ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

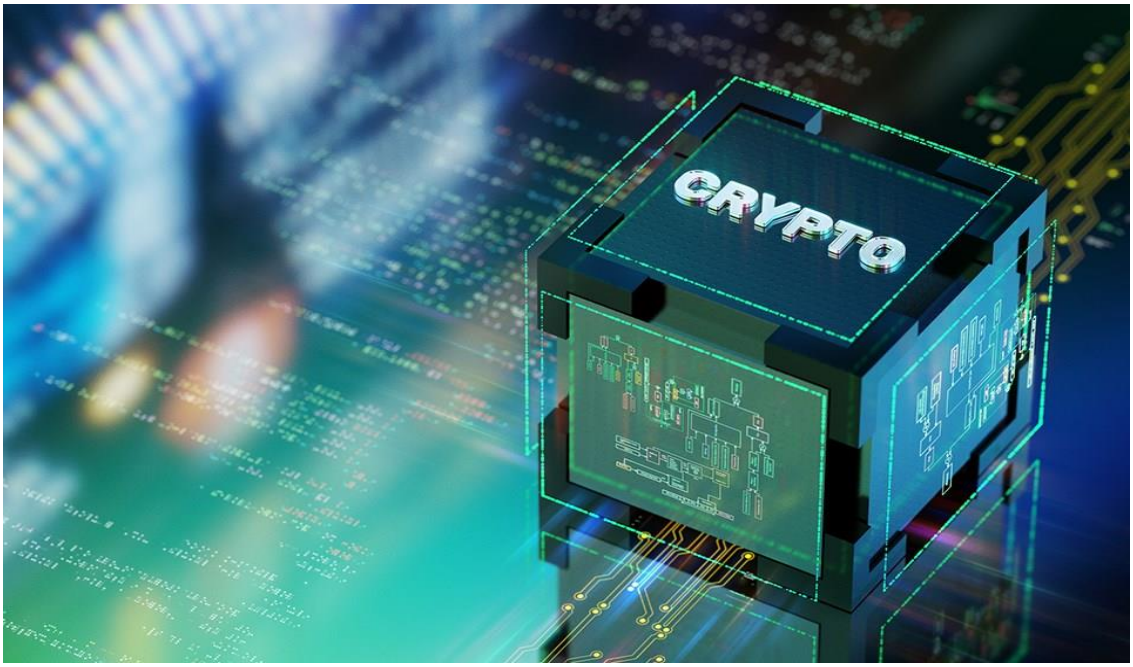
ΤΜΗΜΑ ΟΡΓΑΝΩΣΗΣ ΚΑΙ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΣΤΗ ΔΙΟΙΚΗΣΗ ΕΠΙΧΕΙΡΗΣΕΩΝ (MBA)

Διπλωματική Εργασία

Η Αγορά των Κρυπτονομισμάτων



Επιβλέπων καθηγητής: Ν. Φίλιππας

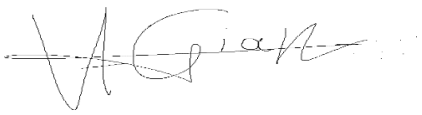
Γιακουμόπουλος Αναστάσιος

Πειραιάς 2024

«Δηλώνω υπεύθυνα ότι η διπλωματική εργασία για τη λήψη του μεταπτυχιακού τίτλου σπουδών, του Πανεπιστημίου Πειραιώς, στη Διοίκηση Επιχειρήσεων: MBA με τίτλο: «Η Αγορά των Κρυπτονομισμάτων (The cryptocurrency market)» έχει συγγραφεί από εμένα αποκλειστικά και στο σύνολό της. Δεν έχει υποβληθεί ούτε έχει εγκριθεί στο πλαίσιο κάποιου άλλου μεταπτυχιακού προγράμματος ή προπτυχιακού τίτλου σπουδών, στην Ελλάδα ή στο εξωτερικό, ούτε είναι εργασία ή τμήμα εργασίας ακαδημαϊκού ή επαγγελματικού χαρακτήρα.

Δηλώνω επίσης υπεύθυνα ότι οι πηγές στις οποίες ανέτρεξα για την εκπόνηση της συγκεκριμένης εργασίας, αναφέρονται στο σύνολό τους, κάνοντας πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου»

Υπογραφή Μεταπτυχιακού φοιτητή/τριας:



Ονοματεπώνυμο: Γιακουμόπουλος Αναστάσιος

Ημερομηνία: 17/08/2024

Ευχαριστίες

Θα ήθελα να ευχαριστήσω την οικογένεια μου για την στήριξη της και τον καθηγητή μου Ν. Φίλιππα που ήταν δίπλα μου κατά την συγγραφή της εργασίας.

Περίληψη

Με την πάροδο των ετών όλο και περισσότερο ακούγεται ο όρος «κρυπτονομίσματα». Ο στόχος και η συμβολή αυτής της διατριβής είναι να δώσει στον αναγνώστη την κατάλληλη γνώση για το τι είναι η αγορά των Κρυπτονομισμάτων και τι είναι τα κρυπτονομίσματα με πολύ απλά λόγια. Ξεκινώντας από την δημιουργία τους και φτάνοντας μέχρι το στάδιο αποτυχίας τους. Ιδιαίτερο ενδιαφέρον παρουσιάζουν τα πολλά χαρακτηριστικά που κατέχουν και οι πολλές κατηγορίες που τα διακρίνουν. Επιπλέον αυτή η διατριβή φιλοδοξεί να εξηγήσει στον αναγνώστη τον τρόπο λειτουργίας των Κρυπτονομισμάτων μέσω της ανάλυσης της τεχνολογίας Blockchain, εξηγώντας τον τρόπο λειτουργίας της τεχνολογίας, την συνεισφορά των χρηστών σε αυτήν αλλά και τα πεδία εφαρμογής της πέραν της αγοράς Κρυπτονομισμάτων. Στην συνέχεια αναλύεται η πορεία αλλά και η κυριαρχία του κύριου εκπρόσωπου των Κρυπτονομισμάτων έναντι των υπολοίπων, του Bitcoin. Εν κατακλείδι, εξηγούνται διάφοροι τρόποι συναλλαγών στα κρυπτονομίσματα, δίνοντας έτσι στον αναγνώστη την γνώση για το τρόπο αλλά και το μέρος για να αγοράζει και να πουλάει αυτά τα ψηφιακά περιουσιακά στοιχεία που φαίνεται ότι είναι απαραίτητα σε ένα ολιστικό χαρτοφυλάκιο .

Abstract

Over the years, the term «cryptocurrencies» has been increasingly heard. The goal of this thesis is to provide the reader with the appropriate knowledge about what the cryptocurrency market is and what cryptocurrencies are. Starting from their creation and reaching the point of their potential failure. The numerous characteristics they possess and the various categories that distinguish them are of particular interest. Additionally, this thesis aims to explain to the reader how cryptocurrencies function through an analysis of blockchain technology, detailing how the technology operates, the contribution of users to it, as well as its applications beyond the cryptocurrency market. Following this, the journey and dominance of the main representative of cryptocurrencies, Bitcoin, over the others is analyzed. Lastly, various methods of cryptocurrency transactions are explained, providing the reader with the knowledge of how and where to buy and sell these digital currencies.

Κεφάλαια

Κεφάλαια Πινάκων και εικόνων

1. Εισαγωγή

Η εξέλιξη του χρήματος έχει παραλληλιστεί στενά με την πρόοδο της τεχνολογίας, από τα πρώτα συστήματα ανταλλαγής έως τα σύγχρονα ψηφιακά νομίσματα. Καθώς τα παγκόσμια χρηματοοικονομικά γίνονται ολοένα και περισσότερο ψηφιοποιημένα οι εναλλακτικές επενδύσεις και συγκεκριμένα τα κρυπτονομίσματα έχουν αναδειχθεί ως μια ανατρεπτική δύναμη. Τα κρυπτονομίσματα αντιπροσωπεύουν μια ριζική απομάκρυνση από τις παραδοσιακές μορφές χρήματος, προσφέροντας αποκεντρωμένες, ψηφιακές λύσεις που αμφισβητούν τα ίδια τα θεμέλια των συμβατικών χρηματοπιστωτικών συστημάτων. Το χρήμα, στις παραδοσιακές του μορφές, χρησιμεύει από καιρό ως μέσο ανταλλαγής, όπου με ευκολία ένα νόμισμα μπορεί να ανταλλαχθεί για προϊόντα ή υπηρεσίες Επιπλέον χρησιμεύει ως μέσο αποθήκευσης αξίας καθώς μπορεί να αποθηκευτεί και να ανακτηθεί στο μέλλον με κάποιου είδους πρόβλεψη για τη μελλοντική του αξία. Ενώ ακόμα χρησιμεύει και ως μονάδα μέτρησης αξιών διότι διαμορφώνει την ανταλλακτική αξία κάθε εμπορεύματος σε όρους χρήματος. Ωστόσο, η έλευση της τεχνολογίας Blockchain και η άνοδος Κρυπτονομισμάτων όπως το Bitcoin και το Ethereum έχουν επαναπροσδιορίσει αυτούς τους ρόλους.

Τα κρυπτονομίσματα προσφέρουν νέους δρόμους για επενδύσεις, λειτουργώντας ανεξάρτητα από τις κεντρικές αρχές και παρέχοντας ευκαιρίες για διαφοροποίηση πέρα από τις συμβατικές κατηγορίες περιουσιακών στοιχείων, όπως μετοχές και ομόλογα. Οι εναλλακτικές επενδύσεις, συμπεριλαμβανομένων των περιουσιακών στοιχείων κρυπτογράφησης, έχουν κερδίσει την έλξη για τη δυνατότητά τους να προσφέρουν υψηλές αποδόσεις, αν και συχνά συνοδεύονται από αυξημένη αστάθεια και κίνδυνο. Η εξέλιξη της τεχνολογίας έχει επιταχύνει την ανάπτυξη της αγοράς Κρυπτονομισμάτων, επιτρέποντας την ανάπτυξη αποκεντρωμένων χρηματοοικονομικών συστημάτων και εφαρμογών.

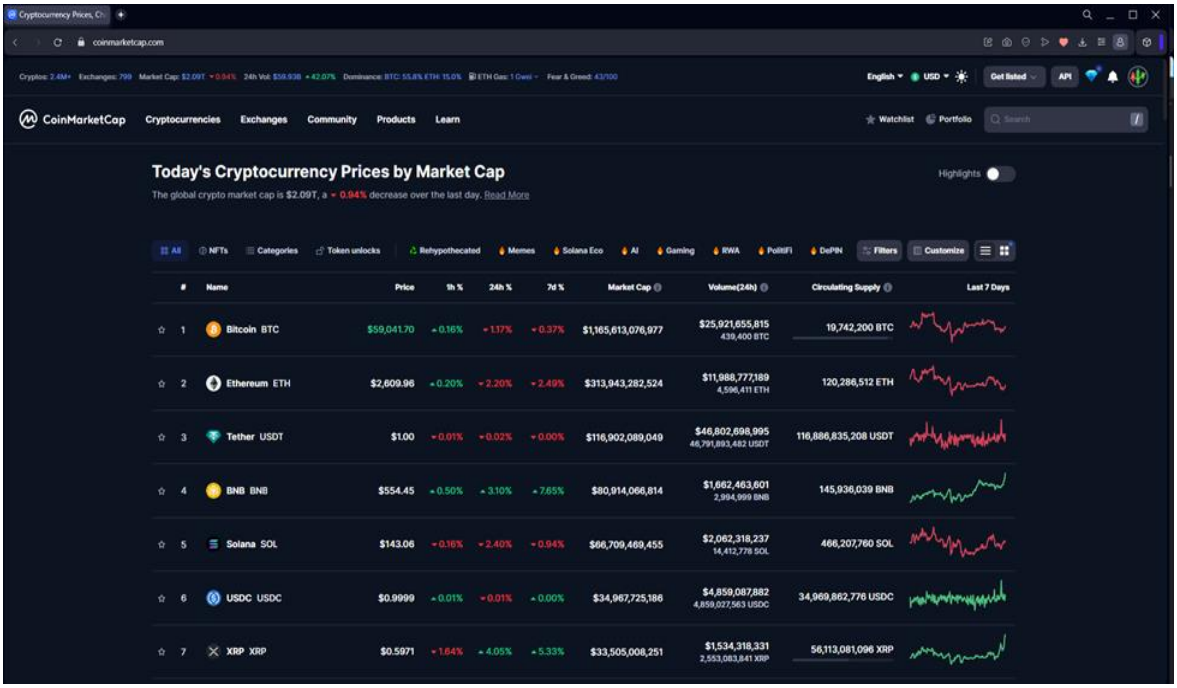
1.1 Κρυπτονομίσματα

Αντίθετα με το μοντέλο των κλασσικών επενδύσεων που έχει προαναφερθεί υπάρχουν και οι εναλλακτικές επενδύσεις. Μια από αυτές όπως προαναφέρθηκε είναι τα κρυπτονομίσματα, αλλά τι είναι ακριβώς είναι αυτά? Τα Κρυπτονομίσματα είναι μια μορφή ψηφιακού ή εικονικού νομίσματος που χρησιμοποιεί κρυπτογραφία για την ασφάλεια, καθιστώντας αδύνατη την παραχάραξη. Η λέξη Κρυπτονόμισμα απαρτίζεται από δυο μέρη, το πρώτο συνθετικό περιλαμβάνει την λέξη κρυπτο η οποία πηγάζει από την συντομογραφία της λέξης κρυπτογραφία, ενώ ως δεύτερο συνθετικό απαρτίζεται από την λέξη νόμισμα. Ο όρος κρυπτογραφία αναφέρεται σε διάφορες τεχνικές ασφαλούς επικοινωνίας και κρυπτογράφησης. Στο οικοσύστημα των Κρυπτονομισμάτων, η κρυπτογραφία διαδραματίζει βασικό ρόλο στη διασφάλιση της ασφάλειας των συναλλαγών, στη διαχείριση της δημιουργίας νέων μονάδων και στον έλεγχο της ταυτότητας κατά την μεταφορά περιουσιακών στοιχείων. Τα κρυπτονομίσματα είναι συνήθως αποκεντρωμένα, δεν υπάγονται σε κάποια κεντρική εξουσία και λειτουργούν με μια τεχνολογία που ονομάζεται Blockchain.

Αρχικά προωθήθηκαν ως ένα εναλλακτικό μέσο πληρωμών διαθέσιμο παγκοσμίως για την εκτέλεση διασυνοριακών συναλλαγών. Επειδή όμως με τον καιρό δεν μπόρεσαν να κρατήσουν ένα επίπεδο σταθερότητας και να λειτουργούν ως ένα αποτελεσματικό μέσο ανταλλαγής, οι κάτοχοι τους στράφηκαν στην δεύτερη φύση τους, την επενδυτική. Τα κρυπτονομίσματα κατέχουν μόνο ψηφιακή μορφή και δεν υπόκεινται σε υλική μορφή όπως τα συμβατικά νομίσματα (Fiat Coins) που διατίθενται στην αγορά. Οι τρόποι απόκτησης των Κρυπτονομισμάτων πραγματοποιούνται μέσω ψηφιακών ανταλλακτηρίων, μέσω ενός τρόπου εξόρυξης (mining), μέσων μηχανημάτων ATM, ή και με την απευθείας μεταφορά τους από ένα ψηφιακό πορτοφόλι σε ένα άλλο. (Sergeenkov, 2021)

Εικόνα 1 Απεικόνιση ενδεικτικών Κρυπτονομισμάτων (Hyatt.2021)

Στην παρακάτω φωτογραφία αναπαρίσταται η λιστα με τα καλύτερα κρυπτονομίσματα που υπάρχουν στην αγορά σύμφωνα με το coinmarketcap. Το coinmarketcap θα αναφερθει συχνά μιας και είναι ο μεγαλύτερος ιστότοπος παρακολούθησης τιμών κρυπτονομισμάτων καθώς κατέχει κατατάξεις, γραφήματα και πληροφορίες για αυτά. Πληροφορίες όπως τη διαθέσιμη προσφορά, δηλαδή ο αριθμός των νομισμάτων που διατίθενται στην αγορά, τη τιμή που κατέχουν την δεδομένη χρονική στιγμή, ο όγκος των συναλλαγών που πραγματοποιούνται καθημερινά, η κεφαλαιοποίηση της αγοράς, η οποία δείχνει την αξία που οι επενδυτές τοποθετουν σε ένα νόμισμα και πολλά ακόμη



Εικόνα 2 ο ιστότοπος και τα χαρακτηριστικά του Coinmarketcap (Coinmarketcap.com)

1.2 Ιδιότητες Κρυπτονομισμάτων

Τα κρυπτονομίσματα βασίζονται σε λειτουργίες ομότιμων (peer to peer) δικτύων και όχι σε κάποιον κεντρικό διακομιστή (server). Οι ίδιοι οι χρήστες ελέγχουν το δίκτυο και πιστοποιούν τις συναλλαγές καθώς η ασφάλεια του δικτύου ανήκει κατά αποκλειστικότητα μόνο σε εκείνους που συμμετέχουν. Οι συναλλαγές Peer-to-peer (P2P) περιλαμβάνουν την άμεση ανταλλαγή περιουσιακών στοιχείων μεταξύ δύο χρηστών χωρίς την ανάγκη για κάποιον μεσάζοντα, όπως για παράδειγμα μια τράπεζα. Αυτό σημαίνει ότι τα άτομα αυτά μπορούν να μεταφέρουν κεφάλαια απευθείας μεταξύ τους μέσα από ψηφιακές πλατφόρμες που διευκολύνουν αυτές τις συναλλαγές. Οι συναλλαγές p2p είναι αποκεντρωμένες πράγμα που σημαίνει ότι δεν υπάρχει μια κεντρική αρχή που να επιβλέπει και να ελέγχει την διαδικασία. Αυτό έχει ως αποτέλεσμα να υπάρχουν χαμηλότερες προμήθειες αλλά και ταχύτεροι χρόνοι συναλλαγών σε σύγκριση με τα παραδοσιακά χρηματοοικονομικά συστήματα. (Nakamoto, 2008)

Όλες οι συναλλαγές καταγράφονται μέσω μιας τεχνολογίες που ονομάζεται Blockchain σε μια βάση δεδομένων η οποία είναι δημόσια (public ledger) . Κάθε συναλλαγή από την στιγμή που επικυρωθεί και εισέρθει σε ένα μπλοκ δεν είναι εφικτό να αλλάξει η να ακυρωθεί. Οι συναλλαγές αυτές είναι ανώνυμες καθώς πραγματοποιούνται με πιστοποίηση ψηφιακών υπογραφών και δεν απαιτείται η γνωστοποίηση προσωπικών πληροφοριών του εκάστοτε χρήστη. Μια σημαντική ιδιότητα των Κρυπτονομισμάτων είναι η δυνατότητα μετατροπής τους σε συμβατικά νομίσματα (fiat currencies), όπως το ευρώ (**€)** , το δολάριο ($) , η αγγλική λύρα (£) και το ιαπωνικό γιεν (¥) . Επιπλέον όπως προαναφέρθηκε η έντονη μεταβλητότητα της τιμής τους είναι μια χαρακτηριστική ιδιότητα τους . Αυτό προκύπτει από την έλλειψη κάποιας κεντρικής αρχής η οποία θα μπορούσε να ασκήσει νομισματική πολιτική και να σταθεροποιήσει την τιμή. Άρα οι τιμές τους καθορίζονται κατά κύριο λόγο από τους νόμους προσφοράς και ζητητής της αγοράς.

Τέλος υπάρχει προκαθορισμένος αριθμός έκδοσης Κρυπτονομισμάτων που μπορούν να διατεθούν στην αγορά όπως το bitcoin που έχει ένα ανώτερο όριο προσφοράς και δεν μπορούν να διατεθούν περισσότερα. Με αυτό τον τρόπο αποφεύγονται οι πληθωριστικές τάσεις σε αντίθεση με τα νομίσματα fiat όπου οι αρμόδιες αρχές μπορούν να επέμβουν και να αυξήσουν τον αριθμός έκδοσης.

1.3 Ιστορική αναδρομή των Κρυπτονομισμάτων

Οι πρώτες προσπάθειες για την δημιουργία ενός αποκεντρωμένου ψηφιακού νομίσματος έγιναν το 1980 με το " e-cash " από τον David Chaum , το 1998 με το " Bit gold " από τον Nick Szabo και την ίδια χρονιά με το " B-money " από τον Wei Dai οι οποίες όλες απέτυχαν καθώς το βασικό πρόβλημα όλων αυτών ήταν η το πρόβλημα της διπλής δαπάνης και η αποτροπή του ιδίου νομίσματος να μην ξοδευτεί δύο φορές. Όμως όλες αυτές οι προσπάθειες έθεσαν τις βάσεις για την δημιουργία και την ανάπτυξη σύγχρονων Κρυπτονομισμάτων. Το 2008, ο Satoshi Nakamoto δημοσίευσε ένα whitepaper , « Bitcoin: A Peer-to-Peer Electronic Cash System », το οποίο καθόριζε το σχέδιο για ένα νόμισμα με βάση την λειτουργία Peer-to-Peer. (Nakamoto, 2008)

Μέχρι και σήμερα παραμένει ένα μυστήριο στον κόσμο των Κρυπτονομισμάτων η ταυτότητα του/της Satoshi μιας και δεν ξέρουμε αν πρόκειται κιόλας για ένα μόνο άτομο ή για ολόκληρη ομάδα. Πολλοί υποστηρίζουν ότι ο/η Nakamoto έκρυψε σκόπιμα την ταυτότητα του και έμεινε ανώνυμος μιας και το Bitcoin δεν θα είχε τόση επιτυχία αν ο δημιουργός του αποκαλυπτόταν και γινόταν «εύκολος στόχος». Εν τέλει το 2009 το δίκτυο του Bitcoin έρχεται σε εφαρμογή με την δυνατότητα οι χρήστες του να μπορούν να εξορύξουν bitcoin με την χρήση επεξεργαστών υπολογιστή χωρίς ιδιαίτερη προσπάθεια, καθώς η τιμή του κυμαίνεται γύρω στα μηδέν δολάρια. Το 2009 δεν υπήρχαν ανταλλακτήρια μέχρι που το 2010 ιδρύεται το πρώτο ψηφιακό ανταλλακτήριο στο οποίο πραγματοποιούνται αγοραπωλησίες bitcoin με όνομα bitcoinmarket.com. Το εν λόγω ανταλλακτήριο δεν βρίσκεται όμως σε λειτουργία σήμερα.

Στις 22 Μάιου του 2010 πραγματοποιείται η πρώτη συναλλαγή με bitcoin ως τρόπο πληρωμής για την αγορά ενός αγαθού. Συγκεκριμένα αγοράστηκαν δύο πίτσες με κόστος 10.000 Bitcoin, τα οποία μπορεί τότε να μην είχαν σημαντική αξία μιας και το καθένα άξιζε 0.0041 δολάρια αλλά σήμερα μιλάμε για ένα ποσό της τάξεως των 600 εκατομμυρίων δολαρίων. (The New York Times, 2013)

Το 2011 δημιουργείται το δεύτερο κρυπτονόμισμα και το πρώτο altcoin (alternative to Bitcoin) με όνομα Namecoin βασισμένο στην τεχνολογία blockchain του Bitcoin. Στόχος του είναι να μειωθεί η λογοκρισία στο διαδίκτυο, να αυξήσει την ασφάλεια, την ιδιωτικότητα και να προστατεύσει την ιδιοκτησία μιας διεύθυνσης που δίνει πρόσβαση σε έναν ιστότοπο. (namecoin, 2024)

Το 2014 εκδίδεται το Tether (USD ₮) το οποίο γίνεται το πρώτο Stablecoin και το πιο διαπραγματεύσιμο μέχρι και σήμερα με βάση τα στοιχεία στο Coinmarketcap.com. Το Tether φιλοδοξεί να ενώσει την σταθερότητα των νομισμάτων fiat με την καινοτόμο πλευρά της τεχνολογίας blockchain προσφέροντας ένα συνδυασμό και των δύο αυτών πλευρών. Αυτό επιτυγχάνεται αρχικά προφέροντας ανταλλακτήρια και εφαρμογές ψηφιακών πορτοφολιών, υπηρεσίες πληρωμών μέχρι και πρωτόκολλα αποκεντρωμένης χρηματοδότησης (Defi). Επιπλέον όλα τα Tether tokens αντιστοιχούν σε κλίμακα 1προς 1 με ένα αντίστοιχο νόμισμα fiat (π.χ. 1 USD ₮= 1USD). Το Tether υποστηρίζει το δολάριο των ΗΠΑ (USD), το Ευρώ (EUR), το κινέζικο Γιουάν (CNH) και το μεξικάνικο Πέσο (MXN). (Tether, 2024)

Στις 30 Ιουλίου του 2015 δημιουργείται από τον Vitalik Buterin η πλατφόρμα του Ethereum. Μια πλατφόρμα αποκεντρωμένων εφαρμογών με κύριο χαρακτηριστικό της την εφαρμογή των έξυπνων συμβολαίων. Το κρυπτονόμισμα το οποίο χρησιμοποιείται στην πλατφόρμα είναι το Ether (ETH). Ένα νόμισμα το οποίο αργότερα θα γίνει και ο μεγαλύτερος εκπρόσωπος των εναλλακτικών νομισμάτων (altcoins). Ενώ ένα χρόνο αργότερα και συγκεκριμένα το Σεπτέμβριο του 2016, το Ethereum έπεσε θύμα χακαρίσματος στο Dao (Decentralized autonomous organization), έναν αποκεντρωμένο αυτόνομο οργανισμό που ξεκίνησε το 2016 στο blockchain του Ethereum. Σκοπός του ήταν η άντληση κεφαλαίων από επενδυτές μέσα από την διαδικασία ICO. Αφού συγκεντρώθηκαν κεφάλαια συνολικής αξίας 150 εκατομμυρίων από την πώληση διακριτικών (token), ο Dao δέχθηκε επίθεση και παραβιάστηκε με αποτέλεσμα ένα μεγάλο μέρος των χρημάτων να κλαπούν. Τα κλεμμένα κεφάλαια έπρεπε να αποκατασταθούν αλλά επειδή όλα τα μέρη δεν συμφωνούσαν με αυτή την απόφαση, πραγματοποιήθηκε μια διάσπαση της αλυσίδας blockchain σε δυο μέρη. Το πρώτο μέρος αποτελούμενο από το Ethereum και το δεύτερο από το Ethereum classic.

2. Η ζωή των Κρυπτονομισμάτων

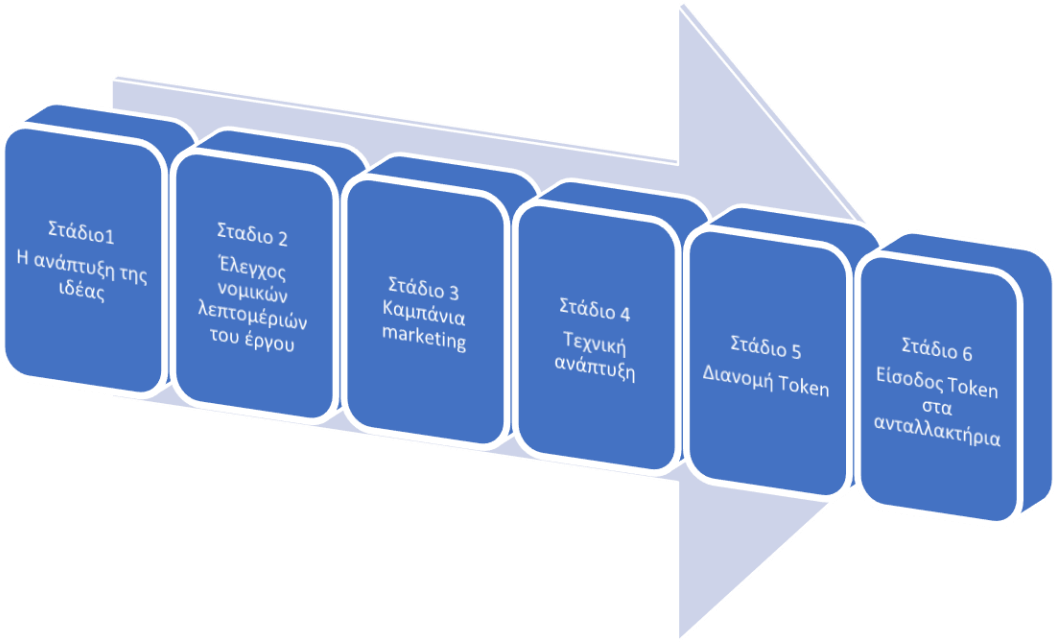
2.1 Πως εκδίδονται τα Κρυπτονομίσματα?

Τα κρυπτονομίσματα εκδίδονται με την αρχική δημόσια προσφορά η αλλιώς initial coin offering (ICO) παρόμοια όπως η αρχική δημόσια προσφορά των μετοχών (IPO) στο παραδοσιακό χρηματοοικονομικό σύστημα. Το ICO είναι ένας μηχανισμός συγκέντρωσης κεφαλαίων στον σύστημα των Κρυπτονομισμάτων με στόχο την δημιουργία νέου νομίσματος. Η χρηματοδότηση δεν γίνεται απευθείας με συμβατικά νομίσματα (Fiat) αλλά οι επενδυτές ανταλλάσσουν κρυπτονομίσματα με το νεοεκδιδόμενο νόμισμα. Αυτό σημαίνει ότι οι επενδυτές θα πρέπει πρώτα να έχουν αγοράσει κάποιο άλλο κρυπτονόμισμα και να το ανταλλάξουν για τα νέα νομίσματα. Τα ICO θεωρούνται από πολλούς επενδυτές καλά είδη επενδύσεων, ενώ άλλοι επενδυτές ασπάζονται μια αντίθετη άποψη για αυτά.

Τα ICO θεωρούνται από αρκετούς επενδυτές μια καλή επένδυση καθώς εισέρχονται σε ένα πρώιμο στάδιο απόκτησης του νομίσματος σε χαμηλότερες τιμές σε σχέση με μελλοντικού χρόνους. Επιπλέον έχουν πρόσβαση στο συγκεκριμένο προϊόν και στις υπηρεσίες. Ένας ακόμα σημαντικός λόγος είναι πως τα ICO γίνονται μέσω διαδικτύου και δεν υπάγονται σε κάποιο γεωγραφικό περιορισμό, κάτι που σημαίνει ότι οποιοσδήποτε ανεξάρτητα με το που βρίσκεται μπορεί να συμμετέχει. Επιπλέον τα ICO δεν έχουν περιορισμό στο μέγεθος του επενδυτή, κάτι που σημαίνει ότι μπορεί να συμμετέχει ο καθένας ανεξαρτήτου μεγέθους του χαρτοφυλακίου του. Ένα πολύ επιτυχημένο ICO θεωρείται εκείνο του Ethereum, το οποίο συγκέντρωσε 18 εκατομμύρια δολάρια το 2014 και καθιέρωσε την τεχνολογία Blockchain του Ethereum ως την κορυφαία για έξυπνα συμβόλαια και DApps

Από την άλλη πλευρά πολλοί ισχυρίζονται πως η επένδυση στα ICO ελλοχεύει κινδύνους και μεγάλο ρίσκο. Τα τελευταία χρόνια πολλά ICO χρησιμοποιήθηκαν από κάποιους ως ένα δόλιο σχέδιο για να εκμεταλλευτούν ανυποψίαστους επενδυτές και να τους αποσπάσουν μεγάλα χρήματα χρησιμοποιώντας ένα ψεύτικο νόμισμα. Χρησιμοποίησαν παραπλανητικές ή ψευδείς πληροφορίες στα white paper (τα οποία εξηγούν τεχνικές λεπτομέρειες του project) κάτι που μπέρδεψε τους επενδυτές κατά την αξιολόγηση της επένδυσης τους. Τέλος με βάση στατιστικά στοιχεία λιγότερα από τα μισά ICO επιβιώνουν ακόμα και αν είναι όλα σωστά από πλευράς νομιμότητας μετά τους πρώτους μήνες από την δημόσια αυτή προσφορά. Χαρακτηριστικό παράδειγμα είναι εκείνο του Tezos όπου παραβιάστηκε η νομοθεσία περί κινητών αξιών στις ΗΠΑ. (Coinbase, 2024. Clayton, 2017)

2.2 Τα στάδια εφαρμογής του ICO



Εικόνα 3 στάδια εφαρμογής ICO

- Στάδιο 1ο Η ανάπτυξη της ιδέας.

  Σε αυτό το στάδιο βασικός στόχος είναι να ενημερωθεί το κοινό για το σχέδιο, τα χαρακτηριστικά, την βασική ιδέα του project και τον τρόπο λειτουργίας του. Παρουσιάζεται το whitepaper, το οποίο είναι το μέσο επικοινωνίας του project στο κοινό. Περιγράφει τεχνικές πληροφορίες του έργου, το χρονοδιάγραμμα του έργου, αλλά και πληροφορίες όπως η διαδικασία δημιουργίας και προσφοράς των token. Είναι το πιο σημαντικό έγγραφο για το marketing καθώς από αυτό θα εξαρτηθεί ο όγκος της χρηματοδότησης που θα συγκεντρωθεί.

- Στάδιο 2ο Έλεγχος νομικών λεπτομερειών του έργου

  Σε αυτό το στάδιο, το project περνάει από μια διαδικασία ελέγχου για να διαπιστωθεί κατά πόσο συμβαδίζει με τους νόμους και τους κανονισμούς.

- Στάδιο 3ο Καμπάνια Marketing

  Σε αυτό το στάδιο η ομάδα που εκδίδει το ICO διαφημίζει το project για να προσελκύσει επενδυτές. Μία έξυπνη τακτική που χρησιμοποιείται είναι η διάθεση δωρεάν token (airdrop).

- Στάδιο 4ο Τεχνική ανάπτυξη

  Σε αυτό το στάδιο η ομάδα αναπτύσσει και ελέγχει τα έξυπνα συμβόλαια (smart contracts) καθώς και την διαδικασία έκδοσης των tokens.

- Στάδιο 5ο Διανομή Token

  Σε αυτό το στάδιο πραγματοποιείται η άντληση κεφαλαίων, όπου όπως έχει προαναφερθεί οι επενδυτές ανταλλάσσουν τα κρυπτονομίσματα με το νέο νόμισμα.

- Στάδιο 6ο Εισαγωγή token στα ανταλλακτήρια

  Πρόκειται για το τελευταίο στάδιο όπου τα token εισάγονται στα ανταλλακτήρια αν και εφόσον πληρούν τις προϋποθέσεις του κάθε ανταλλακτηρίου.

  (Hale, 2018)

2.3 Διαφορές IPO και ICO

Ιδιαίτερο ενδιαφέρον παρουσιάζουν οι διαφορές μεταξύ ICO και IPO οι οποίες και παραπείθονται στο παρακάτω διάγραμμα. Όπως προαναφέρθηκε ICO είναι η δημόσια εγγραφή των Κρυπτονομισμάτων, ενώ IPO είναι η δημόσια εγγραφή των μετοχών.

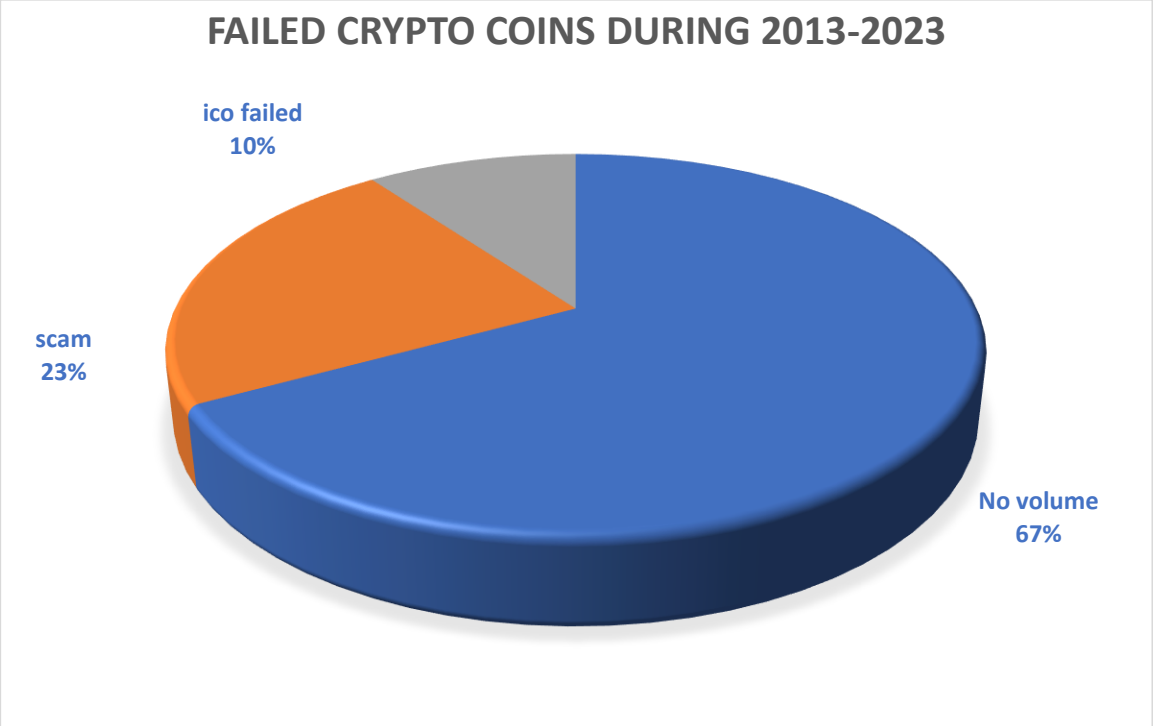
	ICO	IPO
Εκδότες	Start ups	Μεγάλες επιχειρήσεις
Μελλοντικές Απολαβές	Μελλοντικά αγαθά / υπηρεσίες	Μερίσματα
Τι εισπράττουν οι επενδυτές	Tokens	Μετοχές
Επενδυτές	Ευρύ επενδυτικό κοινό	Θεσμικοί
Τρόποι πληρωμών	Κρυπτονομίσματα	Συμβατικά νομίσματα
Διάρκεια	Μικρή Διάρκεια	Μεγάλη διάρκεια
Προσβασιμότητα	Για όλους	Περιορισμένη
Διαμεσολαβητής	Πλατφόρμες Blockchain	Επενδυτικές τράπεζες
Ρυθμιστικό πλαίσιο	Έλλειψη	Ισχυρό
Λειτουργικά κόστη	χαμηλά	Πολύ υψηλά
Κίνδυνος	Υψηλός	Μέτριος προς χαμηλός
Επίπεδο ανάπτυξης ιδέας	Ανεπτυγμένη	Ανεπτυγμένη

Πίνακας 1 διαφορές μεταξύ ICO & IPO

Ο παραπάνω πίνακας δημιουργήθηκε με στοιχεία που συλλέχτηκαν από τις εξής πηγές (Sharma, 2020. Cakebread, 2020. Hale, 2018)

2.4 Γιατί αποτυγχάνουν πολλά Κρυπτονομίσματα?

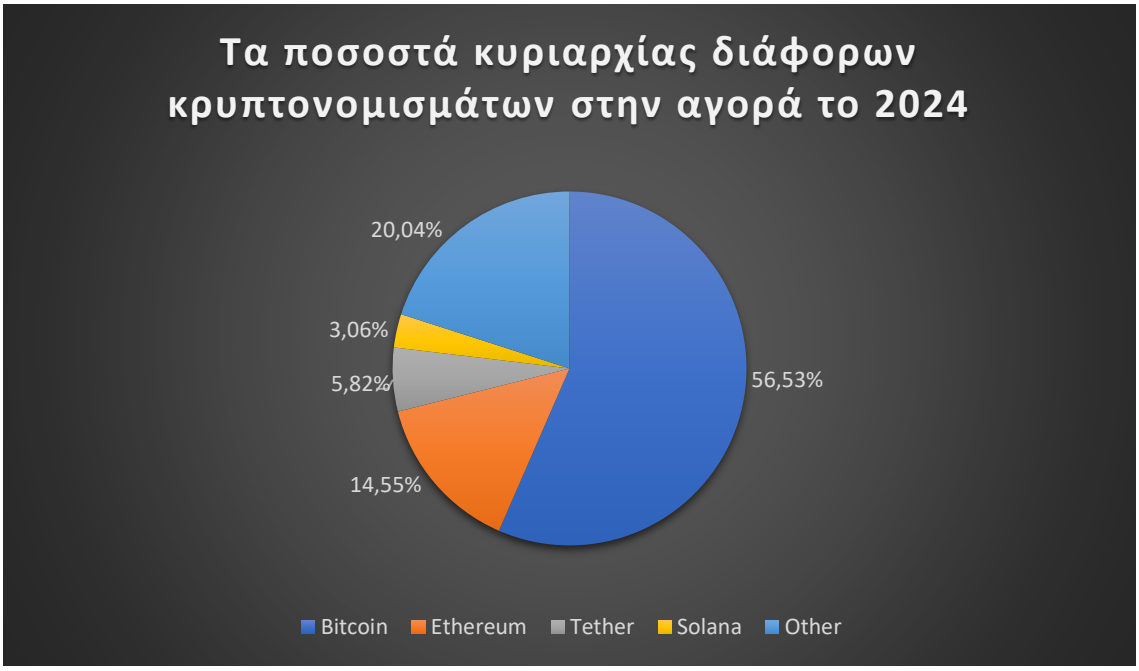
Μετά την έκδοση του Bitcoin αλλά και την επιτυχία του, άνοιξε ο δρόμος σε νέα νομίσματα, πολλά από τα οποία είχαν ως στόχο να το ανταγωνιστούν, ενώ άλλα πρότειναν μια νέα λύση κρυπτογράφησης. Από το 2019 πολλά κρυπτονομίσματα ήρθαν στο προσκήνιο και έγιναν δημοφιλή ενώ άλλα έμειναν στην αφάνεια. Με το τέλος του 2023 το Coinmarketcap ανέφερε την ύπαρξη περίπου 23.000 Κρυπτονομισμάτων σε διάφορες κατηγορίες και με συνολική αξία όλων αυτών να ανέρχεται στα 1,2 τρισεκατομμύρια δολάρια. Ωστόσο μεταξύ αυτών των token δεν είναι όλα ενεργά ή πολύτιμα, με τον πραγματικό αριθμό ενεργών μάρκων κρυπτογράφησης να ανέρχεται γύρω στις 9000. Αρχικά πολλά νομίσματα δεν έχουν επιτυχία διότι υπάρχει έλλειψη χρηματοδότησης για την διατήρηση του έργου κρυπτογράφησης μετά το Ico (initial coin offering), δηλαδή μίας διαδικασίας δημόσιας προσφοράς μέσω του διαδικτύου. Επιπλέον επειδή δεν υπήρχε μεγάλος όγκος συναλλαγών καθημερινά, όπως και επίσης επειδή υπήρχαν πολλά νομίσματα απάτης. (Aran & Pallavi, 2023)



Εικόνα 4 παράθεση ποσοστών αποτυχίας Κρυπτονομισμάτων (Aran & Pallavi, 2023)

Ακόμα ένας σημαντικός λόγος δεν μπορεί να είναι άλλος από τα ζητήματα ασφαλείας, όπου αρκετά κρυπτονομίσματα δεν καταφέρνουν να διατηρήσουν, αντιμετωπίζοντας παραβιάσεις ασφαλείας αλλά και hacks, με αποτέλεσμα την υπονόμευση της εμπιστοσύνης των χρηστών προς αυτά.

Τέλος ο κορεσμός της αγοράς είναι ένας ακόμα λόγος που δεν πετυχαίνουν πολλά κρυπτονομίσματα και δεν καταφέρνουν να ξεχωρίσουν. Αν αναλογιστούμε ότι μόνο το bitcoin κατέχει ως μερίδιο αγοράς το 56.5%, το Ethereum το 14.5% και το Tether το 5.8%, απομένει περίπου 20% μερίδιο για χιλιάδες νομίσματα που παλεύουν να βρεθούν στην κορυφή.



Εικόνα 5 απεικόνιση ποσοστών κυριαρχίας Κρυπτονομισμάτων στην αγορά (Coinmarketcap, 2024)

3. Altcoins

3.1 Ορισμός

Καθώς το Bitcoin είχε μια ανοδική πορεία και η τιμή του εκτοξεύτηκε το 2017, δημιουργήθηκαν προσδοκίες για μια ανερχόμενη αγορά με μέλλον και πολλά κέρδη από τους επενδυτές. Καθώς τα κρυπτονομίσματα δεν υπάγονται σε κάποια κεντρική αρχή ή κάποιό ρυθμιστικό πλαίσιο, ο καθένας μπορούσε να δημιουργήσει το δικό του με αποτέλεσμα ολοένα και περισσότερα νομίσματα να δημιουργούνται και να προσπαθούν να καταλάβουν μερίδιο στην ανερχόμενη αυτή αγορά, όπου πρωτοπόρος δεν ήταν άλλος από το Bitcoin. Τα νομίσματα αυτά ονομάστηκαν Altcoins (alternative to Bitcoin), τα οποία βασίστηκαν πάνω στην τεχνολογία του blockchain του Bitcoin, κάτι το οποίο ήταν και η καινοτομία του. Με πιο απλά λόγια τα εναλλακτικά νομίσματα είναι όλα τα κρυπτονομίσματα πέραν του Bitcoin.

Μία ιδιαίτερη παρατήρηση είναι πως τα νομίσματα αυτά, αν όχι όλα, τα περισσότερα, ακολουθούν την ίδια συμπεριφορά του bitcoin σε γεγονότα και καταστάσεις ως προς την πορεία του στην αγορά. Αυτό προκύπτει λόγω της κυριαρχίας του Bitcoin στην αγορά, όπως εξηγείται αναλυτικά παρακάτω στο κεφάλαιο 4.2. Εν ολίγης όταν το Bitcoin έχει μια συμπεριφορά ανοδική σε τιμή, τα altcoins ακολουθούν αυτήν την συμπεριφορά και έχουν και τα ίδια ανοδική πορεία. Αντίστοιχα όταν το Bitcoin έχει μία πτωτική τάση στην αγορά, αντίστοιχα τα εναλλακτικά νομίσματα έχουν μια πτωτική πορεία. Αυτό δεν γίνεται στον ίδιο βαθμό ή κατά το ίδιο ποσοστό καθώς αυτό εξαρτάται από πολλούς και διάφορους παράγοντες που θα αναλυθούν σε μεταγενέστερα κεφάλαια.

3.2 Γιατί είναι σημαντικά τα Altcoins στο σύστημα των Κρυπτονομισμάτων?

Παρόλο που η κυριαρχία του Bitcoin στην αγορά Κρυπτονομισμάτων είναι αισθητή, μιας και κατέχει πάνω από το 55% μερίδιο αγοράς σύμφωνα με το Coinmarketcap, η ύπαρξη των altcoins είναι πολύ σημαντική έως και αναγκαία.

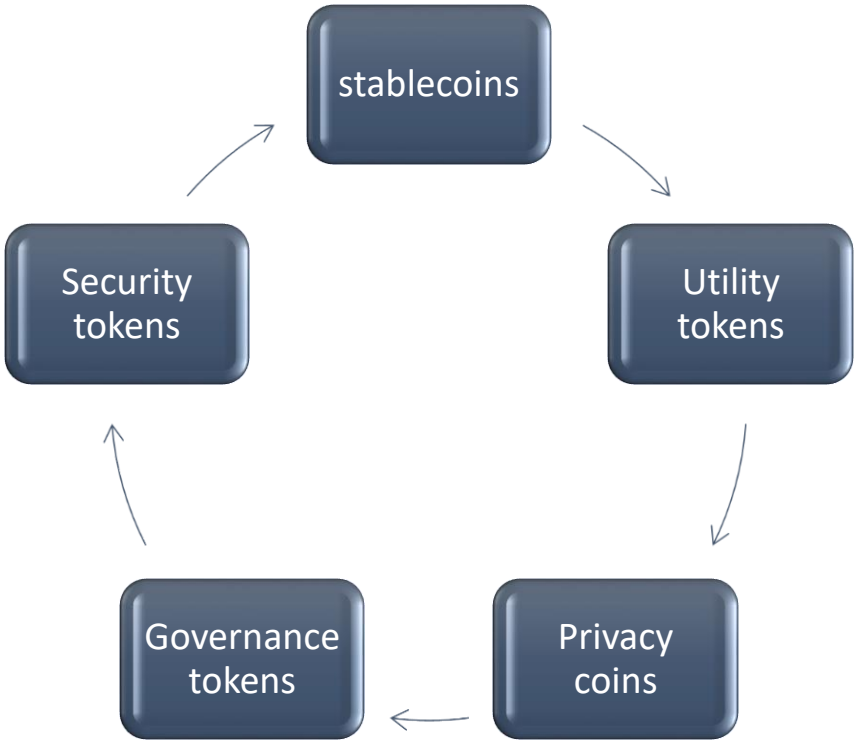
Αρχικά τα εναλλακτικά αυτά νομίσματα διακρίνονται από καινοτομία καθώς συμβάλουν στην τεχνολογική πρόοδο του οικοσυστήματος της κρυπτογραφίας. Είναι οι οδηγοί στην καινοτομία φέρνοντας νέες λύσεις και λειτουργίες σε προβλήματα που το bitcoin ενδέχεται να μην αντιμετωπίσει αποτελεσματικά. Τα altcoins φέρουν νέες βελτιωμένες μορφές συναλλαγών πιο γρήγορες και με λιγότερα κόστη, χαρακτηριστικό παράδειγμα

το Litecoin. Βοηθούν πολύ στην ανάπτυξη του τομέα της ιδιωτικότητας των συναλλαγών, αναπτύσσοντας την ασφάλεια και την προστασία των προσωπικών δεδομένων των χρηστών. Τέτοια νομίσματα είναι το dash και το Monero. Επιπλέον στοχεύουν στην μείωση της ενέργειας και του χρόνου που απαιτείται για την δημιουργία μπλοκ στα συστήματα blockchain, όπως το Ethereum, το οποίο είναι και ο πιο σημαντικός εκπρόσωπος των Altcoins. (Vigna & Casey, 2015)

Επίσης τα εναλλακτικά νομίσματα προσφέρουν οικονομική ποικιλομορφία καθώς εισάγουν καινοτόμα οικονομικά μοντέλα στην αγορά Κρυπτονομισμάτων και προσφέρουν πολλές αλλά και διαφορετικές επιλογές επένδυσης στους χρήστες, καλύπτοντας έτσι διάφορες προτιμήσεις επενδυτών. Επιπλέον τα εναλλακτικά νομίσματα βοηθούν στην τμηματοποίηση της αγοράς των Κρυπτονομισμάτων. Με τον όρο τμηματοποίηση της αγοράς εννοούμε την διαδικασία διαίρεσης της ευρείας αγοράς σε μικρότερα τμήματα ή υποαγορές με βάση ορισμένες ανάγκες ή χαρακτηριστικά. Στόχος λοιπόν είναι να προσεγγιστεί ένα ευρύτερο κοινό επενδυτών. Ιδιαίτερο ενδιαφέρον παρουσιάζει το παράδειγμα του Ripple ή αλλιώς XRP το οποίο λειτουργεί στον χρηματοπιστωτικό κλάδο και πραγματοποιεί διασυνοριακές πληρωμές και συναλλαγές. Επίσης το Ethereum είναι ένα σημαντικό κρυπτονόμισμα, το οποίο στοχεύει στους προγραμματιστές αποκεντρωμένων εφαρμογών.

Επιπλέον τα altcoins προσφέρουν μια διαφοροποίηση στα χαρτοφυλάκια των επενδυτών. Με την διαφοροποίηση αυτή προσφέρεται διασπορά του κινδύνου και ως αποτέλεσμα να υπάρξουν μελλοντικά κέρδη. Ένας ακόμα λόγος της σημαντικότητας των εναλλακτικών νομισμάτων στην αγορά Κρυπτονομισμάτων είναι πως μέσω του ανταγωνισμού που προκύπτει δημιουργείται εξέλιξη. Αυτό συμβαίνει διότι υπάρχει μεγάλος ανταγωνισμός και όλα τα altcoins προσπαθούν να αποκτήσουν μερίδιο στην αγορά, έτσι λοιπόν για να ξεχωρίσει κάποιο και να πάρει μεγαλύτερο μερίδιο πρέπει να προσφέρει τις καλύτερες υπηρεσίες, πράγμα που κάνει τους προγραμματιστές να ασχολούνται όλο και περισσότερο με την ανάπτυξη και την εξέλιξη των τεχνολογιών τους, αλλά και των πρωτοκόλλων τους. Με αυτόν τον τρόπο συμβάλουν όχι μόνο στην εδραίωση της τεχνολογία Blockchain αλλά και στην ευρύτερη μετάδοση και υιοθέτηση της και σε άλλους κλάδους πέραν των Κρυπτονομισμάτων. Εν κατακλείδι αυτές οι καινοτομίες δεν βοηθούν μεμονωμένα τα νομίσματα που τις κατέχουν αλλά την ανάπτυξη του κλάδου συνολικά, κάτι που καθιστά αναγκαία την ύπαρξη τους ! (*Burniske& Tatar, 2017)*

3.3 Οι Βασικές υποκατηγορίες των Altcoins



Εικόνα 6 απεικόνιση των υποκατηγοριών altcoin

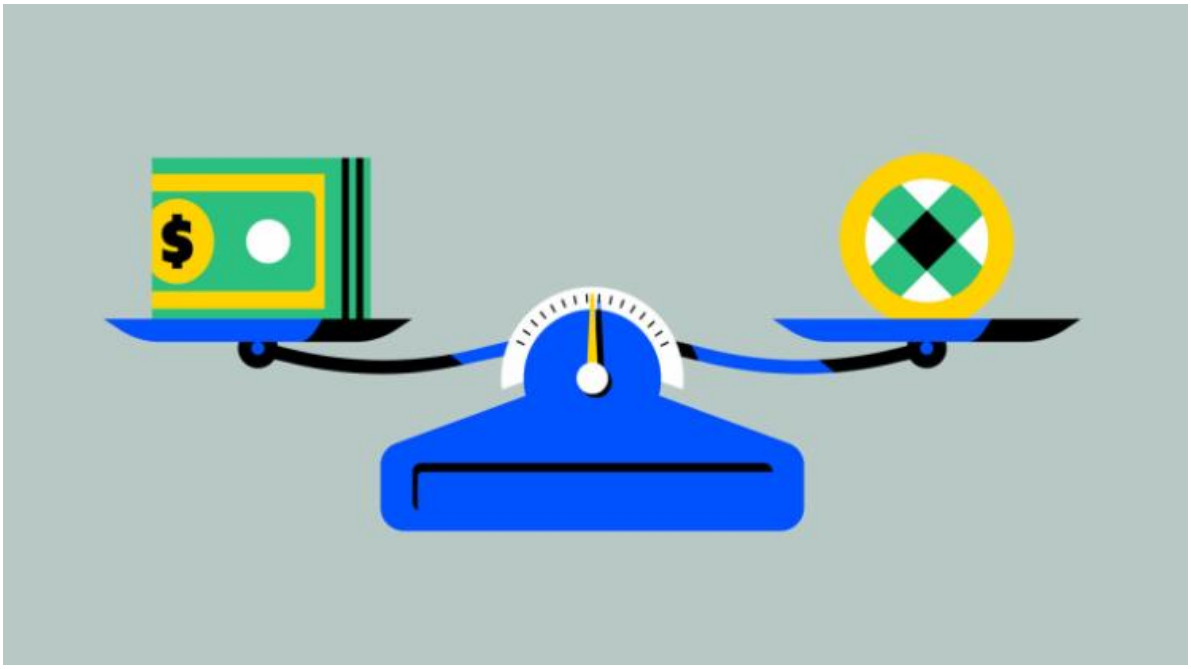
Στην συνέχεια θα αναφερθούν δυο διαφορετικές έννοιες, τα token και τα coin. Στο οικοσύστημα των Κρυπτονομισμάτων η κύρια διαφορά τους είναι ως προς την δομή τους και τον σκοπό που εξυπηρετούν.

- Τα Coins λειτουργούν με βάση την δικιά τους τεχνολογία Blockchain και χρησιμεύουν ως μέσο ανταλλαγής.

- Τα Token λειτουργούν σε ήδη υπάρχοντα δίκτυα Blockchain. Συνδέονται με ένα έργο η πρωτόκολλο εντός ενός οικοσυστήματος και μπορούν να χρησιμοποιηθούν με πολλούς τρόπους οι οποίοι θα αναλυθούν περαιτέρω στη συνέχεια.

3.3.1 Stablecoins

Τα Stablecoins είναι ένας τύπος Κρυπτονομισμάτων τα οποία έχουν δημιουργηθεί για να διατηρούν μια σταθερή αξία σε σχέση με ένα συγκεκριμένο περιουσιακό στοιχείο ή σε ένα σύνολο περιουσιακών στοιχείων. Σε αντίθεση με άλλα κρυπτονομίσματα, τα οποία έχουν ακραίες διακυμάνσεις τιμών, τα stablecoins στοχεύουν να παρέχουν σταθερότητα σε αυτές κάτι που τα καθιστά ακατάλληλα για επενδύσεις κερδοσκοπικού χαρακτήρα. Ο τρόπος με τον οποίο λειτουργούν είναι πως συνδέονται με ένα νόμισμα Fiat όπως το δολάριο ΗΠΑ, ένα εμπόρευμα όπως ο χρυσός, ή ένα μείγμα περιουσιακών στοιχείων και χρησιμοποιούνται ως μέσο ανταλλαγής, ως μέσο αποθήκευσης αξίας, ή ως μια λογιστική μονάδα στο οικοσύστημα Κρυπτονομισμάτων. Το κάθε stablecoin έχει ακριβώς την ίδια αξία με το αντίστοιχο νόμισμα fiat, καθώς συνδέει την αγοραία του αξία με αυτήν των Fiat. Οι αναλογίες πάντα θα κυμαίνονται στο 1:1 δηλαδή 1$ αντιστοιχεί σε 1 Tether και αντίστοιχα 50$ αναλογούν σε 50 tether. Το Tether υποστηρίζει το δολάριο των ΗΠΑ (USD), το Ευρώ (EUR), το κινέζικο Γιουάν (CNH) και το μεξικάνικο Πέσο (MXN). Τα πιο δημοφιλή παραδείγματα stablecoins περιλαμβάνουν το Tether (USDT), το USD Coin (USDC) και το DAI. (Lewis, 2018)

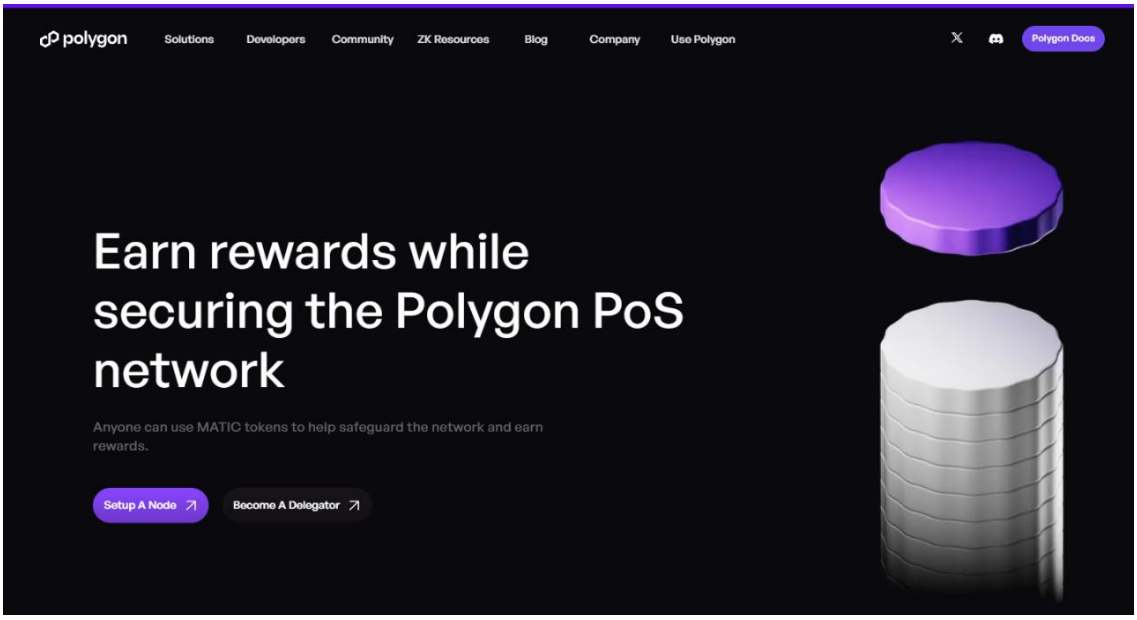


Εικόνα 7 ισοζύγιο μεταξύ νομισμάτων fiat και stablecoins (Coinbase. 2024)

3.3.2 Utility tokens

Αυτά τα εναλλακτικά κρυπτονομίσματα δίνονται κατά την διάρκεια πλήθους πωλήσεων καθώς ένα έργο εκτελεί ένα Ico. Όταν μια εταιρία δημιουργεί utility tokens σημαίνει ότι δημιουργεί ένα είδος ψηφιακού κουπονιού και δίνει την δυνατότητα στους κατόχους του να αγοράσουν προϊόντα ή υπηρεσίες και να εξαργυρώσουν ανταμοιβές εντός της πλατφόρμας. Επιπλέον οι κάτοχοι των κουπονιών έχουν το δικαίωμα να ψηφίσουν και να προσφέρουν σχόλια στις διαδικασίες ανάπτυξης και λήψης αποφάσεων της πλατφόρμας. Το ενδιαφέρον των επενδυτών προσελκύεται συχνά από την τιμή του utility token η οποία αντικατοπτρίζει την αξία που μπορεί να προσφέρει το έργο σε ένα ευρύ κοινό (Sharma, 2024)

Ένα πολύ χαρακτηριστικό παράδειγμα utility token είναι το MATIC, το οποίο εκδίδεται από την πλατφόρμα του κρυπτονομίσματος Polygon και χρησιμοποιείται ως μέθοδος πληρωμής για τέλη συναλλαγών στο δίκτυο Polygon. Επιπλέον οι κάτοχοι MATIC μπορούν να γίνουν επικυρωτές και με αυτό τον τρόπο να βοηθήσουν στην ανάπτυξη και την ασφάλεια του δικτύου. Για να μπορέσουν να γίνουν επικυρωτές θα πρέπει να ποντάρουν ένα ποσό MATIC και να το αποστείλουν σε μία συγκεκριμένη ηλεκτρονική διεύθυνση ή κάποιο ψηφιακό πορτοφόλι. Ο χρήστης με το μεγαλύτερο αριθμό MATIC που έχει ποντάρει θα επιλέγεται. Τα νομίσματα αυτά δεν επιστρέφονται ούτε δαπανούνται μέχρι να ολοκληρωθεί με ασφάλεια η διαδικασία επικύρωσης. Το MATIC μπορεί να αγοραστεί αλλά και να πωληθεί μέσω και άλλων ψηφιακών ανταλλακτηρίων, όπως επίσης και να ανταλλαχθεί για κάποιο άλλο περιουσιακό στοιχείο. (POL Token, 2024)



Εικόνα 8 ιστοσελίδα polygon (POL Token, 2024)

3.3.3 Security tokens

Τα security tokens δημιουργούνται ως ένα είδος επένδυσης με την μορφή μερισμάτων, δηλαδή ένα είδος επιπρόσθετων νομισμάτων που μοιράζονται στους κατόχους διακριτικών κάθε φορά που η εταιρία παρουσιάζει κέρδη στην αγορά. Οι ιδιοκτήτες αυτών των διακριτικών ασφαλείας λαμβάνουν μερίδιο ιδιοκτησίας της εταιρίας αναλογικά με τον αριθμό που κατέχουν. Όπως και στα utility tokens έτσι και στα security tokens οι ιδιοκτήτες αυτών μπορούν να συμμετέχουν σε συστήματα ψηφοφοριών και στις διαδικασίες λήψης αποφάσεων της εκάστοτε εταιρίας. Πρόκειται λοιπόν για μια έκδοση ψηφιακού τίτλου ιδιοκτησίας. Αυτό όμως δεν σημαίνει ότι μπορούν οι ιδιοκτήτες αυτών να ελέγχουν την διαδικασία χειραγωγώντας την, αλλά κατά κύριο λόγο στοχεύει στο να αλληλοεπιδρούν περισσότερο στις υπηρεσίες αυτής. Τα διακριτικά ασφαλείας μπορούν να βοηθήσουν τις επιχειρήσεις να έχουν πιο γρήγορη πρόσβαση σε κεφάλαια, τα διακριτικά αυτά μπορούν να μεταβιβαστούν αλλά και να πωληθούν παγκοσμίως. Οι εταιρείες και οι κρατικοί φορείς που εκδίδουν τέτοιους τίτλους υπόκεινται σε αυστηρές ρυθμίσεις, καθώς πρέπει να είναι και εγγεγραμμένες στην επιτροπή κεφαλαιαγοράς (SEC) (Sharma, 2024).

Χαρακτηριστικό παράδειγμα είναι το Polymath το οποίο παρέχει την δυνατότητα έκδοσης διακριτικών ασφαλείας, ενώ παράλληλα στοχεύει στην αντικατάσταση απαρχαιωμένων διαδικασιών και στην εισαγωγή νέων πρωτοπόρων χρηματοοικονομικών μέσων, αντιμετωπίζοντας έτσι δυσκολίες όπως το ζήτημα της εμπιστευτικότητας, το ζήτημα της επαλήθευσης (KYC), αλλά και των διακανονισμών. Στόχος της να απλοποιεί διαδικασίες δημιουργίας ψηφιακών τίτλων αλλά και διαχείρισης αυτών σύμφωνα, πάντα με τις κανονιστικές απαιτήσεις. Η polymath έχει αναπτύξει το polymesh, ένα σύστημα blockchain που ρυθμίζει περιουσιακά στοιχεία με τρόπο ώστε να ανταποκρίνονται στις ρυθμιστικές αρχές της επιτροπής κεφαλαιαγοράς (SEC). Στόχος του polymesh είναι η δημιουργία ενός πιο ασφαλούς αλλά και αποτελεσματικού περιβάλλοντος για ψηφιακά στοιχεία (digital assets). (Polymath. 2024)

3.3.4 Privacy coins

Τα privacy coins η αλλιώς νομίσματα απορρήτου είναι κρυπτονομίσματα τα οποία έχουν ως στόχο την ενίσχυση του απορρήτου, την βελτίωση της ανωνυμίας και την μείωση της ιχνηλασιμότητας. Προσπαθούν να διασφαλίσουν ασφάλεια στις συναλλαγές μεταξύ χρηστών αλλά και την προστασία των προσωπικών δεδομένων τους. Για να πετύχουν το στόχο τους χρησιμοποιούν πρωτόκολλα απορρήτου, αναβαθμισμένες κρυπτογραφικές τεχνικές και αλγόριθμους συναίνεσης όπως το Proof of Work (PoW) ή το Proof of stake (PoS). Με αυτόν τον τρόπο βοηθούν την πραγματοποίηση ιδιωτικών και ανώνυμων συναλλαγών blockchain, μην επιτρέποντας την ανίχνευση της προέλευσης αλλά και του προορισμού τους. Παρατηρώντας λοιπόν την ανωνυμία που υπάρχει γεννιέται ένα ερώτημα του κατά πόσο θεωρούνται νόμιμα αυτά τα νομίσματα? Από την μία πλευρά πολλές χώρες έχουν απαγορεύσει το εμπόριο νομισμάτων απορρήτου καθώς πιστεύουν ότι μπορεί να χρησιμοποιηθεί ως μια εύκολη λύση για ξέπλυμα μαύρου χρήματος. Ο αριθμός των χωρών αυτών αυξάνεται συνεχώς ενώ από την άλλη πλευρά όλο και περισσότεροι χρήστες ζητούν την ανωνυμία στις συναλλαγές, ένας πολύ γνωστός υποστηρικτής αυτών είναι ο Elon Musk. (Vermaak, 2021)

Ένα πολύ γνωστό νόμισμα απορρήτου είναι το Monero (XMR) το οποίο έκανε την εμφάνιση του το 2014 και σήμερα έχει γίνει ένα από τα πιο διάσημα νομίσματα ανάμεσα στα privacy coins. Στόχος του Monero είναι η ιδιωτικότητα, η ασφάλεια και η μη ανίχνευση των συναλλαγών, καθώς δεν εμφανίζει στοιχεία του αποστολέα και του παραλήπτη, αλλά ούτε και το ποσό της συναλλαγής. Τα μέσα που το βοηθούν να επιτυγχάνει το στόχο του είναι τρία. Αρχικά μυστικές διευθύνσεις, όπου ο αποστολέας δημιουργεί διευθύνσεις μιας χρήσης για τον παραλήπτη για την αποστολή χρημάτων με απόλυτη ιδιωτικότητα, καθώς κανένας άλλος δεν μπορεί να εισέρθει στις διευθύνσεις αυτές. Επιπλέον ένα ακόμα μέσο που χρησιμοποιεί το Monero είναι οι υπογραφές δακτύλου, ένα είδος ψηφιακών υπογραφών, οι οποίες προστατεύουν την ταυτότητα του αποστολέα και οι προορισμοί των συναλλαγών είναι μη ανιχνεύσιμοί. Τέλος χρησιμοποιεί τις εμπιστευτικές συναλλαγές δακτύλου, οι οποίες είναι ο τρόπος με τον οποίο το Monero κρατάει μυστικά τα ποσά των συναλλαγών (Monero, 2024)

3.3.5 Governance tokens

Τα governance tokens ή αλλιώς διακριτικά διακυβέρνησης είναι ένα είδος Κρυπτονομισμάτων τα οποία έχουν δημιουργηθεί για να παρέχουν δικαιώματα ψήφου σε αποκεντρωμένα πρωτόκολλα βασισμένα στο blockchain και να διαμορφώνουν την μελλοντική τους πορεία. Έτσι λοιπόν δίνουν την δυνατότητα συμμετοχής των κατόχων τους σε διαδικασίες ψηφοφορίας και λήψης αποφάσεων σχετικά με την ανάπτυξη και την διαχείριση του συστήματος. Αντίθετα με τα utility tokens τα Governance tokens μπορούν να επηρεάσουν τις αποφάσεις και τις αλλαγές σχετικά με το πρωτόκολλο. Οι οργανισμοί οι οποίοι δίνουν την δυνατότητα ανάπτυξης και ελέγχου των συστημάτων τους από τους χρήστες ονομάζονται αποκεντρωμένοι αυτόνομοι οργανισμοί (DAO). (Ding et al., 2023

Ένας από τους πιο διάσημους αποκεντρωμένους αυτόνομους οργανισμούς είναι ο MakerDao, ο οποίος διοικείται εξ ολοκλήρου από ιδιοκτήτες MKR ανά τον κόσμο. Επιτρέπει στους ιδιοκτήτες MKR να λαμβάνουν αποφάσεις μέσω μιας διαδικασίας ψηφοφορίας σχετικά με ένα πρωτόκολλο αποκεντρωμένης χρηματοδότησης (DeFi), για την διασφάλιση της σταθερότητας, της διαφάνειας και της αποτελεσματικότητας. Το πρωτόκολλο Maker είναι η πρώτη εφαρμογή αποκεντρωμένης χρηματοδότησης. Σε αυτό το πρωτόκολλο λειτουργεί ένα αποκεντρωμένο stablecoin το Dai.Το Dai είναι ένα αποκεντρωμένο κρυπτονόμισμα συνδεδεμένο με το δολάριο των ΗΠΑ. Δημιουργείται από τους χρήστες οι οποίοι καταθέτουν περιουσιακά στοιχεία σε Maker Vaults μέσα στο πρωτόκολλο, ενώ ένας άλλος τρόπος να αποκτηθεί είναι μέσω ψηφιακών ανταλλακτηρίων ως μέσω πληρωμής. Ανεξάρτητα από τον τρόπο απόκτησης του χρησιμοποιείται με τον ίδιο τρόπο όπως τα υπόλοιπα stablecoins (Makerdao, 2024)

4. Bitcoin

4.1 Η αρχή του Bitcoin

Όταν κάποιος ακούει την λέξη κρυπτονομίσματα το πρώτο πράγμα που του έρχεται στο μυαλό είναι το Bitcoin και όχι άδικα, αλλά τι είναι όμως αυτό το Bitcoin? Το Bitcoin αποτελεί το πρώτο αποκεντρωμένο ψηφιακό νόμισμα που σχεδιάστηκε στην θεωρία και εφαρμόστηκε στην πράξη. Ο λόγος που έρχεται στο μυαλό πολλών αμέσως μόλις ακούνε για κρυπτονομίσματα είναι η καθιέρωση του στην αγορά, καθώς λαμβάνει το 57% ως μερίδιο έναντι των υπολοίπων νομισμάτων. Το Bitcoin όπως και τα άλλα κρυπτονομίσματα είναι ένα άυλο ψηφιακό νόμισμα το οποίο διατίθεται μόνο διαδικτυακά. Δημιουργήθηκε το 2008 από τον Satoshi Nakamoto και το 2009 ξεκίνησε να συναλλάσσεται διαδικτυακά . Μέχρι και σήμερα δεν είναι γνωστή η ταυτότητα του/της Satoshi Nakamoto ενώ πολλοί θεωρούν πως μπορεί να μην πρόκειται για ένα πρόσωπο μεμονωμένα αλλά για μια ολόκληρη ομάδα η οποία σχεδίασε αυτό το πανίσχυρο νόμισμα. Το Bitcoin όπως προαναφέρθηκε είναι το πρώτο αποκεντρωμένο νόμισμα καθώς το δίκτυο του είναι το πρώτο αποκεντρωμένο δίκτυο πληρωμών και όλοι οι χρήστες που συμμετέχουν σε αυτό είναι ίσοι μεταξύ τους. Υπάρχει ισότητα μεταξύ τους, καθώς δεν υπάρχει μια συγκεκριμένη ιεραρχία και η όποια επικοινωνία μεταξύ τους γίνεται χωρίς διαμεσολάβηση από τρίτους. Αυτή λοιπόν η αποκεντρωμένη φύση του καθιστά δύσκολο τον έλεγχο του από κυβερνήσεις ή Κεντρικές αρχές. Ακόμα και όταν κράτη όπως η Κίνα απαγόρευσαν τις συναλλαγές Κρυπτονομισμάτων δεν κατάφεραν να ανακόψουν την πορεία του πρωτοπόρου Bitcoin. Αυτή όμως η αποκεντρωμένη φύση του έχει χρησιμοποιηθεί από πολλούς ως μια λύση για παράνομες εμπορικές δραστηριότητες στην διαδικτυακή μαύρη αγορά, γνωστή και ως Silk road. Μαύρη αγορά θεωρείται μια οικονομική δραστηριότητα η οποία δεν υπόκεινται σε έλεγχο και φορολογία από το κράτος, σε αυτήν πραγματοποιούνται συναλλαγές όπως η πώληση και εμπορία προϊόντων και υπηρεσιών με τρόπο παράνομο. Πέραν από την μαύρη αγορά το Bitcoin ξεκίνησε να διατίθεται πολύ νωρίτερα γύρω στο 2010 όταν ξεκίνησε η λειτουργία του πρώτου ανταλλακτηρίου Mt.Gox όπου η ισοτιμία του Bitcoin είχε ως εξής, ένα Bitcoin ισούταν με 0,07 δολάρια, ενώ λίγα χρόνια αργότερα και συγκεκριμένα στις 29/11/2013 καταγράφηκε η μέγιστη ιστορικά του τιμή στα 1242 δολάρια. Το 2015 το Bitcoin τράβηξε την προσοχή της wall street η οποία και επένδυσε αδρά στην τεχνολογία του, εταιρίες όπως η Goldman Sachs, η American express , το Χρηματιστήριο του Nasdaq επένδυσαν στην τεχνολογία του, ενώ λόγω του μεγάλου ενδιαφέροντος που υπήρξε την ίδια χρονιά

δημιουργήθηκε στο χρηματιστήριο της Νέας Υόρκης ένας δείκτης για την πορεία του Bitcoin, ο λεγόμενος NYXBT. (Φίλιππας, 2016)

Παρακάτω παρατίθεται ο πίνακας με την εξέλιξη της τιμής του bitcoin σε δολάρια μεταξύ του Δεκεμβρίου 2013 και του Σεπτεμβρίου 2024.

Εικόνα 9 διάγραμμα εξέλιξης τιμής Bitcoin μέχρι τον Σεπτέμβριο του 2024

4.2 Η κυριαρχία του Bitcoin έναντι των άλλων Κρυπτονομισμάτων

Με την πάροδο των χρόνων δημιουργήθηκαν χιλιάδες εναλλακτικά νομίσματα (altcoins) στο οικοσύστημα των Κρυπτονομισμάτων, τα οποία όπως έχει προαναφερθεί σε προηγούμενα κεφάλαια παρόλο που προσέφεραν μια σειρά από βελτιωμένες λύσεις και τεχνολογίες, δεν κατάφεραν να καταρρίψουν την κυριαρχία του Bitcoin. Η εδραίωση του στην αγορά παραμένει σταθερή , με εκείνο να είναι το μεγαλύτερο ψηφιακό περιουσιακό στοιχείο με βάση την κεφαλαιοποίηση της αγοράς . Η δυναμική του μερίδιού του έναντι της υπόλοιπης αγοράς θεωρείται ασύλληπτη, αν αναλογιστούμε πως κατέχει το 57% του μεριδίου αγοράς. Μπορεί να μην κατέχει την καλύτερη τεχνολογία έναντι των άλλων νομισμάτων αλλά εδραιώθηκε ως πρωτοπόρος από μια σειρά από λόγους. Ένας από αυτούς είναι πως δημιουργήθηκε και εφαρμόστηκε πρώτο, αυτό δημιούργησε μια σειρά από συγκριτικά πλεονεκτήματα έναντι των υπολοίπων. Μια νέα τεχνολογία η ένας νέος επενδυτικός τίτλος να πολλαπλασιάζει την τιμή του 100 φορές ή 1000 φορές φαντάζει ασυνήθιστο φαινόμενο. Φανταστείτε να ξεκινάει η τιμή του Bitcoin από σχεδόν 0 ευρώ το 2009 και να ανέρχεται μέχρι και στα 71.000 ευρώ το 2024, πράγμα ασύλληπτο! Ο κόσμος των επενδυτών πίστεψε σε αυτό και για αυτό το λόγο κυριάρχησε στην αγορά, παρόλες τις δυσκολίες που προέκυψαν κατά την άνοδο του. Το Bitcoin σε αντίθεση με πολλά κρυπτονομίσματα τα οποία αποτυγχάνουν να καταλάβουν μερίδιο αγοράς, εκείνο εδραιώθηκε στην αγορά και στα ανταλλακτήρια, στα οποία κατέχει την μεγαλύτερη ρευστότητα. Λόγω της δύναμης που κατέχει επηρεάζει κατά μεγάλο βαθμό την πορεία της αγοράς των Κρυπτονομισμάτων. Όταν δηλαδή το Bitcoin παρουσιάζει μια ανοδική πορεία ως προς την τιμή στην αγορά, αντίστοιχα και η υπόλοιπη αγορά παρουσιάζει άνοδο. Αυτό δεν σημαίνει πως η ανοδική πορεία θα είναι στον ίδιο βαθμό η κατά το ίδιο ποσοστό. Ενώ όταν το bitcoin παρουσιάζει μια πτώση στην τιμή του και έχει καθοδική πορεία, είθισται να έχουν και τα εναλλακτικά νομίσματα την ίδια συμπεριφορά. (Paybis, 2024)

Η κυριαρχία του bitcoin είναι στην πραγματικότητα ένα μέτρο αξίας του Bitcoin σε σύγκριση με την συνολική κεφαλαιοποίηση της αγοράς όλων των άλλων Κρυπτονομισμάτων. Η συνολική αξία ενός νομίσματος υπολογίζεται πολλαπλασιάζοντας την τρέχουσα τιμή του στην αγορά με τον συνολικό αριθμό νομισμάτων που υπάρχουν σε κυκλοφορία. Το ποσοστό κυριαρχίας του Bitcoin λοιπόν υπολογίζεται διαιρώντας την κεφαλαιοποίηση της αγοράς του Bitcoin με την συνολική κεφαλαιοποίηση αγοράς όλων των Κρυπτονομισμάτων. Στην συνέχεια πολλαπλασιάζεται αυτός ο αριθμός με το 100 για να παρουσιαστεί ένα ποσοστό. (Paybis, 2024)

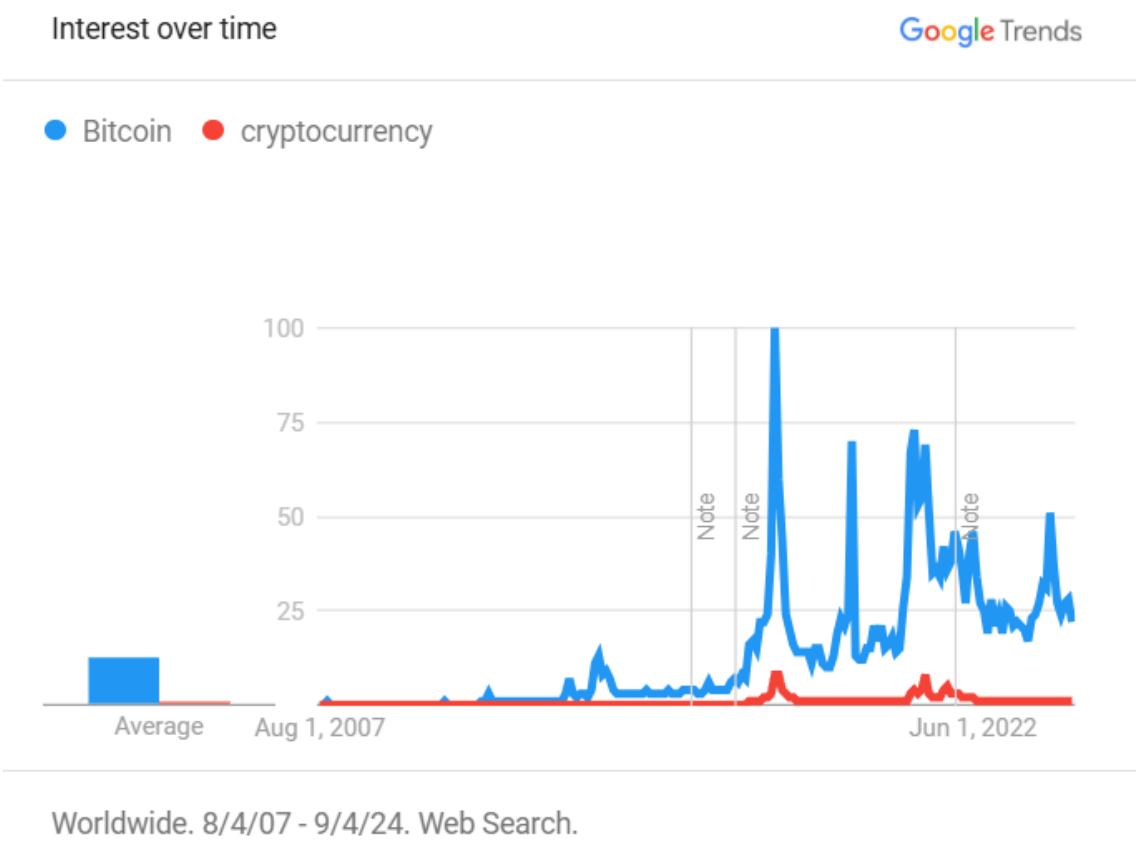
Bitcoin Dominance = (Bitcoin Market Cap/Total Crypto Market Cap) x 100

Η μέτρηση και τα αποτελέσματα του ποσοστού κυριαρχίας είναι πολύ σημαντικά καθώς από την μια δείχνουν τι μέρος της αγοράς καταλαμβάνει το Bitcoin, ενώ ακόμα δείχνουν και το πόση εμπιστοσύνη υπάρχει από την πλευρά των επενδυτών προς το Bitcoin. Πέραν από την εμπιστοσύνη ως προς το Bitcoin με αυτόν τον δείκτη παρατηρείται και κατά πόσο υπάρχει εμπιστοσύνη ως προς τα Altcoins, μιας και όταν υπάρχει χαμηλή κυριαρχία αυτό έχει ως συνέπεια αυξανόμενο ενδιαφέρον ως προς τα altcoins. Αυτή η μέτρηση είναι πολύ σημαντική και παρακολουθείται από τους αναλυτές, καθώς αντικατοπτρίζει τις αλλαγές στις τάσεις στην αγορά. (Paybis, 2024)

Ακολουθεί το διάγραμμα κυριαρχίας του Bitcoin. Παρουσιάζεται η πορεία του η οποία από το 2014 όπου και είχε το 100% της αγοράς, με την πάροδο των χρόνων και την δημιουργία νέων νομισμάτων φτάνει σημέρα (Σεπτέμβριος 2024) να ανέρχεται σε 57.7%

Εικόνα 10 διάγραμμα της πορείας της κυριαρχίας του Bitcoin

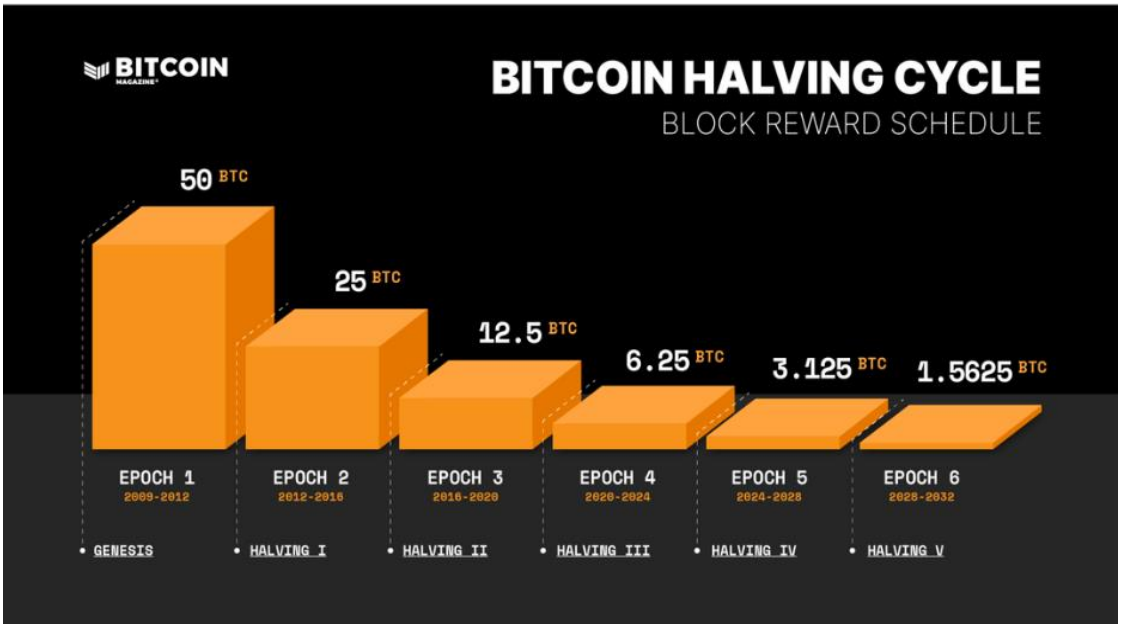
Πέραν από τα ανταλλακτήρια και την αγορά των Κρυπτονομισμάτων η ιδέα του Bitcoin εδραιώθηκε και στην καθημερινότητα , με όλο και περισσότερα βιβλία να συγγράφονται για αυτό, όλο και περισσότερα σεμινάρια να δημιουργούνται και να διδάσκονται και όλο και περισσότεροι προγραμματιστές να εξειδικεύονται στην τεχνολογία blockchain του. Οι άνθρωποι έχουν ταυτίσει την έννοια του bitcoin με αυτή του κρυπτονομίσματος, αυτό μπορεί να παρατηρηθεί και από το επόμενο διάγραμμα, το οποίο δείχνει τις αναζητήσεις που υπήρξαν ανά τον κόσμο σε όλα τα προηγούμενα χρόνια ανάμεσα στον όρο Bitcoin και τον όρο των Κρυπτονομισμάτων. Ιδιαίτερο ενδιαφέρον παρουσιάζει πως το Bitcoin ως ο βασιλιάς των Κρυπτονομισμάτων από το έτος δημιουργίας του μέχρι και σήμερα (2024) κατέχει μεγαλύτερα ποσοστά αναζήτησης, κάτι που τον καθιστά πιο δημοφιλή έναντι της ίδιας ομάδας-οικογένειας στην οποία ανήκει.



Εικόνα 11 ποσοστά αναζήτησης των όρων Bitcoin & Κρυπτονομίσματα (Google Trends, 2024)

4.3 Bitcoin halving

Κάθε τέσσερα χρόνια είναι προγραμματισμένο να συμβαίνει ένα εξαιρετικά σημαντικό γεγονός για το Bitcoin, αυτό είναι το Halving. Σε αυτό το γεγονός η προσφορά χρήματος από την παραγωγή νέων νομισμάτων Bitcoin μειώνεται κατά το ήμισυ. Αυτό σημαίνει πως η ανταμοιβή των συνεισφερόντων οι οποίοι διασφαλίζουν το δίκτυο θα μειωθεί κατά 50%. Το halving πρακτικά σημαίνει πως κάθε τέσσερα χρόνια θα αυξάνεται το κόστος παραγωγής για κάθε νέο νόμισμα. Δηλαδή στον ίδιο χρόνο και στο ίδιο κόστος οι παραγωγοί Bitcoin θα ανταμείβονται με τα μισά νομίσματα. Να σημειωθεί πως το θεμελιώδες πρωτόκολλο του Bitcoin ορίζει πως ο συνολικός αριθμός Bitcoin που μπορεί να υπάρξει ποτέ κυμαίνεται στα 21 εκατομμύρια και η υπέρβαση του καθίσταται αδύνατη. Με το Halving η ποσότητα των νομισμάτων που διατίθενται δεν μειώνεται αλλά ούτε αλλάζει η ποσότητα εκείνων που τα κατέχουν. Αυτό που αλλάζει είναι ο ρυθμός παραγωγής των νέων νομισμάτων. Μια εύλογη ερώτηση που παρουσιάζεται είναι πως θα έχουν έσοδα οι εξορύκτες όταν θα σταματήσουν να δημιουργούνται νέα Bitcoin. Το τέλος παραγωγής του Bitcoin βέβαια απέχει πολύ, μιας και το εκτιμώμενο έτος είναι το 2140. Παρ όλα αυτά η απάντηση είναι πολύ απλή, θα ανταμείβονται από τις προμήθειες των συναλλαγών. Μιας και το Bitcoin γίνεται όλο και πιο σπάνιο και η δημοτικότητα του αυξάνεται, θα αυξάνονται και οι συναλλαγές, άρα θα κερδίζουν όλο και περισσότερα χρήματα από τις προμήθειες. Η ανταμοιβή ξεκίνησε από 50 Bitcoin ανά μπλοκ και μειώνεται κατά το ήμισυ κάθε τέσσερα χρόνια. Παρακάτω παρατίθεται ο πίνακας με τις ανταμοιβές και τις ημερομηνίες του γεγονότος αυτού. (Bitcoinhalving, 2024)



Εικόνα 12 Bitcoin halving επιβραβεύσεις ανά τα χρόνια (Bitcoinhalving, 2024)

4.4 Δείκτης κατακερματισμού Bitcoin

Δείκτης κατακερματισμού ή αλλιώς Hash rate είναι μία μέτρηση υπολογιστικής ισχύος στο δίκτυο Blockchain. Θεωρείται μια σημαντική παράμετρος καθώς υπολογίζει πόσο δύσκολη είναι η εξόρυξη στο δίκτυο και με αυτόν τον τρόπο προσδιορίζει το επίπεδο ασφαλείας του δικτύου. Καθώς σε ένα κατανεμημένο σύστημα Peer-to-peer όπως αυτό του Bitcoin θα πρέπει να αντιμετωπιστούν υπέρογκα μεγέθη δεδομένων στις συναλλαγές, ο δείκτης κατακερματισμού αποδεικνύεται ως μία κρίσιμη μέτρηση. Ο δείκτης αυτός μετράει τον αριθμό των εικασιών που πραγματοποιεί κάθε υπολογιστής ανά δευτερόλεπτο στο δίκτυο για να λύσει τον κατακερματισμό (hash). Ο κατακερματισμός είναι μια μαθηματική συνάρτηση η οποία μετατρέπει μια είσοδο ενός συνόλου δεδομένων οποιουδήποτε μεγέθους σε μία κρυπτογραφημένη έξοδο σταθερού μήκους. Άρα ο δείκτης κατακερματισμού λειτουργεί ως δείκτης απόδοσης, καθώς δείχνει τον ρυθμό όπου ένα πρόγραμμα εξόρυξης απαιτεί για να υπολογίσει έναν έγκυρο κατακερματισμό μπλοκ. Όσο περισσότεροι πόροι απαιτούνται για την ανακάλυψη του επόμενου μπλοκ τόσο πιο ασφαλές είναι το δίκτυο, μιας και γίνεται πιο δύσκολη μια επίθεση στο δίκτυο από κακόβουλους χρήστες. Ο δείκτης αυτός παίζει πολύ σημαντικό ρόλο στην πορεία της τιμής και της αξίας που κατέχει το Bitcoin. Αυτό προκύπτει καθώς όσο πιο υψηλός είναι ο δείκτης, τόσο πιο ασφαλές είναι το δίκτυο, ως αποτέλεσμα να επιλέγεται περισσότερο από τους επενδυτές μιας και εκείνοι δεν θα ήθελαν να επενδύσουν τα χρήματα τους σε κάτι το οποίο είναι μη ασφαλές. Όταν το δίκτυο φτάσει για παράδειγμα σε δείκτη κατακερματισμού (hash rate) 5 TH/S, αυτό μεταφράζεται πως το δίκτυο πραγματοποιεί 5 τρισεκατομμύρια υπολογισμούς το δευτερόλεπτο για την επεξεργασία των συναλλαγών. Στο δίκτυο του bitcoin το ποσοστό κατακερματισμού σχετίζεται και με την αποζημίωση που λαμβάνει ένας εξορυκτής ή μια πισίνα εξόρυξης. Ένα υψηλό ποσοστό του δείκτη αντιστοιχεί σε αυξημένη πιθανότητα να επιτύχει μια εξόρυξη ενός μπλοκ, άρα και να αποζημιωθεί ο εξορυκτής. (Narayanan et al., 2016)

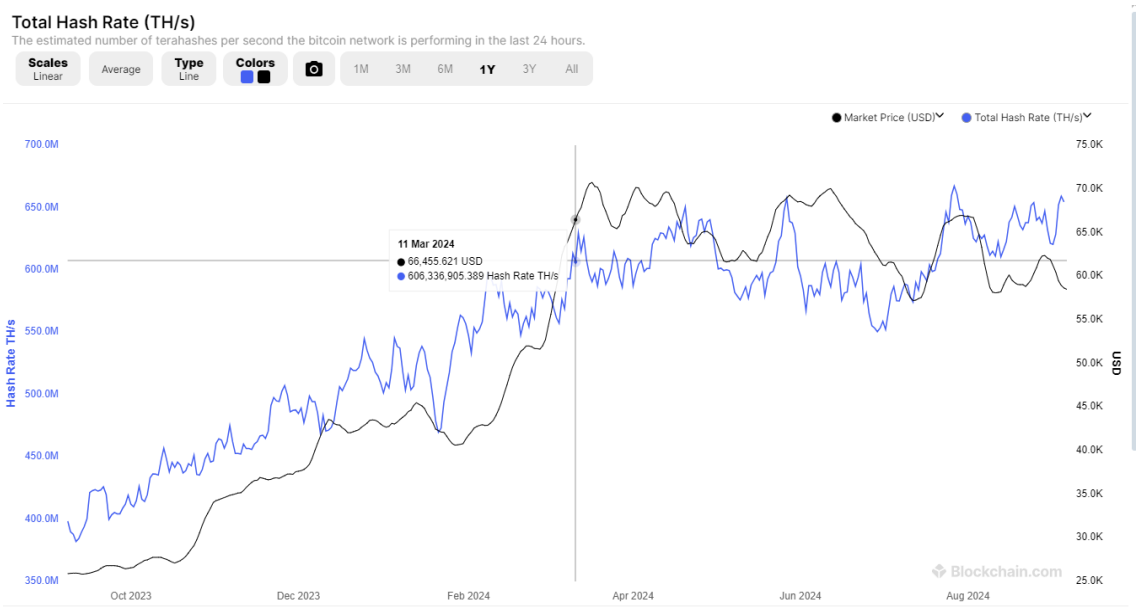
Παρόλο που ο ακριβής αριθμός της ισχύς κατακερματισμού του Bitcoin είναι άγνωστος, μπορεί να εκτιμηθεί μέσω του αριθμού μπλοκ που εξορύσσονται, αλλά και από την δυσκολία αυτών. Επειδή οι ημερήσιοι αριθμοί μπορεί να αυξομειώνονται περιοδικά και ο αριθμός των μπλοκ που εξορύσσονται να αλλάζει καθημερινά ακόμα και με μία σταθερή ισχύ κατακερματισμού, Οι αναλυτές εξετάζουν και μελετούν την αναπαράσταση της ισχύς με τον μέσο όρο επτά ημερών. (Blockchain, 2024)

Στον παρακάτω πίνακα αναπαρίσταται τα δίαφορα μεγέθη κατακερματισμού

Hashrate Units	Hash Size	Hashes Per Second
H/s (Hash)	1	One
kH/s (KiloHash)	1,000	One Thousand
MH/s (MegaHash)	1,000,000	One Million
GH/s (GigaHash)	1,000,000,000	One Billion
TH/s (TeraHash)	1,000,000,000,000	One Trillion
PH/s (PetaHash)	1,000,000,000,000,000	One Quadrillion
EH/s (ExaHash)	1,000,000,000,000,000,000	One Quintillion
ZH/s (ZettaHash)	1,000,000,000,000,000,000,000	One Sextillion
YH/s (YottaHash)	1,000,000,000,000,000,000,000,000	One Septillion

Πίνακας 2 μεγέθη κατακερματισμού (Bitcoin Magazine, 2024)

Στο παρακάτω διάγραμμα αναπαρίσταται το γράφημα του δείκτη κατακερματισμού του Bitcoin.

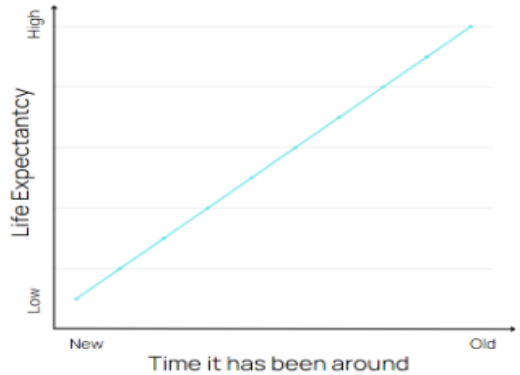


Εικόνα 13 διάγραμμα δείκτη κατακερματισμού Bitcoin (Blockchain, 2024)

4.5 Φαινόμενο Lindy και Bitcoin

Το φαινόμενο Lindy διαδόθηκε από τον Nassim Nicholas Taleb, έναν γνωστό μαθηματικό για το έργο του στην διαχείριση κινδύνου και την στατιστική ανάλυση. Το φαινόμενο Lindy είναι ένα θεώρημα το οποίο στηρίζεται στους νόμους των πιθανοτήτων και εξηγεί πως το προσδόκιμο ζωής μιας ιδέας είναι ανάλογο με την τρέχουσα ηλικία της. Εφαρμόζεται σε ιδεολογίες, θρησκείες, τεχνολογίες και όχι σε ανθρώπους ή φθαρτά όντα. Με άλλα λόγια το φαινόμενο αυτό εξηγεί πως όσο περισσότερο διαρκεί κάτι, τόσο περισσότερο είναι πιθανό να συνεχίσει να διαρκεί και στο μέλλον. Μια ιδέα η οποία διαρκεί στο βάθος χρόνων παρουσιάζει γερές βάσεις και ανθεκτικότητα. Αν για παράδειγμα μια τεχνολογία υπάρχει και υποστηρίζεται για 50 χρόνια, αναμένεται να παραμείνει σχετική για ακόμα 50. Φυσικά και υπάρχουν εξαιρέσεις μιας και όλο και περισσότερες νέες ιδέες ή τεχνολογίες κάνουν την εμφάνιση τους και αυτό καθιστά το φαινόμενο Lindy ως έναν εμπειρικό νόμο και όχι κάτι θέσφατο.

Το φαινόμενο lindy θα μπορούσε να λειτουργήσει και στην αγορά των Κρυπτονομισμάτων και συγκεκριμένα για το Bitcoin, το οποίο εδώ και 15 χρόνια είναι ο πρωτοπόρος και ο κυρίαρχος έναντι των υπολοίπων. Παρατηρώντας κατά την πάροδο των χρόνων ύπαρξης του Bitcoin, τις δυσκολίες αλλά και τους «πόλεμους» που έχει περάσει, γίνεται αντιληπτό πόσο γερές βάσεις έχει θέσει αλλά και το πόσο ανθεκτικό έχει γίνει στην αγορά των Κρυπτονομισμάτων. Πολλές κυβερνήσεις με επιθέσεις κατά του Bitcoin όπως με την χρήση υψηλών φόρων στους επενδυτές για τα κέρδη τους από τα κρυπτονομίσματα, αλλά και με επιθέσεις πιο άμεσες όπως εκείνη της Κίνας, όπου το 2017 απαγόρευσε την λειτουργία ανταλλακτηρίων και συναλλαγών υπό το Κινεζικό έδαφος, προσπάθησαν να επηρεάσουν την ανοδική του πορεία, δίχως όμως αποτέλεσμα. Στην αρχή επικράτησε μια πτώση της τιμής λόγω του πανικού που υπήρχε μεταξύ των επενδυτών, αλλά το αποτέλεσμα είχε ως νικητή το Bitcoin, το οποίο και συνέχισε να ανεβαίνει όλο και πιο ψηλά στο σκαλί του βάθρου.



Εικόνα 14 διάγραμμα αναπαράστασης του lindy effect (Bhaisora, 2024)

Ακόμα και όταν πολλοί δόλιοι χρήστες προσπάθησαν επανειλημμένως να βλάψουν το Bitcoin με κακόβουλες επιθέσεις ή χακαρίσματα (hacks), δεν κατάφεραν να ανατρέψουν αυτή την αξιοζήλευτη πορεία του. Για πολλούς επενδυτές το Bitcoin θεωρείται άτρωτο γιατί με κάθε χρονιά που περνάει, το Bitcoin συνεχίζει να βρίσκεται και πάλι στο επίκεντρο, χωρίς να χαθεί στην αφάνεια, χωρίς να καταρριφθεί η πορεία του και γιατί κανένα από τα υπόλοιπα κρυπτονομίσματα δεν έχει καταφέρει να του κλέψει την δόξα. Για αυτούς ακριβώς τους λόγους το Bitcoin καθίσταται ο κυρίαρχος της αγοράς των Κρυπτονομισμάτων. Με βάση το φαινόμενο Lindy, το Bitcoin το οποίο έχει ανελιχθεί στην αγορά και έχει αντέξει 15 έτη πολέμων και έχει εδραιωθεί ως πρωτοπόρο, θα κατέχει μια ισχυρή κυριαρχία στην αγορά των Κρυπτονομισμάτων για ακόμη 15 έτη, μιας και οι επενδυτές προτιμούν να επενδύουν σε περιουσιακά στοιχεία τα οποία έχουν αποδειχθεί πως είναι ανθεκτικά απέναντι σε δυσκολίες, έναντι εκείνων που παρουσιάζουν αστάθεια και ευπάθεια. (Bhaisora, 2024)

4.6 Ethereum, ο μεγάλος αντίπαλος του Bitcoin

Παρόλο που το Bitcoin με την πάροδο των ετών κυριάρχησε στην αγορά των Κρυπτονομισμάτων και έχει τον μεγαλύτερο όγκο συναλλαγών ημερησίως, μιας και είναι η πιο συνηθισμένη επιλογή των επενδυτών, ένα άλλο νόμισμα έχει τραβήξει αρκετά το ενδιαφέρον και την προσοχή των επενδυτών. Αυτό δεν είναι άλλο από το Ethereum (ETH). Το Ethereum ως ο μεγαλύτερος εκπρόσωπος των altcoin προσπαθεί να απειλήσει την πρωτοκαθεδρία του Bitcoin. Σύμφωνα με τα στοιχεία του Coinmarketcap το Ethereum κατέχει το 14.5% της αγοράς και είναι το δεύτερο πιο ισχυρό νόμισμα στο οικοσύστημα των Κρυπτονομισμάτων, με το τρίτο νόμισμα να απέχει πολύ από την δεύτερη θέση με ποσοστό 5.8%.

Το Ethereum ξεκίνησε το 2015 βασιζόμενο όπως και αρκετά ακόμη altcoins στην καινοτομία του Bitcoin. Μπορεί να είναι βασισμένο στην καινοτομία του Bitcoin αλλά έχει πολλές διαφορές. Μπορεί το Bitcoin να έφερε την αποκέντρωση του χρήματος αλλά το Ethereum ως ένα δίκτυο υπολογιστών σε όλο τον κόσμο φιλοδοξεί να αποτελέσει την αποκέντρωση όλου του Internet αλλά με έναν αρκετά οργανωμένο τρόπο. Το δίκτυο αυτό ακολουθεί ένα σύνολο κανόνων που ονομάζεται πρωτόκολλο Ethereum. Το δίκτυο του λειτουργεί ως θεμέλιο για κοινότητες, οργανισμούς, εφαρμογές και ψηφιακά στοιχεία που ο καθένας μπορεί να δημιουργήσει αλλά και να τα χρησιμοποιήσει χωρίς να υπάρχει μια κεντρική αρχή. Το Ethereum δεν ελέγχεται από κάποιον τρίτο και ο τρόπος με τον οποίο λειτουργεί είναι μέσω συνδεδεμένων υπολογιστών, οι οποίοι εκτελούν λογισμικό βασισμένο στο πρωτόκολλο του. Ενώ και το Bitcoin αλλά και το Ethereum λόγω της αποκεντρωμένης φύσης τους επιτρέπουν στους χρήστες να πραγματοποιούν συναλλαγές χωρίς την παρουσία κάποιου μεσάζοντα, το Ethereum κατέχει ένα συγκριτικό πλεονέκτημα που ονομάζεται smart contracts. Τα Smart contracts είναι προγράμματα υπολογιστών που λειτουργούν στο δίκτυο blockchain του Ethereum και διασφαλίζουν την ασφάλεια αλλά και την τήρηση των όρων στις συναλλαγές. Κανείς δεν μπορεί να τα τροποποιήσει καθώς είναι αυτοματοποιημένα και εκτελούνται όπως ακριβώς έχουν προγραμματιστεί χωρίς την παρέμβαση τρίτων. Με απλά λόγια το Ethereum είναι μια αποκεντρωμένη πλατφόρμα που προσφέρει ένα ευρύ φάσμα εφαρμογών στους χρήστες της όπως οικονομικά εργαλεία, βάσεις δεδομένων ακόμα και παιχνίδια. (Ethereum,2024)

Το Ether (ETH) είναι το κρυπτονόμισμα που χρησιμοποιείται από το δίκτυο του Ethereum και έχει έναν ιδιαίτερο ρόλο καθώς χρησιμοποιείται ως «καύσιμο» για την λειτουργία και την ασφάλεια του δικτύου. Αυτό προκύπτει καθώς όταν οι χρήστες χρησιμοποιούν μια

εφαρμογή Ethereum ή θέλουν να αποστείλουν ETH πρέπει να πληρώσουν ένα τέλος συναλλαγής σε ETH. Η ύπαρξη των τελών συναλλαγής λειτουργούν ως κίνητρο σε κάποιον επικυρωτή μπλοκ να επεξεργαστεί και να επαληθεύσει την συναλλαγή, καθώς εκείνος θα λάβει ως ανταμοιβή μια μικρή ποσότητα ETH. Η επιλογή εκείνων γίνεται μέσω μιας διαδικασίας στην οποία οι επικυρωτές ποντάρουν ένα ποσό νομισμάτων τους, στέλνοντας τα σε ένα ειδικό πορτοφόλι. Ο επικυρωτής που θα έχει στείλει περισσότερα νομίσματα σε σχέση με τους άλλους θα επιλεχθεί. Το κεφάλαιο που έχει αποστείλει δεν μπορεί να δαπανηθεί ή να επιστραφεί μέχρι να εξασφαλιστεί η πραγματοποίηση της συναλλαγής με ασφάλεια και αξιοπιστία. Αυτό καθιστά τους επικυρωτές αξιόλογους, μιας και σε περίπτωση απάτης θα χάσουν το κεφάλαιο που έχουν επενδύσει. Με αυτόν ακριβώς τον τρόπο το Ethereum καθίσταται ένα πολύ ασφαλές σύστημα πληρωμών. Σε αντίθεση με το Bitcoin που είναι μόνο ένα σύστημα πληρωμών το Ethereum είναι μια πλατφόρμα για χρηματοοικονομικές υπηρεσίες, για παιχνίδια, για κοινωνικά δίκτυα αλλά και άλλες πολλές εφαρμογές. (Ether, 2024)

Εικόνα 15 στατιστικά στοιχεία για την πλατφόρμα Ethereum 09/09/2024 (Ethereum, 2024)

Το Ethereum είναι μία πολύ ανερχόμενη πλατφόρμα με πολλές ιδιαιτερότητες και μεγάλη ποικιλία εφαρμογών. Προσφέρει πολύ περισσότερα από το Bitcoin καθώς όμως χρησιμοποιεί και σε πολύ μεγάλο βαθμό λιγότερη κατανάλωση ενέργειας για την επικύρωση συναλλαγών αλλά και την δημιουργία μπλοκ στο σύστημα blockchain. Είναι ένας σοβαρός αντίπαλος για το Bitcoin. Μπορεί να απέχει αρκετά σε ποσοστό από την κυριαρχία του Bitcoin, όμως το δίκτυο του Ethereum αλλά και αυτά που προσφέρει σε αυτό, το καθιστούν ως ένα πρωτοποριακό και εκσυγχρονισμένο δίκτυο με πολλές δυνατότητες, το οποίο ίσως κάποια στιγμή μπορέσει να εκθρονίσει το Bitcoin, αυτό όμως θα το κρίνει μόνον η αγορά και οι επενδυτές.

5. Blockchain

5.1 Ορισμός και στάδια του Blockchain.

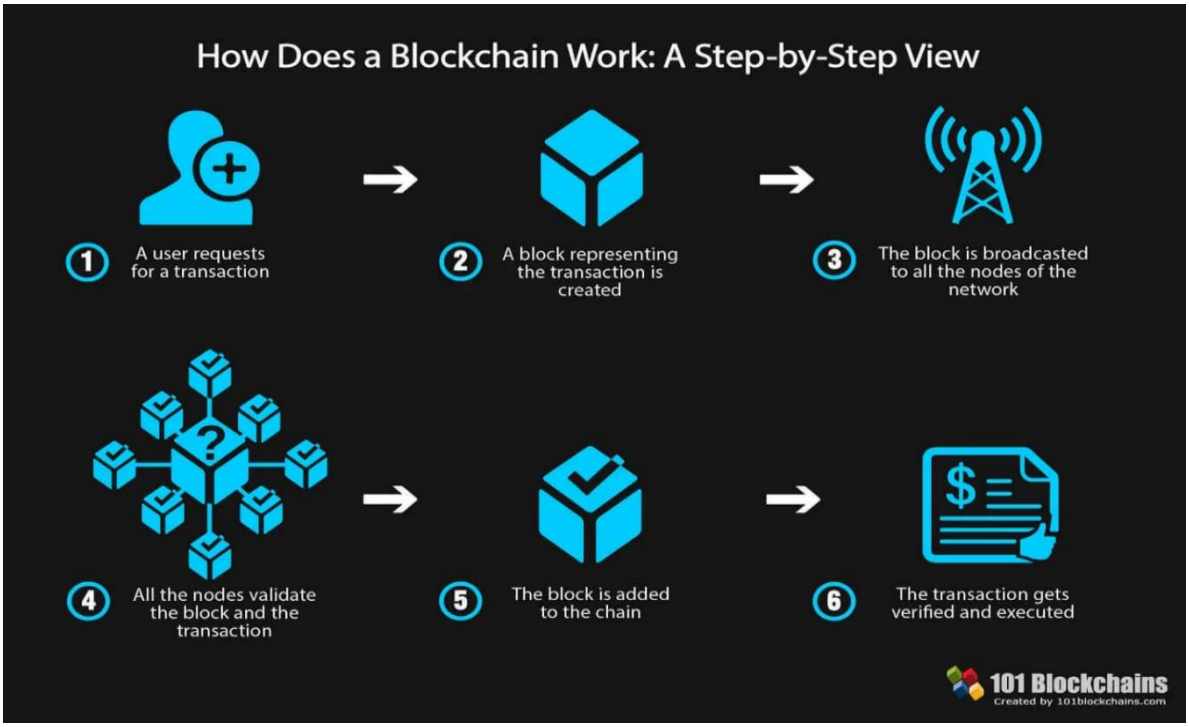
Πρόκειται για μια ακόμα πρωτοποριακή και επαναστατική τεχνολογία που αναπτύχθηκε και θα αλλάξει τον τρόπο που οι άνθρωποι χειρίζονται το διαδίκτυο, τις συναλλαγές τους και τα δεδομένα τους. Ο όρος αυτός αναφέρθηκε πριν αρκετές φορές ως μια τεχνολογία που χρησιμοποιούν τα κρυπτονομίσματα αλλά έχει πολλές ακόμα εφαρμογές πέραν του οικοσυστήματος των Κρυπτονομισμάτων. Ας εμβαθύνουμε στην ορολογία αλλά και στον τρόπο λειτουργείας.

Αρχικά ο όρος Blockchain δεν είναι τίποτε άλλο από μια σύνθετη λέξη απαρτιζόμενη από δυο μέρη, την λέξη Block και την λέξη chain. Με τον όρο Block περιγράφονται οι ψηφιακές πληροφορίες που αποθηκεύονται, όπως για παράδειγμα προσωπικά δεδομένα, συναλλαγές και πολλά ακόμη. Με τον όρο chain (αλυσίδα) περιγράφεται η διασύνδεση των πληροφοριών αυτών, οι οποίες είναι αποθηκευμένες σε μία δημόσια βάση δεδομένων «Public Ledger» στην οποία πρόσβαση έχει ο κάθε χρήστης «Node» του δικτύου. Με τον όρο «Node» εννοούμε έναν από τους υπολογιστές που εκτελούν το λογισμικό της αλυσίδας μπλοκ για την επικύρωση και την αποθήκευση των συναλλαγών στο δίκτυο. (McKinsey&Company, 2024)

Εν ολίγοις το Blockchain είναι μια αποκεντρωποιημένη τεχνολογία που βοηθάει στην ασφαλή ανταλλαγή πληροφοριών. Τα δεδομένα αποθηκεύονται σε μια βάση δεδομένων και χρησιμοποιούνται τεχνικές κρυπτογράφησης για την ασφαλή διατήρηση αυτών των δεδομένων σε πολλά ανεξάρτητα αντίγραφα. Οι συναλλαγές αποθηκεύονται σε ένα λογιστικό βιβλίο που ονομάζεται «καθολικό (Ledger)». Τα δεδομένα καταχωρούνται σε Blocks, αν δεν επικυρωθούν από τους χρήστες του δικτύου, τα block δεν προστίθενται στην αλυσίδα. Οι επικυρώσεις αυτές στηρίζονται σε ένα σύνολο κανόνων που ονομάζονται μηχανισμοί συναίνεσης «Consensus Mechanism». Οι πιο γνωστοί μηχανισμοί συναίνεσης είναι το Proof of Work (PoW) το οποίο και χρησιμοποιείται στο Bitcoin αλλά και το Proof of Stake το οποίο θεωρείται πιο ασφαλές από το Proof of work και χρησιμοποιείται από το Ethereum 2.0. Από την στιγμή που τα δεδομένα επικυρωθούν προστίθενται στην αλυσίδα και οι συναλλαγές καταγράφονται στο καθολικό (ledger). Οι κόμβοι (Nodes) για την προσπάθεια επικύρωσης αυτών των δεδομένων ανταμείβονται με ποσά του νομίσματος του συγκεκριμένου blockchain.Τα blocks αλληλοσυνδέονται ώστε η οποιαδήποτε προσπάθεια για τροποποίηση των δεδομένων που έχουν αποθηκευτεί σε αυτά, να καταστεί αδύνατη. (McKinsey&Company, 2024)

Τέλος μιας και αναφέρθηκε πως το blockchain είναι μια αποκεντρωποιημένη βάση δεδομένων, αυτό σημαίνει πως λειτουργεί σε ένα αποκεντρωποιημένο δίκτυο χρηστών, οι οποίοι μοιράζονται την πληροφορία και βρίσκονται σε κάθε γωνιά του πλανήτη. Τα διαχειριστικά δικαιώματα που κατέχουν είναι ισάξια διαμορφωμένα έτσι ώστε οι συμμετέχοντες να μην υποβαθμίζουν το δίκτυο ασκώντας εξουσία η λειτουργώντας ως «αφεντικά». (McKinsey&Company, 2024)

Η πρώτη χρήση Blockchain ήταν το 2009 με την εμφάνιση του Bitcoin, το οποίο με το σύστημα πληρωμών peer-to-peer που είχε εισάγει, αλλά και με την χρήση της τεχνολογίας blockchain, η οποία επιτρέπει απευθείας συναλλαγές μεταξύ χρηστών είχε ως αποτέλεσμα να λυθεί το πρόβλημα της διπλής δαπάνης, χωρίς να υπάρχει κάποιος τρίτος φορέας.



Εικόνα 16 Βήματα λειτουργίας blockchain (Blockchains101, 2018)

5.2 Γενικά χαρακτηριστικά του Blockchain

Μιας και η τεχνολογία blockchain είναι τόσο πρωτοποριακή, δεν θα μπορούσε να μην έχει και ιδιαίτερα χαρακτηριστικά. Τόσο ιδιαίτερα που την κάνουν να ξεχωρίζει.

Αρχικά το blockchain είναι μια ασφαλής βάση δεδομένων καθώς χρησιμοποιεί μηχανισμούς κρυπτογραφίας. (Verma. Dhanda, 2023)

Εκτός από μια ασφαλής βάση δεδομένων το blockchain είναι και μια ψηφιακή βάση δεδομένων η οποία λειτουργεί πλήρως διαδικτυακά. (Verma. Dhanda, 2023)

Επιπλέον λόγω της αποκεντρωμένης φύσης του δικτύου της δεν απαιτείται η ύπαρξη ενός τρίτου έμπιστου φορέα όπως στο τραπεζικό σύστημα. (Verma. Dhanda, 2023)

Ακόμη λόγω της αυτοματοποίησης των διαδικασιών που προσφέρει αλλά και την μη ύπαρξη του μεσάζοντα, έχει μειωμένα κόστη σε αντίθεση με το τραπεζικό σύστημα, όπου εκτός από την ύπαρξη του μεσάζοντα, υπάρχει και το κόστος προμήθειας. (Verma. Dhanda, 2023)

Επίσης μόλις καταγραφεί μια συναλλαγή σε ένα μπλοκ δεν μπορεί να αλλαχτεί ή να διαγραφεί. Αυτό κάνει τις συναλλαγές μη αναστρέψιμες σε αντίθεση με τα παραδοσιακά συστήματα. (Verma. Dhanda, 2023)

Το δίκτυα blockchain χωρίζονται σε δύο κατηγορίες με βάση τον τρόπο εισόδου των χρηστών. Στα Δημόσια (Public) στα οποία οποιοσδήποτε μπορεί να συμμετέχει στο δίκτυο και στα Ιδιωτικά (Private) στα οποία η πρόσβαση επιτρέπεται μόνο σε ορισμένους χρήστες. (Verma. Dhanda, 2023)

Τέλος τα δίκτυα του χωρίζονται σε δυο ακόμα κατηγορίες με βάση τα δικαιώματα κάθε χρήστη για καταχώρηση. Η πρώτη κατηγορία αφορά τα δίκτυα με αδειοδότηση (Permissioned). Σε αυτά μόνο συγκεκριμένα nodes μπορούν να καταχωρήσουν δεδομένα, ενώ μόνο συγκεκριμένες εγγραφές είναι ορατές. Τέλος η δεύτερη κατηγορία αφορά τα δίκτυα χωρίς αδειοδότηση (Permissionless), στα οποία οποιοσδήποτε μπορεί να διαβάσει η να καταχωρήσει δεδομένα στα blocks. (Verma. Dhanda, 2023)

5.3 Εφαρμογές Blockchain

Το blockchain χρησιμοποιείται σήμερα από όλο και περισσότερες εταιρίες σε πολλούς και διαφορετικούς κλάδους πέραν των Κρυπτονομισμάτων. Πολλοί φαντάζονται πως χρησιμοποιείται κατά κύριο λόγω στον οικονομικό κλάδο κάτι το οποίο δεν ισχύει μιας και λειτουργεί σε κλάδους όπως στην εφοδιαστική αλυσίδα , στην υγειονομική περίθαλψη αλλά και την ενέργεια.

Η πρώτη της εφαρμογή δεν θα μπορούσε να είναι άλλη από αυτή στα χρηματοοικονομικά συστήματα όπως εκείνα των τραπεζών αλλά και των χρηματιστηρίων. Μπορεί να φαίνεται περίεργο μιας και το σύστημα αυτό λειτουργεί με ένα κεντροποιημένο σύστημα και προϋποθέτει την ύπαρξη μεσάζοντα, αλλά η τεχνολογία blockchain έχει χρησιμοποιηθεί εδώ για την διαχείριση διαδικτυακών πληρωμών και συναλλαγών. Η Singapore exchange limited είναι μια εταιρία επενδύσεων χαρτοφυλακίου που δραστηριοποιείται στην Ασία και χρησιμοποιεί την τεχνολογία blockchain για την δημιουργία πιο αποτελεσματικών λογαριασμών για διατραπεζικές πληρωμές. Η τεχνολογία blockchain προσφέρει διαφάνεια στις συναλλαγές και προστατεύει σε ασύλληπτο βαθμό τα δεδομένα των χρηστών. Επιπλέον βοηθάει τα χρηματοπιστωτικά ιδρύματα να μειώσουν το κόστος, δημιουργώντας αυτοματοποιημένα συστήματα ροής εργασιών για την παρακολούθηση συναλλαγών χρηστών, προστατεύοντας τα περιουσιακά τους στοιχεία. Τέλος τα χρηματοοικονομικά συστήματα θα μπορούσαν να εκμεταλλευτούν την δύναμη που κατέχει το blockchain και να επιβλέπουν τις ψηφιακές επενδύσεις. (vzhuk, 2022)

Επιπλέον μια εφαρμογή του blockchain είναι στον τομέα της εφοδιαστικής αλυσίδας όπου οι εταιρίες χρησιμοποιούν την εφαρμογή της για την παρακολούθηση και την ανίχνευση υλικών για την πιστοποίηση αυθεντικότητας και προέλευσης. Έτσι με αυτόν τον τρόπο συνδέεται ο παραγωγός με τον αγοραστή, καθώς όταν κατασκευαστεί ένα προϊόν δημιουργείται και ένας QR κωδικός ο οποίος εμπεριέχει σημαντικές πληροφορίες για το προϊόν, όπως ο τόπος προελεύσεως, η ποιότητα αλλά και το είδος (αν είναι οργανικό η βιολογικό), το όνομα του καλλιεργητή ή την εταιρία που το παράγει. Τα δεδομένα αυτά κωδικοποιούνται στην αλυσίδα block και εάν υπάρχει ανάκληση ενός προϊόντος οι κατασκευαστές μπορούν να χρησιμοποιήσουν το blockchain για να διαπιστώσουν σε ποιες παρτίδες προϊόντος υπήρξαν προβλήματα και να τις ανακαλέσουν, μειώνοντας έτσι τον κίνδυνο για μεγαλύτερα μελλοντικά κόστη. (SAP, 2024)

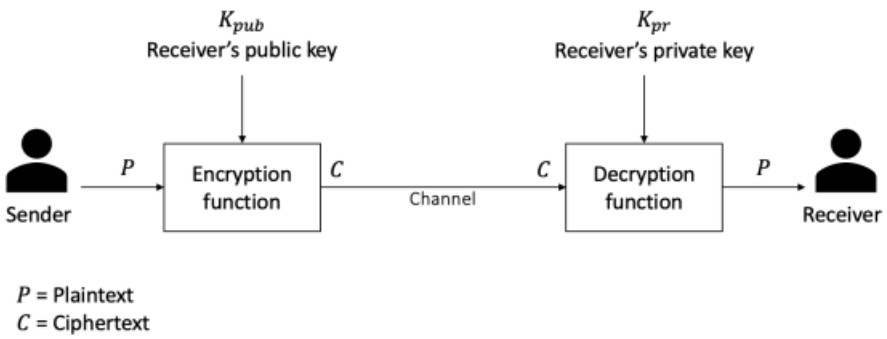
Επίσης μια ακόμη εφαρμογή είναι εκείνη στον κλάδο της ενέργειας όπου εταίρες παροχής ενέργειας χρησιμοποιούν το blockchain για να δημιουργήσουν peer-to-peer πλατφόρμες ανταλλαγής ενέργειας και την πρόσβαση σε ανανεώσιμες πηγές ενέργειας. Οι ιδιοκτήτες που έχουν ηλιακούς συλλέκτες στα σπίτια τους μπορούν να πουλήσουν την πλεονάζουσα ηλιακή τους ενέργεια σε κοντινούς κατοίκους μέσω αυτοματοποιημένων διαδικασιών με έξυπνους μετρητές, οι οποίοι συλλέγουν τις πληροφορίες και τις καταγράφουν με ασφάλεια στο σύστημα blockchain. Τέλος οι χρήστες μπορούν να ενοικιάσουν ηλιακούς συλλέκτες σε περιοχές που δεν έχουν τόση πρόσβαση σε ενέργεια και να εκλάβουν ανταμοιβές και έσοδα από τις κοινότητες αυτές. (Egunjobi, 2024)

Ένας ακόμη τομέας εφαρμογής του blockchain είναι ο τομέας του ανθρωπίνου δυναμικού (HR) στον οποίο μέσω της εφαρμογής του blockchain θα καταγράφονται και θα ελέγχονται τα στοιχεία των υποψηφίων για την εύρεση εργασίας. Τέτοια στοιχεία θα είναι τα πτυχία, η εργασιακή εμπειρία – προϋπηρεσία, οι πιστοποιήσεις και γενικότερα στοιχεία του βιογραφικού σημειώματος. Στόχος είναι λοιπόν μιας και η επαλήθευση των προσόντων των υποψηφίων είναι μια αρκετά χρονοβόρα διαδικασία να γίνει απλούστευση αυτής και να αυτοματοποιηθεί, μειώνοντας έτσι δραστικά το χρόνο που απαιτείται αλλά και η επαλήθευση των διαπιστευτηρίων να γίνεται πιο αποτελεσματικά. Ένα χαρακτηριστικό παράδειγμα είναι εκείνο ενός μη κερδοσκοπικού ιδρύματος (ΜΚΟ) του Velocity network το οποίο χρησιμοποιεί μια πλατφόρμα ανοικτού κώδικα και δίνει στα άτομα των έλεγχο του τρόπου κοινής χρήσης των δεδομένων τους, τα οποία προστατεύονται από τους κανονισμούς GDPR. Επιπλέον δημιουργεί μια πηγή επαληθευμένων πληροφοριών για τους υποψηφίους μιας και τα ακαδημαϊκά ιδρύματα, οι εργοδότες, οι φορείς πιστοποιήσεων αλλά και άλλοι εκδότες διαπιστευτηρίων να μπορούν να επισυνάπτουν τα διαπιστευτήρια στο blockchain αποτρέποντας τους υποψηφίους να συμπεριλαμβάνουν στο βιογραφικό τους παραπλανητικές πληροφορίες για επιτεύγματα ή δεξιότητες. Με αυτό τον τρόπο οι προσλήψεις σε κάθε οργανισμό που απαιτεί μια συνέντευξη να γίνονται πιο αποτελεσματικά και ταχύτερα. (SAP, 2024)

5.4 Ασύμμετρη κρυπτογραφία

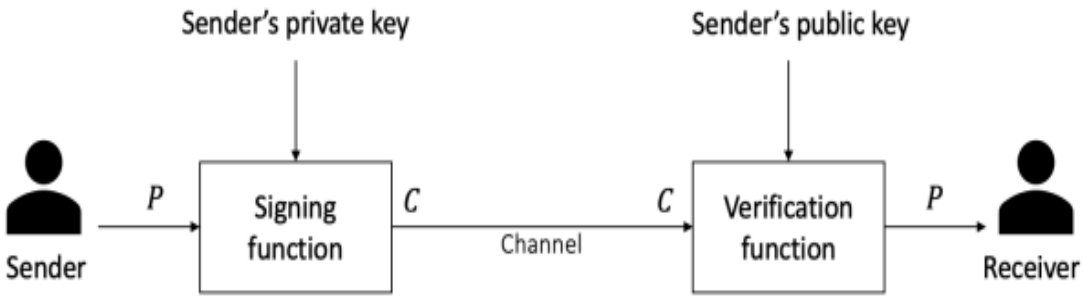
Μία βάση δεδομένων blockchain θεωρείται πολύ ασφαλής μιας και χρησιμοποιεί μηχανισμούς κρυπτογραφίας. Ένας από αυτούς είναι ο μηχανισμός ασύμμετρης κρυπτογραφίας (asymmetric cryptography) ή όπως αλλιώς ονομάζεται κρυπτογραφία δημόσιου κλειδιού (public-key cryptography). Σε αυτόν τον μηχανισμό κάθε χρήστης έχει στην διάθεση του δύο κλειδιά, το δημόσιο (public) και το ιδιωτικό (private). Το δημόσιο κλειδί κοινοποιείται στο δίκτυο και χρησιμοποιείται για την δημιουργία της δημόσιας διεύθυνσης (public address) κάθε χρήστη. Αντιθέτως το ιδιωτικό κλειδί όπως το υποδηλώνει και το όνομα του είναι ένας τυχαία παραγόμενος αριθμός ο οποίος δεν κοινοποιείται στο δίκτυο και παραμένει κρυφός, καθώς τον γνωρίζει μόνο ο ίδιος ο χρήστης. Το ιδιωτικό κλειδί χρησιμοποιείται για την ψηφιακή υπογραφή κάθε συναλλαγής του ιδιοκτήτη του. (Bashir, 2023)

Στο παρακάτω διάγραμμα διαδραματίζεται ο τρόπος με τον οποίο ο αποστολέας κρυπτογραφεί τα δεδομένα P, χρησιμοποιώντας το δημόσιο κλειδί και την κρυπτογράφηση του παραλήπτη και εξάγει κρυπτογραφημένα δεδομένα C. Αυτά τα δεδομένα μεταδίδονται μέσω του δικτύου και φτάνουν στον δέκτη. Κατά την άφιξη τους στον δέκτη, μόνο εκείνος μπορεί να τα αποκρυπτογραφήσει, χρησιμοποιώντας το ιδιωτικό του κλειδί και να εξάγει τα αποκρυπτογραφημένα πλέον δεδομένα P σε μορφή κειμένου. (Bashir, 2023)



Εικόνα 17 τρόπος λειτουργίας κρυπτογραφίας (Bashir, 2023)

Στο παρακάτω διάγραμμα παρατηρείται πώς ο δέκτης χρησιμοποιεί την κρυπτογραφία του δημόσιου κλειδιού για την επαλήθευση της ακεραιότητας του μηνύματος. Συγκεκριμένα ο αποστολέας υπογράφει ψηφιακά τα δεδομένα με την χρήση του ιδιωτικού του κλειδιού και στη συνέχεια μέσω του δικτύου μεταδίδει το μήνυμα στον δέκτη. Κατά την άφιξη του μηνύματος στον παραλήπτη επαληθεύεται η ακεραιότητα του από το δημόσιο κλειδί του αποστολέα. (Bashir, 2023)



Εικόνα 18 μέθοδος αποστολής κωδικοποιημένου μηνύματος (Bashir, 2023)

Όπως παρατηρήθηκε στα παραπάνω διαγράμματα τα οποία αφορούσαν την μέθοδο αποστολής ενός κωδικοποιημένου μηνύματος αλλά και την κρυπτογράφηση και αποκρυπτογράφηση αυτών, προκύπτει το συμπέρασμα πως πρόκειται για μια πολύ ασφαλή διαδικασία. Ο μόνος τρόπος παραβίασης της ιδιωτικότητας και η μη εξουσιοδοτημένη πρόσβαση είναι με την απώλεια και την κοινοποίηση του ιδιωτικού κλειδιού. (Bashir, 2023)

5.5 Proof of Work

Κατά την εξήγηση του πως λειτουργεί το blockchain αναφέρθηκαν οι μηχανισμοί συναίνεσης, οι οποίοι είναι ένα σύνολο κανόνων – κανονισμών, κοινά αποδεκτών από όλους τους χρήστες του δικτύου blockchain. Χρησιμοποιούνται για την επικύρωση των συναλλαγών, οι οποίες αποθηκεύονται σε ένα block και προστίθενται στην αλυσίδα. Ένας τέτοιος μηχανισμός είναι το Proof of work (PoW) και ο λόγος για τον οποίο ονομάζεται κατά αυτόν τον τρόπο είναι ότι το δίκτυο απαιτεί τεράστια επεξεργαστική ισχύ. Ο μηχανισμός Proof of Work είναι ο πρώτος που προτάθηκε και χρησιμοποιήθηκε στο Bitcoin. Σε αυτόν τον μηχανισμό ένας χρήστης δημοσιεύει το επόμενο μπλοκ εφόσον είναι ο πρώτος που θα λύσει ένα σύνολο μαθηματικών προβλημάτων ή όπως αλλιώς ονομάζονται μαθηματικών παζλ. Η επίλυση αυτών των μαθηματικών προβλημάτων είναι μια δύσκολη διαδικασία σε αντίθεση με τον έλεγχο της λύσης η οποία είναι αρκετά εύκολη. Έτσι οι κόμβοι (nodes) μπορούν εύκολα και γρήγορα να επικυρώνουν τυχόν προτεινόμενες λύσεις και επόμενα μπλοκ, όπως επίσης και να απορρίπτουν τα εσφαλμένα. Στόχος σε αυτά τα μαθηματικά προβλήματα είναι να βρεθεί η τιμή της μεταβλητής «nonce» . Για παράδειγμα στο Bitcoin η δυσκολία του παζλ προσαρμόζεται κάθε 2016 μπλοκ για να επηρεαστεί το ποσοστό δημοσίευσης περίπου μια φορά κάθε δέκα λεπτά. Το μαθηματικό πρόβλημα δυσκολεύει όλο και περισσότερο αν ο χρήστης εντοπίζει συχνά την τιμή του. Η προσαρμογή της δυσκολίας πραγματοποιείται με την αύξηση ή την μείωση του αριθμού των αρχικών μηδενικών που απαιτούνται. Αν αυξηθούν τα αρχικά μηδενικά αυξάνεται η δυσκολία του μαθηματικού τύπου καθώς οποιαδήποτε λύση πρέπει να είναι μικρότερη από το επίπεδο δυσκολίας και υπάρχουν λιγότερες πιθανές λύσεις. Ενώ μειώνοντας τον αριθμό των αρχικών μηδενικών μειώνεται το επίπεδο δυσκολίας γιατί υπάρχουν περισσότερες πιθανές λύσεις. Με αυτές τις προσαρμογές διατηρείται η υπολογιστική δυσκολία του παζλ αλλά και η ασφάλεια του πυρήνα του δικτύου Bitcoin. (Yaga, 2019) Ένα παράδειγμα αποτελέσματος είναι το ακόλουθο:

SHA256("blockchain1700876653") =

0x00000003ba55d20c9cbd1b6fb34dd81c3553360ed918d07acf16dc9e75d7c7f1

Χρειάστηκαν 90.263.918 εικασίες και 10 λεπτά και 14 δευτερόλεπτα για την επίλυση του. (Yaga, 2019)

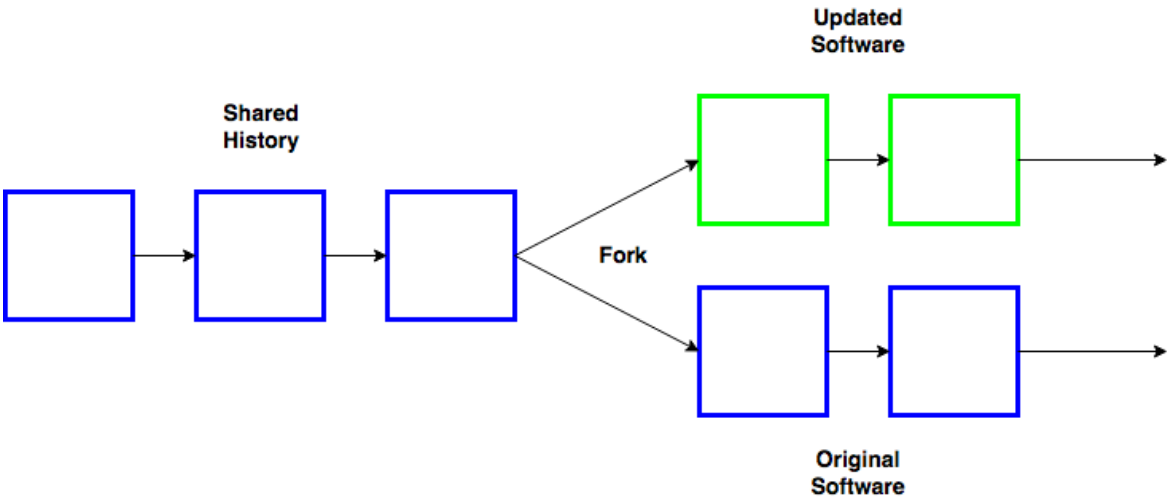
5.6 Proof of Stake

Ένας εναλλακτικός μηχανισμός συναίνεσης είναι το Proof of Stake (PoS) ή αλλιώς απόδειξη στοιχήματος, ο οποίος προτάθηκε ως μία εναλλακτική λύση στο ήδη υπάρχον μηχανισμό συναίνεσης Proof of Work. Το Proof of Stake μπορεί να είναι ένας διαφορετικός τρόπος επικύρωσης συναλλαγών αλλά ο σκοπός του είναι ο ίδιος με αυτόν του Proof of Work, αυτό που αλλάζει δραματικά είναι η διαδικασία για την επίτευξη αυτού του σκοπού. Αρχικά ενώ στο proof of work η επιλογή του χρήστη για την δημοσίευση των μπλοκ γινόταν με το ποιος χρήστης θα επέλυε πρώτος ένα μαθηματικό πρόβλημα, στον μηχανισμό συναίνεσης η επιλογή λειτουργεί διαφορετικά. Εδώ η επιλογή του χρήστη που θα δημοσιεύσει ένα νέο μπλοκ στο σύστημα blockchain συνδέεται με το ποσό των νομισμάτων που ο χρήστης κατέχει, δείχνοντας έτσι πως έχει μερίδιο στο νόμισμα. Όσο μεγαλύτερο μερίδιο κατέχει ο χρήστης ο οποίος ονομάζεται επικύρωσής αν επιλεγεί, τόσο μεγαλύτερες οι πιθανότητες επιλογής του, καθώς τόσο πιο πιθανό είναι να θέλει να επιτύχει το σύστημα και τόσο πιο απίθανο να θέλει να το βλάψει. Ο χρήστης λοιπόν ποντάρει ένα μέρος του μεριδίου του στέλνοντας τα νομίσματα σε μια συγκεκριμένη διεύθυνση ή κρατώντας τα σε ένα ειδικό ψηφιακό πορτοφόλι. Μόλις πραγματοποιηθεί το ποντάρισμα, τα κρυπτονομίσματα που έχουν ποντάριστεί δεν μπορούν να δαπανηθούν. Έτσι η επιλογή του χρήστη πραγματοποιείται αναλογικά με το ποσό των νομισμάτων που έχει ποντάρει ως προς το συνολικό ποσό στοιχηματισμένων Κρυπτονομισμάτων από όλους τους χρήστες. Σε αντίθεση με το παραδοσιακό μηχανισμό συναίνεσης Proof of Work στο οποίο τα νομίσματα εξορύσσονται, στο Proof of Stake τα νομίσματα είναι ήδη διανεμημένα. Με αυτόν τον τρόπο απαιτείται λιγότερη επεξεργαστική ισχύ (ηλεκτρική ενέργεια). Όταν ένας κόμβος επιλεχθεί για να σφυρηλατήσει το επόμενο μπλοκ, θα ελέγξει αν οι συναλλαγές εσωτερικά του μπλοκ είναι έγκυρες. Αν και εφόσον πληρούνται οι προϋποθέσεις σύμφωνα με τους κανόνες-κανονισμούς, τότε ο κόμβος υπογράφει το μπλοκ και το προσθέτει στην αλυσίδα. Ως ανταμοιβή ο κόμβος λαμβάνει τα τέλη συναλλαγής. (YAGA, 2019)

Χαρακτηριστικά παραδείγματα Κρυπτονομισμάτων που χρησιμοποιούν τον μηχανισμό συναίνεσης Proof of Stake είναι το Solana, το Polkadot, το Avalanche, ενώ το Ethereum βρίσκεται υπό την μεταβίβαση στο Proof of Stake με την αναβάθμιση του δικτύου του σε Ethereum 2.0.

5.7 Forking

Forks ονομάζονται οι αλλαγές που πραγματοποιούνται στα πρωτόκολλα δικτύου και στις δομές δεδομένων του blockchain. Τα πρωτόκολλα είναι βασικά σύνολα κανόνων που επιτρέπουν την κοινή χρήση δεδομένων μεταξύ των υπολογιστών του δικτύου. Τα πρωτόκολλα είναι σημαντικά καθώς καθορίζουν την δομή του Blockchain και της κατανεμημένης βάσης δεδομένων. Αυτές οι αλλαγές είναι στην πραγματικότητα αναβαθμίσεις, καθώς στοχεύουν στην αύξηση της λειτουργικότητας αλλά και στην αντιμετώπιση κινδύνων ασφαλείας. Οι Κατηγορίες που απαρτίζουν τα Forks είναι τα hard forks και τα soft forks. Σε ένα soft fork οι αναβαθμίσεις-αλλαγές είναι συμβατές προς τα πίσω με κόμβους που δεν έχουν αναβαθμιστεί. Ενώ για ένα hard fork οι αλλαγές δεν είναι συμβατές προς τα πίσω, καθώς οι κόμβοι που δεν έχουν ενημερωθεί, θα απορρίψουν τα νέα μπλοκ που ακολουθούν τις αλλαγές. Αυτό μπορεί να οδηγήσει σε διάσπαση του δικτύου blockchain, δημιουργώντας πολλαπλές εκδόσεις του. (YAGA., 2019)

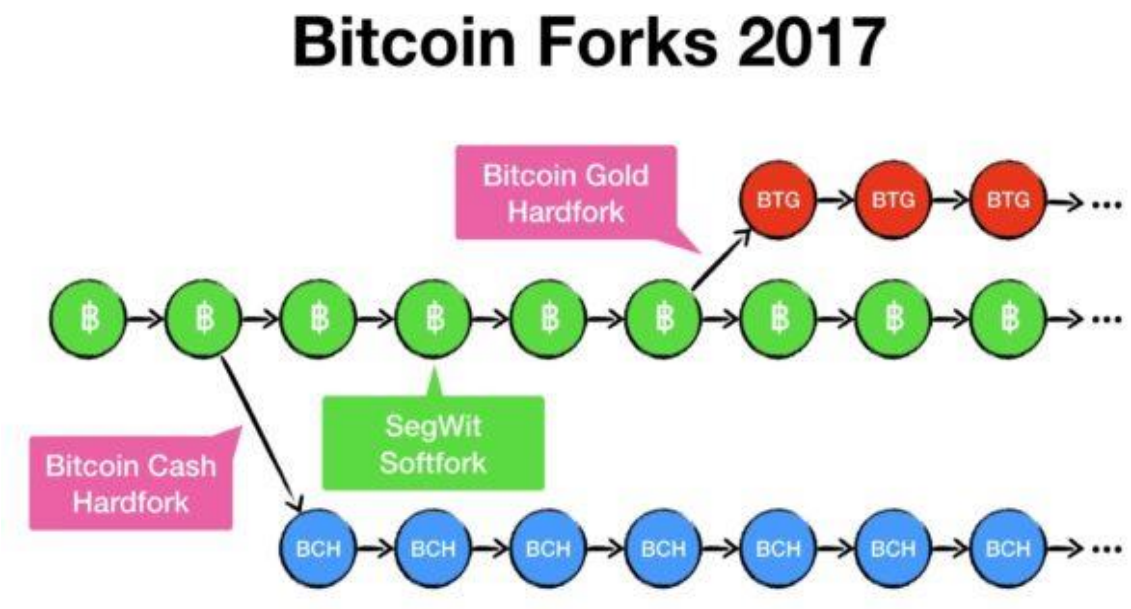


Εικόνα 19 διάσπαση αλυσίδων από την διαδικασία fork (Maddrey, 2018)

Τα soft forks είναι ένας μηχανισμός σταδιακής αναβάθμισης του δικτύου που επιτρέπει στους συμμετέχοντες είτε έχουν αναβαθμίσει το λογισμικό τους είτε όχι να αναγνωρίζουν νέα μπλοκ και να υπάρχει συμβατότητα με το δίκτυο. Η εφαρμογή τους είναι πολύ εύκολη καθώς χρειάζεται μόνο η αναβάθμιση του λογισμικού από την πλειοψηφία των συμμετεχόντων. Όπως περιεγράφηκε πριν οι συμμετέχοντες ανεξάρτητα με το αν έχουν κάνει την αναβάθμιση μπορούν να ελέγξουν τις νέες αναβαθμισμένες συναλλαγές, κάτι

τέτοιο δεν ισχύσει για τους εξορύκτες (Miners), οι οποίοι αν δεν έχουν αναβαθμίσει το σύστημα τους, κάθε προσπάθεια για εξόρυξη ενός νέου αναβαθμισμένου μπλοκ θα απορρίπτεται. (YAGA., 2019)

Τα hard forks είναι ένας μηχανισμός αναβάθμισης λογισμικού η οποία δεν είναι συμβατή με παλαιότερες εκδόσεις. Όλοι οι κόμβοι δημοσίευσης θα πρέπει να αλλαχθούν και να χρησιμοποιούν πλέον το νέο αναβαθμισμένο πρωτόκολλο. Οι κόμβοι που δεν θα ενημερωθούν θα αποκόπτονται από το δίκτυο, καθώς θα απορρίπτουν τα νέα διαμορφωμένα block και θα δέχονται μόνο εκείνα με την παλαιότερη έκδοση. Αυτό θα έχει ως αποτέλεσμα να δημιουργηθούν δυο εκδόσεις blockchain ταυτόχρονα, η αρχική έκδοση blockchain και η νέα έκδοση που θα λειτουργεί με το νέο αναβαθμισμένο σύστημα πρωτοκόλλων. Αν οι κόμβοι αναβαθμιστούν, τότε θα μπορούν να συνεχίσουν να πραγματοποιούν συναλλαγές στην ενημερωμένη αλυσίδα. Η διάσπαση της αλυσίδας έχει ως αποτέλεσμα την δημιουργία ενός νέου νομίσματος. Ένα χαρακτηριστικό παράδειγμα είναι εκείνο του Ethereum και του Ethereum classic. Όπως και του bitcoin με το bitcoin gold και το bitcoin cash. (YAGA., 2019)



Εικόνα 20 Η διάσπαση της αλυσίδας Bitcoin μετά το fork του 2017 (Aracely, 2020)

5.8 Smart contracts

Φανταστείτε πως θέλετε να πραγματοποιήσετε μια περίπλοκη συναλλαγή μεταξύ του εαυτού σας και κάποιου άλλου. Θα πηγαίνατε σε κάποιον δικηγόρο ή ακόμα και σε συμβολαιογράφο για να συντάξει το συμφωνητικό, του όρους και θα περιμένατε την άλλη πλευρά να συμφωνήσει στους όρους που έχουν τεθεί. Αφού θα υπήρχε συμφωνία μεταξύ των δυο μερών και εφόσον πληρούνταν οι προϋποθέσεις θα προχωρούσε η πραγματοποίηση της συναλλαγής. Ακριβώς με αυτόν τον τρόπο θα λειτουργούσατε στην καθημερινή σας ζωή. Τα έξυπνα συμβόλαια έχουν δημιουργηθεί για να εκπληρώνουν τέτοιες συναλλαγές. Επρόκειτο για ένα λογισμικό υπολογιστή που λειτουργεί στο δίκτυο του blockchain, το οποίο εκτελεί και επαληθεύει μια αυτοεκτελούμενη ψηφιακή συμφωνία, η οποία επιτρέπει σε δυο η περισσότερα μέρη να ανταλλάξουν οτιδήποτε έχει αξία με διαφάνεια. Επειδή όπως προαναφέρθηκε τα έξυπνα συμβόλαια λειτουργούν στο δίκτυο του blockchain, αυτό έχει ως αποτέλεσμα να μην χρειάζεται η ύπαρξη κάποιου τρίτου μέρους που θα ελέγχει την συναλλαγή. Έτσι λοιπόν τα έξυπνα συμβόλαια παίρνουν το ρόλο του διαιτητή και μιας και υλοποιούνται με την χρήση κώδικα και όχι από κάποιον άνθρωπο, εξαλείφεται η πιθανότητα για λάθη. Επιπλέον επειδή ακριβώς λειτουργεί σε ένα αποκεντρωμένο σύστημα και δεν απαιτείται η ύπαρξη κάποιου μεσάζοντα, υπάρχει όφελος, εξοικονομώντας χρήματα άλλα και χρόνο μιας και αυτοματοποιεί τις διαδικασίες. Τα έξυπνα συμβόλαια λοιπόν θέτουν τους κανόνες της συμβάσης αλλά και τις τιμωρίες σε περίπτωση παράβασης. Όταν τα δυο μέρη συμφωνήσουν στους όρους του έξυπνου συμβολαίου, τότε υπογράφουν κρυπτογραφικά το έξυπνο συμβόλαιο και στην συνέχεια ενεργοποιείται αυτόματα η πραγματοποίηση της σύμβασης. Οι εφαρμογές που υποστηρίζονται από έξυπνα συμβόλαια ονομάζονται αποκεντρωμένες εφαρμογές η dapps και περιλαμβάνουν τεχνολογία αποκεντρωμένης χρηματοδότησης. Ένα παράδειγμα εφαρμογής τους είναι το Uniswap. Το Uniswap είναι ένα αποκεντρωμένο ανταλλακτήριο που επιτρέπει στους χρήστες του να εμπορεύονται συγκεκριμένα κρυπτονομίσματα με την μέθοδο των έξυπνων συμβολαίων χωρίς την ύπαρξη κάποιας κεντρικής αρχής που θα ορίζει τις ισοτιμίες. Ένα ακόμα παράδειγμα είναι το compound . Επρόκειτο για μια πλατφόρμα που χρησιμοποιεί έξυπνα συμβόλαια, τα οποία επιτρέπουν στους χρήστες να αποκτήσουν δάνειο και στους επενδυτές να κερδίσουν από τους τόκους, χωρίς να υπάρχει η ανάγκη για μια τράπεζα. (Ejeke, 2022)

5.9 Πως γίνεται η Εξόρυξη (Mining) ?

Αναφέρθηκε πολλές φορές στις προηγούμενες ενότητες ο όρος εξόρυξη (mining) και περιεγράφηκε εν συντομία. Σε αυτό το κεφάλαιο 5.9 θα αναλυθεί ο τρόπος και τα μέσα που απαιτούνται για την πραγματοποίηση μιας εξόρυξης.

Αντίθετα με το παραδοσιακό χρηματοοικονομικό σύστημα, όπου τα παραδοσιακά νομίσματα (Fiat currencies) υποστηρίζονται από μία κεντρική αρχή ή μια κυβέρνηση, στο οικοσύστημα των Κρυπτονομισμάτων δεν συμβαίνει κάτι αντίστοιχο. Επειδή στα κρυπτονομίσματα δεν υπάρχει κάποια κεντρική αρχή να τα υποστηρίζει, η δημιουργία τους προέρχεται από την λύση μιας περίπλοκης σειράς μαθηματικών υπολογισμών που ονομάζεται εξόρυξη. Όπως έχει προαναφερθεί, ο σκοπός της επίλυσης αυτών των υπολογισμών γίνεται για την επιβεβαίωση των συναλλαγών αλλά και την διατήρηση της ασφάλειας του δικτύου. Οι εξορυκτές (miners) ανταμείβονται για την συμβολή τους στην επίλυση των μαθηματικών πράξεων, για κάθε νέο νόμισμα που «ανακαλύπτουν» λαμβάνουν μια ανταμοιβή και για κάθε προσθήκη μπλοκ στο δίκτυο blockchain συλλέγουν προμήθεια από τις συναλλαγές. Αυτοί είναι οι βασικοί λόγοι που το σύστημα αυτό έχει γίνει πολύ επιτυχημένο και όλο και περισσότεροι χρήστες στοχεύουν στο να γίνουν εξορυκτές Κρυπτονομισμάτων. Όμως δεν πρόκειται για κάτι εύκολο, καθώς η διαδικασία εξόρυξης απαιτεί πολλού πόρους, κάτι το οποίο καθιστά δύσκολο σε όλους τους χρήστες να γίνουν εξορυκτές. (Hoffman, 2020)

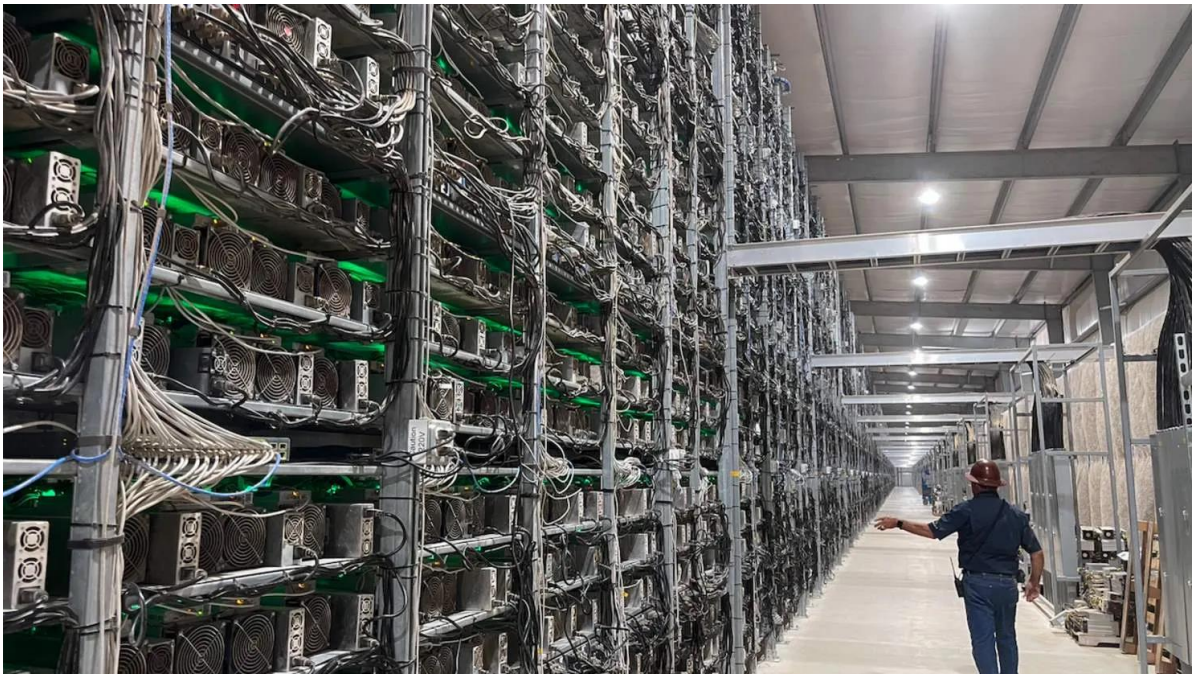
Ο πρώτος τρόπος εξόρυξης στην αρχή πραγματοποιούνταν με την χρήση CPU ή της βασικής μονάδας επεξεργασίας των υπολογιστών. Η χρήση της CPU ήταν αναγκαία καθώς εκείνη εκτελεί όλες τις λειτουργίες ενός προγράμματος. Ήταν ο μόνος τρόπος για να πραγματοποιηθεί η εξόρυξη αλλά δεν ήταν και τόσο αποτελεσματικός. Καθώς η CPU ήταν αργή στη συνέχεια χρησιμοποιήθηκε η GPU των υπολογιστών, ως μια πιο γρήγορη και πιο ισχυρή λύση. Η GPU είναι υπεύθυνη για την διαχείριση γραφικών και πραγματοποιεί τους πολύπλοκους μαθηματικούς μηχανισμούς. Αρκετοί εξορυκτές κατέχουν πολλαπλές μονάδες GPU προσφέροντας έτσι μεγαλύτερη ισχύ και ταχύτητα στην διαδικασία εξόρυξης. Ένας ακόμα τρόπος είναι το field programmable gate array (FPGA), το οποίο είναι ένα προγραμματιζόμενο ολοκληρωμένο κύκλωμα ειδικά σχεδιασμένο για την εξόρυξη. Θεωρείται από πολλούς ως η καλύτερη λύση εξόρυξης μιας και αυξάνει σε μεγάλο βαθμό την ταχύτητα και την αποτελεσματικότητα της εξόρυξης. Καθίσταται μια από τις καλύτερες λύσεις καθώς χρησιμοποιεί λιγότερη ισχύ και μπορεί να λειτουργήσει συνεχόμενα για 24 ώρες την ημέρα. Τελευταίος τρόπος είναι το ASIC ένα τσιπ ενσωματωμένου κυκλώματος ειδικών εφαρμογών σχεδιασμένο ειδικά

για εξόρυξη. Παρουσιάστηκε το 2013 και κάθε χρόνο αναβαθμίζεται περισσότερο, πράγμα που του δίνει την δυνατότητα να ξεπεράσει εύκολα τις προαναφερθείσες επιλογές για την εξόρυξη. (Hoffman, 2020)

Οι τελευταίες δυο επιλογές είναι και οι πιο επικρατούσες μιας και ο πιο σημαντικός παράγοντας είναι η ταχύτητα και η αποτελεσματικότητα, κάτι που οι μέθοδοι με την χρήση CPU και GPU δεν μπορούσαν να ανταπεξέλθουν στον ίδιο βαθμό. Επειδή πολλοί όμως εξορυκτές δεν διαθέτουν τους πόρους για την εξόρυξη με την χρήση των δυο πιο επικρατέστερων μορφών, χρησιμοποιούν GPU και CPU και συμμετέχουν σε μια πισίνα εξόρυξης (mining pool). Πραγματοποιώντας αυτό συνδυάζουν την υπολογιστική τους δύναμη με την δύναμη άλλων χρηστών για να κερδίσουν λίγα χρήματα. Οι λόγοι για να συμμετάσχει κανείς σε μια πισίνα εξόρυξης είναι πολλοί, καθώς η εξόρυξη μεμονωμένα μπορεί αρχικά να προσφέρει μεγαλύτερες ανταμοιβές και κέρδος αλλά χρειάζεται μεγάλη κατανάλωση ενέργειας, πράγμα που απαιτεί μεγάλο κόστος. Με την χρήση μιας πισίνας εξόρυξης το κόστος της ενέργειας για την διαδικασία είναι φυσικά πολύ μικρότερο. Επιπλέον οι μεμονωμένοι εξορύκτες έχουν την δυσκολία εύρεσης αυτών των μπλοκ, καθώς πολλοί χρειάστηκαν χρόνια για να μπορέσουν να τα ανακαλύψουν και να τους αποφέρουν κέρδη. Τέλος με την συμμετοχή σε μια πισίνα εξόρυξης δίνεται η δυνατότητα παροχής και χρήσης ενός εξειδικευμένου λογισμικού εξόρυξης το οποίο μπορεί να εκτελεστεί σε όσους διακομιστές (servers) επιθυμεί ο χρήστης για την επιτάχυνση της διαδικασίας. (Hoffman, 2020)

Μετά την ολοκλήρωση της διαδικασίας εξόρυξης οι εξορυκτές λαμβάνουν ανταμοιβές για την συνεισφορά τους. Υπάρχουν διάφορες κατηγορίες ανταμοιβών που προσφέρονται ανάλογα με την πισίνα εξόρυξης στην οποία συμμετέχουν οι εξορυκτές. Ενδεικτικά θα αναφερθούν οι πιο συνηθισμένες κατηγορίες ανταμοιβών σε πισίνες εξόρυξης. Αρχικά η πρώτη κατηγορία ανταμοιβής είναι η PPS (Pay Per Share) όπου οι εξορυκτές λαμβάνουν άμεσες πληρωμές για κάθε μπλοκ που το σύστημα τους επιλύει. Επιπλέον κατηγορία είναι η PROP η οποία είναι μια αναλογική μέθοδος πληρωμής, καθώς οι ανταμοιβές μοιράζονται σε κάθε ανθρακωρύχο της πισίνας αναλογικά με τον αριθμό των μεριδίων που έχει βρει. Τέλος ο BPM ή Slush Pool είναι ο τύπος πισίνας ο οποίος χωρίζει την ανταμοιβή με βάση το μέρος συμμετοχής, δηλαδή χωρίζει τους εξορυκτές σε εκείνους που συμμετείχαν στο τέλος της διαδικασίας και σε εκείνους που σε συμμετείχαν καθ' όλη την διάρκεια της εξόρυξης, δίνοντας τους διαφορετικά μερίδια ανάλογα με την κατηγορία στην οποία βρίσκονται. (Hoffman, 2020)

Εικόνα 21 Αναπαράσταση εξορυκτή ASIC(Market, A.M. 2024)



Εικόνα 22 Το μεγαλύτερο ορυχείο εξόρυξης Bitcoin στην βόρεια Αμερική (Sigalos, 2021)

6. Συναλλαγές Κρυπτονομισμάτων

6.1 Τρόποι αγοράς και πώλησης Κρυπτονομισμάτων

Το πιο πολύτιμο ψηφιακό περιουσιακό στοιχείο στην σύγχρονη εικονική οικονομία είναι τα κρυπτονομίσματα. Όλο και περισσότερα άτομα πραγματοποιούν συναλλαγές με τα κρυπτονομίσματα με την πάροδο των χρόνων. Πως όμως αγοράζονται και πωλούνται τα ψηφιακά αυτά νομίσματα? Οι βασικοί τρόποι για να αποκτήσει ή να πωλήσει ένας χρήστης κρυπτονομίσματα είναι τέσσερις. Ο πρώτος τρόπος είναι με την μέθοδο χρήστη με χρήστη (p2p), ο δεύτερος είναι με LocalBitcoins, ο τρίτος είναι μέσω αυτόματων μηχανημάτων ανάληψης Κρυπτονομισμάτων και ο τελευταίος πραγματοποιείται μέσω ανταλλακτηρίων Κρυπτονομισμάτων (cryptocurrency exchanges).

Το peer to peer ή P2P είναι ο πιο απλούστερος τρόπος συναλλαγής. Δίνει την δυνατότητα στους χρήστες να αγοράζουν, να εμπορεύονται και να πωλούν κρυπτονομίσματα χωρίς την βοήθεια κάποιου τρίτου μέρους. Έτσι πραγματοποιούνται συναλλαγές μεταξύ δύο χρηστών μέσω λογισμικού. Για να μπορέσει να πραγματοποιηθεί η συναλλαγή πρέπει και οι δύο χρήστες να έχουν συμβατά πορτοφόλια. Το μόνο που απαιτείται είναι να γνωρίζει ο χρήστης κάποιον άλλο χρήστη ο οποίος έχει στο πορτοφόλι του κρυπτονομίσματα τα οποία ο πρώτος θέλει να προμηθευτεί. Με άλλα λόγια το peer to peer είναι ένα δίκτυο όπου κάθε υπολογιστής σε αυτό λειτουργεί ως ένας πελάτης, εκεί μπορούν να πραγματοποιηθούν συναλλαγές μεταξύ χρηστών χωρίς γεωγραφικούς περιορισμούς. Επειδή δεν υπάρχει η ύπαρξη ενός τρίτου μέρους όπως αναφέρθηκε παραπάνω, αυτό έχει ως αποτέλεσμα να μην υπάρχουν κόστη συναλλαγών αλλά ούτε και προμήθειες.

Τα LocalBitcoins είναι ένας αντίστοιχος τρόπος συναλλαγής χρήστη με χρήστη με την διαφορά ότι εδώ δεν καθίσταται γνωστή η ταυτότητα του χρήστη με τον οποίο συναλλάσσεστε . Πρόκειται για μία πλατφόρμα μέσω της οποίας πραγματοποιούνται οι συναλλαγές χωρίς γεωγραφικούς περιορισμούς. Η πλατφόρμα αυτή λειτουργεί ως εγγυητής για την διασφάλιση των συναλλαγών, καθώς σε περίπτωση διαφωνίας ή απάτης η πλατφόρμα επεμβαίνει για να λύσει το όποιο πρόβλημα έχει δημιουργηθεί. Για την λύση του προβλήματος η πλατφόρμα βασίζεται σε ένα σύνολο κανόνων που έχουν τεθεί πριν την έναρξη της εκάστοτε συναλλαγής. Όπως και στον πρώτο τρόπο έτσι και εδώ πρέπει ο κάθε χρήστης να έχει στην διάθεση του συμβατικό πορτοφόλι.

Τα αυτόματα μηχανήματα ανάληψης Κρυπτονομισμάτων γνωστά σε όλους ως και ATM είναι ένα είδος ATM όπως των συμβατικών νομισμάτων (Fiat) αλλά με την διαφορά ότι σε αυτά οι χρήστες αγοράζουν και πωλούν κρυπτονομίσματα με αντάλλαγμα μετρητά χρήματα. Η αγορά των Κρυπτονομισμάτων διατίθεται σε όλα τα ATM ενώ η πώληση περιορίζεται σε ορισμένα. Σε αντίθεση με τα ATM των συμβατικών νομισμάτων (Fiat) τα οποία συνδέονται με τον λογαριασμό του χρήστη που τα χρησιμοποιεί, τα ATM Κρυπτονομισμάτων συνδέονται με το ψηφιακό πορτοφόλι του χρήστη. Για την αγορά ενός κρυπτονομίσματος ο χρήστης καταθέτει τα χρήματα για την αγορά και με την χρήση ενός κωδικού Qr πραγματοποιείται η συναλλαγή και τα νομίσματα μεταφέρονται στο συνδεδεμένο ψηφιακό πορτοφόλι του χρήστη. Στα ATM τα οποία προσφέρουν την ικανότητα πώλησης Κρυπτονομισμάτων η διαδικασία για την πώληση είναι παρόμοια καθώς και εδώ ο χρήστης θα πρέπει να σαρώσει έναν κωδικό Qr του ψηφιακού πορτοφολιού του για να πωλήσει κρυπτονομίσματα από αυτό. Όταν ολοκληρωθεί η διαδικασία ο χρήστης εισπράττει τα χρήματα σε μετρητά ή σε κάρτα. Σε αυτή την μέθοδο όμως υπάρχουν μεγάλα κόστη συναλλαγών, ενώ τα μεγέθη των συναλλαγών σχετικά με τις αναλήψεις και τις καταθέσεις υπάγονται σε περιορισμούς. Συνολικά ανά τον κόσμο υπάρχουν 38246 ATM Κρυπτονομισμάτων τα οποία δραστηριοποιούνται σε 68 χώρες. (Coinatmradar, 2024)

Τελευταίος τρόπος αγοράς και πώλησης των Κρυπτονομισμάτων είναι τα ανταλλακτήρια Κρυπτονομισμάτων (cryptocurrency exchanges). Τα ανταλλακτήρια αυτά είναι ένα είδος ψηφιακών αγορών στις οποίες γίνονται αγοροπωλησίες από χρήστες σε όλο τον κόσμο. Θεωρείται ως ο ασφαλέστερος τρόπος για να αγοράσει ή να πουλήσει κάποιος κρυπτονομίσματα. Χωρίζονται σε δύο κατηγορίες τα κεντροποιημένα (centralized) και τα αποκεντρωποιημένα (decentralized). Τα ανταλλακτήρια αλλά και οι κατηγορίες τους θα αναλυθούν στο επόμενο κεφάλαιο 6.2 .

6.2 Ανταλλακτήρια Κρυπτονομισμάτων

Ένα ανταλλακτήριο Κρυπτονομισμάτων είναι μια ψηφιακή αγορά στην οποία δίνεται η δυνατότητα στους αγοραστές και στους πωλητές να ανταλλάσσουν κρυπτονομίσματα ή άλλα περιουσιακά στοιχεία έναντι συμβατικών νομισμάτων (fiat) ή Κρυπτονομισμάτων. Τα ανταλλακτήρια με άλλα λόγια λειτουργούν ως ένας μεσάζοντας μεταξύ αγοραστών και πωλητών. Τα ανταλλακτήρια λειτουργούν και ως μεσιτεία καθώς δέχονται διάφορες μορφές ηλεκτρονικών πληρωμών με αντάλλαγμα κρυπτονομίσματα. Όταν ένας χρήστης αγοράσει με μια μέθοδο ηλεκτρονικής πληρωμής ένα ποσό Κρυπτονομισμάτων, το ανταλλακτήριο έχει την δυνατότητα να στείλει αυτά τα αγορασμένα κρυπτονομίσματα στο πορτοφόλι του. Για την πραγματοποίηση συναλλαγών το ανταλλακτήριο επιβάλλει ένα τέλος συναλλαγής. Υπάρχουν δύο είδη ανταλλακτηρίων, τα κεντροποιημένα (centralized) και τα αποκεντρωποιημένα (decentralized). (CoinMarketCap, 2024)

Τα περισσότερα ανταλλακτήρια στην αγορά των Κρυπτονομισμάτων είναι κεντροποιημένα. Αυτά τα ανταλλακτήρια έχουν νομική/εταιρική υπόσταση και υπόκεινται σε κάποια ρυθμιστικά πλαίσια ανάλογα με την χώρα στην οποία εδρεύουν. Τα ανταλλακτήρια αυτά δρουν ως μεσάζοντας ανάμεσα σε αγοραστές και πωλητές. Ο κάθε χρήστης δεν χρειάζεται να έχει δημιουργήσει από πριν την εγγραφή του κάποιο πορτοφόλι, μιας και τα ανταλλακτήρια του προσφέρουν κατά την εγγραφή του. Ωστόσο όμως τα κλειδιά του κάθε πορτοφολιού που προσφέρονται δεν ανήκουν στους χρήστες. Πέραν από την παροχή πορτοφολιού στου χρήστες τα ανταλλακτήρια αυτά προσφέρουν διάφορες επιπλέον παροχές όπως δανεισμός κεφαλαίων, staking rewards, ενώ υπάρχει και η δυνατότητα μόχλευσης κεφαλαίων. Σε αντίθεση με τα αποκεντρωποιημένα, τα κεντροποιημένα προσφέρουν την δυνατότητα κατάθεσης, ανάληψης και συναλλαγής με συμβατικά νομίσματα, κάτι που στα αποκεντρωποιημένα καθίσταται αδύνατο. Ενώ ως θετικό τους είναι η μεγάλη ρευστότητα που κατέχουν, το κόστος μεταφοράς κεφαλαίων παραμένει υψηλό. (DeVito, 2021)

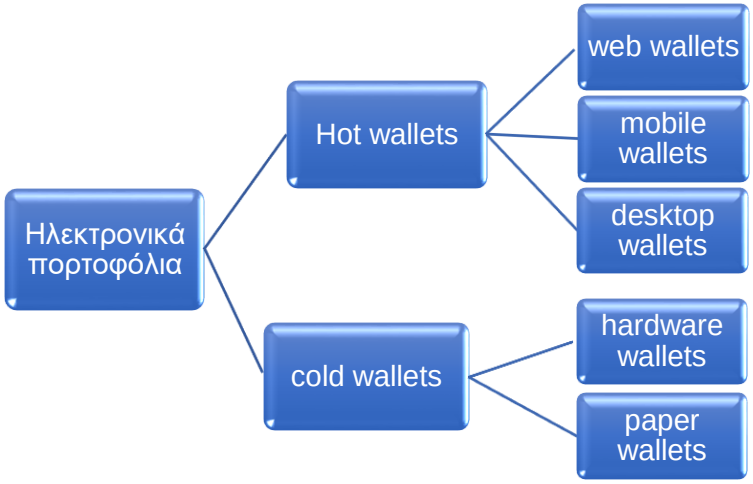
Τα ανταλλακτήρια αυτά ενέχουν υψηλό κίνδυνο. Μπορεί να είναι πολύ εύχρηστα για τους χρήστες και για αυτό να πραγματοποιούνται εκατομμύρια συναλλαγές καθημερινά, όμως επειδή πολλά ανταλλακτήρια κρατούν αξία εκατομμυρίων γίνονται εύκολος στόχος από χάκερ. Για αυτόν ακριβώς τον λόγο η επιλογή του εκάστοτε ανταλλακτηρίου πρέπει να γίνεται με γνώμονα την ασφάλεια του λογισμικού που κατέχει. Ενδεικτικά τα πιο μεγάλα κεντροποιημένα ανταλλακτήρια Κρυπτονομισμάτων ανά τον κόσμο είναι η Coinbase, η Binance, το Bitstamp, το Kraken.

Σε αντίθεση με τα κεντροποιημένα ανταλλακτήρια τα αποκεντρωποιημένα δεν ανήκουν σε κάποια εταιρεία, άρα δεν υφίστανται εταιρική υπόσταση και για αυτό το λόγο δεν υπόκεινται σε κάποιο κανονιστικό πλαίσιο. Είναι δομημένα και λειτουργούν σε ένα δίκτυο blockchain το οποίο τους επιτρέπει την δημιουργία αποκεντρωμένων εφαρμογών. Μέσω αυτών των εφαρμογών φέρνουν σε επαφή τους αγοραστές με τους πωλητές. Τα στοιχεία των αγοραστών και των πωλητών δεν γίνονται γνωστά. Όπως αναφέρθηκε προηγουμένως, δεν υπάρχει δυνατότητα κατάθεσης, ανάληψης ή συναλλαγής με συμβατικά νομίσματα (fiat). Σε αντίθεση με τα κεντροποιημένα ανταλλακτήρια όπου εκεί οι χρήστες δεν χρειάζεται να έχουν κάποιο πορτοφόλι μιας και τους το παρέχει το ανταλλακτήριο, στα αποκεντρωποιημένα δεν συμβαίνει κάτι τέτοιο και ο χρήστης πρέπει να έχει ήδη δημιουργήσει το δικό του ηλεκτρονικό πορτοφόλι το οποίο και να είναι συμβατό με το δίκτυο blockchain που λειτουργεί το ανταλλακτήριο. Κάθε συναλλαγή που πραγματοποιείται καταγράφεται στο δίκτυο του blockchain. Ο κίνδυνος σε σχέση με τα κεντροποιημένα ανταλλακτήρια είναι σαφώς μειωμένος, καθώς οι συναλλαγές που πραγματοποιούνται γίνονται απευθείας μεταξύ των χρηστών και δεν υπάρχει η ανάγκη να μοιραστούν οι πληροφορίες σε κάποιον τρίτο και έτσι κάποιος χρήστης να γίνει εύκολος στόχος από χάκερ. Επειδή ακριβώς δεν ζητούνται προσωπικά δεδομένα, αυτό έχει ως αποτέλεσμα να υπάρχει μεγάλη ασφάλεια της ιδιωτικότητας του λογαριασμού αλλά και των συναλλαγών. Ο προσδιορισμός του κόστους των συναλλαγών, δηλαδή κατά πόσο υπάρχουν μεγάλα κόστη συναλλαγών ή μικρά, δεν μπορεί να κυμανθεί καθώς εξαρτάται από το εκάστοτε δίκτυο blockchain. Τα μεγαλύτερα αποκεντρωποιημένα ανταλλακτήρια Κρυπτονομισμάτων σε όλο τον κόσμο είναι το Uniswap, το Sushiswap, το Curve, το Loorping και το Kyber. (DeVito, 2021)

6.3 Τρόποι αποθήκευσης Κρυπτονομισμάτων

Παρόλο που τα κρυπτονομίσματα κατέχουν μόνο ψηφιακή μορφή πρέπει να αποθηκεύονται σε ένα ασφαλές μέρος, όπως και στην περίπτωση των συμβατικών νομισμάτων τα οποία αποθηκεύονται από τους ιδιοκτήτες τους σε ένα πορτοφόλι ή σε μια θυρίδα ή σε έναν λογαριασμό σε μια τράπεζα. Με τον ίδιο τρόπο και στον τομέα των Κρυπτονομισμάτων οι χρήστες μπορούν να αποθηκεύσουν τα κρυπτονομίσματα που κατέχουν σε όποιο είδος πορτοφολιού αυτοί επιλέξουν. Τα είδη πορτοφολιών διαφέρουν καθώς έχουν και διαφορετικά χαρακτηριστικά μεταξύ τους. Οι χρήστες καλούνται να επιλέξουν ποιο από αυτά τα πορτοφόλια κατέχει τα χαρακτηριστικά που τους ταιριάζουν περισσότερο. Κάθε κρυπτονόμισμα υποστηρίζεται από τουλάχιστον ένα ή περισσότερα ηλεκτρονικά πορτοφόλια.

Τα ηλεκτρονικά αυτά πορτοφόλια χωρίζονται σε δύο κατηγορίες: τα Hot και τα cold πορτοφόλια. Εκείνα με την σειρά τους χωρίζονται σε υποκατηγορίες με τα Hot wallets να έχουν τις εξής: τα Web, τα desktop και τα Mobile. Ενώ τα cold wallets χωρίζονται στα hardware και στα Paper.



Εικόνα 23 Κατηγορίες Ηλεκτρονικών πορτοφολιών

Τα ηλεκτρονικά πορτοφόλια έχουν δύο μέρη, το ιδιωτικό και το δημόσιο κλειδί. Το δημόσιο κλειδί είναι απαραίτητο για την δημιουργία μιας δημόσιας διεύθυνσης, η οποία είναι ορατή σε όλους στο δίκτυο και είναι απαραίτητη για την αποστολή χρημάτων. Το δεύτερο μέλος είναι το ιδιωτικό κλειδί, το οποίο είναι μια ιδιωτική διεύθυνση, η οποία προστατεύεται με κωδικό πρόσβασης και είναι γνωστή μόνο από τον ίδιο τον χρήστη. Είναι το πιο σημαντικό μέλος καθώς είναι αναγκαίο για την πρόσβαση και για τον έλεγχο ενός πορτοφολιού. Το ιδιωτικό κλειδί μπορεί να χρησιμοποιηθεί και για την ανάκτηση του

πορτοφολιού. Επιπλέον χρησιμοποιείται για την μεταφορά χρημάτων σε έναν άλλο πορτοφόλι που μπορεί να κατέχει ο ίδιος χρήστης. Η γνώση του ιδιωτικού κλειδιού πρέπει να μην αποκαλύπτεται σε τρίτους καθώς κάποιος με την χρήση αυτού μπορεί να εισέλθει στο πορτοφόλι και να αποσπάσει χρήματα. (Hoffman, 2020)

Τα Hot wallets ονομάζονται και software wallets, αυτά τα πορτοφόλια είναι άμεσα συνδεδεμένα με το διαδίκτυο και τα κλειδιά αυτών δημιουργούνται και αποθηκεύονται σε αυτά. Είναι τα πιο εύκολα πορτοφόλια για χρήση από νέους χρήστες καθώς είναι ο πιο γρήγορος και εύκολος τρόπος να πραγματοποιηθεί μια συναλλαγή. Συνιστάται στους χρήστες να μην τοποθετούν όλα τα νομίσματα που κατέχουν στο διαδικτυακό τους πορτοφόλι. Αυτό προκύπτει καθώς αυτά είναι ένας πολύ δελεαστικός στόχος των χάκερ, οι οποίοι στοχεύουν να παρακάμψουν την ασφάλεια τους και να αποσπάσουν μερίδιο ή ακόμα και όλο το ποσό των νομισμάτων που εμπεριέχονται. Ένας τρόπος που πραγματοποιείται αυτό είναι με το Phishing, ένα κακόβουλο λογισμικό πειρατείας. Τα περισσότερα κρυπτονομίσματα προσφέρουν όλους του τύπους των Hot wallet, οι οποίοι αναλύονται στην συνέχεια. (Hoffman, 2020)

Τα web wallets ή όπως ονομάζονται αλλιώς πορτοφόλια Ιστού, λειτουργούν μέσω μιας αλληλεπίδρασης με κάποιο πρόγραμμα περιήγησης (browser), επιτρέποντας στους χρήστες τους να έχουν πρόσβαση στα κρυπτονομίσματα τους στο διαδίκτυο. Ο χρήστης με αυτόν τον τρόπο δεν χρειάζεται να κατεβάσει ή να εγκαταστήσει κάποια εφαρμογή. Η χρήση αυτών γίνεται κατά κύριο λόγο σε αποκεντρωμένα ανταλλακτήρια. Οι χρήστες πρέπει να είναι πολύ προσεκτικοί όταν συνδέουν τα πορτοφόλια τους σε πλατφόρμες, καθώς η αλληλεπίδραση με κακόβουλους ιστότοπους μπορεί να θέσει την ασφάλεια του πορτοφολιού τους σε κίνδυνο. (Hoffman, 2020)

Τα mobile wallets ή όπως αλλιώς ονομάζονται πορτοφόλια για κινητά, είναι απλά μια εφαρμογή στο κινητό. Καθίστανται εξαιρετικά για άτομα τα οποία βρίσκονται συνεχώς εν κινήσει. Το μόνο που απαιτείται είναι η πρόσβαση στο διαδίκτυο για το «κατέβασμα» (download) της εφαρμογής και την εγκατάσταση της. Είναι βολικότερα στην χρήση καθώς το βασικό τους πλεονέκτημα είναι η φορητότητα. Ακόμα βοηθούν στην πιο γρήγορη και πιο άμεση πραγματοποίηση των συναλλαγών με την χρήση Qr code. Σε αυτά μπορεί να δημιουργηθεί ένα Qr code και στην συνέχεια να σαρωθεί, κάνοντας έτσι την συναλλαγή πιο γρήγορη και πιο άμεση. Καθίστανται πιο ασφαλή από τα web wallet αλλά λιγότερο από τα desktop τα οποία θα αναλυθούν στην συνέχεια. Αυτό προκύπτει καθώς το κινητό τηλέφωνο είναι λιγότερο ασφαλές σε σχέση με τον υπολογιστή, μιας και τα τηλέφωνα μπορούν να παραβιαστούν πιο εύκολα με την χρήση κακόβουλου λογισμικού, όπως αυτό του keylogger ή ακόμα και από ιούς από το διαδίκτυο. Τέλος σε περίπτωση απώλειας

της συσκευής εάν δεν έχει πραγματοποιηθεί κάποιο Back-up για να μπορέσουν να σωθούν τα δεδομένα, αυτό μπορεί να οδηγήσει και στην απώλεια των κεφαλαίων. (Hoffman, 2020)

Τα desktop wallets ή αλλιώς επιτραπέζια πορτοφόλια θεωρούνται ότι είναι ένας από τους ασφαλέστερους τύπους πορτοφολιών. Για να λειτουργήσουν το μόνο που απαιτείται είναι να «κατεβάσει» (download) ο χρήστης ένα λογισμικό ή μια εφαρμογή και απλώς να την εγκαταστήσει. Θεωρούνται από τα πιο ασφαλή καθώς παρέχουν στον χρήστη την ικανότητα να αποθηκεύσει τα κλειδιά του στον υπολογιστή του, εμποδίζοντας έτσι τους χάκερ να τα υποκλέψουν. Όμως αν ο υπολογιστής δεν χρησιμοποιεί τα κατάλληλα μέσα ασφαλείας, μπορεί να είναι εκτεθειμένος και έτσι να παραβιαστεί το πορτοφόλι του χρήστη. Η παραβίαση του υπολογιστή μπορεί να οφείλεται σε ιούς malware ή viruses. Για αυτόν ακριβώς τον λόγο θα πρέπει οι χρήστες να δημιουργούν αντίγραφα ασφαλείας στον υπολογιστή τους. (Hoffman, 2020)

Τα cold wallets θεωρούνται ως ο ασφαλέστερος τύπος ηλεκτρονικών πορτοφολιών. Αυτό προκύπτει επειδή χρησιμοποιούν μια μέθοδο που ονομάζεται «cold storage». Αυτή περιλαμβάνει την δημιουργία αλλά και την αποθήκευση των ιδιωτικών κλειδιών του χρήστη εκτός διαδικτύου μέσω μιας ασφαλούς διαδικασίας. Για αυτόν το λόγο και ονομάζονται επίσης ως cold storage wallets ή και offline wallets. Η αποθήκευση των κλειδιών εκτός διαδικτύου μετριάζει τον κίνδυνο απώλειας κεφαλαίων σε περίπτωση χακαρίσματος. Έτσι οι χρήστες κατέχουν τον απόλυτο έλεγχο των ιδιωτικών τους κλειδιών. (Hoffman, 2020)

Hardware wallets ή όπως αλλιώς ονομάζονται πορτοφόλια υλικών δεν είναι τόσο εύκολα στην χρήση όσο άλλα πορτοφόλια. Σε αυτόν τον τύπο πορτοφολιού τα νομίσματα αποθηκεύονται εκτός σύνδεσης διαδικτύου. Είναι αρκετά ασφαλή καθώς διατρέχουν κίνδυνο μόνο όταν συνδέονται με το διαδίκτυο. Τα πορτοφόλια αυτά έχουν δύο μέρη, το πρώτο είναι εκείνο που συνδέεται με το διαδίκτυο, και εκείνο που λειτουργεί χωρίς αυτό. Στο πρώτο μέλος το δημόσιο κλειδί εκτελεί τις ίδιες λειτουργίες όπως σε όλα τα άλλα πορτοφόλια. Σε αυτό το μέλος δεν υπάρχει πρόσβαση στο ιδιωτικό κλειδί επομένως δεν υπάρχει πρόσβαση σε συναλλαγές. Όταν θέλουν οι χρήστες να πραγματοποιήσουν μια συναλλαγή συνδέονται εκτός διαδικτύου μέσω μιας συσκευής usb ή σαρώνουν έναν κωδικό Qr για εξουσιοδότηση και για να ολοκληρωθεί η συναλλαγή. Αν και θεωρείται η πιο ασφαλής επιλογή έχει κάποια τρωτά σημεία όπως ότι δεν υποστηρίζεται από όλα τα κρυπτονομίσματα, αν και με τον καιρό όλο και περισσότερα εντάσσονται. Επιπλέον υπάρχει τρόπος παραβίασης στο software. Τέλος σε περίπτωση απώλειας της συσκευής

θα πρέπει να έχει γίνει το ανάλογο back-up, ειδάλλως τα κεφάλαια θα καταστούν μη ανακτήσιμα. (Hoffman, 2020)

Τα Paper wallets ή αλλιώς χάρτινα πορτοφόλια είναι ένας πολύ αξιόλογος τρόπος διαχείρισης των Κρυπτονομισμάτων με ασφάλεια. Όπως και τα Hardware wallets τα paper wallets αποθηκεύουν τα ψηφιακά νομίσματα εκτός σύνδεσης. Σε αυτά τα πορτοφόλια δίνεται η δυνατότητα εκτύπωσης των ιδιωτικών κλειδιών αλλά και της διεύθυνσης σε φυσικό χαρτί. Κανένα από τα κλειδιά του χρήστη δεν εισάγεται στον υπολογιστή μέχρι να είναι εκείνος έτοιμος να τα χρησιμοποιήσει. Επιπλέον τα κλειδιά δεν αποθηκεύονται σε τρίτο διακομιστή (third party server). Το μεγάλο μειονέκτημα αυτού του είδος πορτοφολιού είναι πως αν απολεσθεί το χαρτί στο οποίο έχουν εκτυπωθεί τα κλειδιά, τα κεφάλαια δεν μπορούν ποτέ να ανακτηθούν. Θεωρείται ένας ξεπερασμένος τύπος πορτοφολιού και για αυτόν τον λόγο όλο και λιγότεροι χρήστες τον χρησιμοποιούν με την πάροδο των χρόνων. (Hoffman, 2020)

7. Επίλογος

Η αγορά Κρυπτονομισμάτων παρόλο που βρίσκεται ακόμη στα αρχικά της στάδια, έχει υποστεί αξιοσημείωτες μεταμορφώσεις από την έναρξή της. Τα κρυπτονομίσματα, μέχρι πρότινος θεωρούνταν ως μια εξειδικευμένη ιδέα, ενώ τώρα κατέχουν μια σημαντική θέση στις παγκόσμιες χρηματοπιστωτικές αγορές, καθώς έχουν αποδείξει την ανθεκτικότητα και την καινοτομία τους. Αυτή η διατριβή έχει διερευνήσει την άνοδο της αγοράς των Κρυπτονομισμάτων, εστιάζοντας στη δημιουργία, τα χαρακτηριστικά και τους διάφορους παράγοντες που συμβάλλουν στην επιτυχία ή την αποτυχία τους. Από την κυριαρχία του Bitcoin μέχρι την αυξανόμενη επιρροή των εναλλακτικών νομισμάτων (altcoins) αλλά και την δημιουργία αποκεντρωμένων εφαρμογών (DApps), οι οποίες καταδεικνύουν τις διαφορετικές δυνατότητες των ψηφιακών περιουσιακών στοιχείων. Ιδιαίτερο ενδιαφέρον παρουσιάζει ο τρόπος λειτουργίας και τα χαρακτηριστικά της τεχνολογίας Blockchain αλλά και οι εφαρμογές της πέραν από την αγορά των Κρυπτονομισμάτων. Επιπλέον ένας βασικός παράγοντας για την ανάπτυξη των Κρυπτονομισμάτων είναι η αποκεντρωμένη τους φύση, η οποία δίνει την δυνατότητα για συναλλαγές Peer-to-Peer χωρίς μεσάζοντες. Ωστόσο, το μέλλον των Κρυπτονομισμάτων δεν είναι χωρίς προκλήσεις. Η έλλειψη ρυθμιστικού πλαισίου, τα ζητήματα ασφάλειας και η αστάθεια των τιμών τους εξακολουθούν να θέτουν κινδύνους για τους επενδυτές και το ευρύτερο χρηματοπιστωτικό σύστημα. Όμως παρά τους κινδύνους, η αγορά έχει μεγάλες δυνατότητες για την αναμόρφωση των παγκόσμιων οικονομικών, μπορεί λόγω της έλλειψης του ρυθμιστικού πλαισίου αλλά και της μεγάλης μεταβλητότητας των τιμών τους, να μην θεωρείται πιθανό στο μέλλον να αντικαταστήσουν τα συμβατικά νομίσματα Fiat, όμως είναι και θα είναι μια πολύ καλή εναλλακτική λύση στα παραδοσιακά επενδυτικά περιουσιακά στοιχεία.

8. Βιβλιογραφία

Φίλιππας, Ν. 2016. Το Bitcoin ως το νόμισμα της νέας εποχής [WWW Document]. Ινστιτούτο Χρηματοοικονομικού Αλφαβητισμού. URL https://www.gfli.gr/to-bitcoin-os-to-nomisma-tis-neas-epochis/ (accessed 9.14.24).

Aracely, 2020. What is Bitcoin forking – horux, 2020. URL https://horux.cz/what-is-bitcoin-forking/ (accessed 9.14.24).

Aran, A, & Pallavi, R, 2023. Charting the Number of Failed Crypto Coins, by Year (2013-2022) [WWW Document]. Visual Capitalist. URL https://www.visualcapitalist.com/cp/ranked-dead-crypto-coins-by-year/ (accessed 9.14.24).

Bashir, I. 2023. Mastering Blockchain - Fourth Edition: Inner workings of blockchain, from cryptography and decentralized identities, to DeFi, NFTs and Web3 4th ed. Edition. Birmingham: Packt Publishing

Bhaisora, s, s. 2024. The Lindy Effect: Can a Company’s Age Predict Its Stock Market Performance? | Wright Blogs [WWW Document], n.d. URL https://www.wrightresearch.in/blog/the-lindy-effect-can-a-companys-age-predict-its-stock-market-performance/ (accessed 9.14.24).

Bitcoin halving. 2024. Next Bitcoin Halving: Countdown to Block 840,000 [WWW Document], n.d. URL https://www.bitcoinhalving.com/ (accessed 9.15.24).

Bitcoin Magazine. 2024. Bitcoin Hashrate | BM Pro [WWW Document], n.d.. Bitcoin Magazine Pro. URL https://www.bitcoinmagazinepro.com/charts/bitcoin-hashrate-chart/ (accessed 9.14.24).

Blockchains101, 2018. The Blockchain CIO- Ultimate Blockchain Executive’s Guide [WWW Document]. 101 Blockchains. URL https://101blockchains.com/blockchain-cio-executives-guide/ (accessed 9.14.24).

Blockchain. 2024. Blockchain.com | Charts - Total Hash Rate (TH/s) [WWW Document], n.d. URL https://www.blockchain.com/explorer/charts/[id] (accessed 9.14.24).

Burniske, C, & Tatar, J. 2017. Cryptoassets: The Innovative Investor's Guide to Bitcoin and Beyond, New York: McGraw Hill

Cakebread, S, 2020. The IPO Playbook: An Insider's Perspective on Taking Your Company Public and How to Do It Right, California: Silicon Valley Press

Clayton, J. 2017. SEC.gov | Statement on Cryptocurrencies and Initial Coin Offerings [WWW Document], n.d. URL https://www.sec.gov/newsroom/speeches-statements/statement-clayton-2017-12-11 (accessed 9.14.24).

Coinatmradar.2024. Bitcoin ATM Map – Find Bitcoin ATM, Online Rates [WWW Document], n.d. URL https://coinatmradar.com/ (accessed 9.14.24).

Coinbase. 2024. What are Initial Coin Offerings (ICOs) and how do they work? [WWW Document], n.d. URL https://www.coinbase.com/learn/tips-and-tutorials/what-are-initial-coin-offerings-and-how-do-they-work (accessed 9.14.24).

Coinbase.2024 What is a stablecoin? [WWW Document], n.d. URL https://www.coinbase.com/learn/crypto-basics/what-is-a-stablecoin (accessed 9.14.24).

CoinMarketCap. 2024. Cryptocurrency Prices, Charts And Market Capitalizations [WWW Document], n.d. . CoinMarketCap. URL https://coinmarketcap.com/ (accessed 9.15.24).

CoinMarketCap. 2024. Exchange Definition | CoinMarketCap [WWW Document], n.d.. CoinMarketCap Academy. URL https://coinmarketcap.com/academy/glossary/exchange (accessed 9.14.24).

DeVito, W, R. 2021.Cryptocurrency for Beginners: Ultimate Guide for Trading & Investing Bitcoin and Other Top Altcoins. Independent publisher

Ding, Q., Liebau, D., Wang, Z., Xu, W., 2023. A Survey on Decentralized Autonomous Organizations (DAOs) and Their Governance. https://doi.org/10.2139/ssrn.4378966

Egunjobi, O.O., Gomes, A., Egwim, C.N., Morais, H., 2024. A systematic review of blockchain for energy applications. e-Prime - Advances in Electrical Engineering, Electronics and Energy 9, 100751. https://doi.org/10.1016/j.prime.2024.100751

Ejeke, P. 2022. Smart Contracts: What Is A Smart Contract? Complete Guide To Tech And Code That Is About To Transform The Economy-Blockchain, Web3.0, DApps, DAOs, DEFI, Crypto, IoTs, FinTech, Digital Assets Trading. Independent publisher

Ether. 2024. What is ether (ETH)? [WWW Document], n.d. . ethereum.org. URL https://ethereum.org/en/eth/ (accessed 9.14.24).

Ethereum. 2024. What is Ethereum? [WWW Document], n.d. . ethereum.org. URL https://ethereum.org/en/what-is-ethereum/ (accessed 9.14.24).

GoogleTrends. 2024.GoogleTrends[WWWDocument],n.d.URL https://trends.google.gr/trends/explore?date=2008-01-01%202024-09-04&q=bitcoin,cryptocurrency&hl=el (accessed 9.14.24).

Hale, V. 2018. Launch an ICO & Token Crowdsale: The Complete Guide to Prepare your Startup for Launching Successful Initial Coin Offering, raising Venture & Cryptocurrency Capital. Independent publisher

Hoffman, N. 2020. Cryptocurrency: The Ultimate Guide to The World of Cryptocurrency and How I Became a Crypto Millionaire in 6 Months. New Delhi: Tenzy Publisher

Hyatt, C.J, 2021. What is Cryptocurrency & How Does it Work? [WWW Document]. URL https://www.nasdaq.com/articles/news-and-insights/what-is-cryptocurrency-and-how-it-works (accessed 9.14.24).

Lewis, A. 2018. The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them, Miami: Mango publishing

Maddrey, N., 2018. Blockchain Forks Explained. Digital Asset Research. URL https://medium.com/digitalassetresearch/blockchain-forks-explained-8ccf304b97c8 (accessed 9.14.24).

Makerdao. 2024. The Maker Protocol White Paper | Feb 2020 [WWW Document], n.d. URLhttps://makerdao.com/en/whitepaper/https://makerdao.com/en (accessed 9.14.24).

Market, A.M., 2024. Unveiling the Future of Cryptocurrency Mining: The Revolutionary ASIC Miner. Medium. URL https://medium.com/@Asic-Miners/unveiling-the-future-of-cryptocurrency-mining-the-revolutionary-asic-miner-78631f4a7686 (accessed 9.14.24).

McKinsey&Company. 2024. What is blockchain technology? | McKinsey [WWW Document], n.d. URL https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-blockchain#/ (accessed 9.14.24).

Monero. 2024. FAQ [WWW Document], n.d. . getmonero.org, The Monero Project. URL https://www.getmonero.org/get-started/faq/index.html (accessed 9.14.24).

Nakamoto, S., n.d. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System.

Namecoin.2024. Namecoin [WWW Document], n.d. URL https://www.namecoin.org/ (accessed 9.14.24).

Narayanan, A., Bonneau, J., Felten, E., Miller, A., Goldfeder, S. 2016. Bitcoin and Cryptocurrency Technologies | Princeton University Press [WWW Document], n.d. URL

https://press.princeton.edu/books/hardcover/9780691171692/bitcoin-and-cryptocurrency-technologies (accessed 9.15.24).

Paybis. 2024. What is Bitcoin Dominance and How to Use it to Your Advantage? [WWW Document], n.d.. Paybis Blog. URL https://paybis.com/blog/glossary/what-is-bitcoin-dominance/ (accessed 9.14.24).

POL Token. 2024. POL Token | Powering the Polygon experience [WWW Document], n.d. URL https://polygon.technology/pol-token (accessed 9.14.24).

Polymath.2024. Polymath, n.d. Why Polymesh: Why We Built a New, Fit-For-Purpose Blockchain [WWW Document]. URL https://info.polymath.network/blog/why-we-built-a-new-fit-for-purpose-blockchain (accessed 9.14.24).

SAP.2024. Blockchain: The New Technology for Trust [WWW Document], n.d..SAP. URLhttps://www.sap.com/products/artificial-intelligence/what-is-blockchain.html (accessed 9.14.24).

Sergeenkov, A., 2021. What Is Cryptocurrency? [WWW Document]. URL https://www.coindesk.com/learn/what-is-cryptocurrency/ (accessed 9.14.24).

Sharma, T.K., 2020. IPOs vs. ICOs vs. STOs: Major Differences | Blockchain Council. URL https://www.blockchain-council.org/blockchain/ipos-vs-icos-vs-stos-major-differences/ (accessed 9.14.24).

Sharma, T.K., 2024. Security Tokens vs. Utility Tokens: A Concise Guide. URL https://www.blockchain-council.org/blockchain/security-tokens-vs-utility-tokens-guide/ (accessed 9.14.24).

Sigalos, M., 2021. Bitcoin mining has totally recovered from Chinese ban [WWW Document]. CNBC. URL https://www.cnbc.com/2021/12/10/bitcoin-network-hashrate-hits-all-time-high-after-china-crypto-ban.html (accessed 9.14.24).

Tether.2024. Why use Tether? [WWW Document], n.d. URL https://tether.to/en/why-tether (accessed 9.14.24).

The New York Times. 2013. An Abridged History of Bitcoin [WWW Document], n.d. URL https://www.nytimes.com/interactive/technology/bitcoin-timeline.html (accessed 9.14.24).

Verma, R., Dhanda, N., 2023. Chapter 5 - Blockchain types: A characteristic view, in: Pandey, R., Goundar, S., Fatima, S. (Eds.), Distributed Computing to Blockchain. Academic Press, pp. 69–85. https://doi.org/10.1016/B978-0-323-96146-2.00013-9

Vermaak, W, 2021. What Are Privacy Coins? | CoinMarketCap [WWW Document], n.d. CoinMarketCap Academy. URL https://coinmarketcap.com/academy/article/what-are-privacy-coins (accessed 9.14.24).

Vigna, P, & Casey, M. 2015. The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order, New York: St. Martin's Press

Vzhuk, 2022. Popular blockchain use cases across industries [WWW Document]. URL https://online.stanford.edu/popular-blockchain-use-cases-across-industries (accessed 9.14.24).

Yaga, Dylan, et al. 2019. Blockchain technology overview. arXiv preprint arXiv:1906.11078