ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ

ΤΜΗΜΑ ΛΟΓΙΣΤΙΚΗΣ ΚΑΙ ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΗΣ
ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΠΡΟΓΡΑΜΜΑΤΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΣΧΟΛΗ ΕΠΙΣΤΗΜΩΝ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΤΜΗΜΑ ΛΟΓΙΣΤΙΚΗΣ ΚΑΙ ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΗΣ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΣΤΗΝ ΛΟΓΙΣΤΙΚΗ ΦΟΡΟΛΟΓΙΑ ΚΑΙ ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΗ ΔΙΟΙΚΗΣΗ

Διπλωματική εργασία

# BITCOIN BLOCKCHAIN AND ECONOMICS

του

ΡΑΠΤΗ ΧΡΗΣΤΟΥ

Επιβλέποντας καθηγητής: Ζαπράνης Αχιλλέας

Υποβλήθηκε ως απαιτούμενο για την απόκτηση του μεταπτυχιακού διπλώματος στην Λογιστική Φορολογία και Χρηματοοικονομική Διοίκηση

Θεσσαλονίκη Σεπτέμβριος 2023

# ΠΕΡΙΛΗΨΗ

Ανάλογα με την επιλεγμένη προοπτική, το Bitcoin και τα άλλα κρυπτονομίσματα αποτελούν είτε μια μοναδική ευκαιρία για τον τερματισμό της εθνικής υποστήριξης που βασίζεται στο χρέος (νόμισμα) είτε μια απειλή για μια καλά εδραιωμένη οικονομική τάξη που διασφαλίζει την οικονομική σταθερότητα. Ένα κεντρικό ζήτημα στην έντονη συζήτηση γύρω από τα κρυπτονομίσματα είναι εάν έχουν κάποια εγγενή αξία. Στα πρώτα κεφάλαια της παρούσας διπλωματικής παρουσιάζεται μία σύντομη ανάλυση της τεχνολογίας Blockchain, στην οποία βασίζεται το Bitcoin. Στο τρίτο κεφάλαιο επεξηγείται η εννοιολογική σημασία του Bitcoin και ο τρόπος λειτουργείας του. Στο τέταρτο κεφάλαιο αναφέρεται το άθροισμα όλων των ιδιοτήτων που θα μπορούσαν να χαρακτηρίσουν το Bitcoin ως χρήμα, συσχετίζοντάς το με άλλα περιουσιακά στοιχεία και εξετάζεται η εγγενής αξία μέσω της βιωσιμότητας της κατανάλωσης ενέργειας που απαιτείται για την δημιουργία του. Στο τελευταίο κεφάλαιο παρουσιάζεται το νομικό πλαίσιο του Bitcoin και ποιες χώρες στρέφονται σε αυτό και την σημασία του, όταν επικρατούν φαινόμενα όπως ο πληθωρισμός στην οικονομία. Τέλος, συζητιέται αν το Bitcoin μπορεί να αντικαταστήσει τις παρούσες τράπεζες και αν η τεχνολογία του αποτελεί μία ακόμα φούσκα ή αν θα αποτελέσει ένα κομμάτι του χρηματοπιστωτικού τομέα.

# ABSTRACT

Depending on the perspective chosen, cryptocurrencies are either a unique opportunity to end debt-based national support (currency) or a threat to a well-established economic order that ensures economic stability. A central issue in the heated debate surrounding cryptocurrencies is whether they have any intrinsic value. In the first chapters of this thesis, a brief analysis of the Blockchain technology, on which Bitcoin is based, is presented. The third chapter explains the conceptual meaning of Bitcoin and how it works. The fourth chapter states the sum of all the properties that could qualify Bitcoin as money, relating it to other assets and examines its intrinsic value through the sustainability of the energy consumption required to create it. The last chapter presents the legal framework of Bitcoin and which countries turn to it and its importance when phenomena such as inflation prevail in the economy. Finally, it is discussed whether Bitcoin can replace the current banks and whether its technology is another bubble or whether it will become a part of the financial sector.

# ΑΦΙΕΡΩΣΕΙΣ

Αφιερώνεται στην οικογένεια μου που με υποστήριξε από τα πρώτα μαθητικά βήματα και σε όλους τους τομείς είχα την απόλυτη στήριξη τους.

# ΕΥΧΑΡΙΣΤΙΕΣ

Με την εκπόνηση της παρούσας μου εργασίας ολοκληρώνονται με επιτυχία οι μεταπτυχιακές μου σπουδές στο μοναδικό Πανεπιστήμιο Μακεδονίας, στο οποίο ήταν τιμή μου να σπουδάσω δίπλα σε τόσο αξιόλογους και εξαιρετικούς καθηγητές.

Στο σημείο αυτό, θα ήθελα να ευχαριστήσω ιδιαιτέρως τον επιβλέποντα καθηγητή κο Ζαπράνη Αχιλλέα. Με τις εξαιρετικές γνώσεις επάνω στο αντικείμενο του Χρηματοοικονομική και Νευρωνικά Συστήματα και την δική μου ενασχόληση επιλέχθηκε αυτό το θέμα. Τον ευχαριστώ ιδιαιτέρως με την επιλογή του να συνεργαστούμε και την συνεργασία που παρείχε σε όλη την διάρκεια για την ορθή επίτευξη της διπλωματικής μου εργασίας.

# ΠΡΟΛΟΓΟΣ

Όλο και μεγαλύτερη είναι η ανάγκη για την εύρεση καινοτόμων ιδεών στον χώρο της κρυπτογραφίας, λόγω της ραγδαίας εξέλιξης της κοινωνίας και της τεχνολογίας. Το χρηματοοικονομικό σύστημα και τον τομέα των οικονομικών συναλλαγών έρχεται να συναντήσει μια από τις πιο επαναστατικές ιδέες στον χώρο αυτόν.

Η ψηφιακή οικονομία του σήμερα βασίζεται σε μία τρίτη αξιόπιστη πηγή που διασφαλίζει την ασφάλεια των ψηφιακών αρχείων και την ιδιωτικότητα. Σχεδόν όλες οι ηλεκτρονικές συναλλαγές ελέγχονται, όπως για παράδειγμα μία αρχή που πιστοποιεί ότι ένα ψηφιακό πιστοποιητικό είναι αυθεντικό. Οι δεσμοί αυτοί εξάρτησης καταρρίπτονται με την εφεύρεση ενός νέου ψηφιακού τρόπου οργάνωσης αρχείων.

Το 2008 ο Satoshi Nakamoto δημιούργησε ένα νέο ψηφιακό νόμισμα το οποίο ονομάζεται Bitcoin. Το Bitcoin είναι ένα peer to peer (P2P) σύστημα πληρωμών και ένα σύστημα ανοιχτού κώδικα, για την διαχείριση του οποίου χρησιμοποιούνται μέθοδοι κρυπτογραφίας. Είναι με άλλα λόγια το πρώτο ψηφιακό νόμισμα το οποίο δεν υπάρχει σε φυσική μορφή χρημάτων. Τα παραπάνω προσδίδουν στο Bitcoin ένα μεγάλο πλεονέκτημα, ότι για την ανταλλαγή του δεν είναι αναγκαία η χρήση κάποιου διαμεσολαβητή. Επιπλέον, δεν ελέγχεται από καμία κυβέρνηση ή υπηρεσία λόγω των κρυπτογραφικών αρχών που ακολουθεί. Το δίκτυο των ανθρώπων που το χρησιμοποιούν καθορίζουν την παραγωγή του.

Οι συναλλαγές του Bitcoin καταγράφονται και παρακολουθούνται από ένα «λογιστικό βιβλίο» που ονομάζεται Blockchain. Για να διασφαλιστεί ότι όλες οι συναλλαγές είναι νόμιμες και έχουν καταγραφεί σωστά, πολλαπλά αντίγραφα αυτού του «βιβλίου» υπάρχουν και συγκρίνονται μεταξύ τους.

Αν και τα κρυπτονομίσματα είναι ένα αντικείμενο που παρουσιάζει μεγάλες προοπτικές εξέλιξης, η τεχνολογία στην οποία στηρίζονται έχει μετατραπεί σε ένα από τα πιο πολυσυζητημένα τεχνολογικά επιτεύγματα, με τεράστιες επενδύσεις και μία ολόκληρη βιομηχανία να χτίζεται πάνω της. Οι δυνατότητες και οι χρήσεις της συγκεκριμένης τεχνολογίας εισέρχονται εκτός από την αγορά του και σε πολλούς άλλους τομείς.

Το Blockchain είναι μια καινοτομία της οποίας οι κατασκευαστικές ιδιότητες προσφέρουν όλο και περισσότερες ουσιαστικές βάσεις στον ψηφιακό κόσμο, όπου οδηγούν στον καθορισμό υψηλότερων επιπέδων ανάθεσης και αυτονομίας. Το ενδιαφέρον του

ιδιωτικού τομέα και των κυβερνητικών αρχών έχει προκαλέσει ο ασφαλής και αμετάβλητος χαρακτήρας του.

Η τεχνολογία του πυροδότησε τόσο μεγάλο πάθος άλλα και τόσο μεγάλη διαμάχη μεταξύ ειδικών από την εμφάνιση του Διαδικτύου. Αδιαμφισβήτητα, η εξερεύνηση του Blockchain είναι μια από τις προκλήσεις που έχουν να αντιμετωπίσουν οι επιστήμονες και είναι ικανή να αλλάξει ολοκληρωτικά τα δεδομένα που μέχρι τώρα γνωρίζαμε ειδικά στον χρηματοοικονομικό τομέα.

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΛΗΨΗ ..... 2
ABSTRACT ..... 3
ΑΦΙΕΡΩΣΕΙΣ ..... 4
ΕΥΧΑΡΙΣΤΙΕΣ ..... 5
ΠΡΟΛΟΓΟΣ ..... 6
ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ ..... 11
ΚΕΦΑΛΑΙΟ 1 ..... 12
ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΤΕΧΝΟΛΟΓΙΑ BLOCKCHAIN ..... 12
ΚΕΦΑΛΑΙΟ 2 ..... 13
ΤΕΧΝΟΛΟΓΙΑ BLOCKCHAIN ..... 13
2.1 Βασικές Έννοιες Στην Κρυπτογραφία ..... 13
2.1.1 Συμμετρική Κρυπτογραφία ..... 13
2.1.2 Κρυπτογράφηση Δημόσιου Κλειδιού ..... 14
2.1.3 Αυθεντικοποίηση Μηνύματος ..... 16
2.1.3.1 Συναρτήσεις Κατακερματισμού ..... 17
2.1.3.2 Μέθοδος Merkle Trees ..... 19
2.1.3.3 Ψηφιακές Υπογραφές ..... 22
2.2 Αρχιτεκτονική Του Μηχανισμού Blockchain ..... 26
2.2.1 Η Δομή Του Block ..... 26
2.2.2 Η Σύνδεση Των Μπλοκ Μεταξύ Τους ..... 27
2.2.3 Δίκτυο Ομότιμων Κόμβων ..... 28
2.2.3.1 Μη Δομημένα Δίκτυα Ομότιμων Κόμβων ..... 30
2.2.3.2 Δομημένα Δίκτυα Ομότιμων Κόμβων ..... 31
2.2.3.3 Υβριδικά Μοντέλα Δικτύων ..... 31
2.2.3.4 Πλεονεκτήματα Δικτύου Ομότιμων Κόμβων Στην Τεχνολογία Blockchain ..... 32
2.2.4 Εξόρυξη Μπλοκ (Mining) ..... 32
2.2.5 Genesis Μπλοκ ..... 34
2.2.6 Πρωτόκολλα Συναίνεσης ..... 35
2.2.6.1 Proof of Work (PoW) ..... 35
ΚΕΦΑΛΑΙΟ 3 ..... 37
Η ΠΕΡΙΠΤΩΣΗ ΤΟΥ BITCOIN ..... 37
3.1 Ιστορική Αναδρομή Του Bitcoin ..... 37

3.2 Τι Είναι Το Bitcoin ..... 38
3.3 Τα Πλεονεκτήματα του Bitcoin ..... 39
3.4 Τα Μειονεκτήματα Του Bitcoin ..... 40
3.5 Πως Λειτουργεί Το Bitcoin ..... 42
3.6 Πως Πραγματοποιούνται Οι Συναλλαγές ..... 43
3.7 Επαλήθευση Των Συναλλαγών ..... 44
3.7.1 Κρυπτογραφικά Hash ..... 45
3.7.2 Nonces ..... 45
3.8 Το Bitcoin Σε Τεχνικό Επίπεδο ..... 46
3.8.1 Πως Δημιουργούνται Τα Bitcoins ..... 47
3.8.2 Τρόπος εξόρυξης (Mining) ..... 47
3.8.3 Από Τι Εξαρτάται Η Δημιουργία τους ..... 48
ΚΕΦΑΛΑΙΟ 4 ..... 49
ΕΓΓΕΝΗΣ ΑΞΙΑ BITCOIN ..... 49
4.1 Η Αξία Του Bitcoin ..... 49
4.2 Οι Προκλήσεις Της Αποτίμησης Του Bitcoin ..... 51
4.2.1 Αριθμητική Αποτίμηση Του Bitcoin ..... 52
4.3 Αξιολόγηση Βάση Των Κυβερνητικών Νομισμάτων ..... 53
4.3.1 Κυβερνητικά νομίσματα ..... 53
4.3.2 Μέσο Αποθήκευσης Αξίας ..... 54
4.3.3 Υποστηρίζει Τα Χαρακτηριστικά Του Χρήματος ..... 56
4.3.4 Το Bitcoin Ως Νόμισμα: Ποσοτική Θεωρία Του Χρήματος ..... 58
4.4 Αξιολόγηση Βάση Των Εμπορευμάτων ..... 59
4.5 Εγγενής Αξία Ως Μέσο Αποθήκευσης Ενέργειας Και Επένδυση Κεφαλαίου ..... 61
4.6 Mining Και Εγγενής Αξία ..... 63
4.7 Hash Rate Και Τιμή Bitcoin ..... 66
4.8 Βιωσιμότητα Και Κατανάλωση Ενέργειας Του Bitcoin ..... 66
4.9 Συμπέρασμα ..... 74
ΚΕΦΑΛΑΙΟ 5 ..... 75
ΥΦΙΣΤΑΜΕΝΗ ΚΑΤΑΣΤΑΣΗ ΚΑΙ ΣΥΜΠΕΡΑΣΜΑΤΑ ..... 75
5.1 Νομικό Πλαίσιο Του Bitcoin ..... 75
5.2 Χώρες Όπου Το Bitcoin Είναι Νόμιμο Και Παράνομο ..... 76
5.2.1 Χώρες Όπου Το Bitcoin Είναι Νόμιμο ..... 76
5.2.2 Χώρες Όπου Το Bitcoin Είναι Παράνομο ..... 79

5.2.3 Συμπέρασμα....80
5.3 Χώρες Με Υψηλό Πληθωρισμό Και Το Bitcoin....81
5.3.1 Τι Προκαλεί Τον Πληθωρισμό....81
5.3.2 Πως βοηθάει το Bitcoin....83
5.3.3 Παραδείγματα χωρών που στρέφονται στο Bitcoin....83
5.3.4 Συμπέρασμα....84
5.4 Μπορεί το Bitcoin Να Αντικαταστήσει Τις Κεντρικές Τράπεζες;....84
5.4.1 Τα Πλεονεκτήματα του Bitcoin Έναντι Των Τραπεζών....85
5.4.2 Τα Μειονεκτήματα του Bitcoin Έναντι Των Τραπεζών....86
5.4.3 Συμπέρασμα....87
5.5 Η Σημασία Των CBDCs....87
5.6 Υπάρχει Φούσκα Στο Bitcoin;....88
5.6.1 Γιατί Μία Φούσκα Δεν Είναι Τόσο Κακή....89
5.7 Ναι Στην Τεχνολογία Blockchain Και Στο Bitcoin;....90
5.8 Γενικό Συμπέρασμα....90
ΒΙΒΛΙΟΓΡΑΦΙΑ....93

# ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

Εικόνα 1-Απεικόνιση Συμμετρικής Κρυπτογραφίας. ..... 14
Εικόνα 2-Κρυπτογράφηση Δημόσιου κλειδιού ..... 16
Εικόνα 3-Αναπαράσταση είσοδού τριών μηνυμάτων-κλειδιών τυχαίου μεγέθους. ..... 19
Εικόνα 4-Αναπαράσταση ενός Merkle Tree με κόμβους-φύλλα ..... 21
Εικόνα 5-Η δομή ενός Merkle Tree στο μπλοκ της αλυσίδας Blockchain. ..... 22
Εικόνα 6-Διάγραμμα μηχανισμού της ψηφιακής υπογραφής. ..... 25
Εικόνα 7-Παράδειγμα μιας αλυσίδας Blockchain με τα μπλοκ να συνδέονται μεταξύ τους με χρονολογική σειρά. ..... 26
Εικόνα 8-Εσωτερική δομή του μπλοκ. ..... 27
Εικόνα 9-Αναπαράσταση μοντέλου πελάτη-εξυπηρετητή και ομότιμων κόμβων. ..... 30
Εικόνα 10-Η διαδικασία εξόρυξης ενός μπλοκ. ..... 34
Εικόνα 11-Το φαινόμενο Fork. ..... 34
Εικόνα 12-Γραφική απεικόνιση της λειτουργείας μιας συναλλαγής με Bitcoin. ..... 43
Εικόνα 13-Κρυπτογραφικά Hash για μετατροπή δεδομένων σε αριθμητικές λέξεις. ..... 45
Εικόνα 14-Χαρακτηριστικά του χρήματος. ..... 50
Εικόνα 15-Τιμή Bitcoin vs Αστάθεια ανά χρόνο. ..... 56
Εικόνα 16-Hash rate vs Price. ..... 66
Εικόνα 17-Κατάταξη κατανάλωσης ενέργειας. ..... 67
Εικόνα 18-Συνολική παγκόσμια παραγωγή από ανανεώσιμες πηγές ενέργειας. ..... 67
Εικόνα 19-Συνολική κατανάλωση ενέργειας από μη ενεργές συσκευές στην Αμερική. ..... 68
Εικόνα 20-Σύγκριση κατανάλωσης ενέργειας του Bitcoin και βραστήρων νερού στην Ευρωπαϊκή Ένωση. ..... 69
Εικόνα 21-Ανανεώσιμες πηγές ως μέρος του ενεργειακού μίγματος. ..... 70
Εικόνα 22-Πηγές ενέργειας των εγκαταστάσεων κατακερματισμού. ..... 70
Εικόνα 23-Πηγές ενέργειας ανά Ήπειρο. ..... 71
Εικόνα 24-NREL Duck Curve. ..... 73
Εικόνα 25-Χώρες με υπερπληθωρισμό. ..... 82

# ΚΕΦΑΛΑΙΟ 1

# ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΤΕΧΝΟΛΟΓΙΑ BLOCKCHAIN

Στην τεχνολογία του Bitcoin καταγράφονται τα δεδομένα και οι συναλλαγές που έχουν πραγματοποιηθεί μεταξύ τους μέσω ενός αποκεντρωμένου δικτύου ομότιμων κόμβων (P2P). Τα δεδομένα στο δίκτυο αποθηκεύονται σε πακέτα ( Block ), τα οποία συνδέονται μεταξύ τους δημιουργώντας μια αλυσίδα, από την οποία προέρχεται και το όνομα της τεχνολογίας Blockchain.

Το δίκτυο του Blockchain είναι διανεμημένο ισότιμα. Έτσι υπάρχει απουσία προτεραιότητας και κανένα πρόσωπο μέσα στο δίκτυο δεν υπερέχει έναντι άλλου. Όλοι οι χρήστες που συμμετέχουν στο δίκτυο, κρατάνε ο καθένας ένα αντίγραφο του αρχείου καταχωρήσεων και έχουν πρόσβαση σε αυτό, κάτι που εξασφαλίζει την διαφάνεια των συναλλαγών και την ασφάλεια[10]. Το Σύνταγμα κανόνων που ονομάζεται πρωτόκολλο συναίνεσης και ρυθμίζεται από τους συμμετέχοντες ελέγχει καθορίζει την διαδικασία της δημιουργίας και διαφύλαξης του αρχείου. Η απόδειξη τιμιότητας και εμπιστοσύνης μεταξύ των δύο τελευταίων δεν είναι αναγκαία για την σύνταξη ενός συμπαγούς πρωτοκόλλου[13].

Κάθε συναλλαγή προτού καταχωρηθεί στην αλυσίδα, ελέγχεται από τα πρόσωπα του δικτύου με βάση τους κανόνες που έχουν συμφωνηθεί. Όταν εξακριβωθεί και επαληθευτεί, τοποθετείται σύμφωνα με τον χρόνο κατά τον οποίο έχει πραγματοποιηθεί.

Σε ένα μεγάλο αριθμό χρηστών μοιράζεται το αρχείο που δημιουργείται, που είναι κρυπτογραφημένο και δεν επιτρέπει την αλλαγή στις εγγραφές που έχουν ήδη περαστεί σε αυτό. Έτσι, δίνεται η δυνατότητα να μην μπορεί να χειραγωγηθεί εύκολα λόγω της απουσίας του κεντρικού διαχειριστή, αυξάνοντας την αξιοπιστία του συστήματος[7]. Έτσι δεν χρειάζεται να βασίζεται σε μία εξωτερική αρχή για την επικύρωση της ακεραιότητας και της αυθεντικότητας των δεδομένων, λειτουργώντας ως ένα αμετάβλητο αρχείων συναλλαγών. Στη συστοιχία μπορεί να αποθηκευτεί οποιαδήποτε πληροφορία, γεγονός το οποίο συμβάλει στην εκτεταμένη χρήση του[8].

Το Blockchain χαρακτηρίζεται ως μία κατανεμημένη, κρυπτογραφημένη βάση δεδομένων στο οποίο επαληθεύονται και αποθηκεύονται πληροφορίες σημαντικές οι οποίες αντιστοιχούν σε συστοιχία και μετατρέπονται σε μία αλυσίδα στην οποία ο κάθε κόμβος (node) που συμμετέχει στο δίκτυο μπορεί να έχει πρόσβαση, ενώ δύσκολη αποτελεί η αντιστρεψιμότητα και η τροποποίηση της πληροφορίας εφόσον αυτήν έχει καταγραφεί στο μητρώο. Η πληροφορία μπορεί να αφορά κάποια πνευματική ιδιοκτησία ή περιουσιακό στοιχείο, μέχρι και ένα σύστημα νομικών εγγράφων[9]. Το 2015 η τεχνολογία Blockchain χαρακτηρίστηκε από το περιοδικό “The Economist” ως “μηχανή εμπιστοσύνης”. Οι αλυσίδες αυτές είναι εξαιρετικά ανθεκτικές λόγω των κρυπτογραφικών τεχνικών και της αποκεντρωμένης και κατανεμημένης φύσης τους.

# ΚΕΦΑΛΑΙΟ 2

# ΤΕΧΝΟΛΟΓΙΑ BLOCKCHAIN

## 2.1 Βασικές Έννοιες Στην Κρυπτογραφία

Είναι κοινός αποδεκτό ότι σε τομείς όπως είναι η ασφαλής πρόσβαση σε συστήματα και υπηρεσίες, η ανάκτηση και διαχείριση ευαίσθητων δεδομένων, οι ηλεκτρονικές συναλλαγές η κρυπτογραφία παίζει σημαντικό ρόλο. Ιδιαίτερα τα τελευταία χρόνια η ανάπτυξη των τηλεπικοινωνιών έχει καταστήσει την κρυπτογραφία αναπόσπαστο κομμάτι των τεχνολογικών εξελίξεων και αντικείμενο έντονης ερευνητικής δραστηριότητας η οποία την έχει μετατρέψει σε επιστήμη, με αυστηρούς ορισμούς και αποδείξεις.

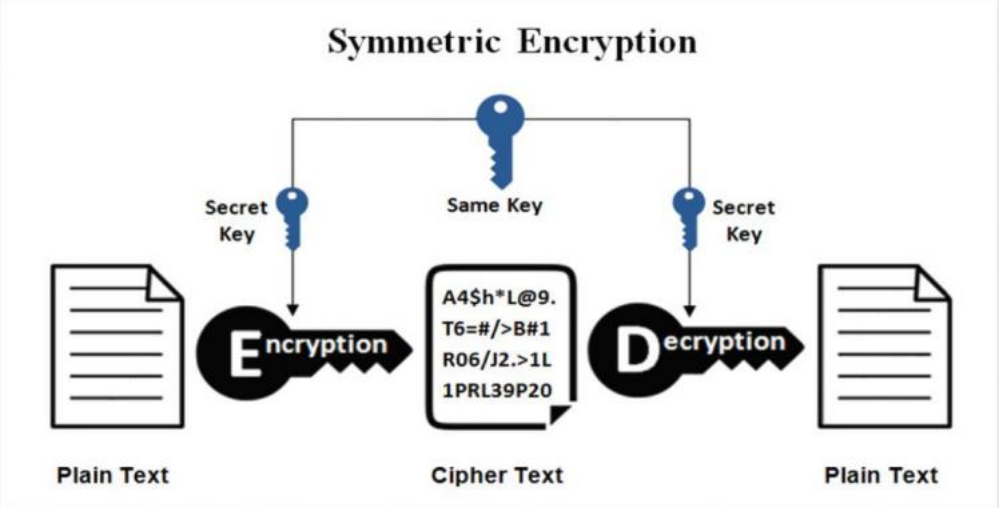
Στην τεχνολογία του Blockchain είναι πλέον γνωστός ο τρόπος που λειτουργεί και η ασφάλεια τους πηγάζει αποκλειστικά από αριθμητικούς αλγορίθμους που επιτρέπουν την εκτέλεση πράξεων, ώστε να είναι πολύ δύσκολη η υπολογιστική δυσκολία των αντίστροφων πράξεων. Η κρυπτογράφηση προσφέρει προάγει την ισότιμη συμμετοχή όλων στο πολιτικό, οικονομικό και κοινωνικό γίγνεσθαι και τελικά τον σεβασμό της ιδιωτικής ζωής.

### 2.1.1 Συμμετρική Κρυπτογραφία

Στη συμμετρική κρυπτογραφία (Symmetric Cryptography) υπάρχει ένα μοναδικού κλειδί, το οποίο χρησιμοποιείται τόσο στην αποκρυπτογράφηση ενός μηνύματος όσο και στην κρυπτογράφηση του. Το κλειδί αυτό πρέπει να είναι γνωστό μόνο στα συναλλασσόμενα μέρη[15].

Πριν εμφανιστεί η κρυπτογράφηση του δημοσίου κλειδιού το 1970, το συμβατικό είδος κρυπτογράφησης αποτελούσε το μοναδικό είδος κρυπτογράφησης. Παραμένει μέχρι και σήμερα το πιο ευρέως διαδεδομένο είδος κρυπτογράφησης με πολλές εφαρμογές, όπως την κρυπτογράφηση του σκληρού δίσκου και την εξασφάλιση ασφαλούς σύνδεσης σε HTTPS ιστοσελίδες. Κάνοντάς χρήση ενός μυστικού κλειδιού και ενός αλγορίθμου κρυπτογράφησης E(K,X), μετατρέπει το αρχικό μήνυμα (plaintext) σε κρυπτογραφημένο (ciphertext). Το κρυπτοκείμενο μπορεί να συμβάλει στην ανάκτηση του αρχικού μηνύματος χρησιμοποιώντας το ίδιο κλειδί και έναν αλγόριθμο αποκρυπτογράφησης D(K,Y). Σημαντικοί συμμετρικοί αλγόριθμοι κρυπτογράφησης είναι ο AES, ο 3DES, ο DES[15].

*Εικόνα 1-Απεικόνιση Συμμετρικής Κρυπτογραφίας. Η κρυπτογράφηση και η αποκρυπτογράφηση πραγματοποιούνται με χρήση του ίδιου κλειδιού.*




## 2.1.2 Κρυπτογράφηση Δημόσιου Κλειδιού

Η κρυπτογραφία του δημόσιου κλειδιού (Public key Cryptography) αποτελεί αν όχι την μεγαλύτερη, μία από τις μεγαλύτερες επαναστάσεις στην ιστορία της κρυπτογραφίας.

Αποτελεί μία ευκαιρία για την αλλαγή της ως τώρα φιλοσοφίας των συστημάτων της κρυπτογραφίας. Στηρίζεται κυρίως σε μαθηματικές συναρτήσεις σε αντίθεση με την συμμετρική κρυπτογραφία η οποία εντάσσει τις μεθόδους αντικατάστασης και αντιμετάθεσης. Η κατηγορία αυτή είναι ασύμμετρη και περιέχει την χρήση δύο ξεχωριστών κλειδιών για την κρυπτογράφηση και αποκρυπτογράφηση. Η πρώτη πραγματοποιείται με ένα δημόσιο κλειδί, ενώ η δεύτερη με ένα ιδιωτικό. Τα δύο κλειδιά αυτά έχουν επίδραση σε τομείς όπως η διανομή κλειδιού, η αυθεντικοποίηση και την εμπιστευτικότητα[15].

Η συμμετρική κρυπτογράφηση έφερε δύο δύσκολά προβλήματα, τα οποία αντιμετωπίστηκαν μέσω της κρυπτογράφησης του δημοσίου κλειδιού. Στην αρχή απαραίτητη είναι η διανομή του κλειδιού, που στην συμμετρική κρυπτογράφηση είτε δύο επικοινωνούντες εκ των προτέρων να μοιράζονται ένα κλειδί, το οποίο τους έχει παραχωρηθεί, είτε με τη χρήση ενός κέντρου διανομής κλειδιών. Ο Whitefield Diffie, που θεωρείται ένας από τους δημιουργούς της κρυπτογράφησης δημοσίου κλειδιού συνειδητοποίησε ότι αυτή η δεύτερη απαίτηση καταργούσε την κύρια οντότητα της κρυπτογραφίας, δηλαδή την ικανότητα να υπάρχει καθολική μυστικότητα στην επικοινωνία. Ο Diffie στη συνέχεια ασχολήθηκε με το αντικείμενο των «ψηφιακών υπογραφών». Η διάδοση της κρυπτογραφίας για εμπορικούς και ιδιωτικούς σκοπούς θα χρειάζονταν όλα τα ηλεκτρονικά μηνύματα και έγγραφα να υπάρχει κάτι ισοδύναμο των υπογραφών που απαιτούνται στα γραπτά έγγραφα. Αναδύεται το ερώτημα αν θα μπορούσε να είναι σίγουρο ένα μέλος πως το ψηφιακό μήνυμα που έλαβε ήταν από ένα άλλο συγκεκριμένο άτομο[15].

Το 1976 ο Diffie και Hellman ανακάλυψαν την κρυπτογράφηση δημόσιου κλειδιού, έναν τρόπο που έλυνε και τα δύο προβλήματα.

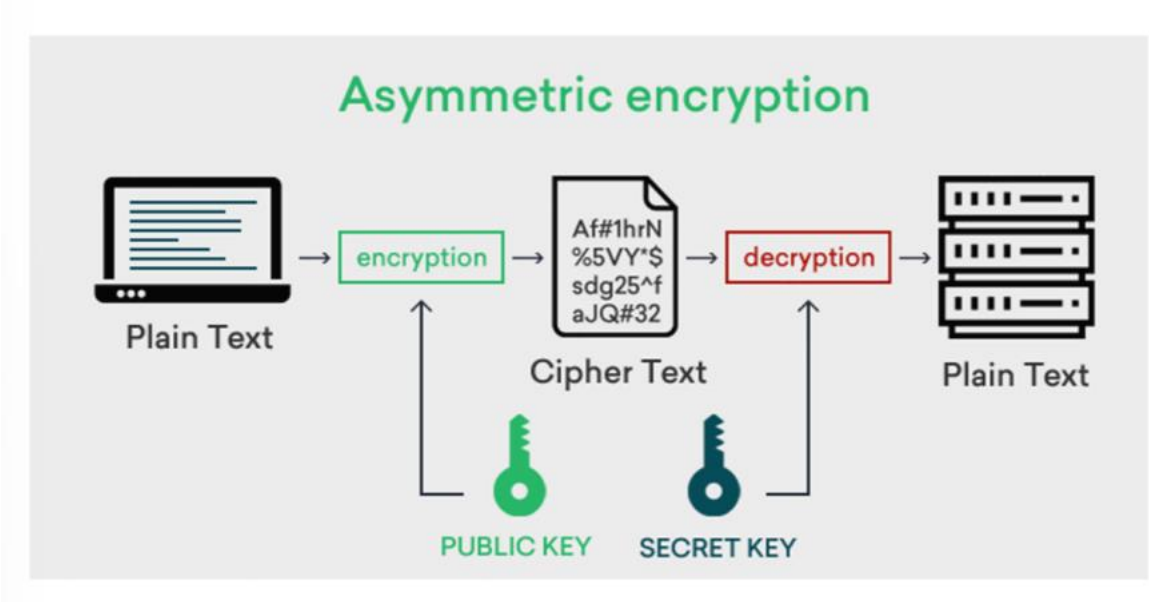
Οι ασύμμετροι αλγόριθμοι όπως αναφέρθηκε πιο πάνω χρησιμοποιούν δύο κλειδιά, ένα για την κρυπτογράφηση και ένα διαφορετικό για την αποκρυπτογράφηση που συνδέεται με το πρώτο. Γνωρίζοντας μόνο τον κρυπτογραφικό αλγόριθμο και το κλειδί κρυπτογράφησης, είναι υπολογιστικά αδύνατο να καθοριστεί κλειδί κρυπτογράφησης. Τα βήματα που χρειάζονται για την εκτέλεση του αλγορίθμου είναι:

- Κάθε χρήστης παράγει ένα ζεύγος κλειδιών που θα χρησιμοποιηθούν κατά την κρυπτογράφηση και αποκρυπτογράφηση μηνυμάτων΄
- Το ένα από τα δύο κλειδιά τοποθετείται σε ένα δημόσιο προσπελάσιμο αρχείο (δημόσιο κλειδί) και το άλλο κλειδί μένει κρυφό.

- Χρησιμοποιώντας το δημόσιο κλειδί του ενός συμμετέχοντα ο άλλος συμμετέχον μπορεί να του στείλει ένα εμπιστευτικό μήνυμα.
- Όταν λάβει το μήνυμα, το αποκρυπτογραφεί χρησιμοποιώντας το δικό του ιδιωτικό κλειδί και κανένας άλλος δεν μπορεί να αποκρυπτογραφήσει το μήνυμα γιατί μόνο ο ίδιος γνωρίζει το ιδιωτικό κλειδί.

Έτσι όλοι οι μετέχοντες γνωρίζουν τα δημόσια κλειδιά, άλλα τα ιδιωτικά κλειδιά δεν διανέμονται και παράγονται τοπικά από κάθε συμμετέχοντα. Το ιδιωτικό κλειδί του χρήστη πρέπει να παραμένει προστατευμένο και μυστικό, για να είναι ασφαλής η επικοινωνία. Για να αντικαταστήσει το ιδιωτικό κλειδί, αρκεί να δημοσιεύσει το νέο δημόσιο κλειδί και να κρατήσει μυστικό το νέο ιδιωτικό κλειδί[15].

*Εικόνα 2-Κρυπτογράφηση Δημόσιου κλειδιού. Η κρυπτογράφηση πραγματοποιείται με δημόσιο κλειδί, ενώ η αποκρυπτογράφηση με ιδιωτικό κλειδί.*




## 2.1.3 Αυθεντικοποίηση Μηνύματος

Η πιο αχαρτογράφητη περιοχή στην ασφάλεια δικτύων είναι το θέμα των ψηφιακών υπογραφών, καθώς και το συναφές θέμα της αυθεντικοποίησης του μηνύματος. Οι σχετικές επιγραφές, καθώς και τα μέτρα αντιμετώπισης αυτών είναι πολύ συγκεχυμένα. Βέβαια οι σημερινοί σχεδιαστές κρυπτογραφικών πρωτοκόλλων εργάζονται με ένα στερεό μοντέλο.

Η ακεραιότητα ενός μηνύματος επιβεβαιώνεται μέσο του μηχανισμού ή της υπηρεσίας της αυθεντικοποίηση του μηνύματος. Είναι ο μηχανισμός που πιστοποιεί ότι τα μηνύματα που

λαμβάνει προέρχονται από την πηγή που ισχυρίζεται ότι τα στέλνει ο άλλος συμμετέχον και δεν έχουν υποστεί μεταβολές. Η αυθεντικοποίηση μηνύματος μπορεί επίσης να προστατεύσει από επιθέσεις τροποποίησης μηχανισμού, αλλά και να επικυρώσει τη σωστή αλληλουχία των μηνυμάτων. Τις επιθέσεις αποποίησης προέλευσης μπορεί να αντιμετωπίσει η τεχνική αυθεντικοποίησης της ψηφιακής τεχνικής[15].

Ο Κώδικας Αυθεντικοποίησης Μηνύματος (Message Authentication Code- MAC) και η Συνάρτηση Κατακερματισμού, είναι οι δύο πιο κοινές κρυπτογραφικές τεχνικές που χρησιμοποιούνται για την αυθεντικοποίηση του μηνύματος. Ο αλγόριθμος MAC απαιτεί την χρήση ενός κρυφού κλειδιού. Παράγει έναν κώδικα αυθεντικοποίησης του μηνύματος τοποθετώντας στην είσοδο ένα μήνυμα μεταβλητού μήκους και ένα μυστικό κλειδί. Ο παραλήπτης μπορεί να πιστοποιήσει την ακεραιότητα του μηνύματος, δημιουργώντας έναν κώδικα αυθεντικοποίησης μηνύματος, έχοντας στην κατοχή του το μυστικό κλειδί. Η συνάρτηση κατακερματισμού αντιστοιχίζει ένα μεταβλητού μήκους μήνυμα σε μία σταθερού μήκους τιμή ή σύνοψη μηνύματος (Message digest). Πρέπει η ασφαλής συνάρτηση κατακερματισμού να συνδυαστεί με ένα μυστικό κλειδί για να γίνει η αυθεντικοποίηση του μηνύματος[15].

Κάθε μηχανισμός ψηφιακής υπογραφής ή αυθεντικοποίησης διαθέτει δύο λειτουργικά επίπεδα. Στο τελευταίο επίπεδο αναγκαία είναι μία συνάρτηση που δημιουργεί έναν αυθεντικοποιητή, δηλαδή μία τιμή που θα χρησιμοποιείται για την αυθεντικοποίηση του μηνύματος. Σε ένα υψηλότερο επίπεδο, αυτή η συνάρτηση χαμηλότερου επιπέδου, χρησιμοποιείται ως πρωταρχικό πρωτόκολλο αυθεντικοποίησης για να επιτρέψει σε ένα χρήστη να πιστοποιεί την αυθεντικότητα του μηνύματος. Η Συνάρτηση Κατακερματισμού (Hash Function) και ο Κώδικας Αυθεντικοποίησης Μηνύματος (MAC), είναι οι δύο σημαντικότεροι τύποι συναρτήσεων που μπορούν να χρησιμοποιηθούν για να παράγουν ένα αυθεντικοποιητή.

#### 2.1.3.1 Συναρτήσεις Κατακερματισμού

Για την σχεδίαση τεχνικών στην αυθεντικοποίηση της πληροφορίας, οι συναρτήσεις κατακερματισμού αποτελούν το κύριο εργαλείο. Χρησιμοποιούνται για την παραγωγή «ψηφιακών δακτυλικών αποτυπωμάτων» και είναι συστατικό πολλών κρυπτοσυστημάτων. Η

συνάρτηση κατακερματισμού αποδέχεται ως είσοδο ένα μήνυμα μεταβλητού μήκους και παράγει μια έξοδο σταθερού μήκους, γνωστή και ως κώδικας κατακερματισμού. Στις MAC η ύπαρξη κλειδιού είναι αναγκαία για την εφαρμογή τους ενώ στις συναρτήσεις κατακερματισμού δεν είναι. Έτσι έχει την δυνατότητα να υπολογίσει την κατακερματισμένη τιμή του μηνύματος, δεδομένου ενός μηνύματος εισόδου. Για παράδειγμα, το πρότυπο Secure Hash Standard (SHS) προσδιορίζει πέντε συναρτήσεις κατακερματισμού, τις SHA-512, SHA-384, SHA-256, SHA-224, SHA-1. Ένα μήνυμα εξόδου είναι εύκολο να δημιουργηθεί από ένα μήνυμα εισόδου και μία συνάρτηση κατακερματισμού. Οι συναρτήσεις αυτές δέχονται μαθηματικές ιδιότητες οι οποίες μπορούν να κάνουν το κείμενο δύσκολα ανιχνεύσιμο. Δηλαδή, είναι σχεδόν αδύνατον να υπολογιστεί η αρχική είσοδος, δεδομένου μιας εξόδου. Επομένως έχουν μία σημαντική ασσυμετρία. Είναι εύκολο να εκτιμηθούν, αλλά δύσκολο να αντιστραφούν[15][16][17].

Μία τιμή κατακερματισμού h αποτελείται από μία συνάρτηση H που έχει μορφή h=H(M), όπου M ένα μεταβλητού μήκους μήνυμα και H(M) η κατακερματισμένη τιμή σταθερού μήκους. Όταν το μήνυμα είναι έτοιμο προς αποστολή, ο αποστολέας προσαρτά την τιμή κατακερματισμού στο μήνυμα. Ο δείκτης υπολογίζει εκ νέου την τιμή κατακερματισμού από το μήνυμα που έλαβε, αυθεντικοποιόντας έτσι το συγκεκριμένο μήνυμα. Στην ουσία είναι μαθηματικές συναρτήσεις που παίρνουν ως είσοδο κάποιο δεδομένο τυχαίου μεγέθους και δίνουν πίσω μία αναπαράσταση σταθερού μεγέθους. Βέβαια, απαιτούνται κάποια μέτρα προστασίας τις τιμής αυτής, λόγω του ότι η συνάρτηση κατακερματισμού δε θεωρείται μυστική[15].

Σκοπός μίας συνάρτησης κατακερματισμού είναι να παρέχει ένα αποτύπωμα ενός αρχείου. Πρέπει να πληρούνται κάποιες προϋποθέσεις από μία συνάρτηση κατακερματισμού προκειμένου να μπορεί να χρησιμοποιηθεί για αυθεντικοποίηση μηνύματος. Σε δύο κατηγορίες μπορούν να χωριστούν οι συναρτήσεις κατακερματισμού, βάση τις ιδιότητες και τις απαιτήσεις που ακολουθούν: τις μονόδρομες συναρτήσεις κατακερματισμού (One way Has Functions-OWFH) και τις συναρτήσεις αντίστασης σε συγκρούσεις(Collision Resistant Hash Functions-CRHF). Οι ιδιότητες αυτές είναι :

- Παράγουν σταθερή έξοδο και εφαρμόζονται σε τμήματα δεδομένων οποιουδήποτε μεγέθους.

- Η κατακερματισμένη τιμή H(x) υπολογίζεται εύκολα αν δοθεί ένα x, μετατρέποντας σε πρακτική την υλοποίηση σε λογισμικό και σε υλικό. Διαφορετικά η συνάρτηση κατακερματισμού δεν θα είναι αποτελεσματική.
- Για κάποια τιμή h δεν είναι εφικτό να υπολογιστεί το x, ώστε H(x)=h. Αυτή είναι η ιδιότητα του μονόδρομου (one way property). Η ιδιότητα αυτή δηλώνει ότι με δεδομένο ένα μήνυμα είναι απλό να παραχθεί ένας κώδικας, αλλά και ουσιαστικά αδύνατο να ανακτηθεί το μήνυμα δοθέντος του κώδικα. Είναι σημαντικό στην τεχνική αυθεντικοποίησης να συμπεριλαμβάνεται η χρήση μίας μυστικής τιμής.
- Έχοντας ως είσοδο οποιοδήποτε x, να είναι υπολογιστικά μη εφικτό να βρεθεί y≠x τέτοιο ώστε H(x)=H(y), δηλαδή ασθενής αντίσταση σε συγκρούσεις( weak collision resistance). Σύμφωνα με την ιδιότητα αυτήν παρέχεται η εγγύηση ότι δεν μπορεί να υπάρχει εναλλακτικό μήνυμα που να κατακερματίζεται στην ίδια τιμή με ένα δεδομένο μήνυμα. Επομένως, όταν χρησιμοποιείται κρυπτογραφημένος κώδικας κατακερματισμού, παρεμποδίζεται η πλαστογραφία.
- Είναι αδύνατον υπολογιστικά να βρεθεί ζεύγος (x,y) τέτοιο ώστε H(x)=H(y). Η ιδιότητα αυτή ονομάζεται ισχυρή αντίσταση σε συγκρούσεις (strong collision resistance) και σχετίζεται με το αν γίνει μία επίθεση και πόσο ανθεκτική είναι η συνάρτηση κατακερματισμού.

*Εικόνα 3-Αναπαράσταση είσοδού τριών μηνυμάτων-κλειδιών τυχαίου μεγέθους.*

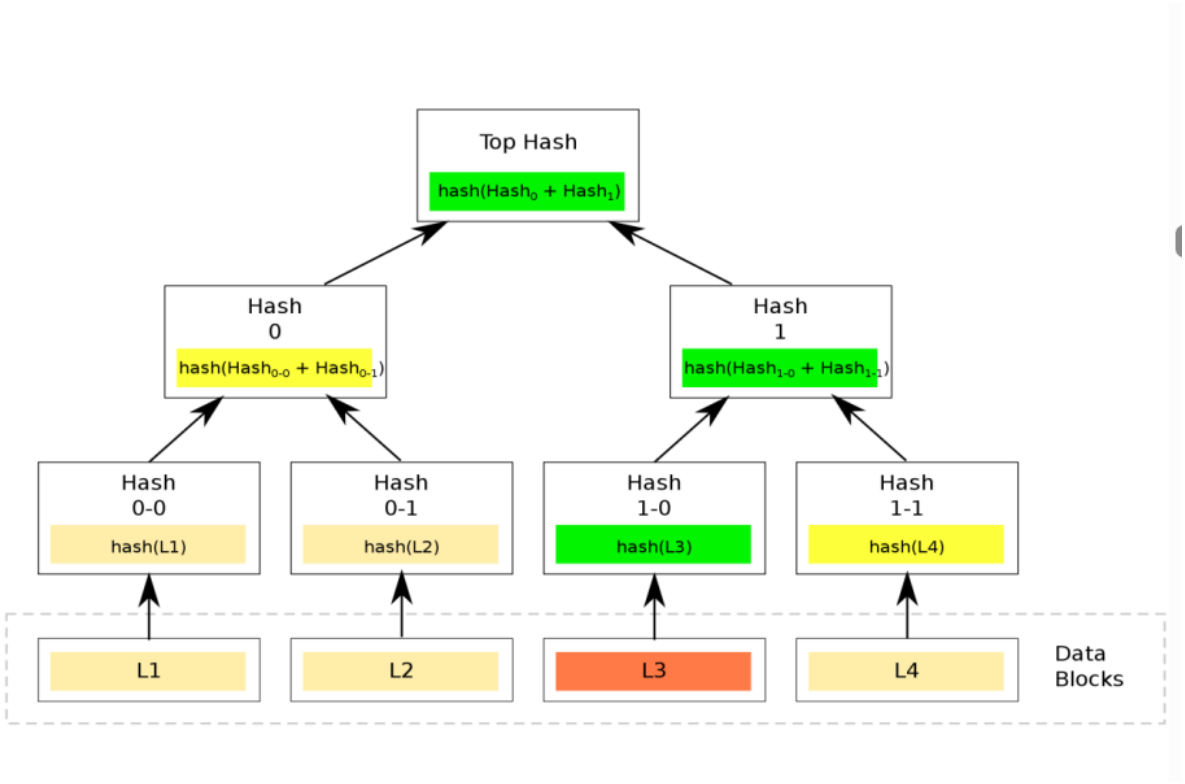

### 2.1.3.2 Μέθοδος Merkle Trees

Το 1979 ο ειδικός υπολογιστών Ralph Merkle δημοσίευσε ένα επιστημονικό άρθρο με ονομασία “A Certified Digital Signature” στο οποίο έδινε μία αποτελεσματική μέθοδο για την διαδικασία της επαλήθευσης δεδομένων, που ονομάστηκε Markle Trees. Η ιδέα αυτήν έφερε την επανάσταση στον τρόπο λειτουργείας των κρυπτογραφημένων πρωτοκόλλων και κατ’ επέκταση στον χώρο της κρυπτογραφίας. Τα Merkle Trees χρησιμοποιούνται στο Bitcoin και επομένως στον μηχανισμό Blockchain[1].

Οποιαδήποτε συναλλαγή καταγράφεται σε κάποια συστοιχία της αλυσίδας και έχει μία μοναδική ταυτότητα τιμής(ID). Η τιμή αυτή είναι ένας κωδικός 64 χαρακτήρων που καταλαμβάνει μνήμη 256 bits, σχεδόν σε όλους τους μηχανισμούς του Blockchain. Ο χώρος μνήμης αποτελεί πρόβλημα, διότι μία αλυσίδα Blockchain αποτελείται από χιλιάδες συστοιχίες και καθένα από αυτό περιλαμβάνει τεράστιο πλήθος συναλλαγών. Για τον λόγω αυτό η βελτιστοποίηση στο κομμάτι αυτό είναι απαραίτητη. Η ελαχιστοποίηση του χρόνου επεξεργασίας και η ταυτόχρονη εξασφάλιση του υψηλότερου επιπέδου ασφάλειας, προϋποθέτει την χρήση όσο το δυνατών λιγότερων δεδομένων κατά την επεξεργασία και επαλήθευση. Η μέθοδος Merkle Trees ήρθε να δώσει λύση σε αυτό. Στην ουσία, τα Merkle Trees μέσα από μία μαθηματική πράξη καταλήγουν σε έναν κωδικό 64 χαρακτήρων, αφού πρώτα λαμβάνουν έναν μεγάλο αριθμό αναγνωριστικών τιμών οι οποίες είναι σχετικές με τις συναλλαγές. Ο κωδικός αυτός είναι πολύ σημαντικός γιατί μέσω μιας τιμής Merkle Root, επιτρέπει όλους τους υπολογιστές να επαληθεύουν γρήγορα και αποτελεσματικά ότι μία συγκεκριμένη συναλλαγή πραγματοποιήθηκε σε μία συστοιχία[1].

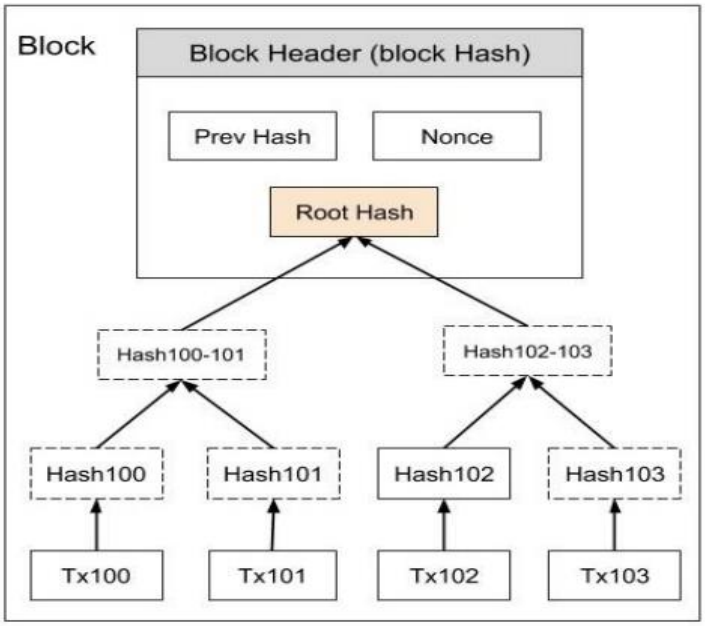
Σε ένα Merkle Trees κάθε κόμβος αναγράφει μία κατακερματισμένη τιμή, ο οποίος αποτελεί ένα δυαδικό δέντρο. Το δέντρο αποτελείται από τους κόμβους-γονείς, κόμβους-φύλλα, και την ρίζα. Οι κόμβοι- φύλλα έχουν μία ετικέτα με την τιμή κάθε συναλλαγής που πραγματοποιείται στη συστοιχία. Οι τιμές εισόδου ομαδοποιούνται σε ζεύγη. Κάθε κόμβος του δέντρου που δεν είναι φύλλο και έχει δύο παιδιά, περιλαμβάνει και τις τιμές των παιδιών του. Μία νέα τιμή η οποία θα αναγράφεται στον κόμβο-γονέα θα προκύψει από τον συνδυασμό των δύο τιμών, ο οποίος συνδυασμός θα περάσει από μία συνάρτηση κατακερματισμού. Στη συνέχεια, η διαδικασία θα επαναληφθεί και θα προκύψουν οι τιμές των επόμενων κόμβων-γονέων. Τελικά μέσα από όλη αυτήν την διαδικασία οδηγούμαστε σε μία μοναδική τιμή, την ρίζα Merkle Tree, που είναι αυτήν που θα επιτρέψει την αποτελεσματική επαλήθευση της πληροφορίας και θα καθορίσει το σύνολο των συναλλαγών στη συστοιχία. Στην περίπτωση που υπάρχει παραπάνω αριθμός συναλλαγών, τότε η τελευταία από αυτές αντιγράφεται και στην συνέχεια ζευγαρώνεται με τον εαυτό της[2].

*Εικόνα 4-Αναπαράσταση ενός Merkle Tree με κόμβους-φύλλα και τις τιμές τους να φαίνονται στο τελευταίο επίπεδο και την Merkle Root στο πρώτο επίπεδο (Top Hash).*




Η πρώτη εφαρμογή των Merkle Trees ήταν στο Bitcoin. Η χρήση των Merkle Trees μειώνει αποτελεσματικά τον χρόνο που απαιτείται για να βρεθεί αν μία συναλλαγή βρίσκεται σε κάποια συγκεκριμένη συστοιχία. Πολύ πιο εύκολη γίνεται με αυτόν τον τρόπο η διαδικασία αναζήτησης μίας πληροφορίας σε ολόκληρη την βάση δεδομένων μέσω μίας ρίζας. Επιπλέον, δίνεται η δυνατότητα διανομής μεγάλου όγκου δεδομένων σε μικρότερα τμήματα, ενώ παρά το μέγεθος του όγκου, εξαλείφεται το εμπόδιο επαλήθευσης της ακεραιότητας του περιεχομένου. Τα Merkle Trees αποτελούν μέρος του μηχανισμού Blockchain και των δικτύων ομότιμων κόμβων (Peer – to – Peer) με πρωταγωνιστικό ρόλο στον έλεγχο και την επικαιροποίηση της αυθεντικότητας των δεδομένων. Η όλο και μεγαλύτερη γνώση του τρόπου λειτουργείας τους και της τεχνολογίας τους μπορεί να στην ολοένα καλύτερη κατανόηση της τεχνολογίας του Blockchain.

*Εικόνα 5-Η δομή ενός Merkle Tree στην συστοιχία της αλυσίδας Blockchain.*



Transactions Hashed in a Merkle Tree

## 2.1.3.3 Ψηφιακές Υπογραφές

Η νέα ψηφιακή εποχή οδήγησε στην ανάγκη για δόμηση καναλιών διανομής τα οποία θα είναι ασφαλή με την ύπαρξη ταυτοποίησης από τα αρμόδια πρόσωπα, η οποία θα είναι ίσιας σημασίας με αυτή της γραπτής υπογραφής. Η θεωρία των κρυπτονομισμάτων λαμβάνει νέες δυνατότητες από την εξέλιξη στην επιστήμη υπολογιστών.

Το 1976, ο Whitfield Diffie και ο Martin Hellman παρουσίασαν την ιδέα των ψηφιακών υπογραφών. Αργότερα, ο αλγόριθμος RSA που εφευρέθηκε από τους Ronald Rivest, Adi Shamir και Len Adleman χρησιμοποιήθηκε στις ψηφιακές υπογραφές. Μετά από δοκιμές η μέθοδος αυτή αναδείχθηκε ανασφαλής. Το 1989 κυκλοφόρησε το Lotus Notes 1.0, το οποίο αποτελεί το πιο γνωστό λογισμικό που χρησιμοποίησε ψηφιακές υπογραφές[5][6].

Για την επικύρωση της γνησιότητας και της ακεραιότητας ενός μηνύματος, λογισμικού ή ψηφιακού εγγράφου, χρησιμοποιείται μία ψηφιακή υπογραφή η οποία αποτελεί μία μαθηματική τεχνική. Για να πιστοποιηθεί το έγγραφο στέλνει ένα «ηλεκτρονικό δακτυλικό

αποτύπωμα» και διασφαλίζει ότι θα παραμείνει αναλλοίωτο κατά την άφιξή του στον παραλήπτη. Η λύση του προβλήματος της παραβίασης και πλαστογραφίας στις ψηφιακές επικοινωνίες έρχεται μέσα από την ψηφιακή υπογραφή, προσφέροντας πιο εγγενή ασφάλεια, λειτουργώντας ως ένα ψηφιακό ισοδύναμο της χειρόγραφης υπογραφής ή σφραγίδας. Αποτελεί μία σημαντική εξέλιξη στην κρυπτογραφία δημόσιου κλειδιού και παρέχει ένα σύνολο χαρακτηριστικών ασφάλειας που θα ήταν δύσκολο να υλοποιηθούν διαφορετικά. Όπως ακριβώς γίνεται και στην ψηφιακή υπογραφή, η ψηφιακή υπογραφή διαθέτει συγκεκριμένες ιδιότητες:

- Πιστοποιεί την ημερομηνία και ώρα της υπογραφής αλλά και τον υπογράφοντα.
- Αυθεντικοποιεί τα δεδομένα κατά τη στιγμή της υπογραφής.
- Μπορεί να επαληθευτεί από τρίτους, έτσι ώστε να μην υπάρχουν αμφισβητήσεις.

Αυτές εξασφαλίζουν την ασφάλεια και την ακεραιότητα των ηλεκτρονικών δεδομένων, επιτρέποντας την επίτευξη εμπιστοσύνης μεταξύ αποστολέα και παραλήπτη[21]

Οι ψηφιακές υπογραφές σχετικά με τον τρόπο λειτουργίας τους βασίζονται στην κρυπτογραφία δημόσιου κλειδιού, γνωστή και ως ασύμμετρη κρυπτογραφία. Από τον αλγόριθμο δημοσίου κλειδιού, δημιουργούνται δύο κλειδιά, ένα δημόσιο και ένα ιδιωτικό τα οποία είναι μαθηματικά συνδεδεμένα. Τα δύο κρυπτογραφικά κλειδιά ελέγχουν την προέλευση της υπογραφής. Το άτομο με την ψηφιακή υπογραφή χρησιμοποιεί το δικό του ιδιωτικό κλειδί για την κρυπτογράφηση των σχετικών δεδομένων. Η αποκρυπτογράφηση των δεδομένων γίνεται μέσω του δημόσιου κλειδιού, έτσι και επαληθεύονται. Ο υπολογισμός του ιδιωτικού κλειδιού, δεν μπορεί να γίνει με κανέναν τρόπο από την γνώση του δημοσίου κλειδιού κρυπτογράφησης. Εκεί βασίζεται και η επιτυχία του. Αν μετά την υπογραφή αλλάξει το έγγραφο, τότε εκείνη ακυρώνεται[22][23].

Ο συγκεκριμένος μηχανισμός βασίζεται σε τρείς βασικές λειτουργίες. Αρχικά η δημιουργία ενός ιδιωτικού και ενός δημόσιου κλειδιού μέσο του αλγόριθμου δημοσίου κλειδιού. Με το δημόσιο κλειδί ελέγχεται η ψηφιακή υπογραφή, ενώ με το ιδιωτικό δημιουργείται. Επιπλέον, ο αλγόριθμος για την προσθήκη της υπογραφής σε κάποιο έγγραφο, αξιοποιεί το ιδιωτικό κλειδί το οποίο ανήκει μόνο στον υπάρχοντα. Επιπλέον, ελέγχεται η αυθεντικότητα και η ακεραιότητα του εγγράφου από τον έλεγχο της υπογραφής, στον οποίο χρησιμοποιείται το δημόσιο κλειδί. Τέλος, αξιοσημείωτο ρόλο παίζει η συνάρτηση κατακερματισμού, που θα συμπεριληφθεί σε ολόκληρη την διαδικασία[23].

Αναλυτικότερα, ο αλγόριθμος ασύμμετρης κρυπτογράφησης αλλά και η συνάρτηση κατακερματισμού που θα χρησιμοποιήσουν τα άτομα στην μεταξύ τους επικοινωνία, επιλέγεται από τους ίδιους.

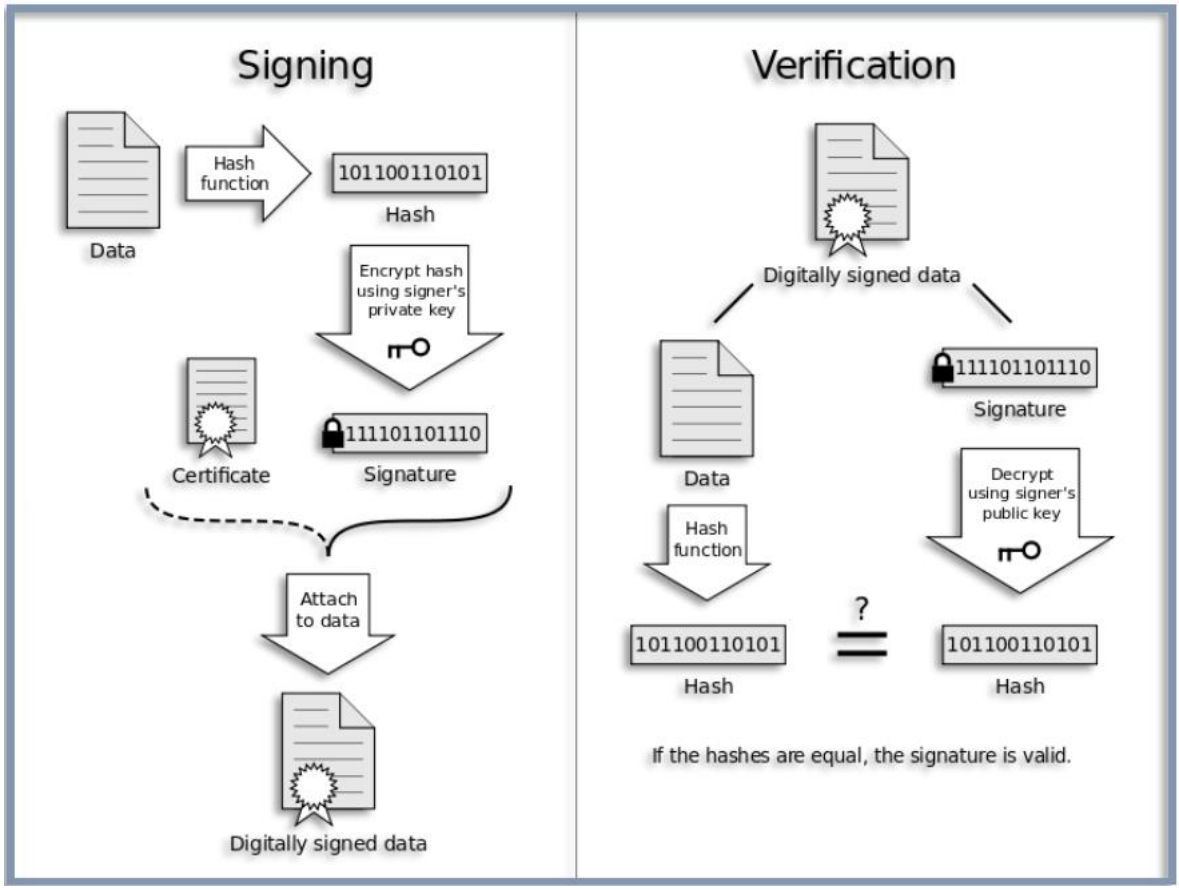
**Αλγόριθμος Προσθήκης Υπογραφής**

Ο αποστολέας που θέλει να επισυνάψει τα υπογεγραμμένα έγγραφα, εφαρμόζει την συνάρτηση κατακερματισμού πάνω στα έγγραφα αυτά, ώστε να μπορεί να παράγει την τιμή κατακερματισμού ως αποτέλεσμα. Στην συνέχεια, βάση του ιδιωτικού κλειδιού που έχει στην κατοχή του ο υπογράφοντας, η τιμή αυτή κρυπτογραφείται. Η κρυπτογραφημένη σύνοψη σε συνδυασμό με την επιπρόσθετες πληροφορίες, αποτελούν τη ψηφιακή υπογραφή η οποία επισυνάπτεται με τα απαραίτητα δεδομένα και τελικά αποστέλλονται στον χρήστη που θα κάνει την επαλήθευση. Η κρυπτογράφηση δεν γίνεται σε όλο το μήνυμα αλλά μόνο στην παραγόμενη κατακερματισμένη τιμή, για τον λόγω ότι η ευελιξία που έχει ο αλγόριθμος κατακερματισμού, να μπορεί να μεταβάλει μία αυθαίρετη είσοδο σε μία σταθερού μήκους τιμή, που συνήθως είναι αρκετά μικρότερη. Έτσι αντί να υπογράφεται ένα μεγάλου μεγέθους μήνυμα, χρειάζεται να υπογραφεί μία σταθερού και μικρού μήκους τιμή, εξοικονομώντας χρόνο.

**Αλγόριθμος Ελέγχου Υπογραφής**

Ο χρήστης ο οποίος λαμβάνει δεδομένα με την ψηφιακή υπογραφή, θα πραγματοποιήσει έλεγχο αυτής. Θα αποκρυπτογραφήσει την κατακερματισμένη τιμή του εγγράφου, χρησιμοποιώντας το δημόσιο κλειδί. Στην συνέχεια η υπογραφή θα περάσει μαζί με το μήνυμα που έλαβε από τον αλγόριθμο κατακερματισμού, οδηγώντας σε μία επιπλέον έξοδο. Συγκρίνοντας την έξοδο με την τιμή που δημιουργήθηκε από την κρυπτογράφηση, ελέγχεται η αυθεντικότητα της υπογραφής. Αν οι δύο τιμές αυτές είναι ίδιες, τότε δεν υπάρχει αλλοίωση και η υπογραφή επικυρώνεται. Αν οι τιμές είναι διαφορετικές, τότε η υπογραφή δημιουργήθηκε από ένα ιδιωτικό κλειδί που δεν αντιστοιχεί στο δημόσιο κλειδί που παρουσιάστηκε από τον υπογράφοντα.

*Εικόνα 6-Διάγραμμα μηχανισμού της ψηφιακής υπογραφής. Περιλαμβάνει τη σχεδίαση της υπογραφής και την επαλήθευσή της.*




Η τεχνολογία ψηφιακών υπογραφών προϋποθέτει ότι όλο τα συμβαλλόμενα μέρη εμπιστεύονται ότι το άτομο που δημιουργεί την υπογραφή έχει κρατήσει μυστικό το ιδιωτικό κλειδί. Διαφορετικά, αυξάνει την πιθανότητα δημιουργίας ψεύτικων υπογραφών. Έτσι η δημιουργία των κλειδιών πρέπει να γίνεται με έναν ασφαλή τρόπο, για την προστασία της ακεραιότητας της ψηφιακής υπογραφής. Ο Πάροχος Υπηρεσιών Πιστοποίησης (Certificate Authority) επιλύει αυτό το πρόβλημα. Μέσω του οργανισμού αυτού πιστοποιείται η σχέση ενός χρήστη με το δημόσιο κλειδί του. Πολλές φορές, επισυνάπτεται και ένα ψηφιακό πιστοποιητικό του δημοσίου κλειδιού μαζί με τα έγγραφα και την ψηφιακή υπογραφή.

Η τεχνολογία αυτή χρησιμοποιείται από τις βιομηχανίες για την βελτίωση της ακεραιότητας των εγγράφων και για την βελτιστοποίηση των διαδικασιών. Στα περισσότερα νέα προγράμματα ηλεκτρονικού ταχυδρομείου υποστηρίζεται η χρήση ψηφιακών υπογραφών και ψηφιακών πιστοποιητικών, διευκολύνοντας την υπογραφή εξερχόμενων μηνυμάτων αλλά και την επικύρωση ψηφιακά υπογεγραμμένων εισερχόμενων μηνυμάτων. Επίσης οι ψηφιακές

υπογραφές χρησιμοποιούνται στις επικοινωνίες και τις συναλλαγές που εκτελούνται μέσω του διαδικτύου, για να αποδειχθεί η αυθεντικότητα και η ακεραιότητα των δεδομένων.

## 2.2 Αρχιτεκτονική Του Μηχανισμού Blockchain

Η τεχνολογία του Blockchain χαρακτηρίζεται από συνδεδεμένες συστοιχίες, που είναι συνδεδεμένες μεταξύ τους και καταγράφουν μία σειρά από δεδομένα. Η αρχιτεκτονική της βασίζεται σε συγκεκριμένα χαρακτηριστικά. Αποτελείται από πολλές συστοιχίες τα οποία έχουν συγκεκριμένη δομή και βασίζεται σε λειτουργίες οι οποίες διασφαλίζουν την αυθεντικότητα της πληροφορίας, όπως η δημιουργία συστοιχίας και το πρωτόκολλο συναίνεσης.

*Εικόνα 7-Παράδειγμα μιας αλυσίδας Blockchain με τα μπλοκ να συνδέονται μεταξύ τους με χρονολογική σειρά.*

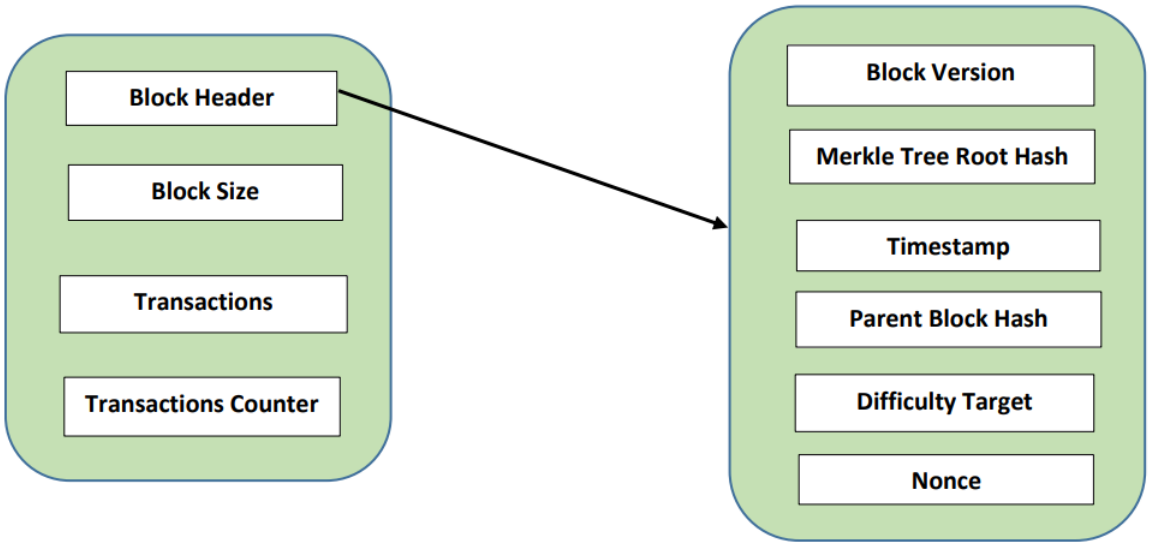

### 2.2.1 Η Δομή Του Block

Οι συστοιχίες είναι δομές δεδομένων, οι οποίες καταγράφουν το σύνολο των συναλλαγών και διανέμουν πληροφορίες στους κόμβους του δικτύου Blockchain. Οποιαδήποτε μεταβολή στα εσωτερικά τους δεδομένα καθίσταται αδύνατη, αφού οι δομές αυτές είναι πλήρως συνδεδεμένες μεταξύ τους. Η επικεφαλίδα (block header) και το σώμα (block body), αποτελούν την εσωτερική δομή μιας συστοιχίας. Αναλυτικότερα η επικεφαλίδα της συστοιχίας περιλαμβάνει:

1. Block Version: περιλαμβάνει την έκδοση του μπλοκ και υποδεικνύει ποιοι κανόνες πρέπει να ακολουθούνται για την επικύρωση.
2. Merkle Tree Root Hash: είναι η κρυπτογραφημένη τιμή που προκύπτει από την εφαρμογή της συνάρτησης κατακερματισμού σε όλες τις συναλλαγές που περιέχονται στο μπλοκ.
3. Parent Block Hash: αποτελεί την κατακερματισμένη τιμή του προηγούμενου μπλοκ, δηλαδή τη Hash τιμή.
4. Timestamp: περιλαμβάνει το χρόνο, κατά τον οποίο δημιουργήθηκε το μπλοκ.
5. Difficulty Target: η δυσκολία που απαιτείται για να επικυρωθεί το συγκεκριμένο μπλοκ.
6. Nonce: ένας ακέραιος τυχαίος αριθμός ο οποίος χρησιμοποιείται από τον αλγόριθμο "Proof Of Work" και μεταβάλλεται κατά την διαδικασία της "εξόρυξης".

Το block body περιλαμβάνει τις συναλλαγές (Transactions) και τον μετρητή των συναλλαγών (Transaction Counter). Ο μετρητής των συναλλαγών είναι ο συνολικός αριθμός των καταχωρήσεων που πραγματοποιούνται στο μπλοκ. Ο μέγιστος αριθμός συναλλαγών καθορίζεται από το μέγεθος του μπλοκ (Block size) και το μέγεθος τις κάθε συναλλαγής. Το είδος της εφαρμογής που εφαρμόζεται καθορίζει και τα μέγεθος του block[11].

*Εικόνα 8-Εσωτερική δομή του μπλοκ.*




## 2.2.2 Η Σύνδεση Των Μπλοκ Μεταξύ Τους

Όλες οι συστοιχίες στην αλυσίδα περιλαμβάνουν δεδομένα τα οποία τοποθετούνται σε χρονολογική σειρά. Σε κάθε συστοιχία που παράγεται, υπολογίζεται και η κατακερματισμένη τιμή του. Η δομή των δεδομένων αυτή, βοηθάει να παραχθεί μια μοναδική αναπαράσταση όλων των δεδομένων που είναι η ρίζα του (Merkle Tree Root Hash). Στο πλαίσιο της τεχνολογίας Blockchain, ο αλγόριθμος κατακερματισμού που χρησιμοποιείται για τον υπολογισμό της τιμής Merkle Tree Root Hash, είναι ο Secure Hashing Algorithm 256 (SHA-256), ο οποίος δημιουργεί μία αναπαράσταση μεγέθους 256-bits της αντίστοιχης συστοιχίας των συναλλαγών. Η έξοδος θα έχει πάντοτε μέγεθος 256-bits, οποιοδήποτε και αν είναι το μέγεθος των δεδομένων, γεγονός που παίζει ρόλο στην αποθήκευση μεγάλου όγκου δεδομένων και συναλλαγών. Η σταθερού μεγέθους κατακερματισμένη τιμή αντικαθιστά τις άπειρες συναλλαγές χωρίς να είναι απαραίτητη η απομνημόνευσή της, με αποτέλεσμα να «διαβάζονται» οι συναλλαγές μόνο μέσω αυτής. Είναι ένα ψηφιακό αποτύπωμα μοναδικό που δημιουργείται σε κάθε μπλοκ και λόγω των ιδιοτήτων του η πιθανότητα αποκρυπτογράφησης είναι απίθανη[12].

Κάθε συστοιχία περιλαμβάνει και την κατακερματισμένη τιμή του προηγούμενου μπλοκ στην επικεφαλίδα του. Έτσι συνδέονται μεταξύ τους δημιουργώντας την αναμενόμενη αλυσίδα. Στην περίπτωση αλλαγής δεδομένων, θα πρέπει να αλλάξει και το μοναδικό αποτύπωμα που καθορίζει τη συστοιχία. Άμα για κάποιον λόγω αλλάξει η κατακερματισμένη τιμή, τότε θα πρέπει να αλλάξει και να επαναπροσδιοριστεί και το πεδίο της επόμενης συστοιχίας. Το πεδίο «Parent Block Hash» της συστοιχίας πρέπει να αλλάξει και λάβει μία νέα τιμή, οδηγώντας σε ένα ντόμινο που θα μεταβάλει και θα αλλοιώσει ολόκληρη την αλυσίδα. Μέσο της ιδιότητας αυτής προστατεύονται οι πληροφορίες που υπάρχουν μέσα στη συστοιχία. Μόνη της όμως δεν δύναται να εγγυηθεί την ασφάλεια της αλυσίδας και κατ' επέκταση των συναλλαγών και των δεδομένων. Έτσι η τεχνολογία του Blockchain περιλαμβάνει και άλλα χαρακτηριστικά που προσφέρον την ασφάλεια των δεδομένων[3][4].

### 2.2.3 Δίκτυο Ομότιμων Κόμβων

Τα κυρίαρχα μοντέλα δικτυακών εφαρμογών είναι δύο:

1. Η αρχιτεκτονική πελάτη-εξυπηρετητή (Client Server)

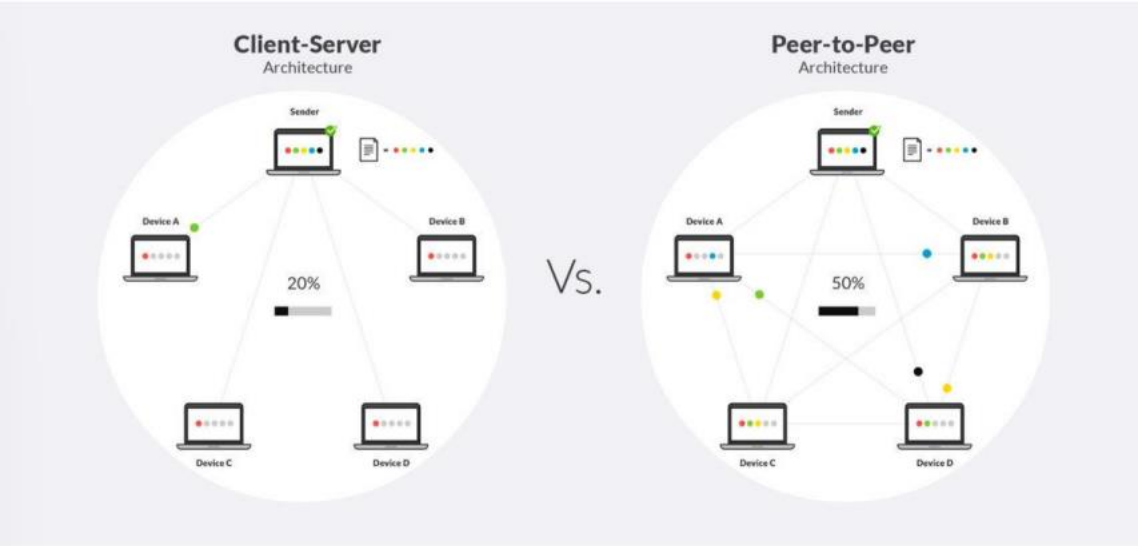
2. Η αρχιτεκτονική ομότιμων κόμβων (Peer-to-Peer / P2P)

Το επικρατέστερο μοντέλο έως και σήμερα, είναι αυτό του πελάτη-εξυπηρετητή (Client Server). Στο μοντέλο αυτό υπάρχουν οι πελάτες-κόμβοι που εξαρτώνται από τον εξυπηρετητή να τους προσφέρει υπηρεσίες και αυτός με την σειρά του προσπαθεί να ανταπεξέλθει. Έτσι ο ρόλος του εξυπηρετητή αποτελεί καθοριστικός. Αν όμως ο εξυπηρετητής κάνει λάθος τότε το δίκτυο καταρρέει.

Αντιθέτως, στο δίκτυο των ομότιμων κόμβων (P2P), οι συμμετέχοντες αποθηκεύουν και μοιράζονται συλλογικά τα αρχεία. Το P2P σύστημα δεν έχει ένα κεντρική διαχείριση αλλά αποτελείται από ένα κατανεμημένο δίκτυο χρηστών και όλοι οι κόμβοι έχουν την ίδια ισχύ και τα ίδια δικαιώματα να ενεργήσουν μέσα σε αυτό. Κάθε κόμβος περιέχει αντίγραφο όλων των αρχείων, δίνοντας την δυνατότητα να έχει την ιδιότητα τόσο του εξυπηρετητή όσο και του πελάτη, εξαλείφοντας την ανάγκη ύπαρξης διακομιστή. Όταν ο κόμβος παίρνει την ιδιότητα του πελάτη, μπορεί να έχει πρόσβαση σε αρχεία και πληροφορίες οποιοδήποτε συνδεδεμένου κόμβου. Όταν παίρνει την ιδιότητα του εξυπηρετητή, είναι η πηγή από την οποία οι υπόλοιποι κόμβοι λαμβάνουν δεδομένα. Και οι δύο αναφερόμενες λειτουργείες μπορούν να πραγματοποιηθούν ταυτόχρονα. Μέσα στο σύστημα κυριαρχούν η ισοτιμία και η αυτονομία με τον κάθε κόμβο να έχει ενεργό ρόλο στη λήψη αποφάσεων. Η διαμόρφωση ενός πρωτόκολλου του συνεταιριστικού συστήματος που καθορίζεται από αυστηρούς κανόνες, καθορίζει την ομαλή επικοινωνία και συνεργασία μεταξύ τους. Οι κόμβοι μπορεί να διαφέρουν στην τοπική διαμόρφωση, στο εύρος ζώνης, στην ποσότητα αποθήκευσης και στην ταχύτητα επεξεργασίας[12][14].

Στα δίκτυα P2P καθώς η βάση χρηστών μεγαλώνει, γίνονται πιο γρήγορα και αποδοτικά, αφού κάθε κόμβος λαμβάνει αρχεία, μετά τα αποθηκεύει και στην συνέχεια τα μεταδίδει. Επίσης η κατανεμημένη αρχιτεκτονική καθιστά τα συστήματα πολύ ανθεκτικά σε διάφορες επιθέσεις. Η τεχνολογία Blockchain βασίζεται στην αρχιτεκτονική ομότιμων κόμβων. Η τεχνολογία Blockchain καταγράφει όλη την δραστηριότητα και δεν υπάρχει κανένας μεσάζοντας για την καταγραφή συναλλαγών στην αλυσίδα. Έτσι διάφορους ρόλους μπορεί να αποκτήσει ο κάθε συμμετέχοντας. Οι πλήρεις κόμβοι είναι αυτοί που παρέχουν ασφάλεια και στο δίκτυο, ελέγχοντας τις συναλλαγές, αποθηκεύοντας και ενημερώνοντας ένα αντίγραφο του Blockchain.

*Εικόνα 9-Αναπαράσταση μοντέλου πελάτη-εξυπηρετητή και ομότιμων κόμβων.*




Τα δίκτυα ομότιμων κόμβων μπορούν να διαχωριστούν με βάση την αρχιτεκτονική τους. Οι τρείς τύποι στους οποίους διακρίνονται είναι τα δομημένα (structured), τα μη δομημένα (unstructured) και τα υβριδικά δίκτυα (hybrid).

### 2.2.3.1 Μη Δομημένα Δίκτυα Ομότιμων Κόμβων

Στα μη δομημένα δεν υπάρχει οργάνωση των κόμβων. Σχηματίζονται από τυχαίες συνδέσεις των κόμβων. Τους διακρίνει η ισχυρότητα και ανθεκτικότητα έναντι υψηλής δραστηριότητας καταιγισμού, όταν πολλοί κόμβοι εισέρχονται και εξέρχονται από το δίκτυο. Τα δίκτυα αυτά έχουν το πλεονέκτημα της ευελιξίας και της ευκολίας στο να επιτρέπουν τοπικές βελτιστοποιήσεις σε διαφορετικές περιοχές της επικάλυψης. Παρόλα αυτά, η έλλειψη συγκεκριμένης δομής προκαλεί κάποιους περιορισμούς. Τα μη δομημένα δίκτυα απαιτούν πολύ μεγαλύτερη χρήση μνήμης, καθώς τα ερωτήματα αναζήτησης δεδομένων αποστέλλονται σε μεγαλύτερο αριθμό κόμβων. Έτσι στην περίπτωση που ένας κόμβος επιθυμεί να αναζητήσει μία πληροφορία, τότε το ερώτημα μεταφέρεται μέσω του δικτύου ώστε να βρεθούν όλοι οι χρήστες που μοιράζονται αυτά τα δεδομένα. Ως αποτέλεσμα δημιουργείται πολύ μεγάλη κίνηση στο δίκτυο, χρησιμοποιώντας περισσότερη μνήμη. Επιπλέον επειδή δεν υπάρχει συσχέτιση μεταξύ των κόμβων, δεν υπάρχει εγγύηση ότι με την αναζήτηση αυτή, το ερώτημα θα βρει και θα φτάσει στον κόμβο με τα επιθυμητά δεδομένα και επομένως δεν διασφαλίζεται η εύρεση της πληροφορίας. Επιπρόσθετα, σε ορισμένες περιπτώσεις η έρευνα μπορεί να

ακολουθεί ένα φαύλο κύκλο σε αναζητήσεις με δημοφιλές περιεχόμενο, διότι μπορεί να είναι διαθέσιμο σε αρκετούς κόμβους. Ακόμα, η εύρεση σπάνιων δεδομένων είναι πολύ σπάνιο να είναι επιτυχής, διότι τα δεδομένα αυτά μοιράζονται συγκεκριμένοι κόμβοι[28].

#### 2.2.3.2 Δομημένα Δίκτυα Ομότιμων Κόμβων

Τα δομημένα δίκτυα σε αντίθεση με τα μη δομημένα δίκτυα ομότιμων δικτύων, επιτρέπουν στους κόμβους να αναζητούν αποτελεσματικά αρχεία, ακόμα και αν το περιεχόμενο τους δεν είναι ευρέως διαθέσιμο, ακολουθώντας μία οργανωμένη αρχιτεκτονική. Αυτό επιτυγχάνεται μέσω συναρτήσεων κατακερματισμού οι οποίες διευκολύνουν την αναζήτηση στις βάσεις δεδομένων. Ο πιο διαδεδομένος τύπος δομημένων δικτύων υλοποιεί έναν κατανεμημένο πίνακα κατακερματισμού, στον οποίο χρησιμοποιείται μία παραλλαγή της «συνεπούς» συνάρτησης κατακερματισμού (consistent hashing), ώστε να αντιστοιχίσει κάθε αρχείο σε έναν κόμβο. Έτσι γίνεται πιο αποτελεσματική η αναζήτηση δεδομένων μέσα στο δίκτυο, αφού μπορούν να ανακτηθούν εύκολα μέσω του πίνακα κατακερματισμού. Οι κόμβοι πρέπει να τηρούν λίστες γειτόνων οι οποίοι πληρούν συγκεκριμένα κριτήρια, για την ομαλή και σωστή λειτουργεία του δικτύου. Ως αποτέλεσμα, το δίκτυο γίνεται πιο ευάλωτο σε συνθήκες υψηλού ρυθμού σύνδεσης και αναχώρησης κόμβων. Τα δομημένα δίκτυα ενώ είναι πιο αποδοτικά, έχουν μεγάλο κόστος εγκατάστασης και συντήρησης[28].

#### 2.2.3.3 Υβριδικά Μοντέλα Δικτύων

Τα υβριδικά μοντέλα δικτύων συνδυάζουν το μοντέλο πελάτη-εξυπηρετητή με την αρχιτεκτονική του δικτύου ομότιμων κόμβων. Ένα υβριδικό μοντέλο δηλαδή είναι η σχεδίαση ενός κεντρικού διαχειριστή, για την διευκόλυνση της σύνδεσης μεταξύ των κόμβων στο δίκτυο και την βοήθεια στην εύρεση αυτών. Υπάρχουν πολλά μοντέλα που συνδυάζουν την λειτουργεία μέσω κεντρικής μονάδας που προέρχεται από τον πελάτη-εξυπηρετητή και την ισότητα μεταξύ των κόμβων που συνιστάται στο δίκτυο ομότιμων κόμβων. Τα υβριδικά μοντέλα τείνουν να παρουσιάζουν βελτιωμένη απόδοση σε σύγκριση με άλλα μοντέλα, λόγω του ότι αξιοποιούν βασικά πλεονεκτήματα από τον συνδυασμό των δύο δικτύων. Η εκτέλεση

λειτουργιών αναζήτησης πληροφορίας καθιστά απαραίτητη την χρήση κεντρικού διακομιστή. Η ακριβής λειτουργεία της αλυσίδας μπορεί να ποικίλει ανάλογα ποια τμήματα είναι αποκεντρωμένα και ποια όχι[14][25].

#### 2.2.3.4 Πλεονεκτήματα Δικτύου Ομότιμων Κόμβων Στην Τεχνολογία Blockchain

Ένα από τα πιο σημαντικά πλεονεκτήματα των ομότιμων κόμβων έναντι των παλαιών παραδοσιακών μοντέλων πελάτη-εξυπηρετητή, είναι ότι προσφέρουν μεγαλύτερη ασφάλεια. Όσο μεγαλύτερος είναι ο αριθμός των κόμβων στην αλυσίδα, τόσο την καθιστά ακλόνητη από επιθέσεις Denial of Service (DoS).

Κάθε προσπάθεια του εισβολέα να αλλάξει τα δεδομένα είναι αδύνατη, διότι χρειάζεται η πλειονότητα των κόμβων να καταλήξει σε συναίνεση πριν προστεθούν δεδομένα στον κόμβο. Η ιδιότητα αυτή αναφέρεται περισσότερο σε μεγάλα δίκτυα στα οποία συμμετέχουν πολλοί χρήστες. Ως αποτέλεσμα, η απαίτηση της συναινετικής πλειοψηφίας σε συνδυασμό με το δίκτυο ομότιμων κόμβων, δίνει στην τεχνολογία Blockchain μια σημαντική άμυνα αντοχής στην κακόβουλη δραστηριότητα.

Η αρχιτεκτονική του κατανεμημένου δικτύου στον μηχανισμό Blockchain και του Bitcoin προσφέρει ασφάλεια και τον καθιστούν ανθεκτικό στον έλεγχο από τις κεντρικές αρχές, διότι σε αντίθεση με τους τραπεζικούς λογαριασμούς τα ηλεκτρονικά πορτοφόλια δεν «παγώνουν». Επιπλέον, η αντίσταση επεκτείνεται, αφού πλέον δεν είναι αναγκαία η δέσμευση από κάποιο τρίτο πρόσωπο[18].

### 2.2.4 Εξόρυξη Μπλοκ (Mining)

Η εξόρυξη είναι η διαδικασία προσθήκης συναλλαγών και εγγράφων στο σύστημα του Blockchain. Έτσι δημιουργούνται νέες συστοιχίες με την διαδικασία αυτή. Ο κύριος σκοπός της παραπάνω διαδικασίας είναι να οδηγήσει τους χρήστες να φτάσουν σε μία ασφαλή και

ανθεκτική στις παραβιάσεις συναίνεση. Οι κόμβοι που βοηθάνε στην διαδικασία της συναίνεσης ονομάζονται «εξορύκτες».

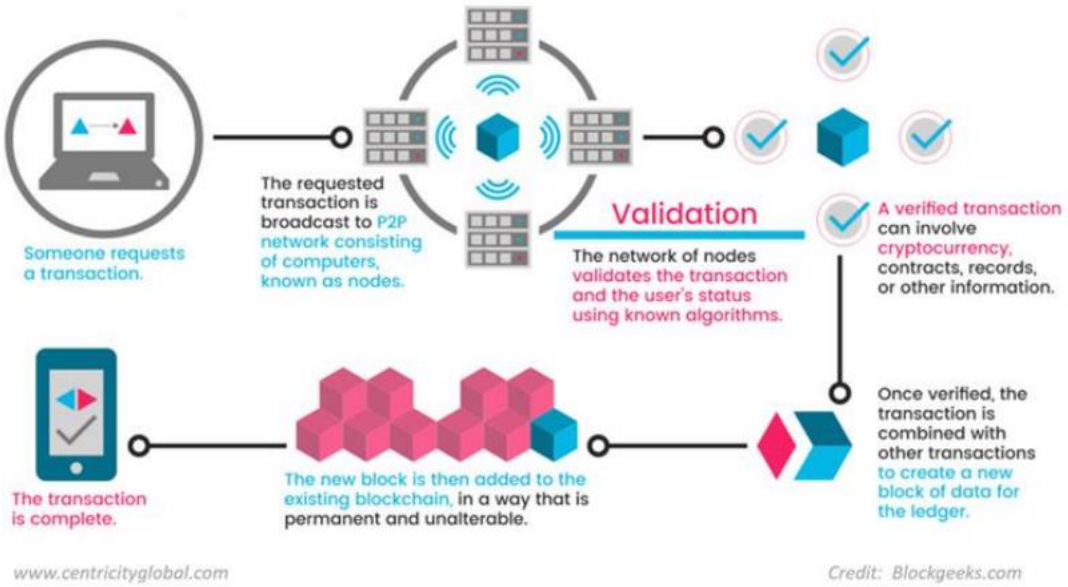
Ο «εξορύκτης» είναι ο πλήρης κόμβος ο οποίος ομαδοποιεί τις συναλλαγές σε συστοιχίες και ανταγωνίζεται με τους άλλους προκειμένου να προσθέσει την δικιά του συστοιχία στην αλυσίδα, λύνοντας γρήγορα ένα κρυπτογραφικό παζλ. Όταν έρθει η ώρα να εντάξει τις συναλλαγές στην συστοιχία, δημιουργεί για τη συστοιχία αυτή, μία μοναδική κατακερματισμένη τιμή (hash). Αυτό επιτυγχάνεται όταν ο «εξορύκτης» μεταβάλει μια τιμή nonce που περιέχεται στην επικεφαλίδα της συστοιχίας μέχρι αυτή να γίνει μικρότερη από μια συγκεκριμένη τιμή στόχο η οποία αναφέρεται και ως τιμή δυσκολίας (difficulty target). Πρέπει να λυθεί η παρακάτω εξίσωση:

**H(txs || nonce || parent block hash)<ε**

Η τιμή hash περιλαμβάνει ένα συγκεκριμένο πλήθος μηδενικών. Ο «εξορύκτης», μέσω της μαθηματικής διαδικασίας μεταβάλει την nonce, κατασκευάζοντας την απαραίτητη hash τιμή. Η τιμή nonce είναι μία τυχαία τιμή μεγέθους 32 bits που μεταβάλλεται συνέχεια μέχρι να ικανοποιηθεί η εξίσωση. Όταν βρεθεί η τιμή για την συστοιχία, ο «νικητής» το δημοσιοποιεί στο δίκτυο με σκοπό να το ελέγξουν οι υπόλοιποι κόμβοι. Αν ελέγχει και είναι έγκυρο, ο «εξορύκτης» ανταμείβεται με ένα ποσό BTC που σήμερά είναι 6,25. Τέλος, σύμφωνα με τα παραπάνω επιτυγχάνεται η συναίνεση (consensus)[18].

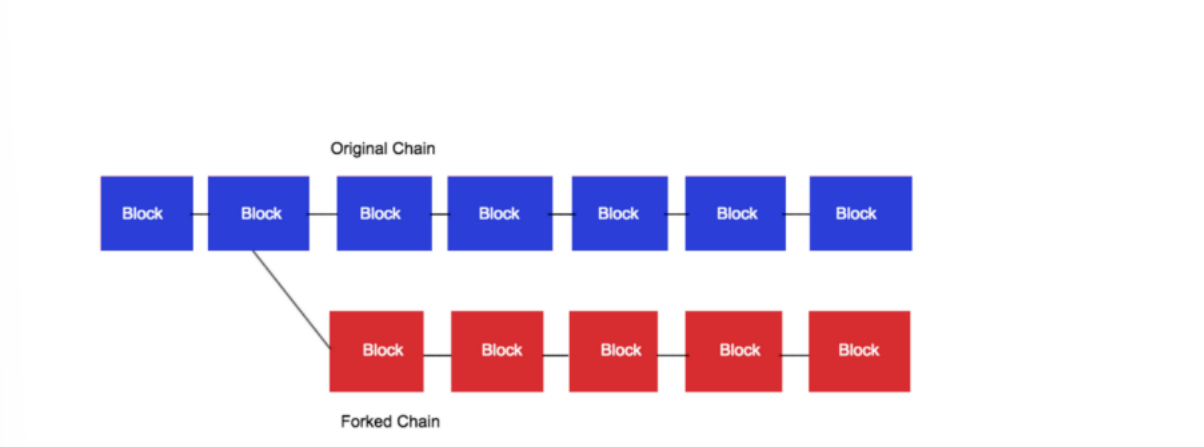
Όσο αυξάνεται η υπολογιστική ισχύς, τόσο μεγαλώνει η δυσκολία της επίλυσης του κρυπτογραφικού παζλ ώστε να διατηρηθεί σταθερό το ποσοστό παραγωγής συστοιχίας στην αλυσίδα. Όταν η συμμετοχή πολλών κόμβων στην προσπάθεια εξόρυξης είναι μεγάλη, τότε σημαίνει ότι η αμοιβή είναι υψηλή, οδηγώντας σε υψηλό βαθμό δυσκολίας. Έτσι αποτρέπεται η προσπάθεια κακόβουλων επιθέσεων στο δίκτυο[18].

*Εικόνα 10-Η διαδικασία εξόρυξης ενός μπλοκ.*




Στην ακραία περίπτωση που δημιουργηθούν την ίδια χρονική στιγμή δύο συστοιχίες που είναι έγκυρες, τότε η αλυσίδα Blockchain διαχωρίζεται σε δύο συνήθως νέες αλυσίδες. Το φαινόμενο αυτό ονομάζεται Fork. Το πρόβλημα που δημιουργείται στην αλυσίδα είναι η μη τήρηση χρονολογικής σειράς των συστοιχιών. Η επίλυση έρχεται όταν προστεθούν στην αλυσίδα συστοιχιών και η μία από τις δύο γίνει μεγαλύτερη. Το δίκτυο δέχεται την αλυσίδα με το μεγαλύτερο μήκος. Έτσι επιτυγχάνεται η συνέπεια των χρηστών του δικτύου.

*Εικόνα 11-Το φαινόμενο Fork.*




## 2.2.5 Genesis Μπλοκ

Η πρώτη συστοιχία στην αλυσίδα του Blockchain είναι το Genesis Μπλοκ. Είναι η βάση στην οποία προστίθενται συστοιχίες για να σχηματίσουν την δομή της αλυσίδας και είναι γνωστό ως συστοιχία 0. Η τιμή συστοιχίας απουσιάζει από την επικεφαλίδα αφού δεν υπάρχει προηγούμενη συστοιχία. Η τιμή αυτή είναι 0 δείχνοντας ότι δεν έχει πραγματοποιηθεί καμία συναλλαγή πριν το συγκεκριμένη συστοιχία.

### 2.2.6 Πρωτόκολλα Συναίνεσης

Σε ένα δίκτυο που χρησιμοποιεί την τεχνολογία Blockchain και απουσιάζει η κεντρική αρχή, είναι αναγκαίο ένα πρωτόκολλο συναίνεσης, βάση του οποίου οι συγκεκριμένες πληροφορίες θα επαληθεύονται και θα εγκρίνονται από τους συμμετέχοντες προτού καταχωρηθούν στο σύστημα. Έτσι επιτυγχάνεται η ακεραιότητα των δεδομένων και η εμπιστοσύνη μεταξύ των χρηστών.

#### 2.2.6.1 Proof of Work (PoW)

Ο αλγόριθμος Proof of Work που δημιουργήθηκε για να αποφευχθούν τα περιττά μηνύματα του ηλεκτρονικού ταχυδρομείου, εμφανίστηκε πρώτη φορά το 1992 από τον ερευνητή Dwork. Έτσι αποτρέπονταν η αποστολή ανεπιθύμητων μηνυμάτων μέσω της χρήσης κρυπτογραφικών μεθόδων και συναρτήσεων κατακερματισμού, η χρήση των οποίων απαιτούσαν πολύπλοκους υπολογισμούς και κατανάλωση χρόνου[28].

Το 2002 χρησιμοποιήθηκε ξανά για την αποτροπή ανεπιθύμητης αλληλογραφίας αλλά με άλλη τεχνική. Η συνάρτηση κατακερματισμού SHA-1 επισυνάπτει μέσα σε αυτή, το περιεχόμενο του μηνύματος, η χρονική σφραγίδα και μια τιμή του μετρητή. Οι επιτήδειοι που θα προσπαθήσουν την επίθεση με πολλαπλά μηνύματα, θα τους κοστίσει χρόνο και ενέργεια για να υπολογίσουν την τιμή κατακερματισμού, αποθαρρύνοντάς τους[28].

Στην συνέχεια ο Satoshi Nakamoto χρησιμοποίησε τον αλγόριθμο PoW στο Peer to Peer σύστημα ανταλλαγής Bitcoin, όπου δεν απαιτούνταν η συμμέτοχή τρίτου για τις συναλλαγές. Είναι μία στρατηγική συναίνεσης για την επέκταση της αλυσίδας των συστοιχιών και την προσθήκη των συναλλαγών μέσα σε αυτά. Πρέπει όμως να επικυρωθούν όλες οι συναλλαγές που έγιναν στην συστοιχία από όλα τα πρόσωπα του δικτύου πριν από την προσθήκη της συστοιχία στην αλυσίδα Blockchain, κάτι που απαιτεί σύνθετους υπολογισμούς. Οι «εξορύκτες» θα πρέπει να λύσουν ένα δύσκολο μαθηματικό πρόβλημα, συμβάλλοντας έτσι στην αλυσίδα. Αυτός που θα λύσει το κρυπτογραφικό παζλ, θα δημιουργήσει την επόμενη συστοιχία και θα ανταμειφθεί.

Όλες οι εκκρεμείς συναλλαγές της νέας συστοιχίας πρέπει να συγκεντρωθούν από τους «εξορύκτες» και να υπολογίσουν την κατακερματισμένη τιμή (Merkle Root) αυτών με την χρήση του αλγόριθμου SHA=256. Η πορεία όλων των παραπάνω καθορίζεται από την τιμή nonce η οποία αλλάζει για να βρεθεί η κατακερματισμένη τιμή της συστοιχίας που ταιριάζει. Η τιμή αυτή αναγράφεται στην επικεφαλίδα της συστοιχίας και μεταφέρεται σε όλους τους κόμβους για να γίνει η επαλήθευση. Η διαδικασία εξόρυξης σταματάει και ελέγχεται η εγκυρότητα της συστοιχίας. Αφού εγκριθεί η συστοιχία, η αλυσίδα αυξάνεται κατά ένα στο τέλος της και ο «εξορύκτης» παίρνει την ανταμοιβή που του αναλογεί[20][11].

Η διαδικασία επίλυσης του παζλ ώστε να εγκριθεί και να προστεθεί η συστοιχία στην αλυσίδα καταναλώνει την περισσότερη ενέργεια. Όλες οι υπόλοιπες διαδικασίες που αναφέρονται πιο πάνω δεν απαιτούν πολύ χρόνο και ενέργεια[20].

Η ισχύ των «εξορυκτών» μεταβάλει την δυσκολία επίλυσης του μαθηματικού προβλήματος. Αν το δίκτυο αυξηθεί με την συμμετοχή περισσότερων «εξορυκτών», τότε αυξάνουν την υπολογιστική δύναμή τους και οι συστοιχίες δημιουργούνται πιο εύκολα, οδηγώντας σε αύξηση της δυσκολίας του προβλήματος. Η κυρίαρχη αρχή του αλγορίθμου είναι ότι καμία οντότητα δεν πρέπει να κατέχει περισσότερο του 50% της συνολικής υπολογιστικής δύναμης, καθώς με αυτόν τον τρόπο μπορεί να ελέγχει αποτελεσματικά το σύστημα. Αυτή είναι η λεγόμενη 51% επίθεση. Βέβαια όταν το δίκτυο είναι πολύ μεγάλο τότε αυτό είναι ακατόρθωτο, διότι είναι πιο ανθεκτικό σε τέτοιες επιθέσεις[19].

Ο αλγόριθμος συναίνεσης PoW και η εξόρυξη, αποτελούν διαδικασίες που είναι ανοιχτές για τον οποιοσδήποτε. Κατά συνέπεια δεν είναι απαραίτητη καμίας γνώση ή πιστοποίησης για την συμμετοχή, δημιουργώντας μια υποστήριξη χιλιάδων κόμβων στο μοντέλο αυτό. Στην περίπτωση της επίθεσης 51%, ο εισβολέας μπορεί να διπλασιάσει τα δικά

του κεφάλαια και να απορρίψει επιλεκτικά τι συναλλαγές που δεν επιθυμεί να συμπεριλαμβάνονται στην συστοιχία.

Μία ακόμα επίθεση στην διαδικασία της εξόρυξης είναι αυτή της εγωιστικής εξόρυξης (selfish mining). Στην περίπτωση αυτή, οι «ειλικρινείς εξορύκτες» στηρίζουν τους εισβολείς και συμμετέχουν στην υλοποίηση του 51%. Ο επιτιθέμενος εκτελεί ακανόνιστη εξόρυξη, διατηρώντας μια ξεχωριστή αλυσίδα Blockchain. Δημοσιεύει επιλεκτικά πολλές συστοιχίες, κάνοντας το υπόλοιπο δίκτυο να απορρίψει τα δικά του αι να χάσει έσοδα. Τα κέρδη των «ειλικρινών εξορυκτών» μπορεί να φτάσουν το 51% της εξόρυξης, ενθαρρύνοντάς τους να προβούν σε αυτήν την ενέργεια[24].

# ΚΕΦΑΛΑΙΟ 3

# Η ΠΕΡΙΠΤΩΣΗ ΤΟΥ BITCOIN

## 3.1 Ιστορική Αναδρομή Του Bitcoin

Πριν την ανακοίνωση του Bitcoin, υπήρχαν και άλλα διαδικτυακά νομίσματα, αλλά κανένα δεν μπόρεσε να επιβιώσει ή να εδραιωθεί στις χρηματοπιστωτικές αγορές. Το Bitcoin.org κατακυρώθηκε το 2008 και παραμένει μέχρι και σήμερα. Στις 31 Οκτωβρίου του ίδιου έτος ένα άτομο ή ένας οργανισμός που χρησιμοποιούσε το όνομα Satoshi Nakamoto δημοσίευσε μια επιστημονική εργασία με τίτλο Bitcoin: A Peer to Peer Electronic Cash System ( Bitcoin: Ένα Ομότιμο Σύστημα Ηλεκτρονικών Μετρητών). Το έγγραφο αυτό έγινε γνωστό ως η «η Λευκή Βίβλος του Satoshi». Το Bitcoin περιεγράφηκε ως ένας ψηφιακός πόρος ανοιχτού κώδικα. Ο όρος «ανοιχτός κώδικας» σήμαινε ότι κανείς δεν τον κατείχε και ότι όλοι μπορούσαν να συμμετέχουν στην χρήση και την ανάπτυξή του[29].

Το 2009 το λογισμικό του Bitcoin έγινε διαθέσιμο προς όλους για πρώτη φορά. Ο Satoshi Nakamoto εξόρυξε τα πρώτα 50 Bitcoin, ξεκινώντας έτσι την πρακτική εξόρυξης κρυπτονομισμάτων. Ήταν η εποχή που μόνο λίγοι προγραμματιστές συμμετείχαν στην ανάπτυξη αυτού και πίστευαν ότι μία μέρα θα θεωρούνταν πρωτοποριακή τεχνολογία[29].

Το 2010 δεν είχε αποδοθεί καμία πραγματική αξία στο Bitcoin. Η πιο διάσημη ιστορία είναι αυτή του Laszlo Hanyecz που αγόρασε 2 πίτσες για 10.000 Bitcoin. Αυτήν αναγνωρίστηκε ως η πρώτη συναλλαγή. Έγραψε για κάποιες λεπτομέρειες σχετικά με την πιο πρόσφατη έκδοση του λογισμικού, αλλά μετά δεν υπάρχει καταγεγραμμένο κανένα ίχνος του[29].

Στον απόηχο της τεχνολογίας του Bitcoin, η ιδέα των αποκεντρωμένων ψηφιακών νομισμάτων άρχισε να εδραιώνεται. Ως αποτέλεσμα, εμφανίστηκαν τα πρώτα altcoins[29].

Το 2013 που η τιμή έφτασε τα 100$ ήταν σημαντικό ορόσημο ακόμα και αν η τιμή του έπεσε απότομα. Οι περισσότεροι χρήστες πραγματοποίησαν τεράστιες απώλειες[29].

Το 2014 το μεγαλύτερο ανταλλακτήριο κρυπτονομισμάτων στην αγορά με το όνομα Mt. Gox παραβιάστηκε. Οι επικριτές είπαν ότι επειδή τα κρυπτονομίσματα βασίζονται στην ανωνυμία και την αποκέντρωση, δεν ήταν περίεργο ότι παραβιάστηκε και ότι οι χάκερ ήταν αδύνατο να εντοπιστούν[29].

Το 2015 η αρμόδια για τα παράγωγα αμερικανική υπηρεσία Commodity Futures Trading Commission, ορίζει το Bitcoin ως «παράγωγο» το οποίο εμπίπτει στις αρμοδιότητές της[29].

Το 2017 ο αριθμός των ανταλλακτηρίων μεγάλωσε, κάνοντας πιο εύκολη την αγορά και την πώληση Bitcoin. Τα ICOs επίσης εκτινάχθηκαν. Όλα αυτά συνέλαβαν στην ταχεία ανάπτυξη του οικοσυστήματος, φτάνοντας την τιμή των 20.000$[29].

Το 2018 η ανάπτυξη της αγοράς δεν ήταν βιώσιμη, επομένως εκ των υστέρων η φούσκα έσκασε και οι τιμές άρχισαν μία σταδιακή πτώση[29].

Τον Ιανουάριο του 2020 το CME ξεκινά τη διαπραγμάτευση options σε συμβόλαια Bitcoin. Τον ίδιο χρόνο η ανταμοιβή των εξορύκτες πέφτει από τα 12,5 στα 6,25 Bitcoin[30].

Τον Σεπτέμβριο του 2021 το Bitcoin αναγνωρίζεται ως επίσημο νόμισμα στο El Salvador και μετά από αρκετές προσπάθειες, η SEC δίνει το πράσινο φως για το πρώτο ETF σε Bitcoin. Το ίδιο έτος το Bitcoin καταγράφει το ιστορικό υψηλό, φτάνοντας στα 68.990 δολάρια[30].

## 3.2 Τι Είναι Το Bitcoin

Το Bitcoin είναι ένα ψηφιακό νόμισμα χαρακτηρίζεται ως ένα σύστημα πληρωμών, δίχως φυσική μορφή. Οι χρήστες πραγματοποιούν συναλλαγές μεταξύ τους δίχως την διαμεσολάβηση κάποιας κεντρικής αρχής και όλες οι συναλλαγές είναι καταχωρημένες και διαθέσιμες προς όλο το δίκτυο. Το σύστημα αυτό ονομάζεται Blockchain[39].

Το Bitcoin είναι ένα peer to peer σύστημα πληρωμών και ένα ψηφιακό συνάλλαγμα ανοιχτού κώδικα. Ανήκει στην κατηγορία κρυπτονομισμάτων, αφού χρησιμοποιεί μεθόδους κρυπτογραφίας για την δημιουργία και διαχείριση των χρημάτων καθώς και την επιβεβαίωση της εγκυρότητας των συναλλαγών. Όλο αυτό βέβαια έχει δημιουργηθεί και βασίζεται σε μία γερή βάση δεδομένων η οποία είναι δημόσια. Είναι με λίγα λόγια ένα αποκεντρωμένο νόμισμα, στο οποίο όποιος χρήστης εμπλέκεται άμεσα με αυτό έχει τις ίδιες δυνατότητες με οποιονδήποτε άλλον[39].

Συγκεκριμένα αποτελείται από δίκτυο πληρωμών το οποίο είναι παρόμοιο με τα μέχρι σήμερα συμβατικά δίκτυα πληρωμής. Η διαφορά του Bitcoin από τα αυτά είναι στην αποκέντρωση και στην αποφυγή των διπλών δαπανών. Επιπλέον, τα δίκτυα πιστωτικών καρτών ανήκουν σε κερδοσκοπικές εταιρείες και η διαχείριση γίνεται προς όφελος των μετόχων[39].

## 3.3 Τα Πλεονεκτήματα του Bitcoin

Η γρήγορη μεταβίβαση κεφαλαίων που αποτελεί ένα βασικό πλεονέκτημα του Bitcoin γίνεται σχετικά γρήγορα και αποτελεσματικά, διότι δεν υπάρχει κάποια αρχή να το «εγκλωβίσει» και να υπάρχουν καθυστερήσεις στις συναλλαγές. Συμβάλει επίσης στην παραγωγικότητα, αφού δεν υπάρχουν συνοριακοί φραγμοί και γίνεται ελεύθερη ροή κεφαλαίων. Επιπλέον, οι συναλλαγές γίνονται άμεσα, με χαμηλό κόστος και μεγάλη ευκολία, σε αντίθεση με τον υπόλοιπο κόσμο που βασίζονται στην αποστολή εμβασμάτων, τα οποία απαιτούν κάποια συγκεκριμένη χρονική διάρκεια εκτέλεσης. Πέραν των κατά την αποστολή ή την παραλαβή υπάρχει ένα σχετικά μεγάλο τέλος συναλλαγής του χρηματοπιστωτικού ιδρύματος. Αντίθετα, στο δίκτυο του Bitcoin η μεταφορά γίνεται σε μικρότερο χρόνο και με ένα πολύ μικρό κόστος σχετικά με τα χρηματοπιστωτικά τέλη[31].

Η διαφάνεια των συναλλαγών είναι από τα πιο βασικά πλεονεκτήματα. Όπως έχει αναφερθεί στο δημόσιο αρχείο συναλλαγών καταγράφονται όλες οι συναλλαγές και επιβεβαιώνονται, δίνοντας την δυνατότητα κάθε επενδυτής να ελέγξει όποια συναλλαγή επιθυμεί[32].

Ο έλεγχος του χρήστη επίσης είναι ένα πλεονέκτημα το οποίο προστατεύει τον χρήστη από την παραβίαση του προσωπικού λογαριασμού του. Ο ιδιοκτήτης μπορεί να εκτελεί συναλλαγές εντός αυτού εφόσον έχει παραμείνει μυστικό το ιδιωτικό κλειδί από τρίτους. Έτσι, η μεταφορά τα μέλη γίνεται μόνο κάτω από συγκεκριμένες συνθήκες[32].

Ο κάθε χρήστης μπορεί να κατέχει περισσότερες από μία διευθύνσεις ώστε να εκτελεί τις συναλλαγές του. Η ιδιωτικότητα των λογαριασμών βασίζονται σε ψευδώνυμα, τα οποία μπορεί να μην συνδέονται με τα προσωπικά στοιχεία του χρήστη, αν και το σύστημα μπορεί να τους συγκρίνει και τους αναγνωρίσει βάση κάποιων χαρακτηριστικών. Έτσι οι συναλλαγές δεν είναι απόλυτα ανώνυμες, αφού και αυτές δημοσιεύονται. Η διαδικασία αυτή δεν μπορεί να καλύψει περιπτώσεις παρανομίας, καθώς το σύστημα καταγράφει μόνιμα τις συναλλαγές μέσω ηλεκτρονικών πορτοφολιών και είναι διαθέσιμες σε όλο το κοινό[33].

Επιπλέον, δεν υπάρχει καμία κεντρική αρχή που να ελέγχει το δίκτυο του Bitcoin. Έτσι οι χρήστες καταφεύγουν σε αυτόν τον τρόπο επένδυσης, ώστε να αποστασιοποιούνται από κρατικές παρεμβάσεις και ρυθμίσεις και να μην επηρεάζονται άμεσα από την πολιτική διαφθορά. Τα εθνικά νομίσματα σε αντίθεση, συνδέονται και στηρίζονται πλήρως από κυβερνητικές πολιτικές, ώστε να ενισχύονται ή όχι[34].

Ένα από το πιο σημαντικά, αν όχι το πιο σημαντικό χαρακτηριστικό του Bitcoin είναι ότι έχει καθορισμένο αριθμό και είναι αποπληθωριστικό. Σε περιόδους πληθωρισμού η αξία του χρήματος μεταβάλλεται συνεχώς και εμφανίζεται σε όλα τα αγαθά και υπηρεσίες. Οι κεντρικές τράπεζες που τα εκδίδουν, μπορούν να μεταβάλουν την αξία του. Για να μείνει σταθερή η τιμή θα πρέπει ένα μέρος του νομίσματος να ισούται με την ποσότητα των αγαθών. Το δίκτυο του Bitcoin συνδέεται μόνο με το πόσο οι χρήστες είναι διατεθειμένοι να το χρησιμοποιήσουν στις συναλλαγές. Η παροχή του Bitcoin στο peer to peer δίκτυο του, έχει οριστεί βάση πρωτοκόλλου[35].

## 3.4 Τα Μειονεκτήματα Του Bitcoin

Ένα από τα μειονεκτήματα είναι η κυριαρχούσα άποψη ότι αποτελεί μία κακή προσπάθεια αντικατάστασης του παραδοσιακού χρήματος. Αυτό συμβαίνει γιατί οι συμμετέχοντες δεν έχουν εξοικειωθεί με την τεχνολογία αυτή και το συνδέουν με το ξέπλυμα χρήματος, τρομοκρατία και άλλα αρνητικά[35].

Μετά από 13 χρόνια από την δημιουργία του το Bitcoin δεν αποτελεί σημαντική επιλογή στον κόσμο. Η πορεία του δείχνει όμως ότι όλο και περισσότεροι ασκούν ενδιαφέρον και επενδύουν, αυξάνοντας και έτσι την δυναμική του. Οι μεγάλες και ανά τακτά χρονικά διαστήματα αυξομειώσεις τις τιμής του όμως, προκαλεί την αποστασιοποίηση πολλών[35].

Η αστάθεια στην τιμή του, απομακρύνει κάποιους επενδυτές, διότι δεν μπορούνε να διασφαλίσουν σε αυτό το επενδυτικό προϊόν τα κεφάλαιά τους. Με την πάροδο των χρόνων το μερίδιό του στην αγορά θα αυξάνεται, μειώνοντας την αστάθεια και κάνοντάς το πιο ευρέως αποδεκτό[35].

Επιπλέον, το ασαφές νομοθετικό πλαίσιο που διακατέχει αποτελεί ένα μειονέκτημα για τους επενδυτές. Η μη σαφής ύπαρξη νομοθετικού πλαισίου συμβάλει στην χρήση χωρίς περιορισμούς. Η μόνη δημόσια έκθεση είναι αυτή της Ευρωπαϊκής Κεντρικής Τράπεζας που αναφέρεται στην δημιουργία του και στον τρόπο λειτουργείας[35].

Στο κομμάτι της συνεχής ενημέρωσης, εννοείται κατά κύριο λόγο η αυξομείωση των τιμών που δέχεται γιατί μπορεί να κυμανθεί από ένα μικρό ποσοστό % ως της τάξης του 50% σε λίγες μέρες. Αυτό αποδεικνύει ότι δεν είναι ένα περιοδικό φαινόμενο αλλά ένα συνεχές[35].

Όπως έχει αναφερθεί παραπάνω, ένας χρήστης μπορεί να έχει πάνω από έναν λογαριασμό με εικονικά στοιχεία. Πάνω σε αυτό συνδέθηκαν οι εγκληματικές δραστηριότητες άμεσα με το ψηφιακό νόμισμα. Βέβαια μεγάλο μέρος των κινήσεων έχουν ως σκοπό και την φοροδιαφυγή. Όπως για παράδειγμα το σκάνδαλο με την εταιρεία Silkroad, που εμπορευόταν παράνομα ναρκωτικά σε όλο τον κόσμο και δέχονταν πληρωμές μόνο με Bitcoin[33].

Το Bitcoin σύμφωνα με τα παραπάνω μπορεί να χρησιμοποιηθεί ως μέσο παράκαμψης του πληθωρισμού και των διεθνών κυρώσεων. Σε χώρες με υψηλό πληθωρισμό το χρησιμοποιούν σαν εναλλακτική λύση έναντι στο εθνικό τους νόμισμα. Το γεγονός όμως ότι πολλοί πολίτες αγόραζαν μέσω πιστωτικής κάρτας οδήγησε σε μία κατάσταση μη εξυπηρέτησης των χρεών, αφού όπως αναφέρθηκε δεν ήταν έτοιμοι για μία μεγάλη ποσοστιαία αυξομείωση. Αν όντως τελικά το Bitcoin είναι μία φούσκα, η οποία κάποια στιγμή θα είναι μη

διατηρήσιμη, το μόνο σίγουρο είναι ότι θα αφήσει πίσω του μια καινοτόμα τεχνολογία συναλλαγών[33].

## 3.5 Πως Λειτουργεί Το Bitcoin

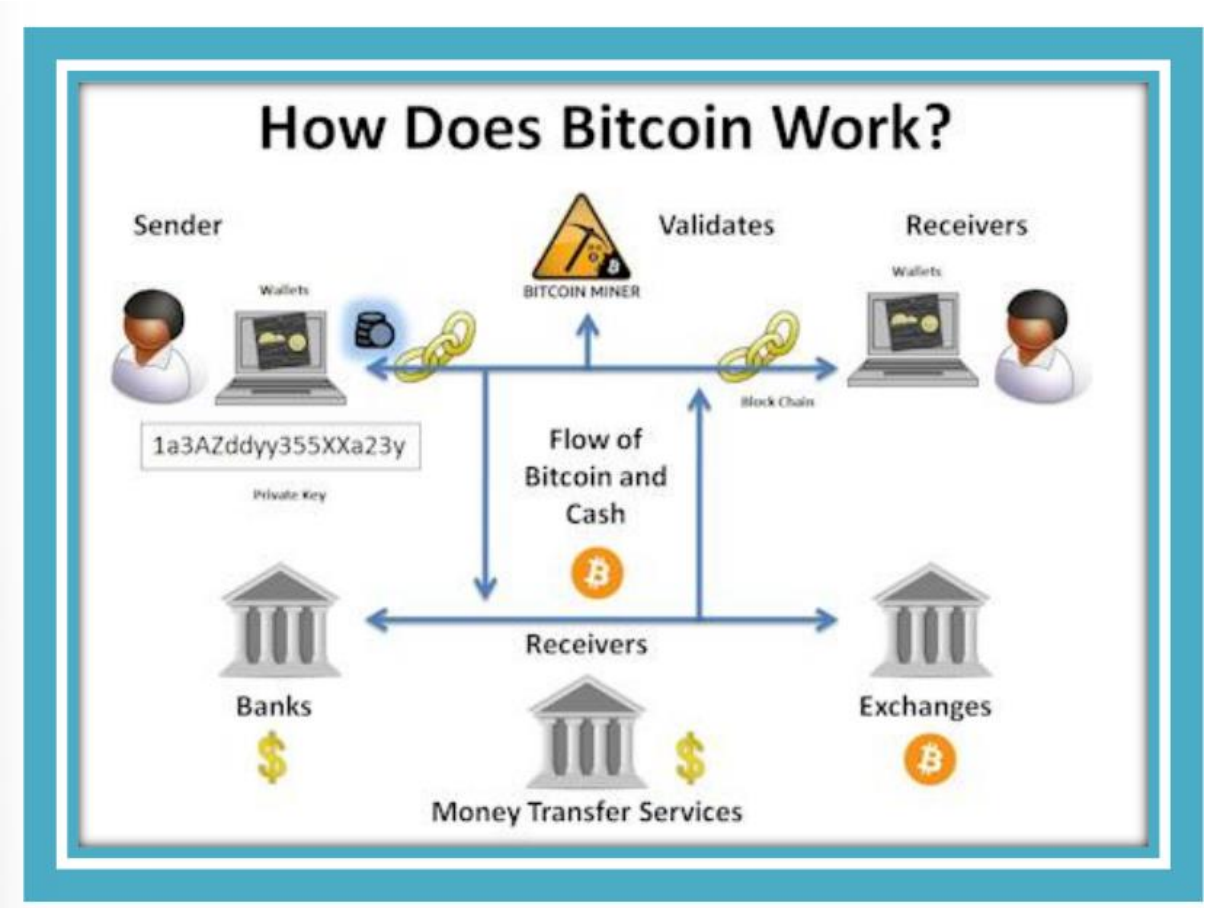
Η τεχνολογία του Bitcoin επιτρέπει τους χρήστες να κάνουν συναλλαγές πολύ εύκολα σαν να στέλνουν ένα μήνυμα. Για να κάνουν συναλλαγές χρησιμοποιούν μία εφαρμογή ηλεκτρονικού πορτοφολίου. Η χρόνος συναλλαγής είναι μηδενικός και ο χρήστης ειδοποιείται κατευθείαν.

Το Bitcoin σε ένα βασικό επίπεδο είναι ένα απλό ψηφιακό αρχείο που μέσα του περιέχει λογαριασμούς και ονόματα, έτσι όποιος θέλει να κάνει μία συναλλαγή τροποποιεί απλά αυτό το αρχείο(συστοιχία). Η κυβερνητική αρχή είναι απούσα. Το σύστημα του Bitcoin εξασφαλίζει ότι κανένας χρήστης δεν μπορεί να χρησιμοποιήσει νομίσματα που ανήκουν σε άλλο χρήστη. Σε κάθε συναλλαγή το ηλεκτρονικό πορτοφόλι αποστέλλει ένα μήνυμα στο δίκτυο του Bitcoin περιγράφοντας πως το αρχείο πρέπει να αλλάξει, συμπεριλαμβάνοντας τον αριθμό των λογαριασμών του αποστολέα και του παραλήπτη όπως και το ποσό που θα μεταφερθεί. Για την αποτροπή της δημιουργίας και της αποστολής μηνύματος από άλλους, εφαρμόζεται η ηλεκτρονική υπογραφή που χρησιμοποιεί το σύστημα σε κάθε αποστολή μηνύματος. Έτσι αποδεικνύεται η πραγματική ταυτότητα του λογαριασμού του χρήστη. Εξυπηρετεί τον ίδιο σκοπό με την κανονική υπογραφή, άλλα βασίζεται σε πολλά περισσότερα. Η τεχνολογία της κρυπτογράφησης δίνει την λύση με πολύ εμφατικό τρόπο, χρησιμοποιείται για να «αποκρύψει» μηνύματα αλλά έχει αναπροσαρμοστεί για να αποδεικνύει την ταυτότητα του χρήστη. Κάθε λογαριασμός έχει το δικό του ιδιωτικό κλειδί που το γνωρίζει μόνο ο κάτοχος του και χρησιμοποιείται για την δημιουργία των ψηφιακών υπογραφών, κρυπτογραφώντας τα μηνύματα της συναλλαγής. Ο παραλήπτης με την σειρά του αποκρυπτογραφεί τα μηνύματα αυτά και μπορεί να αποκαλύψει ποιος είναι ο αποστολέας. Επιπλέον, οι ψηφιακές υπογραφές δεν μπορούν να αντιγραφούν γιατί είναι μοναδικές για κάθε συναλλαγή. Έτσι με τις ψηφιακές να κρατάνε τις συναλλαγές, το ψηφιακό αρχείο δεν μπορεί να αλλάξει.

Το Bitcoin προσφέρει ένα αποκεντρωμένο σύστημα που ο καθένας μπορεί να ελέγχει τις υπογραφές και γενικά όλο το ψηφιακό αρχείο. Επομένως, όταν μία συναλλαγή εκτελείται από έναν χρήστη, ένα μήνυμα έρχεται σε όλους όσους επιθυμούν να βοηθήσουν στην διατήρηση του ψηφιακού αρχείου, δηλαδή στους «εξορύκτες». Ένα προσωπικό αντίγραφο του

ψηφιακού αρχείου κρατάει στην διάθεσή του κάθε «εξορύκτη» και όταν παραλαμβάνει ένα μήνυμα με μία νέα συναλλαγή το ενημερώνει, με την προϋπόθεση πάντα ότι υπάρχει έγκυρη ψηφιακή υπογραφή. Φυσικό είναι βέβαια και να υπάρχει μια καθυστέρηση στο δίκτυο, με τόσα πολλά ψηφιακά αρχεία διασκορπισμένα σε όλον τον κόσμο, που μπορεί να οδηγήσει σε διαφορές μεταξύ τους. Αυτό βέβαια είναι ένα σημαντικό πρόβλημα, γιατί είναι απαραίτητο να υπάρχει η ίδια ενημέρωση παντού. Έτσι, τα άτομα που βοηθάνε στην συντήρηση προσπαθούν να λύσουν ένα puzzle. Ο πρώτος που θα ανακοινώσει την λύση ανταμείβεται και οι υπόλοιποι ενημερώνουν το ψηφιακό αρχείο τους στην συγκεκριμένη έκδοση. Όσα περισσότερα άτομα εργάζονται πάνω στην ίδια έκδοση τόσο πιο γρήγορα θα βρούνε την λύση. Η διαδικασία αυτή επαναλαμβάνεται συνεχώς γιατί οι συναλλαγές γίνονται με μεγάλη συχνότητα[35].

*Εικόνα 12-Γραφική απεικόνιση της λειτουργείας μιας συναλλαγής με Bitcoin.*




## 3.6 Πως Πραγματοποιούνται Οι Συναλλαγές

Μια συναλλαγή δημιουργείται όταν γίνεται αποστολή μιας ποσότητας Bitcoin από έναν χρήστη σε έναν άλλον, ο οποίος επιθυμεί να δεχτεί Bitcoin ως μέσο πληρωμής αντί για συμβατικά νομίσματα. Και οι δύο χρήστες έχουν δημιουργήσει τα ηλεκτρονικά τους πορτοφόλια σε έναν υπολογιστή. Τα ηλεκτρονικά πορτοφόλια παρέχουν πρόσβαση σε πολλαπλές διευθύνσεις Bitcoin και η κάθε διεύθυνση είναι μία σειρά από γράμματα και αριθμούς όπως για παράδειγμα GHF12FGJLGFKRFK21565, έχοντας συγκεκριμένη ποσότητα[36].

Για τον χρήστη-αγοραστή που θα στείλει τα χρήματα, ο χρήστης που θα δεχτεί την πληρωμή δημιουργεί μια καινούργια διεύθυνση. Ο χρήστης στην ουσία παράγει ένα «ζεύγος κλειδιών κρυπτογράφησης», που αποτελείται από ένα δημόσιο και ένα ιδιωτικό κλειδί. Η νέα αυτήν διεύθυνση που παρέχει ένα ιδιωτικό κλειδί το οποίο αποθηκεύεται στο ηλεκτρονικό πορτοφόλι του χρήστη και ένα δημόσιο κλειδί που δημιουργείται ώστε να επαληθεύσει σε οποιοδήποτε ότι ένα υπογεγραμμένο μήνυμα με το ιδιωτικό κλειδί είναι και έγκυρο. Ο χρήστης-αγοραστής έτσι μεταβιβάζει το ποσό στην διεύθυνση του άλλου χρήστη-συμβαλλόμενου[36].

Το πορτοφόλι του κάθε χρήστη κρατά το ιδιωτικό κλειδί για κάθε μία από τις διευθύνσεις. Έτσι το πρόγραμμα που θα χρησιμοποιήσει υπογράφει την αίτηση της συναλλαγής με το ιδιωτικό κλειδί της διεύθυνσης στο οποίο μεταφέρουν και τα Bitcoin. Ο καθένας στην συγκεκριμένη περίπτωση μπορεί να χρησιμοποιήσει το δημόσιο κλειδί για διαπιστώσει αν η πραγματικά η συναλλαγή προέρχεται από νόμιμο ιδιοκτήτη λογαριασμού αλλά και για την επαλήθευση της συναλλαγής. Έτσι ολοκληρώνεται η διαδικασία πραγματοποίησης μίας συναλλαγής[36].

## 3.7 Επαλήθευση Των Συναλλαγών

Η ομάδα που είναι υπεύθυνη για την επαλήθευση και την εγκυρότητα των συναλλαγών ονομάζονται «εξορύκτες». Οι συναλλαγές των τελευταίων 10 λεπτών συνδέονται μέσω των υπολογιστών τους και καταλήγουν σε μία νέα συστοιχία συναλλαγής. Οι «εξορύκτες» έχουν ρυθμίσει τους υπολογιστές τους για να υπολογίζουν «κρυπτογραφικές συναρτήσεις κατακερματισμού»(hash).

### 3.7.1 Κρυπτογραφικά Hash

Οι συναρτήσεις αυτές των κρυπτογραφικών hash μετατρέπουν μία συλλογή από δεδομένα σε μία αλφαριθμητική λέξη σταθερού μήκους που ονομάζεται τιμή κατακερματισμού με βασική προϋπόθεση, ότι η έξοδος της συνάρτησης κατακερματισμού να ξεκινά με έναν συγκεκριμένο αριθμό μηδενικών για να επαληθευτεί η συναλλαγή. Η τιμή κατακερματισμού αλλάζει με την ελάχιστη αλλαγή στα αρχικά δεδομένα. Έτσι γίνεται αντιληπτό ότι η πρόβλεψη για το ποιο σύνολο από τα αρχικά δεδομένα δημιούργησε μια συγκεκριμένη τιμή κατακερματισμού είναι αδύνατη[37].

*Εικόνα 13-Κρυπτογραφικά Hash για μετατροπή δεδομένων σε αριθμητικές λέξεις.*


### 3.7.2 Nonces

Το Bitcoin χρησιμοποιεί τα Nonces για να δημιουργήσουν διαφορετικές τιμές hash από τα ίδια δεδομένα. Ένα Nonces είναι απλά ένας τυχαίος αριθμός που προστίθεται στα δεδομένα πριν την τιμή κατακερματισμού(hashing). Η τιμή hash αλλάζει, μεταβάλλοντας το nonces. Οι πληροφορίες σχετικά με όλες τις προηγούμενες συναλλαγές που έγιναν στο Bitcoin, παρέχονται σε κάθε νέα τιμή κατακερματισμού. Βασιζόμενοι σε έναν συνδυασμό της προηγούμενης τιμής (hash) στη νέα συστοιχία συναλλαγών, οι υπολογιστές εξόρυξης (mining)

υπολογίζουν νέες τιμές (hash). Οι «εξορύκτες» είναι αδύνατο να προβλέψουν ποια nonces θα παράγουν μια τιμή[38].

Έτσι έχει προέλθει η ολοκλήρωση και η επαλήθευση της συναλλαγής, δημοσιεύοντάς την αυτόματα στην αλυσίδα των συστοιχιών(blockchain). Οι «εξορύκτες» προσπαθούν επανειλημμένα να επαληθεύσουν τις επόμενες συναλλαγές. Στην περίπτωση τροποποίησης κάποιων στοιχείων από τους χρήστες, θα πρέπει να επαναληφθεί η επαλήθευση καθώς, απαιτείται ένα διαφορετικό nonce και θα πρέπει να επαναλάβουν την διαδικασία επαλήθευσης, πράγμα που είναι αδύνατο. Η κάθε συστοιχία συναλλαγών που επιλύουν οι «εξορύκτες» περιλαμβάνει και την αμοιβή συμμετεχόντων, βάση της υπολογιστικής ισχύς που πρόσφεραν. Η αμοιβή αυτή ξεκίνησε από τα 50 Bitcoin και υποδιπλασιάζεται κάθε 4 χρόνια μετά το Halving Event [38].

## 3.8 Το Bitcoin Σε Τεχνικό Επίπεδο

Το Bitcoin αποτελεί ένα λογισμικό ανοιχτού κώδικα (open source protocol). Οποιοσδήποτε μπορεί να ελέγξει τις λεπτομέρειες λειτουργείας του, με τον πηγαίο κώδικα του λογισμικού να είναι διαθέσιμος και δημόσιος. Η ανωτέρω αρχή δίνει την δυνατότητα στον καθένα να αντιγράψει τον πηγαίο κώδικα και να αναπτύξει το δικό του λογισμικό. Σε όλες τις χώρες το λογισμικό είναι δωρεάν και δεν υπάρχει κανένας περιορισμός ως προς την χρήση. Η κύρια λειτουργεία του λογισμικού στοχεύει στην μετάδοση των πληροφοριών ανάμεσα στους κόμβους, την πραγματοποίηση των συναλλαγών αλλά και την ενημέρωσή τους για όλο το δίκτυο. Βάση των προγραμματιστών που έχουν δημιουργήσει συναινετικά τα συστατικά στοιχεία του λογισμικού, ενσωματώνοντας από άλλα λογισμικά ανοιχτού κώδικα διαθέσιμες καινοτομίες, αλλά και στοιχεία νέα που ήταν άγνωστα πριν. Οι χρήστες αποδέχονται και εξασφαλίζουν την ισχύ του δικτύου. Η πεποίθηση των χρηστών αποτελείται από την ικανότητα ανταλλαγής πληροφοριών με εγκυρότητα ανεξαρτήτως αποδέκτη εντός του δικτύου, την περιορισμένη και την πεπερασμένη ποσότητα Bitcoins. Έτσι, δημιουργούνται οι βασικές προδιαγραφές για ένα δίκτυο ανταλλάξιμης αξίας. Η αξία που είναι διατεθειμένοι οι χρήστες να τα αλλάξουν πηγάζει από την αξία που βρίσκουν οι ίδιοι και αντανακλάται σε αυτό, με την οποία να βασίζεται ακράδαντα στον νόμο της προσφοράς και της ζήτησης, χωρίς κεντρικές αρχές ενδιάμεσα[36].

Για να αποτελούν ένα μέσο συναλλαγής και να είναι χρήσιμα, πρέπει σταδιακά να μπαίνουν στην κυκλοφορία για την κάλυψη των συναλλαγματικών αναγκών, αλλά και να είναι καθορισμένος ο συνολικός αριθμός τους. Όλα αυτά επιτυγχάνονται τεχνητά και οι κανόνες που διέπουν το δίκτυο καθορίζουν τον ρυθμό παραγωγής και το μέγιστο πλήθος. Η παραγωγή θα φτάσει τον μέγιστο αριθμό των 21.000.000 και ρυθμός παραγωγής θα μειώνεται με τον χρόνο μέχρι το 2140, που στην συγκεκριμένη θα παραχθεί το τελευταίο. Η μέθοδος αυτή αντανακλά την διάθεση του πολύτιμου μετάλλου του χρυσού στην παγκόσμια αγορά. Η εξόρυξή του στα αρχικά στάδια είναι εύκολη και είναι σχετικά πιο προσβάσιμες οι μεγάλες ποσότητες. Προοδευτικά όμως γίνεται όλο και πιο σπάνιο, μέχρι να εξαντληθεί και το τελευταίο απόθεμα του πλανήτη[36].

### 3.8.1 Πως Δημιουργούνται Τα Bitcoins

Η παραγωγή των Bitcoins πραγματοποιείται μέσω της επίλυσης ενός δύσκολου και περίπλοκου μαθηματικού αλγορίθμου. Η μέθοδος αυτή ονομάζεται εξόρυξη ή «mining», το όνομα της οποίας προήλθε από τρόπο λειτουργείας των χρυσωρύχων του προηγούμενου αιώνα.

### 3.8.2 Τρόπος εξόρυξης (Mining)

Όπως αναφέρθηκε παραπάνω, στο δίκτυο του Bitcoin οι συναλλαγές που πραγματοποιούνται, επαληθεύονται πρώτα για την εγκυρότητα τους και στην συνέχεια αφού επαναληφθούν τοποθετούνται μέσα σε μία συστοιχία μαζί με τις υπόλοιπες που είναι ήδη επαληθευμένες. Η παραγωγή νέων συστοιχιών γίνεται κάθε δέκα λεπτά, τα οποία επαληθεύονται, τοποθετούνται το ένα διπλά στο άλλο και συσχετίζονται όλα μεταξύ τους. Η επίλυση του περίπλοκου μαθηματικού αλγόριθμου επιτυγχάνει τον συσχετισμό της προηγούμενης συστοιχίας με το καινούργιο[40].

Η επίλυση του μαθηματικού αλγόριθμου θα επιφέρει την δημιουργία της νέας συστοιχίας, αλλά και ενός συγκεκριμένου αριθμού νέων Bitcoins. Οι συγκεκριμένοι

ονομάζονται «εξορύκτες» και η διαδικασία που ακολουθήθηκε για να επιλύσουν τον αλγόριθμο και να γίνει ο συσχετισμός ονομάζεται εξόρυξη(mining)[40].

Επομένως, ανεξάρτητα από το πόσοι χρήστες προσπαθούν να βρουν την λύση, είναι προφανές ότι πρέπει η δυσκολία του γρίφου να τροποποιηθεί για να μπορεί να προκύπτει ανά δέκα λεπτά περίπου. Αυτό εξαρτάται από τον αριθμό των χρηστών που συμμετέχουν για επίλυση του αλγορίθμου και γίνεται αυτόματα από το δίκτυο. Έτσι, όσο περισσότερη επεξεργαστική ισχύ αντλείται, δηλαδή όσοι περισσότεροι χρήστες συμμετέχουν στην επίλυση του γρίφου, τόσο αυξάνεται η δυσκολία του κι αντίστροφα[40].

Επιπλέον, απαιτείται μεγάλη επεξεργαστική ισχύ για να γίνει «εξόρυξη»(mining). Αρχικά, τα πρώτα προγράμματα που έκαναν χρήση των επεξεργαστών των υπολογιστών και αυτό δημιουργούσε προβλήματα υπερθέρμανσης του υπολογιστή και απαίτησης ρεύματος, πράγμα που μείωνε το κέρδος των χρηστών. Στην συνέχεια, τα προγράμματα έκαναν χρήση των επεξεργαστών των καρτών γραφικών, οδηγώντας σε πιο γρήγορα αποτελέσματα. Αλλά όπως αναφέρθηκε όσοι πιο πολλοί οι χρήστες τόσο πιο δύσκολο να επιλυθεί ο γρίφος. Πλέον έχουν δημιουργηθεί συγκεκριμένες συσκευές που παράγουν πολύ μεγαλύτερη επεξεργαστική ισχύ από έναν υπολογιστή, η χρήση του οποίου είναι ασύμφορη, αφού η ενέργεια που καταναλώνει είναι πολύ μεγαλύτερη από τα μικροποσά των Bitcoin που θα παραχθούν[40].

### 3.8.3 Από Τι Εξαρτάται Η Δημιουργία τους

Η δημιουργία τους όπως αναφέρθηκε παραπάνω δεν εξαρτάται από την βούληση ενός κράτους ή οργανισμού, ούτε από την προσφορά ή ζήτηση για την δημιουργία λιγότερων ή περισσότερων νομισμάτων. Ο ρυθμός της δημιουργίας τους καθορίζεται από το ίδιο το δίκτυο. Το συγκεκριμένο χαρακτηριστικό το προστατεύει από τον μεγάλο θέμα του πληθωρισμού και άλλα προβλήματα κυβερνητικών νομισμάτων. Αν όμως ο αριθμός της κυκλοφορίας του ήταν άπειρος τότε η αξία του μέχρι τώρα θα ήταν σημαντικά μικρότερη. Για αυτό από την αρχή της δημιουργίας του έχει καθοριστεί και δεν μπορεί να αλλάξει ο τρόπος δημιουργίας του, για να μην παράγονται ανεξέλεγκτα και να παραμείνουν περιορισμένα ώστε να έχουν αξία. Η ανταμοιβή για την επίλυση μιας συστοιχίας μειώνεται στο μισό κάθε τέσσερα χρόνια.

# ΚΕΦΑΛΑΙΟ 4

# ΕΓΓΕΝΗΣ ΑΞΙΑ BITCOIN

Στόχος στο κεφάλαιο είναι η προσέγγιση της εγγενής αξίας του Bitcoin. Η μία είναι βάση των χαρακτηριστικών που εμφανίζουν τα κυβερνητικά νομίσματα και η άλλη βάση των χαρακτηριστικών του χρυσού ως μέσο αποθήκευσης αξίας.

Το Bitcoin συχνά θεωρείται ως το νέας γενιάς νόμισμα που θα αντικαταστήσει τα «χάρτινα» νομίσματα. Ωστόσο αυτού του είδους χρήματα έχουν αξία γιατί εκδίδεται από μια νομισματική αρχή και είναι ευρέως χρησιμοποιούμενα σε μία οικονομία. Το δίκτυο του Bitcoin είναι ανοιχτό και αποκεντρωμένο σε όλους τους τομείς.

Ορισμένοι συγκρίνουν την αξία του Bitcoin με του χρυσού. Η ποσότητα και των δύο είναι περιορισμένη και έχουν συγκεκριμένες χρησιμότητες. Ο χρυσός βέβαια είναι εδραίος χρησιμοποιούμενος στην βιομηχανία. Σύμφωνα με τον δημιουργό του που εξέδωσε το white paper, το Bitcoin θα μπορούσε υπό την προϋπόθεση κάποιον συνθηκών να χρησιμοποιηθεί στην λιανική.

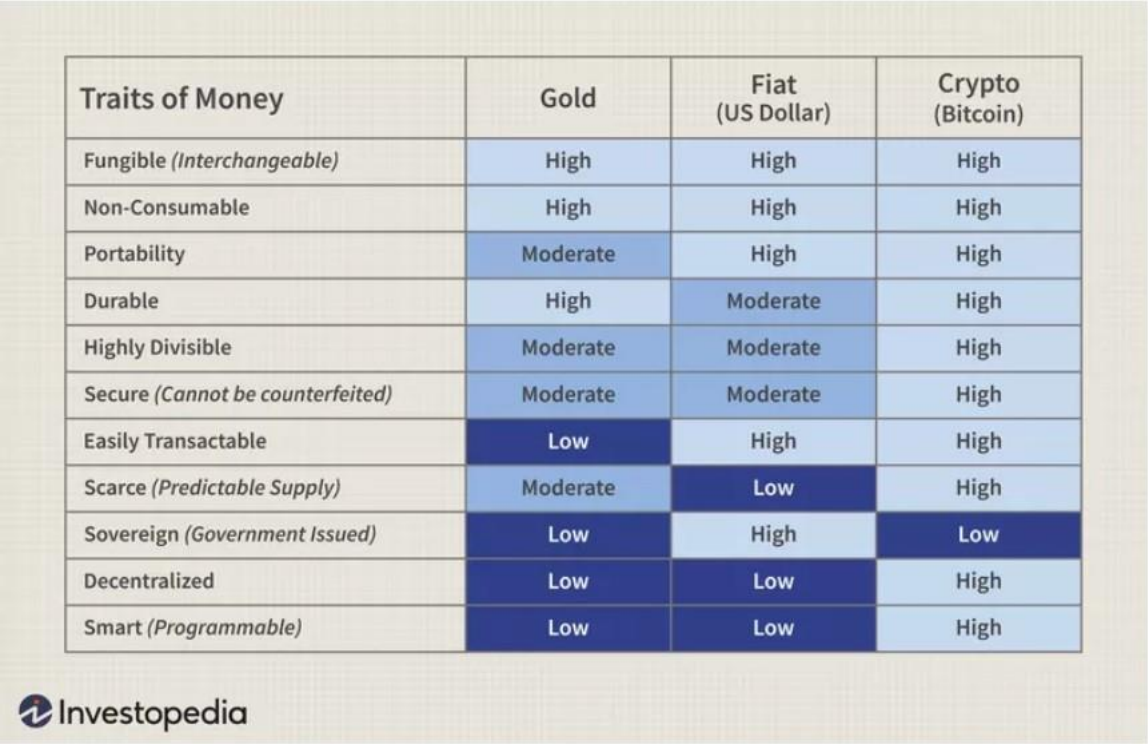
## 4.1 Η Αξία Του Bitcoin

Το Bitcoin δεν έχει την προστασία των κυβερνητικών αρχών, ούτε ένα σύστημα ενδιάμεσων τραπεζών για τη μετάδοση της χρήσης του. Ένα αποκεντρωμένο δίκτυο που αποτελείται από ανεξάρτητους κόμβους, είναι υπεύθυνο για την έγκριση των συναλλαγών, που βασίζονται στην συναίνεση στο δίκτυο του Bitcoin. Δεν υπάρχει καμία ρυθμιστική αρχή με τη μορφή μιας κυβέρνησης ή άλλης νομισματικής αρχής που να ενεργεί αντισυμβαλλόμενος, για να διασφαλίσει τους δανειστές σε περίπτωση ενός ανεπιθύμητου γεγονότος[55].

Ωστόσο, εμφανίζει ορισμένα χαρακτηριστικά ενός συστήματος εγχώριων νομισμάτων. Είναι σπάνιο και δεν μπορεί να παραποιηθεί. Μόνο η διπλή δαπάνη μπορεί να παραποιήσει

την έκδοση του Bitcoin. Αποτελεί την κατάσταση στην οποία ένας χρήστης μεταφέρει το ίδιο Bitcoin σε δύο ή περισσότερες διευθύνσεις που είναι ξεχωριστές μεταξύ τους, προκαλώντας μία διπλή εγγραφή[55].

*Εικόνα 14-Χαρακτηριστικά του χρήματος.*



| Traits of Money | Gold | Fiat (US Dollar) | Crypto (Bitcoin) |
|---|---|---|---|
| Fungible *(Interchangeable)* | High | High | High |
| Non-Consumable | High | High | High |
| Portability | Moderate | High | High |
| Durable | High | Moderate | High |
| Highly Divisible | Moderate | Moderate | High |
| Secure *(Cannot be counterfeited)* | Moderate | Moderate | High |
| Easily Transactable | Low | High | High |
| Scarce *(Predictable Supply)* | Moderate | Low | High |
| Sovereign *(Government Issued)* | Low | High | Low |
| Decentralized | Low | Low | High |
| Smart *(Programmable)* | Low | Low | High |

Investopedia

Ο λόγος πίσω από την αδυναμία επίτευξης της διπλής δαπάνης στο δίκτυο του Bitcoin είναι το μέγεθος του δικτύου του. Μία επίθεση 51%, προϋποθέτει ότι μία ομάδα «εξορύκτης» ελέγχει περισσότερο από το ήμισυ της συνολικής παραγωγής του δικτύου. Η ομάδα αυτή θα μπορούσε να παραποιήσει τις εγγραφές του δικτύου, αφού θα κατείχε την πλειοψηφία της συνολικής ισχύος του Bitcoin και θα μπορούσε να κυριαρχήσει και στο υπόλοιπο δίκτυο. Ωστόσο, μία τέτοια επίθεση χαρακτηρίζεται απίθανη γιατί θα απαιτούσε τεράστια υπολογιστική ισχύ και χρήματα[55].

Αλλά το Bitcoin χρησιμοποιείται σπάνια για συναλλαγές λιανικής και για αυτό τον λόγο αποτυγχάνει το τεστ χρησιμότητας. Η κύρια πηγή αξίας του είναι η περιορισμένη ποσότητά του. Το επιχείρημα για την αξία του Bitcoin είναι παρόμοιο με αυτό του χρυσού-ένα εμπόρευμα που μοιράζεται τα ίδια χαρακτηριστικά με ένα κρυπτονόμισμα. Το Bitcoin έχει μέγιστο αριθμό τα 21 εκατομμύρια[55].

Η αξία του Bitcoin είναι συνάρτηση της σπανιότητας. Καθημερινά η ζήτηση για ένα κομμάτι του Bitcoin αυξάνεται, καθώς η προσφορά μειώνεται. Το Bitcoin έχει περιορισμένη

χρησιμότητα, αντίθετα με τον χρυσός. Η τεχνολογία του Blockchain που χρησιμοποιεί δοκιμάζεται και χρησιμοποιείται ως σύστημα πληρωμών. Ένα σημαντικό αποτέλεσμα της χρήσης του είναι η εκτέλεση ενός διασυνοριακού εμβάσματος με γρήγορο χρόνο ανταπόκρισης και χαμηλό κόστος. Ορισμένες χώρες, όπως το Ελ Σαλβαδόρ, χρησιμοποιούν την τεχνολογία του και στοιχηματίζουν ότι θα εξελιχθεί τόσο, ώστε να γίνει ένα καθημερινό μέσο για συναλλαγές.

Το Bitcoin είναι πολύ πιο διαιρετό από τα κυβερνητικά νομίσματα, διότι μπορεί να διαχωριστεί έως και οκτώ δεκαδικά ψηφία, τα οποία ονομάζονται satoshis. Ο αριθμός των δεκαδικών ψηφίων των κυβερνητικών νομισμάτων έχει μέγιστο τα δύο δεκαδικά ψηφία για καθημερινή χρήση[55].

Με την πάροδο του χρόνου αν η τιμή του Bitcoin συνεχίσει την ανοδική πορεία, τότε οι χρήστες με ένα κλάσμα του θα μπορούν να πραγματοποιούν συναλλαγές. Η ανάπτυξη του Lighting Network για πιο γρήγορες και με λιγότερο κόστος συναλλαγές θα μπορεί να ενισχύσει την αξία του Bitcoin[55].

## 4.2 Οι Προκλήσεις Της Αποτίμησης Του Bitcoin

Το χρηματοπιστωτικό μας οικοσύστημα βρίσκεται ακόμη πολύ στη μέση της προσαρμογής ή της απόρριψης στο Bitcoin. Μία από τις προκλήσεις είναι η αποτίμηση του Bitcoin. Τι είδους πλαίσιο πρέπει να χρησιμοποιήσουμε συλλογικά για να δώσουμε αξία στο Bitcoin;

Αυτό οφείλεται εν μέρει στην ιστορική αστάθεια των τιμών του Bitcoin, καθιστώντας το λιγότερο από ιδανικό ως νόμισμα. Είναι δύσκολο να κάνεις τους ανθρώπους να αποδεχθούν ένα νόμισμα του οποίου η τιμή αγοράς μπορεί να πέσει κατακόρυφα την επόμενη μέρα. Ωστόσο, οι υποστηρικτές του Bitcoin συμφωνούν ότι οποιεσδήποτε διακυμάνσεις τιμών θα πρέπει να εξομαλυνθούν με την πάροδο του χρόνου μαζί με την υιοθέτηση της κύριας τάσης.

Θέματα ασφαλείας, όπως η κλοπή και η πειρατεία σε μη ρυθμιζόμενα ανταλλακτήρια και πορτοφόλια, αποθαρρύνουν επίσης τους χρήστες να συναλλάσσονται με Bitcoin. Αυτό θα πάρει χρόνο για να λυθεί καθώς ωριμάζει το κρυπτογραφικό οικοσύστημα. Εν τω μεταξύ, οι επενδυτές μπορούν να αντιμετωπίσουν αυτό το ζήτημα με αυστηρούς οικονομικούς κανονισμούς θεσμικού επιπέδου.

Ένα άλλο ζήτημα είναι ότι το Bitcoin πρέπει ακόμα να αξιολογηθεί ως χρήμα για να μπορέσουμε να το παρομοιάσουμε με χρυσό. Εάν δεν καταφέρουμε να καθορίσουμε την εγγενή νομισματική του αξία, τότε, όπως επισημαίνει η λευκή βίβλος της ΕΥ , δεν υπάρχει μεγάλη διαφορά στο Bitcoin από συλλεκτικά αντικείμενα όπως η τέχνη ή τα εκλεκτά κρασιά.

### 4.2.1 Αριθμητική Αποτίμηση Του Bitcoin

Αν το Bitcoin έχει πραγματική αξία, σημαντικό είναι να υπολογιστεί το ποσοστό που κατέχει στην αγορά. Μία αυθαίρετη τιμή που μπορούμε να ορίσουμε είναι 10%, τόσο ως μέσο αποθήκευσης αξίας όσο και ως νόμισμα.

Ένας τρόπος να το προσδιορίσουμε είναι να εξετάσουμε την τρέχουσα παγκόσμια αξία όλων των μέσων ανταλλαγής και αποθήκευσης που είναι συγκρίσιμα με το Bitcoin και να υπολογίσουμε την αξία του σε ποσοστό. Εδώ θα χρησιμοποιήσουμε το κρατικό χρήμα ως κυρίαρχο μέσο ανταλλαγής.

Απαραίτητο είναι να προσδιοριστούν τα μέσα με τα οποία θα γίνει. Αρχικά, το M1 είναι η προσφορά χρήματος σύμφωνα με τις καταθέσεις ρευστότητας και νόμισμα. Το M1 περιλαμβάνει τα ρευστότερα τμήματα της προσφοράς χρήματος επειδή περιέχει περιουσιακά στοιχεία και νόμισμα που μετατρέπονται γρήγορα σε μετρητά. Η κατηγοριοποίηση του M3 ορίζεται ως ένα ευρύτερο μέτρο της προσφοράς χρήματος μιας οικονομίας. Δίνει έμφαση στο χρήμα ως αποθήκη αξίας παρά ως μέσο ανταλλαγής. Επίσης περιλαμβάνει όλο το M1 στην τιμή του, το οποίο πρέπει να αφαιρεθεί για να προσδιοριστεί το μέσο αποθήκευσης αξίας[52].

Έτσι σύμφωνα με τα στατιστικά, η συνολική προσφορά χρήματος (M1) αξίζει σήμερα 48.9 τρισεκατομμύρια δολάρια, η οποία είναι η τρέχουσα παγκόσμια αξία των μέσων ανταλλαγής. Το M3 το οποίο αξίζει 83 τρισεκατομμύρια μείον το M1 υπολογίζεται στα 34.1 τρισεκατομμύρια. Σε αυτό θα προσθέσουμε την παγκόσμια αξία του χρυσού που χρησιμοποιείται ως μέσο αποθήκευσης αξίας[51].

Σύμφωνα με το Παγκόσμιο Συμβούλιο Χρυσού υπολογίζεται ότι από την αρχή της ανθρωπότητας μέχρι το 2010 είχαν εξορυχτεί 168.300 τόνοι χρυσού. Με την τρέχουσα τιμή να βρίσκεται στα 1980 δολάρια ανά ουγγία, η ποσότητα αξίζει περίπου 10 τρισεκατομμύρια δολάρια[53].

Το άθροισμα για την παγκόσμια αξία των μέσων ανταλλαγής και των αποθεματικών αξία ανέρχεται σύμφωνα με τα παραπάνω στα 93 τρισεκατομμύρια δολάρια. Αν το ποσοστό της αγοράς που έχει κατακτήσει το Bitcoin είναι 10%, τότε η τιμή επί τον συνολικό αριθμό των κυκλοφορούντων Bitcoin (κεφαλαιοποίηση) θα ανέλθει στα 9,3 τρισεκατομμύρια. Με τον πεπερασμένο αριθμό των Bitcoin να ανέρχεται στα 21 εκατομμύρια, η τιμή του ενός Bitcoin θα ήταν 443.000 δολάρια.

## 4.3 Αξιολόγηση Βάση Των Κυβερνητικών Νομισμάτων

Όπως αναφέρθηκε πολλοί υποστηρικτές του Bitcoin, το θεωρούν ως κάτι που υπερέχει απλά μία νέα επενδυτική μορφή, αλλά ως ένα προσβάσιμο σε όλους εργαλείο . Όπως και να έχει δεν εμπόδισε τους σκεπτικιστές να συζητούν τη χρήση του Bitcoin ως νόμισμα ή ως ένα εργαλείο που μπορούν να παρακάμψουν το σύγχρονο χρηματοπιστωτικό σύστημα.

### 4.3.1 Κυβερνητικά νομίσματα

Η εγγενής αξία ενός νομίσματος που έχει εκδοθεί από μία κυβέρνηση είναι εξαιρετικά αμφιλεγόμενη. Επειδή τα σημερινά νομίσματα δεν υποστηρίζονται πλέον από περιουσιακά στοιχεία, συχνά διατυπώνεται το επιχείρημα ότι τα κυβερνητικά νομίσματα δεν έχουν εγγενή αξία. Για παράδειγμα, το 1970 ένα χαρτονόμισμα των 10 δολαρίων αντιπροσώπευε μία απαίτηση σε χρυσό. Σήμερα τα 10 δολάρια είναι απλώς αγοραστική δύναμη που υποστηρίζεται από την πίστη της κυβέρνησης των ΗΠΑ και την αναγνώρισή της ως νόμιμο χρήμα[54].

Αντίθετα, η πεποίθηση είναι ότι η αξία προέρχεται από την διασφάλιση των κυβερνήσεων που τα εκδίδουν. Ως πλήρως λειτουργική και αξιόπιστη οντότητα, το μητρικό της νόμισμα λειτουργεί ως μέσο συναλλαγής, λογιστική μονάδα και ως αποθήκευση αξίας τόσο για τους πολίτες όσο και για άλλες κυβερνήσεις. Με απλά λόγια, η εγγενής αξία του κυβερνητικού νομίσματος βασίζεται στο γεγονός ότι μπορεί να χρησιμοποιηθεί για την ανταλλαγή αξίας και την αποθήκευση αξίας, επειδή άλλοι βλέπουν αξία σε αυτό. Πολλές

φορές, η εκδότρια κυβέρνηση του διαθέτει τα εργαλεία και τους μοχλούς, όπως δημοσιονομικές πολιτικές, έτσι ώστε η χρήση τους να είναι απαραίτητη από όλους[54].

Οι χώρες που μπορούν να αντιμετωπίσουν επαρκώς σοβαρές οικονομικές επιπτώσεις και ελκυστική οικονομική ανάπτυξη μπορούν να θεωρηθούν ως «ασφαλή καταφύγια», προσελκύοντας έτσι την ζήτηση για το νόμισμά τους από ιδιώτες, επιχειρήσεις και κυβερνήσεις. Τα επιτόκια μίας χώρας, η αύξηση του ΑΕΠ, το πλεόνασμα του εμπορικού ισοζυγίου και ο πληθωρισμός, είναι παράγοντες που οδηγούν την υγεία του έθνους και της οικονομίας του, επηρεάζοντας την αντιληπτή αξία του νομίσματος της χώρας. Με απλά λόγια, η δύναμη του «οικοσυστήματος» ενός κράτους ή μιας χώρας κάνει το εν λόγω νόμισμα πιο πολύτιμο εγγενώς[54].

### 4.3.2 Μέσο Αποθήκευσης Αξίας

Σύμφωνα με την άποψη ότι το Bitcoin είναι ένα μέσο αποθήκευσης αξίας, είναι πιο πιθανό να αποθηκεύσουμε το Bitcoin παρά να το ξοδέψουμε. Έτσι ένα μοντέλο όπως η Quantity Theory of Money – το οποίο βασίζεται σε ένα μοντέλο χρήματος που αλλάζει συχνά χέρια για την αγορά αγαθών και υπηρεσίιών, δεν θα λειτουργούσε[66].

Όσοι ενστερνίζονται την φιλοσοφία της αποθήκευσης αξίας, συγκρίνουν το Bitcoin έναντι της συνολικής αγοράς χρυσού, όπως η χρηματοπιστωτική εταιρεία 21Shares[66].

Στη μέθοδο αυτή, διαιρούμε την κεφαλαιοποίηση της αγοράς του χρυσού ( 10 τρισεκατομμύρια δολάρια) με τον συνολικό αριθμό Bitcoin σε κυκλοφορία (19.442.000) για να προσδιορίσουμε την τιμή ενός Bitcoin. Το αποτέλεσμα είναι περίπου 514.000 δολάρια[66].

Πολλοί δυσκολεύονται να φανταστούν ότι το μερίδιο αγοράς του Bitcoin θα φτάσει ποτέ στο ίδιο μέγεθος με αυτό του χρυσού.

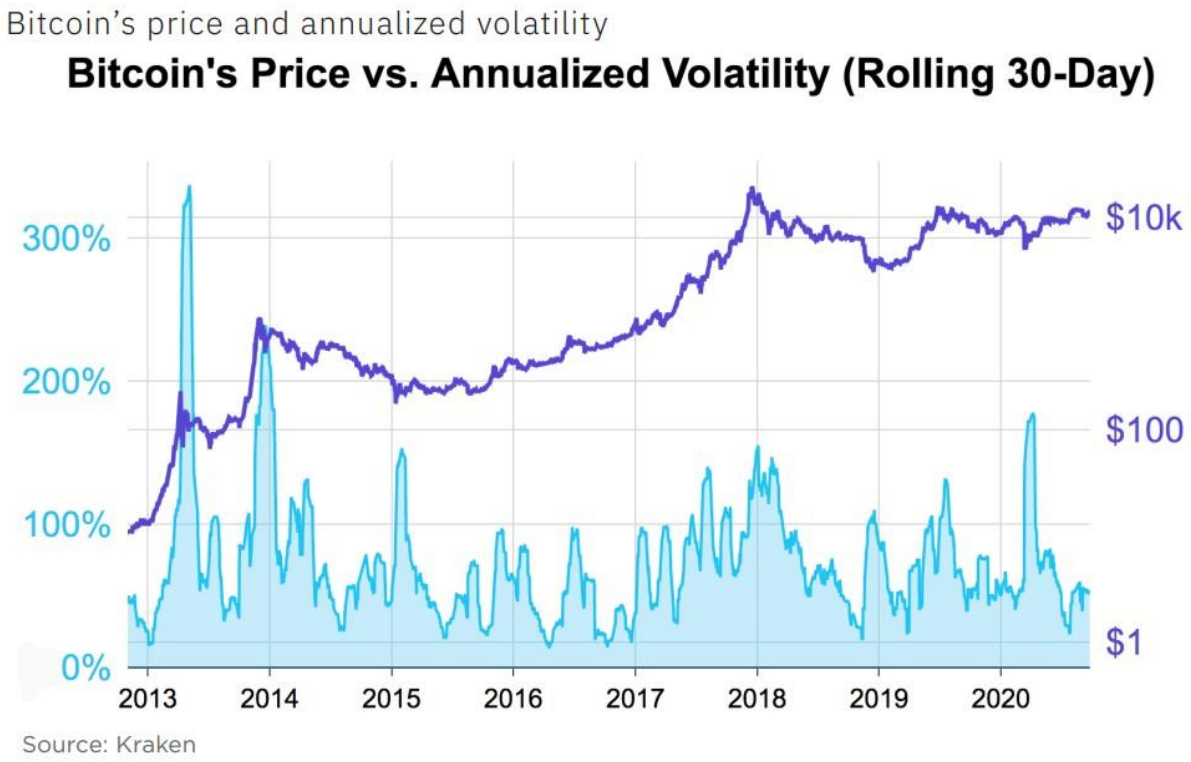
Επίσης, κάποιοι υποστηρίζουν ότι το Bitcoin δεν έχει εγγενή αξία επειδή δεν έχει όλες τις ιδιότητες ενός «πραγματικού» νομίσματος. Δηλαδή, το Bitcoin μπορεί να λειτουργεί ως λογιστική μονάδα και μέσο ανταλλαγής, αλλά δεν είναι ένα σταθερό μέσο αποθήκευσης αξίας. Οι σκεπτικιστές συνεχίζουν να υποστηρίζουν ότι η υπερβολική ευμετάβλητη φύση του Bitcoin υπονομεύει την ικανότητά του να είναι ένα μέσο αποθήκευσης αξίας και επομένως δεν πληροί και τα τρία κριτήρια ενός νομίσματος. Επιπλέον, υποστηρίζουν ότι όχι μόνο το Bitcoin δεν

μπορεί να κατατεθεί σε μία τράπεζα, αλλά ότι η σταθερή προσφορά ύψους 21 εκατομμυρίων δεν συνιστά βιώσιμο νόμισμα σε μία αναπτυσσόμενη οικονομία[54].

Όπως ανέφερε ο Paul Krugman: «Για να είναι επιτυχημένο, το χρήμα πρέπει να είναι και μέσο ανταλλαγής και εύλογα σταθερό απόθεμα αξίας. Και παραμένει εντελώς ασαφές γιατί το Bitcoin πρέπει να είναι ένα σταθερό μέσο αποθήκευσης αξίας… Είχα και συνεχίζω να έχω διάλογο με έξυπνους τεχνολόγους που είναι θετικοί στο Bitcoin-αλλά όταν προσπαθώ να τους κάνω να μου εξηγήσουν γιατί το Bitcoin είναι αξιόπιστο μέσο αποθήκευσης αξίας, φαίνεται ότι πάντα επιστρέφουν με εξηγήσεις σχετικά με το πως είναι ένα καταπληκτικό μέσο ανταλλαγής. Ακόμα κι αν το αγοράσω ( που δεν το κάνω εξ ολοκλήρου), δεν λύνει το πρόβλημά μου»[54].

Ωστόσο θα μπορούσε κανείς να υποστηρίξει ότι η αστάθεια του Bitcoin δεν αποτελεί εμπόδιο στον ισχυρισμό του ως αξιόπιστου μέσου αποθήκευσης αξίας, αλλά μοχλός της επιτυχίας και της υιοθέτησης του μέχρι σήμερα. Όπως φαίνεται στο παρακάτω σχήμα, η άνοδος του Bitcoin στην τρέχουσα θέση συνοδεύτηκε από μία σταδιακή, αλλά ουσιαστική, πτώση σε αστάθεια. Επιπρόσθετα, από τις 3.691 ημέρες που το Bitcoin έχει διαπραγματευτεί σε μία ανοιχτή αγορά, περίπου τις 3.494 ημέρες (94,7%) ήταν κερδοφόρες σε σχέση με την τιμή των 10.250$[54].

*Εικόνα 15-Τιμή Bitcoin vs Αστάθεια ανά χρόνο.*




### 4.3.3 Υποστηρίζει Τα Χαρακτηριστικά Του Χρήματος

Σύμφωνα με την Ομοσπονδιακή Τράπεζα των ΗΠΑ του St. Louis, μία από τις 12 περιφερειακές αποθεματικές τράπεζες που αποτελούν την Κεντρική Τράπεζα των ΗΠΑ, η ανθεκτικότητα, η φορητότητα, η διαιρετότητα, η ομοιομορφία, η περιορισμένη προσφορά και η αποδοχή είναι τα εφτά χαρακτηριστικά του χρήματος. Για πολλούς λόγους, πολλοί υποστηρικτές του Bitcoin πιστεύουν ακράδαντα ότι το Bitcoin πληροί όλα τα χαρακτηριστικά και επομένως είναι «σκληρό» χρήμα με πραγματική εγγενή αξία[54].

Ανθεκτικότητα

Το Bitcoin μπορεί να χαθεί αν σταλεί σε λάθος διεύθυνση ή εάν χαθούν τα ιδιωτικά κλειδιά. Αλλά δεν μπορεί να κα καταστραφεί και δεν είναι επιρρεπές σε φθορά. Επιπλέον, τα ιδιωτικά κλειδιά μπορούν να δημιουργηθούν εύκολα και χωρίς κόπο[54].

Φορητότητα

Επειδή το Bitcoin υπάρχει σε bits, οποιαδήποτε ποσότητα Bitcoin μπορεί να αποθηκευτεί και να μεταφερθεί σε φορητό υπολογιστή, κινητό, συσκευή USB ή ακόμα και σε ένα κομμάτι χαρτί. Δεδομένου ότι το υλικό που απαιτείται για την ασφάλεια και την μεταφορά του είναι ασυσχέτιστο με το ποσό αποθήκευσης, είτε είναι 1$ είτε 1 δισεκατομμύριο, το Bitcoin μπορεί να χαρακτηριστεί φορητό[54].

Διαιρετό

Ενώ οι υπάρχουσες μορφές χρημάτων διαιρούνται με δύο δεκαδικά ψηφία, το Bitcoin φτάνει μέχρι και οκτώ. Η μικρότερη ονομαστική αξία του ή 0,00000001, είναι ένα «Satoshi»[54].

Ομοιομορφία

Κάθε Bitcoin μπορεί να έχει εξορυχθεί σε διαφορετική χρονική περίοδο, αλλά είναι όλα τα ίδια. Στο υπάρχον σύστημα κυβερνητικών νομισμάτων, αυτό δεν ισχύει πάντα, αφού στις αρχές του 1900 ένα ασημένιο δολάριο ή χαρτονόμισμα δύο δολαρίων πωλούνταν σε premium στην ονομαστική του αξία[54].

Περιορισμένη ποσότητα

Εάν η πλειοψηφία των χρηστών και των συμμετεχόντων του δικτύου δεν συμφωνήσει να αλλάξει την νομισματική πολιτική του Bitcoin, πράγμα που όπως αναφέραμε είναι εξαιρετικά δύσκολο, θα υπάρξουν μόνο 21 εκατομμύρια Bitcoin[54].

Αποδοχή

Από το 2020, το Bitcoin γίνεται αποδεκτό από σχεδόν 16.000 επιχειρήσεις παγκοσμίως, από τις οποίες οι 2.500 εδρεύουν στις ΗΠΑ. Αυτός ο αριθμός έχει αυξηθεί κατά +28.000% από τον Νοέμβριο του 2013, όταν ο συνολικός αριθμός των επιχειρήσεων που δέχονταν Bitcoin ήταν περίπου 550[54].

Υποστηρίζεται από ένα δίκτυο ήχου

Όσοι αντιλαμβάνονται το Bitcoin ως καθαρά ψηφιακό νόμισμα διακηρύττουν ότι δεν έχει καμία εγγενή αξία επειδή «δεν υποστηρίζεται από τίποτα». Δηλαδή, το Bitcoin δεν μπορεί να εξαργυρωθεί για κάτι άλλο χρήσιμο ή/και αξίας, ενώ τα κυβερνητικά νομίσματα έχουν ιστορικά υποστηριχθεί από ένα υποκείμενο εμπόρευμα ή περιουσιακό στοιχείο. Βέβαια η «πλήρη πίστη της κυβέρνησης» είναι ένα σημαντικό προνόμιο. Έτσι οι ίδιοι καταλήγουν στο συμπέρασμα ότι το Bitcoin δεν είναι χρήμα και δεν έχει καμία εγγενή αξία[54].

Όπως ανέφερε ο Stefan Hofrichter, Head of Global Economics & Strategy at Allianz Global Investors: «Κατά την άποψή μας η εγγενής αξία του πρέπει να είναι μηδενική: ένα Bitcoin δεν είναι μία απαίτηση για κανέναν-σε αντίθεση για παράδειγμα, με κρατικά ομόλογα, μετοχές ή χαρτονομίσματα»[54].

Ωστόσο η λογική αυτή δεν αναγνωρίζει ότι ακριβώς όπως το δολάριο είναι επιθυμητό, για παράδειγμα λόγω της εμπιστοσύνης σε ένα από τα πιο ισχυρά οικονομικά κράτη παγκοσμίως, έτσι και το Bitcoin είναι επιθυμητό λόγω της ισχύος του δικτύου του ή του «οικοσυστήματος». Το Bitcoin έχει χτίσει την φήμη του ως το πιο κρυπτογραφικά ασφαλές, αποκεντρωμένο και ευρέως διαδεδομένο ψηφιακό περιουσιακό στοιχείο. Όλα αυτά υποστηρίζονται από δισεκατομμύρια δολάρια σε υπολογιστική ισχύ και εκατομμύρια συμμετέχοντες. Αυτή η συνεχώς αυξανόμενη εμπιστοσύνη στο τι μπορεί να κάνει το Bitcoin σήμερα και τι θα μπορούσε να κάνει αύριο δημιουργεί μία ελκυστική μορφή χρημάτων ή/και ένα μέσο αποθήκευσης αξίας, εξ ου και η εγγενής αξία του[54].

### 4.3.4 Το Bitcoin Ως Νόμισμα: Ποσοτική Θεωρία Του Χρήματος

Αν και το Bitcoin περιέχει τα περισσότερα από τα παραπάνω χαρακτηρίστηκα, δεν υπάρχει ακόμα συναίνεση σχετικά με τον τρόπο προσδιορισμού της πραγματικής αξίας. Αυτό είναι ακόμα πιο δύσκολο αφού η τιμή του Bitcoin οφείλεται σε μεγάλο βαθμό στην κερδοσκοπία. Πως κρίνουμε να είναι υποτιμημένο ή υπερτιμημένο[66];

Μία μέθοδος που προτιμάται από την λογιστική εταιρεία EY, είναι η εφαρμογή της κλασικής Ποσοτικής Θεωρίας του Χρήματος στο Bitcoin. Αυτή η μέθοδος αναπαρίσταται σε μία απλή εξίσωση:

$$M*V=P*T$$

- M = προσφορά χρήματος (σε αυτήν την περίπτωση, η προσφορά των Bitcoins σε κυκλοφορία)
- V = ταχύτητα (πόσο γρήγορα αλλάζει χέρια το Bitcoin σε μία δεδομένη περίοδο)
- P = τιμή του Bitcoin (αυτό που προσπαθούμε να βρούμε)
- T = ο όγκος συναλλαγών (αξία αγαθών και υπηρεσιών που συναλλάσσονται με Bitcoin σε μία περίοδο)

Το M είναι εύκολο να συνδεθεί, αφού η συνολική ποσότητα των Bitcoin που έχουν δημιουργηθεί είναι 19.442.000.

Το V αναφέρεται στη συχνότητα αλλαγής χρημάτων, αλλά, για τους σκοπούς αυτού του τύπου θα πρέπει να υπολογίζονται μόνο οι πραγματικές δαπάνες για αγαθά και υπηρεσίες. Η αγορά και πώληση Bitcoin για κερδοσκοπικούς σκοπούς δεν συμπεριλαμβάνεται[66].

Εν το μεταξύ το T είναι η συνολική αξία των αγαθών και των υπηρεσιών που αγοράζονται με Bitcoin, εκφρασμένη σε νόμισμα fiat( παραδείγματος χάρη 500 δισεκατομμύρια δολάρια ΗΠΑ). Είναι δύσκολο να το εκτιμήσουμε αυτήν την στιγμή, καθώς οι επιχειρήσεις βρίσκονται ακόμα σε στάδιο αποδοχής του Bitcoin ως πληρωμής[66].

## 4.4 Αξιολόγηση Βάση Των Εμπορευμάτων

Επειδή τα εμπορεύματα, όπως το καλαμπόκι, το σιτάρι, το ασήμι και ο χρυσός, έχουν ιστορία χρήσης και αξίας μεταξύ των κοινωνιών και των πολιτισμών, η εγγενής τους αξίας είναι συνάρτηση της χρησιμότητας και του πεπερασμένου. Ο χρυσός παραμένει επιθυμητός όχι απλώς επειδή είναι γυαλιστερός, αλλά επειδή είναι σπάνιος μπορεί να χρησιμοποιείται σε κοσμήματα, χρησιμεύοντας ως μέσο ανταλλαγής και αποθήκευσης αξίας για αιώνες λόγω της ομοιογενούς, διαιρετής, ανθεκτικής και σπάνιας φύσης[54].

Η λογική απόρριψης του Bitcoin βασίζεται στο γεγονός δεν έχει καμία εγγενής αξία επειδή είναι διαφορετικό από ένα φυσικό, παραδοσιακό εμπόρευμα, όπως ο χρυσός. Η λογική αυτή βασίζεται στην άποψη ότι το Bitcoin δεν μπορεί να κρατηθεί στο χέρι, και η χρησιμότητά του βασίζεται μόνο στην ικανότητα να αποστέλλεται μεταξύ των συμμετεχόντων στο δίκτυο[54].

Σύμφωνα με τον Peter Schiff, Euro Pacific Capital: «Αυτό που λείπει από τα Bitcoins είναι η δική τους θεμελιώδης εγγενής αξία. Δεν μπορείτε να κάνετε τίποτα με ένα Bitcoin, εκτός από το να το ανταλλάξετε με κάτι που θέλετε. Έτσι, εγγενώς, το ίδιο το Bitcoin δεν έχει καμία αξία».

Πολλοί βλέπουν την πραγματικότητά αυτή ως απόδειξη ότι οι παραδοσιακές και υπεράκτιες τραπεζικές υπηρεσίες έχουν μια πραγματική, αλλά ανεκπλήρωτη ζήτηση που το

Bitcoin μπορεί και θα συνεχίζει να εκπληρώνει. Αυτές οι υπηρεσίες περιλαμβάνουν, αλλά δεν περιορίζονται στα ακόλουθα:

Παραδοσιακή και Υπεράκτια Τραπεζική

Επειδή οποιοσδήποτε με σύνδεση στο διαδίκτυο μπορεί να αγοράσει Bitcoin και να συμμετέχει στο δίκτυο, το Bitcoin μπορεί συχνά να χρησιμεύει ως καλύτερη εναλλακτική λύση στις παραδοσιακές και υπεράκτιες τραπεζικές υπηρεσίες για πολλούς. Σε αντίθεση με τις υπάρχουσες προσφερόμενες, οι χρεώσεις του Bitcoin είναι διαφανείς, τα πορτοφόλια δεν υπόκεινται σε αυθαίρετα ελάχιστα υπόλοιπα, οι συναλλαγές δεν βασίζονται σε τρίτους, οι συναλλαγές είναι σχεδόν στιγμιαίες 24x7x365, είναι δύσκολο να κατασχεθούν απροσδόκητα και τα προσωπικά δεδομένα είναι λιγότερο σε κίνδυνο. Για πρώτη φορά στην ιστορία, όποιος έχει σύνδεση στο διαδίκτυο μπορεί να λειτουργήσει ως δική του τράπεζα ενώ συμμετέχει στην οικονομία με πλήρη έλεγχο της περιουσίας του[54].

Περισσότεροι από 1,7 δισεκατομμύρια άνθρωποι σε όλον τον κόσμο παραμένουν χωρίς τραπεζικό λογαριασμό, με τις αυριανές γενιές να έχουν στρέψει την εμπιστοσύνη τους στις τεχνολογικές υπηρεσίες, ως αποτέλεσμα της δυσπιστίας προς τις τράπεζες. Έτσι ένας στους τέσσερεις καταναλωτές χρησιμοποιεί σήμερα ένα κινητό πορτοφόλι καθημερινά και σχεδόν οι μισοί (46%) τα χρησιμοποιούν πολλές φορές την βδομάδα.

Το γεγονός που έχει σημασία σύμφωνα με τους υποστηρικτές είναι ότι η χρησιμότητα του Bitcoin υπάρχει, μεταξύ όλων των άλλων, στη λειτουργεία του ως εναλλακτική  σε ότι είναι οι εμπορευματοποιημένες υπηρεσίες[54].

Υπηρεσίες Εμβασμάτων

Η Παγκόσμια τράπεζα υπολόγισε ότι 551 δισεκατομμύρια δολάρια στάλθηκαν σε χώρες χαμηλού και μεσαίου εισοδήματος, δηλαδή πάνω από +4% σε σχέση με το τα προηγούμενα έτη. Συνολικά, η ζήτηση για υπηρεσίες εμβασμάτων συνεχίζει να αυξάνεται παρά το μεγάλο κόστος. Οι τράπεζες χρεώνουν κατά μέσο όρο 7% σε χρεώσεις μεταφοράς και οι προμήθειες μπορούν να φτάσουν το 10%, όταν ο προορισμός είναι η Αφρική ή σε νησί του Ειρηνικού Ωκεανού.  Δεν είναι μόνο ότι είναι ακριβά, αλλά είναι αργά και βασίζονται σε τρίτο πάροχο υπηρεσιών που οι χρήστες πρέπει να εμπιστεύονται. Βέβαια παρόλα αυτά, βασίζονται στην εμπιστοσύνη του τραπεζικού συστήματος[54].

Από την άλλη πλευρά, το Bitcoin μπορεί να σταλεί αμέσως, με μικρό ποσοστό προμήθειας και σε λίγη ώρα. Για παράδειγμα, στις 26 Ιουνίου του 2020, Bitcoin αξίας 1

δισεκατομμυρίου μεταφέρθηκε σε λιγότερο από 10 λεπτά με χρέωση 0,48$. Με χρέωση 7%, ένα παρόμοιο έμβασμα 1 δις δολάρια θα κόστιζε 70 εκατομμύρια δολάρια και μπορεί να χρειαζόταν έως και μία βδομάδα για να εκκαθαριστεί[54].

Πληρωμές

Από την γέννηση του διαδικτύου, οι πάροχοι υπηρεσιών πληρωμών συνεχίζουν να αναδεικνύονται και αναμφισβήτητα να ανταγωνίζονται σχεδόν αποκλειστικά για το μέγεθος του υπάρχοντος δικτύου τους. Μεταξύ Paypal, Square, Venmo, Zelle και Apple Pay, μεταξύ άλλων, δεν υπάρχει έλλειψη μέσων με τα οποία μπορεί κάποιος να πραγματοποιήσει συναλλαγές.

Ωστόσο, η υπηρεσία που χρησιμοποιεί κάποιος για οποιαδήποτε συναλλαγή εξαρτάται σε μεγάλο βαθμό από το εάν ο αποστολέας/παραλήπτης χρησιμοποιεί την ίδια υπηρεσία. Όπως συμβαίνει με τις τραπεζικές υπηρεσίες και τις υπηρεσίες εμβασμάτων, οι υπηρεσίες πληρωμών έχουν μετατραπεί σε υπηρεσίες βασικών προϊόντων που απαιτούν από τους χρήστες να εμπιστεύονται την υπηρεσία παρόχου για την εκτέλεση των υπηρεσιών που υπόσχονται. Το δίκτυο του Bitcoin μπορεί να στείλει σε οποιονδήποτε σε όλον τον κόσμο χωρίς να βασίζεται σε μία οντότητα ή άτομο[54].

## 4.5 Εγγενής Αξία Ως Μέσο Αποθήκευσης Ενέργειας Και Επένδυση Κεφαλαίου

Η απλή λογική ότι το Bitcoin αποτελείται από bit και byte, που μπορούν να διαγραφούν με το πάτημα ενός κουμπιού φαίνεται αρκετά διαισθητική. Αντίστοιχα, το 2018, ο αντιπρόεδρος της Berkshire Hathaway, Charlie Munger, κατονόμασε το Bitcoin «άχρηστο, τεχνητό χρυσό». Επομένως, είναι λογικό να εξεταστούν ορισμένα αντεπιχειρήματα που υποστηρίζουν το Bitcoin, εξετάζοντας την προσπάθεια που απαιτείται για τη δημιουργία και την ασφάλεια του. Με λίγα λόγια, το Bitcoin υποστηρίζεται από την ποσότητα ενέργειας που απαιτείται για την εξόρυξη και η οποία στην ουσία, δεν είναι τίποτα άλλο παρά ένας μηχανισμός που διασφαλίζει την ασφάλεια του δικτύου και βοηθάει στην επίτευξη των συμφωνιών. Το κόστος εξόρυξης είναι εφάπαξ κόστος, αλλά όσοι έχουν επενδύσει σε αυτό μπορεί να έχουν βιώσιμο ενδιαφέρον για αυτό, καθώς διακυβεύουν κάτι. Αυτό δεν είναι μόνο το ίδιο το νόμισμα, αλλά ειδικά το εξαιρετικά εξειδικευμένο υλικό που χρησιμοποιείται για την εξόρυξη. Η ίδια λογική ισχύει για

όλα τα κρυπτονομίσματα που χρησιμοποιούν το PoW ως μέρος του μηχανισμού συναίνεσης[67].

Η χρήση της ποσότητας ενέργειας που αποθηκεύεται στο Bitcoin για την αξιολόγηση της αξίας του, έχει μια εντυπωσιακή ομοιότητα με τη συχνά επικρινόμενη θεωρία της αξίας του Karl Marx's. Σύμφωνα με αυτή την θεωρία, είναι το ποσό της εργασίας που πηγαίνει στην παραγωγή ενός εμπορεύματος, που καθορίζει την αξία του τελευταίου. Στην περίπτωση του Bitcoin, η εργασία αντιστοιχεί στην ποσότητα ενέργειας που απαιτείται για τη δημιουργία συστοιχιών δεδομένων. Και πάλι η ασάφεια της έννοιας της αξίας δημιουργεί προβληματισμό: «η θεωρία της εργασιακής αξίας σύμφωνα με τον Karl Marx's διακρίνεται σε μία κεντρική πτυχή: δεν παράγεται ούτε υπεραξία, ούτε η αξία. Η αξία είναι μια κοινωνική σχέση που διαμορφώνεται στο κοινωνικό επίπεδο μεταξύ εταίρων ανταλλαγής»(Lippert, 2019). Αυτή η άποψη της αξίας ως σχέσης ευθυγραμμίζεται στενά με την κατανόηση του χρήματος που μπορεί να βρεθεί στον Αντωνόπουλο, ο οποίος αναφέρεται στο χρήμα ως «γλώσσα» ή στον Ingham (2004), ο οποίος αντιμετωπίζει το χρήμα από κοινωνιολογική προοπτική και τονίζει τη σημασία των κοινωνικών σχέσεων, που βασίζονται σε κοινωνικούς κανόνες και σχέσεις εξουσίας. Σε αυτό το πνεύμα, ο Tucker (2018) επισημαίνει: «Όλα αυτά σημαίνουν ότι η αξία του Bitcoin δεν προκαλείται από τη εργασία που εκτελείται για την δημιουργία τους. Η αξία του Bitcoin προέρχεται από την αξία του στην πραγματική χρήση». Επεξηγεί περαιτέρω τη συλλογιστική του, δίνοντας το παράδειγμα της δημιουργίας μπισκότων από μπάλες μαλλιών που βγάζει μία γάτα, που απαιτείται σαφώς σημαντική προσπάθεια (για την γάτα), αλλά δεν δημιουργεί αξία (για κανέναν άλλον). Αν και αυτό το παράδειγμα είναι ενδεικτικό, ο Tucker δεν λαμβάνει υπόψη ότι οι λογικοί επιχειρηματίες έχουν συνήθως μια διεξοδική αξιολόγηση σχετικά με την βιωσιμότητα των επενδύσεών τους[67].

Η ανταγωνιστική εξόρυξη του Bitcoin, προέκυψε με την πάροδο του χρόνου ως απάντηση στην αυξημένη αποτίμηση της αγορά και επομένως θα μπορούσε να χρησιμεύσει ως μέσος για την αξιολόγηση της συνολικής αποτίμησης του κρυπτονομίσματος από την κοινότητα. Με άλλα λόγια, η αξία που προσδιορίζεται σε ένα αγαθό ή μια υπηρεσία από τους συμμετέχοντες στην αγορά δεν είναι το μοναδικό κριτήριο αξίας όπως υπονοεί ο Tucker, αλλά η τρέχουσα αποτίμηση χρησιμεύει ως ανατροφοδότηση για όσους είναι πρόθυμοι να επενδύσουν τους πόρους τους στην δημιουργία περισσότερων Bitcoin. Ως εκ τούτου, με την πάροδο του χρόνου, το κόστος της εξόρυξης Bitcoin πλησιάζει τα έσοδα που μπορούν να αποκομίσουν από αυτό, ενώ η πώληση μπισκότων μαλλιών μπορεί πράγματι να είναι μάλλον βραχυχρόνια προσπάθεια[67].

Με απλά λόγια, οι «εξορύκτες» είναι πρόθυμοι να επενδύσουν τα χρήματά τους με βάση τις τρέχουσες προσδοκίες ή την προηγούμενη εμπειρία τους. Αυτός είναι πιθανώς ο λόγος που τα μπισκότα από τρίχα γάτας δεν έχουν προσφερθεί ποτέ στην αγορά. Οι προσδοκίες τους μπορεί να είναι λανθασμένες βραχυπρόθεσμα, αλλά με την πάροδο του χρόνου οι πληροφορίες που λαμβάνουν από την αγορά, χρησιμεύουν ως ανατροφοδότηση για το πόσο κερδοφόρα είναι η επένδυσή τους. Με άλλα λόγια, το ποσό της ενέργειας που επενδύεται για την παραγωγή του Bitcoin, μπορεί να μην αντιπροσωπεύει πλήρως την αξία του, αλλά μάλλον την προσδοκία των «εξορυκτών» για το πόση θα είναι η μελλοντική αξία. Με την πάροδο του χρόνου, αυτό μπορεί να χρησιμεύσει ως μέσο αποτίμησης της αξίας[67].

Από την άποψη αυτή, η εγγενής αξία του χρυσού ή του Bitcoin εξαρτάται από την προτιμώμενη χρήση τους ως νόμισμα ή ακόμη και ως αποθήκη αξίας και τη λειτουργία της υποκείμενης κρυπτογραφίας. Εάν ένα νόμισμα δεν υιοθετηθεί ως μέσο ανταλλαγής ή ως αποθήκη αξίας, θα χάσει την αποτίμησή του. Φυσικά αυτή η αποτίμηση μπορεί να επηρεαστεί σοβαρά από ξαφνικά γεγονότα. Εάν, για παράδειγμα, η υποκείμενη κρυπτογραφία του Bitcoin επρόκειτο να σπάσει απροσδόκητα, είναι δίκαιο να ειπωθεί αυτό. Ωστόσο, όλοι αυτοί οι πιθανοί κίνδυνοι, που περιλαμβάνουν τη νομοθεσία καθώς και τη σημασία της μελλοντικής ζήτησης χρηστών, είναι γνωστά σε όσους επενδύουν στον εξοπλισμό και στην ενέργεια για την εξόρυξη του Bitcoin. Ως εκ τούτου, οι επενδύσεις σε εξοπλισμό και ενέργεια που απαιτούνται για την εξόρυξη του Bitcoin μπορούν να χρησιμοποιηθούν ως μέσο για τον υπολογισμό της εγγενής αξίας του[67].

## 4.6 Mining Και Εγγενής Αξία

Είμαστε σε θέση τώρα να δούμε τον αντίστοιχο κύκλο στην διαδικασία εξόρυξης του Bitcoin και πάλι ένας «εξορύκτης» θα ξεκινήσει με ένα αρχικό κεφάλαιο το οποίο θα επενδύσει στα δύο μέσα που απαιτούνται για την εξόρυξη του Bitcoin. Το ένα βέβαια όπως εξηγήσαμε στην προηγούμενο κεφάλαιο είναι το hardware, που ανά τακτά χρονικά διαστήματα οι «εξορύκτες» πρέπει να ανανεώνουν, αφενός γιατί καινούργια μοντέλα βγαίνουν στην κυκλοφορία με μεγαλύτερη υπολογιστική ισχύ άρα προσδίδουν στον «εξορύκτη» που θα τα κατέχει μεγαλύτερο hash rate και άρα το δίνουν ανταγωνιστικό πλεονέκτημα έναντι των ανταγωνιστών[41].

Βέβαια ένα άλλο μέρος του κόστους προέρχεται από την ανάγκη συντήρησης όλων αυτών των μηχανημάτων γιατί υπάρχουν και αστοχίες υλικού. Το δεύτερο και ακόμα πιο σημαντικό μέσο για την εξόρυξη των Bitcoins, είναι η ενέργεια (κατανάλωση ρεύματος). Οι επεξεργαστές που βοηθούν στην παραγωγή δουλεύουν στο μέγιστο επομένως καταναλώνουν πολύ μεγάλα ποσά ενέργειας. Ο «εξορύκτης» που θα καταφέρει πρώτος να βρει ένα hash το οποίο να είναι μικρότερο από το όριο που καθορίζει το τρέχον επίπεδο της δυσκολίας, ενημερώνει τους υπόλοιπους κόμβους του δικτιού ότι βρήκε το συγκεκριμένο hash, δίνοντάς τους και το συγκεκριμένο ακέραιο αριθμό με τον οποίο το πέτυχε, ούτως ώστε οι υπόλοιποι να μπορούν να το επαληθεύσουν. Στην συνέχεια, ανταμείβεται με νέα νομίσματα Bitcoin. Τα καινούρια αυτά νομίσματα ενσωματώνουν την αξία του hardware καθώς και την αξία της ηλεκτρικής ενέργειας που απαιτήθηκε για την εξόρυξή τους. Αυτή είναι η εγγενής αξία του bitcoin[41].

Έτσι η εγγενής αξία συνδέεται με βάση το οριακό κόστος παραγωγής ενός Bitcoin. Η εξόρυξη του Bitcoin όπως αναφερθήκαμε, χρειάζεται μεγάλη ποσότητα ηλεκτρικής ενέργειας και αυτό μεταβάλει το πραγματικό κόστος. Σύμφωνα με την οικονομική θεωρία, σε μία ανταγωνιστική αγορά μεταξύ παραγωγών που παράγουν όλοι το ίδιο προϊόν, η τιμή πώλησης αυτού του προϊόντος θα τείνει προς το οριακό κόστος παραγωγής του. Εμπειρικά στοιχεία έχουν δείξει ότι η τιμή ενός Bitcoin τείνει να ακολουθεί το κόστος παραγωγής[41].

Στη συνέχεια ο «εξορύκτης» θα πουλήσει τα Bitcoins τα οποία εξόρυξε για «χάρτινο» νόμισμα και έτσι θα κλείσει και πάλι ο κύκλος της παραγωγής. Θεωρητικά το τελικό κεφάλαιο θα είναι μεγαλύτερο από το αρχικό και η διαφορά θα είναι το κέρδος του «εξορύκτη». Η εγγενής αξία του bitcoin είναι διαφορετική από την τιμή στην οποία ο «εξορύκτης» καταφέρνει να πουλήσει τα Bitcoins για «χάρτινο» νόμισμα. Επίσης αν και η εγγενής αξία των Bitcoin προέρχεται από το hardware και το ρεύμα που χρειάστηκε για την εξόρυξη του, αν για οποιοδήποτε λόγο σταματήσει η ροή του «χάρτινου» νομίσματος, για παράδειγμα αν ο «εξορύκτης» δεν καταφέρει να πωλήσει τα Bitcoin για «χάρτινο» νόμισμα τότε η εγγενής αξία του Bitcoin θα καταστραφεί[41].

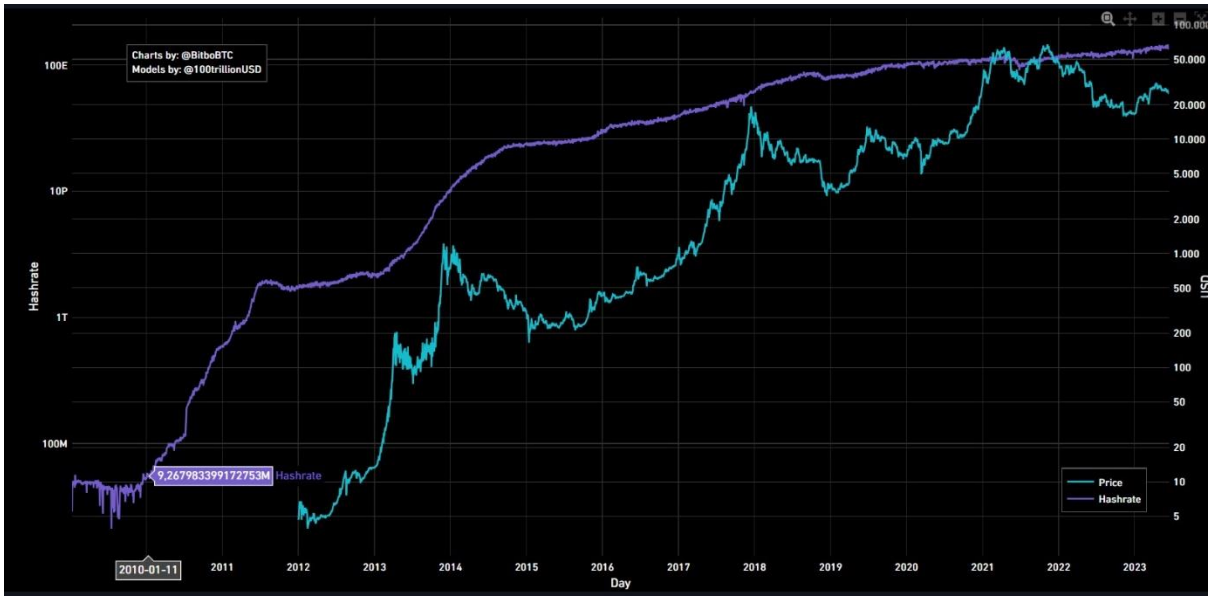
Στη περίπτωση αυτή τα Bitcoin παραμένουν αναύλωτα και επομένως μπορούν να κυκλοφορήσουν ανεξάρτητα από το «χάρτινο» νόμισμα. Ωστόσο, το τρέχον επαγγελματικό μοντέλο της εξόρυξης του παύει να ισχύει. Αυτό είναι και το μοναδικό σημείο στο οποίο οι κυβερνήσεις δυνητικά θα μπορούσαν να παρέμβουν[41].

Βέβαια καμία κυβέρνηση ή κεντρική αρχή δεν μπορεί να σταματήσει τη διαδικασία της επεξεργασίας των συναλλαγών και της εξόρυξης των Bitcoin, γιατί αυτή γίνεται από πολλούς ανεξάρτητους παραγωγούς, δεν υπάρχει μια κεντρική αρχή από πίσω που να μπορούν να κινηθούν νομικά εναντίον της και ακόμα και εάν ένα κράτος έκανε παράνομο το «mining» στην επικράτειά του απλά θα βλέπαμε περισσότερους «εξορύκτες» να εμφανίζονται σε κάποιες άλλες χώρες. Η κάθε κυβέρνηση έχει έλεγχο στο δικό της νόμισμα και μπορεί αν θέλει να απαγορεύσει τη χρήση του δικού της νομίσματος για αγορά ή πώληση Bitcoins. Αν δεν έκαναν το ίδιο ταυτόχρονα όλες οι κυβερνήσεις του κόσμου θα ήταν άσκοπο, γιατί για παράδειγμα αν η Ευρωπαϊκή Κεντρική Τράπεζα απαγορεύσει να γίνονται αγοραπωλησίες ανάμεσα σε ευρώ και Bitcoin αλλά είναι άλλο κράτος παράδειγμα η Αμερική συνεχίζει να επιτρέπει τις αγοροπωλησίες από δολάρια σε Bitcoin, αυτό που θα έκανε θα ήταν να αλλάξει τα ευρώ που έχει για δολάρια και στη συνέχεια να αγοράζει Bitcoin με δολάριο ή αντίστροφα ένας πωλητής Bitcoin, θα πουλούσε Bitcoin για αμερικανικό δολάριο και στη συνέχεια θα άλλαζε το δολάριο για ευρώ. Επομένως ακόμα και αν αυτός είναι ένας τρόπος με τον οποίο οι κυβερνήσεις προσπαθούν να ελέγξουν το Bitcoin αν το επιθυμούσαν, απαιτεί την πλήρη συμφωνία και συνεργασία μεταξύ τους, κάτι που φαντάζει αδύνατο γιατί δεν είναι όλες οι χώρες συμμαχικές μεταξύ τους. Είναι δηλαδή περισσότερο ένα θεωρητικό ενδεχόμενο που η πιθανότητα του τείνει στο μηδέν[41].

Όσο το Bitcoin κατοχυρώνεται στη συνείδηση της κοινωνίας ως ένα μέσο αποθήκευσης αξίας η γενική τάση για την τιμή του είναι ανοδική, με αποτέλεσμα οι διάφοροι «εξορύκτες» να έχουν όλο και μεγαλύτερο κίνητρο να εξορύξουν νέα νομίσματα Bitcoin. Αυτό οδηγεί σε αγορά όλο και μεγαλύτερου εξοπλισμού καθώς και στο συνεταιρισμό πολλών «εξορυκτών» μεταξύ τους, στην δημιουργία «mining pools». Ταυτόχρονα το περισσότερο και καλύτερο hardware απαιτεί και περισσότερη ενέργεια για να «τρέξει» άρα και η κατανάλωση ενέργειας είναι όλο και μεγαλύτερη. Αυτή λοιπόν η υπολογιστική ισχύς που συνέχεια αυξάνεται, ποσοτικοποιείται από έναν δείκτη που αθροίζει το συνολικό hash rate όλων των «εξορυκτών» των Bitcoin στον κόσμο[41].

## 4.7 Hash Rate Και Τιμή Bitcoin

*Εικόνα 16-Hash rate vs Price.*




Στο παραπάνω διάγραμμα αυτό βλέπουμε με τη μοβ καμπύλη την πορεία του συνολικού hash rate του Bitcoin δικτύου, από την αρχή το 2009 μέχρι και σήμερα. Ο άξονας το ψ είναι ζωγραφισμένο σε λογαριθμική κλίμακα. Στην δεύτερη καμπύλη βλέπουμε την πορεία της τιμής του bitcoin και παρατηρούμε λοιπόν ότι παρά τις επιμέρους διακυμάνσεις στις τιμές του bitcoin, η γενική ανοδική τάση του συμβαδίζει, με την ανοδική τάση του συνολικού hash rate του Bitcoin δικτύου. Αν ξανά προσδιοριστεί τι είναι το συνολικό hash rate, είναι ο αριθμός των φορών που οι «εξορύκτες» του Bitcoin δικτύου «τρέξανε» την hashing συνάρτηση. Κάθε ένας τέτοιος υπολογισμός γίνεται στους ειδικούς επεξεργαστές που έχουν αγοράσει οι «εξορύκτες» και φυσικά απαιτεί την κατανάλωση ενέργειας. Επομένως η αύξηση του συνολικού hash rate υποδηλώνει την αύξηση του ρυθμού με τον οποίο συσσωρεύεται αξία στα νομίσματα του Bitcoin[41].

Το ερώτημα που προκύπτει, είναι δεδομένου ότι η εγγενής αξία του Bitcoin οφείλεται σε μεγάλο βαθμό στην ενέργεια που καταναλώνεται για την εξόρυξη του και η ενέργεια αυτή αυξάνεται συνεχώς. Είναι το bitcoin είναι επιβλαβές για το περιβάλλον; [41].

## 4.8 Βιωσιμότητα Και Κατανάλωση Ενέργειας Του Bitcoin

Το πρώτο ερώτημα είναι πόση και τι είδους ενέργεια καταναλώνει το δίκτυο του bitcoin για να απαντηθούν τα ερωτήματα αυτά θα πρέπει να αναφερθούν στατιστικά στοιχεία, που έχει συγκεντρώσει το κέντρο εναλλακτικής οικονομίας του πανεπιστημίου του Cambridge[45].

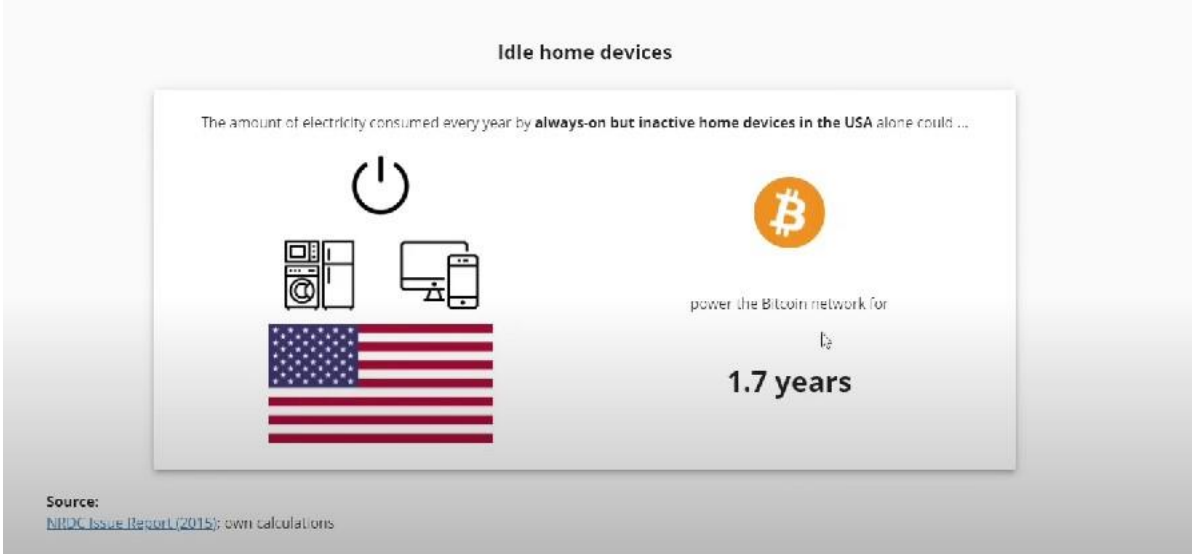
*Εικόνα 17-Κατάταξη κατανάλωσης ενέργειας.*


Η σημερινή κατανάλωση του δικτύου του Bitcoin εκτιμάται περίπου στις 127 τεραβατώρες το χρόνο. Αυτό το ποσό ενέργειας είναι πόσο περίπου καταναλώνει η αργεντινή και Ουκρανία μέσα σε ένα χρόνο.

*Εικόνα 18-Συνολική παγκόσμια παραγωγή από ανανεώσιμες πηγές ενέργειας.*

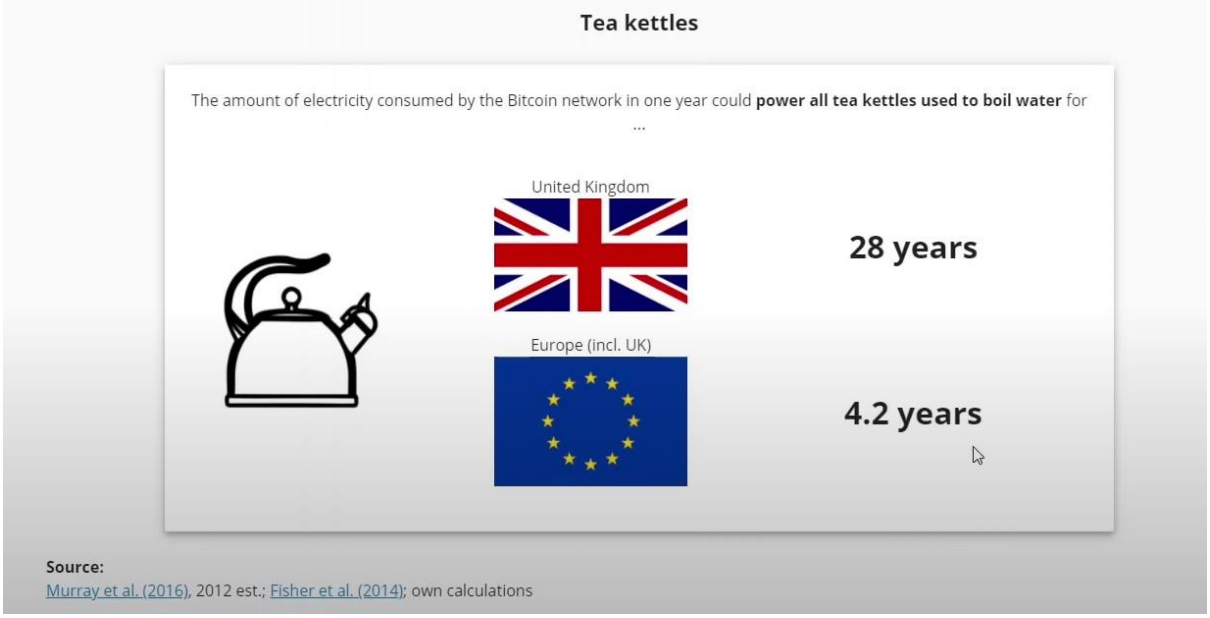
Το ίδιο site παρέχει κάποια πολύ ενδιαφέροντα δεδομένα για να μπορέσουμε να συγκρίνουμε τις ανάγκες του bitcoin δικτύου, με την σημερινή παραγωγή ενέργειας από ανανεώσιμες πηγές. Για παράδειγμα η ενέργεια που παράγεται από υδροηλεκτρικά εργοστάσια αρκεί για να καλύψει 33 φορές τις ετήσιες ανάγκες του Bitcoin, η ενέργεια που παράγεται από βιομάζα αρκεί για να καλύψει 5 φορές τις ανάγκες του δικτύου του Bitcoin, ενώ τέλος άλλες πηγές ενέργειας όπως η ηλιακή και αιολική αρκούν για να καλύψουν 11 φορές τις ετήσιες ανάγκες του δικτύου του Bitcoin[45].

*Εικόνα 19-Συνολική κατανάλωση ενέργειας από μη ενεργές συσκευές στην Αμερική.*




Κάποια άλλα ενδιαφέροντα στοιχεία που θα μας βοηθήσουν να κατανοήσουμε τις ενεργειακές ανάγκες του Bitcoin στην σωστή τους διάσταση παρουσιάζονται. Το πρώτο είναι ότι η ενέργεια που καταναλώνεται από σπιτικές συσκευές στις Ηνωμένες Πολιτείες μόνο, οι οποίες είναι ανενεργές αλλά συνέχεια συνδεδεμένες στο δίκτυο καλύπτει τις ανάγκες της λειτουργίας του δικτύου Bitcoin για 1,7 χρόνια[45].

*Εικόνα 20-Σύγκριση κατανάλωσης ενέργειας του Bitcoin και βραστήρων νερού στην Ευρωπαϊκή Ένωση.*

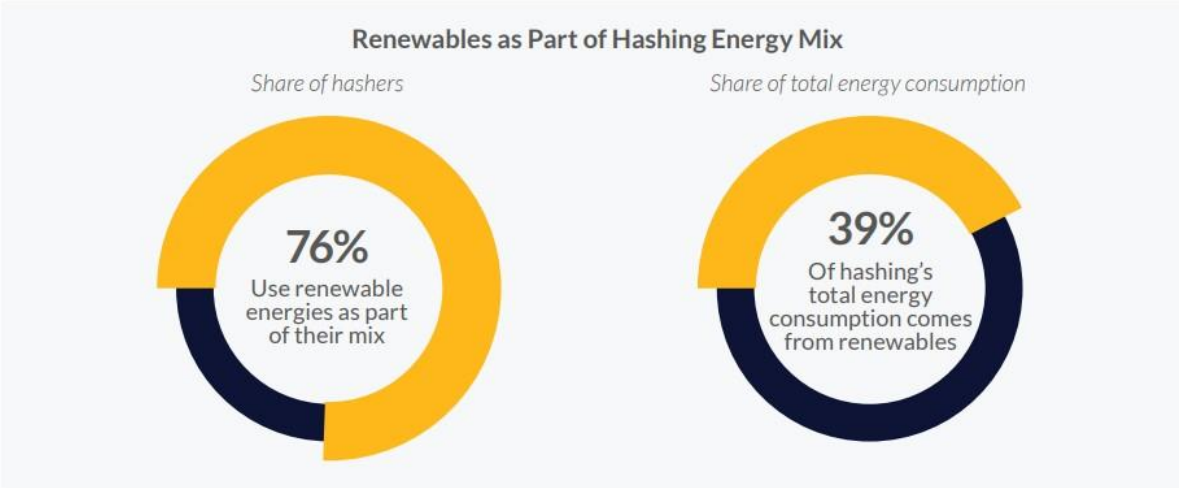



Επίσης, η ενέργεια που καταναλώνει σε ένα χρόνο το δίκτυο του Bitcoin ισοδυναμεί με την ενέργεια που καταναλώνουμε σε βραστήρες νερού μέσα σε 4,2 χρόνια στην Ευρωπαϊκή Ένωση[45].

Το επόμενο ερώτημα είναι τι μέρος της ενέργειας που καταναλώνει το δίκτυο του Bitcoin προέρχεται από ανανεώσιμες πηγές. Σε σχέση με αυτό υπάρχουν διαφορετικές εκτιμήσεις το άνω άκρο αυτών των εκτιμήσεων ανέρχεται στο 74%, ενώ το κάτω άκρο ανέρχεται σε 39%. Η μελέτη του κάτω άκρου η οποία εκδόθηκε τον Σεπτέμβριο του 2020 από την ίδια ομάδα το πανεπιστήμιο του Cambridge και μας ενημερώνει ότι το 76% των «εξορυκτών» χρησιμοποιούν στο ενεργειακό τους μίγμα, κάποια πηγή ανανεώσιμης ενέργειας, ενώ από το σύνολο της ενέργειας που καταναλώνουν το 39% εκτιμάται ότι προέρχεται από ανανεώσιμες πηγές[45].

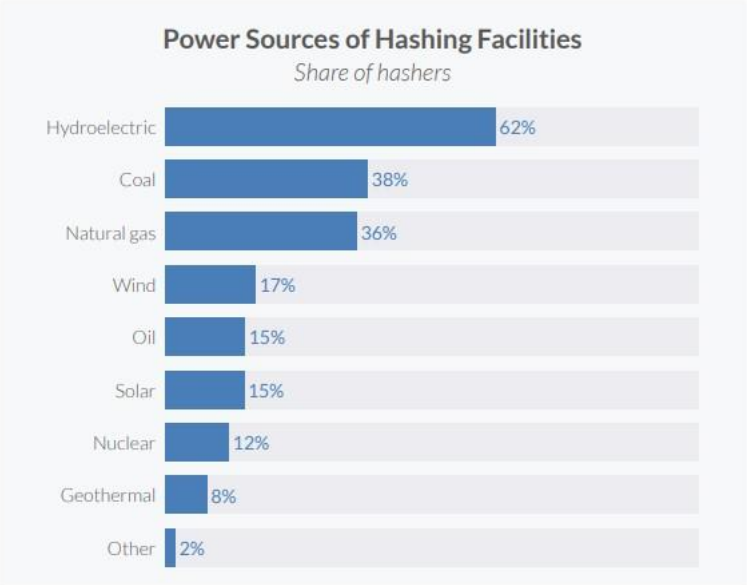
*Εικόνα 21-Ανανεώσιμες πηγές ως μέρος του ενεργειακού μίγματος.*

**Figure 15: PoW mining is primarily powered by non-renewable energy sources**




Σε σχέση τώρα με τις πηγές ενέργειας που χρησιμοποιούν οι «εξορύκτες», το 62% των χρησιμοποιούν σε κάποιο βαθμό υδροηλεκτρική ενέργεια, το 38% από αυτούς άνθρακα, το 36% φυσικό αέριο, το 17% αιολική ενέργεια, 15% πετρέλαιο, 15% ηλιακή ενέργεια, 12% πυρηνική ενέργεια, 8% γεωθερμική ενέργεια και 2% άλλες πηγές[45].

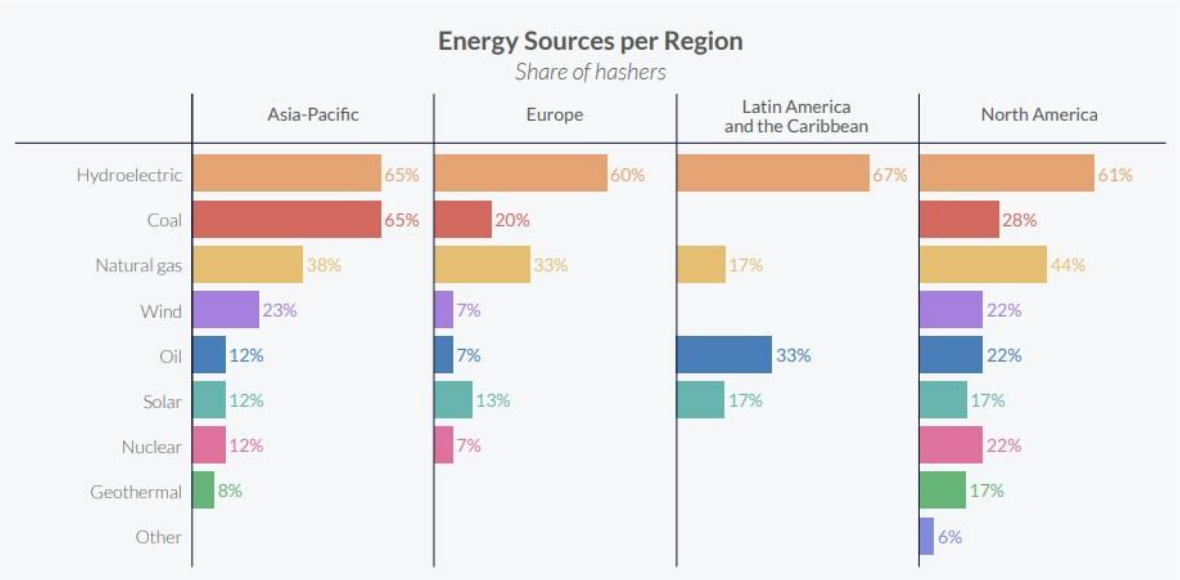
*Εικόνα 22-Πηγές ενέργειας των εγκαταστάσεων κατακερματισμού.*




Ενδιαφέρον παρουσιάζει και η διαφοροποίηση του μείγματος των διαφόρων πηγών ενέργειας ανάλογα τις περιοχές του κόσμου. Επίσης, το ποσοστό των «εξορυκτών» που χρησιμοποιούν σε κάποιο βαθμό υδροηλεκτρική ενέργεια ανέρχεται περίπου στα 2/3 σε όλες

τις ηπείρους. Ο άνθρακας χρησιμοποιείται περισσότερο στην Ασία, πολύ λιγότερο στην Ευρώπη και τη βόρειο Αμερική και καθόλου στη Λατινική Αμερική. Σχετικά πανομοιότυπη είναι η εικόνα με το φυσικό αέριο με μόνο την Λατινική Αμερική να υπολείπεται έναντι των άλλων. Η αιολική ενέργεια χρησιμοποιείται περισσότερο στην Ασία και στην βόρειο Αμερική, λιγότερο στην Ευρώπη και καθόλου στη Λατινική Αμερική. Το πετρέλαιο χρησιμοποιείται περισσότερο στην Αμερική και λιγότερο στην Ασία και την Ευρώπη. Περίπου ομοιογενής είναι εικόνα για την ηλιακή ενέργεια, ενώ η πυρηνική χρησιμοποιείται περισσότερο στην βόρεια Αμερική και την Ασία. Τέλος η γεωθερμική ενέργεια χρησιμοποιείται μόνο στην βόρειο Αμερική και την Ασία[45].

*Εικόνα 23-Πηγές ενέργειας ανά Ήπειρο.*




Επιστρέφοντας στο συνολικό ποσοστό που καταλαμβάνουν οι ανανεώσιμες πηγές ενέργειας στη λειτουργία του Bitcoin δικτύου όλες οι μελέτες σε φανερώνουν μια συνεχή τάση αύξησης αυτού του ποσοστού. Το δεύτερο σημαντικό στοιχείο είναι να ελεγχθεί πώς συγκρίνεται αυτό το ποσοστό σε σχέση με τις άλλες ανθρώπινες δραστηριότητες σύμφωνα με τα στατιστικά του παγκόσμιου οργανισμού ενέργειας. Για το πρώτο τρίμηνο του 2020 το μερίδιο των ανανεώσιμων πηγών από την συνολική παραγωγή ενέργειας στον κόσμο ανήλθε στο 28%. Συγκρίνοντας αυτό το 28% με το 39% που έχει πετύχει το δίκτυο του Bitcoin αποδεικνύει, ότι το δίκτυο του Bitcoin έχει μεταβεί σε ανανεώσιμες πηγές πολύ πιο γρήγορα από άλλες ανθρώπινες δραστηριότητες. Ενα τελευταίο σημείο σε σχέση με αυτό είναι ότι όλες αυτές οι στατιστικές μελέτες δεν αναλύουν περιπτώσεις που η ενέργεια που καταναλώνεται από κάποιον «εξορύκτη» επαναχρησιμοποιείται στη συνέχεια με ένα σωστό τρόπο για κάποια άλλη δραστηριότητα. Για παράδειγμα στην Σουηδία μια Bitcoin mining εταιρεία που

ονομάζεται Genesis διοχετεύει τη θερμότητα που παράγεται από τους επεξεργαστές που κάνουν «εξόρυξη» σε θερμοκήπια σε μια περιοχή της βόρειας Σουηδίας. Τα θερμοκήπια αυτά θα χρειάζονταν έτσι κι αλλιώς να καταναλώσουν ενέργεια για να δημιουργήσουν τη θερμότητα που απαιτείται[45].

Το δεύτερο σημαντικό ερώτημα είναι αν το Bitcoin είναι πιο ενεργοβόρο από το χρυσό, δεδομένου ότι όλο και περισσότεροι σήμερα αντιλαμβάνονται τη χρήση του ως μέσου αποθήκευσης αξίας. Σε ένα πρόσφατο άρθρο του Forbes από τις 10 Μαρτίου αναφέρεται ότι η βιομηχανία της εξόρυξης του χρυσού καταναλώνει το χρόνο περίπου 132 τεραβατώρες. Το νούμερο είναι πολύ κοντά στην κατανάλωση που κάνει το Bitcoin, περίπου στις 127 τεραβατώρες το χρόνο. Το νούμερο αυτό αφορά μόνο την διαδικασία της εξόρυξης του χρυσού και όχι την μεταφορά του ή την επεξεργασία του, ενώ οι 127 τεραβατώρες το χρόνο το δίκτυο του Bitcoin είναι η συνολική κατανάλωση η οποία καλύπτει και τις ανάγκες των συναλλαγών, της μεταφοράς δηλαδή αξίας σε παγκόσμιο επίπεδο[46]. Επιπλέον, οι παραγωγοί του χρυσού δεν έχουν κάνει ακόμα βήματα μετάβασης στην πράσινη ενέργεια με το Rueters να κρούει τον κώδωνα του κινδύνου και να παρουσιάζει στοιχεία για την αργοπορία της μετάβασης της συγκεκριμένης βιομηχανίας σε ανανεώσιμες πηγές ενέργειας[47].

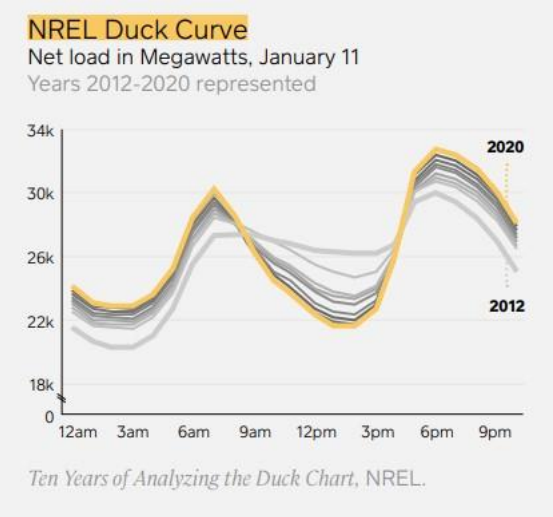
Μία χρήση του Bitcoin την οποία δεν θα μπορούσε να σκεφτεί ο Satoshi Nakamoto είναι αυτή του φίλτρου αερίων διοξειδίου του άνθρακα. Συγκεκριμένα στο άρθρο από την Cointelegraph αναφέρεται η πρόσφατη τάση στις Ηνωμένες Πολιτείες σχετικά με την χρήση φυσικού αερίου, το οποίο μέχρι τώρα ήταν απόβλητο της διαδικασίας παραγωγής πετρελαίου και καιγόταν στην ατμόσφαιρα, να μετατρέπεται σε ενέργεια η οποία κατευθύνεται σε Data Centers που κάνουν «εξόρυξη» και αναπτύσσονται δίπλα από τις εγκαταστάσεις παραγωγής πετρελαίου. Με αυτό τον τρόπο διάφορες εταιρείες εξόρυξης του πετρελαίου έχουν πετύχει 71% μείωση στην εκπομπή αερίων διοξειδίου του άνθρακα, ενώ ταυτόχρονα αποκομίζουν και οικονομικό όφελος μέσω της εξόρυξης[48].

Η ίδια ακριβώς ιδέα φαίνεται ότι η χρησιμοποίηση στην πράξη και η Gazprom σε εγκαταστάσεις παραγωγής πετρελαίου στην δυτική Σιβηρία. Έτσι πέρα από μικρές πετρελαϊκές εταιρείες των Ηνωμένων Πολιτειών φαίνεται σιγά σιγά ότι και κολοσσοί του χώρου, δραστηριοποιούνται στον χώρο του Bitcoin «mining». Αναπτύζουνε ήδη δηλαδή κέντρα «εξόρυξης» Bitcoin[49].

Μία ακόμα διάσταση που αποκτά το Bitcoin όλο και περισσότερο είναι αυτή ενός είδους μπαταρίας περισσευούμενης ενέργειας. Σε ένα άρθρο που εξέδωσε η εταιρεία Square

παρουσιάζεται η «εξόρυξη» του Bitcoin ως ένας καταλύτης για την παγκόσμια μετάβαση της παραγωγής ενέργειας σε ανανεώσιμες πηγές. Το πρόβλημα που υπήρχε και με τις παλιές μεθόδους παραγωγής ενέργειας αλλά υπάρχει ακόμα περισσότερο στις ανανεώσιμες, είναι ότι η ζήτηση ρεύματος δεν είναι η ίδια κατά τη διάρκεια της ημέρας, αλλά αυτή κορυφώνεται αργά το απόγευμα ή νωρίς το βράδυ όταν οι άνθρωποι επιστρέφουν σπίτι και ανοίγουν τις συσκευές τους.

*Εικόνα 24-NREL Duck Curve.*




Δεν υπάρχουν αποτελεσματικές τεχνολογίες αποθήκευσης για πολύ μεγάλες ποσότητες ενέργειας, με αποτέλεσμα αν μια πηγή παραδοσιακή ή ανανεώσιμη υπεραποδίδει κάποια στιγμή κατά την οποία δεν υπάρχει ζήτηση, αυτή η ενέργεια να χάνεται για πάντα. Ειδικά για τις ανανεώσιμες πηγές το πρόβλημα είναι ακόμα μεγαλύτερο γιατί όπως αναφέρεται ο ήλιος λάμπει κατά τη διάρκεια της ημέρας αλλά όχι το βράδυ, ενώ ο άνεμος είναι πιο απρόβλεπτος περισσότερο κατά τη διάρκεια της νύχτας. Το πρόβλημα λοιπόν για μια εταιρεία που επενδύει στον τομέα των ανανεώσιμων πηγών είναι ότι μεγάλο μέρος της παραγωγής της πήγαινε χαμένο. Εδώ έρχεται ο ρόλος των Bitcoin «εξορυκτών», πολλοί εκ των οποίων κάνουν συνεργασίες με τέτοιες εταιρίες παραγωγών ενέργειας από ανανεώσιμες πηγές, οι οποίες προβλέπουν ότι οι «εξορύκτες» θα καταναλώσουν μόνο αυτή την περισσευούμενη ενέργεια που αλλιώς θα πήγαινε χαμένη. Από τέτοιες συμφωνίες κερδίζουν και οι δύο πλευρές. Αφενός οι «εξορύκτες» κερδίσουν καλύτερες τιμές για την ενέργεια που καταναλώνουν, αφετέρου οι εταιρείες που παράγουν ρεύμα από ανανεώσιμες πηγές, βελτιώνουν την κερδοφορία τους και έχουν κίνητρο να κάνουν περαιτέρω

επενδύσεις με μεγαλύτερη ασφάλεια. Με την έλλειψη μιας αναπτυγμένης τεχνολογίας μπαταριών που θα αποθήκευε ενέργεια, το Bitcoin αποκτά την διάσταση μιας έμμεσης μπαταρίας η οποία βέβαια δεν αποθηκεύει ενέργεια όμως αποθηκεύει την αξία της περισσευούμενης ενέργειας που αλλιώς θα καταστρεφόταν[50].

## 4.9 Συμπέρασμα

Όπως και η ομορφιά, η εγγενής αξία είναι στα μάτια του θεατή. Είναι η κορύφωση από όλους τους συμμετέχοντες στην αγορά που αντιλαμβάνονται την εγγενή αξία ενός περιουσιακού στοιχείου, όπως το Bitcoin. Όσοι βλέπουν πραγματική αξία στο Bitcoin και στις εγγενείς δεξιότητες του, έχουν χρησιμοποιήσει παραδόξως μια συμβατική και αντισυμβατική προσέγγιση για να κατανοήσουν τι κάνει το Bitcoin παρόμοιο με τα παραδοσιακά χρηματοοικονομικά περιουσιακά στοιχεία, κάνοντάς το πρώτο στο είδος του. Αν και είναι πιθανό ότι κανένα άτομο δεν θα έχει την ίδια εγγενή αξία για το Bitcoin, η έλευση του Bitcoin στη σημερινή εποχή της πληροφορίας, δικαιολογεί μια μεθοδική επανεκτίμηση της έννοιας της «εγγενούς αξίας», του τρόπου με τον οποίο μετοχές, ομόλογα, ακίνητα, συλλεκτικά αντικείμενα και κυβερνητικά νομίσματα αποτιμώνται και γίνονται αντιληπτά. Έτσι, τα ψηφιακά περιουσιακά στοιχεία εμπίπτουν στο φάσμα της αξίας.

Καθώς περνά ο καιρός και το Bitcoin συνεχίζει να περιηγείται σε αχαρτογράφητα νερά, η εγγενής αξία του πιθανότατα να αλλάξει και ως εκ τούτου και η αγοραία του αξία. Έχοντας αυτό κατά νου, είναι χρήσιμο να γνωρίζουμε όλο και περισσότερο πως, γιατί και πότε το Bitcoin θα μπορούσε να έχει αξία και ποιες εννοιολογικές ομοιότητες μπορεί να έχει με τα παραδοσιακά χρηματοοικονομικά περιουσιακά στοιχεία. Αν και ο δρόμος είναι μπροστά για το Bitcoin είναι αβέβαιος, ένα είναι σίγουρο, ότι το Bitcoin έχει αξία.

# ΚΕΦΑΛΑΙΟ 5

# ΥΦΙΣΤΑΜΕΝΗ ΚΑΤΑΣΤΑΣΗ ΚΑΙ ΣΥΜΠΕΡΑΣΜΑΤΑ

## 5.1 Νομικό Πλαίσιο Του Bitcoin

Από τον Ιούνιο του 21, το Bitcoin ήταν νόμιμο στις ΗΠΑ, την Ιαπωνία, το Ηνωμένο Βασίλειο και τις περισσότερες ανεπτυγμένες χώρες. Στις ανεπτυγμένες αγορές, το νομικό καθεστώς του Bitcoin εξακολούθησε να ποικίλλει δραματικά. Η Κίνα περιόρισε σε μεγάλο βαθμό το Bitcoin χωρίς στην πραγματικότητα να ποινικοποιεί την κατοχή του. Η Ινδία απαγόρευσε στις τράπεζες να συναλλάσσονται με Bitcoin και άφησε το γενικό νομικό καθεστώς των κρυπτονομισμάτων ασαφές. Γενικά είναι απαραίτητο να εξεταστούν οι νόμοι για το Bitcoin σε συγκεκριμένες χώρες[56].

Ακόμα και όπου το Bitcoin είναι νόμιμο, οι περισσότεροι από τους νόμους που ισχύουν για άλλα περιουσιακά στοιχεία ισχύουν και για το Bitcoin. Η φορολογική νομοθεσία είναι ο τομέας όπου οι περισσότεροι άνθρωποι πιθανό να αντιμετωπίσουν προβλήματα. Για φορολογικούς σκοπούς, το Bitcoin αντιμετωπίζεται συνήθως ως ιδιοκτησία και όχι ως νόμισμα. Ωστόσο, υπάρχουν εξαιρέσεις, όπως το Ελ Σαλβαδόρ που έγινε η πρώτη χώρα που αναγνώρισε το Bitcoin ως νόμιμο χρήμα τον Ιούνιο του 2021[56].

Στις ΗΠΑ όπου γεννούνται τα νομοθετικά πλαίσια και συνήθως ακολουθούν και οι υπόλοιπες χώρες, η Υπηρεσία Εσωτερικών Εσόδων(IRS) έχει δείξει αυξανόμενο ενδιαφέρον για το Bitcoin και έχει εκδώσει οδηγίες. Το 2014, η υπηρεσία εξέδωσε ειδοποίηση IRS 2014-21 για να παρέχει πληροφορίες σχετικά με τη φορολογική μεταχείριση των εικονικών νομισμάτων. Το εικονικό νόμισμα είναι ο όρος που χρησιμοποιεί το IRS για κρυπτονομίσματα. Για το 2020, η IRS πρόσθεσε μία ερώτηση στην πρώτη σελίδα του εντύπου 1040 που απαιτεί από τους φορολογούμενους να δηλώνουν εάν συμμετείχαν σε συναλλαγές σε εικονικό νόμισμα[56].

Το Bitcoin υπάρχει σε μία απελευθερωμένη αγορά, επομένως δεν υπάρχει κεντρική αρχή έκδοσης. Οι διευθύνσεις Bitcoin δεν απαιτούν Αριθμούς Κοινωνικής Ασφάλισης (SSN) ή άλλες προσωπικές πληροφορίες, όπως τυπικούς τραπεζικούς λογαριασμούς. Αυτό αρχικά προκάλεσε ανησυχίες σχετικά με την χρήση του Bitcoin για παράνομη δραστηριότητα[56].

Στα πρώτα χρόνια του, η αντιληπτή ανωνυμία του Bitcoin οδήγησε σε πολλές παράνομες χρήσεις. Οι έμποροι ναρκωτικών ήταν γνωστό ότι το χρησιμοποιούσαν, με πιο

γνωστό παράδειγμα την αγορά του Silk Road. Ήταν ένα τμήμα του λεγόμενου σκοτεινού ιστού όπου οι χρήστες μπορούσαν να αγοράσουν παράνομα ναρκωτικά. Όλες οι συναλλαγές στο Silk Road χρησιμοποιούσαν Bitcoin. Τελικά έκλεισε από το FBI τον Οκτώβριο του 2013[56].

Ωστόσο, το Bitcoin έχει αρκετά σοβαρά ελαττώματα για όσους αναζητούν την ανωνυμία. Συγκεκριμένα, το Bitcoin δημιουργεί ένα μόνιμο δημόσιο αρχείο όλων των συναλλαγών. Μόλις ένα άτομο συνδεθεί με μια διεύθυνση, αυτό το άτομο μπορεί να συνδεθεί με άλλες συναλλαγές χρησιμοποιώντας αυτήν την διεύθυνση. Άλλα ανταγωνιστικά κρυπτονομίσματα παρέχουν πλέον καλύτερη προστασία απορρήτου. Δεδομένης αυτής της κατάστασης, η παράνομη δραστηριότητα απομακρύνεται από το Bitcoin.

## 5.2 Χώρες Όπου Το Bitcoin Είναι Νόμιμο Και Παράνομο

Ενώ ορισμένοι νομοθέτες και αξιωματούχοι ενδέχεται να μην υποστηρίζουν τη χρήση του λόγω έλλειψης ελέγχου και παράνομων δεσμών, πολλοί έχουν θεσπίσει κανονισμούς βάσει της νομοθεσίας της χώρας τους για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και την χρηματοδότηση της τρομοκρατίας (AML/CFT) σε προσπάθειες να μειώσουν τη χρήση του για αυτούς τους σκοπούς[57].

Η Price Waterhouse Coopers (PwC) δημιούργησε μία έκθεση για την παγκόσμια ρύθμιση των κρυπτονομισμάτων. Η έκθεση εντόπισε επιλεγμένες χώρες των οποίων οι κυβερνήσεις ανέθεσαν στους χρηματοοικονομικούς ρυθμιστικούς οργανισμούς τους να αναπτύξουν κανονισμούς και προτεραιότητες για τα χρηματοπιστωτικά ιδρύματα σχετικά με τα και τη χρήση τους σε AML/CFT[57].

Η PwC εντόπισε επίσης πολλές χώρες που δεν επιτρέπουν τη χρήση του Bitcoin. Παρακάτω παρουσιάζονται μερικές από τις χώρες που το Bitcoin και τα κρυπτονομίσματα είναι νόμιμα ή παράνομα.

### 5.2.1 Χώρες Όπου Το Bitcoin Είναι Νόμιμο

Ηνωμένες Πολιτείες

Το Δίκτυο Επιβολής Οικονομικών Εγκλημάτων του Υπουργείου Οικονομικών των ΗΠΑ έχει εκδώσει οδηγίες για το Bitcoin από το 2013. Το Υπουργείο Οικονομικών έχει ορίσει το Bitcoin ως μετατρέψιμο νόμισμα με ισοδύναμη αξία σε πραγματικό νόμισμα ή ως ένα νόμισμα που μπορεί να λειτουργήσει ως υποκατάστατο του[57].

Σύμφωνα με την ισχύουσα νομοθεσία των ΗΠΑ, κάθε οντότητα που διαχειρίζεται ή ανταλλάσσει Bitcoin, όπως ανταλλακτήρια κρυπτονομισμάτων που πρόσφατα μπήκαν στο «στόχαστρο», εμπίπτει στον ορισμό της επιχείρησης παροχής υπηρεσιών χρήματος (MSB). Ως εκ τούτου, ένα MSB υπόκειται στον νόμο περί τραπεζικού απορρήτου και πρέπει να εγγραφεί στο Υπουργείο Οικονομικών των ΗΠΑ και να υποβάλει αναφορές για συναλλαγές άνω των 10.000$[57].

Επιπλέον το Υπουργείο Οικονομικών των ΗΠΑ και το Δίκτυο Επιβολής Οικονομικών Εγκλημάτων έχουν δημιουργήσει στρατηγικές και βοηθούν σε νομοθετικές διαδικασίες για την ανάπτυξη κανονισμών, μαζί με τον καθορισμό εθνικών προτεραιοτήτων για την παρακολούθηση και την αναφορά κρυπτονομισμάτων[57].

Ευρωπαϊκή Ένωση

Η Ευρωπαϊκή Ένωση αναγνωρίζει το Bitcoin και άλλα κρυπτονομίσματα ως περιουσιακών στοιχείων κρυπονομισμάτων. Δεν είναι παράνομη η χρήση Bitcoin εντός της ΕΕ. Ωστόσο, η Ευρωπαϊκή Αρχή Τραπεζών, η ρυθμιστική αρχή νομίσματος στην Ένωση, δήλωσε ότι οι δραστηριότητες κρυπτονομισμάτων είναι εκτός του ελέγχου της και συνεχίζει να προειδοποιεί το κοινό και τις επιχειρήσεις για τους κινδύνους[57].

Το 2020, η Ευρωπαϊκή Επιτροπή ολοκλήρωσε την πρόταση νομοθεσίας για τη ρύθμιση των περιουσιακών στοιχείων κρυπονομισμάτων, την οποία εντός της Ένωσης έχουν εγκρίνει πολλοί οργανισμοί. Τροποποιήθηκε τα επόμενα δύο χρόνια και τον Οκτώβριο του 2022 στάλθηκε στην Ευρωπαϊκή Επιτροπή για ψηφοφορία μια τελική συμβιβασμένη έκδοση. Στις 20 Απριλίου 2023 το Ευρωπαϊκό Κοινοβούλιο ενέκρινε τον κανονισμό για τις αγορές περιουσιακών στοιχείων κρυπονομισμάτων (MiCA). Η MiCA ρυθμίζει τις υπηρεσίες που σχετίζονται με περιουσιακών στοιχείων κρυπονομισμάτων και stablecoins και θα τεθεί σε ισχύ στις αρχές του 2025[57].

Η νομοθεσία δεν διέπει τις κινητές αξίες των κρυπτονομισμάτων και τα NFTs. Σκοπός είναι να αποτρέψει τον κατακερματισμό των δημοσιονομικών ρυθμιστικών πλαισίων και να εξισορροπήσει τους όρους χρηματοοικονομικού ανταγωνισμού σε ολόκληρη την ΕΕ. Η

επιτροπή θέλει επίσης να διασφαλίσει ότι το κοινό έχει πρόσβαση και μπορεί να χρησιμοποιήσει με ασφάλεια τα κρυπτονομίσματα[57].

Καναδάς

Ο Καναδάς διατηρεί μια γενικά φιλική προς το Bitcoin στάση, όπως ο νότιος γείτονάς του, όπου το Αμερικανικό Bitcoin θεωρείται εμπόρευμα από την Canada Revenue Agency (CRA) για σκοπούς φορολογίας εισοδήματος. Οποιοδήποτε εισόδημα από την συναλλαγή με χρήση Bitcoin θεωρείται επιχειρηματικό εισόδημα ή κέρδος κεφαλαίου και πρέπει να αναφέρεται[57].

Ο Καναδάς θεωρεί τα ανταλλακτήρια κρυπτονομισμάτων ως επιχειρήσεις παροχής χρημάτων. Αυτό τους θέτει υπό την αρμοδιότητα του νόμου περί εσόδων από εγκλήματα (ξέπλυμα χρήματος) και περί χρηματοδότησης της τρομοκρατίας (καναδική έκδοση των νόμων AML/CFT). Ως αποτέλεσμα, τα ανταλλακτήρια κρυπτονομισμάτων πρέπει να εγγραφούν στο Κέντρο Ανάλυσης Χρηματοοικονομικών Συναλλαγών και Αναφορών του Καναδά (FINTRAC), να αναφέρουν ύποπτες συναλλαγές, να συμμορφώνονται με τα σχέδια συμμόρφωσης και ακόμη να τηρούν ορισμένα στοιχεία[57].

Αυστραλία

Όπως και ο Καναδάς, η Αυστραλιανή Φορολογική Υπηρεσία θεωρεί το Bitcoin ένα χρηματοοικονομικό περιουσιακό στοιχείο με αξία που μπορεί να φορολογηθεί όταν συμβαίνουν συγκεκριμένα γεγονότα. Για παράδειγμα, εάν πραγματοποιούνται συναλλαγές, ανταλλάσσεται, πουλιούνται, μετατρέπεται σε εγχώριο νόμισμα ενεργοποιείται ένας φόρος κεφαλαιουχικών κερδών. Απαιτείται επίσης να διατηρούνται αρχεία για τυχόν συναλλαγές που πραγματοποιούνται χρησιμοποιώντας το Bitcoin για φορολογικούς λόγους[57].

Γαλλία

Η Γαλλία έχει εφαρμόσει κανονισμούς για κρυπτονομίσματα και περιουσιακά στοιχεία κρυπτονομισμάτων, όπως προσδιορίζονται από τον Νομισματικό και Χρηματοοικονομικό Κώδικα (MFC). Η κυβέρνηση έχει ορίσει τα ψηφιακά περιουσιακά στοιχεία ως ψηφιακή χρησιμότητα, ψηφιακές πληρωμές και ψηφιακή ασφάλεια. Το MFC δεν ρυθμίζει τα NFT[57].

Οι υπηρεσίες ψηφιακών περιουσιακών στοιχείων ρυθμίζονται επίσης από τον κώδικα, ο οποίος περιλαμβάνει επιχειρήσεις που αγοράζουν ή πωλούν ψηφιακά στοιχεία, παρέχουν υπηρεσίες ανταλλαγής, ενεργούν για λογαριασμό τρίτων ή προσφέρουν συμβουλές[57].

Ελ Σαλβαδόρ

Το Ελ Σαλβαδόρ έγινε η πρώτη χώρα στον κόσμο που χρησιμοποίησε το Bitcoin ως νόμιμο χρήμα, αφού υιοθετήθηκε ως τέτοιο από τη Νομοθετική Συνέλευση της χώρας το 2021. Έχει προωθηθεί από τον Nayib Bukele, τον πρόεδρο του Ελ Σαλβαδόρ, ο οποίος ισχυρίστηκε ότι θα βελτίωνε την οικονομία διευκολύνοντας τις τραπεζικές συναλλαγές για τους κατοίκους[57].

Άλλες χώρες που το Bitcoin είναι νόμιμο είναι η Δανία, Γερμανία, Ιαπωνία, Ελβετία, Ισπανία και Ηνωμένο Βασίλειο.

### 5.2.2 Χώρες Όπου Το Bitcoin Είναι Παράνομο

Κίνα

Η Κίνα είναι η μεγαλύτερη χώρα που απαγορεύει όλα τα κρυπτονομίσματα. Ξεκίνησε την απαγόρευση των τοπικών ανταλλαγών κρυπτονομισμάτων το 2017 και σιγά σιγά προχώρησε σε πλήρη απαγόρευση με ότι σχετίζονται με κρυπτονομίσματα τον Σεπτέμβριο του 2021[58].

Σε αντίθεση με τις περισσότερες χώρες σε αυτήν την λίστα, το σκεπτικό της Κίνας για την απαγόρευση έχει να κάνει με τις ανησυχίες της Κεντρικής Κυβέρνησης ότι η παραοικονομία των κρυπτονομισμάτων θα μπορούσε να βλάψει την οικονομική ανάπτυξη της Κίνας[58].

Νεπάλ

Το Νεπάλ απαγόρευσε επίσης τα κρυπτονομίσματα τον Σεπτέμβριο του 2021. Η Nepal Rastra Bank, η κεντρική τράπεζα της χώρας, κήρυξε παράνομη την χρήση, την εξόρυξη και το εμπόριό τους. Ο λόγος για αυτήν την δραστική απόφαση φαίνεται να είναι ο φόβος των απατεώνων που άνθησε[58].

Αφγανιστάν

Το Αφγανιστάν απαγόρευσε επίσης τα κρυπτονομίσματα τον Σεπτέμβριο του 2021. Μετά την κατάκτηση της χώρας από το καθεστώς των Ταλιμπάν, η οικονομία κατέρρευσε. Ο μόνος τρόπος για συναλλαγές με τον έξω κόσμο ήταν η χρήση κρυπτονομισμάτων και συγκεκριμένα του Bitcoin και δημιουργήθηκε μια μεγάλη οικονομία μαύρης αγοράς[58].

Μπαγκλαντές

Το Μπαγκλαντές εντάχθηκε σε αυτήν την κατηγορία πολύ νωρίτερα από την Κίνα ή το Νεπάλ, κηρύσσοντας παράνομη κάθε δραστηριότητα που σχετίζεται με το Bitcoin και τα κρυπτονομίσματα το 2017. Η κυβέρνηση ισχυρίστηκε ότι η διακίνηση τους θα παραβίαζε τους νόμους της χώρας για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και ακόμη τον αντιτρομοκρατικό νόμο[58].

Μαρόκο

Το Μαρόκο απαγόρευσε τα κρυπτονομίσματα πριν από μερικά χρόνια, αλλά είναι η μόνη χώρα που μπορεί να ανατρέψει την απόφαση κάποια στιγμή το 2023. Έχει συνταχθεί νόμος που θα άλλαζε την κατάσταση των ψηφιακών νομισμάτων στο βασίλειο της Βόρειας Αφρικής, αν και οι νόμοι αυτοί θα είναι πολύ πιο αυστηροί από τους κανόνες των άλλων χωρών[58].

Αίγυπτος

Η Αίγυπτος είναι η τελευταία χώρα της Βόρειας Αφρικής που απαγόρευσε οποιαδήποτε μορφή δραστηριότητας των κρυπτονομισμάτων. Η απαγόρευση τέθηκε σε ισχύ το 2020, με την κεντρική τράπεζα να τονίζει ότι η αξία του Bitcoin δεν συνδέεται με κανένα υλικό περιουσιακό στοιχείο και ότι επιτρέπεται η διαπραγμάτευση μόνο αναγνωρισμένων εθνικών νομισμάτων στην χώρα[58].

Βολιβία

Η Βολιβία είναι η πρώτη χώρα που απαγόρευσε το Bitcoin και τα κρυπτονομίσματα. Από το 2014, οι Βολιβιανοί νομοθέτες ανησυχούσαν για τις επιπτώσεις που είχε το εμπόριο στην χώρα τους και στους κατοίκους της[58].

### 5.2.3 Συμπέρασμα

Οι κανονισμοί για τα κρυπτονομίσματα εξακολουθούν να αναπτύσσονται μέρα με την μέρα παγκοσμίως, καθώς συνεχίζουν να κερδίζουν σε χρήση και αποδοχή. Πολλές χώρες αναμένεται να θεσπίσουν νομοθεσία αφότου η ΕΕ εφαρμόσει την πρότασή της για το MiCA. Το νομοθετικό τοπίο θα συνεχίσει να αλλάζει καθώς ο χώρος ωριμάζει σχετικά με το τι είναι το Bitcoin και άλλα κρυπτονομίσματα-ένα περιουσιακό στοιχείο, νόμιμο χρήμα, νόμισμα, τρόπος πληρωμής ή όλα τα παραπάνω. Στον αντίποδα οι νόμοι μπορεί να φέρουν στην επιφάνεια πτυχές του χώρου όπου έρχονται σε σύγκρουση με τους κανόνες των χωρών αυτών.

## 5.3 Χώρες Με Υψηλό Πληθωρισμό Και Το Bitcoin

Μέρα με την μέρα το Bitcoin και τα άλλα κρυπτονομίσματα γίνονται όλο και πιο δημοφιλή. Υπάρχουν όμως ορισμένες τοποθεσίες σε όλον τον κόσμο, όπου η υιοθέτηση έχει αυξηθεί. Χώρες που βίωσαν πρόσφατα οικονομικές πολιτικές που οδηγούν σε πληθωρισμό και υπερπληθωρισμό, έχουν δει τους κατοίκους τους να στρέφονται στο Bitcoin ως εναλλακτική λύση στο ταχέως υποτιμούμενο εγχώριο νόμισμα[59].

Όπως έχει δείξει η ιστορία, σε ορισμένες περιπτώσεις όταν ο πληθωρισμός γίνεται αρκετά υπομονετικός, ολόκληρη η οικονομία θα στραφεί στην αποδοχή ενός εναλλακτικού νομίσματος, ακριβώς όπως η Ζιμπάμπουε άρχισε να δέχεται δολάρια ΗΠΑ έναντι του δικού της νομίσματος. Αυτή η μετάβαση σε μία πιο αξιόπιστη μορφή αποθήκευσης πλούτου θα μπορούσε να είναι το νόμισμα μιας άλλης χώρας, όπως το δολάριο ΗΠΑ, ο χρυσός, ή και ακόμα το Bitcoin[59].

### 5.3.1 Τι Προκαλεί Τον Πληθωρισμό

Υπάρχει μία σημαντική διαφορά μεταξύ της αιτίας και του αποτελέσματος του πληθωρισμού και δυστυχώς και τα δύο ονομάζονται «πληθωρισμός». Πιο συγκεκριμένα, η αιτία είναι ο «νομισματικός πληθωρισμός» (δηλαδή η αύξηση της προσφοράς χρήματος) και το αποτέλεσμα είναι ο «πληθωρισμός τιμών» (δηλαδή μία αύξηση στο κόστος αγαθών και

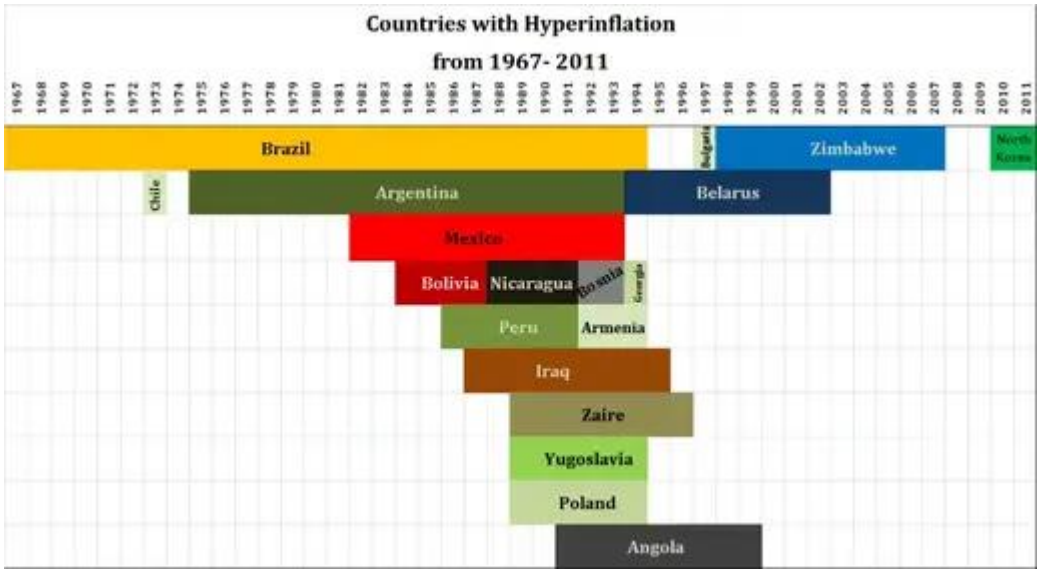
υπηρεσιών). Όταν η προσφορά χρήματος ξεφεύγει από τον έλεγχο και γίνεται πληθωριστική, απειλεί τον 5ο νόμο του χρήματος και αυτός είναι μία περιορισμένη προσφορά[59].

Ακόμη και σε χαμηλότερα επίπεδα πληθωρισμού όπως το 5%, οι καταναλωτές τείνουν να προσπαθούν να ξοδεύουν γρηγορότερα αντί να κρατούν το νόμισμα και να το αφήνουν να υποτιμηθεί. Αυτό αυξάνει την ταχύτητα του χρήματος (πόσο καιρό οι άνθρωποι κρατούν τα χρήματά τους), η οποία επίσης τροφοδοτεί τον πληθωρισμό, επειδή οι άνθρωποι είναι πρόθυμοι να αγοράσουν πράγματα σε υψηλότερη τιμή αντί να κρατήσουν το χρήμα που υποτιμάται. Αυτό μπορεί εύκολα να γυρίσει προς αντίθετη κατεύθυνση και να γίνει υπερπληθωρισμός[59].

Έτσι η κύρια αιτία του πληθωρισμού και στην συνέχεια του υπερπληθωρισμού είναι η κακή πολιτική της Κεντρικής Τράπεζας με την «δημιουργία υπερβολικής προσφοράς» ενός νομίσματος. Βέβαια συχνά δεν φταίνε οι Κεντρικές Τράπεζες επειδή η κυβέρνηση ξοδεύει περισσότερα από όσα εισπράττει, έτσι οι αρμόδιοι δίνουν εντολή στην Κεντρική Τράπεζα να τυπώσει περισσότερα χρήματα για να πληρώσει τους «λογαριασμούς» [59].

Ο υπερπληθωρισμός δεν είναι τόσο ασυνήθιστος. Παρακάτω είναι οι 19 χώρες με υπερπληθωρισμό την περίοδο 1967 έως 2011.

*Εικόνα 25-Χώρες με υπερπληθωρισμό.*




Κατά την διάρκεια αυτής της περιόδου το Bitcoin δεν ήταν ακόμα επιλογή, έτσι οι πολίτες συχνά τα αντικαθιστούσαν με πολύτιμα μέταλλα ή νομίσματα από άλλες χώρες. Σε εκείνο το σημείο τα καθεστώτα καταφεύγουν συχνά σε δρακόντεια νομοθεσία, που οδηγεί σε

ελέγχους τιμών και νομισματικούς ελέγχους για να διατηρήσουν την τάξη. Αυτό πάντα τελικά αποτυγχάνει καθώς οι πιέσεις στο σύστημα είναι μεγαλύτερες[59].

Τον τελευταίο καιρό, χώρες όπως οι Αργεντινή και η Βενεζουέλα, έχουν στραφεί στο Bitcoin ως εναλλακτική λύση στο τοπικό τους νόμισμα. Στην περίπτωση της Βενεζουέλας, η κυβέρνηση προσπάθησε να δημιουργήσει το δικό της κρυπτονόμισμα, το οποίο δεν λειτούργησε, καθώς εξακολουθούν να ελέγχουν τους μοχλούς της προσφοράς[59].

### 5.3.2 Πως βοηθάει το Bitcoin

Υπάρχει ένας λόγος για τον οποίο οι άνθρωποι που κατοικούν σε χώρες με μεγάλο πληθωρισμό και που η κυβέρνηση προσπαθεί να ελέγξει την δημόσια και ιδιωτική ζωή των ανθρώπων, στρέφονται στο Bitcoin. Ο ένας είναι ο παράγοντας της ιδιωτικότητας. Στην Βενεζουέλα, για παράδειγμα, τα ελεγχόμενα από τις τιμές ράφια είναι άδεια από είδη πρώτης ανάγκης, αλλά αν υπάρχει άλλο νόμισμα στην κατοχή( δολάριο ή Crypto) οι καταστηματάρχες βρίσκουν αυτά τα αγαθά εύκολα. Ένα πλεονέκτημα για την συγκεκριμένη περίπτωση αλλά και μειονέκτημα σε άλλες περιπτώσεις είναι ότι το Bitcoin κρύβεται πιο εύκολα και γίνεται ηλεκτρονικά η συναλλαγή[59].

Μία από τις ανησυχίες του Bitcoin και γενικά του κλάδου είναι η μεταβλητότητά του. Ως μέσο ανταλλαγής, ήταν δύσκολο για την αγορά να εκτιμήσει την αξία του. Αυτό σε συνδυασμό με διάφορες υποθέσεις οδήγησε σε υπερβολική πληθωρικότητα που προκαλεί υψηλή αστάθεια. Εν το μεταξύ, τα άτομα των χωρών αυτών με εγγυημένες απώλειες στο νόμισμα της χώρας τους, είναι πρόθυμα να προσαρμοστούν στο Bitcoin, αφού είναι πιο σταθερό από το τοπικό νόμισμα. Μέχρι τώρα όπως φαίνεται οι ακραίες αυτές συνθήκες των αδύναμων χωρών δίνουν το βήμα για το Bitcoin και όχι οι ανεπτυγμένες χώρες με δυνατά εγχώρια νομίσματα[59].

### 5.3.3 Παραδείγματα χωρών που στρέφονται στο Bitcoin

- Η Αργεντινή έχει υποφέρει επανειλημμένα από υπερπληθωρισμό. Προφανώς, δεν έχει σημασία ποιος είναι επικεφαλής της κυβέρνησης. Φαίνεται ότι πάντα ξοδεύουν περισσότερα από όσα έχουν. Μόλις τον Μάρτιο του 2019 ο πληθωρισμός τους ήταν γύρω στο 34%.
- Βενεζουέλα-οι ντόπιοι έχουν βιώσει δραματικό υπερπληθωρισμό για τα είδη πρώτης ανάγκης και ταυτόχρονα απαιτούν Bitcoin σε απίστευτες τιμές. Μόλις τον Μάρτιο του 2023 ο πληθωρισμός της Βενεζουέλας έφτασε το 439,6%.
- Τουρκία-η τοπική λίρα βρίσκεται σε πτώση εδώ και πολύ καιρό έναντι πολλών άλλων νομισμάτων. Κατά την διάρκεια αυτής της πτώσης, οι Τούρκοι και οι κάτοικοι της Τουρκίας στρέφονται στο Bitcoin. Ο πληθωρισμός της Τουρκίας έφτασε τον Οκτώβριο του 2022 στο 83%[59].

### 5.3.4 Συμπέρασμα

Ο καθορισμός ενός αποθηκευτικού χώρου αξίας που έχει μειωμένη προσφορά και διαφάνεια στο δίκτυο, επιτρέπει τον αποπληθωρισμό. Σε μεγάλη χρονική κλίμακα, το Bitcoin έχει επιτύχει αξιοσημείωτη διατήρηση αξίας, ενώ βραχυπρόθεσμα μπορεί να χαθεί στο «κύμα» από την μεγάλη αυξομείωση της τιμής.

Οι επενδυτές φυσικό είναι να αντιδρούν σε όλη την καταστροφή που φέρνει ο πληθωρισμός ποντάροντας εναντίον του και μετατρέποντας ένα εναλλακτικό στοιχείο όπως το Bitcoin στο πρωταγωνιστικό αστέρι το 2020. Το Bitcoin κληρονόμησε πολλά ίδια σημεία που έκανε τον χρυσό προτιμώμενο αντιστάθμισμα του πληθωρισμού. Αλλά όταν πρόκειται για την αντιστάθμιση έναντι του πληθωρισμού, όπως είπε ο Καναδός οικονομολόγος JP Konong: «Αν κοιτάξετε γύρω από το σπίτι σας, όλα αποτελούν αντιστάθμιση του πληθωρισμού. Το ίδιο σας το σπίτι, το τραπέζι, η εκπαίδευσή σας είναι αντιστάθμιση του πληθωρισμού, γιατί όλα αυτά τα πράγματα θα αυξηθούν σε αξία καθώς πέφτει η αγοραστική δύναμη του νομίσματος»[60].

## 5.4 Μπορεί το Bitcoin Να Αντικαταστήσει Τις Κεντρικές Τράπεζες;

Οι Κεντρικές Τράπεζες επηρεάζουν το παγκόσμιο χρηματοπιστωτικό σύστημα μέσω διαφόρων νομισματικών πολιτικών, οι οποίες τους επιτρέπουν να ρυθμίζουν τον πληθωρισμό και να διατηρούν την οικονομική τους σταθερότητα. Για παράδειγμα, μία Κεντρική Τράπεζα μπορεί να αυξήσει ή να μειώσει την προσφορά χρήματος που κυκλοφορεί στην οικονομία. Περισσότερο πλασματικό χρήμα που κυκλοφορεί σημαίνει ότι οι καταναλωτές ξοδεύουν περισσότερα μετρητά και ως αποτέλεσμα η οικονομία αναπτύσσεται.

Ωστόσο το Bitcoin ακολουθεί μια διαφορετική προσέγγιση ως νόμισμα. Αντίθετα από τα εγχώρια νομίσματα, η ανώτατη προσφορά του θα ανεβάσει την τιμή του καθώς αυξάνεται η ζήτηση. Όλες οι συναλλαγές είναι ασφαλείς, καθώς χρησιμοποιεί ένα προηγμένο σύστημα επικύρωσης που ονομάζεται «εξόρυξη».

### 5.4.1 Τα Πλεονεκτήματα του Bitcoin Έναντι Των Τραπεζών

Η ιδέα πίσω από το Bitcoin ήταν να εξαλειφθεί ο κεντρικός έλεγχος των χρημάτων από κυβερνητικούς φορείς και να διασφαλιστούν ασφαλείς συναλλαγές. Τα πλεονεκτήματα του Bitcoin έναντι των χρηματοπιστωτικών ιδρυμάτων:

- Αυτονομία χρήστη

Τα συμβατικά νομίσματα έχουν πολλαπλούς κινδύνους. Για παράδειγμα, ορισμένες τράπεζες είναι ευάλωτες σε κύκλους κατάρρευσης, ακόμη και σε αποτυχίες. Επομένως, δεν υπάρχει πλήρης έλεγχος των χρημάτων από τους πολίτες, ειδικά αν το σύστημα αποτύχει. Το Bitcoin παρέχει αυτονομία χρήστη, πράγμα που σημαίνει ότι οι ιδιοκτήτες κρυπτονομισμάτων έχουν πάντα πρόσβαση στα κεφάλαια τους[61].

- Ανωνυμία

Οι τράπεζες απαιτούν τα προσωπικά στοιχεία, όπως διεύθυνση κατοικίας, όνομα και ημερομηνία γέννησης, μεταξύ άλλων. Από την άλλη πλευρά, υπό ορισμένες συνθήκες συναλλαγών, το Bitcoin δεν απαιτεί την αποκάλυψη προσωπικών πληροφοριών, πράγμα που σημαίνει ότι οποιοσδήποτε έχει σύνδεση στο διαδίκτυο μπορεί να κατέχει το νόμισμα. Ωστόσο η πλήρης ανωνυμία μπορεί να είναι δύσκολη, καθώς όλες οι συναλλαγές μπορούν να εντοπιστούν στις διευθύνσεις πορτοφολίου[61].

- Συναλλαγές

Το Bitcoin χρησιμοποιεί ένα σύστημα πληρωμών peer-to-peer όπως έχει αναφερθεί, που επιτρέπει στους χρήστες να μεταφέρουν χρήματα από οπουδήποτε στον κόσμο. Αυτό σημαίνει ότι τα τέλη είναι πολύ πιο χαμηλότερα κατά την αποστολή χρημάτων διεθνώς. Το αρνητικό είναι ότι υπάρχει ένα σταθερό ελάχιστο ποσό που μπορεί να σταλεί.

Επίσης, οι συναλλαγές είναι ασφαλείς, γεγονός που καθιστά πιο δύσκολο για τους εγκληματίες να κλέψουν τα χρήματα των χρηστών. Όταν το blockchain ανιχνεύσει κακόβουλη δραστηριότητα, χωρίζεται και συνεχίζει να επεξεργάζεται τις συναλλαγές στη νόμιμη αλυσίδα[61].

- Προσιτότητα

Οι χρήστες του Bitcoin μπορούν να στέλνουν και να λαμβάνουν το νόμισμα ανώνυμα από οποιαδήποτε συσκευή με σύνδεση, παρέχοντας ένα συγκεκριμένο επίπεδο άνεσης, αρκεί να υπάρχει σύνδεση στο διαδίκτυο. Επίσης, οι αγορές δεν απαιτούν συστήματα τρίτων όπως οι τράπεζες, που σημαίνει ότι παρακάμπτεται ο μεσάζοντας, εξοικονομώντας χρόνο και χρήμα[61].

### 5.4.2 Τα Μειονεκτήματα του Bitcoin Έναντι Των Τραπεζών

Ενώ το Bitcoin παρέχει πλεονεκτήματα έναντι των τραπεζών, έχει πολλές αδυναμίες:

- Οι συναλλαγές είναι μη αναστρέψιμες

Ένα αρνητικό του Bitcoin είναι ότι δεν μπορεί κάποιος να ακυρώσει την συναλλαγή του. Επομένως, εάν κάποιος στείλει σε λάθος διεύθυνση, θα χαθεί για πάντα. Η συναλλαγή είναι μη αναστρέψιμη και κανένας δεν μπορεί να τροποποιήσει την κατάσταση[61].

- Αργή ταχύτητα μεταφοράς

Όταν το Bitcoin κυκλοφόρησε για πρώτη φορά το 2009, ήταν μία νέα τεχνολογία. Ωστόσο, σε σύγκριση με άλλα νομίσματα σήμερα, η ταχύτητα είναι σχετικά χαμηλή. Ως εκ τούτου, το Bitcoin θεωρείται από ορισμένους ως μέσο ανταλλαγής και αποθήκευσης αξίας όπως ο χρυσός αντί για ένα νόμιμο νόμισμα, καθώς υπάρχουν πολύ καλύτερες επιλογές αυτήν την στιγμή[61].

- Περιορισμένη χρήση

Αν και η αγορά των κρυπτονομισμάτων αναπτύσσεται με γρήγορους ρυθμούς, η χρήση του Bitcoin είναι περιορισμένη. Η υιοθέτηση είναι το κλειδί για την επιτυχία του Bitcoin.

Ωστόσο, μεγάλες εταιρείες δέχονται Bitcoin ως πληρωμή, όπως η Microsoft, PayPal, Whole Foods και Newegg[61].

### 5.4.3 Συμπέρασμα

Στο τρέχον οικονομικό σύστημα οι Κεντρικές Τράπεζες βρίσκονται στην κορυφή της παγκόσμιας οικονομίας. Εκτός από κάποια παραδείγματα που αναφέρθηκαν παραπάνω, το σύνολο των χωρών παγκοσμίως χρησιμοποιούν τις Κεντρικές Τράπεζες ως διαχειριστή των οικονομιών τους. Αν και έχει πολλά πλεονεκτήματα, η μεγάλη συγκέντρωση της εξουσίας σε μία αρχή, οδηγεί πολλές φορές σε πολύ σοβαρές οικονομικές υφέσεις.

Η τεχνολογία του Bitcoin αναδεικνύεται ως μία εναλλακτική λύση με το αποκεντρωμένο σύστημά του και την αλγοριθμική εμπιστοσύνη. Ωστόσο, το νομικό πλαίσιο των κρυπτονομισμάτων είναι ακόμα υπό αμφισβήτηση και με ελάχιστα ποσοστά υιοθέτησης. Εν το μεταξύ, είναι έτοιμες να προωθήσουν το δικό τους ψηφιακό νόμισμα που θα εκδίδεται από τις ίδιες, με στοιχεία τεχνολογίας και σχεδιασμού του Bitcoin.

Είναι πιο πιθανό σε αυτό το σημείο οι κεντρικές τράπεζες να αρχίσουν να εισάγουν τα δικά τους ψηφιακά νομίσματα κεντρικής τράπεζας (CBDC). Από το 2023, πολλές χώρες βρίσκονται σε διάφορα στάδια εξερεύνησης ευκαιριών CBDC, σχεδιασμού πιλοτικών προγραμμάτων CBDC και απόδειξης τις ιδέας για CBDC. Από τις 18 Μαΐου 2023, η Τζαμάικα και οι Μπαχάμες είναι οι μόνες χώρες που κυκλοφόρησαν επίσημα το δικό τους ψηφιακό νόμισμα.

## 5.5 Η Σημασία Των CBDCs

Πολλές κεντρικές τράπεζες, συμπεριλαμβανομένης της Ομοσπονδιακής Τράπεζας των ΗΠΑ, εξετάζουν το ενδεχόμενο να εισάγουν τα δικά τους ψηφιακά μετρητά, γνωστά ως ψηφιακό νόμισμα κεντρικής τράπεζας (CBDC). Για τους υποστηρικτές, τα CBDC υπόσχονται την ταχύτητα και άλλα οφέλη των κρυπτονομισμάτων χωρίς τους σχετικούς κινδύνους. Δεκάδες χώρες που αντιπροσωπεύουν περισσότερο από το 90% της παγκόσμιας οικονομίας, εξετάζουν τα CBDC. Έντεκα χώρες έχουν κυκλοφορήσει πλήρως τα CBDC. Από την πιλοτική εφαρμογή του ψηφιακού Γιουάν το 2019, η Κίνα αναμένεται να επεκτείνει το πιλοτικό της πρόγραμμα CBDC στον πληθυσμό της, που ξεπερνά το ένα δισεκατομμύριο μέχρι τέλους του 2023. Στις Ηνωμένες Πολιτείες, υπάρχει διαφωνία μεταξύ των αξιωματούχων της FED για την ανάγκη για ψηφιακό δολάριο[64].

Ένας τρόπος για την εφαρμογή των CBDCs θα ήταν οι πολίτες να έχουν λογαριασμούς απευθείας στην Κεντρική Τράπεζα. Αυτό θα έδινε στις κυβερνήσεις ισχυρούς νέους τρόπους διαχείρισης της οικονομίας. Οι πληρωμές κινήτρων και άλλα οφέλη θα μπορούσαν να πιστωθούν απευθείας στους πολίτες και η παρουσία της Κεντρικής Τράπεζας θα καθιστούσε τα CBDCs ένα ασφαλές ψηφιακό περιουσιακό στοιχείο. Αλλά η εισαγωγή τους θα μπορούσε επίσης να δημιουργήσει νέα προβλήματα, συγκεντρώνοντας μία τεράστια ποσότητα δύναμης, δεδομένων και κινδύνου σε μία ενιαία τράπεζα και δυνητικά θέτοντας σε κίνδυνο την ιδιωτική ζωή και την ασφάλεια στον κυβερνοχώρο[64].

Ορισμένοι ειδικοί υποστηρίζουν ότι η δυνατότητα των CBDCs να αποκόψουν τις εμπορικές τράπεζες ως μεσάζοντες εγκυμονεί κινδύνους, επειδή αυτές οι τράπεζες διαδραματίζουν κρίσιμο οικονομικό ρόλο, δημιουργώντας και κατανέμοντας πιστώσεις (δηλαδή δάνεια). Εάν οι άνθρωποι επέλεγαν να συναλλάζονται απευθείας με τη Fed, αυτό θα απαιτούσε από την Κεντρική Τράπεζα, είτε να διευκολύνει τον καταναλωτικό δανεισμό, κάτι που μπορεί να μην είναι εξοπλισμένη να κάνει, είτε να βρει νέους τρόπους για την εγγύηση πιστώσεων[64].

## 5.6 Υπάρχει Φούσκα Στο Bitcoin;

Είναι δύσκολο να πει κάποιος να υπάρχει φούσκα στο Bitcoin – εν μέρει επειδή είναι δύσκολο να προσδιοριστεί η πραγματική του αξία. Δύο παράγοντες κάνουν την εκτίμηση ιδιαίτερα δύσκολη.

- Το Bitcoin έχει ένα σύντομο ιστορικό. Οι νέες εταιρείες μπορεί να είναι ασταθείς, επομένως οι τιμές είναι επιρρεπείς σε γρήγορες και δραματικές αλλαγές καθώς η αγορά καθορίζει την δίκαια τιμή τους. Αυτές οι ξαφνικές ανατροπές τιμών μπορούν να δώσουν την εμφάνιση φούσκας που σχηματίζεται και σκάει.
- Το Bitcoin είναι θεμελιωδώς διαφορετικό. Οι επενδυτές έχουν μεθόδους να αξιολογήσουν την αξίας μίας εταιρείας, ακόμη και νέας. Αλλά αυτές οι προσεγγίσεις δεν λειτουργούν με το Bitcoin και τα άλλα κρυπτονομίσματα. Το Bitcoin δεν είναι εταιρεία και δεν παράγει έσοδα - ένας σημαντικός παράγοντας για τον προσδιορισμό της αξίας μίας εταιρείας[62].

Από το 2022 μέχρι σήμερα οι τιμές έχουν υποχωρήσει κατά πολύ. Ωστόσο, οι ειδικοί διαφωνούν για το αν πρόκειται για μία προσωρινή οπισθοδρόμηση ή για την αρχή του τέλους. Ταυτόχρονα, οι ρυθμιστικές αρχές αυξάνουν τον έλεγχο των κρυπτονομισμάτων, γεγονός που θα μπορούσε να υποδηλώνει ότι ενσωματώνεται περισσότερο στο χρηματοπιστωτικό σύστημα της χώρας. Επιπλέον, ορισμένες παραδοσιακές χρηματοοικονομικές εταιρείες, συμπεριλαμβανομένων των Fidelity, Visa και Mastercard, εργάζονται για να καθιερώσουν το Bitcoin[62].

### 5.6.1 Γιατί Μία Φούσκα Δεν Είναι Τόσο Κακή

Ορισμένοι οικονομολόγοι ισχυρίζονται ότι οι φούσκες είναι αναπόσπαστο κομμάτι της σωστής λειτουργείας της οικονομίας και μπορούν να παρακινήσουν μία μεγάλη εισροή επενδύσεων. Για παράδειγμα, η φούσκα dotcom είχε ως αποτέλεσμα την καλωδίωση οπτικών ινών σε παγκόσμια κλίμακα και την δημιουργία ενός παγκόσμιου δικτύου με τεράστια χωρητικότητα. Αυτήν η χωρητικότητα δεν ζητήθηκε στην πραγματικότητα και πολλές εταιρείες χρεοκόπησαν εξαιτίας της, αλλά διευκόλυνε την οικονομική ανάπτυξη τα επόμενα χρόνια και μείωσε την τιμή της διεθνούς επικοινωνίας[63].

Κατά την διάρκεια της κατάρρευσης των μετοχών dotcom, οι τίτλοι της Amazon έχασαν περίπου το 90% από το μέγιστο, δηλαδή ακόμα περισσότερο από το Bitcoin που έχασε το 2018 περίπου 80%. Στη συνέχεια, όταν η αγορά «καθάρισε», η Amazon κατάφερε όχι μόνο να καλύψει την διαφορά αλλά να αυξήσει σημαντικά την κεφαλαιοποίηση. Η ίδια κατάσταση μπορεί να παρατηρηθεί με το Bitcoin σήμερα[63].

## 5.7 Ναι Στην Τεχνολογία Blockchain Και Στο Bitcoin;

Στην πραγματικότητα, το Bitcoin και άλλα κρυπτονομίσματα θα δουν σίγουρα τόσο καλά όσο και κακά νέα τα επόμενα χρόνια. Σκοπός των ψηφιακών νομισμάτων είναι να αναδιαμορφώσουν τις χρηματοπιστωτικές αγορές σε παγκόσμια κλίμακα, αλλά ο δρόμος μπροστά φαίνεται δύσκολος γεμάτος με απροσδόκητες ανατροπές.

Οι κυβερνήσεις σε όλον τον κόσμο θα συνεχίσουν να προσπαθούν να ρυθμίσουν το Bitcoin και τα κρυπτονομίσματα. Κάποιοι θα αγκαλιάσουν την τεχνολογία ενώ άλλοι θα συνεχίσουν να επιβάλουν περιορισμούς. Αυτός ο «πόλεμος» μπορεί να δημιουργήσει περιόδους ακραίας αστάθειας[65].

Περισσότερες επιχειρήσεις πιθανότατα να χρησιμοποιήσουν το Bitcoin και άλλα κρυπτονομίσματα, με μικρό ρυθμό υιοθέτησης. Πολλές επιχειρήσεις θα αποστασιοποιηθούν από το ρίσκο, λόγω κινδύνων αστάθειας και ρυθμιστικών ανησυχιών. Επίσης το Bitcoin πιθανότατα να αποκτήσει σκληρό ανταγωνισμό από άλλα κρυπτονομίσματα και κυβερνητικά ψηφιακά νομίσματα. Το δίκτυο του Bitcoin είναι πιθανό να δει περαιτέρω βελτιώσεις, αλλά μικρές και σταδιακές. Βέβαια, οι αλλαγές στο πρωτόκολλο του Bitcoin απαιτούν την συναίνεση όλων των «εξορυκτών» και των χειριστών κόμβων, κάτι που είναι πολύ δύσκολο να επιτευχθεί[65].

Η τιμή του Bitcoin είναι πιθανό να παραμείνει ασταθής, με σημαντικές διακυμάνσεις των τιμών να αποτελούν τον κανόνα και όχι την εξαίρεση. Αυτή η αστάθεια μπορεί να μειωθεί καθώς η αγορά ωριμάζει[65].

Συμπερασματικά, ενώ το μέλλον του Bitcoin είναι αβέβαιο, ένα είναι το μόνο σίγουρο: το μέλλον είναι ψηφιακό και η μελλοντική παγκόσμια οικονομία θα επωφεληθεί από αυτές τις τεχνολογίες.

## 5.8 Γενικό Συμπέρασμα

Τις τελευταίες δεκαετίες παρατηρήθηκε μία έξαρση στην ανάπτυξη λογισμικών και τεχνολογικών καινοτομιών, όπως η τεχνολογία Blockchain, βάση της οποίας αναπτύχθηκε το Bitcoin. Η τεχνολογία αυτή δεν μπορεί να λύσει όλα τα προβλήματα και μάλιστα δημιουργεί νέα, όπως και άλλες τεχνολογίες του παρελθόντος. Ενδεχομένως στον μακροχρόνιο ορίζοντα να αποτελεί μία συνηθισμένη τεχνολογία, όπως το διαδίκτυο.

Η τεχνολογία του Blockchain, που αποτελεί μία διαφορετική φιλοσοφία από αυτή του κρατικού νομίσματος, ενσωματώθηκε από το οικοσύστημα του Bitcoin ώστε να αναπτύξει μία νέα μορφή ψηφιακών συναλλαγών. Αρχικά, η ύπαρξή της αναδείχθηκε αμελητέα για τους περισσότερους, αλλά στα μετέπειτα χρόνια αναδείχθηκε άξιο προσοχής. Το μεγαλύτερο πλεονέκτημά του αποτελεί ο αποκεντρωμένος χαρακτήρας του, που δεν αφήνει κανέναν οργανισμό να παρέμβει στην λειτουργεία του. Ένα ακόμα πλεονέκτημα αποτελεί η ανωνυμία των συναλλαγών, που από την άλλη όψη μπορεί να προσελκύσει την οργάνωση κάποιων παράνομών δραστηριοτήτων. Επίσης, η μεγάλη αυξομείωση της τιμής του Bitcoin, διογκώνεται σε περιόδους πολιτικοοικονομικών ανακατατάξεων. Η τεχνολογία της δημιουργίας των συστοιχιών και των συναλλαγών του Bitcoin απαιτεί πολύ μεγαλύτερη κατανόηση από το σημερινό πλαίσιο συναλλαγών.

Το Bitcoin αποτελεί μία ψηφιακή αναπαράσταση αξίας που δεν εκδίδεται από καμία κεντρική αρχή, που δεν συνδέεται με κανένα εγχώριο νόμισμα. Βέβαια, μπορεί να χρησιμοποιηθεί ως μέσο συναλλαγών από κάθε μορφής προσώπων, το οποίο μπορεί να αποθηκευτεί ηλεκτρονικά και να διευκολύνει με αυτόν τον τρόπο τις συναλλαγές χωρίς κάποιον ενδιάμεσο. Οι συναλλαγές γίνονται με ένα peer to peer σύστημα πληρωμών, ως ένα ψηφιακό συνάλλαγμα ανοιχτού κώδικα.

Διαπιστώθηκε ότι η νομιμότητα του Bitcoin, χρίζει διαφορετικής αντιμετώπισης και ποικίλει ανάλογα με την εκάστοτε χώρα. Η έλλειψη μίας παγκόσμιας νομοθετικής ρύθμισης για το Bitcoin και τα κρυπτονομίσματα, δημιουργεί προβλήματα νομοθετικά και φορολογικά. Σε κάποιες χώρες η συναλλαγές είναι πλήρως απελευθερωμένες, αναγνωρίζοντάς το ως μέσο ανταλλαγής αξίας ή περιουσιακό στοιχείο, ενώ σε άλλες είναι πλήρως απαγορευμένο. Οι χρηματοπιστωτικές ρυθμιστικές αρχές αντιμετωπίζουν ιδιαίτερες προκλήσεις όσον αφορά την ενημέρωση των κανόνων για την κάλυψη του Bitcoin και των άλλων κρυπτονομισμάτων και συναφών χρηματοοικονομικών προϊόντων που συχνά εμπίπτουν μεταξύ ρυθμιστικών ρωγμών.

Το ενδιαφέρον των θεσμικών επενδυτών οδηγεί το ευρύ ενδιαφέρον για το Bitcoin και τα κρυπτονομίσματα, αλλά τα ζητήματα σχετικά με τη φύλαξη, την ασφάλεια και την αποδοτικότητα του κεφαλαίου μπορεί να φέρει τα αντίθετα αποτελέσματα για το ψηφιακό περιουσιακό στοιχείο.

Η τεχνολογία που προσφέρει το Bitcoin αναπτύσσεται και βελτιώνεται συνεχώς, προσφέροντας στο παγκόσμιο ηλεκτρονικό εμπόριο το πλεονέκτημα της μεταφοράς διασυνοριακών πληρωμών με ένα πολύ μικρό ή αμελητέο ποσό, επηρεάζοντας την οικονομία και δημιουργώντας μία εγγενή αξία. Οι Κεντρικές Τράπεζες, υιοθετούν στοιχεία της τεχνολογίας του Bitcoin και στοχεύουν τα επόμενα χρόνια να κυκλοφορήσουν τα δικά τους κεντρικά ψηφιακά νομίσματα, βελτιώνοντας τις υπάρχουσες υπηρεσίες τους.

Κυριαρχεί πεποίθηση ότι η εγγενής αξία ενός νομίσματος προέρχεται από την διασφάλιση των κυβερνήσεων που τα εκδίδουν. Η εγγενής αξία του κυβερνητικού νομίσματος βασίζεται στο γεγονός ότι μπορεί να χρησιμοποιηθεί για την ανταλλαγή αξίας και την αποθήκευση αξίας, επειδή άλλοι βλέπουν αξία σε αυτό. Στον αντίποδα, το Bitcoin έχει χτίσει την φήμη του ως το πιο κρυπτογραφικά ασφαλές, αποκεντρωμένο και ευρέως διαδεδομένο ψηφιακό περιουσιακό στοιχείο. Η συνεχής αυξανόμενη εμπιστοσύνη που κερδίζει μέρα με την μέρα θα μπορούσε να οδηγήσει στο μέλλον σε μία συσσώρευση χρημάτων ως μέσο αποθήκευσης αξίας, εξισώνοντάς το με την πραγματική του εγγενή αξία.

Το μέλλον που υπόσχεται η τεχνολογική επανάσταση που έχει γεννήσει το Bitcoin είναι λαμπρό. Ενώ ενστερνίζονται το μετασχηματιστικό δυναμικό της τεχνολογίας blockchain προς όφελος των πολιτών τους, οι κυβερνήσεις θα πρέπει να διαδραματίσουν ενεργό ρόλο στη διαχείριση των τεχνολογικών, οικονομικών και κοινωνικών κινδύνων.

Ακόμα και αν τα κρυπτονομίσματα δεν πετύχουν, δεν υπάρχει αμφιβολία ότι η τεχνολογία του Bitcoin δημιούργησε έναν νέο και σημαντικό τομέα καινοτομίας. Όπως συμβαίνει με πολλούς άλλους τομείς, οι εταιρείες που χρησιμοποιούν την τεχνολογία του Bitcoin για να εργαστούν σε διάφορους και απλούς τομείς, όπως η βελτίωση των εγγράφων μεταφοράς εμπορευματοκιβωτίων, μπορεί να δημιουργήσουν μία μόνιμη εγγενής αξίας.

Το επόμενο Διαδίκτυο, ψηφιακός χρυσός ή κάτι άλλο; Η ιστορία του Bitcoin εξελίσσεται, οπότε προς το παρόν, μπορεί να είναι ό,τι πιστεύετε ότι είναι.

# ΒΙΒΛΙΟΓΡΑΦΙΑ

## Άρθρα Σε Επιστημονικά Περιοδικά

- Με ένα(1) Συγγραφέα


[10] Blockchain: Η τεχνολογία που αλλάζει για πάντα οικονομία και διαδίκτυο. (2017, December 10). Ανάκτηση από https://www.insider.gr/epiheiriseis/tehnologia/69555/blockchain-itehnologia-poy-allazei-gia-panta-oikonomia-kai-d

[7] Media, G. (2019). Blockchain: η τεχνολογία πίσω από το Bitcoin. Ανάκτηση από: https://www.basecoin.gr/blockchain-technologia-piso-apo-ta-kryptonomismata/

[8] Rodriguez, T. S. (2018, December 2). Blockchain for Dummies. Ανάκτηση από https://medium.com/swlh/blockchain-for-dummies-d3daf2170068

[9] Thamas, Y. (2019, March 11). The Importance of Blockchain Technology and Decentralization.

[16] PRENEEL, B. (2003, February). Analysis and Design of Cryptographic Hash Functions. Ανάκτηση από: https://www.e-reading.club/bookreader.php/141503/Analysis_and_Design_of_Cryptographic_Hash_Functions.pdf

[17] Jonathan Emmett, P. A. (2016). Method and system for protecting execution of cryptographic hash functions. Ανάκτηση από: https://patents.google.com/patent/WO2012129638A2/en

[1] Daniel. (2018, July 19). What's A Merkle Tree? A Simple Guide To Merkle Trees. Ανάκτηση από: https://komodoplatform.com/en/academy/whats-merkle-tree/

[2] Blaise Gassend, G. E. (2002). Caches and Merkle Trees for Efficient Memory Authentication. MIT Laboratory for Computer Science. Ανάκτηση από: https://people.csail.mit.edu/devadas/pubs/hpca03.pdf

[21] Paul, E. (2017, September 12). What is Digital Signature- How it works, Benefits, Objectives, Concept. Ανάκτηση από https://www.emptrust.com/blog/benefits-of-using-digitalsignatures

[22] TechTarget. (2020). Digital signature.

[23] DocuSign. (2018). Understanding digital signatures. Ανάκτηση από: https://www.docusign.com/how-it-works/electronic-signature/digital-signature/digital-signature-faq

[3] Audience, J. S.-G. (2018, May 6). How does blockchain work in 7 steps — A clear and simple explanation. Ανάκτηση από: https://blog.goodaudience.com/blockchain-for-beginners-what-is-blockchain-519db8c6677a

[20] Parikshit Hooda, G. (n.d.). Proof of Work (PoW) Consensus. Ανάκτηση από https://www.geeksforgeeks.org/proof-of-work-pow-consensus/

[30]13 Χρόνια bitcoin. Ανάκτηση από The Power Game: https://www.powergame.gr/crypto-power/178555/13-chronia-bitcoin-i-istoria-apo-to-miden-sta-69-000-dolaria/

[32]Plassaras, N. A. (2013). Regulating digital currencies: bringing Bitcoin within the reach of IMF. Ανάκτηση από: https://chicagounbound.uchicago.edu/cjil/vol14/iss1/12/

[33] Mavreli, K., & Μαυρέλη, Κ. (2015). Το ψηφιακό νόμισμα Bitcoin. Ανάκτηση από: https://apothesis.lib.hmu.gr/handle/20.500.12688/5673

[34] Sassower, R. (2013). Legality and Morality: Intellectual Property, Virtual Currency, and Corporate Responsibility. Ανάκτηση από: https://link.springer.com/chapter/10.1057/9781137312402_4

[37] Bitcoin Hash Functions Explained. Ανάκτηση από CoinDesk: Bitcoin Hash Functions Explained - CoinDesk

[38] What Is A Bitcoin Nonce [Simple]. Ανάκτηση από The Money Morgens: What Is A Bitcoin Nonce [Simple]? (themoneymongers.com)

[42] Cambrige (2021) Bitcoin Electricity Consumption Index Πηγή: https://ccaf.io/cbnsi/cbeci/comparisons

[44] Global Energy Review 2020. Ανάκτηση από IEA : https://www.iea.org/reports/global-energy-review-2020/renewables

[45] Genesis Mining Transforms Excess Bitcoin Datacenter Heat to Greenhouse Power in Sweden (2020). Ανάκτηση από Remitano : https://remitano.com/news/eu/7739-genesis-mining-transforms-excess-bitcoin-datacenter-heat-to-greenhouse-power-in-sweden

[46] Bitcoin's Energy Consumption Is A Highly Charged Debate – Who's Right? Ανάκτηση από Forbes: https://www.forbes.com/sites/lawrencewintermeyer/2021/03/10/bitcoins-energy-consumption-is-a-highly-charged-debate--whos-right/?sh=1b4a31f97e78

[47] Gold εξορύκτες must ramp up renewable energy to meet climate goals: industry group (2020). Ανάκτηση από Reuters: https://www.reuters.com/article/us-mining-gold-emissions-idUSKBN28J0Z4

[48] North American crypto εξορύκτες prepare to challenge China's dominance (2021). Ανάκτηση από Cointelegraph: https://cointelegraph.com/magazine/north-american-crypto-εξορύκτες-prepare-to-challenge-chinas-dominance/

[49] Gazprom Neft Mines Bitcoin as an Alternative to Flaring Unwanted Gas (2021). Ανάκτηση από JPT: https://jpt.spe.org/gazprom-neft-mines-bitcoin-as-an-alternative-to-flaring-unwanted-gas

[50] Bitcoin is Key to an Abundant, Clean Energy Future (2021). Ανάκτηση από Square: https://assets.ctfassets.net/2d5q1td6cyxq/5mRjc9X5LTXFFihIlTt7QK/e7bcba47217b60423a01a357e036105e/BCEI_White_Paper.pdf

[51] Στατιστικά στοιχεία από GOBANKINGRATE Ανάκτηση από: https://www.gobankingrates.com/money/economy/how-much-money-is-in-the-world/

[53] World Gold Council(2011) Ανάκτηση από: World Gold Council. Liquidity in the global gold market.

[54] KRAKEN INTELLIGENCE (2020). The Great Debate BITCOIN & INTRINSIC VALUE. Ανάκτηση από: https://blog.kraken.com/news/what-is-bitcoins-intrinsic-value-our-new-kraken-intelligence-report-explores

[58] Countries where Bitcoin is illegal(2023) Ανάκτηση από Cloudwards: Where Is Crypto Illegal in 2023 [A Full List of Countries] (cloudwards.net)

[59] How High Inflation Drives Countries Towards Crypto (2021). Ανάκτηση από inflationData: How High Inflation Drives Countries Towards Crypto (inflationdata.com)

[60] Bitcoin and Inflation: Everything You Need to Know (2021). Ανάκτηση από CoinDesk: Bitcoin and Inflation: Everything You Need to Know - CoinDesk

[61] Can Bitcoin Kill Central Banks? (2021). Ανάκτηση από SOUK: Can Bitcoin Kill Central Banks? - Shout Out UK

[62] Bitcoin Bubble: Definition and What Investors Need to Know (2022). Ανάκτηση από Nerdwallet: Bitcoin Bubble: Definition and What Investors Need to Know - NerdWallet

[63] Is Bitcoin a Bubble? (2020). Ανάκτηση από Freewallet: Is Bitcoin a Bubble? | Freewallet

[65] What's the Future of Bitcoin? (2023). Ανάκτηση από The Money Fool: What's the Future of Bitcoin? Here Are the Best, Worst, and Most Likely Scenarios. | The Motley Fool

[66] Valuing Bitcoin: what are the challenges & solutions? (2021). Ανάκτηση από: Valuing Bitcoin: what are the challenges & solutions? (fintoniagroup.com)

[67] Horst Treiblmaier (August 2022) Ανάκτηση από: Do Cryptocurrencies Really Have (no) Intrinsic Value?

- Με δύο(2) Συγγραφείς

[31]Duivestein, S., &Savalle, P. (2014). Bitcoin: It's the Platform, Not the Currency, Stupid! Ανάκτηση από: https://www.worldcc.com/Resources/Content-Hub/View/ArticleId/7030/Bitcoin-Its-the-platform-not-the-currency-stupid

[64] Cryptocurrencies, Digital Dollars, and the Future of Money (2023). Ανάκτηση από cfr: Cryptocurrencies, Digital Dollars, and the Future of Money | Council on Foreign Relations (cfr.org)

[6] W. Diffie, M. H. (1976, November). New directions in cryptography. IEEE. Ανάκτηση από: https://www-ee.stanford.edu/~hellman/publications/24.pdf

- Με τρεις(3) συγγραφείς

[5] R.L. Rivest, A. S. (1977). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Ανάκτηση από: https://dl.acm.org/doi/10.1145/359340.359342

- Με τέσσερεις(4) συγγραφείς

[24] Amitai Porat, A. P. (2018). Blockchain Consensus: An analysis of Proof-of-Work and its applications. Ανάκτηση από: https://www.scs.stanford.edu/17au-cs244b/labs/projects/porat_pratap_shah_adkar.pdf

- Με πέντε(5) συγγραφείς

[18] Fan Zhang, I. E. (2017, August 18). REM: Resource-Efficient Mining for Blockchains. Ανάκτηση από: https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-zhang.pdf

[19] Arthur Gervais, G. O. (2016, October). On the Security and Performance of Proof of Work Blockchains. Ανάκτηση από: https://eprint.iacr.org/2016/555.pdf

[11] Zibin Zheng, S. X. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. 2017 IEEE 6th International Congress on Big Data. Ανάκτηση από: https://www.henrylab.net/wp-content/uploads/2017/10/blockchain-conference-2017.pdf

- Με επτά(7) συγγραφείς

[43] Apolline Blandin, Dr. Gina Pieters, Yue Wu, Thomas Eisermann, Anton Dek, Sean Taylor, Damaris Njoki (2020). 3RD GLOBAL CRYPTOASSET BENCHMARKING STUDY. Ανάκτηση από: https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/3rd-global-cryptoasset-benchmarking-study/

## Βιβλία

Ευστάθιος Ζάχος, Α. Π. (2015). Υπολογιστική Κρυπτογραφία.

[15] WILLIAM, S. (2012). ΚΡΥΠΤΟΓΡΑΦΙΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ. ΙΩΝ

[4] Antonopoulos, A. M. (2014). Mastering Bitcoin.

[28] Marco Danelutto, P. F. (2017). Making Grids Work: Proceedings of the CoreGRID Workshop on Programming Models Grid and P2P System Architecture Grid Systems. Heraklion, Crete, Greece.

## Ιστοσελίδες

[13] Βικιπαίδεια. (n.d.). Blockchain. Ανάκτηση από https://el.wikipedia.org/wiki/Blockchain

[12] Academy, B. (n.d.). Peer-to-Peer Networks Explained. Ανάκτηση από https://academy.binance.com/blockchain/peer-to-peer-networks-explained

[14] Wiki, P. F. (2019). Peer to Peer. Ανάκτηση από https://wiki.p2pfoundation.net/Peer_to_Peer

[25] From Wikipedia, t. f. (2020). Peer-to-peer. Ανάκτηση από https://en.wikipedia.org/wiki/Peer-to-peer

[24]From Binance Academy. Ανάκτηση από https://academy.binance.com/en/glossary/selfish-mining

[29]From kriptomat. Ανάκτηση από https://kriptomat.io/gr/kryptonomismata/mia-syntomi-istoria-ton-kryptonomismaton/

[36] Βικιπαίδεια. (n.d.). Bitcoin. Ανάκτηση από Bitcoin - Βικιπαίδεια (wikipedia.org)

[39] Τι είναι το Bitcoin. Ανάκτηση από PCsteps : Τι είναι το Bitcoin Και Αξίζει Να Ασχοληθείς Μαζί Του? | PCsteps.gr

[40] Πως δημιουργούνται τα Bitcoins (2014). Ανάκτηση από Bitcoinx: https://bitcoinx.gr

[52] Invistopedia money terms. Ανάκτηση από https://www.investopedia.com/terms/m/m1.asp

[55] Invistopedia Bitcoin Value. Ανάκτηση από: https://www.investopedia.com/ask/answers/100314/why-do-bitcoins-have-value.asp

[56] Invistopedia Is Bitcoin legal. Ανάκτηση από: https://www.investopedia.com/ask/answers/121515/bitcoin-legal-us.asp

[57] Invistopedia Countries where Bitcoin is legal. Ανάκτηση από: Χώρες όπου το Bitcoin είναι νόμιμο και παράνομο (investopedia.com)

## Εκπαιδευτικά βίντεο

[35] CuriousInventor, (2014) «The essence of how bitcoin Works(non technical)». Βίντεο (διαδικτυακό). Ανακτήθηκε στις 22/5/2016. Διαθέσιμο στον διαδικτυακό τόπο: YouTube

[41] Cryptovios, (2021) «Η εγγενής αξία του Bitcoin». Βίντεο (διαδικτυακό). Ανακτήθηκε στις 23/04/2021. Διαθέσιμο στον διαδικτυακό τόπο: YouTube