ΣΧΟΛΗ ΕΠΙΣΤΗΜΩΝ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΤΜΗΜΑ ΛΟΓΙΣΤΙΚΗΣ ΚΑΙ ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΗΣ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΣΤΗΝ ΛΟΓΙΣΤΙΚΗ
ΦΟΡΟΛΟΓΙΑ ΚΑΙ ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΗ ΔΙΟΙΚΗΣΗ

Διπλωματική Εργασία

Το Bitcoin και το Τρίλημμα της επεκτασιμότητας

Καρράς Γεώργιος

Επιβλέπων Καθηγητής: Ζαπράνης Αχιλλέας

Αύγουστος 2023

ΕΥΧΑΡΙΣΤΙΕΣ

Ολοκληρώνοντας τον κύκλο σπουδών μου στο μεταπτυχιακό πρόγραμμα ¨Λογιστική φορολογία και Χρηματοοικονομική διοίκηση¨ του Πανεπιστημίου Μακεδονίας, θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή μου κ. Ζαπράνη Αχιλλέα, τόσο για την καθοδήγηση και βοήθεια που μου πρόσφερε, όσο και για την συμβολή του στο να αναπτύξω περεταίρω τις γνώσεις μου πάνω σε ένα τρομερά καινοτόμο και ενδιαφέρον θέμα όπου είναι το Bitcoin. Επίσης, θα ήθελα να ευχαριστήσω και όλους τους διδάσκοντες που «συνάντησα» κατά τη διάρκεια της φοίτησης μου στο μεταπτυχιακό καθώς όλοι τους συνέβαλαν στον εμπλουτισμό των γνώσεων μου.

Τέλος, θα ήθελα να ευχαριστήσω πολύ και την οικογένεια μου που μου στάθηκε σε όλη την διάρκεια του μεταπτυχιακού προγράμματος.

"I do think Bitcoin is the first (encrypted money) that has the potential to do something like changing the world."

Peter Thiel, co-founder of PayPal

"The future of money is digital currency."

Bill Gates, co-founder of Microsoft

ΠΕΡΙΛΗΨΗ

Τα ψηφιακά νομίσματα, και ιδιαίτερα το Bitcoin, αποτελούν μια από τις σημαντικότερες καινοτομίες που έχει αναδείξει η εξέλιξη της τεχνολογίας τις τελευταίες δεκαετίες. Αν και βρίσκονται ακόμα σε πρώιμο στάδιο, έχουν εισχωρήσει αρκετά στις ζωές εκατομμυρίων ανθρώπων. Στην παρούσα διπλωματική εργασία δίνεται βάση στο Bitcoin, το πρώτο που δημιουργήθηκε αλλά και μεγαλύτερο σε κεφαλαιοποίηση ψηφιακό νόμισμα. Οι ανώνυμες συναλλαγές, η ασφάλεια που προσφέρει σε αυτές, η διαφάνεια τους καθώς και η αποκέντρωση του είναι μερικά από τα χαρακτηριστικά που κάνουν το Bitcoin τόσο ελκυστικό. Στον αντίποδα, ένα σοβαρό εμπόδιο που επιβραδύνει αρκετά την υιοθέτηση του παγκοσμίως είναι η ταχύτητα με την οποία εκτελούνται οι συναλλαγές καθημερινά χρησιμοποιώντας το. Σκοπός της διπλωματικής, είναι να αναλυθεί το δίκτυο του Bitcoin καθώς και τεχνολογία που το ακολουθεί, να σχολιαστούν τα τρία χαρακτηριστικά που απασχολούν κάθε χρηματοπιστωτικό ίδρυμά τα οποία είναι η αποκέντρωση η ταχύτητα και η ασφάλεια, και τέλος να παρατεθούν μερικές από τις επικρατέστερες λύσεις που χρησιμοποιούνται σήμερα για την λύση στο πρόβλημα της ταχύτητας του δικτύου του Bitcoin. Στο πρώτο μέρος της διπλωματικής εργασίας θα αναλυθεί η ιστορια του Bitcoin, θα συγκριθεί με το χρήμα αλλά και με τον χρυσό και θα σχολιαστεί ο τρόπος που παράγεται αλλά και άλλα τεχνικά χαρακτηριστικά του. Μετέπειτα, στο δεύτερο σκέλος της εργασίας θα αναφερθούν οι λύσεις που μπορούν να υιοθετηθούν για να μετατραπεί το δίκτυο του Bitcoin σε ένα πιο αξιόπιστο και εύχρηστο δίκτυο συναλλαγών αλλά και αν αυτό τελικά είναι εφικτό.

ABSTRACT

Digital currencies, and Bitcoin in particular, are one of the most important innovations that the evolution of technology has highlighted in recent decades. Although they are still at an early stage, they have invading into the lives of millions of people. In this th esis, the focus is on Bitcoin, the first created and the largest digital currency in terms o f capitalization. The anonymous transactions, the security it offers, its transparency an d its decentralization are some of the features that make Bitcoin so attractive. On the c ontrary, a serious obstacle that is slowing down its adoption worldwide is the speed at which transactions are carried out daily using it. The purpose of this thesis is to analyz e the Bitcoin network and the technology that follows it, to comment on the three char acteristics that concern every financial institution, which are decentralization, speed, a nd security, and finally to list some of the most prevalent solutions that are currently u sed to solve the problem of Bitcoin network's speed.

In the first part of this thesis the history of Bitcoin will be analyzed, it will be compare d with money and gold and the way it is produced and other technical characteristics o f Bitcoin will be commented on. Later, in second time, it will be discussed the solutions which can be adopted to transform the Bitcoin netwo rk into a more reliable and easy transaction network to use and if all this stuff is ultimately possible to work.

ΠΕΡΙΕΧΟΜΕΝΑ

Ευχαριστίες……..…2

Περίληψη……4

Abstract…….….5

Κατάλογος Εικόνων…….....8

ΚΕΦΑΛΑΙΟ 1: Bitcoin……..9

1.1 Τι Είναι Bitcoin…….....9

1.2 Ιστορία Του Bitcoin……...10

1.3 Η Πρώτη Ισοτιμία – Συναλλαγή…….……...11

1.4 Πως Λειτουργεί Το Δίκτυο Του Bitcoin……..…12

1.5 Halving Event……..……13

1.6 Τρόποι Αγοράς Και Διαφύλαξης Bitcoin…….……..15

1.7 Πλεονεκτήματα Και Μειονεκτήματα Του Bitcoin…….……17

ΚΕΦΑΛΑΙΟ 2: Χρήμα…….……19

2.1 Τι Είναι Χρήμα…….……..19

2.2 Η Εξέλιξη Του Χρήματος……..……..20

2.3 Χρήμα Και Bitcoin…….…….……21

ΚΕΦΑΛΑΙΟ 3: Χρυσός……..…….……...23

3.1 Bitcoin Και Χρυσός…….……..……..23

3.2 Πόσο Σπάνιος Είναι ο Χρυσός Και Πόσο Το Bitcoin…….……..……..23

3.3 Πόσο Εύχρηστος Είναι ο Χρυσός Και Πόσο Το Bitcoin……..……..…25

ΚΕΦΑΛΑΙΟ 4: Εξόρυξη Του Bitcoin…….…….……..……..26

4.1 Εξέλιξη Του Mining……..…..…….…….27

4.2 Η Διαδικασία Εξόρυξης……...…….……28

4.3 Το Μυστικό Για Σταθερή Παραγωγή……..…..…….29

4.4 Ο Ζωντανός Οργανισμός Που Λέγεται Bitcoin Και Τα Έξοδα Διαβίωσης Του……..30

ΚΕΦΑΛΑΙΟ 5: Το Τρίλημμα Του Δικτύου Του Bitcoin.....31

5.1 Το Τρίλημμα Του Δικτύου Του Bitcoin……31

5.2 Ποιος Διοικεί Το Bitcoin……..32

5.3 Πόσο Ασφαλές Είναι Το Δίκτυο Του Bitcoin……...…33

5.4 Ποιες Είναι Οι Δυνατότητες Κλιμάκωσης Του Δικτύου……..35

ΚΕΦΑΛΑΙΟ 6: Λύσεις Στο Πρόβλημα Κλιμάκωσης Του Bitcoin……..36

6.1 Lighting Network…….36

6.1.a Τι Είναι Το Lighting Network…….37

6.1.b Πως Λειτουργεί Το Lighting Network……38

6.1.c Θετικά Και Αρνητικά Του Lighting Network ……40

6.2 Αύξηση Στο Μέγεθος Των Συστοιχιών……...44

6.3 Liquid Network……48

6.4 Blockchain Sharding ……...51

Συμπεράσματα……..55

Βιβλιογραφία……57

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

Εικόνα 1: Bitcoin ……..……. 8

Εικόνα 2: Άγαλμα Του Ιδρυτή Του Bitcoin, Satoshi Nakamoto Στην Βουδαπέστη .. 10

Εικόνα 3: Συστοιχίες Στο Δίκτυο Του Bitcoin ...…….. 11

Εικόνα 4: Ρυθμός Παραγωγής Bitcoin Ανά Συστοιχίες.…… 13

Εικόνα 5: Cold Wallets, Ειδικές Συσκευές Για Διαφύλαξη Κρυπτονομισμάτων 15

Εικόνα 6: Bitcoin Και Χρήμα ...…….. 19

Εικόνα 7: Bitcoin Και Χρυσός ...…… 21

Εικόνα 8: Εξόρυξη Bitcoin ……. 25

Εικόνα 9: Μονάδα Εξόρυξης Bitcoin ……. 26

Εικόνα 10: Το Τρίλημμα Του Bitcoin ...…….. 29

Εικόνα 11: Το Δίκτυο Του Bitcoin …….. 30

Εικόνα 12: Bitcoin …….. 31

Εικόνα 13: Lighting Network ……. 34

Εικόνα 14: Παράδειγμα Μεταφοράς Αξίας Στο Lighting Network ……... 36

Εικόνα 15: Συστοιχίες Του Δικτύου Του Bitcoin ……. 42

Εικόνα 16: Liquid Network …… 45

Εικόνα 17: Blockchain Sharding …… 48

ΚΕΦΑΛΑΙΟ 1: BITCOIN

«Εικόνα 1»

1.1)Τι είναι Bitcoin

Το Bitcoin, είναι το πρώτο ψηφιακό νόμισμα στην ιστορία των χρηματοοικονομικών αγορών και αποτελεί τον πρωτοπόρο στον κόσμο των «κρυπτονομισμάτων». Με την δημιουργία του (2009), αναπτύχθηκε μια σπουδαία τεχνολογία η οποία έκανε αρκετό κόσμο να την αγαπήσει και να την κάνει τόσο δημοφιλή σήμερα. Το βασικό χαρακτηριστικό του είναι πως δημιουργήθηκε με σκοπό να λειτουργεί σε ένα πλήρης αποκεντρωμένο δίκτυο (blockchain) με αποτέλεσμα να μην μπορεί να ελεγχτεί από καμία κυβέρνηση ή κάποια μεμονωμένη οντότητα. Κανείς δεν είναι ιδιοκτήτης του δικτύου του Bitcoin ενώ ελέγχεται συλλογικά από τους χρήστες του ανά τον κόσμο. Επιπρόσθετα άλλο ένα σπουδαίο χαρακτηριστικό του είναι πως στις συναλλαγές δεν χρειάζεται την παρέμβαση ενός μεσάζοντα όπως κάποιας τράπεζας γλιτώνοντας έτσι την προμήθεια που θα κρατούσε για τις υπηρεσίες της αλλά και τον έλεγχο που θα μπορούσε να ασκήσει στους τραπεζικούς λογαριασμούς των χρηστών της.

Ο καθένας με πρόσβαση στο internet και ακολουθώντας κάποια απλά βήματα μπορεί να μεταφέρει αξία σε κάποιον που βρίσκεται δίπλα του ή και σε άλλη χώρα μέσα σε λίγα λεπτά. Μπορεί να του στείλει ένα Bitcoin , πολλαπλά ή ακόμα και ένα μικρό κομματάκι αυτού με τον φόρο μεταφοράς (fee) να αποτελεί ένα σχεδόν αμελητέο ποσό.

Το Bitcoin θα μπορούσε να παρομοιαστεί και σαν ένα λογιστικό βιβλίο στο οποίο όλες οι συναλλαγές καταγράφονται (από την πρώτη μέχρι και σήμερα). Είναι διαθέσιμες στο κοινό χωρίς όμως να μπορεί κάποιος να επέμβει και να τις τροποποιήσει το οποίο αναμφίβολα παρέχει ένα συναίσθημα διαφάνειας και ασφάλειας στον χρήστη.

1.2) Ιστορία Του Bitcoin

Η ιδέα για την δημιουργία ενός παγκόσμιου ψηφιακού νομίσματος που να είναι εντελώς ανώνυμο και έτσι να μην μπορεί να ελεγχτεί από καμία κυβέρνηση γεννήθηκε για πρώτη φορά από τον κρυπτογράφο David Chaum το μακρινό 1985. Μια δημοσίευση του με τίτλο «Security without identification : Transaction Systems to Make Big Brother Obsolete» (Ασφάλεια χωρίς ταυτοποίηση : Συστήματα συναλλαγών που θα κάνουν το Big Brother ξεπερασμένο) ήταν η σπίθα για να ξεκινήσει μια επανάσταση. Βασισμένη στην ιδέα του Chaum δημιουργήθηκε μια ομάδα αλληλογραφίας (mailing list) με το όνομα Cypherpunks σχετικά με το χώρο της κρυπτογραφίας μέσω υπολογιστή. Το 1998 ένα μέλος της ομάδας και μηχανικός λογισμικού, ο Wei Dai , δημοσίευσε την πρόταση του για ένα διαμοιρασμένο σύστημα ηλεκτρονικών χρημάτων το οποίο ονόμασε B-money. Λίγο αργότερα, την σκυτάλη πήρε ένας Αμερικάνος ακαδημαϊκός στον χώρο της πληροφορικής εν ονόματι Nick Szabo, όπου το έτος 2005 στο προσωπικό του blog εξέφρασε την άποψη του για ένα νέο ψηφιακό νόμισμα. Το ονόμασε Bit gold, ένα ψηφιακό συλλεκτικό είδος στο οποίο όχι μόνο θα μπορούσε να έχει πρόσβαση ο καθένας αλλά θα μπορούσε και να το παράγει σε αντίθεση με τον χρυσό. Η μόνη προϋπόθεση όμως να μπορούν να υπάρξουν περιορισμένα κομμάτια έτσι ώστε να μην μειώνεται η αξία του λόγω πληθωρισμού.

Αν και η πρόταση του Szabo δεν εφαρμόστηκε ποτέ, ήταν ο πρόδρομος της δημιουργίας του Bitcoin. Έτσι τον Οκτώβριο του 2008 έγινε η πρώτη επιστημονική δημοσίευση με τίτλο ¨Bitcoin: A Peer-to-Peer Electronic Cash System¨. Ο συγγραφέας την υπέγραψε ως Satoshi Nakamoto. Γύρω από το ψευδώνυμο αυτό έχουν σχηματιστεί αρκετές θεωρίες καθώς μέχρι και σήμερα κανείς δεν γνωρίζει την πραγματική του ταυτότητα, αν ήταν ένα άτομο ή ομάδα ατόμων, την εθνικότητά του, το φύλο του ή την

ηλικία του. Στις αρχές του 2009, έγινε και η πρώτη παραγωγή Bitcoin ενώ ο Satoshi αποσύρθηκε από το έργο του στα τέλη του 2010. Για περίπου έναν χρόνο παρόλα αυτά (2009-2010), το Bitcoin δεν είχε καμία αξία. Ένας χρήστης μάλιστα προσέφερε 10.000 Bitcoin έναντι 50 δολαρίων αλλά για καλή του τύχη τελικά δεν κατάφερε να βρει αγοραστή.

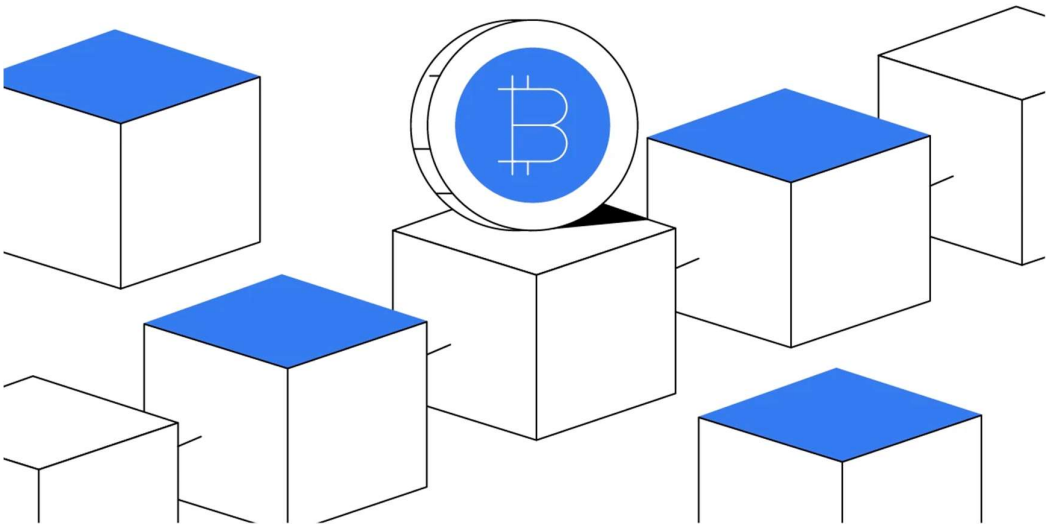
«Εικόνα 2»

1.3) Η Πρώτη Ισοτιμία – Συναλλαγή

Ο Μάρτιος του 2010 ήταν ένας ιστορικός μήνας για το οικοσύστημα του Bitcoin καθώς για πρώτη φορά του δόθηκε αξία. Το ανταλλακτήριο Bitcoin market.com έδωσε

την πρώτη ισοτιμία μεταξύ Bitcoin και δολαρίου στα 0.003 δολάρια. Η πρώτη συναλλαγή έγινε δύο μήνες μετά.

1.4) Πως Λειτουργεί Το Δίκτυο Του Bitcoin



«Εικόνα 3»

Το Bitcoin, θεωρείται πιθανώς η μεγαλύτερη καινοτομία στο χρηματοοικονομικό σύστημα εδώ και έναν αιώνα. Είναι ενδεχομένως μεγαλύτερη και από την εμφάνιση των πιστωτικών καρτών. Είναι ένα εντελώς ψηφιακό νόμισμα και δεν υπάρχει σε καμία άλλη μορφή όπως κερμάτων ή χαρτονομισμάτων άρα η παραγωγή του, η διακίνηση του αλλά και η αποθήκευση του γίνονται αποκλειστικά σε ηλεκτρονική μορφή. Το σύνολο των νομισμάτων που έχουν παραχθεί είναι μοιρασμένο σε ψηφιακά πορτοφόλια (Bitcoin wallets) των χρηστών που συμμετέχουν στο δίκτυο, το οποίο ονομάζεται peer to peer(ομότιμο δίκτυο), και εξαρτάται από τους χρήστες(peers) και μόνο και όχι από κάποιο κεντρικό server όπως μιας τράπεζας για παράδειγμα.

Όταν πραγματοποιείται μια συναλλαγή ανάμεσα από δύο χρήστες, ξεκινάει μια συγκεκριμένη διαδικασία προκειμένου να επιβεβαιωθεί η εγκυρότητα της. Αρχικά

επιβεβαιώνονται οι διευθύνσεις των δύο διαφορετικών πορτοφολιών (wallets). Αμέσως μετά, με κάποιους περίπλοκους μαθηματικούς υπολογισμούς επιβεβαιώνεται η εγκυρότητα και ολοκληρώνεται η συναλλαγή. Κάθε έγκυρη συναλλαγή καταγράφεται σε έναν αποθηκευτικό χώρο που ονομάζεται συστοιχία (block) και δεν μπορεί να διαγραφτεί από αυτό. Όταν η συστοιχία καταγράψει τον μέγιστο αριθμό συναλλαγών που μπορεί "κλείνει" και ένα άλλο παίρνει την θέση του για να συνεχίσει την καταγραφή. Το σύνολο των συστοιχιών ονομάζεται blockchain(αλυσίδα από κουτάκια) και ουσιαστικά είναι ένα κοινόχρηστο δημόσιο λογιστικό βιβλίο πάνω στο οποίο βασίζεται ολόκληρη η τεχνολογία και το δίκτυο του Bitcoin. Όλες οι συναλλαγές που έχουν εκτελεστεί από την πρώτη μέρα ύπαρξης του Bitcoin μέχρι και σήμερα έχουν καταγραφεί στο blockchain καθώς και με την σωστή σειρά.

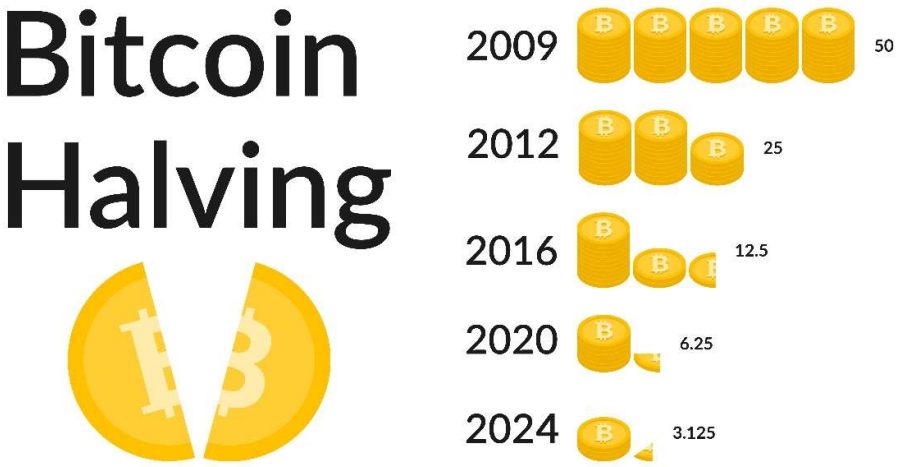
Η καινοτομία του, εκτός από το ότι τα δεδομένα είναι υπογεγραμμένα ψηφιακά μέσω κρυπτογραφίας και άρα έχουμε ήδη από αυτό κάποιο βαθμό ασφάλειας, είναι πως δεν υπάρχει μόνο ένα αντίγραφο αλλά πάρα πολλά διαμοιρασμένα σε υπολογιστές σε όλο τον κόσμο. Αυτό είναι τρομερά σημαντικό επειδή έτσι δεν υπάρχει κάποιος κεντρικός διαχειριστής ο οποίος μπορεί να παρέμβει και να αλλοιώσει τα δεδομένα, οπότε ενισχύεται η αξιοπιστία του δικτύου μιας που υπάρχει η μεγαλύτερη δυνατή διαφάνεια.

1.5) Halving Event

Οι οικονομικοί κύκλοι είναι ένα φαινόμενο το οποίο απασχολεί γενικά όλους τους επενδυτές. Η εναλλαγή από την ανάπτυξη στην ύφεση, είναι μια διαδικασία που επαναλαμβάνεται σε διάφορες παραλλαγές, με την σημαντική λεπτομέρεια όμως, πως δεν είναι σταθεροί και επηρεάζονται σοβαρά από εξωγενείς παράγοντες καθώς και από την ψυχολογία των επενδυτών. Στο Bitcoin τα πράγματα είναι πιο ξεκάθαρα. Κάθε κύκλος είναι μέσα σε σχετικά σταθερό χρονικό πλαίσιο και λόγος είναι το "Halving Event". Πρόκειται, ίσως, για το μεγαλύτερο φαινόμενο στον κόσμο των κρυπτονομισμάτων και αποτελεί συνήθως την αίτια αλλαγής από ύφεση σε ανάπτυξη. Συμβαίνει περίπου κάθε 4 χρόνια, και στην ουσία μειώνεται η ποσότητα παραγωγής στο μισό, με αποτέλεσμα να μειώνεται η διαθέσιμη προσφορά, η ζήτηση να παραμένει

σταθερή ή και να αυξάνεται και η τιμή να ακολουθεί ανοδική τάση. Είναι ένα γεγονός που δεν μπορεί να αλλάξει ή να σταματήσει διότι πρόκειται για μαθηματικές εξισώσεις που βρίσκονται δημόσια στον ανοιχτό κώδικα του Bitcoin, και δεν μπορούν να αλλοιωθούν από τον χρόνο ή να επηρεαστούν από εξωγενές συνθήκες.

Με την λειτουργεία του δικτύου του Bitcoin, τη 1η Ιανουαρίου του 2009, η ανταμοιβή για κάθε νέα συστοιχία ήταν 50 Bitcoin. Σχεδόν τέσσερα χρόνια μετά, τον Νοέμβριο του 2012, πραγματοποιήθηκε το πρώτο Halving Event και η παραγωγή μειώθηκε στα 25. Το ίδιο έγινε και τον Ιούλιο του 2016 όπως και τον Μάιο του 2020, όπου η παραγωγή κάθε φορά μειωνόταν στο μισό. Έτσι από 25 Bitcoin ανά συστοιχία έφτασε στα 12,5 και αργότερα στα 6,25. Έχουν πραγματοποιηθεί τρία Halving Event μέχρι στιγμής και τον Απρίλιο του 2024 αναμένεται το τέταρτο, όπου θα μειώσει την παραγωγή στα 3,125 Bitcoin, αλλά όπως έχει δείξει η ιστορία θα γνωρίσει ανοδική τάση η τιμή του, αφού όλο και περισσότεροι θα αρχίσουν να αντιλαμβάνονται πόσο σπάνιο είναι.



«Εικόνα 4»

Ένα ερώτημα που γεννιέται, αμέσως μετά την ανάλυση του Halving, είναι τι θα ωθεί τους miners να συνεχίζουν να σπαταλάνε όλη αυτή την ενέργεια, για να συνεχίσει να λειτουργεί το δίκτυο του Bitcoin, αφού εξορυχθεί και το τελευταίο Bitcoin. Οι ανταμοιβές τους όμως, εκτός από τις επιβραβεύσεις που λαμβάνουν με κάθε νέα

συστοιχία, βασίζονται και στις συναλλαγές του δικτύου, αφού από κάθε συναλλαγή λαμβάνουν ένα μικρό ποσό σαν ¨φόρο¨. Έτσι θεωρητικά, αν το Bitcoin ¨υιοθετηθεί¨ από περισσότερο κόσμο στο μέλλον, αφού το τελευταίο Bitcoin θα παραχθεί το 2140, οι συναλλαγές θα αυξηθούν κατά πολύ, όπως και η τιμή του, και θα καθιστά βιώσιμο το mining ακόμα και χωρίς τις ανταμοιβές από τις νέες συστοιχίες.

1.6) Τρόποι αγοράς και διαφύλαξης Bitcoin

Η αγορά Bitcoin, έχει καθιερωθεί πλέον ως μια αρκετά εύκολη διαδικασία. Κάποιος που επιθυμεί να ανταλλάξει τα χρήματα του με αυτό, έχει αρκετές επιλογές. Η πιο γνώστη, αλλά και οικονομικότερη από αυτές είναι η χρήση ενός διαδικτυακού ανταλλακτηρίου. Υπάρχουν δεκάδες ανταλλακτήρια που μπορούν να χρησιμοποιηθούν, ενώ το μόνο που χρειάζεται από τον ενδιαφερόμενο για να έχει πρόσβαση σε αυτά, είναι ένα κινητό νέας τεχνολογίας (smart phone) και σύνδεση στο διαδίκτυο. Επίσης, για να δημιουργήσει λογαριασμό κάποιος σε ένα ανταλλακτήριο είναι δωρεάν, θα πρέπει όμως να ακολουθήσει μια διαδικασία ταυτοποίησης των ατομικών του στοιχείων συνήθως. Η διαδικασία αυτήν ονομάζεται KYC (Know Your Customer) και απαιτεί την υποβολή κάποιον εγγράφων όπως την ταυτότητα του νέου χρήστη και ένα πιστοποιητικό διεύθυνσης κατοικίας. Αφού ολοκληρωθεί η διαδικασία της ταυτοποίησης, ο αγοραστής μπορεί να ξεκινήσει τις συναλλαγές, οι οποίες πραγματοποιούνται σε σχετικά σύντομους χρόνους.

Ένας άλλος τρόπος αγοράς Bitcoin, είναι η χρήση ενός ATM Bitcoin. Τα ATM Bitcoin, μοιάζουν αρκετά με τα συνηθισμένα ATM με την μόνη διαφορά πως σε αυτά μπορεί να ανταλλάξει κάποιος ενδιαφερόμενος τα χρήματα του μόνο με κρυπτονομίσματα. Απαραίτητη προϋπόθεση για να ολοκληρωθεί μια συναλλαγή, είναι ο χρήστης να έχει δημιουργήσει κάποιο διαδικτυακό πορτοφόλι που υποστηρίζει το Bitcoin, πριν καταθέσει τα χρήματα του σε αυτό. Υπάρχουν αρκετά τέτοια πορτοφόλια, και εκτός από το ότι είναι δωρεάν, δεν απαιτείται και κάποιου είδους ταυτοποίησής όπως σε ένα ανταλλακτήριο. Αυτό, είναι και το μεγαλύτερο θετικό που μπορούν να προσφέρουν τα ATM Bitcoin, με αντάλλαγμα όμως αρκετά μεγαλύτερους φόρους από

ένα συνηθισμένο ανταλλακτήριο. Ο εντοπισμός των συγκεκριμένων ATM μπορεί να γίνει διαδικτυακά.

Αφού αναλύθηκαν οι δύο πιο επικρατέστεροι τρόποι για την αγορά Bitcoin, είναι αναγκαίο να αναφερθούν και οι επιλογές που έχει κάποιος για την διαφύλαξή του. Αρχικά, αν η συναλλαγή πραγματοποιηθεί μέσω ενός ανταλλακτηρίου, ο αγοραστής μπορεί να αφήσει τα Bitcoin του εκεί, αφού το ανταλλακτήριο, του παρέχει ένα διαδικτυακό πορτοφόλι. Το θετικό σε αυτό, είναι πως δεν απαιτείται από τον χρήστη να προβεί σε περεταίρω διαδικασίες και μπορεί οποιαδήποτε στιγμή να ρευστοποιήσει τα Bitcoin του πάλι σε χρήματα. Στον αντίποδα, η συγκεκριμένη επιλογή μπορεί να αποδειχθεί μοιραία για τον αγοραστή, αφού σε περίπτωση πτώχευσης του ανταλλακτηρίου, το κεφάλαιο του θα «κλειδωθεί» και πολύ πιθανόν τα Bitcoin του να χαθούν. Ταυτόχρονα, το ανταλλακτήριο λειτουργεί σαν τράπεζα και μπορεί να χρησιμοποιεί τα Bitcoin των χρηστών του προς όφελος του μειώνοντας έτσι την αποκέντρωση του δικτύου του Bitcoin.

Μια πιο ασφαλή επιλογή, είναι η αποστολή των Bitcoin σε κάποιο διαδικτυακό αποκεντρωμένο πορτοφόλι. Πρωτίστως, μια κατηγορία τέτοιων πορτοφολιών είναι τα Hot Wallets. Εκεί, ο έλεγχος βρίσκεται στα χέρια του αγοραστή και ενώ είναι πιο ασφαλής, βοηθάει και στην αποκέντρωση του δικτύου. Όπως αναφέρθηκε, η δημιουργία ενός τέτοιου πορτοφολιού είναι εντελώς δωρεάν και μπορεί να πραγματοποιηθεί από τον οποιοδήποτε, άσχετα με το που βρίσκεται ή το ποσό που επιθυμεί να επενδύσει. Τέλος, υπάρχει ένας ακόμα τρόπος αποθήκευσης του Bitcoin ο οποίος αν και απαιτεί κάποια χρήματα, είναι ο πλέον πιο ασφαλής. Αυτός, είναι η αγορά και δημιουργία ενός Cold Wallet. Τα Cold Wallets είναι και αυτά διαδικτυακά αποκεντρωμένα πορτοφόλια τα οποία για να τα αποκτήσει κανείς θα πρέπει να τα αγοράσει, και συνοδεύονται με μία συσκευή (εικόνα 5) για τον χειρισμό τους. Η διαφορά τους με τα Hot Wallets, είναι πως σε ένα Cold Wallet, τα Bitcoin του χρήστη βρίσκονται εκτός διαδικτύου, και καθιστά αδύνατη την επίθεση από κάποιον κακόβουλο χρήστη που επιθυμεί να τα κλέψει, σε αντίθεση με τα Hot Wallets, όπου αν και παρέχουν μια έξτρα προστασία σε σχέση με τα ανταλλακτήρια, δεν είναι λίγες οι φορές που έχουν αναφερθεί επιτυχημένες επιθέσεις σε αυτά. Συμπερασματικά, υπάρχουν αρκετές εναλλακτικές όσο αφορά την αποθήκευση του Bitcoin και η επιλογή τους εξαρτάται από τις προτεραιότητες που θέτει ο κάθε χρήστης.

«Εικόνα 5»

1.7) Πλεονεκτήματα και μειονεκτήματα του Bitcoin

Το δίκτυο του Bitcoin, αποτελεί μια καινοτομία που όμοια της είχε χρόνια να εμφανιστεί. Με την πάροδο των χρόνων, η φήμη του αυξάνεται εκθετικά καθώς εισχωρεί όλο και περισσότερο στις ζωές μικροεπενδυτών αλλά και εταιριών. Όπως κάθε τεχνολογία όμως, φέρνει αρκετά θετικά που διευκολύνουν τους χρήστες της, ή ταυτίζονται μαζί της ακόμα και ιδεολογικά, αλλά παράλληλα χαρακτηρίζεται και από διάφορες αδυναμίες. Ένας υπεύθυνος επενδυτής, θα πρέπει να είναι σε θέση να μελετήσει και να κατανοήσει τα πλεονεκτήματα αλλά και τα μειονεκτήματα του δικτύου του Bitcoin, πριν επενδύσει σε αυτό. Παρακάτω, θα αναφερθούν μερικά από τα κυριότερα.

Ξεκινώντας με τα πλεονεκτήματα, το Bitcoin αρχικά είναι πλήρως αποκεντρωμένο. Όπως θα αναλυθεί και παρακάτω στην σύγκριση του με το χρήμα, το Bitcoin δεν διοικείται από κάποια αρχή με αποτέλεσμα κανείς να μην ευνοείται σε σχέση με έναν άλλον. Ακόμα, όλες οι συναλλαγές που πραγματοποιούνται με την χρήση του δικτύου του Bitcoin, καταγράφονται και είναι ορατές από όλους τους χρήστες του. Ο καθένας

μπορεί να ελέγξει η να παρακολουθήσει καθημερινά τις συναλλαγές που πραγματοποιούνται παγκοσμίως. Ταυτόχρονα, το δίκτυο του Bitcoin παρέχει σοβαρή ασφάλεια στους χρήστες του, αφού ο κάθε χρήστης είναι υπεύθυνος για το διαδικτυακό του πορτοφόλι. Τέλος, όπως θα αναφερθεί και παρακάτω, με την δημιουργία του Bitcoin το 2008 ορίστηκε και η συνολική ποσότητα νομισμάτων που θα κυκλοφορήσουν στην αγορά. Εκτός από τα 21 εκατομμύρια που θα διατεθούν, δεν θα είναι δυνατόν να παραχθούν επιπλέον νομίσματα, κάτι που από μόνο του κάνει αρκετά σπάνιο και ελκυστικό το Bitcoin στους επενδυτές.

Από την άλλη πλευρά, το δίκτυο του Bitcoin αντιμετωπίζει και ορισμένες δυσκολίες με αποτέλεσμα να οδηγεί αρκετούς επενδυτές σε δεύτερες σκέψεις όσο αφορά την επένδυση προς αυτό. Ένα από τα μεγαλύτερα μειονεκτήματα του Bitcoin, είναι η αστάθεια στην τιμή του. Είναι ακατάλληλο σαν επενδυτικό προϊόν, για τους επενδυτές που αναζητούν να διασφαλίσουν τα κεφάλαια τους. Σε αυτό ευθύνεται η μικρή κεφαλαιοποίηση του Bitcoin, σε σχέση με άλλα επενδυτικά προϊόντα, κάτι το οποίο μπορεί να αλλάξει στο μέλλον αν το Bitcoin καταβάλει μεγαλύτερο «μερίδιο» στην αγορά. Επιπρόσθετα, το ασαφές νομοθετικό πλαίσιο που το διακατέχει είναι ένα σοβαρό μειονέκτημα που χαρακτηρίζει το Bitcoin αλλά και τα υπόλοιπα κρυπτονομίσματα. Αυτό συμβάλει στην χρήση του χωρίς περιορισμούς, και θα πρέπει να λυθεί άμεσα καθορίζοντας έτσι και το μέλλον του κλάδου. Επιπλέον, για την λειτουργία του δικτύου του Bitcoin, απαιτείται ισχυρή υπολογιστική δύναμη οπότε και τεράστια ποσά ενέργειας που επιβαρύνουν το περιβάλλον. Ενώ βέβαια η κοινότητα του Bitcoin αναζήτα ανανεώσιμες πήγες ενέργειας για την λειτουργεία του, δεν έχει μέχρι στιγμής τόσο αποτέλεσμα. Ταυτόχρονα, το δίκτυο του Bitcoin μπορεί να πραγματοποιήσει περίπου εφτά συναλλαγές το δευτερόλεπτο, το όποιο το καθιστά τρομερά αργό σε σχέση με άλλα μέσα συναλλαγών που φτάνουν σε αρκετές χιλιάδες συναλλαγές ανά δευτερόλεπτο όπως η Visa ή η PayPal. Προγραμματιστές και εταιρίες προσπαθούν να βρούνε λύσεις στο πρόβλημα αυτό, μερικές από τις σημαντικότερες θα αναλυθούν και παρακάτω, όμως μέχρι στιγμής το πρόβλημα παραμένει χωρίς να υπάρχει ιδιαίτερη βελτίωση. Ακόμα, δεν υπάρχει κάποια δικλίδα ασφαλείας από ανθρώπινα λάθη, απώλεια κωδικών πρόσβασης ή τεχνικά προβλήματα όπως καταστροφή του υπολογιστή με αποθηκευμένους τους κωδικούς όπως υπάρχει στις τράπεζες για παράδειγμα. Ένα τέτοιο συμβάν μπορεί να καθιστή μοιραίο για τα κεφάλαια του επενδυτή. Επιπρόσθετα, οι συναλλαγές είναι μη αναστρέψιμες και σε

κάποιο ανθρώπινο λάθος το αποτέλεσμα δεν γίνεται να αλλάξει. Τέλος, το Bitcoin διαθέτει κρυπτογράφηση και ασφάλεια των προσωπικών στοιχείων του χρήστη. Αυτό, δίνει την δυνατότητα σε κακόβουλους χρήστες να παρανομήσουν, ξεπλένοντας χρήματα ή δημιουργώντας μαύρες αγορές. Ένα τέτοιο περιστατικό, είχε συμβεί πριν μερικά χρόνια όταν είχε δημιουργηθεί το silk road, μια αγορά ναρκωτικών που ήταν ιδιαίτερα δύσκολο να εντοπιστεί. Επομένως, δεν είναι ακατόρθωτο ακόμα και τώρα να πραγματοποιηθεί κάποια παράνομη συναλλαγή.

ΚΕΦΑΛΑΙΟ 2: ΧΡΗΜΑ

2.1) ΤΙ ΕΙΝΑΙ ΧΡΗΜΑ

Τα κρυπτονομίσματα αποτελούν το επόμενο εξελιγμένο στάδιο των ηλεκτρονικών συναλλαγών. Η εμπιστοσύνη στο Bitcoin συνεχώς διευρύνεται, όπως αντανακλάται στην τιμή του και οι κάτοχοι του νιώθουν όλο και μεγαλύτερη αυτοπεποίθηση με το πέρασμα των χρόνων. Αυτό που πρέπει να αναγνωριστεί όμως είναι πως το Bitcoin δεν προορίζεται ως το ¨χρήμα του μέλλοντος¨ αλλά ως ο χρυσός καθώς ο λόγος ύπαρξης του είναι κυρίως στο να αποθηκεύει αξία. Ότι δηλαδή συνέβαινε εκατοντάδες χρόνια με τον χρυσό. Πριν όμως αναλύσουμε τους λόγους για τους οποίους το Bitcoin είναι τόσο πολύτιμο, αλλά και τόσο διαφορετικό με το χρήμα θα πρέπει πρώτα να διευκρινίσουμε την έννοια του χρήματος

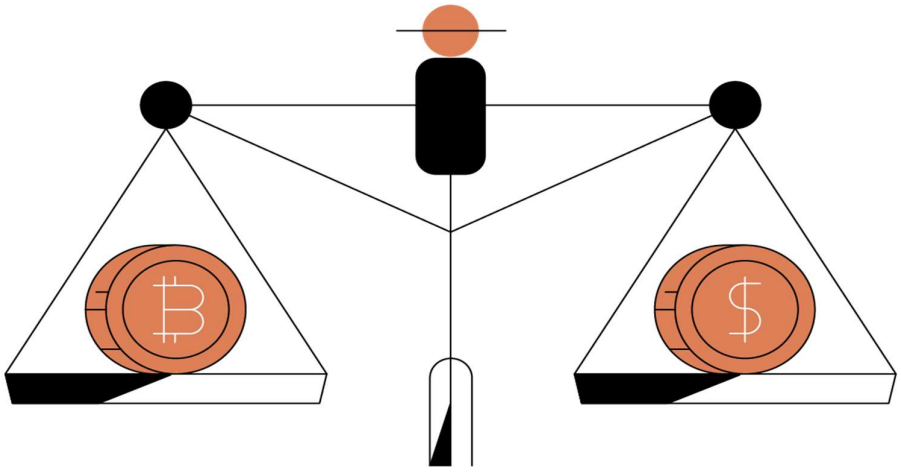
Από τα πολύ παλιά χρόνια έχουν χρησιμοποιηθεί ως χρήμα πάρα πολλά αντικείμενα. Ο σκοπός του χρήματος ήταν να διευκολύνει τις συναλλαγές μεταξύ των συναλλασσόμενων καθώς πριν θα έπρεπε να ανταλλάζουν πράγματα διαφορετικής αξίας μεταξύ τους με τον τρόπο κάποιας συμφωνίας. Το χρήμα ανεξαρτήτως μορφής, επιτελεί μερικές διαφορετικές λειτουργίες. Είναι ένα μέσο συναλλαγής για την αγορά αγαθών και υπηρεσιών, είναι μια λογιστική μονάδα για τον καθορισμό των τιμών και τέλος είναι ένα μέσο αποθήκευσης αξίας και αποταμίευσης. Οτιδήποτε γίνεται ευρέως

αποδεκτό ως μέσο ανταλλαγής μπορεί να γίνει νόμισμα και μόνο με ένα ενιαίο μέσο ανταλλαγής καθίσταται εφικτός ο πολύπλοκος οικονομικός υπολογισμός.

2.2 Η Εξέλιξη Του Χρήματος

Η εξέλιξη του χρήματος, αποτέλεσε μια από τις κατευθυντήριες δυνάμεις πίσω από την εξέλιξη της ανθρωπότητας. Η ιστορία του χρήματος είναι τόσο παλιά όσο και ο πολιτισμός. Συχνά τα νομίσματα είναι το μόνο που έχει απομείνει από κάποιον αρχαίο πολιτισμό. Στους πρωτόγονους λαούς ο καθένας ήταν καταναλωτής αλλά και παραγωγός ταυτόχρονα. Εμφανιζόταν στις τότε αγορές, με σκοπό να ανταλλάξει τα προϊόντα του με άλλα αγαθά που είχε ανάγκη και δεν μπορούσε να παράγει ο ίδιος. Ενώ αρκετές φορές αυτές οι συναλλαγές ήταν αρκετά χρονοβόρες αλλά και δύσκολες από θέμα καθορισμού ανταλλακτικής αξίας ήταν καθημερινό φαινόμενο της τότε εποχής. Τα πράγμα όμως άλλαζαν τροπή όσο αυξάνονταν ο αριθμός των παραγόμενων αγαθών αλλά και ο όγκος παραγωγής. Άρχισε να δημιουργείται η ανάγκη εύρεσης κάποιου μέσου βάση του οποίου θα μπορούν να καθοριστούν οι τιμές όλων τον αγαθών για την διευκόλυνση των συναλλαγών, καθώς και με αυτό θα μπορούσαν να αποκτήσουν κάθε αγαθό οποιαδήποτε χρονική στιγμή χωρίς να πρέπει να δώσουν τα δικά τους προϊόντα. Το μέσο που θα έλυνε αυτό το πρόβλημα θα έπρεπε να είναι κάτι ανθεκτικό αλλά και εύκολο στην μεταφορά του. Ταυτόχρονα, θα έπρεπε η παραγωγή του να ελέγχεται και να μην είναι εύκολο για τον καθένα να το δημιουργήσει. Έτσι, φτιάχτηκαν τα πρώτα νομίσματα από υλικά όπως ασήμι και χρυσό και η έννοια της συναλλαγής δεν ήταν ποτέ ξανά ίδια.

2.3) Χρήμα και Bitcoin



«Εικόνα 6»

Μια συχνή απάντηση στην ερώτηση ¨τι είναι Bitcoin¨ είναι πως το Bitcoin είναι το ¨χρήμα του μέλλοντος¨ ή ένα ακόμα μέσο συναλλαγής παρόμοιο με το χρήμα. Αν κάποιος όμως το ερευνήσει περεταίρω σύντομα θα καταλάβει πως το Bitcoin έχει κάποιες σημαντικές διαφορές με το χρήμα και κατατάσσεται στην κατηγορία των αγαθών φύλαξης αξίας (store of value) όπως ο χρυσός για παράδειγμα, καθώς και άλλα σπάνια μέταλλα και διαμάντια. Είναι έτσι απαραίτητο, να αναφερθούν κάποιες από αυτές τις διαφορές τους για να οριστεί καλύτερα η έννοια του Bitcoin.

- Αποκέντρωση

  Η πρώτη, και πιο αξιοσημείωτη διαφορά ανάμεσα στο χρήμα και το Bitcoin είναι ότι το Bitcoin είναι αποκεντρωμένο. Κανένα ίδρυμα δεν ελέγχει το δίκτυο του, το οποίο διατηρείται από ένα σύνολο εθελοντών που διαθέτουν υπολογιστική δύναμη για την λειτουργεία του. Ο καθένας μπορεί να συμμετέχει χωρίς να υπάρχουν περιορισμοί ή κριτήρια και μπορεί να το κάνει από οποιοδήποτε μέρος του κόσμου θέλει. Σε αντίθεση το χρήμα ελέγχεται από κράτη και τράπεζες και ελάχιστοι μπορούν να το παράγουν και να συμμετέχουν σε αυτήν την διαδικασία.

- Παραποίηση Συναλλαγών

Όταν πραγματοποιηθεί μια συναλλαγή στο δίκτυο του Bitcoin και περάσει πάνω από μια ώρα είναι αδύνατον να ακυρωθεί ή να τροποποιηθεί. Αν και κάτι τέτοιο μπορεί να ακούγεται ανησυχητικό είναι ένα από τα πλεονεκτήματα αυτής της ¨νέας¨ τεχνολογίας διότι καμία συναλλαγή δεν μπορεί να αλλοιωθεί αφού δεν υπάρχει κάποιος κεντρικός επικεφαλής για να επέμβει. Αντίθετα στα παραδοσιακά συστήματα πληρωμής κάτι τέτοιο δεν ισχύει και οι συναλλαγές εύκολα μπορούν να τροποποιηθούν.

- Προσφορά

Ένας από τους κύριους λόγους που κάνει το Bitcoin αρκετά ελκυστικό στους επενδυτές, είναι η περιορισμένη προσφορά του. Ο αλγόριθμος του είναι προκαθορισμένος και ελέγχει αυστηρά την διαδικασία παραγωγής των νέων Bitcoin καθώς θα υπάρξουν μόνο 21 εκατομμύρια. Κάθε δέκα περίπου λεπτά δημιουργείται ένας μικρός αριθμός νέων Bitcoin και η παραγωγή τους θα σταματήσει το 2140. Συμπερασματικά, θεωρητικά αν η ζήτηση προς αυτό μεγαλώνει και η προσφορά παραμένει ίδια, η αξία του ολοένα και θα αυξάνεται.

Στα παραδοσιακά νομίσματα τώρα, η προσφορά τους δεν σταματάει ποτέ. Αν οι κεντρικές τράπεζες θεωρήσουν πως είναι αναγκαίο να εκδώσουν νέα, μπορούν να το κάνουν χειραγωγώντας έτσι και την αξία ενός νομίσματος σε σχέση με άλλα. Το κόστος όμως το επωμίζονται οι πολίτες που κατέχουν το συγκεκριμένο νόμισμα.

- Επαλήθευση Αυθεντικότητας

Τα χαρτονομίσματα είναι σχετικά εύκολο να ελεγχθούν ως προς την αυθεντικότητα τους. Ωστόσο, παρά την ύπαρξη ειδικών χαρακτηριστικών στην επιφάνεια του χαρτιού για την αποτροπή της παραχάραξης, είναι πάντοτε υπαρκτός ο κίνδυνος εξαπάτησης από πλαστά. Αυτές οι δυσκολίες δεν υφίστανται στο Bitcoin. Δεν απαιτείται να τηρείται ειδική διαδικασία από εξειδικευμένους ανθρώπους για την εύρεση πλαστών νομισμάτων. Το σύστημα από μόνο του είναι έτσι δομημένο ώστε να αναγνωρίζει και να αποβάλλει τα πλαστά. Το Bitcoin δεν μπορεί να αντιγραφτεί και είναι αδύνατον να έχει κάποιος ένα κομμάτι και να το πουλήσει δύο φορές.

ΚΕΦΑΛΑΙΟ 3: ΧΡΥΣΌΣ

3.1) Bitcoin Και Χρυσός

«Εικόνα 7»

Ο αιώνας που διανύουμε αναζητά νέα εργαλεία και νέους τρόπους σκέψης. Η τεχνολογία εξελίσσεται ραγδαία, και η καθημερινότητα αλλάζει διαρκώς. Το Bitcoin, είναι μια τρομερή καινοτομία, ίσως και η σημαντικότερη στον χώρο των χρηματοοικονομικών αγορών τον τελευταίο αιώνα, η οποία όπως φαίνεται ήρθε για να μείνει. Ο κύριος ανταγωνιστής του είναι πλέον γνωστό πως είναι ο χρυσός και το ερώτημα είναι αν μπορεί να τον ξεπεράσει. Παρακάτω, θα αναφερθούν μερικοί λόγοι που αναδεικνύουν την ανωτερότητα του Bitcoin σε σχέση με τον χρυσό αλλά και ένα σημαντικό μειονέκτημα του, που ευθύνεται για την δυσπιστία που αντιμετωπίζει έως και σήμερα.

3.2)Πόσο Σπάνιος Είναι ο Χρυσός Και Πόσο Το Bitcoin.

Ο χρυσός είναι ένα μέταλλο το οποίο υπάρχει εδώ και χιλιάδες χρόνια. Αποτελούσε πάντα μια επίδειξη δύναμης αλλά και αριστοκρατίας για τους κατόχους του, κάνοντας έτσι την ζήτηση του, καθώς και την τιμή του, συνεχόμενα ανοδική.

Πλέον, όσο παράλογο και αν ακούγεται έτσι αρχίζει να αντιμετωπίζεται και το Bitcoin, και ο λόγος που συμβαίνει αυτό και για τα δύο αυτά περιουσιακά στοιχεία είναι η σπανιότητα τους. Ποιο θα μπορούσε να θεωρηθεί πιο σπάνιο όμως; Όσο παράδοξο και αν ακούγεται, επειδή πρόκειται για ψηφιακό αντικείμενο, το Bitcoin έχει ξεκινήσει να θέτει τα θεμέλια για να φτάσει τον χρυσό, αν και βρίσκεται ακόμα αρκετά πίσω. Στο χρυσό αρχικά, με βάση τον υφιστάμενο ρυθμό εξόρυξης ανά έτος, θα χρειαστούν περίπου 62 χρόνια για να λάβουμε ίση ποσότητα με την υπάρχουσα ενώ στα επόμενα 25 χρόνια υπολογίζεται πως θα αυξηθεί κατά 52%. Ακόμα, η εξόρυξη του δεν είναι απίθανο να αυξηθεί ραγδαία στα επόμενα χρόνια αυξάνοντας έτσι την προσφορά του. Μια θεωρία που επικρατεί για τον χρυσό και αφορά την αύξηση της τιμής του, είναι πως κάποια στιγμή αρκετά λεφτά θα αποχωρίσουν από την αγορά των ομολόγων (λόγο της αρνητικής πραγματικής απόδοσης τους) και θα στραφούν προς τα εκεί. Ενώ φαίνεται λογικό υπάρχει μια παράμετρος που δεν έχει υπολογιστεί. Η προσφορά του χρυσού συνδέεται στενά με την ζήτηση. Έτσι, αν για παράδειγμα αυξηθεί σημαντικά η τιμή του χρυσού, θα αυξηθούν σημαντικά και οι προσπάθειες που γίνονται στα ορυχεία για την εξόρυξη του. Θα σκάψουν σε μεγαλύτερο βάθος, εκεί όπου δεν τους συνέφερε πριν, και θα χρησιμοποιήσουν πιο κοστοβόρα μέσα, αφού τότε η ίδια ποσότητα χρυσού θα κοστίζει αρκετά περισσότερο. Ταυτόχρονα, άνθρωποί που κατέχουν χρυσό σε μορφή κοσμημάτων είναι αρκετά πιθανό να βιαστούν να τον πουλήσουν αφού η αξία του θα έχει αυξηθεί.

Η προσέγγιση και η λειτουργία του Bitcoin όμως είναι τελείως διαφορετική όσο αφορά την σπανιότητα-προσφορά του. Είναι γνωστό αρχικά, πως το δίκτυο του είναι φτιαγμένο έτσι ώστε να επιτρέπει την ύπαρξη μόνο 21 εκατομμυρίων Bitcoin και πως η παραγωγή του είναι τρομερά αυστηρή. Κάθε 10 περίπου λεπτά παράγεται μια συστοιχία (κουτάκι) και όσοι ¨δούλεψαν¨ για αυτό μοιράζονται περίπου 6,25 Bitcoin. Αυτό όμως, είναι ένα ποσό που αλλάζει περίπου κάθε 4 χρόνια και για την ακρίβεια μειώνεται κατά τα μισά, όπως αναλύθηκε και στην παράγραφο 1.5 .Στα επόμενα 25 χρόνια για παράδειγμα, ενώ αναφέρθηκε πως ο χρυσός θα αυξηθεί κατά 52% το Bitcoin θα αυξηθεί μόλις κατά 15%, και το ποσοστό αυτό όλο και θα μειώνεται όσο περνάνε τα χρόνια ώσπου να φτάσει στο μέγιστο αριθμό παραγωγής το έτος 2140. Συμπερασματικά, είναι πρακτικά αδύνατον να τροποποιηθεί ο ρυθμός παραγωγής του Bitcoin ή να παραχθούν περισσότερα από 21 εκατομμύρια κάτι το οποίο το κάνει τρομερά σπάνιο. Αντίθετα, στην περίπτωση του χρυσού, δεν αποκλείεται στο άμεσο

μέλλον να βρεθεί ακόμα κάποιο νέο μεγάλο κοίτασμα άγνωστο έως τώρα αφού κανείς δεν γνωρίζει την ακριβής ποσότητα του στην Γη.

3.3) Πόσο Εύχρηστος Είναι ο Χρυσός Και Πόσο Το Bitcoin.

Για τις τράπεζες, καθώς και για τους μεγάλους διαχειριστές κεφαλαίων, ο χρυσός ήταν πάντα ένα αδιαμφισβήτητο επενδυτικό καταφύγιο, που προσέφερε ασφάλεια αλλά και σιγουριά σε αρκετές καταστροφές των χρηματοοικονομικών αγορών. Πλέον, έχει εμφανιστεί μια ακόμα επιλογή. Μια επιλογή που μπορεί να ανταγωνιστεί δίκαια τον χρυσό. Το Bitcoin.

Ένα σοβαρό μειονέκτημα του χρυσού όσο αφορά τις κεντρικές τράπεζες κυρίως, είναι η διαφύλαξη και η μεταφορά του. Ενώ, υπερτερεί σε ιστορια και λάμψη σε σχέση με το Bitcoin, είναι αρκετά δυσκίνητος και βαρύς. Ταυτόχρονα, έχει τεράστιο κόστος φύλαξης και ασφάλισης, κάνοντας έτσι την απόδοση του αρκετές φορές ακόμα και αρνητική. Κάτι τέτοιο όμως, δεν ισχύει με το Bitcoin. Στο Bitcoin τα έξοδα φύλαξης είναι απειροελάχιστα όπως και στην μεταφορά του. Τα πάντα γίνονται γρήγορα και με πλήρης ασφάλεια ενώ η απόδοση του δεν έχει κανέναν περιορισμό.

Όσο αφορά τώρα, τους μεγάλους διαχειριστές κεφαλαίων, ή και τους απλούς επενδυτές υπάρχει και εκεί ένα εξίσου σημαντικό μειονέκτημα ως προς την κατοχή χρυσού. Οι ποσότητες που διακινούνται, είτε με διάφορα πιστοποιητικά είτε και σε ψηφιακή μορφή, είναι πολλαπλάσιες από την πραγματική φυσική ποσότητα. Σε ένα υποθετικό σενάριο αύξησης της τιμής, δεν θα είναι λίγοι αυτοί που δεν θα προλάβουν να εξαργυρώσουν τα συμβόλαια τους κάνοντας έτσι αρκετούς να μην αισθάνονται άνετα με την ιδέα επένδυσης σε χρυσό. Τα πιστοποιητικά είναι έγκυρα όσο υπάρχει εμπιστοσύνη στο τραπεζικό ίδρυμα που τα εκδίδει, και δεν είναι λίγες οι φορές στην ιστορία, που κάτι τέτοιο αποδείχθηκε τουλάχιστον επικίνδυνο. Στον αντίποδα, το Bitcoin δεν αντιμετωπίζει καθόλου τέτοιου είδους προβλήματα. Είναι γνωστό πως θα υπάρξουν 21 εκατομμύρια, όπως και ο καθένας θα μπορεί να τα διαχειρίζεται όπως

αυτός θέλει οπουδήποτε στιγμή το αποφασίσει. Τέλος, δεν χρειάζεται να εμπιστευτεί κανέναν για την φύλαξη των επενδύσεων του, καθώς το δίκτυο του Bitcoin είναι αποκεντρωμένο, έχοντας έτσι όλη την δύναμη στα χέρια του.

Κλείνοντας, αφού αναλύθηκαν μερικά μειονεκτήματα του χρυσού σε σχέση με το Bitcoin, είναι αναγκαίο να αναφερθεί και ένας σημαντικός λόγος που κάνει τους επενδυτές δύσπιστους ως προς την επένδυση σε αυτό, σαν αντικείμενο αποθήκευσης αξίας. Ο λόγος αυτός είναι η μεταβλητότητα της τιμής του. Το Bitcoin, και γενικά τα κρυπτονομίσματα βρίσκονται ακόμα σε ένα πρώιμο στάδιο, με αποτέλεσμα η συνολική κεφαλαιοποίηση την αγοράς να είναι σχετικά μικρή. Έτσι, αρκετοί εξωγενείς παράγοντες, όπως αρνητικά νέα για τις χρηματοοικονομικές αγορές γενικότερα, μπορούν να επηρεάσουν σημαντικά την τιμή του. Επιπλέον, δεν είναι λίγες οι φορές όπου αρκετοί επιτήδειοι καταφέρνουν να χειραγωγήσουν την τιμή του Bitcoin προς όφελος τους, κάνοντας το έτσι ακόμα πιο αναξιόπιστο. Αν και λογικό, αν αναλογιστεί κανείς τα ελάχιστα χρόνια ύπαρξης του, είναι κάτι που τρομάζει τους επενδυτές ενώ τους κάνει ακόμα και να το αποφεύγουν. Το μόνο σίγουρο είναι πως η απόφαση για την επιλογή του καταλληλότερου μέσου αποθήκευσης αξίας είναι αρκετά δύσκολη αφού η καινοτομία και ευκολία του Bitcoin έρχονται σε σύγκρουση με την σιγουριά και την ασφάλεια του χρυσού. Τα επόμενα χρόνια θα είναι σίγουρα αρκετά καθοριστικά για το μέλλον αυτών των δύο αντικειμένων.

ΚΕΦΑΛΑΙΟ 4: ΕΞΟΡΥΞΗ ΤΟΥ BITCOIN

«Εικόνα 8»

4.1)Εξέλιξη Του Mining

Ένα περίεργο συναίσθημα, που γεννάει η διατριβή κάποιου με την τεχνολογία του Bitcoin, είναι ότι όσα περισσότερα μαθαίνει για αυτό τόσο πιο έκπληκτος μένει. Θα μπορούσε ευκολά να παρουσιαστεί και σαν έναν «ζωντανό οργανισμό» που κρύβει πολλές καινοτομίες και μπορεί να προσαρμόζεται κατάλληλα στις συνθήκες που επικρατούν. Μια από αυτές τις καινοτομίες, και ίσως η σπουδαιότερη, είναι η διαδικασία που ακολουθείται για την παραγωγή νέων Bitcoin, η οποία ευθύνεται και για την σωστή και αξιόπιστη λειτουργία του δικτύου. Η διαδικασία αυτή ονομάζεται “mining”(εξόρυξη) και οι εθελοντές που την ακολουθούν ονομάζονται miners(εξορύκτες).

Στις 3 Ιανουαρίου το 2009, εξορύχθηκε το πρώτο Bitcoin. Το μόνο που αρκούσε τότε για να συμμετέχει κανείς σε αυτήν την διαδικασία, και να αρχίσει να παράγει Bitcoin, ήταν ένας οικιακός υπολογιστής. Ελάχιστοι το προσπαθούσαν, αφού ελάχιστοι γνώριζαν για την ύπαρξη του Bitcoin, κάνοντας έτσι την εξόρυξη αρκετά απλή και καθόλου ανταγωνιστική. Έπειτα, κάποιος αντιλήφθηκε πως αν συνέδεε τις κάρτες γραφικών, θα ανέβαζε την υπολογιστική ισχύ και έτσι οι ανταμοιβές για τον

ίδιο θα ήταν ακόμα μεγαλύτερες. Μετέπειτα, η συνεχής επιθυμία για περισσότερα, οδήγησε στην δημιουργία μηχανημάτων, καθαρά και μόνο φτιαγμένα για την εξόρυξη Bitcoin, βελτιώνοντας έτσι ακόμα περισσότερο την απόδοση. Φτάσαμε στο σημείο πλέον, όπου η υπολογιστική δύναμη που απαιτείται, να έχει κάνει το "mining" καθαρά βιομηχανική δραστηριότητα, με τεράστιες εγκαταστάσεις που απασχολούν εξειδικευμένο προσωπικό, καθώς ανταγωνίζονται μεταξύ τους για το ποια θα είναι η πρώτη που θα λύσει ένα δύσκολο μαθηματικό πρόβλημα, και θα λάβει ως αμοιβή τα «φρεσκοτυπομένα» Bitcoin.

«Εικόνα 9»

4.2)Η Διαδικασία Εξόρυξης.

Η εξόρυξη είναι μια διαδικασία μέσω της οποίας οι συναλλαγές του Bitcoin επαληθεύονται και προστίθενται στο blockchain (δίκτυο). Οι εθελοντές (miners), δανείζουν την επεξεργαστική ισχύ του υπολογιστή τους καθώς και την τεράστια ενέργεια που χρησιμοποιεί, αφού η διαδικασία πραγματοποιείται ασταμάτητα για μήνες ή και χρόνια, με αντάλλαγμα νέα Bitcoin, καθώς και προμήθειες που προκύπτουν από τις καθημερινές συναλλαγές των χρηστών του δικτύου. Έτσι, η εξόρυξη καθιστά

τον πυρήνα του μοντέλου του Bitcoin. Όταν ένας χρήστης δημιουργεί μια νέα συναλλαγή με έναν άλλον, οι miners αρχικά ελέγχουν αν υπάρχουν στο πορτοφόλι του αποστολέα τα Bitcoin που θέλει να στείλει. Αμέσως μετά, καταχωρούν την συναλλαγή σε μια συστοιχία (κουτάκι) μαζί με άλλες συναλλαγές που έχουν ελεγχθεί. Περίπου κάθε 10 λεπτά, δημιουργείται και ένα νέα συστοιχία για να φιλοξενήσει αυτές τις συναλλαγές, το οποίο σχετίζεται άμεσα με τα προηγούμενα, σχηματίζοντας έτσι μια αλυσίδα (blockchain). Για να γίνει όμως αυτός ο συσχετισμός της νέας συστοιχίας με τα προηγούμενα, χρησιμοποιείται ένας μαθηματικός αλγόριθμος. Με την λύση του, θα δημιουργηθεί το νέα συστοιχία, και μαζί με αυτό θα δημιουργηθούν και τα νέα Bitcoin, τα οποία θα αποδοθούν σε αυτούς που βρήκαν την λύση.

4.3)Το μυστικό για σταθερή παραγωγή.

Η εξόρυξη είναι μια τρομερά ανταγωνιστική επιχείρηση. Μόνο ένας επεξεργαστής θα λάβει την αμοιβή κάθε δέκα λεπτά, ανεξάρτητα από το πόσοι προσπαθούν ταυτόχρονα να βρούνε την λύση του γρίφου. Αυτό που αλλάζει όμως καθώς αυξάνεται ή μειώνεται το πλήθος των miners, είναι η δυσκολία του γρίφου. Όσοι περισσότεροι προσπαθούν, τόσο πιο δύσκολος γίνεται με αποτέλεσμα να χρειάζεται ακόμα περισσότερη υπολογιστική δύναμη. Το αντίθετο συμβαίνει όταν μειώνονται ο ανταγωνισμός. Ο ανταγωνισμός αλλάζει ανάλογα και με την τιμή του Bitcoin. Αν η τιμή του Bitcoin αυξηθεί, περισσότερα άτομα θα το δουν σαν ευκαιρία και θα προσπαθήσουν να συμβάλουν και αυτοί στην παραγωγική διαδικασία διεκδικώντας «ένα κομμάτι από την πίτα». Από την άλλη σε μια περίπτωση πτώσης της τιμής, το κόστος παραγωγής μπορεί να είναι μεγαλύτερο από το αναμενόμενο κέρδος, και έτσι αρκετοί να αποχωρίσουν. Ο λόγος πίσω από την ύπαρξη του μηχανισμού αυτού, είναι να διασφαλιστεί ότι ο μέσος χρόνος δημιουργίας μιας νέας συστοιχίας θα παραμείνει ίσος με δέκα λεπτά, και έτσι η παραγωγή θα παραμείνει σταθερή. Ο αλγόριθμος έχει προγραμματιστεί για αυτόματη προσαρμογή του επιπέδου δυσκολίας κάθε 2016 συστοιχίας ή περίπου για κάθε δύο εβδομάδες.

4.4)Ο Ζωντανός Οργανισμός Που Λέγεται Bitcoin Και Τα Έξοδα Διαβίωσης Του.

Όπως αναφέρθηκε, το Bitcoin έχει δημιουργηθεί έτσι ώστε να μπορεί να προσαρμόζεσαι κατάλληλα σε δυσκολίες και αλλαγές που αντιμετωπίζει, ενώ έτσι κάποιος, θα μπορούσε να το παρομοιάσει και σαν έναν ζωντανό οργανισμό που παλεύει για την επιβίωση του. Ακόμα και αν σταματήσουν να συμβάλουν στην παραγωγική διαδικασία οι μισοί miners δεν θα υπάρξει κανένα πρόβλημα. Απλούστατα, θα μειωθεί η δυσκολία του μαθηματικού αλγορίθμου, και έτσι θα απαιτείται λιγότερη υπολογιστική δύναμη και ενέργεια. Άρα, κάποιοι από αυτούς που είχαν κλείσει τους διακόπτες θα γυρίσουν πίσω αφού θα τους συμφέρει να παράγουν ξανά.

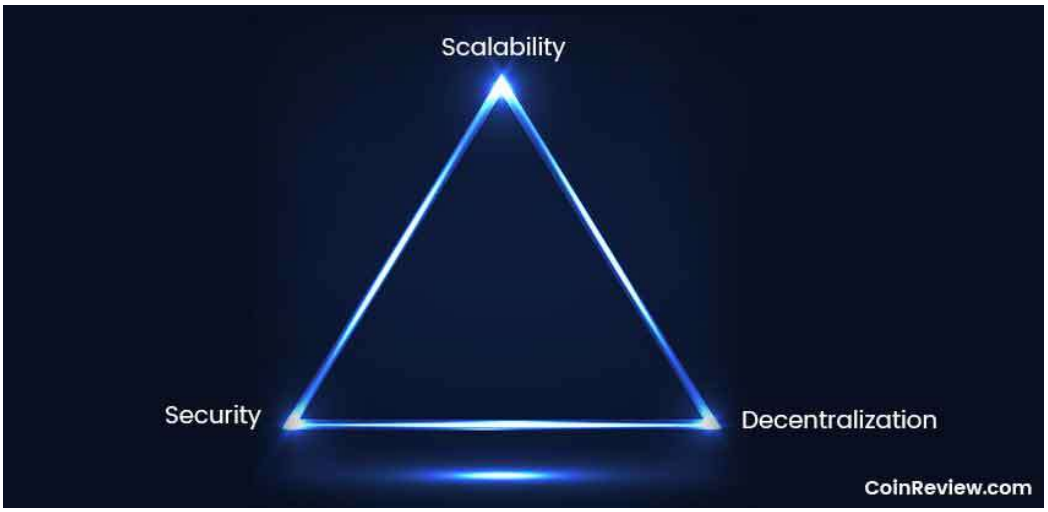
Αυτό δεν αποτελεί μόνο κάποια θεωρητική εκτίμηση, αφού την άνοιξη του 2021 η Κίνα όρισε το mining ως κάτι παραβατικό και κατάφερε να εκδιώξει περίπου το 90% των εξορυκτών από την χώρα. Αυτήν ήταν και η μεγαλύτερη επίθεση που έχει σημειωθεί ποτέ κατά του Bitcoin αφού έχασε ξαφνικά περίπου το 65% των εξορυκτών του. Και όμως, το δίκτυο του Bitcoin παρέμεινε σταθερό συνεχίζοντας να παράγει κάθε δέκα λεπτά μιας νέας συστοιχίας μέχρι και σήμερα.

Όσον αφορά το κόστος λειτουργείας του δικτύου, εξαρτάται από δυο παράγοντες κυρίως. Την επένδυση σε μηχανολογικό εξοπλισμό, και την ηλεκτρική ενέργεια που θα καταναλώνει αυτός. Η εξόρυξη πλέον έχει γίνει τρομερά ανταγωνιστική και απαιτεί σημαντική ποσότητα ενέργειας, όχι μόνο για την λειτουργεία των μηχανημάτων αλλά και για την ψύξη τους, αφού λειτουργούν ασταμάτητα, για την μέγιστη δυνατή απόδοση, φτάνοντας έτσι μεγάλες θερμοκρασίες. Το κόστος όμως της ενέργειας εξαρτάται από τη χώρα στην οποία βρίσκονται οι εγκαταστάσεις, και από τη χρήση ή όχι ανανεώσιμων πηγών ενέργειας.

ΚΕΦΑΛΑΙΟ 5 : ΤΟ ΤΡΙΛΗΜΜΑ ΤΟΥ ΔΙΚΤΥΟΥ ΤΟΥ BITCOIN.

5.1) Το Τρίλημμα Του Δικτύου Του Bitcoin

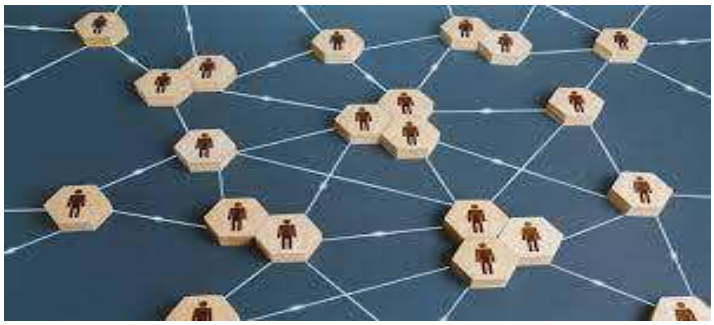
Το Bitcoin, και η τεχνολογία που το αντιπροσωπεύει, αναμφίβολα έχει κεντρίσει το ενδιαφέρον αρκετών αφού βρίσκεται ακόμα σε ένα πρώιμο στάδιο, ενώ παράλληλα οι αποδώσεις που έχει προσφέρει είναι τεράστιες. Δεν είναι λίγες οι φορές που έχει παρομοιαστεί με το ίντερνετ όταν αυτό βρισκόταν ακόμα στα αρχικά του βήματα και ελάχιστοι το εμπιστευόταν. Επενδυτές, προγραμματιστές αλλά και άνθρωποι που αγαπάνε άπλα το διαφορετικό, και πιστεύουν σε μια επερχόμενη οικονομική επανάσταση χωρίς επικεφαλείς, μελετάνε και εμπιστεύονται το Bitcoin όλο και περισσότερο, νιώθοντας έτσι και περισσότερη σιγουριά κρατώντας το. Είναι όμως το Bitcoin μια τεχνολογία που μπορεί να γνωρίσει την παγκόσμια υιοθέτηση, και να βασιστούν ολόκληρες οικονομίες και κράτη πάνω σε αυτό χρησιμοποιώντας το καθαρά σαν μέσο συναλλαγών? Για να μπορέσει να συμβεί κάτι τέτοιο θα πρέπει να πληροί κάποιες προϋποθέσεις. Αφού μιλάμε για ένα πλήρως αποκεντρωμένο δίκτυο θα πρέπει να είναι τρομερά ασφαλές αλλά και τρομερά γρήγορο. Αυτό είναι γνωστό ως το τρίλημμα του Bitcoin.



«Εικόνα 10»

Η ιδέα πάνω σε αυτό, είναι ένας κόσμος όπου δεν θα χρειάζονται μεσάζοντες για οποιαδήποτε συναλλαγή καθώς θα χρησιμοποιείται ένα πλήρως αποκεντρωμένο και ασφαλή δίκτυο. Το τρίλημμα του Bitcoin έγινε δημοφιλές όταν αναφέρθηκε από τον συνιδρυτή του Ethereum, (ένα άλλο μεγάλο κρυπτονόμισμα) τον Vitalik Buterin, και από τότε έχει απασχολήσει αισθητά την κοινότητα του Bitcoin αλλά και όλο τον κόσμο των κρυπτονομισμάτων. Για να γίνει πιο κατανοητό αυτό το φαινόμενο, θα πρέπει να αναλυθούν διεξοδικά, τα τρία διαφορετικά στοιχεία που είναι επιθυμητά και αναγκαία για μία παγκόσμια υιοθέτηση του Bitcoin σαν επίσημο συνάλλαγμα. Τα τρία αυτά στοιχεία είναι η αποκέντρωση, η ασφάλεια και η επεκτασιμότητα.

5.2) Ποιος Διοικεί Το Bitcoin?



«Εικόνα 11»

Ξεκινώντας με την αποκέντρωση, το Bitcoin είναι αποκεντρωμένο βάση σχεδιασμού. Ο έλεγχος του διανέμεται πλήρως, αντί να βρίσκεται στην κατοχή μιας οντότητας και ο οποιοσδήποτε μπορεί να μελετήσει ή να συμμετάσχει στο ανοιχτό δίκτυο του. Όλοι μπορούν να έχουν πρόσβαση στα ίδια δεδομένα, αφού είναι δημόσια έτσι ώστε να ελεγχθούν και να επιβεβαιωθούν, πριν προστεθούν στην ψηφιακή βάση δεδομένων. Αυτό, έχει ως αποτέλεσμα να μην επιτρέπει σε κανέναν να αλλάξει τα αρχεία προς όφελος του αφού οι υπόλοιποι που δραστηριοποιούνται πάνω στο δίκτυο του Bitcoin μπορούν να τον σταματήσουν. Κανένα συγκεκριμένο πρόσωπο, ή κάποιος οργανισμός, δεν μπορεί να το απενεργοποιήσει αφού η λειτουργία του βασίζεται σε χιλιάδες κόμβους, δηλαδή ανθρώπους από όλο τον πλανήτη, που επιλέγουν να τρέχουν

το λογισμικό του διαθέτοντας υπολογιστική δύναμη. Από την άλλη πλευρά, στο παραδοσιακό χρηματοπιστωτικό σύστημα, η ύπαρξη τον τραπεζών είναι κομβική. Οι τράπεζες διασφαλίζουν ότι όλες οι συναλλαγές τηρούνται σωστά, επιβάλλοντας όμως την εμπιστοσύνη στους χρήστες της.

Κάτι που πρέπει να σημειωθεί ωστόσο, είναι ότι σε ένα αποκεντρωμένο σύστημα συναλλαγών, ο χρόνος που απαιτείται για να πραγματοποιηθεί μια συναλλαγή μπορεί να διαφέρει κάθε φορά, ενώ μπορεί να χρειαστεί και αρκετή ώρα για να ολοκληρωθεί. Απαιτούνται τουλάχιστον έξι επιβεβαιώσεις από έξι διαφορετικούς χρήστες έτσι ώστε να θεωρηθεί μια συναλλαγή έγκυρη και μη αναστρέψιμη, ενώ παράλληλα όσο μεγαλύτερος είναι ο όγκος συναλλαγών εκείνη την χρονική στιγμή, τόσο περισσότερο θα αργήσει μια συναλλαγή. Το δίκτυο του Bitcoin μπορεί να χειριστεί περίπου εφτά συναλλαγές το δευτερόλεπτο αλλά το πόσο γρήγορο είναι και αν μπορεί να ανταπεξέλθει σε μια μαζική υιοθέτηση του θα αναλυθεί παρακάτω. Εν κατακλείδι, η διοίκηση του Bitcoin βρίσκεται στα χέρια όλων τον χρηστών του, που επέλεξαν να συμμετάσχουν σε αυτό, χωρίς να έχει κάποιος περισσότερα δικαιώματα από έναν άλλον, άσχετα με το γένος του, την χώρα όπου διαμένει ή την οικονομική του κατάσταση.

5.3)Πόσο ασφαλές είναι το δίκτυο του Bitcoin?

«Εικόνα 12»

Το δίκτυο του Bitcoin, αποτελείται από μια αλυσίδα συστοιχίες η οποία ονομάζεται Blockchain. Ήταν το πρώτο Blockchain που δημιουργήθηκε στον κόσμο των κρυπτονομισμάτων, και αποτελεί ένα δημόσιο δίκτυο όπως αναφέρθηκε. Ενώ η

αποκέντρωση είναι ένα από τα μεγαλύτερα πλεονεκτήματα του δικτύου, σε σχέση με άλλα χρηματοπιστωτικά συστήματα, απαιτεί την μέγιστη ασφάλεια για να το εμπιστευτούν και να το χρησιμοποιήσουν επενδυτές και οντότητές, αφού δεν θα υπάρχει κάποια κεντρική αρχή για να θέτει τους κανόνες και να κρατάει την «τάξη».

Όταν πραγματοποιείται μια συναλλαγή στο δίκτυο του Bitcoin, η συναλλαγή κρυπτογραφείται σε μια τυχαία σειρά γραμμάτων και αριθμών που αποκαλείται hash και η συνολική διαδικασία ονομάζεται κατακερματισμός. Ο ρυθμός κατακερματισμού (hashrate) είναι η συνολική συνδυασμένη υπολογιστική ισχύ που χρησιμοποιείται από τους ανθρακωρύχους για την εξόρυξη του Bitcoin και την δημιουργία νέων συστοιχίες. Με αυτόν τον τρόπο αποκρύπτονται διάφορα ευαίσθητα στοιχεία όπως η ταυτότητα του αποστολέα και του παραλήπτη. Αυτό, αποτελεί έναν παράγοντα που συμβάλει στην ασφάλεια του δικτύου. Παράλληλα, ο καθένας μπορεί να εντοπίσει πορτοφόλια χρηστών χωρίς όμως να μπορεί να εξακριβώσει τα πραγματικά στοιχεία του κατόχου. Ταυτόχρονα, κάθε κόμβος του δικτύου κατέχει ένα αντίγραφο όλων των συστοιχίες, άρα και όλων των συναλλαγών που έχουν πραγματοποιηθεί, με αποτέλεσμα να καθιστάτε σχεδόν αδύνατη η ακύρωση ή αλλαγή κάποιας παλαιότερης συναλλαγής, από κάποιον κακόβουλο χρήστη.

Η μεγαλύτερη ζημία που μπορεί να υποστεί το δίκτυο του Bitcoin, είναι μια επίθεση πλειοψηφίας ή αλλιώς επίθεση 51%. Μια τέτοια επίθεση, απαιτεί μια ομάδα κακόβουλων ανθρακωρύχων να ελέγχουν περισσότερο από το ήμισυ της συνολικής υπολογιστικής δύναμης που χρησιμοποιείται για την λειτουργεία του δικτύου. Με αυτόν τον τρόπο, για όσο χρονικό διάστημα θα έχουν τον έλεγχο, θα μπορούν να αποτρέπουν την επιβεβαίωση νέων συναλλαγών αλλά και να αναιρούν συναλλαγές που έχουν ολοκληρωθεί οδηγώντας σε διπλή δαπάνη. Ακόμα και σε αυτήν την περίπτωση όμως, θα ήταν αδύνατο να δημιουργήσουν νέα κρυπτονομίσματα από το μηδέν ή να επεξεργαστούν παλαιότερα συστοιχίες προς όφελος τους. Μια τέτοια επίθεση θα έβλαπτε τρομερά την αξιοπιστία του δικτύου αλλά δεν θα μπορούσε να το καταστρέψει. Επίσης, αν και θεωρητικά υπάρχει το ενδεχόμενο να πραγματοποιηθεί μια τέτοια επίθεση, είναι πρακτικά σχεδόν αδύνατο διότι η υπολογιστική δύναμη που χρησιμοποιείται πλέον για την λειτουργεία του δικτύου του Bitcoin έχει φτάσει σε τρομερά επίπεδα, και το να ελεγχθεί το 51% φαντάζει τρομερά δύσκολο εγχείρημα ενώ θα απαιτηθεί ένα υπέρογκο ποσό για να πραγματοποιηθεί αποτελεσματικά η επίθεση.

Συμπερασματικά, η ασφάλεια του δικτύου του Bitcoin είναι πολυεπίπεδη. Ο κατακερματισμός αλλά και τα αντίγραφα που κρατάνε όλοι οι κόμβοι του δικτύου με συνδυασμό τους εξορύκτες και την τεράστια υπολογιστική δύναμη που χρησιμοποιούν για την λειτουργία του δικτύου το κάνουν αδιαπέραστο. Από το πρώτο συστοιχίες συναλλαγών το 2009 μέχρι και σήμερα το δίκτυο δεν σταμάτησε να λειτουργεί ούτε μια φορά, αλλά δεν κλάπηκε και ποτέ κάποιο Bitcoin από την αλυσίδα.

5.4)Ποιες είναι οι δυνατότητες κλιμάκωσης του δικτύου?

Το Bitcoin, αποτελεί το πρώτο κρυπτονόμισμα που έχει δημιουργηθεί, και έχει τραβήξει αρκετά βλέμματα πάνω του τα τελευταία χρόνια. Οι ασφαλείς συναλλαγές, σε συνδυασμό με την αποκέντρωση που προσφέρει, έχουν κάνει την αξία του νομίσματος να έχει αυξηθεί εκθετικά. Αν και αποτελεί μια τρομερή καινοτομία, το δίκτυο του δεν είναι τελείως ιδανικό. Η αύξηση της δημοτικότητας του, οδήγησε σε περισσότερους νέους χρήστες να το χρησιμοποιήσουν σαν μέσο συναλλαγών, φέρνοντας έτσι στην επιφάνεια το κυριότερο πρόβλημα του δικτύου που είναι η κλιμάκωση του. Το Bitcoin, μπορεί να εξυπηρετήσει περίπου εφτά συναλλαγές το δευτερόλεπτο και αυτό οφείλεται στον χρόνο που χρειάζεται για να δημιουργηθεί ένα νέο συστοιχίες αλλά και στην χωρητικότητα του. Η συγκεκριμένη απόδοση, είναι σίγουρα κάθε άλλο παρά ιδανική αφού ο μέσος χρόνος συναλλαγών είναι περίπου εξήντα λεπτά, προκαλώντας δυσαρέσκεια στους συναλλασσόμενους.

Έχουν προταθεί αρκετές λύσεις για το πρόβλημα της κλιμάκωσης του Bitcoin, όμως όλες αυτές οι λύσεις έχουν ένα κοινό χαρακτηριστικό. Το κοινό χαρακτηριστικό είναι, πως για να αυξηθούν οι ταχύτητες συναλλαγών στο δίκτυο θα πρέπει να θυσιαστούν κάποιες από τις βασικές αρχές που έθεσε ο δημιουργός του όπως η ασφάλεια ή η αποκέντρωση.

Οι δημοφιλέστερες λύσεις που έχουν εμφανιστεί μέχρι σήμερα χωρίζονται σε δυο κατηγορίες. Της λύσεις επιπέδου ένα (layer 1) και τις λύσεις επιπέδου δυο (layer 2). Αρχικά, οι λύσεις επιπέδου ένα αποτελούν αλλαγές που συμβαίνουν πάνω στο δίκτυο του Bitcoin και το επηρεάζουν άμεσα. Μια τέτοια λύση θα πρέπει να γίνει αποδεκτή από ολόκληρη την κοινότητα και ενδεχόμενος να αλλάξει αρκετούς από τους κανόνες

που είχε θέσει ο Satoshi Nakamoto. Στον αντίποδα, οι λύσεις επιπέδου δυο δεν ενσωματώνονται πάνω στο βασικό δίκτυο του Bitcoin αλλά λειτουργούν παράλληλα με αυτό χωρίς να προβούν σε ριζικές αλλαγές. Είναι στην ευχέρεια του κάθε χρήστη αν θα επιλέξει να το χρησιμοποιήσει ή όχι και ο σκοπός τους είναι συνήθως να μεταφέρουν μεγάλους όγκους συναλλαγών εκτός του βασικού δικτύου με σκοπό την αποσυμφόρηση του. Στο επόμενο κεφάλαιο θα αναλυθούν μερικές από τις δημοφιλέστερες λύσεις επιπέδου ένα και δύο ενώ θα παρατεθούν και τα βασικότερα πλεονεκτήματα αλλά και μειονεκτήματα τους.

Κεφάλαιο 6: Λύσεις στο πρόβλημα κλιμάκωσης του bitcoin

Όπως αναλύθηκε, η αχίλλειος φτέρνα του bitcoin όσο αφορά την παγκόσμια υιοθέτηση του, ως ένα μέσο συναλλαγών είναι ο όγκος στον οποίο μπορεί να εκτελεί συναλλαγές ταυτόχρονα. Προς το παρόν, οι περισσότερες συναλλαγές εκτελούνται σε σύντομο χρονικό διάστημα, ωστόσο αν ο όγκος συναλλαγών συνεχίσει να αυξάνεται θα αυξηθούν ταυτόχρονα και ο χρόνος έγκρισης μιας συναλλαγής αλλά και το κόστος της .Οι εφτά, περίπου, συναλλαγές που μπορεί να πραγματοποιεί το δευτερόλεπτο δεν είναι ικανοποιητικές, ειδικά αν συγκριθούν με τις χιλιάδες συναλλαγές που εκτελούνται από τα παραδοσιακά χρηματοπιστωτικά ιδρύματα. Αυτό, είχε σαν αποτέλεσμα να ωθήσει αρκετούς προγραμματιστές και άτομα του χώρου στο να βρούνε κάποια λύση ώστε να βελτιώσουν τις αποδώσεις του δικτύου του Bitcoin κάνοντας το αρκετά πιο εύχρηστο. Στο κεφάλαιο αυτό θα αναλυθούν κάποιες από αυτές τις «λύσεις» που έχουν αναπτυχθεί, ενώ θα αναφερθούν τα προτερήματα αλλά και τα μειονεκτήματα τους.

6.1) Lighting Network

«Εικόνα 13»

6.1a) Τι είναι το Lighting Network.

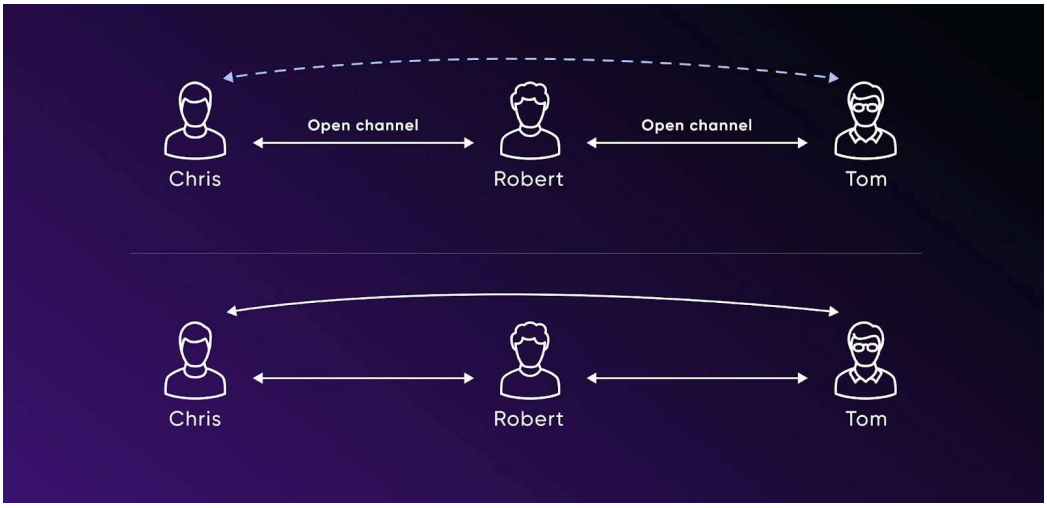
Το Lighting Network, είναι ίσως η πιο γνώστη και αποτελεσματική αναβάθμιση που έχει πραγματοποιηθεί πάνω στο δίκτυο του Bitcoin. Προτάθηκε για πρώτη φορά από τους Joseph Poon και Thaddeus Dryad στις 28 Φεβρουαρίου του 2015 με την δημοσίευση της λευκής βίβλου του με όνομα “Lighting Network whitepaper 0.5 by Joseph Poon and Thaddeus Dryad” και βρίσκεται υπό ανάπτυξη μέχρι και σήμερα. Το Lighting Network είναι ένα πρωτόκολλο πληρωμών επιπέδου 2 (layer 2) που τοποθετείται και λειτουργεί πάνω στο Bitcoin αλλά και σε άλλα κρυπτονομίσματα. Χρησιμοποιεί κανάλια πληρωμών που βρίσκονται εκτός της βασικής αλυσίδας του δικτύου του Bitcoin (off-chain), για να κλιμακώσει την ικανότητα του δικτύου και να διεξάγει συναλλαγές πιο αποτελεσματικά. Οι συναλλαγές που πραγματοποιούνται με την χρήση του Lighting Network είναι πολύ πιο γρήγορες καθώς επιβεβαιώνεται η εγκυρότητα τους πιο άμεσα αλλά και πιο οικονομικές σε σύγκριση με αυτές που πραγματοποιούνται απευθείας στο δίκτυο του Bitcoin (on-chain).

Ο λόγος που δημιουργήθηκε είναι για να πραγματοποιούνται συναλλαγές και εκτός της κύριας αλυσίδας του Bitcoin, με αποτέλεσμα την αποσυμφόρηση του δικτύου. Εάν το Bitcoin στο μέλλον καταφέρει να γίνει ένα μέσο για καθημερινές συναλλαγές, θα

χρειαστεί μια τέτοια τεχνολογία για αρκετούς λόγους. Καταρχάς, λόγου των αυξημένων συναλλαγών, η έγκριση τους από τους κόμβους έτσι ώστε να καταχωρηθούν στα συστοιχίες του Bitcoin, αλλά και η αποθήκευση τους θα είναι τρομερά ακριβή και χρονοβόρα. Επιπλέον, με την αύξηση των συναλλαγών, θα πρέπει να αυξηθεί και η ισχύς της υπολογιστικής δύναμης που απαιτείται για την λειτουργία του Bitcoin άρα και η ενέργεια που δαπανάται από αυτήν. Αυτό από μόνο του καθιστά το δίκτυο του Bitcoin απαγορευτικά δαπανηρό σε παγκόσμια κλίμακα αν χρησιμοποιηθεί για καθημερινές συναλλαγές.

Το Lighting Network, προσπαθεί να επιλύσει αυτά τα προβλήματα δημιουργώντας ένα δεύτερο στρώμα (second layer) επάνω στο αυθεντικό του Bitcoin. Το στρώμα αυτό αποτελείται από πολλά κανάλια πληρωμών μεταξύ χρηστών του Bitcoin για την δημιουργία συναλλαγών. Οι συναλλαγές αυτές, μεταξύ δύο για παράδειγμα χρηστών, μπορούν να είναι πάρα πολλές χωρίς να ενημερώσουν το κύριο δίκτυο του Bitcoin καθώς οι συναλλαγές αυτές υποβάλλονται σε διαφορετική επεξεργασία σε σχέση με της τυπικές που εκτελούνται πάνω στο δίκτυο του Bitcoin. Το δίκτυο του Bitcoin θα ενημερωθεί μόνο όταν ανοίξει ή κλείσει ένα κανάλι πληρωμών χωρίς έτσι να πρέπει να γεμίζει τα συστοιχίες με τις ενδιάμεσε συναλλαγές.

6.1b) Πως λειτουργεί το Lighting Network.



«Εικόνα 14»

Ο τρόπος που λειτουργεί το Lighting Network είναι αρκετά απλός κάνοντας το αρκετά εύχρηστο στις καθημερινές συναλλαγές. Αρχικά, δύο χρήστες για να ξεκινήσουν τις συναλλαγές μεταξύ τους, με την χρήση του Lighting Network, θα πρέπει να βρίσκονται σε ένα κοινό κανάλι πληρωμών. Για να συμβεί αυτό, θα πρέπει να δημιουργήσουν μια συναλλαγή πολλαπλών υπογραφών (multisignature transaction) στο δίκτυο του Bitcoin, και τουλάχιστον ο ένας από τους δυο να δεσμεύσει ένα ποσό χρημάτων που θέλει να χρησιμοποιήσει. Οι δύο πλευρές, θα έχουν από ένα ιδιωτικό κλειδί και για να πραγματοποιηθεί μια συναλλαγή θα πρέπει να υπογράψουν και τα δύο κλειδιά, άρα να συμφωνήσουν και οι δυο. Το άνοιγμα ενός καναλιού διαρκεί περίπου δέκα λεπτά, όσο χρειάζεται δηλαδή για να δημιουργηθεί ένα νέο συστοιχίες, στην συνέχεια όμως οι εμπλεκόμενοι έχουν την δυνατότητα να πραγματοποιήσουν όσες συναλλαγές θέλουν χωρίς κάποιο όριο, χρησιμοποιώντας πάντα τα Bitcoin που έχουν διατεθεί στο κανάλι σαν υπόλοιπο. Ταυτόχρονα, δεν απαιτείται συνεργασία από τους δυο χρήστες για να κλείσουν το κανάλι καθώς μπορούν μονομερώς να το κάνουν τερματίζοντας έτσι τις σχέσεις τους. Αφού κλείσει ένα κανάλι, η τελευταία υπογεγραμμένη και από τους δυο χρήστες συναλλαγή, μεταφέρεται στο δίκτυο του Bitcoin, και έτσι μοιράζονται σωστά τα υπόλοιπα στις δυο πλευρές με βάση τις συναλλαγές που έχουν πραγματοποιηθεί μέσα σε αυτό.

Μια ακόμα σπουδαία δυνατότητα του Lighting Network είναι πώς δεν χρειάζεται ένας χρήστης να έχει ανοιχτά κανάλια πληρωμών με όλους όσους θέλει να πραγματοποιήσει συναλλαγές. Αν έχει ένα ενεργό κανάλι συναλλαγών με κάποιον άλλον, και αυτός ο άλλος έχει με έναν τρίτο, τότε θα μπορεί επίσης να στείλει Bitcoin στον τρίτο μέσο του χρήστη που έχει το ενεργό κανάλι.

Για να γίνει πιο κατανοητό, υπάρχει για παράδειγμα ο χρήστης Α και σκοπεύει να αγοράζει καθημερινά αρκετούς καφέδες και να πληρώσει με Bitcoin από μια καφετέρια η οποία δέχεται Bitcoin. Αν επιλέξει να το κάνει χρησιμοποιώντας το κύριο δίκτυο του Bitcoin, οι φόροι συναλλαγής που θα πληρώσει θα είναι αρκετά υψηλοί και η διαδικασία αρκετά χρονοβόρα. Έτσι, επιλέγει να χρησιμοποιήσει το Lighting Network. Ανοίγει ένα κανάλι πληρωμών με την καφετέρια, και δεσμεύει ένα ποσό για τις αγορές του. Η συναλλαγή αυτήν, καταχωρείται στο δίκτυο του Bitcoin και η καφετέρια μπορεί άμεσα να εξακριβώσει αν ο χρήστης Α έχει όντως καταθέσει το ποσό για να ξεκινήσουν οι συναλλαγές. Παράλληλα, ο χρήστης Β επιθυμεί να αγοράσει και ο ίδιος καφέ από την ίδια καφετέρια αλλά δεν έχει ενεργό κανάλι πληρωμών μαζί της. Έχει όμως με τον

χρήστη Α. Έτσι, του δίνεται η δυνατότητα να χρησιμοποιήσει σαν μεσολαβητή τον χρήστη Α για να αγοράσει τελικά τον καφέ του από την καφετέρια χρησιμοποιώντας το Lighting Network.

6.1c) Θετικά και αρνητικά του Lighting Network

Το Lighting Network αν και παρουσιάστηκε για πρώτη φορά το 2015 βρίσκεται ακόμα σε αρχικό στάδιο. Είναι μια νέα τεχνολογία, που αν και τρομερά καινοτόμα, δεν έχει αποδείξει ακόμα την αξία της. Έτσι, είναι αναγκαίο να αναφερθούν τα θετικά αλλά και τα αρνητικά στοιχεία που την αντικατοπτρίζουν.

Αναλύοντας πρώτα τα θετικά του στοιχεία, κάποια από τα σημαντικότερα είναι:

- Η ταχύτητα που προσφέρει.

Αρχικά, ένα από τα σημαντικότερα προτερήματα του Lighting Network είναι η απίστευτη ταχύτητα που προσφέρει στους χρήστες του. Οι συναλλαγές, όπως αναφέρθηκε, γίνονται εκτός του δικτύου του Bitcoin και έτσι εκτελούνται σχεδόν ακαριαία.

- Το κόστος τον συναλλαγών.

Παράλληλα, τα κόστη για τις συναλλαγές αυτές είναι αισθητά μικρότερα από τα κόστη που θα καλούνταν να καταβάλει κάποιος που θα χρησιμοποιούσε το δίκτυο του Bitcoin. Ο λόγος που συμβαίνει αυτό, είναι διότι οι μοναδικές συναλλαγές που θα ενταχθούν στα συστοιχίες του Bitcoin θα είναι το άνοιγμα και το κλείσιμο ενός καναλιού πληρωμών, και όχι όλες οι συναλλαγές ενδιάμεσα. Όσες και αν είναι αυτές. Οι ενδιάμεσες συναλλαγές συνήθως κοστίζουν αμελητέα ποσά ή πραγματοποιούνται και δωρεάν.

- Απόρρητο.

Το Lighting Network προσφέρει στους χρήστες του ανωνυμία. Δημιουργήθηκε για να λειτουργεί εκτός του δικτύου του Bitcoin με αποτέλεσμα οι συναλλαγές που γίνονται σε αυτό να μην καταγράφονται δημόσια όπως συμβαίνει με το Bitcoin. Ακόμα, και στην περίπτωση που κάποιος χρησιμοποιήσει ένα κανάλι πληρωμών τρίτου για να

πραγματοποιήσει μια συναλλαγή, ο μεσάζοντας θα μπορεί να δει την συναλλαγή αλλά όχι τον προορισμό της ή την πηγή της. Έτσι, ειδικά σε παγκόσμια κλίμακα είναι αδύνατον κάποιος να αποσπάσει αυτές τις πληροφορίες.

- Αποκέντρωση.

Ένα ακόμα σημαντικό προτέρημα του Lighting Network είναι η αποκέντρωση που προσφέρει. Δίνεται η δυνατότητα στον καθένα να δημιουργήσει έναν κόμβο χρησιμοποιώντας υπολογιστική δύναμη και να εισέλθει στο δίκτυο του Lighting Network. Έτσι, δεν θα χρειάζεται κάποιο ανταλλακτήριο για να μεταφέρει Bitcoin από ένα πορτοφόλι σε κάποιο άλλο και θα έχει τον πλήρη έλεγχο των συναλλαγών του. Τέλος, δεν θα χρεώνεται με τα κόστη των συναλλαγών που πραγματοποιεί με την χρήση του Lighting Network, αλλά και θα ανταμείβεται από τα κόστη που θα πληρώνουν άλλοι χρήστες που δεν έχουν τον προσωπικό τους κόμβο και χρησιμοποιούν τον δικό του σαν μεσάζοντα.

- Αριθμός συναλλαγών.

Δεν υπάρχουν θεμελιώδη όρια στο ποσό των συναλλαγών που μπορούν να πραγματοποιηθούν ανά δευτερόλεπτο βάση του πρωτοκόλλου και του τρόπου σχεδιασμού του Lighting Network. Το ποσό αυτό μπορεί να περιοριστεί μόνο από τη χωρητικότητα και τη ταχύτητα των κόμβων που λειτουργούν πάνω στο Lighting Network.

- Ελαστικότητα.

Επιπρόσθετα, το Lighting Network δίνει την δυνατότητα να πραγματοποιούνται συναλλαγές με πολύ μικρά ποσά προσφέροντας έτσι ελαστικότητα στις συναλλαγές.

Στον αντίποδα τονίζονται κάποια από τα αρνητικά στοιχεία που χαρακτηρίζουν το Lighting Network τα οποία είναι :

- Πιθανότητα μελλοντικής κεντρικοποίησης.

Ένα από τα σημαντικότερα πλεονεκτήματα του Lighting Network όπως αναλύθηκε, είναι ότι δίνεται η δυνατότητα στον καθένα να δημιουργήσει τον δικό του

κόμβο και έτσι να μην χρειάζεται κάποιον μεσάζοντα προκειμένου να πραγματοποιεί συναλλαγές. Το πρόβλημα με αυτό, είναι πως για να λειτουργεί κάποιος τον δικό του κόμβο οφείλει να ασχοληθεί αρκετά με την συγκεκριμένη τεχνολογία μελετώντας την εις βάθος προτού το κάνει. Ακόμα χρειάζεται γνώσεις προγραμματισμού και άλλων δεξιοτήτων που δεν κατέχει ο μέσος χρήστης. Η εύκολη λύση λοιπόν για κάποιον που δεν έχει τις γνώσεις ή τον χρόνο για να ασχοληθεί, είναι να χρησιμοποιήσει κάποιον ήδη υπάρχων κόμβο. Αυτό μπορεί να το κάνει εύκολα, εγκαθιστώντας απλά μια εφαρμογή στο κινητό ή τον υπολογιστή του με την προϋπόθεση όμως πως πρέπει να εμπιστεύεται πλέον την ομάδα που διαχειρίζεται τον κόμβο που συνήθως είναι κάποιο μεγάλο ανταλλακτήριο ή κάποιος οργανισμός . Όσο πιο διαδεδομένο θα γίνεται το Lighting Network τόσοι περισσότεροι χρήστες θα το χρησιμοποιούν και όπως είναι λογικό η συντριπτική πλειοψηφία θα επιλέξει να χρησιμοποιεί την γρήγορη και εύκολη οδό. Κάτι που συμβαίνει και σήμερα αλλά σε μικρότερο βαθμό. Το αποτέλεσμα είναι να διοχετευθεί περισσότερη δύναμη στους λίγους και έτσι να χάνεται η αποκέντρωση. Θα συμβεί δηλαδή ότι συμβαίνει και στο τραπεζικό σύστημα, κάτι που είναι τελείως αντίθετο με την ιδεολογία του Bitcoin.

- Διπλή δαπάνη.

Ένα ακόμα σοβαρό πρόβλημα που αντιμετωπίζει το Lighting Network, είναι πως ένας κόμβος για να δεχτεί με ασφάλεια μια συναλλαγή θα πρέπει να είναι συνδεδεμένος στο δίκτυο ασταμάτητα. Εάν το ένα μέρος δεν είναι συνδεδεμένο, υπάρχει κίνδυνος το άλλο μέρος να τερματίσει το κανάλι πληρωμών και να διευθετήσει μια συναλλαγή που δεν είναι απαραίτητα εγκεκριμένη. Πιο συγκεκριμένα, όταν πραγματοποιείται μια νέα συναλλαγή σε ένα κανάλι πληρωμών, ενώ έχουν προηγηθεί και άλλες, υπογράφεται και από τα δύο μέρη και καθορίζει τα υπόλοιπα τους εκείνη την χρονική στιγμή. Σε περίπτωση όμως που το ένα μέρος για κάποιο λόγο αποσυνδεθεί από το Lighting Network, για ένα εύλογο χρονικό διάστημα, δίνει την δυνατότητα στο άλλο να κλείσει το κανάλι και να μεταδώσει στο δίκτυο του Bitcoin μια παλιότερη συναλλαγή ευνοώντας το. Αντίθετα, αν ήταν μονίμως συνδεδεμένο θα μπορούσε να το αποτρέψει αυτό, αμφισβητώντας αυτήν την ενέργεια από το κακόβουλο μέρος. Σε αυτήν την περίπτωση το κακόβουλο μέρος θα έχανε όλο του το κεφάλαιο σαν τιμωρία.

Η απαίτηση να είναι όλοι οι κόμβοι συνδεδεμένοι συνέχεια, είναι πολύ μεγάλη επιβάρυνση για να επεκταθεί το Lighting Network και να καθιερωθεί ως μια παγκόσμια

λύση πληρωμών. Για να αντιμετωπιστεί αυτό, εντάχτηκε στο δίκτυο του μια υπηρεσία με το όνομα “Watchtowers” (σκοπιά) η οποία δημιουργήθηκε για να παρακολουθεί συνεχώς την κατάσταση των καναλιών καθώς και των υπολοίπων των κόμβων, απελευθερώνοντας τους έτσι από την συνεχή σύνδεση. Για να χρησιμοποιήσει κάποιος όμως αυτήν την υπηρεσία, θα πρέπει να αισθάνεται άνετα με τις πληροφορίες που θα παρέχει σε ένα Watchtower. Αυτό, θα είναι σε θέση να γνωρίζει το υπόλοιπο του χρήστη, τον προορισμό των συναλλαγών του, τα ποσά των συναλλαγών του, καθώς και τα ποσά που δέχεται αυτός σαν παραλήπτης. Πληροφορίες οι οποίες θα μπορούσαν να διαρρεύσουν κάποτε βλάπτοντας τον και μειώνοντας έτσι το απόρρητο που προσφέρει το Lighting Network. Τέλος, αυτήν είναι μια λύση ώστε να εμπιστευτεί κάποιος έναν τρίτο για την αποτροπή διπλών δαπανών, κάτι που είναι ακριβώς αυτό που έλυσε ο Satoshi Nakamoto με την δημιουργία του Bitcoin. Όπως είχε δηλώσει και ο ίδιος στην λευκή βίβλο του Bitcoin είναι ότι “Τα κύρια οφέλη χάνονται εάν ένα τρίτο μέρος εξακολουθεί να είναι απαραίτητο για να αποτρέψει τη διπλή δαπάνη”. (Satoshi Nakamoto 2008, whitepaper σελ1)

- Δυσκολία σε μεγάλες συναλλαγές.

Υπάρχουν δύο εκδοχές για να πραγματοποιηθεί μια συναλλαγή με την χρήση του Lighting Network. Η πρώτη είναι τα δυο μέλη να βρίσκονται σε κάποιο κοινό κανάλι πληρωμών και να συναλλάσσονται απευθείας. Σε αυτήν την περίπτωση έχουν την δυνατότητα να δεσμεύσουν μέχρι 0.16 Bitcoin, που είναι και το όριο σε κάθε κανάλι. Αυτήν η εκδοχή έχει βάση όμως, μόνο αν έχουν σκοπό να πραγματοποιήσουν πάνω από δυο συναλλαγές μεταξύ τους, διότι αλλιώς θα μπορούσαν να τις κάνουν με την χρήση του δικτύου του Bitcoin. Η άλλη εκδοχή είναι να μην έχουν κοινό κανάλι μεταξύ τους και να χρειαστεί η συναλλαγή να περάσει από άλλους κόμβους για να φτάσει στον παραλήπτη. Σε περίπτωση όμως, που δεν υπάρχει επαρκής ρευστότητα μεταξύ των κόμβων για την δρομολόγηση αυτής της συναλλαγής, η συναλλαγή θα αποτύχει και το ποσό θα επιστρέψει στον αποστολέα. Αυτό καθιστά το Lighting Network εύχρηστο κυρίως για μικρές συναλλαγές και δυσκολεύει αρκετά την υιοθέτηση του από μεγάλους οργανισμούς και εταιρίες.

- Αστάθεια στην τιμή του Bitcoin.

Όπως είναι γνωστό, αυτό που χαρακτηρίζει την αξία του Bitcoin από επενδυτική σκοπιά είναι οι συχνές και απότομες αλλαγές της. Εξαιτίας της σχετικά μικρής κεφαλαιοποίησης του, η τιμή του μπορεί να αλλάξει απότομα και να επηρεαστεί αρκετά από εξωγενείς παράγοντες. Αυτό το γεγονός έχει δυο αρνητικές επιρροές στο Lighting Network.

Αρχικά, το Lighting Network, για να χαρακτηριστεί ως ένα ισχυρό και παγκόσμιο μέσο πληρωμών, θα πρέπει να επεκταθεί αρκετά και να βρίσκεται σε λειτουργεία ένας μεγάλος αριθμός καναλιών ανά τον κόσμο, συνδέοντας έτσι τους χρήστες μεταξύ τους. Το αντίκτυπο, στις συχνές και απότομες αλλαγές της τιμής του Bitcoin, είναι πως θα ωθήσει αρκετούς που έχουν δεσμεύσει τα κεφάλαια τους σε Bitcoin στο Lighting Network να τα αποδεσμεύσουν κλείνοντας τα κανάλια πληρωμών που συμμετέχουν. Σε περίπτωση που η τιμή του Bitcoin ανεβεί, θα επιθυμούν να πουλήσουν για κέρδος, ενώ αν η τιμή πέσει, εξαιτίας του πανικού θα πουλήσουν από φόβο σε μια μεγαλύτερη μελλοντική πτώση. Αναμφίβολα, σε μια τέτοια κατάσταση αρκετά κανάλια πληρωμών θα κλείσουν και το δίκτυο το Lighting Network θα συρρικνωθεί μειώνοντας έτσι και τις δυνατότητες του.

Επιπλέον, η αστάθεια της τιμής του Bitcoin καθιστά δύσκολη την χρήση του Lighting Network για καθημερινές συναλλαγές. Για παράδειγμα, κάποιος ο οποίος βρίσκεται σε κανάλι συναλλαγών με μια καφετέρια, και αγοράζει καθημερινά καφέ, σε μια αύξηση της τιμής ο καφές θα του κοστίσει περισσότερο από πριν. Από την άλλη πλευρά, το ίδιο θα συμβεί και στην καφετέρια κατά την πληρωμή κάποιου τιμολογίου σε έναν προμηθευτή αν η τιμή ανεβεί.

6.2) Αύξηση στο μέγεθος των συστοιχίες.

«Εικόνα 15»

Όλα τα δεδομένα του δικτύου του Bitcoin, όπως συναλλαγές και υπογραφές συναλλαγών, αποθηκεύονται σε συστοιχίες τα οποία συνδέονται μεταξύ τους με τέτοιο τρόπο ώστε το ένα να εξαρτάται από το προηγούμενο. Με αυτόν τον τρόπο δημιουργείται μια αλυσίδα η οποία είναι και η βάση δεδομένων του Bitcoin. Το μέγεθος των συστοιχίες, είναι μια παράμετρος στο πρωτόκολλο του Bitcoin καθώς επηρεάζει τον αριθμό των συναλλαγών που μπορούν να επιβεβαιωθούν στο δίκτυο, αφού παράγεται ένα συστοιχίες κάθε δέκα λεπτά περίπου. Αν και το Bitcoin κυκλοφόρησε αρχικά χωρίς αυτήν την παράμετρο, ο Satoshi Nakamoto πρόσθεσε ένα όριο στο μέγεθος του κάθε συστοιχίες, όσο ήταν ακόμα ο κύριος προγραμματιστής του έργου. Το όριο αυτό ισχύει μέχρι και σήμερα, και είναι το ένα megabyte ανά συστοιχίες, το οποίο μεταφράζεται σε περίπου τρείς έως εφτά συναλλαγές ανά δευτερόλεπτο, ανάλογα με το μέγεθος τους. Ο λόγος που το έκανε αυτό ο Satoshi Nakamoto, ήταν για να αποτρέψει κάποιον τυχόν εισβολέα από την υπερφόρτωση του δικτύου με τεχνητά συστοιχίες γεμάτα με ψευδείς συναλλαγές.

Μερικά χρόνια μετά, και όσο το Bitcoin αποκτούσε φήμη αλλά και αξία, αρκετοί προγραμματιστές και χρήστες άρχισαν να διαφωνούν σχετικά με την χωρητικότητα των συστοιχίες. Καθώς η χρήση του Bitcoin αυξάνεται, ορισμένοι πιστεύουν πως είναι καιρός να αυξηθεί ή να αρθεί εντελώς το όριο μεγέθους των συστοιχιών, με αποτέλεσμα να εγκρίνονται περισσότερες συναλλαγές το δευτερόλεπτο και να τεθούν βάσεις για ένα παγκόσμιο μέσο πληρωμών. Αυτήν η οπτική χαρακτηρίζεται από κάποια θετικά αλλά και αρνητικά στοιχεία για το δίκτυο και την κοινότητα του Bitcoin και είναι αναγκαίο να αναλυθούν.

Ξεκινώντας από τα θετικά ως προς την μεγέθυνση των συστοιχιών, παρουσιάζονται τα εξής:

- Η ταχύτητα των συναλλαγών θα αυξηθεί εφόσον μεγαλώσει η χωρητικότητα των συστοιχιών

- Οι φόροι των συναλλαγών θα μειωθούν δραματικά, αφού θα εγκρίνονται περισσότερες συναλλαγές το δευτερόλεπτο και δεν θα υπάρχει φόρτος και πίεση στο δίκτυο του Bitcoin.

- Το Bitcoin πλέον θα μπορεί να ανταγωνιστεί άλλα μεγάλα συστήματα πληρωμών, και θα αποκτήσει μεγαλύτερο κύριος

- Το δίκτυο του Bitcoin θα είναι πλέον κατάλληλο για καθημερινές μικροσυναλλαγές και έτσι πιο ελκυστικό, για νέους χρήστες ή και επιχειρήσεις ως μέσο συναλλαγών.

Εντούτοις, στα αρνητικά της μεγέθυνσης των συστοιχιών αναφέρονται τα παρακάτω:

- Αύξηση του κόστους λειτουργίας ενός κόμβου.

Το πρώτο που εντοπίζεται είναι ότι οι μεγαλύτερες συστοιχίες αυξάνουν το κόστος λειτουργείας ενός κόμβου Bitcoin. Το δίκτυο, θα αναπτύσσεται πιο γρήγορα και θα χρειάζεται μεγαλύτερη υπολογιστική δύναμη για να λειτουργεί ένας κόμβος. Ακόμα όσο μεγαλύτερη είναι η συνολική αλυσίδα των συστοιχιών, τόσο περισσότερος χρόνος θα χρειάζεται για την εκκίνηση ενός νέου κόμβου στο δίκτυο, αφού θα πρέπει πρώτα να κατεβάσει και να επικυρώσει όλες τις προηγούμενες συναλλαγές και συστοιχίες. Αυτό, θα αποθαρρύνει αρκετά νέους χρήστες να λειτουργήσουν τον δικό τους κόμβο. Ταυτόχρονα, εφόσον το κόστος για έναν κόμβο θα γίνει πολύ υψηλό, οι χρήστες θα πρέπει να χρησιμοποιούν ελαφρύς κόμβους. Οι ελαφρύς κόμβοι δεν κατεβάζουν ολόκληρη την αλυσίδα των συστοιχιών αλλά κεφαλίδες μόνο για να επικυρώσουν την αυθεντικότητα των συναλλαγών. Πρέπει όμως να βασίζονται σε έναν κανονικό κόμβο για να λειτουργούνε με ασφάλεια. Ο κίνδυνος, θα είναι πως κάποιος κακόβουλος θα

μπορεί να κάνει συναλλαγές με ένα νόμισμα απομίμησης του Bitcoin ενώ οι παραλήπτες δεν θα είναι σε θέση να γνωρίζουν αν είναι αληθινό ή όχι αφού με τον ελαφρύ κόμβο δεν θα έχουν αποθηκευμένη την «ιστορία» του δικτύου του Bitcoin. Ο μόνος τρόπος για να το μάθουν θα είναι την στιγμή που θα προσπαθήσουν να το ξοδέψουν όμως τότε θα είναι αργά.

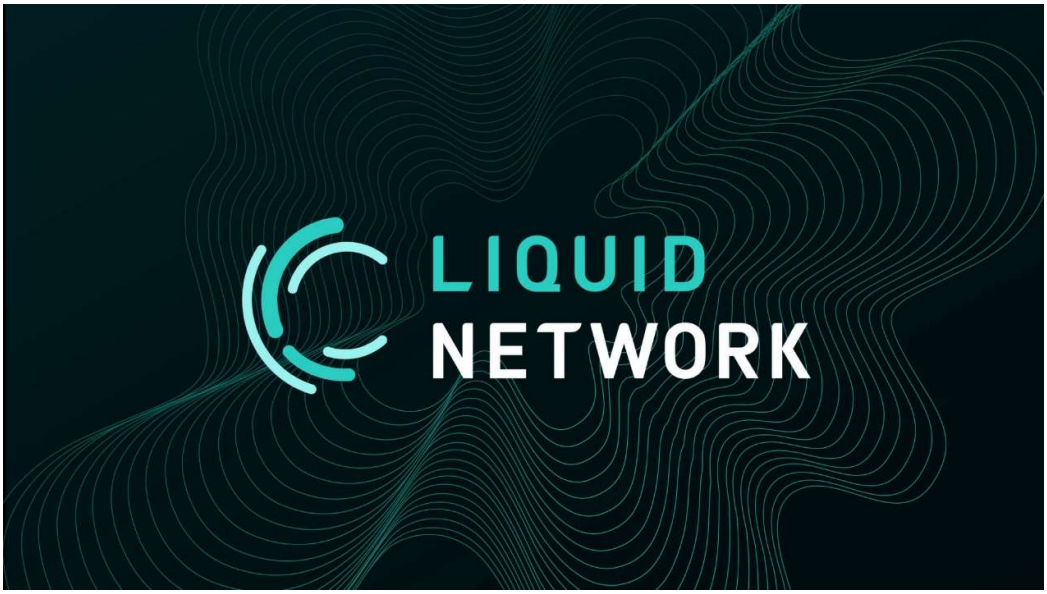
- Συγκεντροποίηση εξόρυξης.

Ένα δεύτερος κίνδυνος, που εντοπίζεται με την αύξηση της χωρητικότητας των συστοιχιών είναι ότι θα μπορούσαν να οδηγήσουν σε συγκέντρωση εξόρυξης. Όταν ένας εξορύκτης βρίσκει ένα νέες συστοιχίες στέλνει αυτό τις συστοιχίες σε ολόκληρο το δίκτυο. Οι μεγαλύτερες συστοιχίες κατά κανόνα, χρειάζονται περισσότερο χρόνο για να καταλήξουν στους υπόλοιπους εξορύκτες. Ενώ οι συστοιχίες μεταφέρονται σε αυτούς, ο εξορύκτης που το βρήκε μπορεί να ξεκινήσει αμέσως την εξόρυξη πάνω στο νέες συστοιχίες αποκτώντας έτσι ένα προβάδισμα για την εύρεση του επόμενου. Οι μεγαλύτεροι εξορύκτες βρίσκουν περισσότερες συστοιχίες όπως είναι λογικό από τους μικρότερους αφού η υπολογιστική δύναμη που χρησιμοποιούν είναι ανώτερη. Αυτήν η διαφορά θα μεγαλώσει αρκετά αν αυξηθεί το μέγεθος των συστοιχιών, και το προβάδισμα που θα έχουν θα είναι τεράστιο. Όλο αυτό, θα οδηγήσει στην μείωση των εξορυκτών, και η εξόρυξη θα γίνει απαγορευτική για αρκετούς. Το αποτέλεσμα θα είναι η εξόρυξη να γίνει πολύ συγκεντρωτική και έτσι θα μειωθεί δραματικά η αποκεντροποίηση του Bitcoin.

- Ζητήματα ασφαλείας

Με τα παραπάνω μειονεκτήματα, είναι προφανές πως το δίκτυο του Bitcoin θα μεταλλαχθεί σε ένα πιο κεντρικοποιημένο δίκτυο, θα έρθει δηλαδή σε αντίθεση με το όραμα που είχε για αυτό ο δημιουργός του. Εκτός όμως από την κεντρικοποίηση του δικτύου θα επηρεαστεί και η ασφάλεια του. Και ο λόγος είναι ο εξής. Διάφοροι οργανισμοί και εταιρίες εξόρυξης με μεγάλα κεφάλαια θα εκτοπίσουν τους μικρότερους εξορύκτες και θα έχουν τον πλήρη έλεγχο. Θα πρέπει οι χρήστες του Bitcoin να εμπιστεύονται αυτούς, και το Bitcoin θα καταλήξει να σαν ένα ακόμα παραδοσιακό χρηματοοικονομικό σύστημα. Τέλος, αν συσσωρευτεί έστω 51% της εξόρυξης σε μια οντότητα, τότε θα είναι σε θέση να ελέγξει το δίκτυο του Bitcoin και να παραποιήσει συναλλαγές προς όφελος της.

6.3) LIQUID NETWORK



«Εικόνα 16»

Το Liquid Network, είναι μια εξίσου σημαντική εναλλακτική που έχει δημιουργηθεί για να λύσει το πρόβλημα που αντιμετωπίζει το Bitcoin με την επεκτασιμότητα. Αν και όχι τόσο δημοφιλές όσο το Lighting Network, αφού και τα δύο είναι πλευρικές αλυσίδες πάνω στο δίκτυο του Bitcoin, συνεχώς αναβαθμίζεται και αρχίζει να αποκτά αρκετούς ενεργούς χρήστες. Το Liquid Network έχει σχεδιαστεί για να επιτρέπει την ιδιωτική, γρήγορη αλλά και ασφαλή μετακίνηση περιουσιακών στοιχείων και ενώ λειτουργεί με βάση το δίκτυο του Bitcoin, λειτουργεί ανεξάρτητα από αυτό χρησιμοποιώντας διαφορετικούς μεθόδους για να πετύχει υψηλότερη απόδοση με πιο εμπιστευτικές συναλλαγές.

Δημιουργήθηκε από την Blockstream, μια εταιρία που ιδρύθηκε το 2014 από τον Adam Black, και ο κύριος λόγος ήταν η ανάπτυξη προϊόντων και υπηρεσιών για την αποθήκευση και συναλλαγή ψηφιακών περιουσιακών στοιχείων. Πάραυτα, διοικείται από μια ομοσπονδία 63 αξιόπιστων οντοτήτων με το όνομα “Liquid Functionaries” η οποία περιλαμβάνει ανταλλακτήρια κρυπτονομισμάτων, χρηματοπιστωτικά ιδρύματα αλλά και άλλες επιχειρήσεις που βασίζονται στο Bitcoin. Αυτοί, παρέχουν την ομαλή

και σωστή λειτουργεία του δικτύου και είναι υπεύθυνοι και για την αξιοπιστία του. Ενώ ο καθένας μπορεί να λειτουργεί αυτόνομα έναν Liquid κόμβο, και να παρακολουθεί το δίκτυο, μόνο 15 οντότητες από την ομοσπονδία μπορούν να εκτελούν πλήρεις κόμβους και να δημιουργούν νέες συστοιχίες. Αυτές οι 15 θέσεις εναλλάσσονται τακτικά μεταξύ των μελών της ομοσπονδίας για να επιτευχθεί μια μορφή αποκέντρωσης.

Ουσιαστικά, ο τρόπος που λειτουργεί το Liquid Network είναι ο εξής. Εκδίδει μια «απομίμηση» του Bitcoin η οποία ονομάζεται L-BTC και ακολουθεί την τιμή του. Αυτό, είναι και το κύριο νόμισμα που χρησιμοποιείται στο δίκτυο του Liquid Network και για να το λάβουν οι χρήστες του θα πρέπει να πραγματοποιήσουν μια διαδικασία που ονομάζεται αμφίδρομη σύνδεση (two-way peg). Μια αμφίδρομη σύνδεση μεταξύ του δικτύου του Liquid Network και του Bitcoin , επιτρέπει σε κάποιον να κλειδώσει ένα επιθυμητό ποσό σε Bitcoin και να λάβει L-BTC ίδιας αξίας ως αντάλλαγμα. Το μόνο που έχει να κάνει, είναι αρχικά να αποστείλει Bitcoin σε μια συγκεκριμένη διεύθυνση στην κύρια αλυσίδα του Liquid Network που ανήκει στην Liquid Federation. Αμέσως μόλις επιβεβαιωθεί το ποσό του Bitcoin που στάλθηκε, ίση ποσότητα L-BTC αποστέλλεται στην διεύθυνση του χρήστη που βρίσκεται στο Liquid Network. Έπειτα, ο χρήστης είναι ελεύθερος να χρησιμοποιήσει το L-BTC σε συναλλαγές. Σε περίπτωση που επιθυμεί να μετατρέψει ξανά το L-BTC σε Bitcoin, και να επιστρέψει στην κύρια αλυσίδα του Bitcoin , θα πρέπει να πραγματοποιήσει την αντιστροφή διαδικασία, στέλνοντας το σε μια συγκεκριμένη διεύθυνση στο Liquid Network ενώ θα λάβει πίσω ίση αξία σε Bitcoin. Η διαδικασία θα ολοκληρωθεί μόλις η συναλλαγή επιβεβαιωθεί από δυο κόμβους. Τέλος, το L-BTC που ανταλλάχθηκε με Bitcoin καταστρέφεται.

Όπως το Lighting Network, το Liquid Network είναι και αυτό ένα δεύτερο στρώμα που λειτουργεί πάνω από το δίκτυο του Bitcoin. Ωστόσο, αυτές οι δυο τεχνολογίες έχουν διαφορετικούς στόχους και δεν αποτελούν απαραίτητα ανταγωνιστές. Ενώ το Lighting Network χρησιμοποιείται κυρίως για καθημερινές μικροπληρωμές, το Liquid Network εστιάζει σε συναλλαγές που περιλαμβάνουν μεγάλες ποσότητες Bitcoin. Επίσης, οι χρήστες τους διαφέρουν. Μικρές επιχειρήσεις βρίσκουν το Lighting Network αρκετά πιο εύχρηστο, σε αντίθεση με χρηματοπιστωτικά ιδρύματα και ανταλλακτήρια που χρησιμοποιούν το Liquid Network για εκτέλεση ιδιωτικών συναλλαγών αλλά και μεταφορά μεγάλων αξιών.

Σαν μια τεχνολογία που έχει δοκιμαστεί από την κοινότητα του Bitcoin, έχουν εντοπιστεί θετικά και αρνητικά στοιχεία όπου και την αντιπροσωπεύουν. Αρχικά, θα ακολουθήσει μια ανάλυση των θετικών.

- Ταχύτερες συναλλαγές.

Η παραγωγή των συστοιχιών στο Liquid Network πραγματοποιείται από 15 κόμβους και απαιτούνται περίπου δυο λεπτά για την δημιουργία μία συστοιχίας σε αντίθεση με το δίκτυο του Bitcoin που χρειάζεται περίπου δέκα λεπτά για κάθε νέα συστοιχία. Έτσι, το Liquid Network μπορεί να καταγράψει και να πραγματοποιήσει συναλλαγές τουλάχιστον πέντε φορές πιο γρήγορα, με αποτέλεσμα να αφαιρέσει αρκετό μέρος του φόρτου από το δίκτυο του Bitcoin.

- Χαμηλότερες χρεώσεις συναλλαγών.

Σε περιόδους συμφόρησης στο δίκτυο του Bitcoin, τα τέλη που καλείται να πληρώσει ένας συναλλασσόμενος είναι αρκετά μεγάλα, και πολλές φορές ξεπερνάνε ακόμα και την αξία την συναλλαγής. Αυτό συμβαίνει διότι για να πάρει προτεραιότητα μια συναλλαγή, σε σχέση με κάποιες άλλες, θα πρέπει να καταβληθούν μεγαλύτερα τέλη στους εξορύκτες. Στο Liquid Network, οι συναλλαγές εκτελούνται αρκετά γρηγορότερα με αποτέλεσμα τα τέλη να είναι αισθητά μικρότερα.

- Μεγαλύτερο απόρρητο.

Το Liquid Network, εφαρμόζει εμπιστευτικές συναλλαγές για την απόκρυψη βασικών πληροφοριών από τρίτους. Σε μία συναλλαγή, τα μοναδικά στοιχεία που καταγράφονται στις συστοιχίες και είναι ορατά από την κοινότητα του Liquid Network είναι η διεύθυνση αποστολής, η διεύθυνση λήψης, καθώς και η χρέωση της συναλλαγής. Με αυτόν τον τρόπο, δίνεται η δυνατότητα στους χρήστες να αποκρύπτουν το ποσό της συναλλαγής ή και άλλα ευαίσθητα στοιχεία που δεν επιθυμούν να προβάλουν δημόσια.

Οι δυνατότητες που προσφέρει το Liquid Network, είναι πραγματικά αρκετά βοηθητικές όσο αφορά την αποσυμφόρηση του δικτύου του Bitcoin και θα μπορούσε να χρησιμοποιηθεί σαν μια λύση για το πρόβλημα την επεκτασιμότητας. Υπάρχουν όμως και κάποια μειονεκτήματα που το χαρακτηρίζουν.

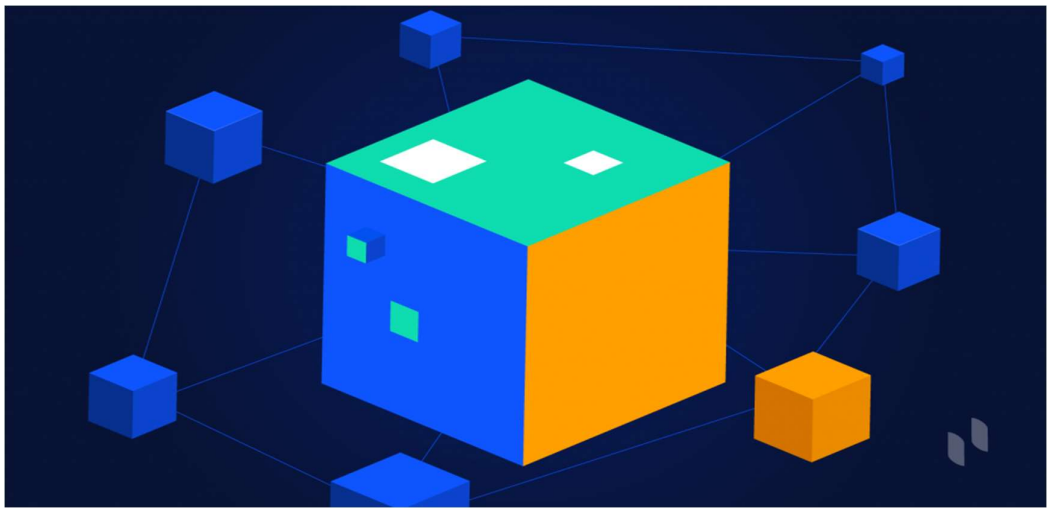
- Συγκεντροποίηση εξουσίας.

Για την συνολική λειτουργεία του Liquid Network, όπως αναφέρθηκε, είναι υπεύθυνη μια ομοσπονδία η οποία αποτελείται από 63 οντότητες. Από αυτούς, 15 δραστηριοποιούνται κάθε φορά, και ανά τακτά χρονικά διαστήματα αλλάζουν μεταξύ τους. Ως εκ τούτου, ένα κεντρικό σύστημα υπόκειται στον έλεγχο του δικτύου, κάνοντας το αυστηρά κεντρικοποιημένο.

- Ευάλωτο

Εκτός από το πρόβλημα που δημιουργείται με την λειτουργεία μόνο 15 κόμβων, στο δίκτυο του Liquid Network, όσο αφορά την αποκέντρωση, παρουσιάζεται και το πρόβλημα αντοχής του δικτύου σε κακόβουλες επιθέσεις. Στο δίκτυο του Bitcoin, οι ενεργοί κόμβοι που είναι υπεύθυνοι για την λειτουργεία του είναι χιλιάδες. Αυτό καθιστά σχεδόν αδύνατη μια πετυχημένη επίθεση εναντίον του. Το Liquid Network από την άλλη, βασίζεται μόνο σε 15, γεγονός που αυξάνει τον κίνδυνο λογοκρισίας και κακόβουλών επιθέσεων που θα οδηγούσαν στην συνολική αποτυχία του δικτύου.

6.4) Blockchain Sharding



«Εικόνα 17»

Η έννοια του δικτύου του Bitcoin βασίζεται σε μια αρχή που υποστηρίζει την ασφάλεια αλλά και την αποκέντρωση. Είναι δύο χαρακτηρίστηκα, που έχουν κάνει την τεχνολογία του τόσο ελκυστική, αλλά ταυτόχρονα περιορίζουν αρκετά την

επεκτασιμότητα του. Για να υπάρχει πλήρης αποκέντρωση και ασφάλεια, το δίκτυο του Bitcoin επιβάλει σε όλους τους ενεργούς κόμβους την επεξεργασία όλων των νέων συναλλαγών, καθώς και την δημιουργία ενός αντίγραφου, που περιλαμβάνει όλες τις συστοιχίες που έχουν ενταχθεί στην αλυσίδα του μέχρι και σήμερα. Παρόλο που τέτοια χαρακτηριστικά, εγγυούνται την ασφάλεια και την αποκέντρωση, δημιουργούν πρόβλημα στην ταχύτητα του δικτύου, αφού η κάθε συναλλαγή θα πρέπει να περάσει από χιλιάδες κόμβους. Έτσι, η υπέρβαση αυτού του φραγμού γίνεται όλο και πιο σημαντική. Μια λύση που έχει αναπτυχθεί για να ξεπεραστεί αυτό το πρόβλημα είναι μια τεχνική που ονομάζεται Blockchain Sharding (διαμοιρασμός της αλυσίδας των συστοιχιών)

Το Blockchain Sharding, χωρίζει το δίκτυο του Bitcoin σε πολλά ανεξάρτητα τμήματα που ονομάζονται Shards, με την δική τους εξουσία, ενώ το καθένα είναι υπεύθυνο για την αποθήκευση και τον υπολογισμό ενός συγκεκριμένου τμήματος δεδομένων. Ο φόρτος εργασίας κατανέμεται ομοιόμορφα μεταξύ των κόμβων, διευκολύνοντας έτσι την λειτουργία του δικτύου, και εξαλείφοντας την ανάγκη εκτέλεσης του ίδιου μεγάλου όγκου εργασίας. Επιπλέον, διαφορετικά τμήματα του Blockchain συγχρονίζονται μεταξύ τους, επιτρέποντας την ανταλλαγή δεδομένων, καθώς και την προβολή εγγραφών από άλλα γειτονικά Shards.

Το Blockchain Sharding, αποτελεί μια λύση επιπέδου ένα. Οι λύσεις επιπέδου ένα, είναι τεχνολογίες που ενσωματώνονται στο κύριο δίκτυο που τις υιοθετεί, αλλά συνήθως αλλάζουν κάποιους κανόνες του. Έτσι, πρέπει μια τέτοια προσθήκη να γίνει αποδεκτή από την κοινότητα για να χρησιμοποιηθεί. Οι λύσεις επιπέδου δύο από την άλλη, λειτουργούν παράλληλα με το κύριο δίκτυο, και δεν αλλάζουν κανένα του κανόνα. Ταυτόχρονα, είναι στην ευχέρεια του κάθε χρήστη αν θα χρησιμοποιεί ή όχι την καινοτομία που του προσφέρει μια μέθοδος επεκτασιμότητας επιπέδου δύο.

Σε αυτό το σημείο, θεωρείται απαραίτητο να αναλυθούν τα κύρια πλεονεκτήματα αλλά και μειονεκτήματα που χαρακτηρίζουν την συγκεκριμένη τεχνολογία. Αρχικά, τα θετικά είναι τα εξής:

- Επεκτασιμότητα.

Όπως είναι αντιληπτό, η ικανότητα του δικτύου να επεκτείνεται συνεχώς με την χρήση της τεχνολογίας Blockchain Sharding είναι πρακτικά απεριόριστη, γεγονός που οδηγεί σε βελτιωμένη απόδοση. Με το Blockchain Sharding, κάθε νέος κόμβος που

συνδέεται στο δίκτυο, δεν επιβαρύνει επιπλέον το ¨μητρώο¨, ενώ αντίθετα απλοποιεί την δουλεία του. Συνολικά, το δίκτυο του Bitcoin θα μπορεί να περιέχει περισσότερες πληροφορίες όταν εφαρμόζεται το Blockchain Sharding.

- Λιγότερο απαιτητικό.

Επιπλέον, ένα αξιοσημείωτο πλεονέκτημα του Blockchain Sharding είναι πως δεν απαιτείται ισχυρή υπολογιστική δύναμη από τους χρήστες του, για να λειτουργήσουν έναν κόμβο. Ένας προσωπικός υπολογιστής, θα είναι πλέον αρκετός και αυτό θα προσφέρει πρόσβαση σε αρκετούς νέους χρήστες που επιθυμούν να συμβάλουν στο δίκτυο του Bitcoin.

- Δημιουργία αποκεντρωμένων εφαρμογών

Με την είσοδο νέων χρηστών, καθώς και με την ύπαρξη περισσότερων κόμβων, το δίκτυο θα γνωρίσει γρηγορότερη ανάπτυξη και αυτό θα δώσει κίνητρο σε προγραμματιστές να δημιουργήσουν νέες αποκεντρωμένες εφαρμογές για την εξυπηρέτηση τους. Τέτοιες εφαρμογές, θα μπορούσαν να είναι αποκεντρωμένα ανταλλακτήρια καθώς και πλατφόρμες ανταλλαγής περιουσιακών στοιχείων.

- Μειωμένο κόστος συναλλαγών

Με τις συναλλαγές να εκτελούνται πιο γρήγορα, θα μειωθεί και το κόστος των συναλλαγών αφού δεν θα υπάρχει η ανάγκη για κάποιον να πληρώσει περισσότερα τέλη για να δρομολογηθεί γρηγορότερα η συναλλαγή του σε σχέση με τους υπόλοιπους.

Σε γενικές γραμμές, η τεχνολογία που μπορεί να προσφέρει το Blockchain Sharding στο δίκτυο του Bitcoin είναι τρομερή. Οι συναλλαγές θα αυξηθούν κατά πολύ ανά δευτερόλεπτο, θα μειωθούν αισθητά οι χρεώσεις των συναλλαγών και θα μειωθούν παράλληλα και οι καθυστερήσεις επεξεργασίας. Το αποτέλεσμα θα είναι πως η συγκεκριμένη μέθοδος θα οδηγήσει σε ένα πιο βελτιωμένο, ευκίνητο και κερδοφόρο δίκτυο. Το Blockchain Sharding όμως, δεν έχει εφαρμοστεί αρκετά από άλλα δίκτυα κρυπτονομισμάτων για να υπάρχει μια ξεκάθαρη απάντηση για το αν είναι μια σωστή επιλογή ή όχι. Χαρακτηρίζεται παράλληλα, από μερικά μειονεκτήματα που έχουν εμφανιστεί με την χρήση του, και είναι αναγκαίο να αναφερθούν.

- Επιρρεπή σε επιθέσεις

Η ικανότητα του δικτύου του Bitcoin, να αποθηκεύει ολόκληρο το ιστορικό συναλλαγών, και να επεξεργάζεται τις ίδιες πληροφορίες σε όλους τους κόμβους, διασφαλίζει την αποκέντρωση και την ασφάλεια του. Παρόλα αυτά, με το Blockchain Sharding, το δίκτυο θα χωριστεί σε τμήματα με το καθένα να επεξεργάζεται τα δικά του δεδομένα, κάνοντας την ανάπτυξη ενός κόμβου αρκετά πιο εύκολη. Το αποτέλεσμα που θα προκύψει από αυτό, είναι πως για κάποιον κακόβουλο χρήστη θα είναι αρκετά πιο εύκολο να οργανώσει μια επίθεση κατά του δικτύου, αφού θα χρειαστεί να πάρει τον έλεγχο μόνο από ένα Shard. Σε περίπτωση που συμβεί αυτό, ο κακόβουλος χρήστης θα μπορεί να διαδώσει κακόβουλες συναλλαγές, και ολόκληρο το δίκτυο μπορεί να κινδυνέψει. Για να συμβεί κάτι παρόμοιο όμως στο δίκτυο του Bitcoin, θα πρέπει κάποιος κακόβουλος χρήστης να πάρει τον έλεγχο από το 51% του δικτύου, κάτι που φαντάζει αρκετά πιο δύσκολο έως και ακατόρθωτο με τα τωρινά δεδομένα. Τελικά, ενώ το δίκτυο βελτιώνεται με την χρήση του Blockchain Sharding, η ασφάλεια, που αποτελούσε ένας από τους πρωταρχικούς στόχους του Satoshi Nakamoto, ελαχιστοποιείται.

- Απώλεια αποκέντρωσης

Ο διαμοιρασμός του δικτύου επιπλέον, μπορεί να οδηγήσει στην απώλεια της αποκέντρωσης, και να δημιουργήσει το πρόβλημα του ενός σημείου αστοχίας σε αυτό. Είναι ευκολότερο να τεθεί σε κίνδυνο ένα μικρότερο αυτόνομο τμήμα ενός δικτύου, αντί για ένα μεγαλύτερο πιο αποκεντρωμένο. Έτσι, κατά κάποιο ακυρώνεται ο σκοπός του.

- Πολυπλοκότητα εφαρμογών

Το Blockchain Sharding, όπως αναφέρθηκε, είναι μια τεχνολογία αρκετά νέα και δεν έχει χρησιμοποιηθεί σχεδόν καθόλου. Έτσι, για αρχή τουλάχιστον, θα είναι αρκετά περίπλοκη στην χρήση της, προσθέτοντας δυσκολίες στους χρήστες της. Ταυτόχρονα, θα κάνει την βάση δεδομένων και τις εφαρμογές της πιο πολύπλοκες.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Όπως φαίνεται, το Bitcoin ήρθε για να αλλάξει τα δεδομένα. Αποτελεί μια επανάσταση σύμφωνα με τους υποστηρικτές του, καθώς δικαίως έχει χαρακτηριστεί ως η μεγαλύτερη καινοτομία του χρηματοοικονομικού συστήματος τις τελευταίες δεκαετίες. Στα πρώτα χρόνια ίδρυσης του, δεν είχε αποκτήσει την αναγνώριση που του αναλογούσε, πλέον όμως, εκατομμύρια κόσμος μιλάει για αυτό, ενώ ταυτόχρονα αρκετές επιχειρήσεις ανά τον κόσμο το χρησιμοποιούν σαν επενδυτικό μέσο αλλά και ως μέσο συναλλαγών. Η κεφαλαιοποίηση του, βρίσκεται ακόμα σε πρώιμο στάδιο σε σχέση με άλλα εδραιωμένα χρηματοπιστωτικά ιδρύματα, με αποτέλεσμα η αξία του να μεταβάλλεται με απότομους ρυθμούς. Αυτό, αποθαρρύνει αρκετούς επενδυτές να ασχοληθούν με το Bitcoin, κάνοντας τους να το αντιμετωπίζουν σαν μια επενδυτική «φούσκα». Παρά τα μειονεκτήματα τους όμως, το Bitcoin έχει σίγουρα να προσφέρει αρκετά, καθώς παρομοιάζεται σαν ένας ζωντανός οργανισμός, αυτόνομος από κάθε οντότητα, που προσαρμόζεται κρατώντας όμως τους βασικούς κανόνες λειτουργίας του ανέγγιχτούς. Λειτουργεί με σεβασμό στα προσωπικά δεδομένα των χρηστών του, και εξασφαλίζει την εμπιστοσύνη μεταξύ τους, με την ασφάλεια που τους παρέχει. Αντίθετα, αντιμετωπίζει προβλήματα επεκτασιμότητας τα οποία αρκετοί υποστηριχτές του προσπαθούν να λύσουν, όμως μέχρι στιγμής δεν έχει καθιερωθεί κάποια επίσημη και ευρέος αποδεκτή λύση. Σε όλες τις περιπτώσεις που αναλύθηκαν, πάντα αναγκαστικά θυσιάζεται η ασφάλεια ή η αποκέντρωση για να επιτευχθεί η επιθυμητή ταχύτητα και να εξυπηρετήσει αξιοπρεπώς τους χρήστες του. Αυτό έρχεται σε αντίθεση με την ιδεολογία του δημιουργού του Bitcoin, τον Satoshi Nakamoto, που πρωταρχικός του στόχος ήταν ένα αυτόνομο και ασφαλές επενδυτικό μέσο σε αντίθεση με τα ήδη υπάρχοντα. Έτσι, τουλάχιστον μέχρι σήμερα, δεν έχει βρεθεί κάποια τρομερά αξιόπιστη λύση που θα μπορούσε να μετατρέψει το δίκτυο του Bitcoin ως ένα παγκόσμιο δίκτυο συναλλαγών με σκοπό να ανταγωνιστεί άλλα κορυφαία όπως η Visa ή η PayPal .

Στην παρούσα διπλωματική, αναλύθηκε η τεχνολογία του Bitcoin. Αρχικά, αναφέρθηκε η ιστορία του, ο τρόπος λειτουργίας του, καθώς και η διαδικασία παραγωγής του. Επιπρόσθετα, αναφέρθηκε ίσως και η μεγαλύτερη αδυναμία του, η επεκτασιμότητα του, και παρατέθηκαν τρόποι αντιμετώπισής της. Σκοπός της διπλωματικής, ήταν να φανεί χρήσιμη και να προσφέρει μερικές γνώσεις σε όσους επιθυμούν να μελετήσουν και να κατανοήσουν λίγο καλύτερα την τεχνολογία του Bitcoin. Το ερώτημα που γεννιέται, είναι αν το Bitcoin θα μπορέσει στο μέλλον να

υιοθετηθεί παγκόσμιος ως ένα μέσο συναλλαγών ή αν θα καθιερωθεί μόνο σαν ένα μέσο διαφύλαξης αξίας όπως για παράδειγμα ο χρυσός και άλλα συναφή . Το μόνο σίγουρο είναι πως η τεχνολογία αλλάζει με ραγδαίους ρυθμούς, και οι ακόλουθοι του θα προσπαθήσουν να αντιμετωπίσουν τους περιορισμούς του, χωρίς ωστόσο να είναι σίγουρο πως κάτι τέτοιο θα επιτευχθεί. Τα επόμενα χρόνια θα είναι κομβικά για την ιστορια του αλλά και για την ιστορία όλου του κλάδου των κρυπτονομισμάτων, αφού ακόμα δεν τους έχει δοθεί αρκετός χρόνος για να αποδείξουν αν τελικά αξίζουν.

ΒΙΒΛΙΟΓΡΑΦΙΑ

ΕΛΛΗΝΙΚΗ

Αντωνόπουλος, Α. (2017) «*Mastering Bitcoin*», O' Reilly Media, Inc, USA

Φίλιππας, Ν & Ρούκης, Μ. (2016). «*Το κρυπτονόμισμα Bitcoin θα είναι το νόμισμα της νέας ψηφιακής εποχής*».

Μαυρέλη, Κ. (2015). «*Το ψηφιακό Νόμισμα Bitcoin*».

Basecoin, (2019). «*Bitcoin και οι διαφορές του με τα παραδοσιακά νομίσματα*»

Greepto, (2021). «*Τι είναι το Bitcoin Halving*»

Greepto, (2021). «*Τι είναι το Lighting Network*»

Πλασσάρας Ν. (2013*) «Regulating digital currencies: bringing Bitcoin within the reach of IMF».*

ΞENH

DeMartino, Ian. (2016) The Bitcoin Guidebook: "*How to obtain, invest and spend the world's first decentralized cryptocurrency"*, USA: SKYHORSE PUBLISHING.

Nakamoto, S. (2008) "*Bitcoin is a peer -to- peer electronic cash system"*, Online Available: https://bitcoin.org/bitcoin.pdf

Narayanan A., Bonneau J., Felten W., Miller A, Goldfeder S. (2016*) "Bitcoin and Cryptocurrency Technologies*, Princeton University Press".

Tapscott D., Tapscott A. (2018) Blockchain Revolution: "*How the technology behind Bitcoin and cryptocurrency is changing the world"*.

Binance Academy, (2022) "*What Is the Blockchain Trilemma*?"

Binance Academy, (2021) "*How to Mine Bitcoin*"

Frankenfield J. (2023) "*Lighting Network: What Is It and How It Works".*

Adaeze U. (2023) "*5 Risks and Issues with The Bitcoin Lighting Network*".

Kohler C. (2023) "*Can You Lose Funds Using the Lighting Network*?"

Henslee J., Resnick Z. (2022) "*Why the Lighting Network Doesn't Work*"

Kohler C. (2023) "*Why Lighting Payments May Fail*"

Wikipedia (2023) "*Lighting Network*"

Poon J., Dryja T. (2016) *The Bitcoin Lighting Network: Scalable Off-Chain Instant Payments."*

Oluwademilade A. (2022) "*All You Need to Know About Sidechains*"

Gwaro E. (2023) "*What Is the Bitcoin Liquid Sidechain and How Does It Works*"

Bitcoin Magazine, (2022) "*What is the Bitcoin Block Size Limit*"

Awosika E., (2022) "*A Beginner's Guide to The Liquid Network*"

Rokytska Y., (2023) "*Blockchain sharding. Is it a risky way to scale the network*?"

Benson J., (2020) "*What Makes the Bitcoin Blockchain Secure*?"

Kubat M. (2015) "*Virtual currency Bitcoin in the scope of money definition and store of value".*

Vasek M., Thornton M., Moore T. (2014) *"Empirical analysis of denial-of-service attacks in the Bitcoin ecosystem. In international conference on financial cryptography and data security".*

Chean E., Fry J. (2015). *"Speculative bubbles in bitcoin markets? An empirical investigation into the fundamental value of Bitcoin".*

Yui M. Hyuga T. (2014) *"Japan says Bitcoin is not currency amid calls for regulations".*

Niepelt D. (2016) *"Bitcoin may have implications for money policy"*.

CoinDesk, (2016) "*How do Bitcoin Transactions Work*"

Wikipedia, (2017) "Money"

ΔΙΑΔΙΚΤΥΟ

https://scholar.google.com/

https://cryptohellenicbloc.com/

https://www.investing.com/

https://www.capital.gr/

https://bitcoin.org/el/

https://river.com/

https://www.bankofgreece.gr/

https://medium.com/

https://greepto.gr/

https://hackernoon.com/

https://decrypt.co/

https://www.ccn.com/

https://bitcoinmagazine.com/