπως στο παρελθόν. Για αυτόν τον λόγο πήρα την απόφαση να διακόψω τις λειτουργίες και να αποζημιώσω τις καταθέσεις. Τις ημέρες που ακολουθούν, θα συνεργαστούμε με τους πελάτες μας για να βεβαιωθούμε πως όλοι θα αποζημιωθούν. Παρακαλώ, δείξτε υπομονή καθώς διαχειριζόμαστε τα αιτήματά σας."

Roman Shtylman

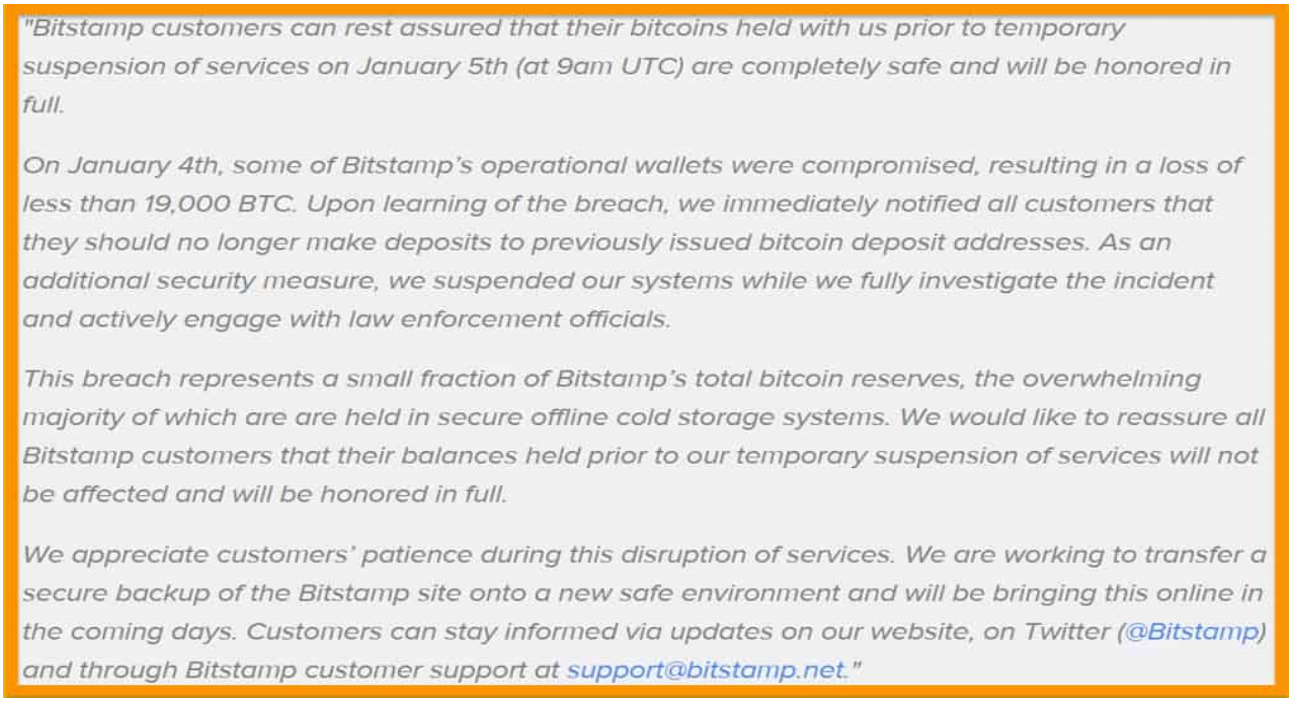
3) Poloniex

Μιαν ακόμα εταιρεία συναλλαγών, όχι μόνο Bitcoin αλλά και άλλων ψηφιακών νομισμάτων παραβιάστηκε τον Μάρτιο του 2014. Σε αυτή την περίπτωση δεν δημοσιεύτηκε ο αριθμός των bitcoin που εκλάπησαν. Η Poloniex ωστόσο ανακοίνωσε στους χρήστες της πως η αξία των bitcoin θα έπεφτε κατά 12.3%, ποσοστό που υποστηρίζεται -δίχως να έχει αποδειχθεί- πως αποτελεί και τον αριθμό των bitcoin που κλάπηκαν (δηλαδή 97 bitcoin) από τα πορτοφόλια της. Παρά την επίθεση η Poloniex εξακολουθεί να βρίσκεται σε λειτουργία και κατάφερε να αποζημιώσει τους πελάτες της, ωστόσο υπήρξε και άλλη φορά που αποτέλεσε στόχο hackers το 2017, δίχως να έχουν διατυπωθεί επίσημες δηλώσεις

Πηγή: https://poloniex.com/media-kit

4) BitStamp

Η BitStamp ιδρύθηκε το 2011 και αποτέλεσε ανταγωνίστρια της Mt. Gox. Τον Ιανουάριο του 2015 ωστόσο τα πρωτόκολλα ασφάλειας της παραβιάστηκαν και 19.000 Bitcoin κλάπηκαν. Όχι πολύ καιρό μετά την επίθεση, η BitStamp διέκοψε προσωρινά την λειτουργία της δημοσιεύοντας το παρακάτω κείμενο:



"Bitstamp customers can rest assured that their bitcoins held with us prior to temporary suspension of services on January 5th (at 9am UTC) are completely safe and will be honored in full.

On January 4th, some of Bitstamp's operational wallets were compromised, resulting in a loss of less than 19,000 BTC. Upon learning of the breach, we immediately notified all customers that they should no longer make deposits to previously issued bitcoin deposit addresses. As an additional security measure, we suspended our systems while we fully investigate the incident and actively engage with law enforcement officials.

This breach represents a small fraction of Bitstamp's total bitcoin reserves, the overwhelming majority of which are are held in secure offline cold storage systems. We would like to reassure all Bitstamp customers that their balances held prior to our temporary suspension of services will not be affected and will be honored in full.

We appreciate customers' patience during this disruption of services. We are working to transfer a secure backup of the Bitstamp site onto a new safe environment and will be bringing this online in the coming days. Customers can stay informed via updates on our website, on Twitter (@Bitstamp) and through Bitstamp customer support at support@bitstamp.net."

Πηγή: https://coinsutra.com/biggest-bitcoin-hacks/

"Οι πελάτες της BitStamp μπορούν να είναι βέβαιοι πως παρά την προσωρινή διακοπή της λειτουργίας μας στις 5 Ιανουαρίου, τα bitcoin τους είναι απολύτως ασφαλή και θα αποζημιωθούν πλήρως.

Στις 4 Ιανουαρίου, μερικά από τα πορτοφόλια της BitStamp παραβιάστηκαν με αποτέλεσμα την απώλεια λιγότερων από 19.000 bitcoin. Με το που λάβαμε γνώση για την διαρροή ενημερώσαμε τους πελάτες μας να διακόψουν προσωρινά τις καταθέσεις.

Ως ένα επιπλέον μέτρο ασφαλείας διακόψαμε όλες τις λειτουργίες, ενώ διερευνούμε διεξοδικά το περιστατικό έχοντας ήδη έρθει σε επαφή με εκπροσώπους του νόμου.

Η διαρροή επηρέασε μόνο ένα μικρό κομμάτι των συνολικών bitcoin που διαχειρίζεται η BitStamp, ενώ το μεγαλύτερο μέρος διατηρείται σε ασφαλείς off-line διακομιστές. Θα θέλαμε να βεβαιώσουμε όλους τους πελάτες της BitStamp πως τα υπόλοιπά τους δεν θα επηρεαστούν από αυτή την προσωρινή διακοπή των λειτουργιών μας και θα αποζημιωθούν πλήρως.

Εκτιμούμε την υπομονή των πελατών μας κατά την διάρκεια αυτής της διακοπής της λειτουργίας μας. Εργαζόμαστε για την μεταφορά του BitStamp σε ένα νέο πιο ασφαλές περιβάλλον και θα επαναφέρουμε την λειτουργία του στις ακόλουθες ημέρες. Οι πελάτες μας μπορούν να ενημερώνονται για της εξελίξεις στην ιστοσελίδα μας, στο Twitter (@BitStamp) και μέσω της υπηρεσίας εξυπηρέτησης πελατών της BitStamp στην σελίδα support@bitstamp.net*."*

Η BitStamp εξακολουθεί να λειτουργεί και έχει καταφέρει να κερδίσει την εμπιστοσύνη των πελατών της, έχοντας λάβει πολλά περισσότερα μέτρα ασφαλείας μετά το περιστατικό.

Πηγή: https://www.bitstamp.net/

5)Bitfinex

Πηγή: https://coiniq.com/bitfinex-vs-kraken/

Αυτή αποτέλεσε και την δεύτερη μεγαλύτερη κλοπή bitcoin μετά αυτή του Mt. Gox στην ιστορία του μέχρι και σήμερα, καθώς χάθηκαν 120.000 bitcoin αξίας 72 εκατομμυρίων δολαρίων. Τον Αύγουστο του 2016, hackers εντόπισαν μίαν αδυναμία στον ψηφιακό πορτοφόλι της Bitfinex ή οποία ήταν αρκετή για να τους δώσει πρόσβαση στην πλατφόρμα συναλλαγών. Οι χρήστες της αποζημιώθηκαν με αργούς μα σταθερούς ρυθμούς και η Bitfinex συνεχίζει την λειτουργία της μέχρι και σήμερα. Αυτές ωστόσο δεν ήταν οι μόνες εταιρείες που αντιμετώπισαν μια τέτοιου είδους εξωτερική απειλή. Πολλές ακόμα έχασαν έναν μεγάλο αριθμό bitcoin, με τις περισσότερες από αυτές να μην έχουν την δυνατότητα να αποζημιώσουν τους πελάτες τους με αποτέλεσμα την διακοπή των λειτουργιών τους.

Στον παρακάτω πίνακα εμφανίζονται με χρονολογική σειρά επιθέσεις που πραγματοποιήθηκαν κατά συναλλαγματικών αγορών, από το 2011 μέχρι και το 2017:

Bitcoin Heists – A Timeline

Many of the thefts from bitcoin exchanges since June 2011

Date	Exchange	Bitcoins missing
Apr 17	Yapizon	3,816
Oct 16	Bitcurex	2,300
Aug 16	Bitfinex	119,756
May 16	Gatecoin	250
Mar 16	CoinTrader	81
Mar-Apr 16	ShapeShift	469
Mar 15	Allcrypt	42
Feb 15	KipCoin	>3,000
Feb 15	Bter	7,170
Jan 15	796 Exchange	1,000
Jan 15	Bitstamp	<19,000
Aug 14	BitNZ	39
Jul 14	Cryptsy	11,325
Jul 14	Moolah/Mintpal	>3,700
Mar 14	Poloniex	97
Feb 14	Mt. Gox	650,000
Nov 13	BIPS	1,295
May 13	Vircurex	1,454
Dec 12	BitMarket.eu	18,788
Sep 12	Bitfloor	24,000
Jul 12	BTC-e	4,500
Jul 12	Bitcoinica	40,000
Jul 12	Mt. Gox	1,852
May 12	Bitcoinica	18,547
Mar 12	Bitcoinica	43,554
Oct 11	Bitcoin7	5,000

Sources: Reuters, Professor Tyler Moore at the University of Tulsa, CryptoCompare and various websites.

Πηγή: https://coinsutra.com/biggest-bitcoin-hacks/

2.4 Μέτρα ασφαλείας

Οι κίνδυνοι αυτοί μπορούν να περιοριστούν και σε ορισμένες περιπτώσεις να εξαλειφθούν εάν λάβουμε τα απαραίτητα μέτρα ασφαλείας για να προστατέψουμε πρώτα το ψηφιακό μας πορτοφόλι και έπειτα αυτά των υπόλοιπων χρηστών. Παρόλο που οι μεγαλύτερες απώλειες bitcoin προκλήθηκαν από επιθέσεις τρίτων, το πιο συνήθες πρόβλημα είναι το ανθρώπινο λάθος (Antonopoulos, 2017). Είναι απαραίτητο ο κάθε χρήστης να είναι καλά ενημερωμένος και εξοικειωμένος με την χρήση του ψηφιακού πορτοφολιού και των συναλλαγματικών αγορών που βρίσκονται στο διαδίκτυο πριν επενδύσει στο ψηφιακό νόμισμα. Πρόκειται για ένα ζήτημα αρκετά σημαντικό στο οποίο θα πρέπει να δώσουμε την απαραίτητη προσοχή, πόσο μάλλον αν λάβουμε υπόψη πως, παρόλο που δεν προσφέρουν όλες οι αγορές αποζημίωση σε περίπτωση εξωτερικής κυβερνοεπίθεσης, καμία από αυτές δεν μας αποζημιώνει σε περίπτωση προσωπικού λάθους. Εάν αποφασίσουμε να επενδύσουμε στο ψηφιακό νόμισμα, πρέπει να έχουμε στο μυαλό μας πως κανείς δεν πρόκειται να μας προστατέψει εάν κάνουμε κάποιο λάθος ή εάν δεν είμαστε σίγουροι για την λειτουργία του πορτοφολιού και πως δεν υπάρχει αντίστοιχη εξυπηρέτηση πελατών που θα βοηθήσει σε τυχόν απορίες ή αδιέξοδα (Bojanova & Hurlburt, 2014).

Εάν θελήσουμε να συνδεθούμε σε μία ηλεκτρονική αγορά, είναι απαραίτητο να δείξουμε την απαραίτητη εμπιστοσύνη στην αγορά αυτή και στα μέτρα ασφαλείας που έχει λάβει. Υπάρχουν ωστόσο και πολλά μέτρα που μπορούμε να λάβουμε σε προσωπικό επίπεδο, που έχουν την δυνατότητα να κάνουν -αν όχι αδύνατη-, σίγουρα πολύ δύσκολη μία ηλεκτρονική διαρροή. Για να δώσουμε την απαραίτητη προσοχή στο θέμα, πρέπει να έχουμε πάντα το εξής στο μυαλό μας : το δημόσιο κλειδί που χρησιμοποιούμε αφορά την ταυτοποίησή μας από τους υπόλοιπους χρήστες. Το ιδιωτικό μας κλειδί παρέχει πρόσβαση στα ψηφιακά νομίσματά μας. Εάν χάσουμε το ιδιωτικό μας κλειδί, η μοίρα των καταθέσεών μας βρίσκεται στα χέρια άλλου (Antonopoulos, 2015) . Εάν το κλειδί είναι δικό μας, τότε οι καταθέσεις είναι και αυτές δικές μας. Εάν το κλειδί δεν είναι πια προσωπικό, τότε οι καταθέσεις δεν μας ανήκουν πια (Khatwani, 2018). Ως εκ τούτου, μείζονος σημασίας είναι πρώτα η προστασία του ιδιωτικού μας κλειδιού και μετά κάθε άλλου συνθηματικού που χρησιμοποιούμε για την διαχείριση των bitcoin μας.

Ο A. Antonopoulos υποστηρίζει πως ασφαλέστερη επιλογή για την αποθήκευση των bitcoin μας είναι το Cold Storage. Σύμφωνα με το βιβλίο του “Mastering Bitcoin” (2015), τα κλειδιά μας δεν είναι τίποτα παραπάνω από μακροσκελείς κωδικούς τους οποίους είναι πιο εύκολο να προστατέψουμε όταν τους έχουμε τυπωμένους σε ένα χαρτί παρά αν βρίσκονται εκτεθειμένοι στο διαδίκτυο. Το πρώτο πράγμα λοιπόν που

είναι σημαντικό ο χρήστης να κάνει για να προστατέψει τον εαυτό του, είναι να έχει στην διάθεση του ένα αν όχι δύο σημειωματάρια. Αν και η ιδέα ίσως φαντάζει ανόητη, είναι απαραίτητο να λάβουμε τα μέτρα μας κρατώντας μερικά αντίγραφα ασφαλείας των κωδικών που πρόκειται να χρησιμοποιήσουμε όταν επενδύουμε στο bitcoin (Antonopoulos, 2017; Leigh, 2018). Εάν χάσουμε την πρόσβαση σε αυτά τα συνθηματικά, είτε γιατί εκλάπησαν, είτε γιατί τα ξεχάσαμε, έχουμε χάσει και τις επενδύσεις μας οπότε ένα εφεδρικό σχέδιο θα μπορούσε να δώσει την λύση. Παρόλο που είναι δυνατό να αποθηκεύσουμε τους κωδικούς μας διαδικτυακά, είναι σημαντικό να το αποφύγουμε (Antonopoulos, 2015). Κάθε κωδικός αποθηκευμένος στον ηλεκτρονικό μας υπολογιστή, στο tablet, στο κινητό μας τηλέφωνο ή σε κάθε άλλου είδους συσκευή που έχει πρόσβαση στο διαδίκτυο είναι εκτεθειμένος και είναι πιο εύκολο να παραβιαστεί. Για αυτόν ακριβώς τον λόγο αποθηκεύουμε όλες τις απαραίτητες πληροφορίες που παρέχουν πρόσβαση στο ηλεκτρονικό μας πορτοφόλι σε σημειωματάριο, από το οποίο συνιστάται να κρατάμε αντίγραφο. Αποθηκεύουμε τα σημειωματάρια αυτά σε ασφαλείς τοποθεσίες μα όχι στο ίδιο μέρος. Μία καλή ιδέα είναι το πρώτο να το έχουμε σε ασφαλές μέρος στο σπίτι μας, ενώ το δεύτερο σε τραπεζική θυρίδα, ή σε άλλο μέρος της επιλογής μας. Δεν μπορούμε να είμαστε σίγουροι για τυχόν φυσικές καταστροφές, φθορές ή ανθρώπινα λάθη που μπορεί να αλλοιώσουν ή καταστρέψουν το σημειωματάριό μας, και εάν λάβουμε υπόψιν πως αυτό μας δίνει πρόσβαση στις καταθέσεις μας, είναι καλό να κινηθούμε προσεκτικά. Μάλιστα, στα τετράδια έχουμε την δυνατότητα να συμπληρώσουμε την αντίστοιχη λίστα με τα προσωπικά στοιχεία μας ως ιδιοκτήτες αλλά και το ποσό με το οποίο είμαστε διατεθειμένοι να επιβραβεύσουμε κάποιον που θελήσει να μας επιστρέψει το σημειωματάριο εάν τυχόν το χάσουμε (Leigh, 2018).

Ιδιαίτερα σημαντικό είναι να βεβαιωθούμε για την ακεραιότητα της ηλεκτρονικής συσκευής που θα χρησιμοποιούμε για να συνδεόμαστε στις ηλεκτρονικές αγορές και να κάνουμε συναλλαγές bitcoin. Όπως αναλύεται στο άρθρο των Penning, Hoffman, Nikolai, και Wang (2014) υπάρχουν πολλών ειδών κακόβουλα λογισμικά τα οποία έχουν την δυνατότητα να παρέχουν πληροφορίες που αποθηκεύουμε στον υπολογιστή μας σε τρίτους. Αυτό σημαίνει πως πριν δημιουργήσουμε λογαριασμό σε κάποια από τις υπάρχουσες αγορές, θα χρειαστεί να κάνουμε μερικούς διαγνωστικούς ελέγχους στον υπολογιστή, το κινητό ή το tablet για τυχόν εντοπισμό malware και άλλου κακόβουλου λογισμικού. Τέτοιου είδους προγράμματα τρυπώνουν στην συσκευή μας και παρέχουν προσωπικές πληροφορίες μας σε τρίτους χωρίς να το γνωρίζουμε, και για αυτό θα χρειαστεί να προμηθευτούμε με το αντίστοιχο αμυντικό λογισμικό που θα "καθαρίσει" τον υπολογιστή μας από απειλές και θα τον κρατήσει ασφαλή από νέες επιθέσεις, πολλά εκ των οποίων διατίθενται δωρεάν.

Στη συνέχεια, για τη σύνδεση σε κάθε ηλεκτρονική αγορά απαιτείται να δημιουργήσουμε έναν ή περισσότερους κωδικούς. Οι κωδικοί αυτοί αποτελούν το μοναδικό τοίχο που χωρίζει έναν εξωτερικό παρατηρητή από τις επενδύσεις μας

(Leigh, 2018), γιαυτό και χρειάζεται να είμαστε ιδιαίτερα προσεκτικοί στην δημιουργία τους. Θα πρέπει να είναι ισχυροί για να μην "σπάσουν" από τυχόν επιθέσεις hackers. Αυτό σημαίνει πως δεν πρέπει να χρησιμοποιούμε συνηθισμένες φράσεις ή λέξεις, ούτε πληροφορίες που έχουν άμεση σχέση με εμάς όπως ημερομηνίες, ή ονόματα δικά μας ή κοντινών μας προσώπων. Σύμφωνα με την άποψη των Robert Morris και Ken Thompson (1979), αυτές θα είναι και οι πρώτες υποθέσεις των hackers και είναι πιο πιθανό να εντοπίσουν τον κωδικό μας εάν αυτός βασίζεται στην κοινωνική ή προσωπική μας ζωή. Αντί αυτού συνιστάται η χρήση συνδυασμών γραμμάτων και συλλαβών που περιλαμβάνουν πεζά, κεφαλαία, αριθμούς, σύμβολα, ή ακόμα και ξενόγλωσσους χαρακτήρες.

Όπως υποστηρίζουν οι R. Morris και K. Thompson, ένας τέτοιος κωδικός είναι πολύ δύσκολο να εντοπιστεί. Επίσης, το σύστημα των ηλεκτρονικών αγορών, έχει το δικό του αντίγραφο ασφαλείας που υπό συνθήκες μας παρέχει πρόσβαση στο πορτοφόλι μας ακόμα και εάν ξεχάσουμε το ιδιωτικό μας κλειδί. Αυτό συνήθως πραγματοποιείται με ερωτήσεις ασφαλείας τις οποίες έχουμε κληθεί να απαντήσουμε κατά τη διαδικασία της δημιουργίας του λογαριασμού μας, ερωτήσεις όπως "*ποιο ήταν το πρώτο σας αυτοκίνητο;*" ή "*πως ονομαζόταν το πρώτο σας κατοικίδιο;*" . Και πάλι, σε αυτές τις ερωτήσεις, η Casey Leigh δηλώνει πως οφείλουμε να δίνουμε ίδιες περίπλοκες απαντήσεις ακολουθώντας το ίδιο μοτίβο, καθώς αυτές οι πληροφορίες είναι γνωστές στον κοινωνικό μας περίγυρο, ή πολλές φορές και ευρύτερα διαδεδομένες όταν εμείς οι ίδιοι εν αγνοία μας δίνουμε στοιχεία για αυτές σε μέσα κοινωνικής δικτύωσης όπως το Facebook κλπ. Αυτοί οι κωδικοί είναι καλό να αποθηκευτούν στα σημειωματάρια που έχουμε στην διάθεσή μας για αυτόν ακριβώς τον σκοπό.

Ένα ακόμα μέτρο ασφαλείας που μπορούμε να λάβουμε σύμφωνα με την C. Leigh για να προστατέψουμε τους κωδικούς μας, είναι να χρησιμοποιούμε το πληκτρολόγιο που εμφανίζεται στην οθόνη μας από τις ρυθμίσεις ασφαλείας, και όχι το πραγματικό μας πληκτρολόγιο, για να αποτρέψουμε τυχόν κρυμμένα malware να αποθηκεύσουν τις κινήσεις μας (Levine, Dabbish, Byrns, 1984). Σε περίπτωση που επιθυμούμε να έχουμε πρόσβαση στο πορτοφόλι μας μέσω του κινητού μας, θα χρειαστεί να ακολουθήσουμε την ίδια διαδικασία

Έχοντας πλέον στην διάθεση μας μια αξιόπιστη συσκευή και έναν ισχυρό κωδικό μπορούμε να λάβουμε ένα ακόμα μέτρο ασφαλείας, συσχετίζοντας το κινητό μας με τον λογαριασμό που πρόκειται να δημιουργήσουμε. Σύμφωνα με την C. Leigh, για την λειτουργία αυτή προτείνεται να χρησιμοποιήσουμε ένα δεύτερο κινητό που θα λειτουργούμε μόνο για αυτόν τον σκοπό, και όχι αυτό που χρησιμοποιούμε δημόσια. Αφού ολοκληρώσουμε την σύζευξη με επιτυχία, κάθε φορά που θα εισάγουμε τον κωδικό μας, θα απαιτείται να συμπληρώνουμε έναν επιπλέον κωδικό που θα

αποστέλλεται στο κινητό που έχουμε συνδέσει. Οι κωδικοί αυτοί αλλάζουν κάθε περίπου 30 δευτερόλεπτα και εξασφαλίζουν πως μόνο ο κάτοχος του κινητού θα μπορεί να εισάγει τον δεύτερο ασφαλή κωδικό. Αυτό σημαίνει πως για να καταφέρει κάποιος να συνδεθεί στον λογαριασμό μας, θα χρειαστεί τόσο το ιδιωτικό μας κλειδί, όσο και τον κωδικό που θα σταλεί στο κινητό μας. Εφαρμογές που παρέχουν αυτή την δυνατότητα ονομάζονται "two-factor authenticators" με ίσως πιο γνωστή την "Google Authenticator".

Τέλος, όπως δήλωσε στις 2 Μαρτίου του 2017 ο A. Antonopoulos στο συνέδριο "Blockchain Africa Conference", μπορούμε να εκμεταλλευτούμε στο μέγιστο τις παροχές του Cold και Hot Storage για να ασφαλίσουμε τις επενδύσεις μας. Όπως είδαμε, τα Hot Wallets είναι εκείνα που απαιτούν την συνεχή σύνδεσή τους στο διαδίκτυο, ενώ τα Cold όχι. Αυτό κάνει την χρήση των πρώτων πιο πρακτική, κυρίως όταν αφορά καθημερινές ή τουλάχιστον επαναλαμβανόμενες συναλλαγές, ενώ αυτή των δεύτερων πιο ασφαλή. Οπότε, έχουμε τη δυνατότητα να διαχειριζόμαστε δύο πορτοφόλια, ένα της κάθε κατηγορίας, και θα τα χρησιμοποιήσουμε ακριβώς όπως διαχειριζόμαστε τα χρήματά μας σήμερα (Antonopoulos, 2015). Μπορούμε να λάβουμε υπόψιν μία τράπεζα, που έχει ένα σχετικά μικρό ποσό στα ταμεία για να συναλλάσσεται, ενώ το μεγαλύτερο μέρος των κεφαλαίων της ασφαλισμένο μέσα στο συμπαγές χρηματοκιβώτιο. Εμείς οι ίδιοι κυκλοφορούμε έξω έχοντας στο πορτοφόλι μας ένα μικρό ποσό το οποίο ενδεχομένως να χρησιμοποιήσουμε. Έχουμε ανά πάσα στιγμή πρόσβαση στο πορτοφόλι μας, μα αυτό είναι εκτεθειμένο σε εξωτερικούς παράγοντες και για αυτό κρατάμε μέσα ένα σχετικά χαμηλό ποσό (Hot Storage), κρατώντας το υπόλοιπο μέρος των χρημάτων μας σε μία πιο ασφαλή τοποθεσία, για παράδειγμα στο σπίτι μας (Cold Storage).

Όσον αφορά την μέθοδο με τα δύο σημειωματάρια, μπορούμε να μεγιστοποιήσουμε την ασφάλεια μας αποθηκεύοντας τους μόνο ένα μέρος των κωδικών μας σε καθένα αυτά. Μπορούμε δηλαδή να αποθηκεύσουμε το πρώτο μέρος του κλειδιού μας σε ένα σημειωματάριο, το δεύτερο σε ένα άλλο που βρίσκεται σε διαφορετική τοποθεσία, και το τρίτο ή τέταρτο κλπ με τον ίδιο τρόπο. Έτσι ακόμα και εάν το σημειωματάριό μας κλαπεί, ο νέος κάτοχος πάλι δεν θα έχει την δυνατότητα να εκμεταλλευτεί το ψηφιακό μας πορτοφόλι.

Η μέθοδος αυτή μπορεί να χρησιμοποιηθεί ακόμα και αν τα κλειδιά μας είναι αποθηκευμένα σε μια ηλεκτρονική συσκευή, όπου σύμφωνα με τους Simon, Xavier, Elaine & Ersin (2012), έχουμε την δυνατότητα να τα μοιράσουμε σε περισσότερες, κάνοντας τυχόν κατασκοπευτικό λογισμικό στην μία από αυτές τις συσκευές, άχρηστο δίχως τα στοιχεία που βρίσκονται στις υπόλοιπες. Βέβαια αυτό έχει ως αποτέλεσμα την πιο αργή διαχείριση των Bitcoin μας καθώς απαιτείται πλέον ο χειρισμός περισσοτέρων συσκευών.

Μίαν ακόμα εναλλακτική λύση που μπορούμε να εφαρμόσουμε είναι να αποστηθίσουμε όλους τους κωδικούς που χρειάζονται για να έχουμε πρόσβαση στα bitcoin μας, μα για λόγους ασφαλείας οι κωδικοί αυτοί όπως είδαμε είναι ιδιαίτερα σύνθετοι, γεγονός που κάνει πιο δύσκολη την απομνημόνευσή τους. Άλλωστε εάν ξεχάσουμε τον κωδικό μας, αμέσως χάνουμε τα δικαιώματά μας στα bitcoin μας και για αυτό συνιστάται να κρατάμε ένα αντίγραφο ασφαλείας (Leigh, 2018; Antonopoulos, 2015).

2.5 Η Νομική Υπόσταση του Bitcoin

Όπως αναλύθηκε παραπάνω το bitcoin βασίζεται σε ένα P2P σύστημα (peer-to-peer). Αυτό σημαίνει πως όταν επιθυμούμε να στείλουμε ή να λάβουμε bitcoin, απευθυνόμαστε απευθείας στον παραλήπτη ή τον αποστολέα, δίχως να υπάρχει κάποιος ενδιάμεσος τρίτος ο οποίος επιβλέπει την συναλλαγή μας (Grinberg, 2011). Αυτό ίσως είναι και το μεγαλύτερο προτέρημα του bitcoin, καθώς παρέχει απεριόριστη ελευθερία κινήσεων και ανωνυμία. Με άλλα λόγια, κανείς δεν κρύβεται πίσω από το σύστημά του, ούτε κρατικός φορέας, ούτε κάποια συναλλαγματική αγορά. Κανείς δεν ασκεί δύναμη, ούτε πραγματοποιεί ελέγχους πάνω στο σύστημα αυτό (Antonopoulos, 2015), άρα κανείς δεν μπορεί να ελέγξει την εγκυρότητα, την ασφάλεια αλλά και την νομιμότητα των συναλλαγών. Από την μία οπτική αυτό είναι καλό, καθώς ο κάθε χρήστης προστατεύει την αφάνεια της οικονομικής του κατάστασης, χωρίς να είναι απαραίτητο να δώσει στοιχεία της σε τράπεζες, άλλους οικονομικούς φορείς ή ακόμα και σε εξωτερικούς παρατηρητές που επιδιώκουν να υποκλέψουν χρήσιμες πληροφορίες. Οι συναλλαγές λοιπόν γίνονται -όπως πολλοί υποστηρίζουν πως θα έπρεπε να είναι- απόλυτα ιδιωτικές. Τα προβλήματα όμως που εγείρονται από μια τέτοια λεπτομέρεια, είναι σύμφωνα με τους N. Kaplanov (2012) και R. Grinberg (2011) νομικά, ως επί το πλείστον. Μίαν ανώνυμη συναλλαγή μας με τον φούρνο της γειτονιάς μας ή με το σουπερμάρκετ δεν είναι παράνομη. Μα αυτού του είδους η ανωνυμία αποτέλεσε το βασικό πλεονέκτημα για την χρήση του bitcoin ως μέσο συναλλαγής πολλών παράνομων και αθέμιτων συναλλαγών (Bohme et. Al., 2015). Το ηλεκτρονικό εμπόριο παράδειγμα ναρκωτικών ή και οπλικού εξοπλισμού είναι παράνομο.

Ανέκαθεν ωστόσο υπήρχαν οι παράνομες οργανώσεις που προμηθεύονται και εμπορεύονται τέτοια προϊόντα αποφεύγοντας τις αστυνομικές αρχές. Η γέννηση του bitcoin θα λέγαμε ότι λύνει τα χέρια σε τέτοιου είδους οργανώσεις, οι οποίες μπορούν να πραγματοποιούν τις συναλλαγές τους ανώνυμα αποφεύγοντας πολλές φορές με επιτυχία τον εντοπισμό τους από την Δίωξη Ηλεκτρονικού Εγκλήματος. Σύμφωνα με τον R. Bohme και τους συνεργάτες του (2015), πολλές ηλεκτρονικές αγορές με

χαρακτηριστική την περίπτωση της “The Silk Road” ελλοχεύουν στο διαδίκτυο προσφέροντας στους επισκέπτες την δυνατότητα να αποκτήσουν προϊόντα όπως όπλα, ναρκωτικά, προϊόντα παιδικής πορνογραφίας και άλλα μέσα από την ανωνυμία του bitcoin. Πληρωμές με bitcoin πραγματοποιούνται για να καλύψουν κάθε ίχνος της συναλλαγής. Μάλιστα, ο Bohme και οι συνεργάτες του (2015) πραγματεύονται πως η χρήση των ηλεκτρονικών συναλλαγών άνοιξε την πόρτα και στο ηλεκτρονικό ξέπλυμα χρήματος, μέσω της εισαγωγής των χρημάτων στην αγορά.

Τα παραπάνω προβλήματα φαντάζουν ιδιαίτερα σημαντικά, ένα ζήτημα ωστόσο που θα λέγαμε πως μας αφορά ακόμα πιο άμεσα είναι η φοροδιαφυγή. Η χρήση του bitcoin, παρόλο που με μία πρώτη ματιά δείχνει να παραβιάζει τον αμερικανικό Ομοσπονδιακό νόμο που ορίζει πως είναι παράνομη η κατασκευή και χρήση νέου νομίσματος που θα αποτελεί ανταγωνιστή του δολαρίου (Grinberg, 2011), δεν έχει απαγορευθεί, τουλάχιστον στις περισσότερες χώρες, επιτρέποντας σε κάθε συναλλαγή να μπορεί να πραγματοποιηθεί με bitcoin. Η ιδέα του ψηφιακού χρήματος ωστόσο είναι καινούρια και το φορολογικό σύστημα των χωρών δεν έχει διαμορφωθεί ακόμα κατάλληλα για να ελέγχει την εγκυρότητα των στοιχείων που δίνουν οι χρήστες (Bohme et. Al., 2015). Αυτό σημαίνει πως μπορούμε να δηλώσουμε -όσον αφορά το πόθεν έσχες- πως ένα μέρος των ετησίων εσόδων μας προήλθε από συναλλαγές bitcoin.

Αυτό δεν σημαίνει όμως πως ο αντίστοιχος κρατικός φορέας βρίσκεται σε θέση να επιβεβαιώσει την εγκυρότητα των συναλλαγών μας. Παρόλο που οι ηλεκτρονικές αγορές ψηφιακών νομισμάτων υπόκεινται σε αυτήν την νομοθεσία (Slattery, 2014), είναι δηλαδή υποχρεωμένες να παρέχουν στις νομισματικές κρατικές υπηρεσίες στοιχεία για τις συναλλαγές των χρηστών εάν αυτό κριθεί απαραίτητο, δεν είναι ακόμα σίγουρη η ακεραιότητα του ιστορικού αυτού των συναλλαγών που πραγματοποιούνται και η ασφάλειά του σε περίπτωση που κάποιος επιθυμεί να αποκρύψει ή να αλλοιώσει τις συναλλαγές του. Επίσης, οι συναλλαγές καταγράφονται μα όχι και το είδος τους (Grinberg, 2011; Bohme et. Al., 2015; Kaplanov, 2012). Ο χρήστης έχει την δυνατότητα να εμφανίσει τις συναλλαγές του στην ηλεκτρονική αγορά επιβεβαιώνοντας πως ένα μέρος του κεφαλαίου του προήλθε από bitcoin. Είναι δυνατό να έχει λάβει για παράδειγμα 1 bitcoin για την πώληση ναρκωτικών, αυτή η πληροφορία όμως θα είναι γνωστή μόνο στον ίδιο, επιτρέποντάς του να κινηθεί με μεγαλύτερη ελευθερία εάν βρεθεί στον στόχο τυχόν ελέγχου, δηλώνοντας πως αυτό το bitcoin το έλαβε για παροχή άλλου είδους υπηρεσιών. Η έλλειψη περαιτέρω στοιχείων για τις συναλλαγές περιορίζει σε μεγάλο βαθμό τα στοιχεία που έχει στην διάθεσή του ένας κρατικός φορέας για έναν ενδελεχή και σαφή έλεγχο, επιτρέποντας την ανομία, το ξέπλυμα χρήματος και την φοροδιαφυγή (Bohme et Al., 2015).

Ο Thomas Slattery (2014) υποστηρίζει πως παρόλο που το πρόβλημα του εμπορίου παράνομων ουσιών και προϊόντων και η πληρωμή για κάθε είδους παράνομες λειτουργίες και υπηρεσίες είναι μείζονος σημασίας, αυτό της φοροδιαφυγής βρίσκεται ήδη στο στόχαστρο πολλών κρατών καθώς πρέπει αργά η γρήγορα να αντιμετωπιστεί με επιτυχία για την επανένταξη σε μία κατάσταση οικονομικής διαφάνειας και περιορισμού οικονομικών εγκλημάτων.

Silk Road

Έχοντας φτάσει το ετήσιο ύψος συναλλαγών των 15 εκατομμυρίων δολαρίων ΗΠΑ από τον πρώτο κιόλας χρόνο της λειτουργίας του, η αγορά αυτή εξυπηρετεί την παράνομη πώληση και προμήθεια ναρκωτικών ουσιών και άλλων επικίνδυνων προϊόντων (Bohme et Al., 2015). Ακολουθεί πίνακας με τα πιο συχνά εμπορευματοποιημένα προϊόντα στην πλατφόρμα αυτή:

The Ten Most Popular Product Categories on the Silk Road Website in January–July 2012

Category	*Number of items*	*Percentage*
Weed	3,338	13.7%
Drugs	2,193	9.0%
Prescription	1,784	7.3%
Benzodiazepines	1,193	4.9%
Books	955	3.9%
Cannabis	877	3.6%
Hash	820	3.4%
Cocaine	630	2.6%
Pills	473	1.9%

Source: Christin (2013).
Note: Categories are self-reported by sellers.

Πηγή: Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, Technology, and Governance.

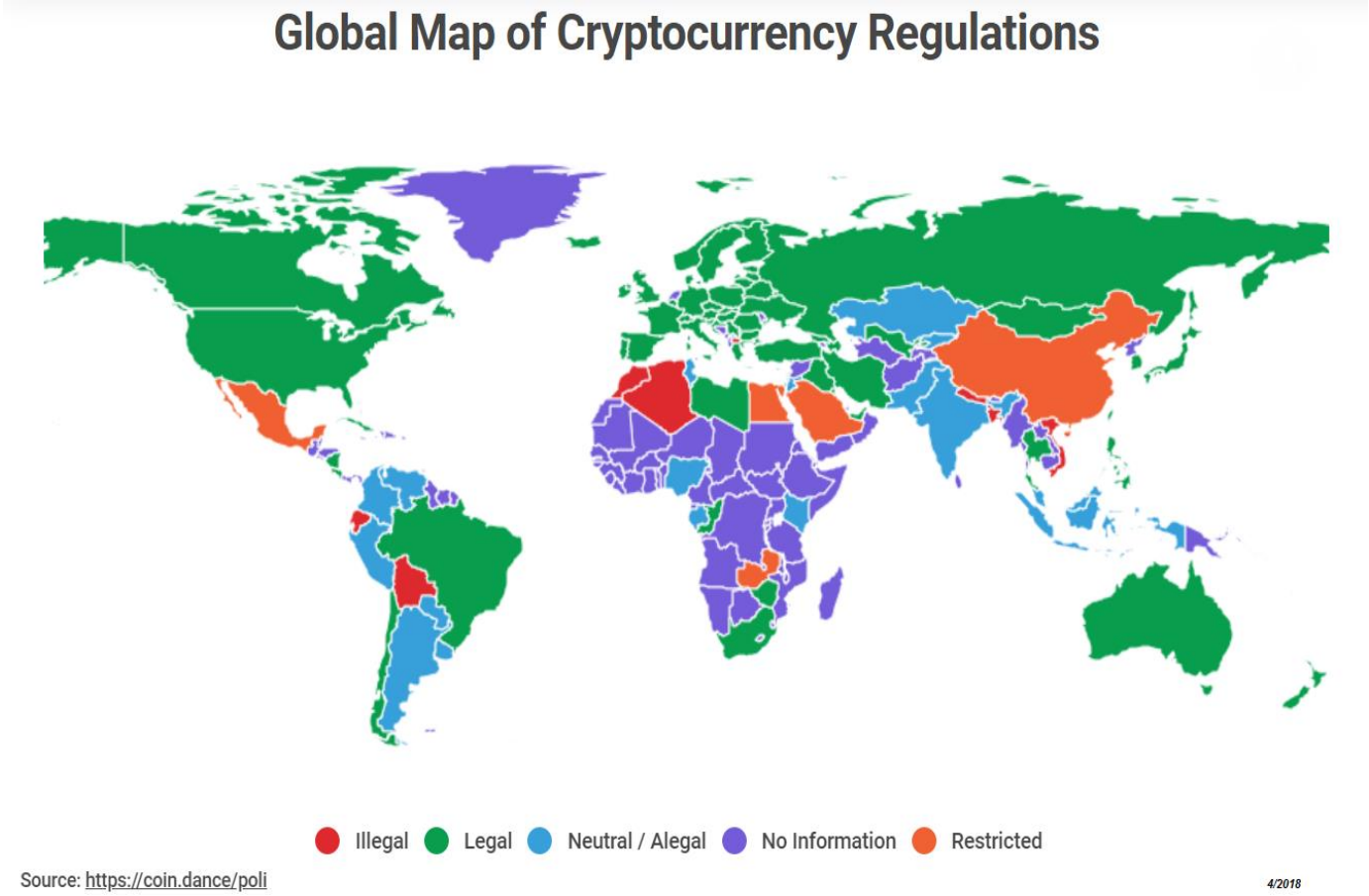
Σύμφωνα με το έργο του Bohme και των συνεργατών του, τον Οκτώβριο του 2013, ο Ross Ulbricht κατηγορήθηκε για ηλεκτρονική απάτη μέσω της διαχείρισης της σελίδας αυτής, ενώ εντοπίστηκαν συναλλαγές 9,9 εκατομμυρίων bitcoin που αντιστοιχούσαν στο ποσό των 214 εκατομμυρίων δολαρίων. Η κίνηση αυτή ωστόσο δεν ήταν καθοριστική καθώς οι υπόλοιποι διαχειριστές κατάφεραν να κρατήσουν την σελίδα ανοικτή για άλλον έναν χρόνο υπό το όνομα "Silk Road 2.0" , μέχρι τον Νοέμβρη του 2014 όπου ξαναέκλεισε μετά από παρέμβαση του FBI και της Europol. Η σελίδα τέθηκε σε λειτουργία για μίαν ακόμα φορά, την οποία όμως διήρκησε μέχρι το 2017, λόγω έλλειψης της απαραίτητης χρηματοδότησης.

Μάλιστα, ο Bohme εμβαθύνει λέγοντας πως η αγορά Silk Road αποτέλεσε την πρώτη που προώθησε σε τόσο μεγάλο βαθμό την εμπορία παράνομων προϊόντων και ο περιορισμός της, όχι μόνο δεν περιόρισε την αθέμιτη χρήση bitcoin, μα την εκτόξευσε δίνοντας μίαν ιδέα της αποτελεσματικότητας και της προοπτικής της ανώνυμης συναλλαγής. Όχι πολύ καιρό μετά το κλείσιμο της σελίδας, πολλές ακόμα διαδικτυακές σελίδες τζόγου στράφηκαν στο bitcoin και στα πλεονεκτήματα που αυτό παρέχει αγνοώντας πλέον τα δολάρια και τα Ευρώ. Χαρακτηριστική είναι και η δημιουργία του διαδικτυακού παιχνιδιού "Satoshi's Dice", στο οποίο ο παίκτης κερδίζει εάν στην ρίψη μερικών ζαριών το άθροισμα είναι μικρότερο από τον αριθμό που έχει επιλέξει ο άλλος παίκτης.

Μίαν ακόμα περίπτωση ηλεκτρονικής απάτης και αποτελεσματικής αντιμετώπισής της αποτέλεσε αυτή του Ρώσου Alexander Vinnik, ο οποίος συνελήφθη από τις Ελληνικές αρχές μετά από αίτημα των αντίστοιχων αμερικανικών. Διαχειριστής της ηλεκτρονικής αγοράς συναλλαγών ψηφιακών νομισμάτων BTC-e, της οποίας η λειτουργία έχει πλέον διακοπεί, ο Vinnik κατηγορήθηκε για ξέπλυμα χρήματος 133 εκατομμυρίων ευρώ που αντιστοιχούν σε 155 εκατομμύρια δολάρια μέσω της χρήσης περίπου 20.640 Bitcoin. Νέα στοιχεία που έχουν δημοσιευθεί από τις ελληνικές αλλά και αμερικανικές αρχές συσχετίζουν τον Vinnik και με την παλαιότερη επίθεση στην Ιαπωνική εταιρεία συναλλαγών Mt. Gox καθώς βρισκόταν ήδη στο στόχαστρο των ερευνών που διενεργούνταν για την προηγούμενη απάτη. Όπως έχει ήδη επιβεβαιωθεί ένας μεγάλος αριθμός των bitcoin της Mt. Gox (300.000), έχουν κλαπεί και στην συνέχεια ξεπλυθεί από την BTC-e, ενώ αρκετά από αυτά βρέθηκαν στο ιδιωτικό πορτοφόλι του Vinnik. Αυτό σημαίνει, πως η ηλεκτρονική αγορά του Vinnik ξέπλυνε σε βάθος 6 χρόνων περίπου 4 δισεκατομμύρια δολάρια. Ο Vinnik μεταφέρθηκε στην Ρωσία για να ανακριθεί μα σήμερα έχει αφεθεί ελεύθερος λόγω έλλειψης στοιχείων. Η BTC-e εξακολουθεί να βρίσκεται εκτός λειτουργίας.

Όλοι οι παραπάνω λόγοι έχουν οδηγήσει αρκετές χώρες στο να περιορίσουν ή ακόμα και να απαγορέψουν την χρήση των ψηφιακών νομισμάτων όπως το bitcoin. Σύμφωνα με την ιστοσελίδα https://coin.dance.com/poli, ανάμεσα σε αυτές βρίσκονται η Βολιβία, το Εκουαδόρ, η Αλγερία, το Μαρόκο, το Νεπάλ, το Μπαγκλαντές και το Βιετνάμ. Αντίστοιχα, σε χώρες όπως η Κίνα, το Μεξικό, η Σαουδική Αραβία, η Αίγυπτος και η Ζάμπια συναντούμε μεγάλους περιορισμούς στις κινήσεις ψηφιακών νομισμάτων, ενώ επιτρέπεται υπό προϋποθέσεις η κατοχή τους από ορισμένες ιδιωτικές ομάδες μετά από έγκριση από τους αντίστοιχους κρατικούς μηχανισμούς της κάθε χώρας. Στις υπόλοιπες χώρες οι συναλλαγές είναι νόμιμες και σε αρκετές από αυτές ασκείται πλέον έλεγχος από τους κρατικούς φορείς οι οποίοι έχουν την δυνατότητα να τις καταστείλουν, ενώ υπάρχουν ακόμα χώρες για τις οποίες δεν υπάρχουν σαφείς πληροφορίες για τις στάσεις του απέναντι σε αυτές τις νέου είδους ηλεκτρονικές συναλλαγές.

Ακολουθεί πίνακας κατανομής, όπως αυτός δημοσιεύθηκε στην ιστοσελίδα https://coin.dance.com/poli στις 13/01/2019:



Πηγή: https://coin.dance.com/poli

3. ΜΕΘΟΔΟΙ ΑΠΟΚΤΗΣΗΣ BIT-COIN

3.1 Mining και τόκοι

Σύμφωνα με τον Bohme και τους συνεργάτες του (2015), αλλά και όπως υποστηρίζει ο A. Antonopoulos (2015), οι μέθοδοι απόκτησης bit-coin σήμερα είναι δύο (2) σε αριθμό. Ο πρώτος αφορά την αγοραπωλησία των bitcoin σε ένα ευρύ ηλεκτρονικό δίκτυο συναλλαγών βασισμένο σε ηλεκτρονικές πλατφόρμες, οι οποίες φέρνουν κοντά τους πωλητές και τους αγοραστές γρήγορα και ανώνυμα, όπως αναλύθηκε σε προηγούμενο κεφάλαιο. Ο πρώτος αυτός τρόπος είναι ιδιαίτερα απλός, κατανοητός και εύκολα εφαρμόσιμος (Kaplanov, 2012). Παρόλο που η αγοραπωλησία bitcoin μέσω των συναλλαγών είναι μια -συγκριτικά με την δεύτερη μέθοδο- εύκολη διαδικασία, είναι σημαντικό να λαμβάνεται πάντα υπόψιν ότι η διασφάλιση των bitcoin μας απαιτεί την απαραίτητη προσοχή στις παραμέτρους ασφαλείας (Eskandari, Barreray, Stobertz, & Clark, 2018).

Η δεύτερη μέθοδος που μπορεί να εφαρμοστεί για την απόκτηση bitcoin είναι το “mining”. Εάν κοιτάξουμε τις συναλλαγές ενός bitcoin “Χ” στην αλυσίδα συναλλαγών αναδρομικά, θα παρατηρήσουμε πως το bitcoin αυτό, την δεδομένη στιγμή ανήκει στον χρήστη “Α”. Προχωρώντας προς τα πίσω, θα διαπιστώσουμε πως το ίδιο bitcoin, ο “Α” το έλαβε από τον “Β” σε μία συγκεκριμένη στιγμή στο παρελθόν, ενώ αντίστοιχα ο “Β” το έλαβε από τον “Γ” ακόμα πιο παλιά. Ακολουθώντας τα βήματα ενός bitcoin, έχουμε την δυνατότητα να εντοπίσουμε και να επαληθεύσουμε την δημιουργία του αλλά και την εισαγωγή του στην αλυσίδα συναλλαγών (block-chain). Σύμφωνα με τον Nakamoto (2008), η δημιουργία ενός bitcoin είναι αποτέλεσμα του “mining”, ή αλλιώς της “εξόρυξης” και είναι ορατή στην αλυσίδα συναλλαγών ώστε όλοι οι υπόλοιποι χρήστες να μπορούν να επαληθεύσουν την εγκυρότητα της νέας εισαχθείσας πληροφορίας.

Όπως πραγματεύεται ο A. Antonopoulos (2015), η εξόρυξη είναι η διαδικασία εκείνη που δημιουργεί νέα νομίσματα και τα εισάγει στην αγορά, ενώ ταυτόχρονα παίζει καθοριστικό ρόλο στην ασφάλεια και ακεραιότητα του δικτύου. Όπως αναφέρθηκε παραπάνω, προκειμένου να παραβιαστεί η ασφάλεια του δικτύου, ο κακόβουλος χρήστης πρέπει να ασκήσει μεγαλύτερη υπολογιστική δύναμη από αυτή που ασκούν αθροιστικά οι ακέραιοι χρήστες προκειμένου να τα καταφέρει. Ένας ακέραιος χρήστης λοιπόν, καταναλώνει ηλεκτρική ενέργεια επιτρέποντας στον ηλεκτρονικό του υπολογιστή να στηρίξει και να προστατέψει το δίκτυο. Αυτό μπορεί να γίνει για παράδειγμα κρατώντας αντίγραφο ολόκληρης της αλυσίδας συναλλαγών στην

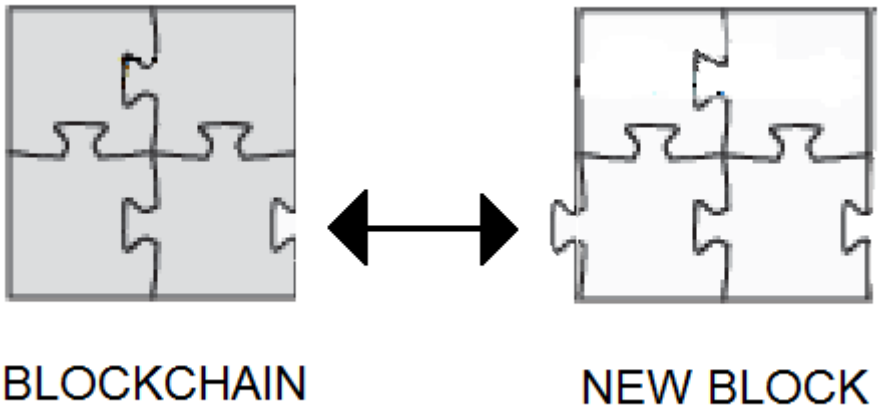
συσκευή του, ή επιδιώκοντας να επαληθεύσει τις νέες συναλλαγές που εμφανίζονται στο δίκτυο, υπερασπίζοντας έτσι την διαφάνειά τους.

Η διαδικασία της υποστήριξης και προστασίας του δικτύου του bitcoin εισάγει την έννοια του "Proof of Work" (Nakamoto, 2008) και δεν απέχει πολύ από αυτό που ορίζουμε ως mining. Το ίδιο το σύστημα δηλαδή επιβραβεύει με bitcoin εκείνους που τάσσονται υπέρ της ορθής λειτουργίας του και φροντίζουν για αυτήν, μέσω της επίλυσης περίπλοκων κρυπτογραφημένων μαθηματικών προβλημάτων (Antonopoulos, 2015). Η αλυσίδα συναλλαγών συνιστάται σήμερα από έναν μεγάλο αριθμό "blocks", δηλαδή κρίκων, ο καθένας από τους οποίους αποτελείται από μια πληθώρα συναλλαγών (Kaplanov, 2012). Ο Kaplanov επίσης ισχυρίζεται πως νέες συναλλαγές σωρεύονται σε έναν νέο κρίκο, ο οποίος πρόκειται να ενταχθεί στην αλυσίδα, όχι όμως πριν εξετασθεί και ελεγχθεί από τους χρήστες που κάνουν mining. Με αυτή την διαδικασία, ελέγχεται η εγκυρότητα του νέου κρίκου πριν εγκριθούν οι συναλλαγές του.

Το mining ολοκληρώνεται με την εξής διαδικασία: ένα μεγάλο πλήθος συναλλαγών που συνιστά το επόμενο block αναμένει την ένταξή του στην αλυσίδα. Ο νέος αυτός κρίκος όμως αποτελείται από έναν τεράστιο όγκο πληροφοριών, ο οποίος αρχικά θα πρέπει να συμπυκνωθεί (Taylor, 2017). Οι miners λοιπόν επιχειρούν να συμπυκνώσουν και να κρυπτογραφήσουν τους νέους κρίκους, εφαρμόζοντας ένα hash algorithm, εμφανίζοντας δηλαδή μόνο τα ψηφιακά αποτυπώματα των νέων κρίκων στην αλυσίδα. Αυτού του είδους η κρυπτογράφηση επιτρέπει στους χρήστες να περιορίσουν μια τεράστια μάζα από ηλεκτρονικές πληροφορίες (σε αυτήν την περίπτωση εκείνες των συναλλαγών) σε ένα αλφαριθμητικό αρχείο του οποίου το μέγεθος δεν ξεπερνά τα 256 bit (Antonopoulos, 2015) . Αυτή η διαδικασία αποδίδει στο νέο block έναν μοναδικό κωδικό μα δεν είναι εύκολη. Οι χρήστες πρέπει να αναζητήσουν εκείνη την αλφαριθμητική αλληλουχία που αντιστοιχεί στο σύνολο των πληροφοριών που επιχειρούν να συμπυκνώσουν, η οποία είναι μοναδική και δεν κατασκευάζεται εκείνη την στιγμή μα προϋπάρχει, μέσα από ένα μεγάλο σύνολο hashes. Λαμβάνοντας αυτές τις παραμέτρους υπ'όψιν είναι κατανοητό πως εξοπλισμός (hardware) mining με ταχύτερους ρυθμούς hashing, δηλαδή τυχαίων δοκιμών τέτοιου είδους αλληλουχιών, ασκούν μεγαλύτερο έργο σε λιγότερο χρόνο και με λιγότερη κατανάλωση ρεύματος, μα το μοναδικό εκείνο hash που αντιστοιχεί στον νέο κρίκο αποτελεί τον νικητήριο λαχνό που αποδίδει σε αυτόν που θα το βρει πρώτος την αντίστοιχη ανταμοιβή.

Οι χρήστες του δικτύου που αναλώνονται στην διαδικασία του mining, επιτρέπουν την ένταξη νέων κρίκων στην αλυσίδα και ταυτόχρονα επιβραβεύονται για τις υπηρεσίες τους (Antonopoulos, 2015). Για την καλύτερη κατανόηση της διαδικασίας, αρκεί να σκεφτούμε ένα puzzle, στο οποίο οι miners δουλεύουν για την συνένωση

του επόμενου κομματιού. Τα blocks είναι έτοιμα, μα ένας μεγάλος αριθμός από δύσκολα μαθηματικά προβλήματα πρέπει να αντιμετωπιστεί για να ολοκληρωθεί η ένταξη του νέου κρίκου, η λύση των οποίων θα μπορούσαμε να πούμε πως δίνει το απαραίτητο σχήμα στις άκρες του puzzle για να μπορέσει να ενωθεί το επόμενο κομμάτι (Σκίτσο 5):



Σκίτσο 5

Σύμφωνα με τον Andreas Antonopoulos (2015), τα πρώτα block που εισήχθησαν με επιτυχία στην αλυσίδα, επιβράβευσαν τους miners με αθροιστικά 50 bitcoin, τον Γενάρη του 2009. Ωστόσο, ο Antonopoulos συνεχίζει λέγοντας πως τα bitcoin που δίνονται ως επιβράβευση στους miners, μειώνονται κατά το μισό, περίπου κάθε τέσσερα (4) χρόνια, ή ανά 210.000 εισαχθέντα blocks. Με αυτούς τους ρυθμούς, υπολογίζεται από τον Kaplanov (2012) πως το τελευταίο bitcoin θα εξορυχθεί μέχρι το 2025μ.Χ. ενώ μέχρι τότε, ο αριθμός όλων των bitcoin θα ανέρχεται περίπου στα 21 εκατομμύρια.

Από τα παραπάνω ωστόσο πηγάζει ένα λογικό ερώτημα όσον αφορά τον αριθμό των miners. Είναι ίσως αυτονόητο να πούμε πως εάν μόνο ένας χρήστης επιχειρήσει να επαληθεύσει την εγκυρότητα του νέου κρίκου και να τον εισάγει στην αλυσίδα, όταν τα καταφέρει, θα λάβει την αντίστοιχη επιβράβευση. Τι πρόκειται να συμβεί όμως και πως θα διανεμηθούν τα bitcoin αυτά, σε περίπτωση που πολλοί χρήστες επιχειρούν ταυτόχρονα να λύσουν τις μαθηματικές εξισώσεις για την εισαγωγή του ίδιου κρίκου; Την απάντηση στην ερώτηση αυτή δίνει ο Kaplanov (2012) λέγοντας πως μόνο αυτός που θα τα καταφέρει πρώτος θα λάβει την αντίστοιχη ανταμοιβή. Τα προβλήματα αυτά είναι ιδιαίτερα περίπλοκα και χρειάζεται χρόνος και υπολογιστική ισχύς για να

λυθούν, συνεπώς ένας δυνατότερος και πιο εξελιγμένος ηλεκτρονικός υπολογιστής είναι πιο πιθανό να τα καταφέρει πρώτος (Kaplanov, 2012). Στην συνέχεια, οι λύσεις των προβλημάτων αυτών θα δημοσιευθούν μαζί με την δημιουργία των νέων bitcoin (των οποίων ο αριθμός εξαρτάται από το μέγεθος της αλυσίδας όπως είδαμε παραπάνω), ενώ οι υπόλοιποι χρήστες, μπορούν να επιβεβαιώσουν τις λύσεις των προβλημάτων αυτών, και στην συνέχεια την απόκτηση της "αμοιβής" από αυτόν που τις δημοσίευσε. Σε αυτήν όμως την περίπτωση, ο κόπος όλων των υπόλοιπων miners θεωρείται περιττός, ανεξάρτητα από το πόσο κοντά έφτασαν στην λύση.

Για την αντιμετώπιση αυτού του προβλήματος, οι Bohme και συνεργάτες (2015), αναφέρονται επίσης στην δημιουργία των "mining pools", τα οποία αντιστρέφουν τις παραμέτρους, εκμεταλλεύονται το πλήθος των συμμετεχόντων, μετατρέποντας τον ανταγωνισμό σε συνεργασία και κέρδος. Όπως υποστηρίζεται στο άρθρο τους, τα mining pools εκμεταλλεύονται την ισχύ πολλών miners ταυτόχρονα για την επίλυση των μαθηματικών προβλημάτων, τα οποία με την πάροδο του χρόνου γίνονται διαρκώς πιο απαιτητικά, και μετά την λύση τους ο κάθε χρήστης επιβραβεύεται αναλογικά με την ισχύ που διέθεσε στο σύνολο. Λαμβάνοντας αυτά υπόψιν, προκύπτει πως η συμμετοχή σε mining pools συμφέρει τον χρήστη, καθώς είναι ιδιαίτερα δύσκολο να ανταγωνιστεί μόνος του ένα σύνολο συσκευών το οποίο είναι πιθανό να ολοκληρώσει την διαδικασία πολύ πιο γρήγορα. Από την άλλη μεριά, ο Bohme και οι συνεργάτες του παραθέτουν τους πιθανούς κινδύνους ενός μεγάλου mining pool, το οποίο σε περίπτωση που διαχειρίζεται πάνω από το 50% της συνολικής διαδικασίας του mining, έχει την δυνατότητα -όπως είπαμε σε προηγούμενο κεφάλαιο- να αλλοιώσει τα στοιχεία που παρατίθενται στο δίκτυο.

Μέσα στην διαδικασία του mining εντοπίζεται και μία ακόμα έμμεση μέθοδος να αποκτηθούν bitcoin, σε πολύ όμως μικρά ποσοστά (Antonopoulos, 2015). Κατά την διάρκεια κάθε συναλλαγής, υπολογίζεται ένα πολύ μικρό ποσοστό της το οποίο αποτελεί και τον τόκο της. Τα μικρά αυτά ποσά σωρεύονται με τα υπόλοιπα που ανήκουν στον νέο κρίκο που περιμένει να εισαχθεί στην αλυσίδα, και τέλος πηγαίνουν στον χρήστη ο οποίος κατάφερε με επιτυχία να λύσει τα προβλήματα και να τον εντάξει στο blockchain, ωστόσο αποτελούν κάτι λιγότερο σε αξία από το 0.5% του συνολικού κέρδους του miner από την επιβράβευση (Antonopoulos, 2015).

Μάλιστα, σύμφωνα με τον Antonopoulos (2015) αλλά και τον Kaplanov (2012), μετά την εξόρυξη του τελευταίου bitcoin, οι miners θα επιβραβεύονται μονάχα με τους τόκους. Καθώς όμως τα ποσά τους είναι ιδιαίτερα μικρά, είναι διακριτός ο κίνδυνος της κατακόρυφης πτώσης των miners εφόσον δεν θα ανταμείβονται για την ισχύ και το ρεύμα που καταναλώνουν, και συνεπώς η ασφάλεια του δικτύου θα είναι πιο ευάλωτη καθώς θα την στηρίζουν λιγότεροι χρήστες.

3.2 Mining Hardware

Λαμβάνοντας υπ όψιν τις απόψεις των Kaplanov (2012), Antonopoulos (2015), καθώς και των Bohme και συνεργατών του (2015), αντιλαμβανόμαστε πως η διαδικασία του mining δεν είναι μια τόσο δύσκολη και δυσνόητη διαδικασία όσο ίσως αρχικά ακούγεται. Όπως αναλύθηκε παραπάνω, τα μαθηματικά προβλήματα που θα κληθεί να λύσει μια ηλεκτρονική συσκευή για την εισαγωγή του νέου block στην αλυσίδα, γίνονται διαρκώς πιο απαιτητικά και πιο δύσκολα, ενώ ας θυμηθούμε και πως σε περίπτωση που πολλοί χρήστες επιχειρούν ταυτόχρονα να λύσουν τα προβλήματα αυτά αυτόνομα, μόνο ο πιο γρήγορος θα λάβει την ανταμοιβή (Antonopoulos, 2015).

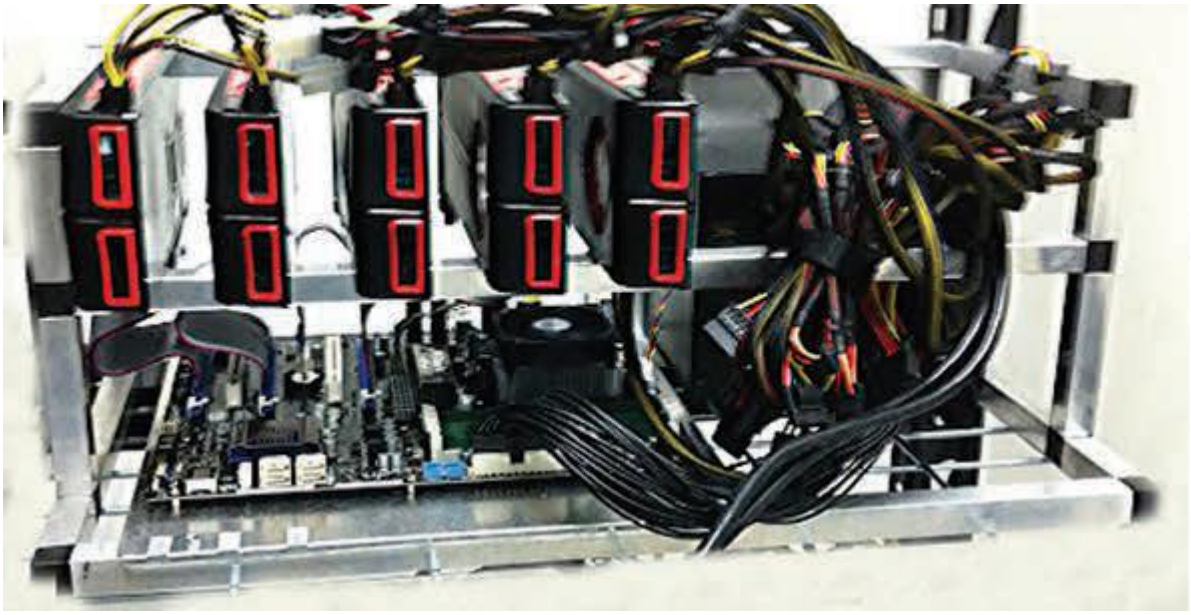
Η έκβαση αυτού του αγώνα δρόμου εξαρτάται από την υπολογιστική ισχύ που μπορεί να διαθέσει ο κάθε χρήστης, κάνοντας έναν ηλεκτρονικό υπολογιστή ειδικά σχεδιασμένο για mining πιο ικανό από τους υπόλοιπους. Επίσης, την στιγμή που οι απαιτήσεις του συστήματος για το mining έχουν ανέβει κατακόρυφα από την αρχή της δημιουργίας τους, η κατανάλωση ηλεκτρικού ρεύματος αφορά πλέον ένα ζήτημα που πρέπει να λάβει την απαραίτητη προσοχή (Taylor, 2017). Αυτό σημαίνει πως, παρόλο που ο κάθε χρήστης του δικτύου bitcoin έχει την δυνατότητα να ασχοληθεί με το mining χωρίς να χρειαστεί να προμηθευτεί συγκεκριμένα κομμάτια υπολογιστικού εξοπλισμού (hardware) (Antonopoulos, 2015), η αποδοτικότητα της διαδικασίας το απαιτεί, καθώς σύμφωνα με τον Taylor (2017), με την πάροδο του χρόνου και εν όψει των εκθετικών απαιτήσεων του mining, έχουν κατασκευαστεί και χρησιμοποιούνται πλέον σε μεγάλο βαθμό ηλεκτρονικοί υπολογιστές και εξαρτήματα ειδικά σχεδιασμένα για την βελτιστοποίηση της διαδικασίας, ισορροπώντας ανάμεσα στον περιορισμό της κατανάλωσης ηλεκτρικής ενέργειας και στην βελτίωση των χρόνων απόδοσης.

Ο Taylor αναφέρεται στις έξι (6) εποχές των mining machines δηλώνοντας πως παρόλο που όταν πρωτοεμφανίστηκε το ψηφιακό νόμισμα και ξεκίνησε η διαδικασία του mining κάθε κεντρική μονάδα επεξεργασίας μπορούσε να είναι αποδοτική, σήμερα το κόστος που θα απαιτηθεί με την ίδια μονάδα θα υπερβεί και θα υπερκαλύψει πιθανά κέρδη, πρώτα και κύρια με τις ποσότητες ηλεκτρικής ενέργειας που θα απαιτηθούν, όπως θα δούμε παρακάτω.

Η πρώτη αυτή δοκιμαστική θα λέγαμε περίοδος κλείνει τον Οκτώβριο του 2010, όταν λογισμικό που υποστηρίζει την εξόρυξη εμφανίστηκε στο διαδίκτυο και υιοθετήθηκε από πολλούς miners σχεδόν αμέσως. Το λογισμικό προσαρμόστηκε εξίσου γρήγορα

στις ανάγκες των miners έχοντας ως μοναδική απαίτηση τις γνώσεις για τον χειρισμό του hardware. Η συνδρομή των GPU στην αποδοτικότητα καθώς και ο ενθουσιασμός των miners, εκτόξευσαν τις προοπτικές στον αέρα αναζητώντας και επεκτείνοντας ταυτόχρονα τα όρια των αποδόσεων (Taylor, 2013). Στην περίοδο αυτήν η συσκευή που αποτέλεσε πρωτοπορία στον κόσμο των miners και προοδευτικά μιαν νέα απαίτηση, συναντάται με πέντε (5) σε αριθμό GPU συνδεδεμένες με μίαν AMD μητρική πλακέτα με τη χρήση καλωδίων PCI για τον περιορισμό του κόστους, με απαραίτητη την παροχή ισχύος με υψηλή απόδοση, αρκετή να τροφοδοτήσει τις κάρτες γραφικών. Έχοντας βελτιστοποιήσει την συσκευή, το επόμενο βήμα ήταν η ταυτόχρονη χρήση περισσότερων GPU, ανεβάζοντας ταυτόχρονα τις απαιτήσεις σε ηλεκτρική ενέργεια αλλά και ικανοποιητική ψύξη.

5 GPU συνδεδεμένες στην ίδια μητρική πλακέτα με καλώδια PCI. 2η εποχή σύμφωνα με τον Taylor :



Πηγή: Bedford Taylor, M. (2017). The Evolution of Bitcoin Hardware.

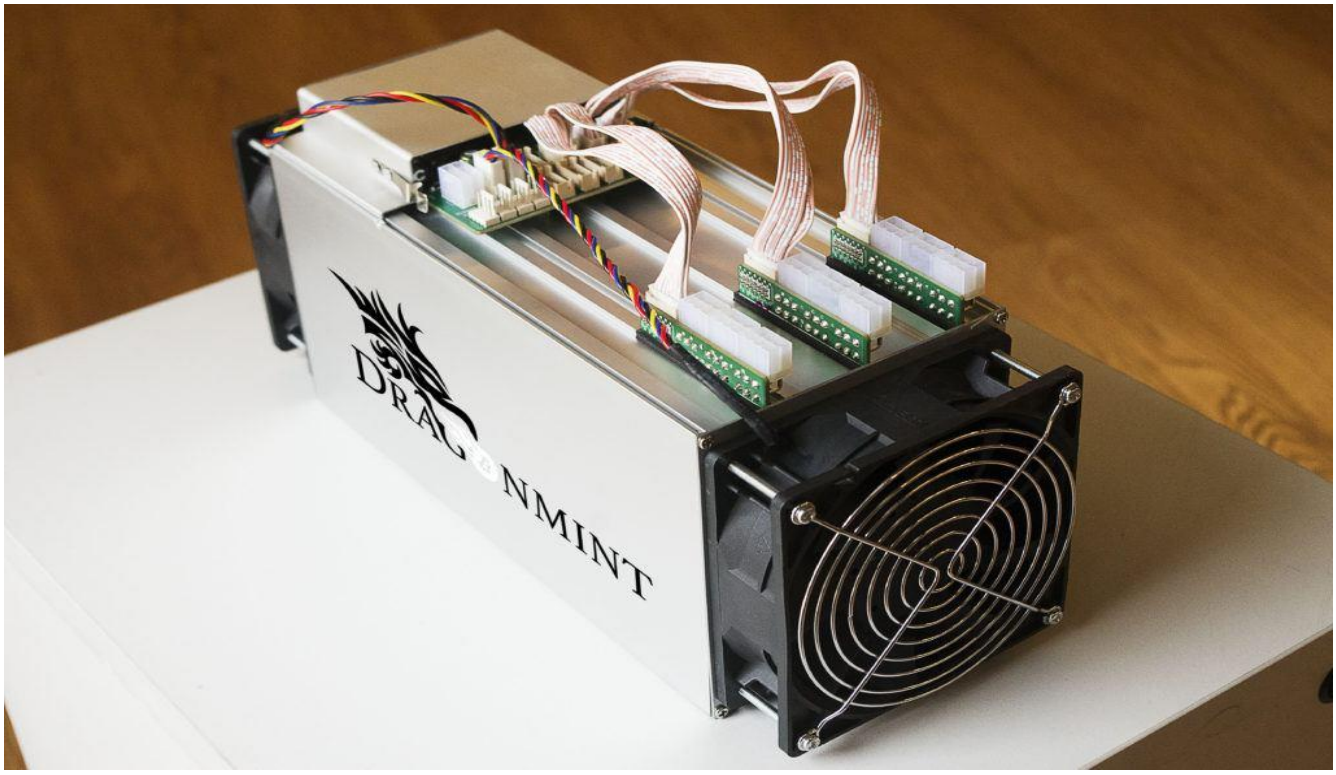
Ο Taylor συνεχίζει λέγοντας πως τον Ιούνιο του 2011 έκαναν την εμφάνισή τους οι FPGA miners, φέρνοντάς μας πια στην τρίτη περίοδο. Εξόρυξη με την χρήση των FPGA είναι σίγουρα αποτελεσματική συμπληρώνει ο Taylor, καθώς παρόλο που δεν

ήταν δυνατό να ανταγωνιστούν το κόστος ανά GH/s με τις τότε GPU που πωλούνταν σε διαδικτυακές ιστοσελίδες λιανικής, το κόστος ηλεκτρικής ενέργειας ήταν μικρότερο από το 20% από αυτό που απαιτούσε η χρήση GPU, επιτρέποντας στους αγοραστές να έχουν αποσβέσει το κόστος τους σε λιγότερο από 2 χρόνια.

Πηγή: https://www.luisllamas.es/que-es-una-fpga/

Οι FPGA miners δεν έμειναν για πολύ στο προσκήνιο ωστόσο καθώς δεν άργησαν να κάνουν την εμφάνισή τους οι ASIC, με εμφανείς βελτιώσεις τόσο στο κόστος όσο και στην κατανάλωση ηλεκτρικού ρεύματος. Τον Ιούνιο του 2012, η εταιρεία BFL, γνωστή πλέον για τις πωλήσεις των FPGA αναγγέλλει την εμφάνιση του νέου προϊόντος. Τρία (3) είναι τα είδη των ASIC που πουλά πλέον η BFL, με τον "Jalapenos" εκάστοτε αξίας 149 δολαρίων με απόδοση 4.5GH/s, τον "Singles" με αξία 1.299 δολάρια και απόδοση 60GH/s και τέλος τον "Mini Rigs" αξίας 30.000 δολαρίων και απόδοση που αγγίζει τα 1.500GH/s. Με αυτές τις τιμές οι μηχανές ASIC μπορούσαν να παράξουν 20 με 50 φορές περισσότερα Bitcoin σε σχέση με τις GPU, αναλογικά με τα χρήματα που επενδύθηκαν στην κάθε περίπτωση.

ASIC της DRAGONMINT :



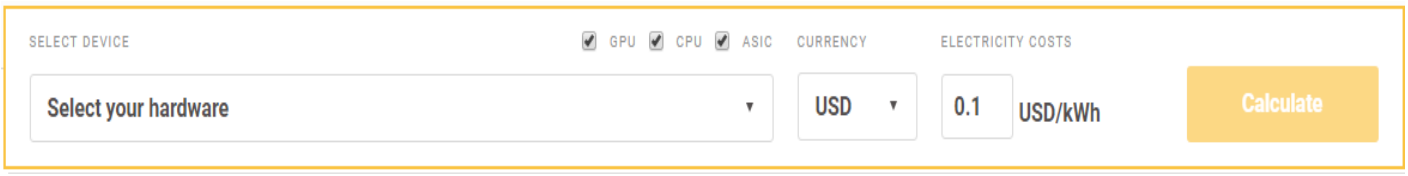
Πηγή: https://halongmining.com/shop/dragonmint-16t-miner/

Ο Taylor αφήνει πίσω του την τέταρτη γενιά του mining αναφερόμενος στον "πόλεμο των ASIC". Έχοντας αναδειχτεί ως ο πιο αποτελεσματικός εξοπλισμός για την διαδικασία του mining, οι ASIC συνέχισαν να κυριαρχούν με διαφορές πλέον να συναντώνται στην απόδοση μεταξύ των διαφορετικών μοντέλων τους αλλά και στην αρχιτεκτονική της κατασκευής τους. Μια πληθώρα από νέα και διαφορετικά μοντέλα εμφανίστηκαν, με όλες τις εταιρείες να στρέφουν τις βλέψεις τους προς την ίδια κατεύθυνση, και τον τεράστιο πλέον ανταγωνισμό να γεννά προβλήματα για πολλές από αυτές. Αυτή η πολυετής κόντρα μας φέρνει στην σημερινή ημέρα και στην τελευταία και έκτη γενιά κατά την οποία λίγες μονάχα εταιρείες κατάφεραν να επιβιώσουν και να αναπτυχθούν μέσα στις δυσμενείς αυτές συνθήκες, με ίσως διασημότερες την Bitfury και την Bitmain.

Σήμερα περισσότερα από 37 μοντέλα ASIC κυκλοφορούν στην αγορά, ενώ μερικοί από τους πιο γνωστούς σύμφωνα με το ηλεκτρονικό ειδησεογραφικό άρθρο του Jordan Tuwiner είναι ο Antminer S9 της εταιρείας Bitmain, ο AvalonMiner της Avalon, και ο Dragonmint 16T της Halong Mining.

3.3 Κατανάλωση ηλεκτρικής ενέργειας και αποδοτικότητα

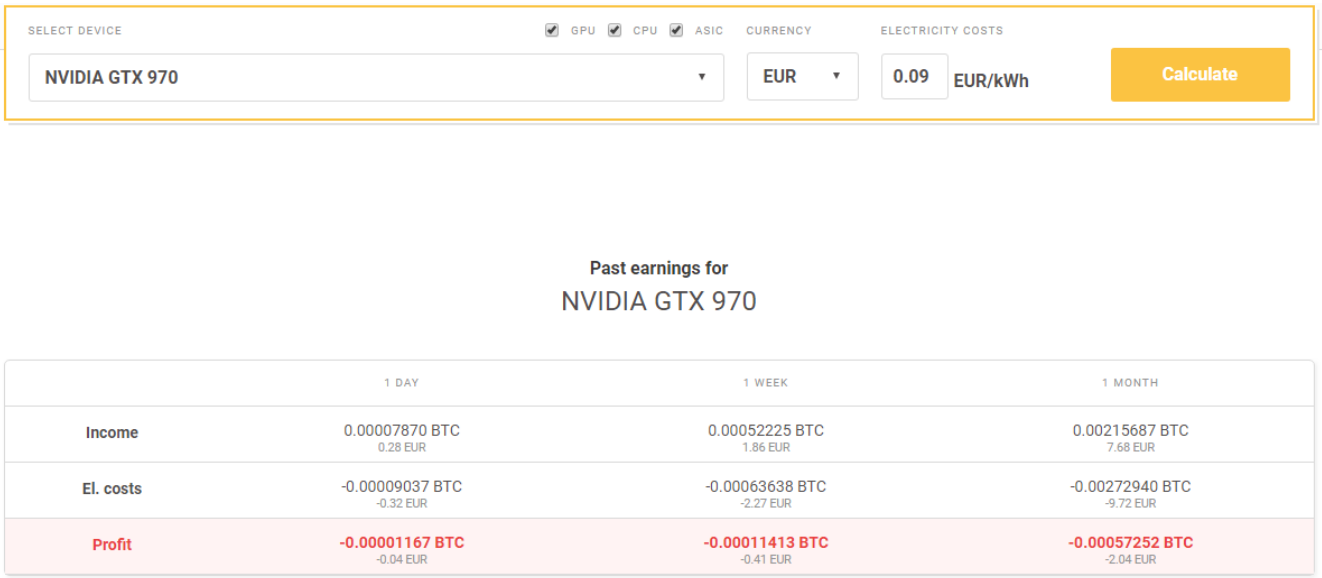
Παρά την υψηλή απόδοση των νέων αυτών μηχανημάτων, η ηλεκτρική ενέργεια που καταναλώνεται για την ολοκλήρωση της διαδικασίας δεν πρέπει να αγνοηθεί καθώς πολλές φορές το κόστος της συνεχούς ηλεκτροδότησης είναι μεγαλύτερο από το ποσό της επιβράβευσης. Χρησιμοποιώντας το εργαλείο NiceHash έχουμε την δυνατότητα να μάθουμε εάν η εξόρυξη είναι μία κερδοφόρα ή ζημιογόνα διαδικασία, λαμβάνοντας ως παραμέτρους το νόμισμα, την κάρτα γραφικών που χρησιμοποιούμε, το κόστος χρέωσης ανά κιλοβατώρα και την σημερινή αξία των bitcoin, η οποία έχει οριστεί περίπου στα 4.100 δολάρια ή 3.600 Ευρώ.



Πηγή: https://www.nicehash.com/profitability-calculator

Παρακάτω θα χρησιμοποιήσουμε την μηχανή για να δούμε εάν μερικές ή περισσότερες από τις κάρτες γραφικών που εντοπίζονται σήμερα στην Ελλάδα μπορούν να ανταπεξέλθουν. Οι κάρτες που θα αναλυθούν αφορούν μερικές από εκείνες των εταιρειών NVIDIA και AMD και καλύπτουν ένα μεγάλο εύρος απόδοσης. Το νόμισμα που θα εφαρμοσθεί θα είναι το Ευρώ (€) και η τιμή ανά κιλοβατώρα θα ορισθεί στα 9 λεπτά (0.09€). Οι παρακάτω κάρτες γραφικών είναι διαθέσιμες για αγορά από το διαδίκτυο, καθώς και σε έναν μεγάλο αριθμό καταστημάτων σε όλη την Ελλάδα :

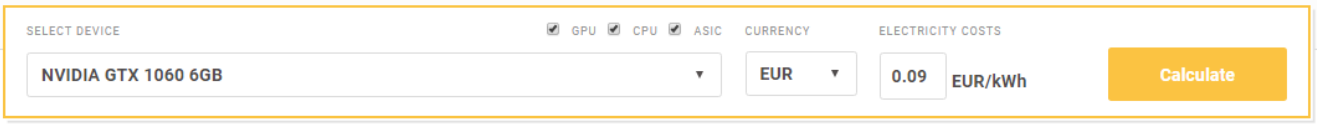
1. NVIDIA GTX970



Πηγή: https://www.nicehash.com/profitability-calculator

Σύμφωνα με την μηχανή NiceHash, η κάρτα γραφικών της NVIDIA GTX970 δεν είναι αποδοτική και παρά την επιτυχή εξόρυξη, σε βάθος ενός μήνα, η χρήση της θα έχει επιφέρει ζημία που ανέρχεται περίπου στα 2 ευρώ. Η τιμή της κάρτας αυτής στην ελληνική αγορά κυμαίνεται στα 65 Ευρώ.

2. NVIDIA GTX1060



Past earnings for

NVIDIA GTX 1060 6GB

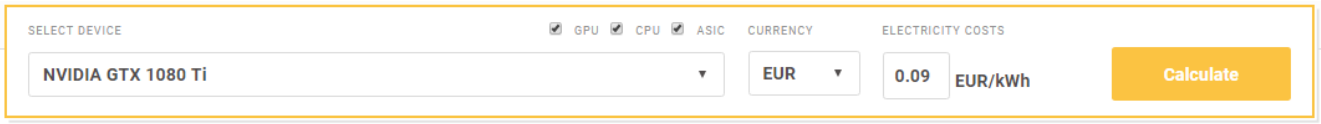
	1 DAY	1 WEEK	1 MONTH
Income	0.00007826 BTC 0.28 EUR	0.00053561 BTC 1.91 EUR	0.00215516 BTC 7.67 EUR
El. costs	-0.00006025 BTC -0.21 EUR	-0.00042425 BTC -1.51 EUR	-0.00181960 BTC -6.48 EUR
Profit	0.00001802 BTC 0.06 EUR	0.00011136 BTC 0.40 EUR	0.00033556 BTC 1.19 EUR

Your hardware is profitable!

Πηγή: https://www.nicehash.com/profitability-calculator

Η κάρτα γραφικών NVIDIA GTX1060 είναι αποδοτική καθώς μπορεί να επιφέρει, μετά την μείωση του ηλεκτρικού κόστους, όφελος 1.20 ευρώ μηνιαίως. Η κάρτα αυτή συναντάται σε τιμές εύρους 200 έως 250 ευρώ.

3. NVIDIA GTX1080TI



Past earnings for
NVIDIA GTX 1080 Ti

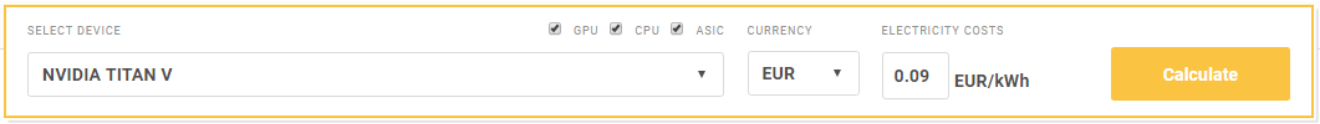
	1 DAY	1 WEEK	1 MONTH
Income	0.00023548 BTC 0.84 EUR	0.00166337 BTC 5.92 EUR	0.00663950 BTC 23.64 EUR
El. costs	-0.00011965 BTC -0.43 EUR	-0.00084766 BTC -3.02 EUR	-0.00363920 BTC -12.96 EUR
Profit	0.00011583 BTC 0.41 EUR	0.00081571 BTC 2.90 EUR	0.00300030 BTC 10.68 EUR

Your hardware is profitable!

Πηγή: https://www.nicehash.com/profitability-calculator

Το σημερινό κέρδος αυξάνεται δραστκά με την χρήση της GTX1080TI αγγίζοντας τα 10 Ευρώ μηνιαίως. Η τιμή της δεν ξεπερνά τα 700 Ευρώ.

4. NVIDIA TITAN V



Past earnings for
NVIDIA TITAN V

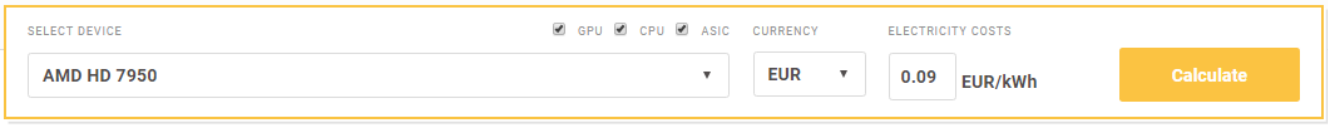
	1 DAY	1 WEEK	1 MONTH
Income	0.00034035 BTC 1.21 EUR	0.00241751 BTC 8.61 EUR	0.00964831 BTC 34.35 EUR
El. costs	-0.00009639 BTC -0.34 EUR	-0.00067880 BTC -2.42 EUR	-0.00291136 BTC -10.37 EUR
Profit	0.00024396 BTC 0.87 EUR	0.00173871 BTC 6.19 EUR	0.00673696 BTC 23.99 EUR

Your hardware is profitable!

Πηγή: https://www.nicehash.com/profitability-calculator

Με το μηνιαίο καθαρό κέρδος να ανέρχεται στα 24 Ευρώ, η TITAN V της NVIDIA είναι μία από τις πιο αποδοτικές κάρτες γραφικών που μπορούν να βρεθούν στην αγορά. Η τιμή της ωστόσο ανέρχεται προσεγγιστικά στις 3.000 Ευρώ.

5. AMD HD7950



Past earnings for
AMD HD 7950

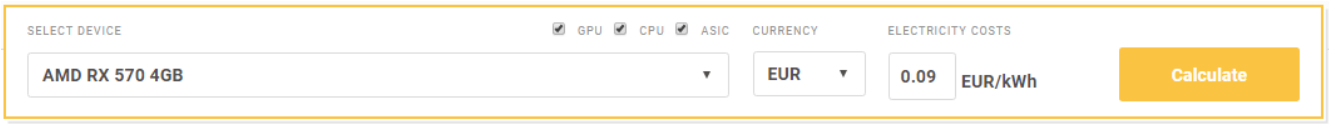
	1 DAY	1 WEEK	1 MONTH
Income	0.00004911 BTC 0.17 EUR	0.00032616 BTC 1.16 EUR	0.00134633 BTC 4.79 EUR
El. costs	-0.00010844 BTC -0.39 EUR	-0.00076365 BTC -2.72 EUR	-0.00327528 BTC -11.66 EUR
Profit	-0.00005934 BTC -0.21 EUR	-0.00043749 BTC -1.56 EUR	-0.00192895 BTC -6.87 EUR

This hardware is not profitable.

Πηγή: https://www.nicehash.com/profitability-calculator

Η HD7950 της AMD όπως φαίνεται παραπάνω δεν πληροί τις αποδοτικές προϋποθέσεις καθώς η ζημία σε βάθος ενός μήνα ανέρχεται σε περίπου 7 Ευρώ. Το κόστος της στην αγορά ανέρχεται περίπου στα 150 Ευρώ.

6. AMD RX570



Past earnings for
AMD RX 570 4GB

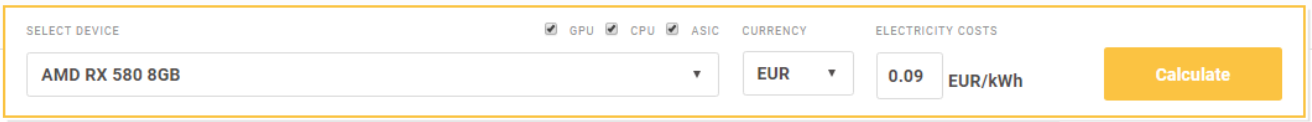
	1 DAY	1 WEEK	1 MONTH
Income	0.00009258 BTC 0.33 EUR	0.00061919 BTC 2.20 EUR	0.00256489 BTC 9.13 EUR
El. costs	-0.00007777 BTC -0.28 EUR	-0.00055098 BTC -1.96 EUR	-0.00236548 BTC -8.42 EUR
Profit	0.00001480 BTC 0.05 EUR	0.00006821 BTC 0.24 EUR	0.00019941 BTC 0.71 EUR

Your hardware is profitable!

Πηγή: https://www.nicehash.com/profitability-calculator

Η AMD RX570 συναντάται στην αγορά επίσης σε τιμές που κλιμακώνονται από τα 150 μέχρι τα 300 Ευρώ, με καλύτερες ωστόσο ισχνές αποδόσεις που δεν ξεπερνούν το 1 Ευρώ ανά μήνα.

7. AMD RX580



Past earnings for
AMD RX 580 8GB

	1 DAY	1 WEEK	1 MONTH
Income	0.00010983 BTC 0.39 EUR	0.00073172 BTC 2.61 EUR	0.00302150 BTC 10.76 EUR
El. costs	-0.00008434 BTC -0.30 EUR	-0.00059395 BTC -2.11 EUR	-0.00254744 BTC -9.07 EUR
Profit	0.00002549 BTC 0.09 EUR	0.00013777 BTC 0.49 EUR	0.00047406 BTC 1.69 EUR

Your hardware is profitable!

Πηγή: https://www.nicehash.com/profitability-calculator

Ελαφρώς καλύτερες επιδόσεις συναντώνται στην RX580 η οποία επιφέρει μηνιαίο κέρδος περίπου 1.5 Ευρώ ενώ η μέση τιμή της αγοράς αυτής της κάρτας είναι τα 250 ευρώ.

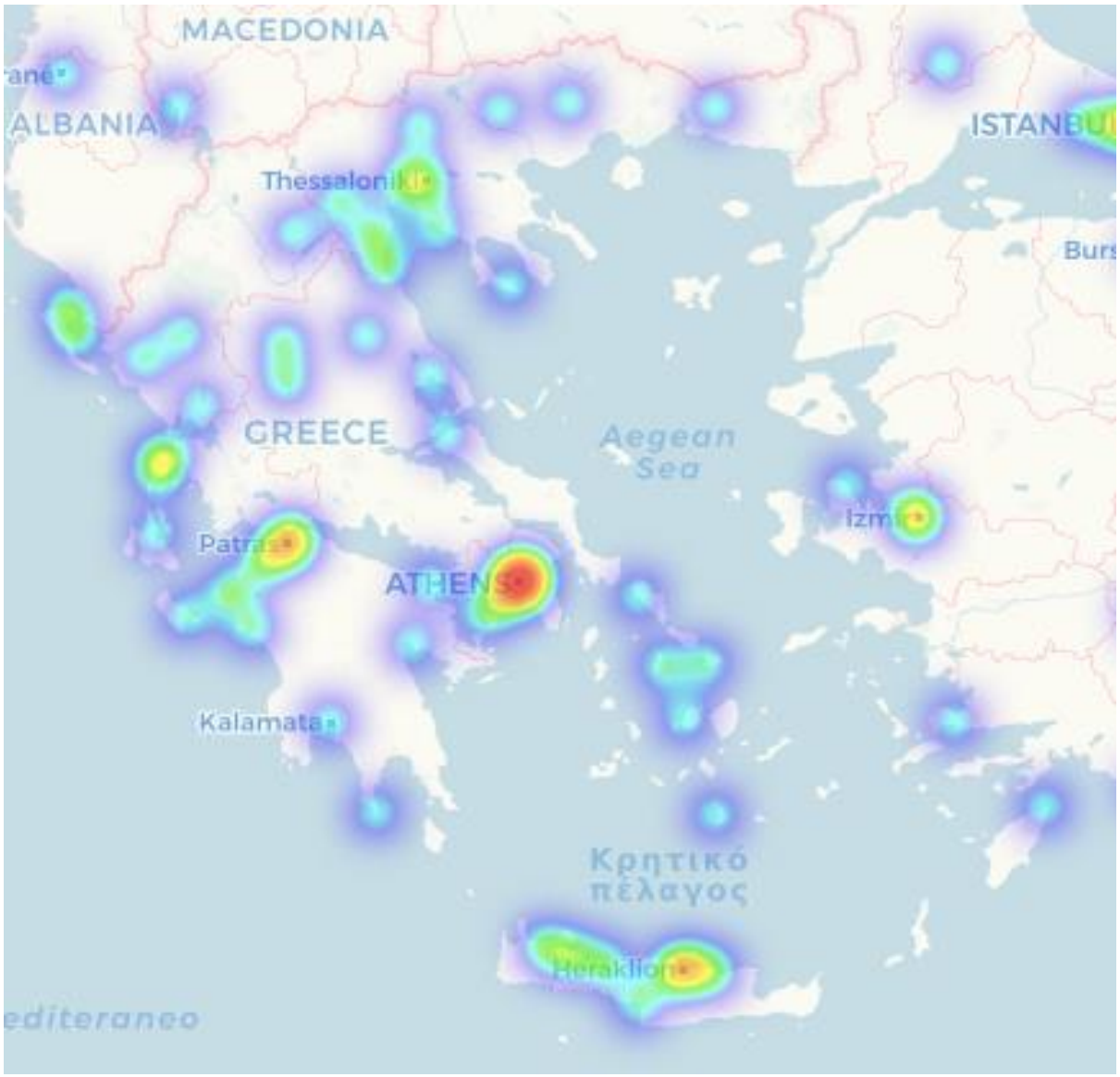
4. BITCOIN ΣΗΜΕΡΑ

4.1 Η απήχηση του bit-coin στον κόσμο

Όπως είδαμε παραπάνω η απόκτηση των bitcoin μπορεί να ολοκληρωθεί με δύο διαδικασίες : την αγορά τους και την εξόρυξή τους. Η στροφή των ανθρώπων στο bitcoin βασίστηκε σύμφωνα με τον Antonopoulos (2015) σε δύο παράγοντες. Ως επί το πλείστον, οι άνθρωποι -ιδίως στην Ελλάδα- ασχολήθηκαν με το bit-coin έχοντας στο μυαλό τους μια μορφή χρηματιστηρίου που θα επέφερε σημαντικά κέρδη. Στις περισσότερες περιπτώσεις, το αρχικό σχέδιο των μελών που επεδίωξαν την απόκτηση bit-coin, ήταν η μεταπώλησή τους για μεγαλύτερη αξία από αυτήν της αγοράς τους και το χρηματικό όφελος που θα επέφερε η διαφορά αυτή. Ωστόσο, λιγότεροι χρήστες μα ένας σημαντικός αριθμός στο σύνολό τους χρησιμοποιούν τα bitcoin για καθημερινές αγορές και πληρωμές. Σε προηγούμενο κεφάλαιο μιλήσαμε για την διαφορά ανάμεσα στο Hot και Cold Storage, όπου σύμφωνα με την άποψη του Antonopoulos, οι χρήστες είναι συνετό να κρατούν ένα χαμηλό σχετικά ποσό στο Hot Storage, στο οποίο η πρόσβαση είναι πιο άμεση και εύκολη για τις καθημερινές τους ανάγκες, ενώ το υπόλοιπο στο πιο ασφαλές και ασφαλισμένο Cold Storage. Οι περισσότεροι λοιπόν κάτοχοι bitcoin σήμερα, κρατούν ένα συγκεκριμένο ποσό της επιλογής τους με το οποίο έχουν την δυνατότητα να συναλλάσσονται, ενώ το υπόλοιπο παραμένει διαθέσιμο για αγοραπωλησία στις ηλεκτρονικές πλατφόρμες, ακολουθώντας τους ρυθμούς των μεταβολών στην τιμή του, και συνεπώς, της ευρύτερης μορφής του χρηματιστηρίου του bitcoin.

Η κατοχή και διαθεσιμότητα των bitcoin ωστόσο δεν σημαίνει απαραίτητα πως έχουμε την δυνατότητα να τα αξιοποιήσουμε για τις καθημερινές μας ανάγκες. Οι ηλεκτρονικές πλατφόρμες συναλλαγών (που δεν είναι λίγες σε αριθμό) βρίσκονται διαρκώς εκεί για να αγοράσουμε είτε να πουλήσουμε τα bitcoin μας. Ωστόσο, όσον αφορά τις καθημερινές πληρωμές τουλάχιστον, είναι λογικό να σκεφτεί κανείς, πως δεν εμπιστεύονται όλοι οι άνθρωποι το bitcoin σήμερα, είτε λόγω τεχνοφοβίας, έλλειψη τεχνογνωσίας, αδυναμία εμπιστοσύνης ενός οπτικά ασταθούς νομίσματος, είτε απλά επειδή θεωρούν την χρήση του περιττή εφόσον καλύπτουν τις ανάγκες τους με ένα νόμισμα χειροπιαστό. Το ίδιο ακριβώς συμβαίνει και με τις εταιρείες και επιχειρήσεις, όχι μόνο στην Ελλάδα αλλά σε όλες εκείνες τις χώρες που το bitcoin έχει εξαπλωθεί. Δεν είναι πολλές οι εταιρείες και τα καταστήματα σήμερα που δέχονται τα bitcoin ως μέσο συναλλαγής, μα θα δούμε παρακάτω πολλές από αυτές που έχουν ενταχθεί στο ψηφιακό δίκτυο και παρέχουν πλέον την δυνατότητα στους πελάτες τους να συναλλάσσονται με το ψηφιακό νόμισμα.

Σύμφωνα με την σελίδα WeAcceptBitcoin.gr, η οποία εμφανίζει μίαν ενημερωμένη λίστα καταχωρηθέντων εταιρειών, επιχειρήσεων και ιδιωτών που αποδέχονται bitcoin, η κινητικότητα του ψηφιακού νομίσματος στην Ελλάδα αναπαριστάται στην ακόλουθη εικόνα :

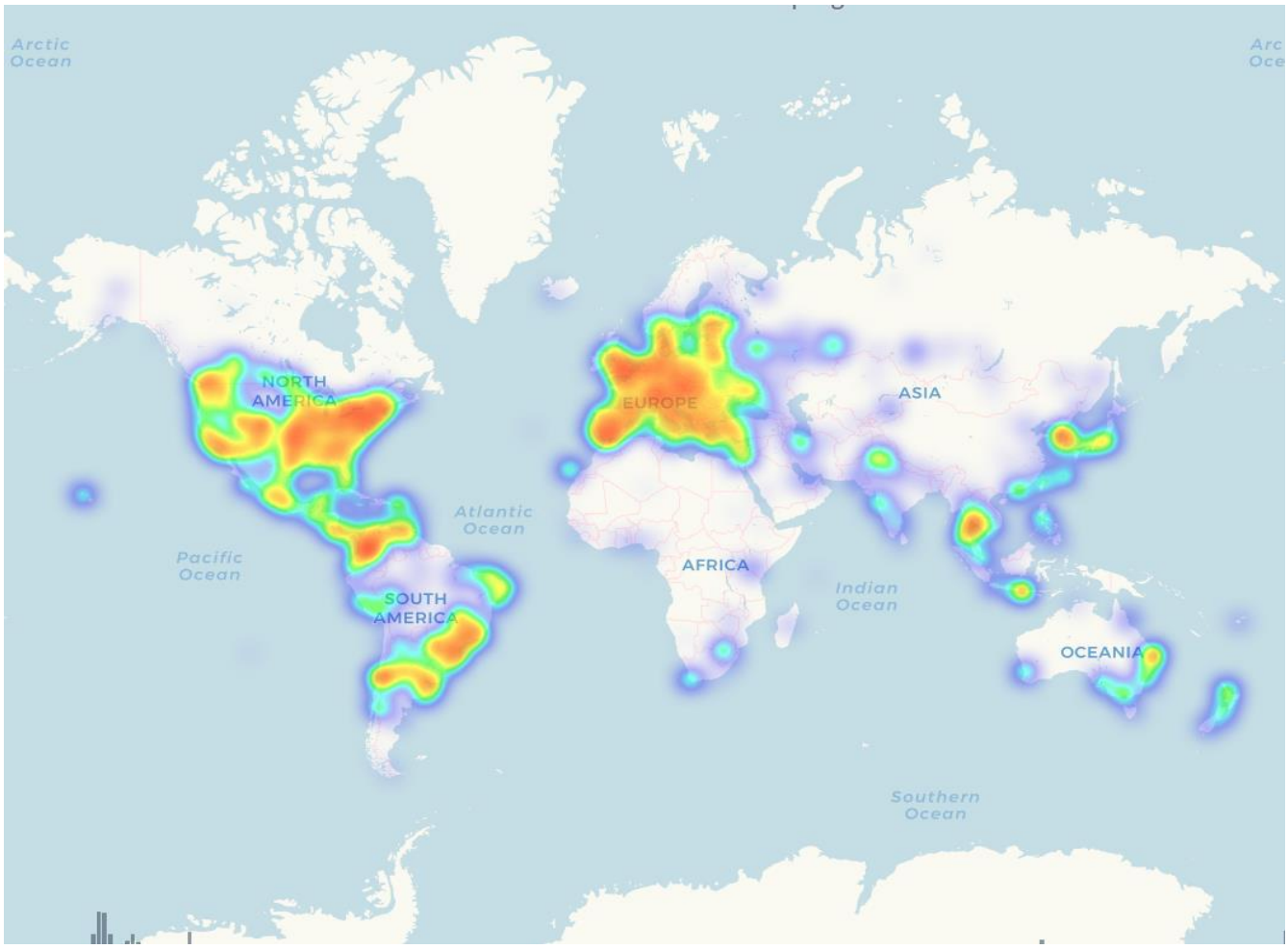


Πηγή: https://weacceptbitcoin.gr/

Βασισμένοι στην ίδια ιστοσελίδα, έχουμε πρόσβαση σε έναν κατάλογο εταιρειών και ιδιωτών που αποδέχονται τα bitcoin σήμερα. Μερικοί από αυτούς είναι οι εξής:

ΟΝΟΜΑ	ΚΑΤΗΓΟΡΙΑ	ΤΟΠΟΘΕΣΙΑ
Bitrefill	Φόρτιση Καρτοκινητών	on-line
Metabook	Μεταχειρισμένα βιβλία	on-line
My Sunshine	Είδη εγκυμοσύνης και παιδικά προϊόντα	Αθήνα, Αττική, Ελλάδα
KEEN Organic Living	Παιδικά ενδύματα	Αθήνα, Αττική, Ελλάδα
Ταβέρνα Άγγελος	Ταβέρνα	Αθήνα, Αττική, Ελλάδα
Bike Lounge	Κατάστημα ποδηλάτων	Μαρούσι, Αττική, Ελλάδα
Έπιπλο Τσουραπά	Κατάστημα επίπλων	Αθήνα, Αττική, Ελλάδα
Feel Your Home	Είδη σπιτιού	Αθήνα, Αττική, Ελλάδα
Omega Gaming Center	Ηλεκτρονικά παιχνίδια	Άλιμος, Αττική, Ελλάδα
u_m@d	Internet Sports cafe	Νέα Σμύρνη, Αττική, Ελλάδα
Γιαμπουράνης	Δικηγορικό γραφείο	Αθήνα, Αττική, Ελλάδα
Ιωαννης Ιγγλεζάκης	Δικηγορικό γραφείο	Θεσσαλονίκη, Μακεδονία, Ελλάδα
MultiCopter	Drones	Χαϊδάρι, Αττική, Ελλάδα
Biofire	Βιολογικά τζάκια	Αθήνα, Αττική, Ελλάδα
Τετράδιο	Βιβλιοπωλείο	Αθήνα, Αττική, Ελλάδα
Sousourades	Γυναικεία ενδύματα	Αθήνα, Αττική, Ελλάδα
Χιώτης	Είδη πυρόσβεσης	Νέα Ιωνία, Αττική, Ελλάδα
Πέγκλης Ευάγγελος	Μικροβιολογικό εργαστήριο	Καλύβια Θωρικού, Αττική, Ελλάδα
Priona Resort	Ενοικίαση δωματίων	Σκοτίνα, Πιερία, Ελλάδα
Paros Paradise Villas	Ενοικίαση εξοχικών κατοικιών	Πάρος, Κυκλάδες, Ελλάδα
Σανδάλια Σάββας	Δερμάτινα σανδάλια	Ρόδος, Ελλάδα
PetWorkz	Κατάστημα για κατοικίδια ζώα	Βούλα, Αττική, Ελλάδα
Anik Snacks	Τρόφιμα Ζακύνθου	Αγία Παρασκευή, Αττική, Ελλάδα
Pointer.gr	Φιλοξενία ιστοσελίδων	Θεσσαλονίκη, Μακεδονία, Ελλάδα
Alda Shop	Τουριστικά είδη	Ρέθυμνο, Κρήτη, Ελλάδα
35°North	Ελαιόλαδο	Σητεία, Κρήτη, Ελλάδα
Δημήτρης Δημητρίου	Λογιστικό γραφείο	Βόλος, Μαγνησία, Ελλάδα
Gee	Καφές και πρωινό	Κομοτηνή, Ροδόπη, Ελλάδα
Skytech	Κατάστημα Η/Υ	Αθήνα, Αττική, Ελλάδα
Advanced Computing	Υπηρεσίες πληροφορικής	Θεσσαλονίκη και Χαλκιδική, Ελλάδα
Hotwater	Υδραυλικά, θέρμανση, κλιματισμός, φυσικό αέριο	Αιγάλεω, Αττική, Ελλάδα
Digifort	Συστήματα ασφαλείας	Αθήνα, Αττική, Ελλάδα
Fit.gr	Συμπληρώματα διατροφής	Αθήνα, Αττική, Ελλάδα
Pharmacy128	Φαρμακείο	Θεσσαλονίκη, Μακεδονία, Ελλάδα
Carner	Αξεσουάρ αυτοκινήτων	Θεσσαλονίκη, Μακεδονία, Ελλάδα
Κίνηση και λειτουργία	Κέντρο φυσικοθεραπείας	Θεσσαλονίκη, Μακεδονία, Ελλάδα
ΕΛΤΑ Παγκρατίου	Ταχυδρομείο	Αθήνα, Αττική, Ελλάδα
Νόστος	Εστιατόριο	Αγία Μαρίνα, Χανιά, Κρήτη, Ελλάδα
Δημήτριος Ντάρας	Φωτογραφία και βιντεοσκόπηση	Ιωάννινα, Ήπειρος, Ελλάδα
OK Anytime Market	Mini-market	Αγία Παρασκευή, Αττική, Ελλάδα
Εκήβολος	Ιδιωτικό ΚΤΕΟ	Ιστιαία, Εύβοια, Ελλάδα
Chronostore	Κατάστημα ρολογιών	Κέρκυρα, Ελλάδα
Σπιτικό	Φούρνος	Θεσσαλονίκη, Μακεδονία, Ελλάδα
Dastart	Cafe	Θεσσαλονίκη, Μακεδονία, Ελλάδα
Alexandros Hair	Κομμωτήριο	Αθήνα, Αττική, Ελλάδα
Fitness Tempo	Γυμναστήριο	Τρίκαλα, Θεσσαλία, Ελλάδα

Αξιοσημείωτη είναι επίσης η αναφορά του Πανεπιστημίου της Λευκωσίας στην Κύπρο, καθώς επίσης και διεθνείς γνωστές εταιρείες όπως η Microsoft, η Dell, αλλά και η Wikipedia για δωρεές. Παρακάτω εμφανίζεται ενδεικτικά η εμπορική κινητικότητα του bitcoin και στον υπόλοιπο κόσμο, όπως αυτό φαίνεται επίσης στην σελίδα WeAcceptBitcoin :



Πηγή: https://weacceptbitcoin.gr/

Όπως βλέπουμε στον παραπάνω πίνακα είναι εμφανές πως το bit-coin έχει υιοθετηθεί από μία πληθώρα εταιρειών και ιδιωτών που καλύπτουν μίαν ευρεία λίστα παροχών. Από καφετέριες και εστιατόρια, ενοικιαζόμενα δωμάτια και bar, μέχρι φούρνους, βιβλιοπωλεία, φαρμακεία και επιπλοπωλεία, δικηγορικά και λογιστικά γραφεία. Το bit-coin μπορεί να χρησιμοποιηθεί σε κάθε είδους επιχείρηση και να γίνει αποδεκτό ως μέσο συναλλαγής, σε περίπτωση που ο ιδιοκτήτης συναινεί και μπορεί να το διαχειριστεί, ενώ είναι εμφανής η ραγδαία εξάπλωση και εφαρμογή του εναλλακτικού αυτού τρόπου πληρωμών.

4.2. Πλεονεκτήματα και Μειονεκτήματα του ψηφιακού νομίσματος

Πλησιάζοντας το τέλος της εργασίας αυτής και λαμβάνοντας υπ'όψιν όλες τις παραπάνω πληροφορίες, όπως αυτές έχουν δημοσιευθεί με τη μορφή βιβλίων, άρθρων και συνεντεύξεων, έχουμε πλέον μία πιο ξεκάθαρη εικόνα του bit-coin μπροστά μας. Έχοντας αναλύσει σε βάθος τα απαραίτητα στοιχεία, έχουμε την δυνατότητα να συγκροτήσουμε τις πληροφορίες αυτές και να κατανοήσουμε έναν πιο συνοπτικό πίνακα που περιλαμβάνει τα πλεονεκτήματα και τα μειονεκτήματα του bit-coin σήμερα, όπως αυτός δημοσιεύθηκε το 2014 από τους G. Hurlburt και I. Bojanova. Σύμφωνα με το άρθρο τους "Bitcoin: Benefit or curse?" στην ακόλουθη λίστα περιλαμβάνονται τα περισσότερα γνωρίσματα του bitcoin χωρισμένα στις δύο αυτές μεγάλες κατηγορίες :

ΠΛΕΟΝΕΚΤΗΜΑΤΑ	ΜΕΙΟΝΕΚΤΗΜΑΤΑ
Αποτελεί το πρώτο ψηφιακό νόμισμα που είναι λειτουργικό	Δεν υπάρχει διαχειριστική ομάδα, συνεπώς δεν μπορεί κανείς να μας βοηθήσει σε περίπτωση προσωπικού λάθους
Είναι πλήρως αποκεντρωμένο: μπορεί να χρησιμοποιηθεί οπουδήποτε και οποτεδήποτε	Παρόλο που είναι ισχνή, υπάρχει η πιθανότητα υποκλοπής προσωπικών μας δεδομένων
Δεν απαιτείται μεγάλο κόστος συντήρησης και ελέγχου	Κάθε συσκευή συνδεδεμένη στο διαδίκτυο είναι δυνατό να παραβιαστεί από κυβερνοεπιθέσεις
Οι συναλλαγές είναι ανώνυμες: δεν υπάρχει ο κίνδυνος υποκλοπής προσωπικών δεδομένων	Το πορτοφόλι μας αντιμετωπίζει κινδύνους φυσικών καταστροφών, απώλειας/κλοπής και φθοράς
Βασισμένες στο proof-of-work, οι συναλλαγές είναι αξιόπιστες	Οι συναλλαγές είναι μή-αναστρέψιμες
Οι συναλλαγές δημοσιοποιούνται για την ανά πάσα στιγμή επιβεβαίωση και επαλήθευσή τους	Η ανωνυμία του bit-coin συμβάλει στην άνθιση της ανομίας, που αφορά από εμπόριο οπλικού εξοπλισμό και ναρκωτικών, μέχρι και φοροδιαφυγή και ξέπλυμα χρήματος
Οι ρυθμοί δημιουργίας bitcoin αλλά και η ανά πάσα στιγμή αξία του είναι αναρτημένες στο διαδίκτυο και προσβάσιμες από όλους	Πολλές χώρες έχουν λάβει κατασταλτικά ή περιοριστικά μέτρα, είτε έχουν κηρύξει το bit-coin παράνομο, περιορίζοντας την εφαρμογή του
Προωθεί τη δημοκρατία μέσω ενός παγκοσμίως κοινού νομίσματος	-

Την παραπάνω γνώμη ενστερνίζονται και ο Kaplanov και Antonopoulos, συμπληρώνοντας ένα ακόμα στοιχείο στα μειονεκτήματα του bit-coin :

- Η εξόρυξη αποτελεί την κατανάλωση ηλεκτρικής ισχύος από τον χρήστη για την στήριξη της ασφάλειας του συστήματος, αλλά και για την ανταμοιβή του. Ο Kaplanov (2012) αλλά και ο Antonopoulos (2015) εκφράζουν την ανησυχία τους, ισχυριζόμενοι πως μετά την εξόρυξη και του τελευταίου bitcoin, οι χρήστες δεν θα βλέπουν πια όφελος στην διαδικασία του mining, θα πάψουν να στηρίζουν το σύστημα καθώς θα πάψει πλέον να αποτελεί μια κερδοφόρα διαδικασία, και η ασφάλεια και ακεραιότητα του δικτύου θα τεθούν σε μεγάλο κίνδυνο.

Αντίστοιχα, ο Bohme (2015) και οι συνεργάτες του συμπληρώνουν το ρίσκο ως ένα ακόμα μειονέκτημα στην παραπάνω λίστα επισημαίνοντας :

- Παρά την ανοδική του πορεία, το δίκτυο του bitcoin αποτελεί μία πιο σύγχρονη μα όχι και τόσο διαφορετική μορφή χρηματιστηρίου. Παρόλο που μπορεί να επιφέρει τεράστια κέρδη, είναι συνετό να μην ξεχνάμε ότι το γεγονός πως κάποιος θα βγει κερδισμένος, σημαίνει αυτόματα πως κάποιος άλλος θα βγει ζημιωμένος. Αρκεί να υπολογίζουμε πάντα το ρίσκο και να θυμόμαστε πως, όπως η τιμή ανέβηκε κατακόρυφα, είναι εξίσου πιθανό να πέσει με τους ίδιους ρυθμούς.

Από την άλλη μεριά, αξιοσημείωτο είναι το σχόλιο του Kaplanov (2012) αλλά και του Benjamin Wallace (2011), οι οποίοι προασπίζονται την ακόλουθη ιδέα :

- Παρά τις αδυναμίες της, η ιδέα του ψηφιακού νομίσματος αποτελεί σίγουρα πρωτοπορία και δεν είναι απίθανο σενάριο το να εξελιχθεί περαιτέρω, να υιοθετηθεί και προοδευτικά να αντικαταστήσει τα υπόλοιπα νομίσματα παγκοσμίως.

Ανεξάρτητα από τις παραπάνω απόψεις, το bitcoin αν και θα λέγαμε πως έφτασε στο απόγειο της επιτυχίας του πριν από μερικά χρόνια, εξακολουθεί να κεντρίζει το ενδιαφέρον πολλών χρηστών κατά μήκος όλου του κόσμου, ο καθένας από τους οποίους έλαβε υπόψιν αυτούς τους παράγοντες, ζύγισε την κατάσταση από την δική του οπτική και τάχθηκε υπέρ του ψηφιακού νομίσματος (Antonopoulos, 2015). Άλλωστε, όπως είπαμε και παραπάνω, σύμφωνα με τα διαδικτυακά αποσπάσματα της Casey Leigh (2018) αλλά και με το έργο του Antonopoulos (2015), καλύτερη πρόληψη αλλά και αντιμετώπιση των κινδύνων, είναι η σωστή και εκτενής ενημέρωση πάνω στο θέμα, η λήψη των απαραίτητων μέτρων ασφαλείας και η κατανόηση του ρίσκου απώλειας των καταθέσεών μας.

5. ΣΥΖΗΤΗΣΗ

Τα ψηφιακά νομίσματα εισήχθησαν στον κόσμο των συναλλαγών και έχουν γνωρίσει τεράστια επιτυχία μέσα σε ένα πολύ μικρό χρονικό διάστημα. Παρά την ανοδική τους πορεία, πολλοί άνθρωποι σήμερα δεν είναι ακόμα έτοιμοι για αυτά, καθώς δεν είναι διατεθειμένοι να εμπιστευθούν νέες μεθόδους πληρωμών, δυσκολεύονται να κατανοήσουν την μηχανική τους, θεωρούν περιττή αυτού του είδους την εξέλιξη, είτε απλά δεν καταφέρνουν να εξοικειωθούν με την τεχνολογία που απαιτείται για την εφαρμογή τους. Είναι γεγονός πως η χρήση του bit-coin απαιτεί τις απαραίτητες γνώσεις στον τομέα της τεχνολογίας, οι οποίες αν και δεν είναι σημαντικά υψηλές, είναι αδιαπραγμάτευτα το πιο σημαντικό, ίσως μοναδικό για πολλούς κριτήριο για την ορθή χρήση του. Εάν λάβουμε υπόψιν πως δεν υπάρχει διαχειριστική ομάδα διατεθειμένη να μας βοηθήσει σε περίπτωση που δεν γνωρίζουμε το πώς πρέπει να κινηθούμε, ούτε για να διορθώσει τυχόν λάθη μας, είναι αυτονόητο πως άτομα που δεν είναι ιδιαίτερα εξοικειωμένα με την τεχνολογία, δεν θα εμπιστεύονταν πρώτα τους εαυτούς τους με μηχανές που δεν ξέρουν να χειρίζονται άπταιστα, πόσο μάλλον για να διαχειριστούν τα χρήματά τους μέσω αυτών.

Ανεξάρτητα από το προσωπικό λάθος η ηλεκτρονική απάτη βασίζεται και στις ατασθαλίες του χρήστη, ο οποίος εάν δεν λάβει τα απαραίτητα μέτρα ασφαλείας, τα ψηφιακά κεφάλαιά του βρίσκονται σε διαρκή κίνδυνο. Συνεπώς, η απομάκρυνση ενός μεγάλου μέρους του πληθυσμού από την χρήση των ψηφιακών νομισμάτων οφείλεται στην έλλειψη τεχνογνωσίας, και όχι στον φόβο μιας νέας διαφορετικής μεθόδου πληρωμών. Αρκεί να θυμηθούμε πως η ίδια κατάσταση αντιμετωπίστηκε σε όλες τις χώρες με το πλαστικό χρήμα, όπου πολλοί ήταν οι άνθρωποι που δεν ήταν διατεθειμένοι να το δοκιμάσουν ή να το εμπιστευθούν. Παρόλο που ακόμα και σήμερα ένα μέρος του πληθυσμού αποφεύγει τις ηλεκτρονικές κάρτες πληρωμών (χρεωστικές – πιστωτικές – προπληρωμένες), το ποσοστό αυτό είναι μικρό, με τις τράπεζες να επιχειρούν να κάνουν τις κάρτες όλο και πιο απλοϊκές στην χρήση και κατανόηση και φιλικές προς τον χρήστη. Την στιγμή που ο χρήστης κατάλαβε την μέθοδο με την οποία λειτουργεί η ηλεκτρονική κάρτα, απέκτησε εμπιστοσύνη στην τράπεζα και κυρίως στον ίδιο του τον εαυτό καθώς ήξερε πλέον τι πρέπει να κάνει και πώς να το κάνει. Τα ίδια ερωτήματα είναι αυτά που αποτρέπουν τον άνθρωπο σήμερα από το να στραφεί στα ψηφιακά νομίσματα, τα οποία ωστόσο είναι λίγο πιο περίπλοκα και απαιτούν μεγαλύτερο κόπο για να κατανοηθούν σε βαθμό ώστε ο χρήστης να νοιώθει πλέον ασφαλής, μα με την στροφή όλο και περισσοτέρων ανθρώπων στην τεχνολογία σήμερα, και όσο το bit-coin παραμένει στο προσκήνιο ως μια ικανοποιητική μέθοδος πληρωμών, φαντάζει θέμα χρόνου το να σπάσουν οι παραπάνω φραγμοί και φοβίες και προοδευτικά να υιοθετηθεί από ακόμα περισσότερους ανθρώπους και ίσως, όπως υποστηρίζει και ο Wallace (2011), το bit-coin να είναι όντως το νόμισμα του μέλλοντος.

Από μία πιο προσωπική οπτική, μοναδική ανησυχία και μεγάλο ερωτηματικό για την πορεία του bit-coin είναι αυτό της ασφάλειας του δικτύου όταν εξορυχθεί το τελευταίο bit-coin. Όπως είδαμε παραπάνω, κάτι τέτοιο δεν υφίσταται, δηλαδή η ταχύτητα με την οποία δημιουργούνται τα bit-coin περιορίζεται και ελαττώνεται μα ποτέ δεν θα μηδενιστεί.

Κάποια στιγμή ωστόσο, η υπολογιστική ισχύς που θα απαιτηθεί για την δημιουργία του επόμενου νομίσματος θα είναι τόσο μεγάλη που η διαδικασία της εξόρυξης δεν θα αποτελεί πλέον κερδοφόρα διαδικασία. Όπως εξηγήσαμε πιο πάνω, ο κάθε χρήστης που ασχολείται με την εξόρυξη, στηρίζει την θεμιτή πλευρά του δικτύου του bit-coin. Αυτό συμβαίνει ασκώντας δύναμη σε ένα σκοινί από την μία μεριά, συνεπώς αυτός που θα επιχειρήσει να αλλοιώσει την αλυσίδα και να λυγίσει το σύστημα προς όφελος του, θα πρέπει να ασκήσει μεγαλύτερη δύναμη από όλους αυτούς που το στηρίζουν. Η διαδικασία της εξόρυξης όμως είναι μια διαδικασία που έχει κόστος, αυτό του ηλεκτρικού ρεύματος. Συνεπώς ο χρήστης που θα καταναλώσει όλη εκείνη την ενέργεια για να στηρίξει το σύστημα (εξόρυξη), περιμένει την κατάλληλη ανταμοιβή σε bit-coin. Μοιάζει λογικό να σκεφτεί κανείς λοιπόν πως όταν η εξόρυξη πάψει να είναι μια κερδοφόρα διαδικασία, πολλοί (αν όχι όλοι) οι χρήστες θα σταματήσουν το mining καθώς θα βγαίνουν ζημιωμένοι και συνεπώς θα σταματήσουν να στηρίζουν το σύστημα, το οποίο θα είναι πλέον πολύ πιο ευάλωτο σε εξωτερικές επιθέσεις. Το προσωπικό όφελος των χρηστών κατά τη διαδικασία του mining θα υπόκειται μονάχα στους τόκους των συναλλαγών οι οποίοι ωστόσο δεν καλύπτουν παρά μόνο ένα μικρό ποσοστό των εξόδων που απαιτούνται. Σε μία στιγμή αδυναμίας η ασφάλεια του συστήματος μοιάζει ιδιαίτερα πιθανό να παραβιαστεί και συνεπώς το bit-coin να χάσει όλη του την αξία.

Από την άλλη, είναι επίσης πιθανό σενάριο η διαδικασία του mining να συνεχιστεί από όλους τους χρήστες και όχι απλά από λίγους όπως σήμερα επιδιώκοντας υψηλά κέρδη, προκειμένου τα έξοδα να μοιραστούν σε ένα μεγάλο αριθμό χρηστών ώστε να είναι ιδιαίτερα χαμηλά, προκειμένου το bit-coin να συνεχίσει να κυριαρχεί. Πιο προβλέψιμο κατά την προσωπική μου γνώμη είναι το πρώτο σενάριο, κατά το οποίο οι miners θα ελαττωθούν σε αριθμό σημαντικά, και το ερώτημα στο οποίο θα απαντήσει μόνο ο χρόνος, είναι το εάν αυτοί που θα απομείνουν θα είναι αρκετοί για να το διατηρήσουν. Από την οπτική του 2019 βασικό μακροχρόνιο πρόβλημα φαντάζει αυτό, μα εάν θυμηθούμε πως οι κυβερνήσεις δεν έχουν καμία ανάμειξη ακόμα με το ψηφιακό αυτό νόμισμα, εάν τελικά αναλάβουν και αυτές πρωτοβουλίες επί του θέματος και μπουν στην εξίσωση με τρόπο υποστηρικτικό είτε μη λαμβάνοντας τα αντίστοιχα μέτρα, τότε η πορεία του bit-coin δεν θα ήταν δυνατό να προβλεφθεί.

ΠΡΟΤΑΣΕΙΣ ΓΙΑ ΜΕΛΕΤΗ:

Η παραπάνω εργασία θα ήταν εύκολο αλλά και ιδιαίτερα ενδιαφέρον να συνεχισθεί και συμπληρωθεί με περαιτέρω πληροφορίες. Όπως αναφέρθηκε από πάνω παρά τους ήδη μεγάλους διασκελισμούς του, το bit-coin θα λέγαμε πως βρίσκεται ακόμα στα αρχικά του στάδια. Κρατικές παρεμβάσεις έχουν σημειωθεί σε περιορισμένο βαθμό και πολλές κυβερνήσεις δεν κρατούν ξεκάθαρη στάση απέναντι σε αυτό το ζήτημα. Σε μίαν αντίστοιχη εργασία μπορεί να αναλυθεί σε μεγαλύτερο βάθος αυτός ο κρατικός παρεμβατισμός και τα μέτρα που έχουν ληφθεί για να ικανοποιήσουν θέματα φορολογίας αλλά και για να αντιμετωπίσουν περιπτώσεις φοροδιαφυγής και ξεπλύματος χρήματος. Επίσης, η εργασία αυτή αφιερώθηκε συγκεκριμένα στο bit-coin, μα υπάρχουν πολλά νέα και προσφάτως εμφανιζόμενα ψηφιακά νομίσματα, όπως το Ethereum και το Ripple και θα ήταν εξίσου ενδιαφέρον να παρακολουθηθεί η πορεία και απήχηση ενός η περισσοτέρων από αυτών αλλά και να εντοπισθούν τυχόν ομοιότητες και διαφορές ανάμεσα στον τρόπο με τον οποίο λειτουργούν.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Eskandari, S., Barrera, D., Stobert, E., & Clark, J. (2015). A First Look at the Usability of Bitcoin Key Management. *Paper presented at NDSS Workshop on Usable Security (USEC) 2015, San Diego, CA, USA, February 8, 2015, Internet Society*.

Nakamoto, S. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System. Cryptography Mailing list at https://metzdowd.com.

Grinberg, R. (2011). Bitcoin: An Innovative Alternative Digital Currency. *Hastings Science & Technology Law Journal*, 4(1), 159-208.

Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, Technology, and Governance. *Journal of Economic Perspectives*, 29(2), 213-238.

Hurlburt, G. F., & Bojanova, I. (2014). Bitcoin: Benefit or Curse? *IT Professional*, 16(3), 10-15.

Barber, S., Boyen, X., Shi, E., & Uzun, E. (2012). Bitter to Better — How to Make Bitcoin a Better Currency. In A. Keromytis (Ed.), *Financial Cryptography and Data Security. 16th International Conference, FC 2012, Kralendijk, Bonaire, Februray 27-March 2, 2012, Revised Selected Papers*. Heidelberg (Germany): Springer.

Yermack, D. (2015). Is Bitcoin a Real Currency? An Economic Appraisal. In D. L. Kuo Chuen (Ed.), *Handbook of Digital Currency. 1st Edition. Bitcoin, Innovation, Financial Instruments, and Big Data* (pp. 31-43). Salt Lake City (USA): Academic Press.

Antonopoulos, A., M. (2015). Mastering Bitcoin: Unlocking Digital Cryptocurrencies *1st Edition*. Sebastopol (USA): O' Reilly Media, Inc.

Bedford Taylor, M. (2013). Bitcoin and the age of Bespoke Silicon. *Paper presented at International Conference on Conference on Compilers, Architectures and Synthesis for Embedded Systems, Montreal, Quebec, Canada – September 29-October 04, 2013*. NJ (USA): IEEE Press Piscataway.

Bedford Taylor, M. (2017). The Evolution of Bitcoin Hardware. *Computer*, 50(9), 58-66.

Penning, N., Hoffman, M., Nikolai, J., & Wang, Y. (2014). Mobile malware security challeges and cloud-based detection. *Paper presented at International Conference on Collaboration Technologies and Systems (CTS), Minneapolis, Minnesota, USA – 19-23 May, 2014*. NY (USA): Curran Associates, Inc.

Kaplanov, N., M. (2012). Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against Its Regulation. *SSRN Electronic Journal*, 25(1), 111-174.

Morris, R., & Thompson, K. (2002). Password Security: A Case History. *Communications of the ACM*, 22(11), 594-597.

Slattery, T. (2014). Taking a Bit out of Crime: Bitcoin and Cross-Border Tax Invasion. *Brooklyn Journal of International Law*, 39(2), 829-873.

Szabo, N. (2011). Bitcoin: What took ye so long?

Wallace, B. (2011). The Rise and Fall of Bitcoin.

U.S. Patent No. 4434323. (1984). Washington, DC: U.S. Patent and Trademark Office.

A. A. (2017, May 11). Bitcoin Q&A [Interview]. *Retrieved from https://www.youtube.com/watch?v=Aji_E9sw0AE*.

What is Blockchain and WHY was it Developed? (A Simple Explanation) [Audio blog review]. (2017, November 1). Retrieved from https://www.youtube.com/watch?v=4AwCMGBn6w0.

How to Buy Cryptocurrency for Beginners (Ultimate Step-by-Step Guide) [Audio blog review]. (2018, January 6). *Retrieved from https://www.youtube.com/watch?v=xYWMzczqgk4*

Weacceptbitcoin. (n.d.). *Retrieved from https://www.weacceptbitcoin.com/*

Bitcoin charts. (n.d.). *Retrieved from https://www.coin.dance.com/poli*

Bitcoin Tips, Tutorials & Community. (2017, June 27). *Retrieved from https://www.coinsutra.com/*