

**ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΑ ΚΑΙ BITCOIN: ΤΡΟΠΟΣ ΛΕΙΤΟΥΡΓΙΑΣ,
ΕΞΕΛΙΞΗ, ΠΡΟΒΛΗΜΑΤΙΣΜΟΙ ΚΑΙ ΧΡΗΣΗ ΤΗΣ ΑΝΑΛΥΤΙΚΗΣ ΤΩΝ
ΔΕΔΟΜΕΝΩΝ ΓΙΑ ΠΡΟΒΛΕΨΕΙΣ ΤΙΜΩΝ**

Πίνακας περιεχομένων

ΕΙΣΑΓΩΓΗ	4
ΚΕΦΑΛΑΙΟ 1 Η ΕΝΝΟΙΑ ΤΟΥ FINTECH ΚΑΙ Η ΕΜΦΑΝΙΣΗ ΤΩΝ ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΩΝ (CRYPTOCURRENCIES)	5
1.1. FinTech έννοια και περιεχόμενο	5
1.2. Ιστορική εξέλιξη εμφάνισης κρυπτονομισμάτων	9
1.3. Η φύση του χρήματος γενικά	16
1.4. Ο ρόλος των κρυπτονομισμάτων στην παγκόσμια οικονομία	21
1.5. Blockchain	25
ΚΕΦΑΛΑΙΟ 2 ΤΟ BITCOIN ΩΣ ΕΠΕΝΔΥΣΗ	28
2.1. Από τις εφαρμογές εικονικού χρήματος στο Bitcoin	28
2.2. Η εκκίνηση του Bitcoin	31
2.4. Η φούσκα του Bitcoin το 2017	35
2.5. Το Bitcoin στην περίοδο της πανδημίας	39
ΚΕΦΑΛΑΙΟ 4 ΕΥΚΑΙΡΙΕΣ ΠΡΟΒΛΗΜΑΤΙΣΜΟΙ ΚΑΙ ΠΡΟΚΛΗΣΕΙΣ	44
4.1. Ευκαιρίες και Πλεονεκτήματα	44
4.1.1. Ασφαλής Τεχνολογία	44
4.1.2. Κόστος Συναλλαγής	47
4.1.3. Υψηλή απόδοση	49
4.2. Προκλήσεις	50
4.2.1. Θεσμικό πλαίσιο	51
4.2.2. Κόστος κατανάλωσης ηλεκτρικής ενέργειας	52
4.2.3. Crash and Bubble	54
4.2.4. Διαδικτυακές επιθέσεις	55
ΚΕΦΑΛΑΙΟ 5 ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΑ ΚΑΙ ΜΕΓΑΛΑ ΔΕΔΟΜΕΝΑ	57
5.1. Η διαδικασία Εξόρυξης Δεδομένων (mining) και εργαλεία εξόρυξης δεδομένων ..	57
5.2. Αλγόριθμοι hash και τεχνικές κατακερματισμού hashing	60

5.3. Πρόβλεψη αξίας του Bitcoin μέσω Μοντελοποίησης	63
5.4. Μέθοδοι πρόβλεψης τιμής Bitcoin.....	64
5.4.1. Το Μοντέλο Bitcoin Stock-to-Flow.....	65
5.4.2. Το μοντέλο Bitcoin Rainbow	68
5.4.3. Το Μοντέλο Puell Multiple.....	70
5.4.4. Το Μοντέλο Mayer Multiple	72
5.4.5. Bitcoin Reserve Risk	73
5.4.6. Relative Unrealized Profit/Loss	75
5.4.7. RHODL Ratio	77
5.4.8. MVRV Z-Score	79
5.4.9. Funding Rates.....	81
5.4.10. Fear & Greed Index	82
5.4.11. Μοντέλα πρόβλεψης τιμών μέσω των κινήσεων των Μεγάλων Επενδυτών ..	83
ΣΥΜΠΕΡΑΣΜΑΤΑ – ΕΠΙΛΟΓΟΣ.....	86
Βιβλιογραφικές αναφορές.....	88

ΕΙΣΑΓΩΓΗ

Το Bitcoin ένα αποκεντρωμένο άυλο ψηφιακό νόμισμα, χωρίς πληθωρισμό το οποίο δεν απαιτεί μία κεντρική τράπεζα για την έκδοσή του. Οι συναλλαγές Bitcoin, παίρνουν τη μορφή ψηφιακών μεταφορών ανάμεσα στους χρήστες του δικτύου bitcoin, χωρίς την ανάγκη ενδιάμεσου. Το Bitcoin είναι ένα τρέχον δημοφιλές κρυπτονόμισμα με ένα πολλά υποσχόμενο μέλλον. Το Bitcoin σχεδιάστηκε ως αποπληθωριστικό σύστημα, κάτι που θα μπορούσε να το βοηθήσει να φτάνει σε συνεχώς αυξανόμενη τιμή. Ωστόσο, με δεδομένη την θεαματική του άνοδο και καθώς διανύει την δεύτερη δεκαετία της εξέλιξής του, υπάρχει ανάγκη για τους επενδυτές να έχουν στη διάθεσή τους μοντέλα για την πρόβλεψη της τιμής του Bitcoin, ώστε με βάση αυτές τις προβλέψεις να προβούν κατά περίπτωση στις ανάλογες κινήσεις εκ μέρους τους. Στο πλαίσιο της παρούσας εργασίας θα αναλυθεί το θέμα των κρυπτονομισμάτων και ειδικότερα του Bitcoin. Μεταξύ άλλων θα αναλυθεί η ιστορική του εξέλιξη, ο τρόπος λειτουργίας του, τα θετικά στοιχεία αλλά και οι προκλήσεις που συνδέονται με την ευρύτατη κυκλοφορία του. Τέλος θα αναλυθεί το ζήτημα της χρήσης της αναλυτικής των δεδομένων για προβλέψεις τιμών για το Bitcoin.

ΚΕΦΑΛΑΙΟ 1 Η ΕΝΝΟΙΑ ΤΟΥ FINTECH ΚΑΙ Η ΕΜΦΑΝΙΣΗ ΤΩΝ ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΩΝ (CRYPTOCURRENCIES)

1.1. FinTech έννοια και περιεχόμενο

Η εμφάνιση του FinTech (συντομογραφία της χρηματοοικονομικής τεχνολογίας, ως αναδυόμενος τεχνικός όρος) υπήρξε ένας από τους πιο σημαντικούς μοχλούς αλλαγής στον κλάδο των χρηματοοικονομικών υπηρεσιών τα τελευταία χρόνια. Ο όρος, έχει κεντρίσει την περιέργεια ακαδημαϊκών, φοιτητών και ιδρυμάτων σε όλο τον κόσμο για περισσότερο από μια δεκαετία. Καινοτόμες εταιρείες χρηματοοικονομικών υπηρεσιών προσφέρουν ένα ευρύ φάσμα νέων χρηματοοικονομικών προϊόντων και νέους τρόπους αλληλεπίδρασης με πελάτες μέσω της ψηφιακής χρηματοδότησης (Stulz, 2019).

Για το εννοιολογικό περιεχόμενο του όρου Fintech, δεν έχει διαμορφωθεί ένας κοινά αποδεκτός ορισμός, ωστόσο έχει επιχειρηθεί να οριστεί το περιεχόμενό του σε διάφορους επιμέρους ορισμούς. Σύμφωνα με τον πιο κοινό ορισμό του FinTech στη βιβλιογραφία, η χρηματοοικονομική τεχνολογία Fintech «τεχνολογικά ενεργοποιημένη καινοτομία στις χρηματοοικονομικές υπηρεσίες που θα μπορούσε να οδηγήσει σε νέα επιχειρηματικά μοντέλα, εφαρμογές, διαδικασίες ή προϊόντα με συναφή ουσιώδη επίδραση στην παροχή χρηματοοικονομικών υπηρεσιών» (FSB, 2017; FSB, 2019).

Αυτή η προσέγγιση για τον ορισμό του FinTech μπορεί να περιγραφεί ως λειτουργική και ευρεία καθώς μπορεί να εφαρμοστεί τόσο σε παραδοσιακούς παρόχους χρηματοοικονομικών υπηρεσιών όσο και σε νεοεισερχόμενους. Σύμφωνα με έναν άλλο ορισμό, το FinTech είναι ένας ξεχωριστός τομέας του κλάδου των χρηματοοικονομικών υπηρεσιών που αποτελείται από οντότητες εκτός από τους παραδοσιακούς παρόχους χρηματοοικονομικών υπηρεσιών, οι οποίοι χρησιμοποιούν τεχνολογία αιχμής για να παρέχουν πιο αποτελεσματικές

χρηματοοικονομικές υπηρεσίες και να δημιουργούν νέες, που επιτρέπουν την παροχή νέας αξίας στους πελάτες (Zavolokina et al., 2020).

Σε γενικές γραμμές η χρηματοοικονομική τεχνολογία Fintech, χρησιμοποιείται για να περιγράψει τη νέα τεχνολογία που επιδιώκει να βελτιώσει και να αυτοματοποιήσει την παράδοση και τη χρήση χρηματοοικονομικών υπηρεσιών. Στον πυρήνα του, το fintech χρησιμοποιείται για να βοηθήσει τις εταιρείες, τα χρηματοπιστωτικά ιδρύματα, τους ιδιοκτήτες επιχειρήσεων και τους καταναλωτές να διαχειρίζονται καλύτερα τις οικονομικές λειτουργίες και τις διαδικασίες χρησιμοποιώντας εξειδικευμένο λογισμικό και αλγόριθμους που χρησιμοποιούνται σε υπολογιστές και, όλο και περισσότερο, σε smartphone (Stulz, 2019).

Σύμφωνα με έναν άλλο ορισμό ο όρος FinTech, αναφέρεται στην τεχνολογία και η καινοτομία που στοχεύει να ανταγωνιστεί τις παραδοσιακές χρηματοοικονομικές μεθόδους στην παροχή χρηματοοικονομικών υπηρεσιών ενώ ο σχετικός κλάδος, είναι ένας αναδυόμενος κλάδος που χρησιμοποιεί την τεχνολογία για να βελτιώσει τις χρηματοοικονομικές δραστηριότητες (Harasim, 2021).

Η χρήση smartphones για mobile banking, επενδύσεις, υπηρεσίες δανεισμού και κρυπτονομίσματα είναι παραδείγματα τεχνολογιών που στοχεύουν να κάνουν τις χρηματοοικονομικές υπηρεσίες πιο προσιτές στο ευρύ κοινό. Οι εταιρείες χρηματοοικονομικής τεχνολογίας αποτελούνται τόσο από νεοφυείς επιχειρήσεις όσο και από καθιερωμένα χρηματοπιστωτικά ιδρύματα και εταιρείες τεχνολογίας που προσπαθούν να αντικαταστήσουν ή να ενισχύσουν τη χρήση χρηματοοικονομικών υπηρεσιών που παρέχονται από υπάρχουσες χρηματοπιστωτικές εταιρείες (Hornuf et al., 2021).

Όταν το fintech εμφανίστηκε τον 21ο αιώνα, ο όρος αρχικά εφαρμόστηκε στην τεχνολογία που χρησιμοποιήθηκε στα back-end συστήματα των καθιερωμένων χρηματοπιστωτικών ιδρυμάτων. Από τότε, ωστόσο, έχει γίνει μια στροφή προς υπηρεσίες που είναι πιο προσανατολισμένες στον καταναλωτή και

επομένως έχουν διατυπωθεί πλέον ορισμοί για το Fintech που είναι πιο προσανατολισμένοι στον καταναλωτή. Το Fintech περιλαμβάνει πλέον διαφορετικούς τομείς και βιομηχανίες όπως μεταξύ άλλων η εκπαίδευση, η λιανική τραπεζική, η συγκέντρωση κεφαλαίων, οι κερδοσκοπικές οργανώσεις καθώς και τον τομέα της διαχείρισης επενδύσεων (Schueffel, 2016).

Ο όρος «χρηματοοικονομική τεχνολογία», σύμφωνα με έναν άλλο ορισμό είναι μια τεχνολογία η οποία μπορεί να εφαρμοστεί σε οποιαδήποτε καινοτομία στον τρόπο με τον οποίο οι άνθρωποι συναλλάσσονται με τις επιχειρήσεις, από την εφεύρεση του ψηφιακού χρήματος έως την τήρηση βιβλίων διπλής εγγραφής (Claessens et al., 2018). Από την επανάσταση του Διαδικτύου και την επανάσταση του κινητού Διαδικτύου/smartphone, η χρηματοοικονομική τεχνολογία έχει αναπτυχθεί εκρηκτικά και η fintech, η οποία αρχικά αναφερόταν στην τεχνολογία υπολογιστών που εφαρμοζόταν στο back office των τραπεζών ή των εμπορικών εταιρειών, τώρα περιγράφει μια ευρεία ποικιλία τεχνολογικών παρεμβάσεων σε προσωπικές και εμπορική χρηματοδότηση (Padilla, 2020).

Η ανάπτυξη του Fintech συνέβαλλε στην ανάπτυξη των κρυπτονομισμάτων. Με τον όρο κρυπτονομίσματα εννοούνται τα ψηφιακά νομίσματα τα οποία βασίζονται στην κρυπτογραφία για την διασφάλιση δοσοληψιών, ιδιοκτησίας και τη δημιουργία νέων μονάδων νομίσματος. Επιπλέον, τα κρυπτονομίσματα είναι μία peer-to-peer αποκεντρωμένη ηλεκτρονική μορφή χρήματος η οποία βασίζεται πάνω στις αρχές της κρυπτογραφίας για την διασφάλιση του δικτύου και την επαλήθευση των συναλλαγών, εκδίδονται και ελέγχονται από τους ίδιους τους χρήστες και όχι από χρηματοπιστωτικά ιδρύματα όπως τα παραδοσιακά νομίσματα (Bunea et al., 2016).

Λόγω πάντως του μεγάλου (και συνεχώς αυξανόμενου) αριθμού των λεγόμενων συστημάτων «κρυπτονομισμάτων» με διαφορετικά τεχνολογικά χαρακτηριστικά, ο όρος «κρυπτονομίσματα» δεν είναι εύκολο να οριστεί. Τα κρυπτονομίσματα αποτελούν δηλαδή έναν τύπο ψηφιακού περιουσιακού στοιχείου

που χρησιμοποιεί τεχνολογία καταμεμημένης λογιστικής ή blockchain για να επιτρέψει μια ασφαλή συναλλαγή (Price Waterhouse Coopers, 2016).

Τα κρυπτονομίσματα ως ένα είδος ψηφιακών νομισμάτων έχουν κάνει την εμφάνισή τους τα τελευταία χρόνια και συγκεκριμένα από το 2008. Παρόλο που η χρήση τους ως μέσο συναλλαγών είναι ακόμα περιορισμένη, αναμένεται με βάση τα στοιχεία ότι θα αποτελέσουν στο εγγύς μέλλον τα κυρίαρχα νομίσματα στην παγκόσμια ψηφιακή οικονομία, η οποία αναδύεται με ταχύτατους ρυθμούς (Hileman & Rauchs, 2017).

Οι ιδιότητες των κρυπτονομισμάτων είναι παρόμοιες ιδιότητες με τα παραδοσιακά νομίσματα, ωστόσο υπάρχει σημαντική διαφοροποίηση, καθώς όπως προαναφέρθηκε χρησιμοποιούν κρυπτογραφικές μεθόδους για την κωδικοποίηση και απόκρυψη πληροφοριών, διασφαλίζοντας με τον τρόπο αυτό, το προσωπικό απόρρητο και τη μοναδικότητα των συναλλαγών (Farell, 2015). Η πλειοψηφία των κρυπτονομισμάτων κρυπτονομίσματα χρησιμοποιούν την τεχνολογία blockchain ή αλλιώς Distributed Ledger Technology. Το blockchain, αποτελεί μια βάση δεδομένων στην οποία καταχωρούνται διάφορες συναλλαγές με ασφάλεια και πιστοποίηση, ενώ αντίγραφα της είναι δυνατό να βρίσκονται σε πολλά δικτυακά σημεία, τα οποία ενημερώνονται ταυτόχρονα και είναι προσβάσιμα από παντού. Η κάθε συναλλαγή, είναι αποθηκευμένη στο blockchain και κοινοποιείται σε όλους τους χρήστες του δικτύου γνωστοποιώντας το ποσό μεταφοράς στις διευθύνσεις τους, διατηρώντας όμως, παράλληλα, κρυφά τα πραγματικά στοιχεία των συναλλασσόμενων (Wheili, 2019).

1.2. Ιστορική εξέλιξη εμφάνισης κρυπτονομισμάτων

Ιστορικά, το εικονικό χρήμα έχει μπει στη μόδα σε διαφορετικούς χρόνους κατά τη διάρκεια της ιστορίας του ανθρώπινου πολιτισμού και συχνά παρέμεινε για μεγάλες χρονικές περιόδους προτού αντικατασταθεί από «απτές» εναλλακτικές λύσεις χρημάτων, για να αντικατασταθεί από το εικονικό χρήμα σε αυτό που έχει περιγραφεί ως σειρά μακροχρόνιων κύκλων χρηματικών μέσων και χρέους (Graeber 2011). Ακόμη και εντός της συγκεκριμένης κατηγορίας ψηφιακών μέσων μετρητών, ορισμένα είδη εικονικού χρήματος υπήρχαν πριν από το Bitcoin, αλλά δεν είχαν αναλάβει την κεντρική ή εξέχουσα θέση που τελικά θα λάμβανε το Bitcoin (Adhami et al., 2018).

Παρά τις μοναδικές προτάσεις του Bitcoin, υπήρχαν άλλα ψηφιακά νομισματικά σε κυκλοφορία στη διαδικτυακή σφαίρα που είχαν χαρακτηριστικά παρόμοια με το Bitcoin, όπως το proof of work μια μορφή κρυπτογραφικής απόδειξης στην οποία ένα μέρος αποδεικνύει σε άλλους ότι έχει δαπανηθεί ένα ορισμένο ποσό μιας συγκεκριμένης υπολογιστικής προσπάθειας. Το ecash είναι το παλαιότερο παράδειγμα. Το Ecash σχεδιάστηκε από τον David Chaum ως ένα ανώνυμο κρυπτογραφικό ηλεκτρονικό χρήμα ή σύστημα ηλεκτρονικών μετρητών το 1983. Το 1983 ο Αμερικανός κρυπτογράφος ανέπτυξε ένα κρυπτογραφικό σύστημα που ονόμασε eCash και δώδεκα χρόνια αργότερα, ανέπτυξε ένα άλλο σύστημα, το DigiCash, το οποίο χρησιμοποίησε την κρυπτογραφία προκειμένου να κάνει απόρρητες οικονομικές συναλλαγές (Blau, 2018).

Πραγματοποιήθηκε μέσω της εταιρείας του DigiCash και χρησιμοποιήθηκε ως σύστημα μικροπληρωμών σε μια τράπεζα των ΗΠΑ από το 1995 έως το 1998. Ειδικότερα, το 1985, ο κρυπτογράφος David Chaum έκανε μια δημοσίευση με τίτλο «*Security without identification: Transaction Systems to Make Big Brother Obsolete*» (Ασφάλεια χωρίς ταυτοποίηση: Συστήματα συναλλαγών που θα κάνουν τον Μεγάλο Αδερφό ξεπερασμένο). Η βασική ιδέα του Chaum ήταν πώς μέσω της

κρυπτογραφίας θα μπορούσαν να δημιουργηθούν ψηφιακά νομίσματα που να είναι εντελώς ανώνυμα, και άρα να μην έχει πάνω τους έλεγχο καμία κυβέρνηση (Bornholdt & Sneppen, 2014).

Επίσης ο Adam Back είχε δημιουργήσει ένα σύστημα απόδειξης εργασίας για τον έλεγχο ανεπιθύμητης αλληλογραφίας γνωστό ως hashcash. Ειδικότερα ο Adam Back βασιζόμενος στην ιδέα του Chaum, δημιούργησε μια mailing list («Cypherpunks») σχετικά με το χώρο της κρυπτογραφίας μέσω υπολογιστή. Σε αυτή τη λίστα, το 1997, διαδόθηκε η μέθοδος Hashcash, την οποία δημιούργησε ο Adam Back, η διαδικασία «*proof of work*»(απόδειξη εργασίας) περιλαμβάνει ένα κομμάτι δεδομένων που παίρνει χρόνο για να δημιουργηθεί, αλλά είναι εύκολο να επαληθευτεί. Αυτή η μέθοδος αποτέλεσε το θεμέλιο της δημιουργίας των κρυπτονομισμάτων (Conte de Leon et al., 2017).

Ο αλγόριθμος απόδειξης εργασίας στο hashcash αναπτύχθηκε περαιτέρω με τη μορφή RPOW από τον Hal Finney. Άλλες προτάσεις για κρυπτονομίσματα περιλάμβαναν το B-Money του Wei Dai και το Bit Gold του Nick Szabo. Ειδικότερα, το 1998, ο μηχανικός λογισμικού Wei Dai δημοσίευσε την πρόταση του για ένα ανώνυμο, διαμοιρασμένο σύστημα ηλεκτρονικών χρημάτων, το οποίο ονόμασε *B-money*. Αντίστοιχα, το 2005 ο Nick Szabo, ακαδημαϊκός, στον χώρο της πληροφορικής, δημοσίευσε την δική του πρόταση για ένα νέο ψηφιακό νόμισμα, το “*Bit gold*”. Ένα ψηφιακό νόμισμα, που σε αντίθεση με το χρυσό θα μπορούσε να το παράγει εύκολα ο καθένας. Θα έπρεπε όμως να είναι διαθέσιμο σε περιορισμένα συνολικά κομμάτια, ώστε να μην χάσει την αξία του λόγω πληθωρισμού (Dos Santos, 2017).

Αν και οι προτάσεις τους δεν εφαρμόστηκαν ποτέ, ήταν ο πρόδρομος της δημιουργίας του Bitcoin. Με αυτούς τους καινοτόμους να βάζουν τις βάσεις, το ίδιο το Bitcoin ήρθε στην επιφάνεια, από ένα άτομο με ψευδώνυμο ή οντότητα γνωστό ως Satoshi Nakamoto. Τον Οκτώβριο του 2008, έγινε η πρώτη επιστημονική δημοσίευση, με τίτλο “*Bitcoin: A Peer-to-Peer Electronic Cash System*” από έναν συγγραφέα που υπέγραψε με το ψευδώνυμο Satoshi Nakamoto.

Ακόμη και σήμερα, κανείς δεν γνωρίζει την πραγματική του ταυτότητα, την ηλικία, το φύλο, ή την εθνικότητά του. ούτε ακόμη αν πρόκειται για ένα άτομο ή για μία ομάδα ατόμων (Fry, 2016).

Ο Wei Dai και ο Hal Finney θεωρήθηκαν ότι ήταν πίσω από το ψευδώνυμο Satoshi Nakamoto, αλλά εξέδωσαν αρνήσεις για το σκοπό αυτό. Ο Nakamoto δημοσίευσε το παραπάνω άρθρο σε μια λίστα αλληλογραφίας κρυπτογραφίας το 2008 και παρουσίασε το σχήμα για ένα δίκτυο peer-to-peer που θα ενθάρρυνε ένα «σύστημα ηλεκτρονικών συναλλαγών» (Nakamoto 2008). Το υποκείμενο μήνυμα ήταν ότι τα στοιχεία της εμπιστοσύνης, της λογοδοσίας ή της επίβλεψης, που χαρακτήριζαν το εμπόριο και τις ανταλλαγές σε όλη την ιστορία, θα αντικατασταθούν από ένα σύστημα που απλώς δεν θα χρειαζόταν οι συναλλασσόμενοι πράκτορες να γνωρίζουν ο ένας τον άλλον (Chohan 2017).

Στις 9 Νοεμβρίου 2008 στάλθηκε ένα e-mail σε μία λίστα ατόμων που είχαν ως κοινό ενδιαφέρον την κρυπτογραφία και τα συστήματα ασφαλείας, το οποίο περιελάμβανε το άρθρο του Satoshi Nakamoto. Στο e-mail αναλυόταν η ιδέα του Nakamoto για την δημιουργία του Bitcoin, η οποία θα στηριζόταν στην κρυπτογραφία και στη χρήση του blockchain, όπου οι συναλλαγές αυτές θα πραγματοποιούνταν απευθείας από χρήστη σε χρήστη (peer to peer) (Ha & Moon, 2018).

Ο Nick Szabo και ο Wei Dai εξέφρασαν επίσης ισχυρή υποστήριξη για το Bitcoin μετά την κυκλοφορία του. Ο ίδιος ο Nakamoto εξόρυξε ένα ποσό περίπου 1 εκατομμυρίου bitcoin, πριν εξαφανιστεί και διακόψει την εμπλοκή του με το κίνημα bitcoin. Ο Gavin Andresen έγινε ο κύριος προγραμματιστής στο Bitcoin Foundation και στη συνέχεια έγινε το ισοδύναμο του «δημόσιου προσώπου» του Bitcoin.

Μετά τη δημοσίευση του άρθρου (Nakamoto 2008), η πραγματική πλατφόρμα για συναλλαγές bitcoin δημιουργήθηκε μέσω της κυκλοφορίας του πρώτου Bitcoin-Client ανοιχτού κώδικα και της ταυτόχρονης έκδοσης Bitcoin. Ο

Nakamoto εξόρυξε το πρώτο μπλοκ bitcoin με ανταμοιβή 50 bitcoin. Αυτό το μπλοκ αναφέρεται συνήθως ως «μπλοκ γένεσης» (Hong, 2017).

Ο Hal Finney κατέβασε την εφαρμογή bitcoin και έλαβε τα πρώτα 10 bitcoin από το Nakamoto, το οποίο αντιπροσώπευε την πρώτη συναλλαγή Bitcoin στην ιστορία. Έως και το Μάρτιο του 2009, οι συναλλαγές με Bitcoin δεν είχαν κάποια ουσιαστική χρήση ενώ η μεταφορά των νομισμάτων αποτελούσε ένα είδος ενασχόλησης μεταξύ όσων δήλωναν υποστηρικτές της κρυπτογραφίας. Ωστόσο αυτό έμελλε να αλλάξει καθώς τον Μάρτη του 2019, δημιουργήθηκε το πρώτο ανταλλακτήριο για Bitcoin το BitcoinMarket.com, προσφέροντας μια κυμαινόμενη συναλλαγματική ισοτιμία για το bitcoin. Πριν από την δημιουργία του πρώτου αυτού ανταλλακτηρίου, οι αγοραστές μπορούσαν να αγοράσουν bitcoin στέλνοντας σε άλλο χρήστη δολάρια ΗΠΑ μέσω PayPal, ενώ το Bitcoin Market θα κρατούσε το bitcoin του πωλητή σε μεσεγγύηση μέχρι ο πωλητής να λάβει τα χρήματά του (Hong, 2017).

Λίγο αργότερα στις 22 Μαΐου, ο Laszlo Hanyecz, ένας από τους πρώτους που υιοθέτησαν το νέο κρυπτονόμισμα που μόλις είχε κωδικοποιηθεί, έκανε την πρώτη συναλλαγή με αντίκρισμα στον πραγματικό κόσμο, καθώς αγόρασε δυο πίτσες από το κατάστημα Papa Johns χρησιμοποιώντας 10.000 bitcoins. Η αγορά ισοδυναμούσε περίπου με \$41 δολάρια το 2010, με βάση την τρέχουσα τιμή για το bitcoin τότε, και θεωρείται ευρέως ως η πρώτη φορά που ένα εικονικό νόμισμα χρησιμοποιήθηκε για να αγοράσει οτιδήποτε στον πραγματικό κόσμο. Το συγκεκριμένο γεγονός αποτέλεσε σταθμό στην πορεία του Bitcoin (Kim, 2017).

Η εν λόγω συναλλαγή, ώθησε στην περαιτέρω αύξηση του ενδιαφέροντος όσων ήδη ασχολούνταν με την εξόρυξη νομισμάτων, όπως επίσης και του ευρύτερου κοινού, δεδομένου ότι άρχισε να γίνεται αντιληπτό ότι το Bitcoin θα μπορούσε να αποτελέσει ένα ηλεκτρονικό νόμισμα η χρήση του οποίου θα ήταν ευρεία στο μέλλον. Η αποδοχή του Bitcoin, από ένα μεγαλύτερο εύρος ατόμων, οδήγησε σε εκείνη την περίοδο στην κατακόρυφη άνοδο της αξίας του κατά 900% από \$0,008 σε \$0,08 για 1 BTC (Kim, 2017).

Τον Ιούλιο του ίδιου έτους ιδρύθηκε από τον Jeb McCaleb, το δεύτερο ανταλλακτήριο το MT.GOX, το οποίο σε ένα μόλις μικρό χρονικό διάστημα, έγινε αποδεκτό και αγαπητό, καθώς περιείχε την ενσωμάτωση και περαιτέρω βελτίωση των βασικών χαρακτηριστικών από το πρώτο ανταλλακτήριο BitcoinMarket. Για το λόγο αυτό εξάλλου, το MT.GOX διατήρησε την ηγεσία στο χώρο των ανταλλακτηρίων (Ksherti, 2017).

Στα μέσα της επόμενης χρονιάς και ειδικότερα, τον Αύγουστο του 2010 παρατηρήθηκε μια δυσλειτουργία στο λογισμικό του Bitcoin, δεδομένου ότι οι συναλλαγές δεν πιστοποιούνταν με τον κατάλληλο τρόπο που όριζε ο κώδικας πριν αυτές ενσωματωθούν στην blockchain. Δηλαδή, λόγω ενός κενό στο λογισμικό του Bitcoin δημιουργήθηκε σε δυο περιπτώσεις ένας δυσανάλογος αριθμό νομισμάτων, σε μία μόνο συναλλαγή, τα οποία στάλθηκαν σε δύο διευθύνσεις στο δίκτυο. Αν και αμέσως η συγκεκριμένη συναλλαγή έγινε αντιληπτή και διαγράφηκε καθώς επίσης και βελτιστοποιήθηκε ο κώδικας του Bitcoin ουσιαστικά επρόκειτο για το πρώτο και μοναδικό ως σήμερα τρωτό σημείο του κώδικα ως προς την ασφάλεια (Luther, 2015).

Έως το τέλος του 2010, έλαβαν χώρα δυο κρίσιμα συμβάντα για την περαιτέρω πορεία και εξέλιξη του Bitcoin. Στις αρχές του Δεκεμβρίου πραγματοποιήθηκε η πρώτη συναλλαγή μέσω της εφαρμογής BitcoinD, μέσω κινητού τηλεφώνου, αξίας 0,42 BTC, κάτι που αποτέλεσε σημείο κλειδί για την εξέλιξη του νομίσματος. Επίσης λίγο αργότερα τον ίδιο μήνα, λειτούργησε το πρώτο mining pool, το οποίο παρείχε την δυνατότητα σε χρήστες που δεν διέθεταν ισχυρά υπολογιστικά συστήματα, να εξορύξουν Bitcoins, από κοινού, μέσω της ενοποίησης των υπολογιστών τους και στη συνέχεια να μοιράζονται τα Bitcoins, με κριτήριο την ισχύ που κάθε χρήστης παρείχε στο σύστημα (Luther, 2015).

Στις αρχές του 2011, η πορεία του Bitcoin ήταν ραγδαία, καθώς είχαν ήδη παραχθεί 5,25εκ. Bitcoin, ενώ στις αρχές Φεβρουαρίου για πρώτη φορά η τιμή του ανέβηκε στο \$1 στο ανταλλακτήριο, MT.GOX. Στο διάστημα που επακολουθεί η αποδοχή του Bitcoin, συνεχίζει να αυξάνεται σταθερά, ενώ στις 2 Ιουνίου η τιμή

του έφθασε στα \$33. Τον Ιούλιο του 2011, κυκλοφόρησε η πρώτη εφαρμογή για Bitcoin στο I-pad το "Bitcoin Mobile" ενώ τον Αύγουστο έλαβε χώρα στη Νέα Υόρκη το πρώτο συνέδριο που αφορούσε το Bitcoin το οποίο έλαβε χώρα στην Νέα Υόρκη. Λίγους μήνες αργότερα τον Νοέμβριο, υλοποιήθηκε ένα ακόμα ευρωπαϊκό συνέδριο για το Bitcoin, στην Πράγα της Τσεχίας (Pieters & Vivanco, 2017).

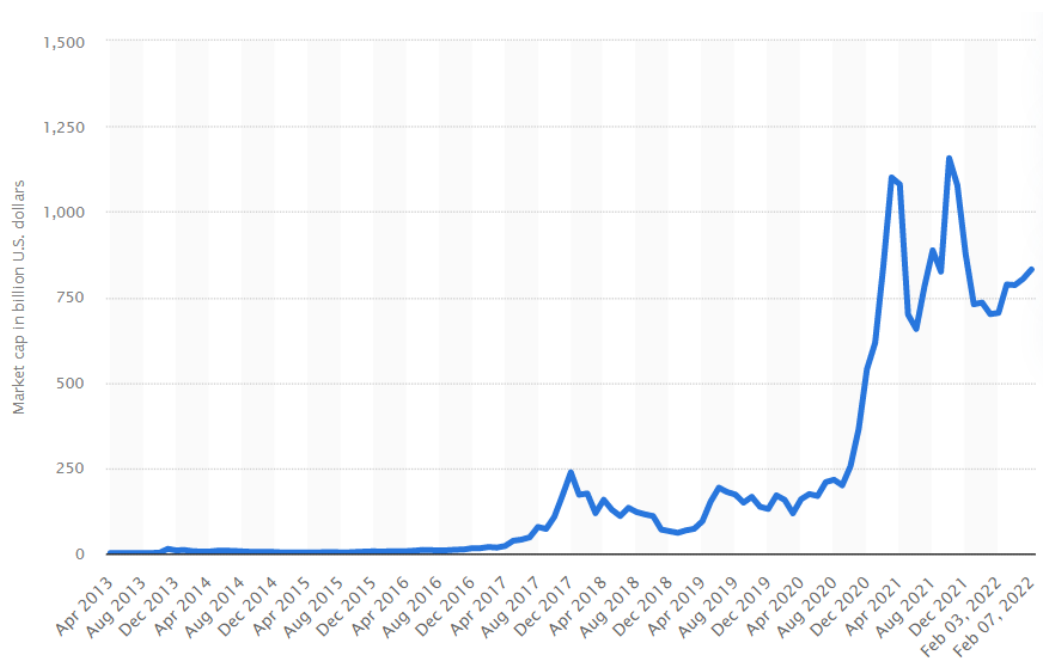
Στις αρχές του 2013 η τιμή του Bitcoin έφθασε στα \$35,84, ενώ τον Μάρτη του 2013, η Αμερικανική Υπηρεσία Οικονομικού Εγκλήματος (FinCEN), εισήγαγε κανονισμούς που αφορούν τα αποκεντρωμένα ψηφιακά νομίσματα αναγνωρίζοντας την νομιμότητα εξόρυξης Bitcoin, από αμερικανούς πολίτες ως άτομα που παρέχουν υπηρεσίες χρηματικών συναλλαγών. Τον Απρίλιο, η τιμή της αγοράς του Bitcoin, ξεπέρασε για πρώτη φορά, το \$1 δις, εξαιτίας της αυξημένης εμπιστοσύνης που είχε αρχίσει να αναπτύσσεται για το Bitcoin, και με δεδομένο ότι όλο και περισσότερες αξιόπιστες εταιρείες άρχισαν πλέον να το δέχονται ως μέσο πληρωμής (Ksherti, 2017).

Στις 6 Αυγούστου ο ομοσπονδιακός δικαστής του Texas Amos Mazzant, απεφάνθη ότι το Bitcoin είναι νόμισμα υποστηρίζοντας ότι η επένδυση Bitcoins είναι «τόσο επενδυτικά συμβόλαια όσο και χαρτονομίσματα και, ως εκ τούτου, είναι τίτλοι». Τον Οκτώβριο του ίδιου έτους, άρχισε να εκτοξεύεται η αναγνώριση του Bitcoin εκτός από την Αμερικανική και την Ευρωπαϊκή, και στην Ασιατική αγορά, καθώς η εταιρεία κολοσσός Baidu άρχισε να το δέχεται ως μέσο πληρωμής, κάτι που είχε ως αποτέλεσμα το κινέζικο ανταλλακτήριο BTC China να ξεπεράσει σε όγκο συναλλαγών το Ιαπωνικό MT.GOX και το Ευρωπαϊκό Bitstamp. (Pieters & Vivanco, 2017).

Στις αρχές του 2014 όλο και περισσότερες εταιρείες άρχισαν να δέχονται Bitcoin ως μέσο πληρωμής τις διαδικτυακές πληρωμές των προϊόντων και υπηρεσιών τους. Ωστόσο καθώς στις αρχές του Φεβρουαρίου το ανταλλακτήριο MT.GOX τέθηκε σε καθεστώς πτώχευσης ανακοινώνοντας ότι είχε πέσει θύμα κλοπής, οδήγησε σε μια ακόμη φορά την αγορά του Bitcoin σε αβεβαιότητα και

βαθιά ύφεση κατεβάζοντας την τιμή του από περίπου \$1000 στα \$500. (Ksherti, 2017).

Ωστόσο καθώς τον Ιούλιο μεγάλες εταιρείες άρχισαν ξανά να εμπιστεύονται το Bitcoin, όπως για παράδειγμα η Dell, η πορεία για το Bitcoin άρχισε να γίνεται και πάλι ανοδική. Παράλληλα τον ίδιο μήνα έλαβε χώρα ένα σημαντικό γεγονός που έμελλε να αλλάξει τον χώρο των κρυπτονομισμάτων καθώς δημιουργήθηκε το ένα δεύτερο κρυπτονόμισμα το Initial Coin Offering (ICO) από τον Vitalik Buterin το οποίο ήταν σχεδιασμένο να προσφέρει περισσότερες λειτουργίες και δυνατότητες από ότι το Bitcoin. Η δημιουργία αυτή, του δεύτερου κρυπτονομίσματος, άνοιξε τον δρόμο για την δημιουργία δεκάδων άλλων τα επόμενα χρόνια. Η εξέλιξη της αγοράς Bitcoin έως και σήμερα παρουσιάζει συνεχή άνοδο. Είναι χαρακτηριστικό ότι τον Οκτώβριο του 2021, το ανώτατο όριο της αγοράς Bitcoin έφτασε στο υψηλότερο ποσοστό όλων των εποχών φθάνοντας τα 1.156 δισεκατομμύρια δολάρια.



1.3. Η φύση του χρήματος γενικά

Τα χρήματα επινοήθηκαν για να λύσουν το πρόβλημα της ανθρωπότητας, του συστήματος ανταλλαγής για την ανταλλαγή αγαθών και υπηρεσιών μεταξύ τους. Σύμφωνα με τον Lietaer (2001), το χρήμα είναι συμφωνία, μέσα σε μια κοινότητα ή κοινωνία, να χρησιμοποιηθεί κάτι ως μέσο ανταλλαγής. Ιστορικά, η ανθρωπότητα έχει χρησιμοποιήσει χρήματα σε διάφορες μορφές, από αγαθά όπως αλάτι, βοοειδή, σιτάρι, μεταλλικό υλικό όπως χρυσός και ασήμι σε αντίθεση με το σήμερα, όπου με την ταχεία ανάπτυξη της τεχνολογίας, επινοούνται εικονικά νομίσματα. Το πιο δημοφιλές εικονικό νόμισμα που χρησιμοποιούσε τεχνική κρυπτογραφίας σε ένα αποκεντρωμένο δίκτυο βρέθηκε από μια οντότητα με το όνομα Satoshi Nakamoto το 2009. (Pieters & Vivanco, 2017).

Όπως αναφέρει ο Shi (2016), με την πάροδο του χρόνου, οι κοινωνίες ανακάλυψαν ότι τα χρήματα μπορούν να διαδραματίσουν αποτελεσματικό και κρίσιμο ρόλο εάν πληρούν τις απαιτήσεις, όπως αποδεκτή, διαιρετή, ομοιογενής, ανθεκτική, κινητή, σπάνια και σταθερή αξία. Αποδεκτό σημαίνει ότι τα χρήματα πρέπει να έχουν μια εγγενή αξία, επομένως πρέπει να είναι επιθυμητά από μόνα τους. Η απαίτηση της αποδοχής είναι περίπλοκη, δεδομένου ότι το παραστατικό χρήμα (fiat money)¹ δεν έχει εγγενή αξία. Η κυβέρνηση το κάνει αποδεκτό μέσω του νόμου περί νομίμου χρήματος (Shi, 2016).

¹ Παραστατικό χρήμα ή αλλιώς χρήμα αναγκαστικής κυκλοφορίας είναι το μέσον πληρωμής το οποίο δεν καλύπτεται από αποθεματικό άλλων υλικών (π.χ. χρυσός) και επομένως στερείται κάποιας εσωτερικής αξίας έστω και έμμεσα. Επιβάλλεται στις συναλλαγές από κάποια αρχή (συνήθως το κράτος) τόσο στις πληρωμές όσο και στις εισπράξεις. Εκφράζεται με κάποια νομισματική μονάδα έχει την μορφή συνήθως χαρτονομισμάτων και κερμάτων, τα οποία μπορεί να έχουν ονομαστική αξία ίση, πολλαπλάσια ή υποπολλαπλάσια της νομισματικής μονάδας. Το χάρτινο χρήμα καλείται παραστατικό χρήμα διότι η χρησιμοποίησή (και αξία) του ως χρήματος εξαρτάται από την πίστωση της κυβέρνησης που το εκδίδει, και όχι από οποιοδήποτε δικαίωμα να μετατραπεί σε μεταλλικά νομίσματα. Πιο συγκεκριμένα, το παραστατικό χρήμα απελευθερώνεται πλήρως από την ποσότητα των πολύτιμων μετάλλων.

Η δεύτερη απαίτηση είναι η διαιρετότητα και σημαίνει ότι τα χρήματα πρέπει να χωρίζονται εύκολα σε μικρά μέρη ώστε οι άνθρωποι να μπορούν να αγοράζουν αγαθά και υπηρεσίες σε οποιαδήποτε τιμή. Για να μοιράζονται εύκολα τα χρήματα πρέπει να είναι ομοιόμορφα ή ομοιογενή. Η επόμενη απαίτηση είναι η ανθεκτικότητα, πράγμα που σημαίνει ότι τα χρήματα πρέπει να είναι μακροχρόνια στη διάρκειά τους και να μην καταστρέφονται εύκολα. Πρέπει επίσης να είναι εύκολα στη μεταφορά. Η απαίτηση της σπανιότητας σημαίνει ότι τα χρήματα πρέπει να είναι σχετικά δύσκολα ή σπάνια να εξευρεθούν και η αξία τους πρέπει να παραμένει σχετικά σταθερή με την πάροδο του χρόνου (Tschorsch & Scheuermann, 2016).

Όσον αφορά την ιστορική εξέλιξη του χρήματος και του παραστατικού χρήματος, όπως αναφέρεται στον Abu-Bakar (2018), η ιστορική εξέλιξη του χρήματος έχει πραγματοποιηθεί σε πολλά στάδια με την πάροδο του χρόνου. Το πρώτο στάδιο είναι το σύστημα ανταλλαγής, όταν οι άνθρωποι ανταλλάσσουν και μεταφέρουν μεταξύ τους αγαθά και υπηρεσίες με άλλα αγαθά και υπηρεσίες. Το δεύτερο στάδιο είναι το σύστημα εμπορευματικού χρήματος, όταν οι άνθρωποι χρησιμοποιούσαν εμπορεύματα όπως το σιτάρι, τους σπόρους ή τα βοοειδή ως μέσο ανταλλαγής. Το τρίτο στάδιο είναι ένα μεταλλικό σύστημα χρήματος, όταν οι άνθρωποι χρησιμοποιούσαν το χρυσό και το ασήμι ως μέσο συναλλαγής. Το σύστημα μεταλλικού χρήματος εξελίχθηκε με την πάροδο του χρόνου, από το βάρος, με βάση τα νομίσματα μέχρι το χαρτί, το οποίο υποστηρίχθηκε 100 τοις εκατό από χρυσό (Shi, 2016).

Το επόμενο στάδιο είναι το παραστατικό χρήμα (fiat money) το οποίο χρησιμοποιήθηκε κατά κύριο λόγο κατά τη διάρκεια των πολέμων, όταν οι κυβερνήσεις χρειάζονταν χρήματα για να πληρώσουν για τους πολέμους ή την έλλειψη χρημάτων. Όμως, η χρήση των χρημάτων fiat δημιούργησε ένα άλλο πρόβλημα, το οποίο ήταν ο υπερπληθωρισμός και η υποτίμηση. Όπως επισημαίνουν οι Davies and Connors (2016), το 1971, όταν ο Πρόεδρος Νίξον ακύρωσε την άμεση μετατρεψιμότητα των δολαρίων ΗΠΑ σε χρυσό, αυτό

αποτελέσει το τέλος των χρημάτων fiat που υποστηρίχθηκαν από χρυσό. Η Κεντρική Τράπεζα άρχισε να εκδίδει μη μετατρέψιμα χρηματικά ποσά και βάσει του νόμου περί νομίμου χρήματος, οι άνθρωποι υποχρεώνονταν να το αποδεχτούν ως πληρωμή για αγαθά ή υπηρεσίες και ρύθμιση χρεών (Tschorsch & Scheuermann, 2016).

Η Τράπεζα της Αγγλίας (2014) περιέγραψε το νόμιμο χρήμα ως εξής: Το νόμιμο χρήμα έχει μια πολύ στενή και τεχνική έννοια, η οποία σχετίζεται με τη ρύθμιση οφειλών. Σημαίνει ότι εάν κάποιος οφείλει σε κάποιον, τότε δεν μπορεί να μηνυθείτε για μη πληρωμή εάν προσφέρει πλήρη εξόφληση των χρεών του σε νόμιμο χρήμα. Σε κάποιες χώρες, υπάρχουν ορισμένοι περιορισμοί κατά τη χρήση των κερμάτων χαμηλότερης αξίας ως νόμιμο χρήμα. Για παράδειγμα, τα κέρματα 1p και 2p στο Ηνωμένο Βασίλειο υπολογίζονται ως νόμιμο χρήμα μόνο για οποιοδήποτε ποσό έως 20p (Urquhart, 2016).

Υπάρχουν πολλές αποδεκτές μέθοδοι πληρωμής που δεν είναι τεχνικά νόμιμο χρήμα. Αυτός είναι ο λόγος για τον οποίο ο όρος «νόμιμο χρήμα» έχει ελάχιστη χρήση στις συνηθισμένες καθημερινές συναλλαγές. Τα περισσότερα καταστήματα στην αγορά, δέχονται πληρωμές με χρεωστική ή πιστωτική κάρτα και ορισμένα δέχονται επιταγές και ανέπαφες πληρωμές. Αυτοί είναι ασφαλείς και βολικοί τρόποι πληρωμής, παρόλο που δεν χαρακτηρίζονται ως νόμιμο χρήμα, είτε κάποιος πληρώνει με τραπεζογραμμάτια, κέρματα, χρεωστικές κάρτες ή οτιδήποτε άλλο, καθώς η πληρωμή είναι απόφαση ανάμεσα σε αυτόν και το άλλο άτομο που εμπλέκεται στη συναλλαγή (Tschorsch & Scheuermann, 2016).

Έτσι, μπορούμε να διακρίνουμε μεταξύ χρήματος και νομίσματος. Το χρήμα είναι μέσο ανταλλαγής και αποθήκευση αξίας. Ο χρυσός και το ασήμι είναι οι βέλτιστες μορφές χρήματος, επειδή διατηρούν την αγοραστική δύναμη για μεγάλο χρονικό διάστημα με περιορισμένη ποσότητα. Ο χρυσός και το ασήμι έχουν επίσης εγγενή αξία. Το νόμισμα είναι συνήθως τα χαρτονομίσματα και τα κέρματα που εκδίδονται από την κυβέρνηση ή την κεντρική τράπεζα ως μέσο συναλλαγής. Δεδομένου ότι το παραστατικό νόμισμα fiat δεν υποστηρίζεται από χρυσό, δεν έχει

καμία εγγενή αξία. Η αξία καθορίζεται από την προσφορά και τη ζήτηση. Περισσότερο νόμισμα σε κυκλοφορία θα το κάνει λιγότερο πολύτιμο (Urquhart, 2016).

Όπως αναφέρθηκε παραπάνω, και όπως επισημαίνει ο Meera (2018), τα χρήματα μπορούν να παίξουν αποτελεσματικό ρόλο εάν πληρούν τις επτά απαιτήσεις. Το ερώτημα συνεπώς που προκύπτει είναι αν το κρυπτονόμισμα που αντιπροσωπεύεται από το Bitcoin έχει εκπληρώσει τις επτά απαιτήσεις σε σύγκριση με άλλα νομίσματα. Πράγματι το Bitcoin έχει τα ίδια χαρακτηριστικά με το παραστατικό νόμισμα fiat που πληροί έξι από τις επτά απαιτήσεις. Και τα δύο δεν έχουν εγγενή αξία. Οι απαιτήσεις σταθερής τιμής αναφέρονται στη συνάρτηση αποθήκευσης αξίας. Το νόμισμα μπορεί να χρησιμοποιηθεί ως αποθήκευση αξίας, αλλά η αξία μπορεί να μειωθεί λόγω του κινδύνου που μπορεί να προκύψει. Για τις διαρκείς απαιτήσεις, σε νόμισμα εμπορεύματος και αυτή η απαίτηση ισχύει ανάλογα με τον τύπο του εμπορεύματος. Για παράδειγμα, προϊόντα όπως το σιτάρι ή το αλάτι είναι ευπαθή μέσω μυκήτων, παρασίτων, νερού, φωτιάς, βακτηριακής δραστηριότητας και επίσης καταστρέφονται από τη διαδικασία της κατανάλωσης (Urquhart, 2016).

Παρά την εξαιρετικά ασταθή τιμή του, η αξία του Bitcoin υπάρχει όταν οι χρήστες του έχουν εμπιστοσύνη να το χρησιμοποιήσουν και να το αποδεχτούν ως πληρωμή. Επιπλέον, ο DeVries (2016) δήλωσε ότι το Bitcoin μπορεί να υιοθετηθεί ευρέως λόγω αυτού που ο DeVries περιέγραψε ως «τρίγωνο της φωτιάς». Χρειάζεται αποδοχή από τον προμηθευτή, αποδοχή από τον χρήστη και καινοτομία. Ως εκ τούτου, όσον αφορά τη φύση του χρήματος, το Bitcoin γίνεται αποδεκτό ως χρήμα: είναι αξιόπιστο, αποδεκτό ως πληρωμή και γίνεται όλο και περισσότερο εναλλακτική μέθοδος πληρωμής σε αυτήν την τρέχουσα παγκόσμια αγορά που τροφοδοτείται από το Διαδίκτυο (De Vries, 2016).

Η ταχεία ανάπτυξη του εμπορίου που βασίζεται στο Διαδίκτυο και της τεχνολογίας κινητής τηλεφωνίας οδήγησαν σε ραγδαίες αλλαγές στην παγκόσμια οικονομία. Πολλές εταιρείες για παράδειγμα, όπως η βιομηχανία λιανικής

καταρρέουν επειδή δεν μπορούν να ανταγωνιστούν εταιρείες ηλεκτρονικού εμπορίου όπως η Alibaba. Τα ηλεκτρονικά συστήματα πληρωμών αλλάζουν τον τρόπο πληρωμής των αγαθών και των υπηρεσιών. Μία από τις σημαντικές εξελίξεις των οικονομικών αλλαγών είναι τα ψηφιακά νομίσματα (De Vries, 2016).

Όπως αναφέρεται στον Putinovici (2018) τα ψηφιακά νομίσματα είναι ψηφιακή αναπαράσταση αξίας που μπορεί να εξαργυρωθεί για αγαθά και υπηρεσίες. Ο Putinovici (2018) τονίζει ότι τα ψηφιακά νομίσματα με βάση την αξία μπορούν να εκφραστούν σε νόμιμο χρήμα. Για παράδειγμα, το PayPal και το ηλεκτρονικό χρήμα είναι ψηφιακά νομίσματα που μπορούν να εκφραστούν με βάση το παραστατικό νόμισμα fiat και μπορούν να ανταλλάσσονται στην πραγματική οικονομία, ενώ τα ψηφιακά νομίσματα που δεν μπορούν να εκφραστούν στο νόμιμο χρήμα ονομάζονται εικονικά νομίσματα.

Επιπλέον, ο Putinovici (2018) εξηγεί ότι τα εικονικά νομίσματα, αντίθετα, χρησιμοποιούνται κυρίως στον εικονικό κόσμο. Έχουν τη δική τους λογιστική μονάδα και δεν μπορούν να εκφραστούν σε παραστατικό νόμισμα fiat. Τα εικονικά νομίσματα έχουν διαφορετικά επίπεδα μετατρεψιμότητας. Τα νομίσματα τυχερών παιχνιδιών (gaming coins), για παράδειγμα, χρησιμοποιούνται μόνο στον εικονικό τους τομέα. Η ανταλλαγή σε παραστατικά νομίσματα fiat εκτός του εικονικού τους τομέα είναι περιορισμένη. Αντίθετα, το μετατρέψιμο εικονικό νόμισμα επιτρέπει την ανταλλαγή σε νόμισμα fiat και επίσης μπορεί να χρησιμοποιηθεί για πληρωμές αγαθών και υπηρεσιών στην πραγματική οικονομία (Putinovici, 2018).

Όταν τα μετατρέψιμα εικονικά νομίσματα χρησιμοποιούν αποκεντρωμένα συστήματα, χρειάζονται τεχνική κρυπτογράφησης για τον εντοπισμό και την επαλήθευση των συναλλαγών και αποκαλούνται κρυπτονομίσματα. Χρησιμοποιώντας αποκεντρωμένα συστήματα, επιτρέπουν τη συναλλαγή peer-to-peer, επομένως δεν χρειάζονται την κεντρική αρχή για τη διαχείριση των συστημάτων και η διαδικασία εκκαθάρισης μπορεί να εξαλειφθεί. Η καινοτομία των κρυπτονομισμάτων δημιούργησε μια πρόκληση για τον σύγχρονο κόσμο (Putinovici, 2018)

1.4. Ο ρόλος των κρυπτονομισμάτων στην παγκόσμια οικονομία

Όλα ξεκίνησαν με το Bitcoin, το οποίο εισήχθη για πρώτη φορά ως λευκή βίβλος το 2009 ως Peer-to-Peer Electronic Cash System. Έκτοτε, προστέθηκαν διάφοροι τύποι ψηφιακών νομισμάτων, με την κεφαλαιοποίηση της αγοράς να φτάνει τα 2,65 τρισεκατομμύρια δολάρια. Η εξειδικευμένη ομάδα επενδυτών επωφελήθηκε από τη τεχνολογία blockchain, καθώς το κρυπτονόμισμα ήταν λιγότερο κοινό σε μεμονωμένους επενδυτές σε όλο τον κόσμο. Το 2014, εταιρείες όπως η Overstock αποδέχθηκαν το Bitcoin ως έναν από τους τρόπους πληρωμής έναντι των διαδικτυακών αγορών. Το ίδιο ακολουθούν διάσημες εταιρείες όπως οι Master Card, Pavilion Hotels, AXA Insurance, Starbucks, Visa, και PayPal (Kajtazi & Moro, 2018).

Πολύ πρόσφατα, τον Μάρτιο του 2021, η JP Morgan παρουσίασε ένα πακέτο έκθεσης σε κρυπτονομίσματα που περιείχε 11 άνισα σταθμισμένες μετοχές αναφοράς. Επιπλέον, τον Μάιο του 2021, η Goldman Sachs το ενέκρινε ως νέα κατηγορία περιουσιακών στοιχείων ενώ πολλοί επενδυτές βλέπουν τα κρυπτονομίσματα ως αντιστάθμιση του πληθωρισμού. Ωστόσο, σε ατομικό μέτωπο, τα κρυπτονομίσματα μπορεί να έχουν τη δυνατότητα να διαταράξουν τη ζωή μας, όπως έκαναν το Διαδίκτυο και τα κινητά τηλέφωνα όλα αυτά τα χρόνια. Ο στόχος των κινητών τηλεφώνων ήταν να επιτρέψουν στους ανθρώπους να επικοινωνούν σε μια απόσταση χιλιομέτρων. Το Διαδίκτυο ήρθε με στόχο την ανταλλαγή γνώσεων μέσω μιας κοινώς προσβάσιμης πλατφόρμας. Αργότερα και τα δύο έγιναν μέρος της ζωής μας και άλλαξαν κάθε πτυχή της. Στο οικονομικό μέτωπο, το κρυπτονόμισμα μπορεί ενδεχομένως να διαταράξει τις οικονομίες με την ικανότητά του να επιφέρει ζημίες στις κεντρικές τράπεζες. Μπορούμε να εξετάσουμε το παράδειγμα του δικτύου bitcoin εδώ. Πρώτον, το Bitcoin δεν μπορεί να είναι προϊόν double-spending καθώς είναι μοναδικό και ασφαλές μέσω κρυπτογραφίας (Lee et al., 2018).

Έτσι, μπορεί κάποιος να ξοδέψει το ίδιο bitcoin δύο φορές. Τα double spending νομίσματα, προσπαθούν να λύσουν το μαθηματικό πρόβλημα double

spending δηλαδή δεν χρειάζεται κάποια αρχή όπως η Κεντρική Τράπεζα να ελέγξει την εγκυρότητα μίας συναλλαγής όπως συνέβαινε μέχρι σήμερα στο οικονομικό μας σύστημα. Δεύτερον, οι αλγόριθμοι υποστηρίζουν την εμπιστοσύνη του bitcoin αν και είναι αποκεντρωμένο. Σημαίνει ότι εκτός εάν οι κόμβοι εγκρίνουν τη συναλλαγή, η συναλλαγή δεν μπορεί να συμπεριληφθεί στο δημόσιο καταναμημένο βιβλίο του Bitcoin. Τρίτον, δεν χρειάζεται ενδιαμέσο για την παραγωγή και τη διανομή του νομίσματος (Lee et al., 2018).

Πολλές κεντρικές τράπεζες σε όλο τον κόσμο υιοθετούν τα στοιχεία του κρυπτονομίσματος για να δημιουργήσουν CBDC (Ψηφιακά Νομίσματα Κεντρικής Τράπεζας). Έτσι, τα κρυπτονομίσματα μπορεί να έχουν τη δυνατότητα να αλλάξουν τον τρόπο λειτουργίας της οικονομίας. Ωστόσο τα κρυπτονομίσματα παρά τα όποια προβλήματα γίνονται όλο και πιο δημοφιλή. Από τον Μάρτιο του 2020, το ψηφιακό νόμισμα έχει αυξηθεί οκτώ φορές. Το 2020, η πανδημία Covid-19 αναστάτωσε τις οικονομίες σε όλο τον κόσμο, αναγκάζοντάς τους να επιβάλουν αυστηρά lockdown για μεγάλο χρονικό διάστημα. Είχε επίσης καταστροφικές συνέπειες στην παγκόσμια οικονομία, με σημαντική πτώση των τιμών των περιουσιακών στοιχείων. Οι αυξανόμενοι φόβοι δημιούργησαν ένα ακραίο περιβάλλον για την αποδοχή των κρυπτονομισμάτων. Με την περιορισμένη προσφορά κρυπτονομισμάτων όπως το Bitcoin, η αξία του Bitcoin αυξήθηκε. Οι επενδυτές φαίνεται ότι επιλέγουν την αστάθεια παρά μια μονόπλευρη αγορά. Με αρκετή μεταβλητότητα, η φήμη για τα κρυπτονομίσματα αυξήθηκε πολλαπλάσια. Όσον δε, αφορά το πως ανταποκρίνονται οι χώρες στα κρυπτονομίσματα, η συνολική ανταπόκριση στις κεντρικές τράπεζες διαφόρων χωρών είναι χλιαρή. Ενώ ορισμένες χώρες υποστηρίζουν ιδιαίτερα τα κρυπτονομίσματα, άλλες κεντρικές τράπεζες είναι προσεκτικές λόγω των ακραίων επιπέδων αστάθειας. Οι έλεγχοι σε θέματα κεφαλαίου και φορολογίας έχουν αυξήσει τις ανησυχίες και τις απαντήσεις. Ωστόσο, πολλές μεγάλες τράπεζες προσβλέπουν στην ανάπτυξη των κρυπτονομισμάτων για να ταιριάζουν με το εκσυγχρονισμένο χρηματοπιστωτικό σύστημα και να επιταχύνονται οι πληρωμές (Hong & Yoon, 2022).

Παρά τα όποια προβλήματα συνδέονται με την κυκλοφορία και τη χρήση τους, σε γενικές γραμμές τα κρυπτονομίσματα μπορούν ωστόσο να ωφελήσουν τον οικονομικό κόσμο. Αυτό γιατί, καταρχάς, δεν απαιτείται μεσάζων για την ανταλλαγή κρυπτονομισμάτων γεγονός που οδηγεί σε αύξηση της ταχύτητας των συναλλαγών. Παράλληλα, δεδομένου ότι δεν υπάρχουν μεσάζοντες, το κόστος συναλλαγής είναι χαμηλότερο. Το χαμηλότερο κόστος συναλλαγής συνεπάγεται αποτελεσματικότητα στην ανταλλαγή και αύξηση του όγκου των συναλλαγών. Επιπρόσθετα, υπάρχει λιγότερη ανάγκη για μια φυσική δομή όπου οι άνθρωποι θα έρχονται και θα συναλλάσσονται ενώ παράλληλα, το πάγιο κόστος είναι χαμηλότερο λόγω της μη απαίτησης μισθών, εξόδων ενοικίου ή λογαριασμών κοινής ωφελείας. Υπάρχουν ακόμη και έμποροι χωρίς κριτήριο ελάχιστης απαίτησης κατάθεσης (Hong & Yoon, 2022).

Επιπλέον, δεν υπάρχουν γεωγραφικά εμπόδια στα κρυπτονομίσματα. Έτσι, δεν υπάρχει κεντρική υπηρεσία για την παρακολούθηση των συναλλαγών. Αυτό διευκολύνει το εύκολο και γρήγορο εμπόριο για τις εταιρείες. Από τον Νοέμβριο του 2021 ένα bitcoin διαπραγματεύεται στα 59.150 \$ ενώ σήμερα η τιμή ανέρχεται στα 28.339 \$. Αυτό σημαίνει ότι πολλοί άνθρωποι δεν θα μπορούσαν να αγοράσουν ούτε ένα bitcoin. Ως εκ τούτου, οι επενδυτές μπορούν να αγοράσουν κλάσματα κρυπτονομισμάτων, γεγονός που ενισχύει περαιτέρω τον όγκο και τη σκοπιμότητα των συναλλαγών. Ένα ακόμη πλεονέκτημα των κρυπτονομισμάτων που βοηθά την οικονομία είναι ότι τα κρυπτονομίσματα μπορούν να γίνουν κοινά νομίσματα μεταξύ των οικονομιών, διευκολύνοντας περισσότερο το εμπόριο (Hong & Yoon, 2022).

Ένα δίκτυο peer-to-peer υποστηρίζει το σύστημα blockchain των κρυπτονομισμάτων. Έτσι, οι συναλλαγές είναι αποκεντρωμένες, σε αντίθεση με το παραδοσιακό χρηματοπιστωτικό σύστημα. Ο χρήστης κρυπτονομισμάτων πιστεύει ότι θα πρέπει να έχει τον απόλυτο έλεγχο των χρημάτων του αντί για έναν τραπεζίτη. Επίσης, οι πολυεθνικές οντότητες συνήθως λαμβάνουν δάνεια σε εγχώρια αλλά και σε ξένα νομίσματα. Η προσθήκη της επιλογής

Κρυπτονομισμάτων μπορεί να διαφοροποιήσει την έκθεση. Έτσι, τα κρυπτονομίσματα μπορούν να παρέχουν πρόσβαση σε ένα διαφοροποιημένο χαρτοφυλάκιο δανείων. Επιπλέον, οι πληροφορίες αποστολέα και παραλήπτη διατηρούνται εμπιστευτικές. Εκτός από αυτό υπάρχουν πολλά επίπεδα ασφαλείας γύρω από τις πληροφορίες που αυξάνουν τη δραστηριότητα στον τομέα των κρυπτονομισμάτων (Liu et al., 2018).

Οι επιχειρηματίες μπορούν να λαμβάνουν πληρωμές σε περισσότερα νομίσματα. Τους βοηθά να έχουν καλύτερη οικονομική κάλυψη και μια απελευθερωμένη οικονομική σύνδεση. Το δίκτυο κρυπτονομισμάτων υποστηρίζεται από τεχνολογία καταμεμημένης λογιστικής ενώ επίσης είναι αυτοματοποιημένο και ψηφιοποιημένο σύστημα. Έτσι, εξαλείφει τον κίνδυνο απάτης και διαφθοράς, το μεγαλύτερο πρόβλημα στο παραδοσιακό χρηματοπιστωτικό σύστημα καθώς ούτε εταιρείες ούτε ιδιώτες μπορούν να το χειραγωγήσουν (Liu et al., 2018).

Ο ρόλος των κρυπτονομισμάτων είναι επίσης σημαντικός για να καταστεί δυνατή η παγκόσμια χρηματοοικονομική ένταξη. Ειδικά στις αναπτυσσόμενες χώρες, τα κρυπτονομίσματα βοηθούν στην αγορά των πόρων και στην παροχή χρηματοοικονομικών υπηρεσιών λόγω της δυνατότητας γρήγορης πρόσβασής τους. Ως εκ τούτου, επιταχύνει την οικονομική και κοινωνική ανάπτυξη της παγκόσμιας οικονομίας (Madey, 2020).

Το σύστημα είναι αποκεντρωμένο, δηλαδή δεν βρίσκεται υπό τον έλεγχο ενός και μόνο προσώπου ή αρχής. Έτσι, ούτε εταιρείες ούτε ιδιώτες μπορούν να το εκμεταλλευτούν, σε αντίθεση με το παραδοσιακό χρηματοπιστωτικό σύστημα, γεγονός που με τη σειρά του, εκτός των άλλων, μειώνει την πιθανότητα απάτης. Τα κρυπτονομίσματα είναι πολύ χρήσιμα για τις αναπτυσσόμενες οικονομίες, καθώς μπορούν να αυξήσουν την οικονομική και κοινωνική τους θέση. Οι επιχειρηματίες αποκτούν περισσότερο έλεγχο και, ως εκ τούτου, η πρόσβαση στο κεφάλαιο γίνεται πολύ πιο εύκολη λόγω της έλευσης των τεχνολογιών blockchain

παράγοντες που από κοινού, συμβάλλουν στην άνοδο των οικονομικών δραστηριοτήτων (Madey, 2020).

Η οικονομία που βασίζεται σε κρυπτογράφηση κινείται προς την ανοικτή πηγή, την παγκόσμια πρόσβαση σε όλους ανεξαρτήτως εθνικότητας ή κοινωνικοοικονομικής κατάστασης. Η παγκόσμια χρηματοοικονομική ένταξη λόγω των κρυπτονομισμάτων μπορεί να παρέχει πρόσβαση σε κρίσιμα χρηματοοικονομικά προϊόντα σε πάνω από 1,8 δισεκατομμύρια ανθρώπους σε όλο τον κόσμο που έχουν παραμείνει χωρίς τραπεζικές υπηρεσίες. Εκτιμάται ότι το ετήσιο ΑΕΠ θα ενισχύσει κατά 3,9 τρισεκατομμύρια δολάρια τις αναδυόμενες οικονομίες (Park & Park, 2021).

Τα έργα blockchain αναπτύσσονται επίσης στη διαχείριση δεδομένων ηλεκτρικής ενέργειας και στο εμπόριο εμπορευμάτων. Η τεχνολογία Blockchain συμβάλλει στην αύξηση της ταχύτητας και της αποτελεσματικότητας σε πραγματικό χρόνο μαζί με τη διαφάνεια. Έτσι, το blockchain θα αυξήσει τον ρυθμό μετάδοσης. Χωρίς καμία ανάγκη για μεσάζοντα, το blockchain μπορεί να καταγράφει και να διακανονίζει συναλλαγές συναλλαγών ενέργειας, ενώ παράλληλα, δεδομένου ότι όλα τα μέρη χρησιμοποιούν την ίδια πλατφόρμα, δεν υπάρχει ανάγκη συμβατότητας (Park & Park, 2021).

1.5. Blockchain

Με λίγα λόγια, ένα blockchain είναι μια ψηφιακή συνεχώς αυξανόμενη λίστα εγγραφών δεδομένων. Πρόκειται ουσιαστικά για ένα μητρώο (ledger) στο οποίο αποθηκεύονται κι επαληθεύονται πληροφορίες και δεδομένα. Μια τέτοια λίστα αποτελείται από πολλά μπλοκ δεδομένων, τα οποία είναι οργανωμένα με χρονολογική σειρά και συνδέονται και ασφαλιζονται με κρυπτογραφικές αποδείξεις και με τέτοιο τρόπο ώστε να δημιουργείται μία συνεχής αλυσίδα δεδομένων, ενώ κάθε τροποποίηση μίας πληροφορίας που έχει καταγραφεί στο

μητρώο να επηρεάζει αναγκαστικά όλες τις μεταγενέστερες καταχωρήσεις (Casino et al., 2018).

Το πρώτο πρωτότυπο μιας blockchain χρονολογείται στις αρχές της δεκαετίας του 1990, όταν ο επιστήμονας υπολογιστών Stuart Haber και ο φυσικός W. Scott Stornetta εφάρμοσαν κρυπτογραφικές τεχνικές σε μια αλυσίδα μπλοκ ως τρόπο για να προστατεύσουν τα ψηφιακά έγγραφα από παραποίηση δεδομένων. Η δουλειά των Haber και Stornetta σίγουρα ενέπνευσε τη δουλειά των Dave Bayer, Hal Finney και πολλών άλλων επιστημόνων υπολογιστών και λάτρεις της κρυπτογραφίας - που τελικά οδήγησαν στη δημιουργία του Bitcoin, ως του πρώτου αποκεντρωμένου συστήματος ηλεκτρονικών μετρητών (ή απλά του πρώτου κρυπτονομίσματος). (Catalini & Gans, 2016).

Αν και η τεχνολογία blockchain είναι παλαιότερη από το Bitcoin, αποτελεί βασικό υποκείμενο στοιχείο των περισσότερων δικτύων κρυπτονομισμάτων, ενεργώντας ως αποκεντρωμένο, κατακεντρωμένο και δημόσιο ψηφιακό βιβλίο που είναι υπεύθυνο για την τήρηση μόνιμου αρχείου (αλυσίδα μπλοκ) όλων των προηγουμένως επιβεβαιωμένων συναλλαγών (Christidis & Devetsikiotis, 2016).

Οι συναλλαγές blockchain πραγματοποιούνται μέσα σε ένα peer-to-peer δίκτυο υπολογιστών (κόμβων) που κατανέμονται παγκοσμίως. Κάθε κόμβος διατηρεί ένα αντίγραφο του blockchain και συμβάλλει στη λειτουργία και την ασφάλεια του δικτύου. Αυτό είναι που κάνει το Bitcoin ένα αποκεντρωμένο ψηφιακό νόμισμα χωρίς σύνορα, που δεν απαιτεί διαμεσολάβηση τρίτων (Conley, 2017).

Ως τεχνολογία κατακεντρωμένης λογιστικής (DLT) το blockchain έχει σχεδιαστεί σκόπιμα ώστε να είναι εξαιρετικά ανθεκτικό σε τροποποιήσεις και απάτες (όπως η διπλή δαπάνη, δηλαδή αν ένας κακόβουλος χρήστης προσπαθήσει να ξοδέψει τα bitcoins του σε δύο διαφορετικούς παραλήπτες ταυτοχρόνως). Αυτό ισχύει επειδή το blockchain του Bitcoin, ως βάση δεδομένων εγγραφών, δεν μπορεί να αλλοιωθεί, ούτε να παραποιηθεί χωρίς μια μη πρακτική ποσότητα ηλεκτρικής ενέργειας και υπολογιστικής ισχύος - πράγμα που σημαίνει ότι το δίκτυο μπορεί να

επιβάλει την έννοια των "πρωτότυπων" ψηφιακών εγγράφων, καθιστώντας Το Bitcoin μια πολύ μοναδική και μη αντιγράψιμη μορφή ψηφιακού νομίσματος (Dai et al., 2018).

Ο λεγόμενος αλγόριθμος συναίνεσης Proof of Work είναι αυτός που έδωσε τη δυνατότητα στο Bitcoin να κατασκευαστεί ως σύστημα Ανοχής Βυζαντινών Σφαλμάτων (BFT), που σημαίνει ότι το blockchain του είναι σε θέση να λειτουργεί συνεχώς ως κατανεμημένο δίκτυο, ακόμη και αν ορισμένοι από τους συμμετέχοντες (κόμβοι) παρουσιάζουν ανέντιμη συμπεριφορά ή αναποτελεσματική λειτουργικότητα. Ανοχή Βυζαντινών Σφαλμάτων (BFT) είναι ιδιοκτησία ενός συστήματος που είναι σε θέση να αντισταθεί στην κατηγορία των αποτυχιών, που προέρχονται από το πρόβλημα των Βυζαντινών Στρατηγών. Αυτό σημαίνει ότι ένα σύστημα BFT είναι σε θέση να συνεχίσει να λειτουργεί ακόμη και αν ορισμένοι από τους κόμβους αποτύχουν ή ενεργούν κακόβουλα (Dell'Erba, 2018).

Ο αλγόριθμος συναίνεσης Proof of Work είναι βασικό στοιχείο της διαδικασίας εξόρυξης Bitcoin. Η τεχνολογία του blockchain μπορεί επίσης να προσαρμοστεί και να εφαρμοστεί σε άλλες δραστηριότητες, όπως η υγειονομική περίθαλψη, η ασφάλιση, η εφοδιαστική αλυσίδα, το IOT κ.λπ. Αν και σχεδιάστηκε για να λειτουργεί ως κατανεμημένο καθολικό (σε αποκεντρωμένα συστήματα), μπορεί επίσης να αναπτυχθεί σε κεντρικά συστήματα ως ένας τρόπος για να διασφαλιστεί η ακεραιότητα των δεδομένων ή να μειωθεί το λειτουργικό κόστος (Deshpande et al., 2017).

ΚΕΦΑΛΑΙΟ 2 ΤΟ BITCOIN ΩΣ ΕΠΕΝΔΥΣΗ

2.1. Από τις εφαρμογές εικονικού χρήματος στο Bitcoin

Το Bitcoin είναι ένα ψηφιακό νόμισμα, το οποίο χρησιμοποιεί τεχνικές κρυπτογράφησης προκειμένου να ρυθμίζει την δημιουργία νέων μονάδων νομίσματος και να επιβεβαιώσει τη μεταφορά ποσών, χωρίς ταυτόχρονα να ελέγχεται από κάποια ρυθμιστική αρχή, που στο παραδοσιακό σύστημα τον ρόλο αυτό έχει η κεντρική τράπεζα. Όταν κάνουμε λόγο για "τεχνικές κρυπτογράφησης", εννοούμε το τρόπο με τον οποίο καθιστούμε μια πληροφορία απροσπέλαστη στα μάτια τρίτων, εκτός εάν διαθέτουν το κατάλληλο "κλειδί" για να αποκτήσουν πρόσβαση σε αυτή. Το Bitcoin αποτελεί ένα αποκεντρωμένο ομότιμο (peer-to-peer) δίκτυο. Το ομότιμο δίκτυο ορίζεται ως ένα δίκτυο υπολογιστών στο οποίο όλοι οι υπολογιστές (peers) που συμμετέχουν σε αυτό, θεωρούνται ισότιμοι. Αυτό σημαίνει ότι δεν υπάρχει ένας κεντρικός διαχειριστής ή ένα κεντρικό σημείο ελέγχου (Luther, 2016).

Το εικονικό χρήμα έχει εμφανισθεί σε διαφορετικές περιόδους κατά τη διάρκεια της ιστορίας του ανθρώπινου πολιτισμού και συχνά παρέμεινε για μεγάλες χρονικές περιόδους προτού αντικατασταθεί από «απτές» εναλλακτικές λύσεις χρημάτων, για να αντικατασταθεί από το εικονικό χρήμα σε αυτό που έχει περιγραφεί ως σειρά μακροχρόνιων κύκλων χρηματικών μέσων και χρέους. Ακόμη και εντός της συγκεκριμένης κατηγορίας των μέσων ψηφιακών μετρητών, ορισμένα είδη ψηφιακών νομισμάτων υπήρχαν πριν από το Bitcoin, αλλά δεν είχαν λάβει την κεντρική ή εξέχουσα θέση ότι το Bitcoin θα υιοθετούσε τελικά. Παρά τις μοναδικές προτάσεις του Bitcoin, υπήρχαν άλλα ψηφιακά νομισματικά μέσα σε κυκλοφορία στη διαδικτυακή σφαίρα που είχαν χαρακτηριστικά παρόμοια με το Bitcoin (όπως Proof of Work (PoW) ή η ψηφιακή σπανιότητα digital scarcity). (Luther, 2016).

Το Proof of Work (PoW) εμφανίστηκε στις αρχές της δεκαετίας του 1990 ως μέσο για τον περιορισμό των ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου. Η ιδέα ήταν ότι οι υπολογιστές ενδέχεται να χρειαστούν να εκτελέσουν μια μικρή εργασία πριν από την αποστολή email. Αυτό το έργο θα ήταν ασήμαντο για κάποιον που στέλνει ένα νόμιμο email, αλλά θα απαιτούσε πολύ υπολογιστική ισχύ και πόρους για τους χρήστες που στέλνουν μαζικά email πιθανών spam. Παράλληλα η ψηφιακή σπανιότητα (digital scarcity) αποτελεί ένα μέσο που επιτυγχάνει την δυνατότητα αυθεντικοποίησης ψηφιακού περιεχομένου, δημιουργώντας μία τεχνητή (ψηφιακή) σπανιότητα και προσδίδοντας κατ' αυτόν τον τρόπο (προστιθέμενη) αξία σε ένα «πρωτότυπο» ψηφιακό αντίτυπο (tokenization --> commodification of digital content). (Warden, 2019).

Το ecash των Chaum and Brands είναι το παλαιότερο παράδειγμα, ενώ ο Adam Back είχε δημιουργήσει ένα σύστημα απόδειξης εργασίας για τον έλεγχο ανεπιθύμητης αλληλογραφίας γνωστό ως hashcash. Ο αλγόριθμος απόδειξης εργασίας στο hashcash αναπτύχθηκε περαιτέρω σε ένα επαναχρησιμοποιήσιμο πρωτόκολλο απόδειξης εργασίας (RPOW) από τον Hal Finney (Warden, 2019).

Οι προτάσεις για κρυπτονομίσματα που είχαν διανεμίει την ψηφιακή σπανιότητα περιλάμβαναν το B-Money (Wei Dai) και το Bit Gold (Nick Szabo). Το πρόβλημα των συλλεκτικών μηχανισμών που βασίζονται στην αγορά για τον έλεγχο του πληθωρισμού νομισμάτων ήταν μέρος της πρότασης της Bit Gold, όπως και άλλες θετικές πτυχές όπως ένα μητρώο περιουσιακών στοιχείων με ανοχή σε σφάλματα, το οποίο ήταν σχεδιασμένο για να αποθηκεύει και να μεταφέρει ασφαλείς λύσεις απόδειξης εργασίας (Liu et al., 2018).

Ωστόσο, ενώ υπήρξαν πρόδρομοι του Bitcoin, ήταν ο Satoshi Nakamoto, ο δημιουργός του Bitcoin, ο οποίος για πρώτη φορά εφάρμοσε την τεχνολογία σε ένα σύστημα ψηφιακών χρημάτων στο white paper του Bitcoin. Με αυτούς τους καινοτόμους να βάζουν τις βάσεις, το ίδιο το Bitcoin, δημιουργήθηκε από ένα ψευδώνυμο άτομο ή οντότητα γνωστό ως Satoshi Nakamoto. Ο Wei Dai και ο Hal Finney είχε υποτεθεί εκείνη τη στιγμή ότι ήταν οι πράκτορες πίσω από την

ονομασία Satoshi Nakamoto, αλλά εξέδωσαν αρνητικές δηλώσεις ότι επρόκειτο για αυτούς (DeVries, 2016).

Ο Nakamoto δημοσίευσε ένα έγγραφο σε μια λίστα αλληλογραφίας κρυπτογραφίας το 2008 με τον τίτλο «Bitcoin: A Peer-to-Peer Electronic Cash System», (Nakamoto 2008). Αυτό το έγγραφο παρουσίασε το σχήμα για ένα δίκτυο peer-to-peer που θα ενθάρρυνε ένα «σύστημα ηλεκτρονικών συναλλαγών χωρίς να βασίζεται στην εμπιστοσύνη» (Nakamoto 2008). Το έγγραφο, παρουσίασε την έννοια της τεχνολογίας blockchain και το Bitcoin περιγράφηκε ως ψηφιακός πόρος και σύστημα ανοικτού κώδικα (open source system). Αυτό πρακτικά σημαίνει ότι κανείς δεν είναι ιδιοκτήτης του και ότι καθένας μπορεί να συμμετέχει στη χρήση και την εξέλιξή του (DeVries, 2016).

Το υποκείμενο μήνυμα ήταν ότι τα στοιχεία της εμπιστοσύνης, της λογοδοσίας ή της επίβλεψης, που χαρακτήριζαν το εμπόριο και τις συναλλαγές/ανταλλαγές χρήματος σε όλη την ιστορία, θα αντικατασταθούν από ένα σύστημα που απλώς δεν θα χρειαζόταν να γνωρίζουν οι συναλλασσόμενοι πράκτορες. Χρησιμοποιώντας το πλαίσιο της έλλειψης εμπιστοσύνης, το σχέδιο του Nakamoto, έλυσε το πρόβλημα της διπλής δαπάνης και το πρόβλημα των βυζαντινών στρατηγών (Byzantine generals problem) ² με έναν εξαιρετικά δημιουργικό τρόπο. Η πρόταση του Nakamoto, ενώ ήταν τόσο αξιοσημείωτη, στην πραγματικότητα δεν είχε την προσοχή που της άξιζε (DeVries, 2016).

² Το πρόβλημα της δημιουργίας ενός πλήρως κατανεμημένου και ταυτόχρονα έμπιστου συστήματος δεν είναι καινούργιο στη επιστήμη των υπολογιστών. Στα κατανεμημένα συστήματα η επιβολή εμπιστοσύνης δημιουργεί την ανάγκη μελέτης των ανοχών στα σφάλματα. Φανταστείτε ένα υπολογιστικό σύστημα με διανεμημένα στοιχεία τα οποία πρέπει να ανταλλάσσουν πληροφορίες μεταξύ τους, αλλά αυτές μπορεί να μην είναι ακριβείς (ή και να μην υπάρχουν) λόγω τεχνικών αστοχιών. Το "Πρόβλημα των βυζαντινών στρατηγών" περιγράφηκε αρχικά από τους Marshall Pease, Robert Shostak και Leslie Lamport το 1982 και περιέχει μια πολύ στυλιζαριμένη περιγραφή του προβλήματος.

2.2. Η εκκίνηση του Bitcoin

Μετά τη διάδοση της εργασίας (Nakamoto 2008), η πραγματική πλατφόρμα για τις συναλλαγές Bitcoin δημιουργήθηκε μέσω της κυκλοφορίας του πρώτου Bitcoin-Client ανοιχτού κώδικα και της ταυτόχρονης έκδοσης Bitcoin. Ο Nakamoto εξόρυξε το πρώτο μπλοκ Bitcoin με ανταμοιβή 50 Bitcoin. Αυτό το μπλοκ αναφέρεται συνήθως ως «μπλοκ γένεσης». Ο Hal Finney ήταν ο πρώτος άνθρωπος που έτρεξε το λογισμικό Bitcoin μετά τον Satoshi Nakamoto και ήταν βασικός προγραμματιστής κατά τον πρώτο χρόνο ζωής αυτού του κρυπτονομίσματος και έλαβε τα πρώτα 10 Bitcoin από τον Nakamoto, τα οποία αντιπροσώπευαν την πρώτη συναλλαγή Bitcoin στην ιστορία. Ο Nick Szabo και ο Wei Dai εξέφρασαν επίσης ισχυρή υποστήριξη για το Bitcoin μετά την κυκλοφορία του. Ο ίδιος ο Nakamoto εξόρυξε ένα ποσό περίπου 1 εκατομμυρίου Bitcoin, πριν εξαφανιστεί και διακόψει την εμπλοκή του με το κίνημα Bitcoin. Ειδικότερα, τον Δεκέμβριο του 2010, ο Satoshi Nakamoto δημοσίευσε το τελευταίο δημόσιο μήνυμά του στο online forum ονόματι bitcointalk. Έγραψε μερικές μικρολεπτομέρειες σχετικά με την τελευταία έκδοση του λογισμικού. Έπειτα, διατήρησε επαφή με κάποιους προγραμματιστές μέσω email, αλλά τα ίχνη του έχουν χαθεί εντελώς από τον Απρίλιο του 2011. Είναι πιθανό ότι η ταυτότητα του θα παραμείνει για πάντα ένα μυστήριο (Dierksmeier & Seele, 2016).

Ο Gavin Andresen έγινε ο κύριος προγραμματιστής στο Bitcoin Foundation και στη συνέχεια έγινε το ισοδύναμο του «δημόσιου προσώπου» του Bitcoin. Ο Andresen αρχικά αγόρασε 10.000 Bitcoin για 50 δολάρια και δημιούργησε την ιστοσελίδα με το όνομα, μέσω της οποίας δώριζε Bitcoin. Στη συνέχεια εξελίχθηκε σε έναν από τους πρωτεργάτες για την ανάπτυξη του κορυφαίου κρυπτονομίσματος.

Στις αρχικές φάσεις κυκλοφορίας, η νομισματική αξία του Bitcoin επιτεύχθηκε μέσω μιας διαδικασίας διαπραγμάτευσης στην αρχική αγορά, όπως για παράδειγμα όταν 10.000 Bitcoin χρησιμοποιήθηκαν για την αγορά (έμμεσα) για

δυο πίτσες, από τον Papa Johns. Σε αυτήν την πρώιμη συγκυρία, παρά την φαινομενική ευπάθεια του συστήματος, ανακαλύφθηκε μόνο μία σημαντική ευπάθεια, η οποία οδήγησε στην υπερπαραγωγή 180 δισεκατομμυρίων Bitcoin. Ωστόσο, αυτά τα νομίσματα αφαιρέθηκαν από το blockchain και ένα ενημερωμένο πρωτόκολλο ασφαλείας αντιμετώπισε το πρόβλημα (Dierksmeier & Seele, 2016).

Ο ανοιχτός κώδικας του Bitcoin βοήθησε άλλους προγραμματιστές κρυπτονομισμάτων να δημιουργήσουν εναλλακτικά νομίσματα με βάση τον κώδικά του. Οι πρώτοι χρήστες του Bitcoin για συναλλακτικούς σκοπούς περιλάμβαναν το Wikileaks (δωρεές) και το Electronic Frontier Foundation. Το 2011, κυκλοφόρησε μια δημοσίευση που σχετίζεται με το Bitcoin, στο Bitcoin Magazine. Το Bitcoin εμφανίστηκε και στην ψυχαγωγία, όπως στη δραματική σειρά του CBS The Good Wife. Η εκπομπή υπαινίχθηκε ότι το Bitcoin δεν ήταν ένα «αληθινό νόμισμα». Το 2012, ξεκίνησε το Ίδρυμα Bitcoin για να επικεντρωθεί στην τυποποίηση, την προστασία και την προώθηση του Bitcoin. Μέχρι το 2012, η παγκόσμια υπηρεσία πληρωμών Bitcoin Bit Pay ανέφερε ότι 1000+ έμποροι δέχονταν Bitcoin στο πλαίσιο της υπηρεσίας επεξεργασίας πληρωμών της. Το 2013, η Coinbase, ένας άλλος επεξεργαστής πληρωμών, ανακοίνωσε ότι πούλησε Bitcoin αξίας 1 εκατομμυρίου \$ (USD) σε ένα μήνα, με ισοδύναμο ανά μονάδα άνω των 22 \$ ανά Bitcoin. Μέχρι το 2013, το Bitcoin άρχισε να μπαίνει στο ραντάρ των ρυθμιστικών φορέων παγκοσμίως και είχε αυξηθεί σε όγκο. Εκείνο το έτος, συνέβησαν πολλά περιστατικά που σχετίζονται με τις συναλλαγές, συμπεριλαμβανομένου του διαχωρισμού της αλυσίδας σε δύο δίκτυα Bitcoin και καθυστερήσεων επεξεργασίας λόγω ανεπαρκούς χωρητικότητας, που οδήγησε σε απότομες πτώσεις των τιμών και ακόμη και σε προσωρινή διακοπή των εμπορικών συναλλαγών με bitcoin (Dierksmeier & Seele, 2016).

Στις ΗΠΑ, το American Financial Crimes Enforcement Network (FinCEN) θέσπισε ρυθμιστικές κατευθυντήριες γραμμές για αποκεντρωμένα εικονικά νομίσματα (συμπεριλαμβανομένου του Bitcoin). Ταξινόμησαν δε τις αμερικάνικες εταιρείες- εξορύκτες Bitcoin που θα πουλούσαν παραγόμενα Bitcoin ως

Επιχειρήσεις Υπηρεσιών Χρημάτων (MSB), ως υποκείμενες σε νομικές υποχρεώσεις, συμπεριλαμβανομένης της εγγραφής τους σε ένα σύστημα μητρώου. Η παραβίαση αυτών των αποφάσεων, συγκεκριμένα η μη εγγραφή των σχετικών επιχειρήσεων στο μητρώο, είχε ως αποτέλεσμα οι αρχές των ΗΠΑ να κατάσχουν λογαριασμούς που σχετίζονται με το χρηματιστήριο. Νέες επιχειρήσεις όπως ο ιστότοπος γνωριμιών OkCupid και η υπηρεσία παραγγελιών φαγητού Foodler άρχισαν να δέχονται Bitcoin. Μια μικρή τάση προς μονοπώληση της επεξεργασίας Bitcoin άρχισε να παρατηρείται όταν σημειώθηκε ότι η εταιρεία BitInstant επεξεργαζόταν περίπου το 30% των εισερχόμενων και εξερχόμενων συναλλαγών από παραδοσιακά χρήματα σε Bitcoin και ότι το BitInstant έκανε περισσότερες από 30.000 συναλλαγές σε ένα μήνα . Οι αμερικανικές αρχές επιβολής του νόμου βρήκαν Bitcoins που χρησιμοποιούνται σε διάφορα περιστατικά και έρευνες, όπως όταν η Υπηρεσία Δίωξης Ναρκωτικών (DEA) είχε αναφέρει Bitcoins ως κατασχεθέν περιουσιακό στοιχείο σε μια ειδοποίηση κατάσχεσης του Υπουργείου Δικαιοσύνης των Ηνωμένων Πολιτειών (Andolfatto & Spewak, 2019).

Στις αναπτυσσόμενες χώρες όπως για παράδειγμα στην Κένυα, σύντομα ξεκίνησαν έργα για τη σύνδεση των πληρωμών Bitcoin με συστήματα ισχυρών υποδομών, με σκοπό την τόνωση της οικονομικής ανάπτυξης στον αναπτυσσόμενο κόσμο. Εν τω μεταξύ, η Robocoin και η Bitcoiniaacs κυκλοφόρησαν μαζί την πρώτη στον κόσμο Αυτοματοποιημένη Ταμειακή Μηχανή (ATM) Bitcoin στις 29 Οκτωβρίου 2013 στο Βανκούβερ του Καναδά, η οποία επέτρεπε στους πελάτες να πουλήσουν ή να αγοράσουν νόμισμα Bitcoin σε ένα καφέ στο κέντρο της πόλης (Andolfatto & Spewak, 2019).

Οι ρυθμιστικές απαντήσεις των χωρών ωστόσο προς το Bitcoin άρχισαν να αποκλίνουν σημαντικά το 2013. Στην Ταϊλάνδη, το Τμήμα Διαχείρισης Συναλλάγματος και Πολιτικής απονομιμοποίησε το Bitcoin δηλώνοντας ότι εφεξής θα ήταν παράνομο δεδομένου ότι στερείται νομικού πλαισίου. Εν τω μεταξύ, ο ομοσπονδιακός δικαστής της Ανατολικής Περιφέρειας του Τέξας έκρινε ότι τα Bitcoin είναι «ένα νόμισμα ή μια μορφή χρήματος» όπως ορίζεται από τους

ομοσπονδιακούς νόμους περί κινητών αξιών και ως εκ τούτου υπόκεινται στη δικαιοδοσία του δικαστηρίου. Ταυτόχρονα, το Υπουργείο Οικονομικών της Γερμανίας χαρακτήρισε τα Bitcoin με τον όρο «μονάδα λογαριασμού»—ένα χρηματοπιστωτικό μέσο—αν και όχι ως ηλεκτρονικό χρήμα ή λειτουργικό νόμισμα, μια ταξινόμηση ωστόσο που έχει νομικές και φορολογικές επιπτώσεις (Dierksmeier & Seele, 2016).

Τον Οκτώβριο του 2013, το FBI κατάσχεσε περίπου 30.000 Bitcoin κατά τη σύλληψη του ιδιοκτήτη της ιστοσελίδας Silk Road. Η Κίνα έγινε το μεγαλύτερο σημείο ανταλλαγής για Bitcoin το 2013, όταν το BTC China έγινε το μεγαλύτερο ανταλλακτήριο σε όγκο bitcoin. Ωστόσο, η νομισματική αρχή της Λαϊκής Τράπεζας της Κίνας απαγόρευσε στα κύρια κινεζικά χρηματοπιστωτικά ιδρύματα να χρησιμοποιούν Bitcoin τον Δεκέμβριο του 2013, οδηγώντας σε πτώση της αξίας του μέσου. Μια ακόμη μεγαλύτερη ποικιλία επιχειρήσεων άρχισε να δέχεται Bitcoin το 2014, συμπεριλαμβανομένων των Zynga, D Las Vegas Casinos, Golden Gate Hotel & Casino, TigerDirect, Overstock.com, Newegg, Dell και Microsoft. Επιπλέον, τα παράγωγα προϊόντα που βασίζονται σε Bitcoin εμφανίστηκαν το 2014, όταν το TeraExchange έλαβε έγκριση από την Επιτροπή Συναλλαγών Συμβάσεων Μελλοντικής Εκπλήρωσης Εμπορευμάτων των ΗΠΑ (CFTC) για να αρχίσει να καταχωρίζει ένα εξωχρηματιστηριακό προϊόν ανταλλαγής του οποίου το υποκείμενο περιουσιακό στοιχείο ήταν η τιμή ενός Bitcoin. Μια κρίση στην κυκλοφορία των bitcoin, προέκυψε όταν η Ιαπωνική Mt. Gox ανέφερε την κλοπή 744.000 Bitcoin και κήρυξε πτώχευση, μετά από μήνες δυσκολιών που αναφέρθηκαν για τους χρήστες. Ένα άλλο hack συνέβη το επόμενο έτος στο βρετανικό χρηματιστήριο Bitstamp, το οποίο ανέφερε ότι είχαν κλαπεί 19.000 Bitcoin από το πορτοφόλι τους (5 εκατομμύρια δολάρια την εποχή εκείνη). Σε αντίθεση με το Mt Gox, το Bitstamp συνέχισε τις συναλλαγές μετά από ένα μικρό διάστημα (Andolfatto & Spewak, 2019).

Μέχρι το 2015, ο αριθμός των εμπόρων παγκοσμίως που συναλλάσσονταν με bitcoin είχε διογκωθεί σε περίπου 180.000. Οι εταιρείες που σχετίζονται με

ψηφιακά νομίσματα συνέχισαν να τραβούν την προσοχή των χρηματοδοτών από τις κύριες αγορές, όπως όταν η 21 Inc η οποία συγκέντρωσε 121 εκατομμύρια δολάρια (USD) σε χρηματοδότηση επιχειρηματικού κεφαλαίου. Η παγκόσμια επέκταση των συναλλαγών που σχετίζονται με το Bitcoin συνέχισε την σταθερή άνοδό της το 2016. Μέχρι τον Σεπτέμβριο του 2016 υπήρχαν 813 ATM παγκοσμίως που εξυπηρετούσαν Bitcoin. Τον Μάρτιο του 2016, το Υπουργικό Συμβούλιο της Ιαπωνίας αναγνώρισε εικονικά νομίσματα όπως το Bitcoin ως λειτουργικά παρόμοια με τα πραγματικά χρήματα. Η μεγαλύτερη διαδικτυακή αγορά της Νότιας Αφρικής, η Bidorbuy ξεκίνησε πληρωμές Bitcoin τόσο για αγοραστές όσο και για πωλητές. Στην Αργεντινή, η Uber μεταπήδησε στο Bitcoin αφού η κυβέρνηση απαγόρευσε τις εταιρείες πιστωτικών καρτών να συναλλάσσονται με την Uber. Όσον αφορά το hacking, το μεγάλο γραφείο συμψηφισμού Bitfinex ανέφερε ότι είχαν κλαπεί 124.000 Bitcoin, που ισοδυναμούν με 60 εκατομμύρια δολάρια (USD) εκείνη την εποχή. Χαρακτηριστικό της καθυστέρησης του ακαδημαϊκού κόσμου στην ανταπόκριση για το bitcoin ήταν ότι μόλις το 2016 κυκλοφόρησε το πρώτο περιοδικό που σχετίζεται με κρυπτονομίσματα, το Ledger (Dierksmeier & Seele, 2016).

2.4. Η φούσκα του Bitcoin το 2017

Στα τέλη του 2017, η τιμή του Bitcoin αυξήθηκε σε δυσθεώρητα επίπεδα, οδηγώντας σε τεράστιο όγκο κερδοσκοπικής δραστηριότητας, μαζί με μια φρενίτιδα ειδήσεων και κάλυψης στα μέσα κοινωνικής δικτύωσης. Στις 17 Δεκεμβρίου 2017 η τιμή του ξεπέρασε το όριο των 19.000 δολαρίων και οι νεότεροι συμμετέχοντες, μαζί με την αισιοδοξία για περαιτέρω νομιμοποίηση και τυποποίηση, οδήγησαν σε μια πηγή ενδιαφέροντος για το bitcoin. Για πολλούς από τους πρώτους που υιοθέτησαν το Bitcoin, φάνηκε ότι είχε ξεκινήσει μια ακώλυτη πορεία προς τη γενική νομιμοποίηση. Οι νεότερες υπηρεσίες, μαζί με τις ανταλλαγές και τα νέα νομίσματα, άρχισαν να σπέρνουν τους σπόρους μιας

ευφορικής διάθεσης, καθώς η πρακτική που ονομάστηκε FOMO, στην οποία πολλοί άνθρωποι, ιδιαίτερα οι millennials, ένιωσαν την ανάγκη να οδηγηθούν στη φρενίτιδα. Το FOMO (Fear of Missing Out) που υπήρξε μια αιτία ανόδου του Bitcoin, είναι ο φόβος των επενδυτών να μείνουν έξω από το ράλι λέγεται επίσης ότι βρίσκεται πίσω από την έκρηξη που σημειώνεται στο κρυπτονόμισμα (Abubakar et al., 2018).

Έτσι, άρχισαν να εμφανίζονται βίντεο σχετικά με τους «Εκατομμυριούχους Bitcoin» που οδηγούν γρήγορα και ακριβά αυτοκίνητα κλπ. Ο αναβρασμός της φούσκας ήταν αισθητός στο Twitter και σε άλλα μέσα ενημέρωσης, προαναγγέλλοντας την αυγή μιας νέας οικονομικής εποχής κατά την οποία το Bitcoin θα εκτόπιζε όλες τις υπάρχουσες δομές χρήματος. Ωστόσο, μέχρι τις 22 Δεκεμβρίου 2017, η τιμή του Bitcoin, είχε καταρρεύσει κατά 47%. Μεγάλο μέρος των επενδυτών που ακολούθησαν τη διαφημιστική εκστρατεία ένιωσαν σοκ, η ευφορία τους αμβλύθηκε, μετά από αντιφατικά σήματα και θόρυβο που εξαπλώθηκαν σε όλα τα κανάλια. Από τη μία πλευρά, πολλοί υποστηρικτές συνέχισαν να υποστηρίζουν ότι αυτή ήταν μια μικρή περίοδος προβλημάτων, και ότι η υπόθεση για το Bitcoin ήταν αποφασιστική. Από την άλλη πλευρά, οι αρνητές είδαν στις μειώσεις ένα σημάδι ότι είχε διαιωμιστεί μια τεράστια απάτη και ότι τα κρυπτονομίσματα ως νέα μορφή χρήματος είχαν αρχίσει πλέον να καταρρέουν. Στη μέση βρέθηκαν εκείνοι που μόλις είχαν αρχίσει να ενδιαφέρονται για το θέμα των κρυπτονομισμάτων, αλλά, μη κατανοώντας απαραίτητα την πολυπλοκότητα ενός αναδυόμενου πεδίου, άρχισαν να κάνουν δεύτερες σκέψεις και ένιωσαν προδομένοι από τις ξαφνικές μειώσεις (Abubakar et al., 2018).

Το Bitcoin ήταν ένα μέσο που σε εκείνη την περίοδο που άρχισε ξαφνικά να χαρακτηρίζεται από σημαντική αστάθεια, δεδομένου ότι δεν είχε φτάσει μέχρι τότε σε ένα τέτοιο επίπεδο ώστε να έχει επιτύχει βαθιά ρευστότητα. Πολλοί επενδυτές δεν μπορούσαν να απολαύσουν την αστάθεια που ήταν ενσωματωμένη σε αυτό που ήταν ακόμα ένα σχετικά νέο μέσο. Στις 12 Ιανουαρίου 2018, άρχισαν να διαδίδονται φήμες ότι η Νότια Κορέα, που μέχρι τότε θεωρούνταν δικαιοδοσία

επιδεκτική σε κρυπτονομίσματα με βάση το θεσμικό πλαίσιο που είχε εισαγάγει, μπορεί να ετοιμάζεται να απαγορεύσει τις συναλλαγές κρυπτονομισμάτων. Αυτό έκανε το Bitcoin να χάσει περαιτέρω 12%. Δύο εβδομάδες αργότερα, η μεγαλύτερη εξωχρηματιστηριακή αγορά κρυπτονομισμάτων της Ιαπωνίας η Coincheck δήλωσε ότι είχαν κλαπεί 530 εκατομμύρια δολάρια κρυπτονομισμάτων από χάκερ. Αυτό ήταν το μεγαλύτερο περιστατικό κλοπής σε κρυπτονομίσματα μέχρι εκείνη την εποχή, αναγκάζοντας το Coincheck να αναστείλει τις συναλλαγές σε Bitcoin. Η τιμή του Bitcoin τέθηκε υπό περαιτέρω πίεση εξαιτίας αυτής της εξέλιξης (Abubakar et al., 2018).

Ρίχνοντας κι περαιτέρω λάδι στη φωτιά, στις 7 Μαρτίου 2018, η cryptoexchange Binance δήλωσε ότι είχαν χρησιμοποιηθεί παραβιασμένα κλειδιά API για τη διεξαγωγή παράτυπων συναλλαγών, δημιουργώντας περαιτέρω αμφιβολίες σχετικά με την ανθεκτικότητα του χώρου. Με μια τόσο δραματική πτώση των τιμών μετά από μια τόσο γρήγορη άνοδο, το Great Bitcoin Crash άφησε αυτό που κάποιοι πίστευαν ότι θα ήταν ανεξίτηλο σημάδι στα κρυπτονομίσματα, μειώνοντας τη νομιμότητά τους και απεικονίζοντας το Bitcoin ως ένα ιδιότροπο νόμισμα χωρίς βιώσιμη χρήση. Στα τέλη Μαρτίου, μεγάλες εταιρείες διαδικτύου, όπως το Facebook, το Twitter και η Google αποφάσισαν να απαγορεύσουν τις διαφημίσεις για Bitcoin, σημειώνοντας τον τεράστιο όγκο κερδοσκοπίας και ψευδούς μάρκετινγκ που γίνονται από εταιρείες του χώρου. Το Bitcoin εισήλθε έτσι σε μια μακρά περίοδο ύφεσης και μέχρι τον Νοέμβριο του 2018, η τιμή του Bitcoin έπεσε στα 5.500 δολάρια ενώ η κεφαλαιοποίηση της αγοράς του έπεσε κάτω από τα 100 δισεκατομμύρια δολάρια για πρώτη φορά από την αρχική ανοδική πορεία του 2017. Στο μεταξύ, οι ρυθμιστικές αρχές σε όλο τον κόσμο είχαν αρχίσει να αντιλαμβάνονται την ισχύ του Bitcoin ως εναλλακτικού νομίσματος και κατηγορίας περιουσιακών στοιχείων, και οι ομάδες τους είχαν εξετάσει προσεκτικά τη φύση του κύκλου άνθησης και κατάρρευσης που είχε υποστεί το Bitcoin. Είχαν επίσης πλήρη επίγνωση της εγγενούς αστάθειας του Bitcoin ως περιουσιακού στοιχείου και αντιμετώπισαν αυξημένη δημόσια πίεση λόγω των απωλειών που υπέστη η μερίδα του ευρύτερου κοινού που κατείχε κρυπτονομίσματα. Την περίοδο

που το Bitcoin ανέβαινε (μέσα έως τέλη 2017) δεν υπήρχε μεγάλη ζήτηση από το κοινό για ρυθμιστική εποπτεία και λογοδοσία, αλλά μόλις έσκασε η φούσκα, ακούστηκαν πολλά παράπονα από τους επενδυτές Bitcoin, για τις απώλειες που υπέστησαν (Andolfatto & Spewak, 2018).

Στις Ηνωμένες Πολιτείες, οι προληπτικές ρυθμιστικές προσπάθειες από την Επιτροπή Κεφαλαιαγοράς (SEC) και την Επιτροπή Συναλλαγών Εμπορευμάτων και Μελλοντικής Εκπλήρωσης (CFTC), οδήγησαν σε πρωτοποριακές δράσεις για τη διαμόρφωση του κυβερνητικού ρόλου στη ρύθμιση του Bitcoin. Για το αμερικανικό πλαίσιο, τα δύο μεγαλύτερα κρυπτονομίσματα κατά κεφαλαιοποίηση αγοράς, το Bitcoin και ο Ether, αντιμετωπίστηκαν ως εμπορεύματα και υπήχθησαν στην αρμοδιότητα του CFTC. Μια σημαντική προσπάθεια οδήγησε επίσης το Υπουργείο Δικαιοσύνης των ΗΠΑ, σε συνεργασία με άλλα ιδρύματα, για την καταπολέμηση του ξεπλύματος χρήματος και την καταπολέμηση της χρηματοδότησης της τρομοκρατίας, να προβούν στην υιοθέτηση σχετικού ρυθμιστικού πλαισίου. Σε αυτήν την περίοδο, τα σχετικά προβλήματα άρχισαν να γίνονται πιο εμφανή, καθώς ανακαλύπτονταν όλο και περισσότερο ότι κάποιοι χρησιμοποιούν το Bitcoin και άλλα νομίσματα για παράνομες ή κακόβουλες δραστηριότητες (Andolfatto & Spewak, 2018).

Αυτή η δυσμενής πτυχή, ωστόσο, δεν ανάγκασε τις ΗΠΑ να απαγορεύσουν εντελώς το Bitcoin. Αντίθετα, οι διάφορες αρχές ακολούθησαν μια διαφοροποιημένη προσέγγιση που εξισορρόπησε τις δημόσιες αξίες της καινοτομίας και της λογοδοσίας. Διάφορες άλλες κυβερνήσεις ακολούθησαν το παράδειγμά τους με τις δικές τους μελέτες και πιλοτικά έργα και κατέληξαν σε διαφορετικά συμπεράσματα σχετικά με τη νομιμότητα του Bitcoin και άλλων νομισμάτων. Ορισμένες χώρες ήταν ανοιχτά εχθρικές προς την ιδέα του Bitcoin και των κρυπτονομισμάτων γενικότερα, κάποιες άλλες ακολούθησαν μια χλιαρή και τεχνικά προσανατολισμένη προσέγγιση, ενώ άλλες γενικά ασπάστηκαν την ιδέα. Η μεγαλύτερη σαφήνεια με βάση τους κανονισμούς σχετικά με την κατάσταση του Bitcoin βοήθησε στη δημιουργία ενδιαφέροντος του ιδιωτικού τομέα για νέες ιδέες

βασισμένες σε blockchain που αφορούσαν την κύρια χρηματοδότηση. Αρχικά, οι θεσμικοί επενδυτές ήταν κάπως διστακτικοί να εισέλθουν στο χώρο και πολλοί managers της χρηματοπιστωτικής βιομηχανίας επέκριναν το Bitcoin ως «απάτη». (Bouri et al., 2020).

Αργότερα, ωστόσο, οι κύριοι θεσμικοί επενδυτές ενθάρρυναν την ιδέα σε διάφορους βαθμούς και οι θεσμικοί επενδυτές άρχισαν να επινοούν στρατηγικές και μέσα για να εισέλθουν στην αγορά, είτε μέσω παραγώγων, κεφαλαίων δεικτών, διαφοροποιημένων προϊόντων ή άλλων μέσων. Αυτό αποτέλεσε μια θετική εξέλιξη στον χώρο των κρυπτονομισμάτων από ορισμένες απόψεις. Από τη μία πλευρά, υπήρχε μια ευπρόσδεκτη προσδοκία ωρίμανσης του κλάδου, με τη ροή κεφαλαίων να οδηγεί σε μείωση της αστάθειας (λόγω υψηλότερου όγκου) και την προσέλκυση πιο δύσπιστων χρηστών (είτε άτομα είτε οργανισμούς) που σκέφτονταν να ξεκινήσουν να συμμετάσχουν στην αγορά Bitcoin. Ταυτόχρονα, άρχισαν να χρησιμοποιούνται νεότερες εκδόσεις του Bitcoin, που αποτέλεσαν τις νέες παραλλαγές από το αρχικό Bitcoin. Οι δημοφιλείς παραλλαγές περιλαμβάνουν τα προϊόντα Bitcoin Cash, Bitcoin Gold, Bitcoin XT, Bitcoin Classic. Κανένα από τα προϊόντα αυτά, ωστόσο, δεν έχει κεντρίσει ως σήμερα, ένα ενδιαφέρον σχεδόν συγκρίσιμο με αυτό του αρχικού Bitcoin, με ορισμένες παραλλαγές να έχουν μάλιστα εξαφανιστεί. Αντίθετα, εκτός από το Bitcoin, είναι άλλα κρυπτονομίσματα (ιδιαίτερα το Ether) που έχουν κερδίσει έδαφος (Andolfatto & Spewak, 2018).

2.5. Το Bitcoin στην περίοδο της πανδημίας

Αφού παρέμεινε σε ένα κενό για μια περίοδο μετά την κατάρρευση του Bitcoin του 2018, και με σημαντική πώλωση μεταξύ των υποστηρικτών και εξίσου σκεπτικιστών και αντιπάλων, συνέβη μια κρίσιμη συγκυρία το 2020 που θα οδηγούσε το Bitcoin σε άνευ προηγουμένου ύψη δημόσιου ενδιαφέροντος και επιτυχία της επένδυσης: η πανδημία Covid-19. Η πανδημία χρησίμευσε ως

εκδήλωση εστίασης για τα κρυπτονομίσματα σε πολλά επίπεδα. Πρώτον, υπήρχε η κοινωνική και ψυχολογική πτυχή του lockdown και του περιορισμού, που περιόρισε την κινητικότητα πολλών ανθρώπων και τους πρόσφερε ένα πλήρες διάλειμμα από την κανονική τους ζωή (Mnif et al., 2020).

Σε τέτοιες συνθήκες, είχαν ένα νέο χώρο για να εξερευνήσουν θέματα ενδιαφέροντος, όπως τα κρυπτονομίσματα. Κάποιοι πείστηκαν από τα πλεονεκτήματά του, αφού βρήκαν τώρα τον χρόνο να σκεφτούν τι ήταν το blockchain και το Bitcoin και δεδομένου ότι τα κρυπτονομίσματα είναι διαπραγματεύσιμα στο διαδίκτυο και από οποιαδήποτε τοποθεσία, οι περιορισμοί κινητικότητας δεν εμπόδισαν επίσης την απορρόφησή τους. Δεύτερον, υπήρξε μια άνευ προηγουμένου ώθηση από τις κυβερνήσεις, ιδιαίτερα (αλλά όχι αποκλειστικά) στον ανεπτυγμένο κόσμο, ως μέσο για να διατηρήσουν τις οικονομίες σε βιώσιμη ανάπτυξη παρά την οξεία παράλυση του μακροοικονομικού συστήματος.

Αυτό το κίνητρο περιλάμβανε άμεσες μεταβιβαστικές πληρωμές σε μεγάλα τμήματα του πληθυσμού τους, ακόμη και σε ομάδες της κοινωνίας που δεν χρειάζονταν το κίνητρο. Τέτοιες ομάδες βρήκαν έτσι πρόσθετο διαθέσιμο εισόδημα και πολλές ομάδες το αξιοποίησαν σε διάφορα περιουσιακά στοιχεία, όπως ακίνητα, μετοχές και κρυπτονομίσματα. Ωστόσο, πρέπει να σημειωθεί ότι η αρχική έκρηξη ήρθε το 2020 στην αγορά μετοχών, ακολουθούμενη από τα ακίνητα και στη συνέχεια τα κρυπτονομίσματα τελευταία (με τη σειρά). Η κεφαλαιοποίηση του Bitcoin εκτοξεύτηκε από 0,2 \$ στις αρχές του 2020 σε σχεδόν 1 τρισεκατομμύριο \$ μέχρι τα τέλη του 2021, μια εκπληκτική άνοδος σε τόσο σύντομο χρονικό διάστημα. Πολλοί σκεπτικιστές των κρυπτονομισμάτων αυτή τη στιγμή διατήρησαν μια κάπως χαμηλών τόνων στάση, ειδικά καθώς άρχισε να εμφανίζεται μια ευρύτερη υιοθέτηση, μεταξύ άλλων από θεσμικά κόμματα, μαζί με μια πολύ ισχυρότερη μεσαία και πολιτιστική παρουσία (ιδιαίτερα στα μέσα κοινωνικής δικτύωσης). Ένας αυξανόμενος αριθμός μεγάλων και μικρών επενδυτών άρχισε να βλέπει το Bitcoin ως νόμιμο διαφοροποιητή στα επενδυτικά τους χαρτοφυλάκια και μια λιγότερο τεχνολογικά έμπειρη ομάδα μεταξύ του παγκόσμιου πληθυσμού

βρήκε το ηλεκτρονικό εμπόριο και άλλες τεχνολογίες χρήσιμες για την πρόσβαση σε κρυπτονομίσματα είτε μέσω άμεσων είτε έμμεσων μέσων (Mnif et al., 2020).

Η εισαγωγή των stablecoin, ως ενδιάμεσων ψηφιακών νομισματικών μέσων, βοήθησε επίσης τους επενδυτές να ασχοληθούν με κρυπτονομίσματα με ελαφρώς μικρότερη μεταβλητότητα και ένα επιπλέον επίπεδο μετατρεψιμότητας. Ακόμη και σε χώρες όπου το Bitcoin δεν ήταν απαραίτητα νόμιμο, οι όγκοι συναλλαγών ήταν δεκάδες δισεκατομμύρια δολάρια. Αλλά μια ιδιαίτερα πρωτοποριακή προσέγγιση υιοθετήθηκε από το Ελ Σαλβαδόρ για να αντιμετωπίσει το Bitcoin ως νόμιμο χρήμα, στο ίδιο επίπεδο με το κρατικό του νόμισμα. Αυτό χαιρετίστηκε ως μια πρωτοποριακή χειρονομία, και μια χειρονομία που αντιμετωπίστηκε με χειροκρότημα στην κοινότητα των κρυπτονομισμάτων. Ωστόσο, το Ελ Σαλβαδόρ αντιμετώπισε τουλάχιστον τρεις μεγάλες προκλήσεις μετά την ανακοίνωση της κίνησης:

δημοσιονομική κρίση, προκλήσεις που βασίζονται σε εμβάσματα και προσβασιμότητα (καθημερινές συναλλαγές). Παρά τις προκλήσεις αυτές, η χώρα προχώρησε σε αυτήν την προσπάθεια. Αλλά την ίδια στιγμή που ορισμένες χώρες άρχισαν να εκφράζουν ισχυρότερη στήριξη για το Bitcoin (με το Ελ Σαλβαδόρ πρωτοπόρο), ορισμένες μεγάλες οικονομίες άρχισαν να απομακρύνονται από τα κρυπτονομίσματα. Το πιο σημαντικό από αυτή την άποψη ήταν η Κίνα, η οποία είχε υιοθετήσει μια σταδιακή προσέγγιση για την απαγόρευση του νομίσματος και αντ' αυτού πρόσφερε ένα Ψηφιακό Νόμισμα της Κεντρικής Τράπεζας (CBDC), το οποίο κοινώς αναφέρεται ως Ψηφιακό Γιουάν. Αυτό το CBDC χρησιμοποιήθηκε πιλοτικά κατά τη διάρκεια της πανδημίας και η υποδοχή φαινόταν ευνοϊκή. Τα πλεονεκτήματα του Bitcoin, ως αποκεντρωμένου και ανώνυμου δικτύου peer-to-peer, ωστόσο, δεν ισχύουν για τα CBDC, κάτι που θεωρείται πλεονέκτημα ή μειονέκτημα ανάλογα από την οπτική εξέτασης. Ωστόσο, η αυξανόμενη παλίρροια των CBDCs αποτελεί μια μακροπρόθεσμη πρόκληση για το Bitcoin (Mnif et al., 2020).

Η έννοια της ανωνυμίας τέθηκε επίσης υπό αμφισβήτηση κατά τη διάρκεια της πανδημίας, χάρη στις μνημειώδεις προσπάθειες των αρχών επιβολής του νόμου, ιδιαίτερα στις Ηνωμένες Πολιτείες, να κυνηγήσουν τους χάκερ και τους επιτιθέμενους που επέλεξαν να χρησιμοποιήσουν το Bitcoin ως μέσο πληρωμής τους. Οι επιτιθέμενοι ransomware, ειδικότερα, αντιλήφθηκαν το Bitcoin ως ένα χρήσιμο μέσο μέσω του οποίου εκβιάζουν τα μέρη με αντάλλαγμα την επιστροφή των παραβιασμένων περιουσιακών στοιχείων. Το πιο διάσημο παράδειγμα ήταν η διακοπή λειτουργίας του Continental Pipeline, ενός βασικού τμήματος υποδομής στην ανατολική ακτή των ΗΠΑ, το οποίο παραβιάστηκε από ransomware. Οι αμερικανικές υπηρεσίες, ωστόσο, κατάφεραν όχι μόνο να εντοπίσουν τους σαμποτέρ, αλλά και να ανακτήσουν το Bitcoin που πληρώθηκε. Αυτό το γεγονός αντιπροσώπευε μια σημαντική υπόθεση για την κατάρριψη του μύθου της ανωνυμίας: ενώ τα κρυπτονομίσματα είναι δύσκολο να εντοπιστούν, δεν είναι ακατόρθωτο (Mnif et al., 2020).

Εν τω μεταξύ, ο διεθνής συντονισμός για την επιβολή του νόμου και την επίβλεψη του Bitcoin και άλλων κρυπτονομισμάτων έγινε πολύ ισχυρότερος κατά τη διάρκεια της πανδημίας. Η Ειδική Ομάδα Χρηματοοικονομικής Δράσης (FATF), για παράδειγμα, εξέδωσε αυστηρές κατευθυντήριες γραμμές προκειμένου οι χώρες να συμμορφώνονται με βέλτιστες πρακτικές, συμπεριλαμβανομένου ενός καινοτόμου «ταξιδιωτικού κανόνα» που ορίζει τη θεμελίωση της κατοχής κρυπτονομισμάτων σε παραδοσιακά τραπεζικά συστήματα σε κινήσεις μεταξύ των χωρών. Άλλοι διεθνείς και πολυμερείς θεσμοί στάθμισαν επίσης το ζήτημα του Bitcoin και της χρήσης του, εγείροντας έτσι ερωτήματα σχετικά με την αποδοχή του από τη μία πλευρά και επιβεβαιώνοντας επίσης την ιδέα ότι το Bitcoin ωρίμαζε ως ιδέα, από την άλλη. Ως εκ τούτου, θα μπορούσε κανείς να παρατηρήσει μια εμβάθυνση της γνωσιακής βάσης σχετικά με τα κρυπτονομίσματα, καθώς και μια πόλωση των πολιτικών από την άλλη. Υπήρξε επίσης μια έκρηξη νέων καινοτομιών, ή μάλλον εκλαΐκευση των υπαρχουσών τεχνολογιών, που συνέβη κατά τη διάρκεια της πανδημίας, η οποία οφείλει μια γένεση στο Bitcoin καθώς βασιζόταν στην εξέλιξη του blockchain (Mnif et al., 2020).

Αν και υπάρχουν πολλά σε αυτήν τη λίστα, μερικά παραδείγματα αρκούν: Web 3.0, NFT και DeFi. Κάθε τεχνολογία προσφέρει διάφορους βαθμούς υπόσχεσης και ανησυχίας για τους επενδυτές και για ρυθμιστικές αρχές, αλλά αυτές οι τεχνολογίες είναι πολύ πιθανό να εξελιχθούν σε σημαντικούς τομείς καινοτομίας τα επόμενα 10 χρόνια. Επιπλέον, προηγούμενα παράγωγα του υποκείμενου blockchain του Bitcoin, όπως dApps, DAOs κλπ., έχουν επίσης προχωρήσει σε κάπως μεγαλύτερη ωρίμανση. Επομένως, παρά την επιτυχία του ίδιου του Bitcoin, υπάρχει μια αναταραχή ανάπτυξης σε πολλούς διαφορετικούς τομείς αυτή τη στιγμή, η οποία αποδίδεται στον κοινό πρόγονο του Bitcoin. Σε έναν κόσμο μετά την πανδημία, μπορεί να υπάρξουν ωστόσο πολλές νέες επαναλήψεις, μαζί με τεχνολογίες που δεν έχουν ακόμη σχεδιαστεί, οι οποίες πιθανότατα θα έρθουν στο προσκήνιο και θα ωθήσουν περισσότερο την κυκλοφορία και υιοθέτηση του Bitcoin (Mnif et al., 2020).

ΚΕΦΑΛΑΙΟ 4 ΕΥΚΑΙΡΙΕΣ ΠΡΟΒΛΗΜΑΤΙΣΜΟΙ ΚΑΙ ΠΡΟΚΛΗΣΕΙΣ

Παρά την τεράστια αποδοχή και άνοδο της κυκλοφορίας των κρυπτονομισμάτων γενικά και του Bitcoin υπήρξαν και αρκετοί επικριτές του κρυπτονομίσματος, ένας από αυτούς είναι εάν είναι μια μορφή στοιχείων του ενεργητικού/περιουσιακό στοιχείο. Στην τρέχουσα μορφή του, έχοντας τη δυνατότητα να εκτελεί νομισματική συναλλαγή, σύμφωνα με τον Kim (2017), το bitcoin και τα κρυπτονομίσματα γενικά είναι πολύ πιο κοντά και ανταποκρίνονται στον ορισμό του νομίσματος.

4.1. Ευκαιρίες και Πλεονεκτήματα

Όντας ένα σχετικά νέο προϊόν, οι ευκαιρίες του κρυπτονομίσματος φαίνονται πολλά υποσχόμενες. Παρά την κλιμάκωση ως προς την τιμή και την αξία του, οι καρποί και οι μελλοντικές ευκαιρίες εξακολουθούν πάντως να αποτελούν ζητούμενο. Ακολουθεί συζήτηση σχετικά με τις ρεαλιστικές ευκαιρίες των κρυπτονομισμάτων για τους χρήστες, τους επενδυτές συμπεριλαμβανομένης και της κυβέρνησης.

4.1.1. Ασφαλής Τεχνολογία

Το blockchain θεωρείται μια από τις καλύτερες πλατφόρμες καθώς και η πιο εξελιγμένη τεχνολογία από την ανακάλυψη του Διαδικτύου. Παρέχει αποτελεσματικότητα για τις ηλεκτρονικές συναλλαγές, όσον αφορά την ασφάλεια και το απόρρητό της. Οι Ying et al. (2018) στη μελέτη περίπτωσης τους κατέληξαν στο συμπέρασμα ότι, εκτός από το ότι επιτρέπει τη χρήση κρυπτονομισμάτων, το

blockchain είναι σε θέση να προστατεύει εμπιστευτικές πληροφορίες και επίσης να εξαλείφει τη διαμεσολάβηση από οποιονδήποτε οργανισμό, παρόλο που υπήρχαν αναφορές που ανέφεραν ότι το Bitcoin βρέθηκε να αποκαλύπτει το 40% της ταυτότητας του χρήστη. Το ζήτημα του απορρήτου της ταυτότητας είναι σημαντικό στοιχείο με βάση τα χαρακτηριστικά του κρυπτονομίσματος που προστατεύουν το προφίλ του χρήστη μέσω του συστήματος αποκέντρωσης. Δύο προβλήματα πάντως στις σχετικές έρευνες που κατέληξαν σε αυτό το συμπέρασμα, είναι ότι δεν χρησιμοποιούν πραγματικό σύστημα blockchain αλλά προσομοίωση. Εκτός από αυτό, δεν υπάρχουν άλλες μελέτες μέχρι σήμερα τουλάχιστον, που να έχουν αποκαλύψει τα ελαττώματα της χρήσης Bitcoin και κρυπτονομισμάτων και τα οποία παρουσιάζουν τον κίνδυνο έκθεσης των προσωπικών πληροφοριών και δεδομένων του χρήστη.

Ένας από τους κινδύνους στην κατοχή ψηφιακών νομισμάτων και του Bitcoin ειδικότερα, είναι η διπλή συναλλαγή, που σημαίνει ότι κάποιος μπορεί να εκδώσει δύο συναλλαγές παράλληλες χορηγώντας το ίδιο νόμισμα σε δύο διαφορετικούς παραλήπτες. Στην περίπτωση της κεντρικής και διαδικτυακής συναλλαγής, το τραπεζικό λειτουργικό σύστημα είναι σε θέση να ανιχνεύσει τέτοια ύποπτη δραστηριότητα. Η τεχνολογία blockchain είναι ιδιαίτερος ασφαλής ωστόσο. Αυτό σημαίνει ότι οι απατεώνες δεν μπορούν να διαπράξουν τέτοιο έγκλημα επειδή δεν μπορεί κανείς να αλλάξει ή να επικυρώσει πολλά λογιστικά βιβλία ταυτόχρονα. Σύμφωνα με έναν ισχυρισμό των Benton et al. (2014), η ασφάλεια του κρυπτονομίσματος μπορεί να σπάσει πάντως, εάν οι απατεώνες είναι σε θέση να ελέγξουν ένα τεράστιο ποσό συμμετοχής στην απόδειξη της ισχύος κατακερματισμού εργασίας. Η ισχύς κατακερματισμού είναι η ικανότητα ελέγχου της υπολογιστικής ισχύος. Οι Kurihara & Fukushima (2017) δήλωσαν ότι η ισχύς κατακερματισμού είναι η ισχύς που χρειάζεται το δίκτυο κρυπτονομισμάτων για να λειτουργεί συνεχώς. Η ισχύς κατακερματισμού υπολογίζεται κατά μέσο όρο σε 10 λεπτά που καταναλώνεται η ισχύς. Ελέγχοντας το μεγαλύτερο μέρος του μεριδίου στην απόδειξη της εργασίας, οι απατεώνες μπορούν να δαπανήσουν διπλά στο ίδιο μπλοκ προετοιμάζοντας κρυφά το blockchain εκ των προτέρων πριν το

μεταδώσουν στο δίκτυο της αλυσίδας. Θεωρητικά, η απάτη μπορεί να γίνει σε μεγάλη κλίμακα, υπό την προϋπόθεση ότι οι απατεώνες μπορούν να ελέγχουν σε ένα συγκεκριμένο ποσοστό την ισχύ κατακερματισμού. Από τον σχετικό αλγόριθμο ο απατεώνας μπορεί να διπλασιάσει τις δαπάνες εάν ελέγχει το 51% της υπολογιστικής ισχύος (Shi, 2016).

Στο πρωτόκολλο απόδειξης εργασίας, η επαλήθευση του εάν υπάρχει διπλή συναλλαγή ή όχι βασίζεται αποκλειστικά στην ισχύ κατακερματισμού, αντί της πιθανότητας πολλαπλών πλαστών ταυτοτήτων. Αυτό έχει διασφαλίσει ότι το ζήτημα των απατεώνων που μπορούν να ελέγχουν την πλειονότητα της ισχύος κατακερματισμού υπονομεύεται από την επαλήθευση άλλης μεθόδου αντί να στηρίζονται αποκλειστικά στην ισχύ κατακερματισμού. Η υπόθεση είναι ότι είναι πολύ πιο δύσκολο να ελέγξεις την πλειοψηφία της ισχύος κατακερματισμού του συστήματος από τον έλεγχο των ταυτοτήτων της πλειοψηφίας (Kurihara & Fukushima, 2017)/

Ο αλγόριθμος κρυπτονομισμάτων είναι πιο ασφαλής και είναι καλύτερος από τη χρήση πιστωτικών καρτών. Παρόλο που δεν έχει ακόμη μελετηθεί, τα κρυπτονομίσματα έχουν πολύ χαμηλότερες χρεώσεις επεξεργασίας με την ασφαλή συναλλαγή που παρέχουν. Ο Van Alstyne (2014) εξήγησε ότι η χρήση κρυπτονομισμάτων είναι πιο ασφαλής όταν οι χρήστες προβαίνουν σε συναλλαγές. Ο μηχανισμός μεταφοράς κρυπτονομισμάτων γίνεται με έλεγχο ταυτότητας από τους αγοραστές και τους πωλητές. Ο έλεγχος ταυτότητας μεταξύ των δύο μερών θα αποτρέψει τους απατεώνες να πλαστογραφήσουν οποιαδήποτε νέα συναλλαγή ή να καθυστερήσουν οποιαδήποτε συναλλαγή επιστροφής χρημάτων. Σε σύγκριση με την πιστωτική κάρτα, η όλη διαδικασία είναι όπως προτείνεται από διάφορους ερευνητές, πιο ασφαλής. Η τεχνολογία πίσω από τη συναλλαγή με πιστωτική κάρτα λειτουργεί εντός του κατόχου της κάρτας, του εμπόρου, της εμπορικής τράπεζας, του δικτύου πιστωτικών καρτών, της εκδότριας τράπεζας και του παρόχου υπηρεσιών (Van Alstyne, 2014).

Για κάθε μεμονωμένη συναλλαγή, η διαδικασία είναι πιο περίπλοκη από ό,τι φαίνεται. Πρέπει να περάσει σε όλες αυτές τις οντότητες προτού οριστικοποιηθεί μια συναλλαγή. Είναι βέβαια γεγονός ότι ευκαιρίες για διάπραξη απάτης μπορεί να υπάρχουν σε οποιοδήποτε από αυτά τα στάδια. Παρόλο που έχουν ληφθεί ορισμένα μέτρα για τη μείωση της απάτης με πιστωτικές κάρτες το σύστημα είναι πιο εύαλωτο σε σύγκριση με το blockchain. Το σύστημα που εφαρμόζεται από την τεχνολογία της πιστωτικής κάρτας εξακολουθεί να μην είναι ασφαλές καθώς η τεχνολογία κρυπτογραφίας διαθέτει το κρυπτονόμισμα.

Ο Carrick (2016) δήλωσε ότι παρά το ότι είναι αλγοριθμικά περίπλοκο, το σύστημα blockchain δεν είναι πολύπλοκο, επί της ουσίας. Η πολυπλοκότητα υπάρχει μόνο στον κόμβο και στο μαθηματικό παζλ που επιλύονται με τη διαδικασία εξόρυξης. Εκτός από αυτό, η τεχνολογία blockchain παρέχει χρήσιμες λειτουργίες σε όλους τους χρήστες. Είναι απίθανο να προηγηθεί ενός χαοτικού συστήματος που βασίζεται στην ανθεκτικότητα και τη μη αναστρεψιμότητα. Τα αρχεία ψηφιακών εγγράφων στο διαδίκτυο και η ταυτοποίηση διατηρούνται καλά στο σύστημα blockchain για τώρα και στο εγγύς μέλλον.

4.1.2. Κόστος Συναλλαγής

Σε όλη την ιστορία, οι άνθρωποι χρησιμοποιούν κάποιο είδος χρηματικού τύπου, για καθημερινές συναλλαγές. Ιστορικά το σύστημα ανταλλαγής ξεκίνησε όταν οι άνθρωποι αντάλασσαν ή ανταλλάσσουν έως και σήμερα τα αγαθά τους, με τη συμφωνία και από τις δύο πλευρές. Καθώς ο χρόνος περνούσε, σχεδιάστηκε το παραστατικό χρήμα (fiat money) ή αλλιώς χρήμα αναγκαστικής κυκλοφορίας το οποίο είναι το μέσον πληρωμής και το οποίο δεν καλύπτεται από αποθεματικό άλλων υλικών για να μπορούν οι άνθρωποι να συναλλάσσονται με ευκολία. Καθώς ο κόσμος μπήκε στον 21ο αιώνα, τα κρυπτονομίσματα, κατέκλυσαν την αγορά. Έτσι, υπήρξαν και βεβαίως συνεχίζουν να υπάρχουν και σήμερα, μεγάλες πολυεθνικές εταιρείες που χρησιμοποιούν το Bitcoin ως τη μορφή νομίσματός

τους, και το χρησιμοποιούν ακόμη και για να πληρώνουν τους μηνιαίους μισθούς των εργαζομένων (Nakamoto, 2019).

Με το τρέχον κόστος συναλλαγής, οι χρεώσεις συναλλαγών σε κρυπτονομίσματα και Bitcoin είναι χαμηλότερες σε σύγκριση με άλλα κανονικά νομίσματα. Με τα εξέχοντα χαρακτηριστικά του κρυπτονομίσματος, δηλαδή το ότι είναι αποκεντρωμένο και απορρυθμισμένο, τα παραπάνω οφείλονται στο χαμηλό κόστος συναλλαγής του. Είναι γεγονός ότι υπήρξαν σημαντικά ζητήματα στο τρέχον σύστημα πληρωμών που εφαρμόζεται με πιστωτικές κάρτες και κάρτες μισθοδοσίας. Ο τόκος που χρεώνεται για τους χρήστες που αθετούν τις πληρωμές τους είναι πολύ υψηλός και αυτό μπορεί να θέσει σε κίνδυνο έναν χρήστη. Αυτό δεν ισχύει για τα κρυπτονομίσματα, όπου οι συναλλαγές πραγματοποιούνται όταν συμφωνούν οι τελικοί χρήστες και μόνο τότε θα πραγματοποιηθούν τα εμβάσματα (Nakamoto, 2019).

Επιπλέον, το κρυπτονομίσμα μπορεί να λειτουργήσει για 24 ώρες την ημέρα, 7 ημέρες την εβδομάδα όλο το χρόνο. Η τιμολόγηση δεδομένων είναι διαθέσιμη άμεσα, με την οποία οποιοσδήποτε στον κόσμο μπορεί να πραγματοποιήσει συναλλαγές χωρίς κανένα κόστος, εφόσον το διαδίκτυο είναι προσβάσιμο. Καθώς ο κόσμος βομβαρδίζεται με την πρόσφατη ανάπτυξη του Διαδικτύου των πραγμάτων (IoT) και την εξάρτηση από μεγάλα δεδομένα, η δυνατότητα συναλλαγών χωρίς χρονικό περιορισμό είναι μια ευκολία για τους χρήστες. Αυτός ο τρόπος πληρωμής διευκολύνει μεταξύ άλλων και τη νέα γενιά που αναμένεται στο μέλλον να γίνουν ιδιοκτήτες επιχείρησης και να εργαστούν εντός του δικού τους χρονικού πλαισίου, χωρίς να χρειάζεται να εργάζονται στις συμβατικές ώρες εργασίας. Αυτός ο τρόπος συναλλαγών είναι επίσης κατάλληλος για τους γνώστες του Διαδικτύου χωρίς να χρειάζεται να επιβαρυνθούν με επιπλέον κόστος που συνεπάγεται η χρήση άλλου συστήματος πληρωμών (Kurihara & Fukushima, 2017).

4.1.3. Υψηλή απόδοση

Τα διακριτικά χαρακτηριστικά του κρυπτονομίσματος καθώς και του Bitcoin και η ικανότητά του να είναι συμβατό με την οικονομική λειτουργία εν γένει, το καθιστούν μοναδικό περιουσιακό στοιχείο (Briere et al., 2015). Η ιστορία δείχνει ότι το Bitcoin είναι ένα πολύ ασταθές νόμισμα, αλλά έχει σημαντική απόδοση για τους επενδυτές. Εκτός από αυτό, ο κίνδυνος του Bitcoin είναι χαμηλός λόγω της αναλογίας του σε πολλά και διαφοροποιημένα χαρτοφυλάκια. Όπως είναι γνωστό στους επενδυτές, το κέρδος από την επένδυση είναι η αγορά οποιουδήποτε εμπορεύματος σε χαμηλή τιμή και η πώληση σε υψηλές τιμές ((Kurihara & Fukushima, 2017).

Οι Ciaian et al. (2016) μελέτησαν τόσο τους καθοριστικούς παράγοντες του παραδοσιακού νομίσματος της προσφοράς και της ζήτησης όσο και τον σύγχρονο δείκτη όπως η ελκυστικότητα του νομίσματος. Μελέτησαν επίσης την αλληλεπίδραση μεταξύ των καθοριστικών παραγόντων της τιμής. Θεωρείται ότι λόγω της ζήτησης της αγοράς, η τιμή του Bitcoin per se θα αυξηθεί ιδιαίτερα όταν η προσφορά Bitcoin σε κυκλοφορία είναι μεγαλύτερη από αυτή που είναι τώρα. Μετά από κάθε τέσσερα χρόνια, όταν το ποσό του Bitcoin θα μειώνεται στο μισό, σημαίνει ότι θα εισαχθεί μικρότερο νέο Bitcoin, επομένως θα είναι πιο σταθερό. Η σπανιότητα του Bitcoin θα κάνει την τιμή μόνο υψηλότερη, εκτός από το ότι είναι το κύριο νόμισμα που χρησιμοποιείται σε μια παγκόσμια διαπραγματεύση. Σε αυτή τη σταθερή περίοδο, το Bitcoin θα έχει ζήτηση τόσο από επενδυτές όσο και από χρήστες. Ο Kristoufek (2013) έδειξε ότι η τιμή του Bitcoin έχει αυξηθεί, παράλληλα με την αναζήτηση ερωτημάτων στη Wikipedia και στο Google Trends. Δείχνει ότι η ύπαρξη των ερωτημάτων αναζήτησης και της τιμής του Bitcoin είναι στοιχεία που σχετίζονται μεταξύ τους. Αυτό δείχνει ότι καθώς η μάζα γνωρίζει την ύπαρξη κρυπτονομισμάτων και πώς μπορεί να ωφεληθούν από τη χρήση τους, η τιμή θα είναι λογικά υψηλότερη. Στο εγγύς μέλλον, όταν περισσότεροι άνθρωποι θα είναι προσανατολισμένοι στους υπολογιστές και στο διαδίκτυο, η τιμή των

κρυπτονομισμάτων θα σταθεροποιηθεί και έτσι οι άνθρωποι που είχαν κρατήσει τα νομίσματά τους θα καρπωθούν τους καρπούς της επένδυσής τους.

Η χρήση κρυπτονομισμάτων μοιάζει απλώς με τη χρήση χρημάτων fiat ή με τη χρήση πιστωτικών καρτών για την αγορά νόμιμων αγαθών από λιανοπωλητές. Εκτός από αυτό, οι Osterrieder et al., (2016) προτείνουν ότι το Bitcoin μπορεί να χρησιμοποιηθεί για ευρύτερους σκοπούς. Η δημοτικότητα του κρυπτονομίσματος, ειδικότερα του Bitcoin, επιταχύνθηκε περαιτέρω λόγω πολλών ιδιαίτερων γεγονότων που συνεπάγονταν τη χρηστικότητα του, όπως η τραπεζική κρίση στην Κύπρο από το 2012 έως το 2013 και η κρίση του ευρωπαϊκού δημόσιου χρέους (ESDC) του 2010-2013 (Bouri et al., 2017). Η Κύπρος είχε κάνει τα βήματα για τη χρήση κρυπτονομισμάτων για να λάβει ένα πρόγραμμα διάσωσης με εισφορά στις τραπεζικές καταθέσεις. Αυτό οφείλεται στην ανασφάλεια της χρήσης παραδοσιακών νομισμάτων.

Ο Dyhrberg (2016) διαπίστωσε ότι η απόδοση του Bitcoin ήταν σημαντική χρησιμοποιώντας την μέθοδο των χρονοσειρών. Για 8 συνεχόμενες εβδομάδες, διαπιστώθηκε ότι υπήρχε ισχυρή απόδοση στο Bitcoin. Με βάση τις περίφημες θεωρίες περιουσιακών στοιχείων, η πρόβλεψη αποδείχθηκε από τα στοιχεία εμπειρικής συνέχισης και αντιστροφής της απόδοσης με την προβλεψιμότητα της χρονοσειράς. Όπως συζητήθηκε, λόγω της αστάθειας των κρυπτονομισμάτων, η χρονική διάρκεια και η αντιστροφή του Bitcoin ήταν μικρότερη σε σύγκριση με άλλα περιουσιακά στοιχεία. Οι θεσμικοί επενδυτές μπορούν να αποκομίσουν κέρδος επενδύοντας σε Bitcoin και λαμβάνοντας υπόψη το χαρτοφυλάκιό τους σε μετοχές.

4.2. Προκλήσεις

Παρά τις ευκαιρίες που υπάρχουν στο Bitcoin και στα κρυπτονομίσματα γενικότερα, εξακολουθούν να υπάρχουν πολλές προκλήσεις. Οι νέοι επενδυτές πιθανότατα έχουν λάβει προληπτικά μέτρα είτε θα επενδύσουν σε μεγάλο βαθμό

είτε όχι επειδή ο κίνδυνος και οι προκλήσεις δημιουργούνται από τις συναλλαγές και τις επενδύσεις σε κρυπτονομίσματα. Παρακάτω αναλύονται οι βασικές προκλήσεις που συνδέονται με τα κρυπτονομίσματα και το Bitcoin.

4.2.1. Θεσμικό πλαίσιο

Όσον αφορά το fiat money, είναι ασφαλές για τους χρήστες να το χρησιμοποιούν, καθώς ρυθμίζεται από την κεντρική τράπεζα μιας χώρας. Παράλληλα αναφορικά με τα κρυπτονομίσματα, ο καθένας μπορεί να έχει πολλαπλούς λογαριασμούς, χωρίς κόστος για τη δημιουργία τους. Δεν υπάρχουν κατάλληλες κεντρικές διαδικασίες ελέγχου και επίσης δεν είναι υποχρεωτική η χρήση του πραγματικού τους ονόματος. Αυτή η διαδικασία είναι μάλλον ασαφής όπου η έννοια των παράνομων δραστηριοτήτων πίσω από όλες τις καταχωρίσεις και συναλλαγές κρυπτονομισμάτων μπορεί να είναι δεδομένη με τον ένα ή τον άλλο τρόπο. Η ανωνυμία στον Ιστό είναι το τέλειο έδαφος για εγκληματίες και απατεώνες να διαπράξουν τη δράση τους. Οι εγκληματίες του κυβερνοχώρου θα μπορούσαν συνεπώς να χρησιμοποιήσουν, αυτήν την πλατφόρμα συναλλαγών για να εκτελέσουν τις παράνομες δραστηριότητές τους και σε βαθμό απάτης και εξαπάτησης. Ο Kaplanon (2020) πιστεύει ότι τα κρυπτονομίσματα είναι πιο πιθανό να χρησιμοποιηθούν από εγκληματίες σε περιπτώσεις απάτης όπως το ξέπλυμα χρήματος και η διακίνηση ναρκωτικών. Παρά το γεγονός ότι η τεχνολογία blockchain εφευρέθηκε για να διευκολύνει τους χρήστες σε όλο τον κόσμο με ευκολία, οι εγκληματίες θα βρίσκουν πάντα τρόπους για να αποκομίσουν κέρδη.

Προηγουμένως, ορισμένες ρυθμιστικές αρχές είχαν αρνηθεί να εγκρίνουν το Bitcoin ως νόμισμα, όπως αναφέρθηκε και παραπάνω, για παράδειγμα στην Κίνα. Η Κίνα είχε απαγορεύσει την εφαρμογή του Bitcoin ή οποιωνδήποτε άλλων ψηφιακών νομισμάτων σε χρηματοπιστωτικά ιδρύματα και κάθε μορφή επιχείρησης. Αυτή η ενέργεια στην οποία προέβη η κυβερνητική αρχή είναι κατανοητή, επειδή οι εμπορικές και επιχειρηματικές δραστηριότητες

κρυπτονομισμάτων δεν μπορούν να εντοπιστούν στην πλατφόρμα συναλλαγών της καθώς επίσης και η ανωνυμία του εμπλεκόμενου προσωπικού. Παρόλο που ορισμένες χώρες υποστήριξαν τη χρήση ψηφιακού νομίσματος, η Κίνα μπορεί να το είχε απαγορεύσει λόγω των δυνατοτήτων της στην άνοδο της οικονομίας και ως μία από τις οικονομικές υπερδυνάμεις του κόσμου (Karlanon, 2020)

4.2.2. Κόστος κατανάλωσης ηλεκτρικής ενέργειας

Εκτός από το αρχικό κόστος της επένδυσης στο υλικό, μια άλλη κύρια δαπάνη που πρέπει να πληρώσει ένας εξορύκτης είναι η κατανάλωση ενέργειας (Hayes, 2017). Για παράδειγμα, στην περίπτωση του Bitcoin, όλες οι συναλλαγές καταγράφονται σε έναν δημόσιο κατάλογο -κάτι σαν ψηφιακό λογιστικό βιβλίο- η συντήρηση του οποίου απαιτεί μεγάλες ποσότητες ενέργειας, ενώ το κρυπτονόμισμα δίδεται ως αμοιβή σε όσους λύσουν με τους υπολογιστές τους πολύπλοκους μαθηματικούς γρίφους. Η διαδικασία αυτή αποκαλείται «εξόρυξη», στα αγγλικά «mining», κι απαιτεί πανίσχυρα υπολογιστικά συστήματα. Συνολικά το bitcoin θεωρείται εξαιρετικά ενεργοβόρο, αφού για να «συντηρηθεί» το σύστημα της παραγωγής του, χρειάζεται κάθε χρόνο το ηλεκτρικό ρεύμα που καταναλώνει μια χώρα όπως η Φιλανδία (ενώ πίσω στο μακρινό 2010, όταν η αξία του ήταν πολύ χαμηλή, μπορούσες να το εξορύξεις με έναν απλό υπολογιστή με δυνατή κάρτα γραφικών και ελάχιστο κόστος ενέργειας). (Akbulaev et al., 2020).

Διαπιστώθηκε ότι η εξόρυξη του ψηφιακού νομίσματος, απαιτεί την κατανάλωση μεγαλύτερων επιπέδων ηλεκτρικής ενέργειας και συνακόλουθα υψηλότερους λογαριασμούς ηλεκτρικού ρεύματος (O'Dwyer & Malone, 2014). Η εξόρυξη κρυπτονομισμάτων είναι γεγονός ότι απαιτεί τεράστια ενέργεια. Το κόστος εξόρυξης διαφέρει από την απόδοση του υλικού. Αναφέρεται ότι η παραγωγή ηλεκτρικής ενέργειας από την εξόρυξη κρυπτονομισμάτων κυμαίνεται από 10 MW (που ισοδυναμεί με μια μικρή μονάδα παραγωγής ενέργειας) έως 3-6

GW (η εκτιμώμενη ενέργεια που καταναλώνεται σε μικρές έως μεσαίες χώρες όπως το Μπαγκλαντές και η Δανία) (Vranken, 2017).

Οι Beer et al., (2014) τόνισαν την πτυχή της βιωσιμότητας των κρυπτονομισμάτων. Διερεύνησε ότι η εξόρυξη αυτών των ψηφιακών νομισμάτων καταναλώνει υψηλή ενέργεια και απαιτεί έντονες δυνατότητες υπολογιστών. Ωστόσο, αυτοί οι εξελιγμένοι υπολογιστές που περιλαμβάνουν CPU, GPU κλπ., είναι απαραίτητοι για την εξόρυξη εντός του blockchain για την αποφυγή διπλών δαπανών. Αναμένεται πάντως ότι οι δραστηριότητες εξόρυξης θα επιβραδυνθούν εντός της επόμενης δεκαετίας και μόνο εκείνες με σημαντικό ενημερωμένο υλικό θα επιβιώσουν στην εξορυκτική δραστηριότητα και τη δυνατότητα μείωσης του κόστους κατανάλωσης ηλεκτρικής ενέργειας.

Οι Becker et al. (2013) περιέγραψαν το κόστος εξόρυξης κρυπτονομισμάτων. Σύμφωνα με διάφορους υπολογισμούς τους, η εξόρυξη Bitcoin καταναλώνει πλέον 204 TWh ηλεκτρικής ενέργειας ετησίως. Ταυτόχρονα, το δεύτερο μεγαλύτερο κρυπτονομίσμα, Ethereum, απαιτεί 104 TWh για ένα σύνολο άνω των 300 TWh διεθνώς δίχως να υπολογίζουμε τα μικρότερα κρυπτονομίσματα. Λόγω του ότι η συντριπτική πλειοψηφία αυτών των νομισμάτων προσαρμόζει την απόδειξη εργασίας, απαιτεί μεγάλη κατανάλωση ενέργειας λόγω της μαθηματικής εργασίας από το εμπλεκόμενο υλικό. Αυτό είναι ιδιαίτερα επιβλαβές σε δραστηριότητες εξόρυξης μεγάλης κλίμακας. Αυτό με τη σειρά του, θα κάνει την εξόρυξη κρυπτονομισμάτων ως τον κακό που συμβάλλει στην εκπομπή διοξειδίου του άνθρακα και θα καταστρέψει τη γη μέσω της υπερθέρμανσης του πλανήτη. Θα πρέπει πάντως να διενεργηθούν περισσότερες μελέτες σχετικά με την επίδραση των κρυπτονομισμάτων στο περιβάλλον καθώς είναι γεγονός ότι δεν αξίζει να θυσιάσεις τη γη για ένα βραχυπρόθεσμο κέρδος. Εάν αποδειχθεί ότι η διαδικασία εξόρυξης θα έκανε περισσότερο κακό παρά καλό, οι κυβερνήσεις ή ακόμη και τα Ηνωμένα Έθνη θα πρέπει να παρέμβουν για να διασφαλίσουν ότι το περιβάλλον δεν θα τεθεί σε κίνδυνο.

4.2.3. Crash and Bubble

Υποστηρίζεται ευρέως ότι μια αποτελεσματική αγορά είναι όπου υπάρχουν διαθέσιμες πληροφορίες του παρελθόντος που μπορούν να αντικατοπτρίζουν πλήρως τις τιμές στην ιστορική τους εξέλιξη. Το κρυπτονομίσματα λέγεται ότι είναι μια αδύναμη μορφή νομίσματος, επειδή οι επενδυτές δεν είναι σε θέση να προβλέψουν τη μελλοντική προοπτική κι αυτό λόγω του ότι δεν υπάρχουν διαθέσιμες πληροφορίες από το παρελθόν (Urquhart, 2016). Αυτό ισχύει από τη στιγμή που η έναρξη του κρυπτονομίσματος εμφανίστηκε μόλις το 2009, σχεδόν πριν από δεκαπέντε χρόνια. Μια επένδυση σε αυτό το σύντομο χρονικό διάστημα σίγουρα δεν έχει ιστορικό παρελθόν και οι επενδυτές δεν μπορούν να βασιστούν στο ιστορικό για να εξασφαλίσουν ότι η επένδυση μπορεί να είναι κερδοφόρα. Οι Akbulac et al., (2020) υπέθεσαν ότι, εάν τα κρυπτονομίσματα έχουν πραγματική μορφή λογαριασμού και αξία αποθήκευσης, δεν θα ήταν τόσο ασταθή. Το ότι είναι ασταθή σημαίνει ότι είναι επιρρεπή σε κινδύνους φουσκών και συντριβών. Παρόλο που όπως προαναφέρθηκε υπήρξαν τέτοια φαινόμενα, η έκταση και το εύρος τους δεν ήταν σε τέτοιο βαθμό ώστε να απειλήσουν την ύπαρξη του Bitcoin και που θα μείωναν τελικά το Bitcoin ή οποιοδήποτε άλλο κρυπτονομίσμα.

Αυτή η αστάθεια στο Bitcoin παρέχει την ένδειξη ότι τα κρυπτονομίσματα θα ήταν ένα εμπόρευμα μη εμπιστοσύνης για μακροπρόθεσμες επενδύσεις. Αυτό σημαίνει ότι μπορεί να υπάρξει το ενδεχόμενο να συμβεί φούσκα και συντριβή σύμφωνα με αυτήν την τάση μεταβλητότητας σύμφωνα με τον Dwyer (2015). Οι Cheung et al. (2015) είχαν ερευνήσει ότι το Bitcoin είχε υποστεί τρεις μεγάλες φουσαλίδες που έσκασαν από το 2011 έως το 2013, οι οποίες είχαν διαρκέσει από 60 έως 106 ημέρες. Το μεγαλύτερο σκάνδαλο σε αυτή την τραγωδία φούσκων είχε κοστίσει στο ανταλλακτήριο Mt Gox το 2013. Υπενθυμίζεται ότι το MT Gox, ένα από τα μεγαλύτερα ανταλλακτήρια Bitcoin στον κόσμο με έδρα την Ιαπωνία, ανακοίνωσε στο τέλος του 2013, σύντομο μήνυμα στην ιστοσελίδα του την Τρίτη ότι όλες οι συναλλαγές αναστέλλονται προσωρινά με στόχο την προστασία των χρηστών. (Yermack, 2013).

Προηγούμενη έρευνα έχει δείξει ότι η κερδοσκοπία μπορεί να οδηγήσει σε αποσταθεροποίηση περιουσιακών στοιχείων (Blau, 2018). Η αστάθεια που εμφανίζει η τιμή του Bitcoin δείχνει ότι καθοδηγείται από τις συναλλαγές που αμαυρώνονται από την κερδοσκοπία. Η κερδοσκοπία μπορεί ενδεχομένως να εξαλείψει την κατάστασή του ως βιώσιμου νομίσματος. Η τιμή του Bitcoin στην αρχική τιμή διαπραγμάτευσης ήταν μόνο μερικά σεντς, ενώ στην πορεία, είχε σκαρφαλώσει στα 1.132,26 \$ προς το τέλος του 2013. Λίγους μήνες αργότερα η τιμή έπεσε σχεδόν κατά 60% (Blau, 2018). Αυτό ήταν ένα σαφές σημάδι φούσκας. Λόγω του περιορισμένου αριθμού ατόμων που χρησιμοποιούν το Bitcoin ως το κύριο κρυπτονόμισμα σήμερα, είναι δύσκολο να αξιολογηθεί η μελλοντική του εξέλιξη (Donier et al., 2015). Σε όλο τον κόσμο, υπάρχουν περίπου λιγότεροι από 9000 λιανοπωλητές που δέχονται το Bitcoin ως τρόπο πληρωμής. Αυτή η αβέβαιη εφαρμογή του Bitcoin μπορεί να οδηγήσει σε απάτη που μπορεί να οδηγήσει σε απώλεια νομισματικών επενδύσεων. Οι επενδυτές θα ήθελαν να αποκομίσουν κέρδη από τα κρυπτονομίσματα, επιδιώκοντας να τους σώσουν δυνητικά από τυχόν κινδύνους κερδοσκοπίας (Li et al., 2018). Αναμένεται ότι τελικά θα προκύψουν φούσκες όταν οι αρχές και η οικονομική πολιτική παρέμβουν μη ευνοώντας το κρυπτονόμισμα, όπως φαίνεται από τη μικρή έκρηξη της φούσκας του Bitcoin σε αρκετές περιπτώσεις που αναφέρθηκαν παραπάνω.

4.2.4. Διαδικτυακές επιθέσεις

Ο Blau (2017) υπέθεσε ότι η τεχνολογία του blockchain που έχει αποκεντρωμένο χαρακτήρα έχει χαμηλή ευαισθησία και ασφάλεια. Ανοίγει την πόρτα στη χειραγώγηση και τη πλαστογραφία. Η τεχνολογία blockchain έχει πολλές προκλήσεις σχετικά με την ταυτότητά της και το σύστημα διαχείρισης πρόσβασης που σχετίζεται με το Διαδίκτυο των Πραγμάτων (IoT). Οι δραστηριότητες εξόρυξης που χρησιμοποιούν τα εν λόγω συστήματα είναι

ευάλωτες σε διάφορους τύπους επιθέσεων. Για παράδειγμα μια επίθεση Sybil που στοχεύει στο δίκτυο μπορεί να γίνει από τους κακόβουλους χειριστές συνδυάζοντας τους πόρους στη δεξαμενή τους. Ενώ τα κακόβουλα μέλη της ομάδας μπορούν δυνητικά να αυξήσουν την υπολογιστική ισχύ σε μια συγκεκριμένη ομάδα εξόρυξης και αργότερα στο μέλλον, να την αποσταθεροποιήσουν. Αυτοί οι χρήστες μεταπηδούν από τη μια πισίνα εξόρυξης στην άλλη προκειμένου να υπονομεύσουν τις επιστροφές εξόρυξης των πισινών και να αποκρύψουν την αποτελεσματικότητα του εξορυσσόμενου μπλοκ (Conte De Leon et al., 2017).

Ένα άλλο μειονέκτημα του κρυπτονομίσματος είναι η επίθεση στο σύστημα που βασίζεται σε κώδικα. Η κωδικοποίηση του δικτύου από τον ιδρυτή Nakamoto είναι ανοιχτή για επίθεση σφαλμάτων. Αυτό το δίκτυο διατηρείται πλέον από μια βασική ομάδα στον ανοιχτό κώδικα μέσω του Github. Μια επίθεση είχε ήδη συμβεί τον Ιούνιο του 2013, όπου οι κόμβοι Bitcoin δέχθηκαν επίθεση από έναν άγνωστο εισβολέα, ο οποίος μετέδωσε τις πληροφορίες στο δίκτυο που δεν εμπλέκονταν σε δραστηριότητες εξόρυξης. Όπως έδειξε η ιστορία, η μελλοντική επίθεση στο δίκτυο blockchain είναι ενδεχόμενη και πολύ πιθανή. Αν και είναι επιτυχημένοι μέχρι στιγμής, οι απατεώνες θα βρουν τελικά τρόπους να επιτεθούν στο δίκτυο κρυπτογράφησης του blockchain, εάν αυτό το θέμα της ευπάθειας δεν αντιμετωπιστεί σοβαρά. (Bradbury, 2013).

ΚΕΦΑΛΑΙΟ 5 ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΑ ΚΑΙ ΜΕΓΑΛΑ ΔΕΔΟΜΕΝΑ

5.1. Η διαδικασία Εξόρυξης Δεδομένων (mining) και εργαλεία εξόρυξης δεδομένων

Εξόρυξη ή mining στην διαδικασία των κρυπτονομισμάτων και του Bitcoin ειδικότερα, είναι η διαδικασία κατά την οποία όλες οι συναλλαγές καταγράφονται σε έναν δημόσιο κατάλογο -κάτι σαν ψηφιακό λογιστικό βιβλίο- η συντήρηση του οποίου απαιτεί μεγάλες ποσότητες ενέργειας, ενώ το κρυπτονόμισμα δίδεται ως αμοιβή σε όσους λύσουν με τους υπολογιστές τους πολύπλοκους μαθηματικούς γρίφους. Δηλαδή με άλλα λόγια το mining κρυπτονομισμάτων είναι η διαδικασία κατά την οποία οι συναλλαγές μεταξύ χρηστών επαληθεύονται και προστίθενται στο δημόσιο καθολικό blockchain. Η διαδικασία mining είναι επίσης υπεύθυνη για την εισαγωγή νέων νομισμάτων στην υπάρχουσα κυκλοφορία. Είναι όπως προαναφέρθηκε, ένα από τα βασικά στοιχεία που επιτρέπουν στα κρυπτονομίσματα να λειτουργούν ως αποκεντρωμένο δίκτυο peer-to-peer, χωρίς την ανάγκη κεντρικής αρχής τρίτου μέρους (Fry & Eng-Tuck, 2016).

Ειδικότερα, ο miner είναι ένας κόμβος στο δίκτυο ο οποίος συλλέγει το σύνολο των συναλλαγών τις οποίες οργανώνει σε blocks. Κάθε φορά που υλοποιούνται συναλλαγές, οι κόμβοι δικτύου τις λαμβάνουν και επαληθεύουν την εγκυρότητά τους. Ακολούθως οι κόμβοι miners συλλέγουν τις εν λόγω συναλλαγές από το χώρο μνήμης συγκεντρώνοντάς τις σε ένα block το οποίο αποκαλείται υποψήφιο block. Το πρώτο βήμα του mining ενός block είναι να κατακερματιστεί μεμονωμένα κάθε συναλλαγή η οποία λαμβάνεται από τη δεξαμενή μνήμης. Πριν την εκκίνηση της διαδικασίας, ο κόμβος miner προσθέτει μια συναλλαγή, και στη συνέχεια στέλνει στον εαυτό του την ανταμοιβή του mining η οποία αποκαλείται block ανταμοιβή. Πρόκειται για μια συναλλαγή, η οποία αναφέρεται ως συναλλαγή coinbase, δηλαδή μια συναλλαγή όπου τα κέρματα δημιουργούνται «από τον

αέρα». Στις περισσότερες περιπτώσεις, είναι η πρώτη συναλλαγή που καταγράφεται σε ένα νέο block (Fry & Eng-Tuck, 2016).

Από τη στιγμή που θα υπάρξει κατακερματισμός κάθε συναλλαγής, το σύνολο των κατακερματισμών, οργανώνεται σε μια δομή που ονομάζεται δέντρο κατακερματισμού (Merkle Tree). Το εν λόγω δένδρο, σχηματίζεται μέσω της οργάνωσης των ποικίλων προϊόντων κατακερματισμού σε ζεύγη και στη συνέχεια κατακερματίζοντάς τα εκ νέου. Ακολούθως, οι έξοδοι, οργανώνονται σε ζεύγη και κατακερματίζονται για ακόμα μια φορά, ενώ το σύνολο της διαδικασίας αυτής επαναλαμβάνεται έως την κορυφή του δέντρου. Η κορυφή του δέντρου αποκαλείται επίσης κατακερματισμός ρίζας (ή Merkle root) και ουσιαστικά πρόκειται για ένα μόνο προϊόν κατακερματισμού. Το εν λόγω προϊόν που τοποθετείται στην κορυφή του δέντρου, αντιπροσωπεύει όλους τους προηγούμενους κατακερματισμούς που έλαβαν χώρα για τη υλοποίησή του (Fang et al., 2019).

Ο κατακερματισμός ρίζας μαζί με τον κατακερματισμό του προηγούμενου block και έναν τυχαίο αριθμό που ονομάζεται nonce τοποθετείται στη συνέχεια στην κεφαλίδα του block. Στη συνέχεια, η κεφαλίδα του block κατακερματίζεται και μέσα από τη διαδικασία αυτή παράγεται μια έξοδος με βάση τα στοιχεία κατακερματισμός ρίζας, κατακερματισμός προηγούμενου block και nonce σε συνδυασμό με κάποιες ακόμη παραμέτρους. Η έξοδος που προκύπτει είναι το block κατακερματισμού και θα χρησιμεύσει ως το αναγνωριστικό του πρόσφατα δημιουργημένου block (υποψήφιο block). Για να θεωρηθεί έγκυρη, η έξοδος (block κατακερματισμού) πρέπει να είναι μικρότερη από μια συγκεκριμένη τιμή-στόχο που καθορίζεται από το πρωτόκολλο. Με άλλα λόγια, το block κατακερματισμού πρέπει να ξεκινά με έναν ορισμένο αριθμό μηδενικών. Η τιμή στόχου – επίσης γνωστή ως δυσκολία κατακερματισμού – προσαρμόζεται τακτικά από το πρωτόκολλο. Αυτό διασφαλίζει ότι ο ρυθμός δημιουργίας νέων blocks παραμένει σταθερός και ανάλογος με την ποσότητα ισχύος κατακερματισμού, που αφιερώνεται στο δίκτυο. Επομένως, κάθε φορά που νέοι miners εντάσσονται στο

δίκτυο και ο ανταγωνισμός αυξάνεται, η δυσκολία κατακερματισμού αυξάνεται, εμποδίζοντας τη μείωση του μέσου χρόνου αποκλεισμού. Αντίθετα, εάν οι miners αποφασίσουν να αποχωρήσουν από το δίκτυο, η δυσκολία κατακερματισμού θα μειωθεί, διατηρώντας τον χρόνο αποκλεισμού σταθερό, παρόλο που υπάρχει λιγότερη υπολογιστική ισχύς αφιερωμένη στο δίκτυο (Fang et al., 2019).

Η διαδικασία mining κρυπτονομισμάτων απαιτεί από τους miners να συνεχίζουν να κατακερματίζουν την κεφαλίδα του block ξανά και ξανά. Ξεπανάλαμβάνουν την διαδικασία, μέσω του nonce, έως ότου κάποιος miner στο δίκτυο, παράγει τελικά ένα έγκυρο block κατακερματισμού. Όταν βρεθεί ένα έγκυρο προϊόν κατακερματισμού, ο ιδρυτικός κόμβος θα μεταδώσει το block στο δίκτυο. Όλοι οι άλλοι κόμβοι θα ελέγξουν εάν ο κατακερματισμός είναι έγκυρος και, εάν ναι, θα προσθέσουν το block στο αντίγραφο του blockchain. Τέλος, θα προχωρήσουν στο mining του επόμενου block (Ghimire, 2019).

Ωστόσο, μερικές φορές συμβαίνει δύο miners να μεταδίδουν ένα έγκυρο block ταυτόχρονα. Το δίκτυο καταλήγει με δύο ανταγωνιστικά blocks. Οι miners αρχίζουν να κάνουν mining το επόμενο block, με βάση το block που έλαβαν πρώτα. Ο ανταγωνισμός μεταξύ αυτών των block θα συνεχιστεί, έως ότου το επόμενο block γίνει mining, με βάση οποιοδήποτε από τα ανταγωνιστικά blocks. Το block που εγκαταλείπεται, ονομάζεται ορφανό block ή μαγαιάτικο. Οι miners αυτού του block θα επιστρέψουν στο mining της αλυσίδας του block που επικράτησε (Ghimire, 2019).

Η ανταμοιβή block δίνεται στον miner που ανακαλύπτει πρώτα τον έγκυρο κατακερματισμό. Η πιθανότητα όμως εύρεσης του κατακερματισμού είναι ίση με το τμήμα της συνολικής mining δύναμης στο δίκτυο. Οι miners με ένα μικρό ποσοστό της mining δύναμης, έχουν μια πολύ μικρή πιθανότητα να ανακαλύψουν το επόμενο block από μόνοι τους. Οι Mining Pools δημιουργούνται για να λύσουν αυτό το πρόβλημα. Μεταφράζονται σε συγκέντρωση πόρων από miners, οι οποίοι μοιράζονται την επεξεργαστική τους δύναμη μέσω ενός δικτύου, για να μοιράσουν

την ανταμοιβή εξίσου μεταξύ όλων στην ομάδα, ανάλογα με την συμβολή τους στην πιθανότητα εύρεσης νέου block (Ghimire, 2019).

5.2. Αλγόριθμοι hash και τεχνικές κατακερματισμού hashing

Όπως αναλύθηκε παραπάνω το Bitcoin διασφαλίζεται μέσω της εξόρυξης, δηλαδή της διαδικασίας χρήσης υπολογιστικής δύναμης για την εξασφάλιση των συναλλαγών έναντι των συγκρούσεων και την εισαγωγή νέων Bitcoin στο σύστημα. Οι ανθρακωρύχοι χρησιμοποιούν εξειδικευμένους κόμβους εξόρυξης. Παρέχονται κίνητρα για την παροχή της υπολογιστικής ισχύος που απαιτείται για τη διασφάλιση του δικτύου με ανταμοιβές μπλοκ και χρεώσεις συναλλαγών, παράγοντας μπλοκ επικυρωμένων συναλλαγών και προσθέτοντάς τα στην αλυσίδα μπλοκ του Bitcoin (Xi et al., 2018).

Οι χρήστες, χρησιμοποιούν την υπολογιστική τους δύναμη σε ανταγωνισμό για να παράγουν μπλοκ, επιλύοντας πολύπλοκους υπολογισμούς, η δυσκολία των οποίων είναι μεταβλητή και ορίζεται αυτόματα από το λογισμικό του Bitcoin. Πρόκειται για την επονομαζόμενη ρύθμιση της δυσκολίας, σύμφωνα με την οποία η πολυπλοκότητα των υπολογισμών αυξάνεται ή μειώνεται κάθε 2016 μπλοκ (περίπου κάθε δύο εβδομάδες), ανάλογα με τη συνολική υπολογιστική ισχύ που αναπτύχθηκε στο δίκτυο εκείνη τη στιγμή. Μόλις επιλυθεί ο τελευταίος υπολογισμός από έναν ανθρακωρύχο, είναι σαν να κερδίζεις τη λοταρία για να δημιουργηθεί το επόμενο μπλοκ. Δημοσιεύουν το αποτέλεσμα ως απόδειξη και περιλαμβάνουν τις πρόσφατες έγκυρες συναλλαγές σε εκκρεμότητα που έχουν προσθέσει σε ένα νέο μπλοκ για το blockchain του Bitcoin. Αυτό μεταδίδεται σε κόμβους σε όλο το δίκτυο για να επαληθεύσει ότι τόσο η λύση, η απόδειξη εργασίας, όσο και οι συναλλαγές που περιλαμβάνονται στο μπλοκ είναι έγκυρες.

Όταν επιλυθεί ένα μπλοκ, οι συναλλαγές που περιλαμβάνονται δείχνουν ότι έχουν μία επιβεβαίωση στο δίκτυο, ορατή στο λογισμικό πορτοφολιών και στους

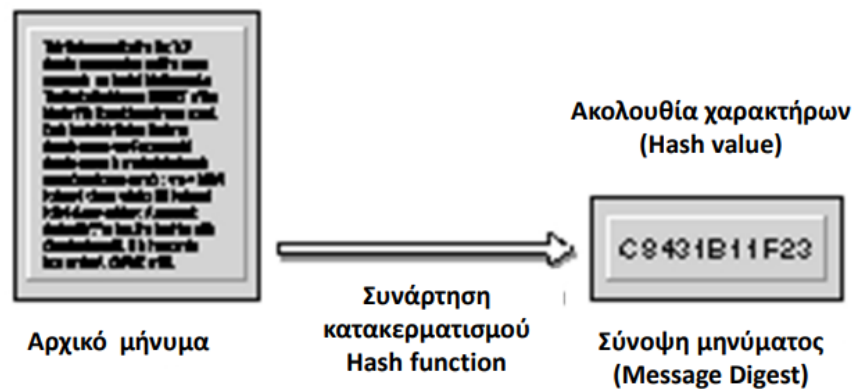
εξερευνητές των μπλοκ. Κάθε μπλοκ που ακολουθεί προσθέτει μια περαιτέρω επιβεβαίωση. Μετά από έξι επιβεβαιώσεις, οι συναλλαγές θεωρούνται οριστικά επαληθευμένες. Σε περίπτωση διένεξης, οι κόμβοι στο δίκτυο Bitcoin θεωρούν ότι η μεγαλύτερη αλυσίδα με τη μεγαλύτερη απόδειξη εργασίας είναι η πραγματική και έγκυρη (Katsiaba, 2017).

Η εξόρυξη Bitcoin χρησιμοποιεί έναν μηχανισμό συναίνεσης απόδειξης εργασίας που βασίζεται στην συνάρτηση κατακερματισμού SHA-256. Ο όρος συνάρτηση κατακερματισμού (hash function) υποδηλώνει τον μετασχηματισμό που λαμβάνει ως είσοδο ένα μήνυμα m οποιουδήποτε μήκους και επιστρέφει στην έξοδο μια ακολουθία χαρακτήρων h περιορισμένου μήκους που καλείται hash value, δηλαδή είναι $h = H(m)$ (Liu et al., 2018).



Εικόνα 1 Συνάρτηση κατακερματισμού

Η ακολουθία χαρακτήρων (hash value) που παρουσιάζει συνοπτικά το μεγαλύτερο μήνυμα ή έγγραφο, καλείται και Σύνοψη Μηνύματος (Message Digest). Μπορούμε να φανταστούμε τη σύνοψη του μηνύματος ως ένα «ψηφιακό αποτύπωμα» (digital fingerprint) του εγγράφου (Liu et al., 2018).



Εικόνα 2 Συνάρτηση κατακερματισμού

Πίσω από τη συντομογραφία SHA 256 υπάρχει μία λειτουργία η οποία βρίσκεται στην καρδιά των κρυπτονομισμάτων όπως το bitcoin. Πρόκειται για την συνάρτηση κατακερματισμού η οποία εντάσσεται στις ομάδα των λειτουργιών SHA 2. Η συντομογραφία SHA σημαίνει Secure Hash Algorithm (ασφαλής αλγόριθμος κατακερματισμού). Μια συνάρτηση κατακερματισμού είναι μια λειτουργία μονής κατεύθυνσης που μετατρέπει τις συμβολοσειρές (strings) οποιουδήποτε μήκους σε συμβολοσειρές ομοιόμορφου μήκους. Το παραπάνω χρησιμοποιείται, εκτός των άλλων, για να ελεγχθεί η ακεραιότητα των αρχείων (Kasgar, 2012).

Ο ασφαλής αλγόριθμος κατακερματισμού πληροί στη βάση του δύο βασικές λειτουργίες για τα κρυπτονομίσματα. Το πιο γνωστό κρυπτονόμισμα που χρησιμοποιεί αυτή τη συνάρτηση κατακερματισμού είναι το bitcoin. Αρχικά, η λειτουργία αυτή θα χρησιμοποιηθεί ως ένας αλγόριθμός proof of work στο bitcoin.

Η έκφραση proof of work (απόδειξη εργασίας) περιγράφει την περίπλοκη δημιουργία εύκολα επαληθεύσιμων αρχείων που προστέθηκαν στην αλυσίδα μπλοκ. Όσοι παρέχουν υπολογιστική ισχύ για αυτήν την απόδειξη εργασίας θα λάβουν coins ως αντάλλαγμα. Αυτή η εργασία γενικά ονομάζεται όπως

προαναφέρθηκε, εξόρυξη. Αυτή η συνάρτηση κατακερματισμού παίζει ρόλο στη δημιουργία διεύθυνσεων Bitcoin. Με μία διεύθυνση bitcoin μπορούν να αποσταλούν coins. Αυτή περιέχει από 25 μέχρι 35 χαρακτήρες. Κατά την αποστολή των coins, η ακριβής διεύθυνση πρέπει να καθοριστεί. Ο κίνδυνος πληκτρολόγησης μίας άλλης διεύθυνσης που υπάρχει από ένα τυπογραφικό λάθος είναι εξαιρετικά μικρή (Casgar, 2012).

5.3. Πρόβλεψη αξίας του Bitcoin μέσω Μοντελοποίησης

Με την ταχύτατη ανάπτυξη του Bitcoin, και το ενδιαφέρον των χρηστών παγκοσμίως, καθημερινά υπάρχουν δημοσιεύματα, σχετικά με μεγάλες απρόσμενες αλλαγές τιμών του Bitcoin όπως και άλλων κρυπτονομισμάτων. Είναι γεγονός ότι κανένα άλλο περιουσιακό στοιχείο δεν έχει λάβει τέτοια προσοχή από τα μέσα ενημέρωσης ούτε έχει προσελκύσει τόσες πολλές εικασίες αναφορικά με τις κινήσεις των τιμών του. Για την πρόβλεψη των τιμών του Bitcoin όπως και άλλων κρυπτονομισμάτων έχουν προταθεί διάφορα μοντέλα πρόβλεψης. Έτσι διάφοροι ακαδημαϊκοί αλλά και οικονομικοί αναλυτές, επιχείρησαν να μοντελοποιήσουν τις κινήσεις των τιμών του Bitcoin, μέσω της χρήσης ποικίλων εργαλείων τεχνικής ανάλυσης και οικονομετρικής μοντελοποίησης. Πρόσφατα, ορισμένοι έμποροι άρχισαν να χρησιμοποιούν το μοντέλο πρόβλεψης τιμών Bitcoin, stock-to-flow (S2F) για την τιμή του Bitcoin και άλλων κρυπτονομισμάτων (Stallings, 2018).

Το μοντέλο stock-to-flow (S2F-απόθεμα σε ροή), που παραδοσιακά χρησιμοποιείται για την παρακολούθηση της απόδοσης των εμπορευμάτων όπως τα πολύτιμα μέταλλα, συγκρίνει την τιμή ενός περιουσιακού στοιχείου με τη διαθέσιμη προσφορά του. Εκτός αυτού, το μοντέλο απόθεμα σε ροή του PlanB σχετικά με την τιμή του Bitcoin έχει γίνει σήμερα ευρέως διαδεδομένο, στον κόσμο των κρυπτονομισμάτων (Morillon & Chacon, 2022).

Το μοντέλο stock-to-flow δεν αποτελεί βέβαια καινοτομία και έχει χρησιμοποιηθεί για τη μοντελοποίηση τιμών λιγоста περιουσιακά στοιχεία με περιορισμένη διαθέσιμη προμήθεια όπως πολύτιμα μέταλλα όπως χρυσός και ασήμι για λίγο τώρα. Βασίζεται στην ιδέα ότι η έλλειψη ενός περιουσιακού στοιχείου οδηγεί σε μεγαλύτερη αξία. Ωστόσο, η πρώτη φορά που χρησιμοποιήθηκε για το Bitcoin ήταν μόνο στις αρχές του 2019. επειδή η προσφορά αυτού του περιουσιακού στοιχείου στην αγορά καθορίζεται από τον τρόπο που κατασκευάστηκε, συγκρίνεται τώρα με άλλα σπάνια περιουσιακά στοιχεία όπως μέταλλα και εμπορεύματα από ορισμένους επενδυτές. Ένας γενικός τύπος για την αναλογία αποθεμάτων προς ροή είναι μονάδες αποθεμάτων διαιρούμενες με μονάδες ροής, έτσι η ποσότητα του ενεργητικού που διατηρείται στα αποθεματικά με την ποσότητα που παράγεται κάθε χρόνο (Morillon & Chacon, 2022).

5.4. Μέθοδοι πρόβλεψης τιμής Bitcoin

Η αγορά των κρυπτονομισμάτων βρίσκεται ήδη στην δεύτερη δεκαετία της. Είναι γεγονός ότι το βασικό χαρακτηριστικό της πρώτης δεκαετίας είναι η υψηλή μεταβλητότητα και μια άνευ προηγουμένου εκρηκτική άνοδο των αποτιμήσεων παρά το γεγονός ότι όπως προαναφέρθηκε υπήρχαν και περίοδοι που χαρακτηρίστηκαν ως φούσκα. Στις αρχές του 2022 η κεφαλαιοποίηση του Bitcoin ξεπέρασε το 1 τρις δολάρια και η συνολική κεφαλαιοποίηση της αγοράς των crypto τα 2 τρις δολάρια. ³Μεγάλοι επενδυτές και τραπεζίτες οι οποίοι αρχικά είχαν

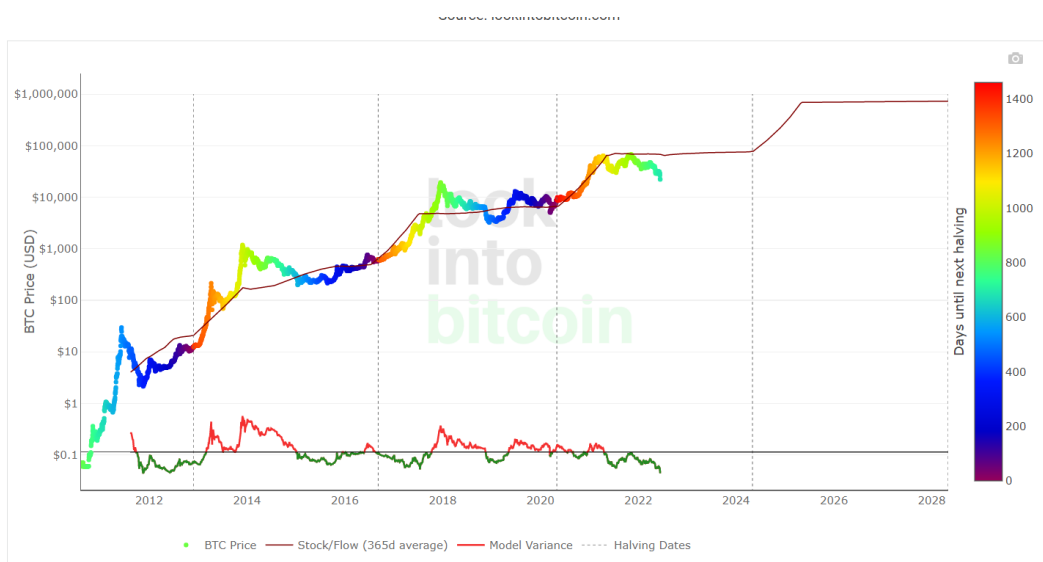
³ Βέβαια στις αρχές Ιουνίου του 2022, το bitcoin κατέγραψε ισχυρή πτώση με το μεγαλύτερο κρυπτονόμισμα του πλανήτη να σημειώνει "βουτιά" της τάξης του 17%, συμπαρασύροντας καθοδικά και τα άλλα, με αποτέλεσμα η συνολική κεφαλαιοποίηση της αγοράς κρυπτονομισμάτων να υποχωρεί κάτω από το επίπεδο του 1 τρις. δολαρίων για πρώτη φορά από τις αρχές του 2021. Ειδικότερα, η τιμή του bitcoin σημειώνει πτώση 17% και κινήθηκε στις 13/6/2022 στο επίπεδο των 22.765 δολαρίων, σύμφωνα με τα στοιχεία της CoinDesk, διολισθαίνοντας στο χαμηλότερο επίπεδο από τον Δεκέμβριο του 2020. Το μεγαλύτερο κρυπτονόμισμα του πλανήτη έχει σημειώσει "βουτιά" περίπου 50% από την αρχή του τρέχοντος έτους.

κατακρίνει την αγορά των κρυπτονομισμάτων, σήμερα τάσσονται με την πλευρά των αγοραστών ενώ συχνά δηλώνουν ότι θα έπρεπε να μην έχουν κρατήσει τους πελάτες τους μακριά από μια αγορά που ανεβαίνει κατά μέσο όρο 200% τον χρόνο, εδώ και μια ολόκληρη 10ετία.

Λόγω της ισχυρής ανάπτυξης της αγοράς του Bitcoin, δημιουργήθηκαν κάποια βασικά μοντέλα πρόβλεψης των κορυφών και των κατώτατων επιπέδων τιμής (κορυφών/πάτων) του Bitcoin. Στη συνέχεια θα αναλυθούν τα βασικότερα μοντέλα πρόβλεψης πάτου/κορυφής της αγοράς του Bitcoin.

5.4.1. Το Μοντέλο Bitcoin Stock-to-Flow

Το Stock to flow είναι ένα εργαλείο πρόβλεψης για την τιμή του Bitcoin. Το 'Stock to Flow' (S/F) είναι ένα δημοφιλές μοντέλο που στηρίζεται στο αξίωμα ότι η μειωμένη προσφορά ενός περιουσιακού στοιχείου οδηγεί σε μακροπρόθεσμη αύξηση της τιμής του.



Γράφημα 1 Το μοντέλο «Stock-to-flow»

Το εν λόγω μοντέλο, δημιουργεί μια γραμμή στο παραπάνω γράφημα που δείχνει ένα εκτιμώμενο επίπεδο τιμών με βάση τον αριθμό των bitcoin που είναι διαθέσιμα στην αγορά σε σχέση με την ποσότητα που παράγεται (εξορύσσεται) κάθε χρόνο. Ειδικότερα, το «Stock-to-flow» είναι ένας αριθμός που δείχνει πόσα χρόνια, με τον τρέχοντα ρυθμό παραγωγής, απαιτούνται για να επιτευχθεί το τρέχον απόθεμα. Όσο μεγαλύτερος είναι ο αριθμός, τόσο υψηλότερη είναι η τιμή. Η βαθμολογία στη γραμμή "απόθεμα σε ροή" είναι η προβλεπόμενη τιμή για το bitcoin τη συγκεκριμένη στιγμή. Καθώς η ποσότητα των προς εξόρυξη bitcoin μειώνεται με την πάροδο του χρόνου, ο αριθμός αποθεμάτων προς ροή (αναλογία s2f) αυξάνεται, καθώς η προσφορά που εισρέει στην αγορά μειώνεται. Αυτός είναι ο λόγος για τον οποίο αυτό το μοντέλο προβλέπει ότι η τιμή του Bitcoin θα αυξηθεί στο μέλλον (Pedregosa, 2019).

Το μοντέλο stock-to-flow αντιμετωπίζει το Bitcoin ως συγκρίσιμο με εμπορεύματα και πολύτιμα μέταλλα όπως ο χρυσός, το ασήμι ή η πλατίνα. Αυτά είναι γνωστά ως εμπορεύματα «αποθήκης αξίας» επειδή διατηρούν την αξία τους για μεγάλα χρονικά διαστήματα λόγω της σχετικής σπανιότητάς τους. Υπό αυτή την έννοια, είναι δύσκολο να αυξηθεί σημαντικά η προσφορά τους. Για παράδειγμα, η διαδικασία αναζήτησης χρυσού και στη συνέχεια εξόρυξής του είναι δαπανηρή και απαιτεί χρόνο και πόρους. Το Bitcoin είναι παρόμοιο επειδή είναι επίσης σπάνιο. Στην πραγματικότητα, είναι το πρώτο σπάνιο ψηφιακό αντικείμενο που υπάρχει. Υπάρχει περιορισμένος αριθμός νομισμάτων και θα χρειαστεί πολλή ηλεκτρική ενέργεια και υπολογιστική προσπάθεια για την εξόρυξη των 2 εκατομμυρίων νομισμάτων που εξακολουθούν να είναι υπό εξόρυξη. Ως εκ τούτου, το ποσοστό προσφοράς είναι σταθερά χαμηλό. (Pedregosa, 2019).

Το μοντέλο Stock-to-Flow (S2F) είναι εξαιρετικά χρήσιμο για επενδυτές και εμπόρους Bitcoin, γιατί μπορεί να χρησιμοποιηθεί ως εργαλείο πρόβλεψης για τον εντοπισμό που μπορεί να πάει η τιμή του Bitcoin στο μέλλον. Υπάρχουν πολλοί άλλοι δείκτες που προβλέπουν επίσης την τιμή του Bitcoin, ωστόσο, το

συγκεκριμένο εργαλείο εστιάζει στο χρονοδιάγραμμα προσφοράς του Bitcoin. (Pedregosa, 2019).

Στο παραπάνω διάγραμμα bitcoin, η τιμή επικαλύπτεται πάνω από τη γραμμή αναλογίας Stock-to-Flow. Μπορούμε να δούμε ότι η τιμή συνεχίζει να ακολουθεί το απόθεμα προς τη ροή του Bitcoin με την πάροδο του χρόνου. Η θεωρία, επομένως, προτείνει ότι μπορούμε να προβλέψουμε πού μπορεί να πάει η τιμή παρατηρώντας την προβλεπόμενη γραμμή Stock-to-Flow, η οποία μπορεί να υπολογιστεί από το κατά προσέγγιση χρονοδιάγραμμα εξόρυξης της μελλοντικής εξόρυξης Bitcoin.

Οι χρωματιστές κουκκίδες στη γραμμή τιμής του παραπάνω γραφήματος δείχνουν τον αριθμό των ημερών μέχρι το επόμενο συμβάν υποδιπλασιασμού του Bitcoin (μερικές φορές αποκαλείται «μισό»). Αυτό είναι ένα γεγονός όπου η ανταμοιβή για την εξόρυξη νέων μπλοκ μειώνεται στο μισό, που σημαίνει ότι οι εξορύκτες λαμβάνουν 50% λιγότερα bitcoin για την επαλήθευση των συναλλαγών που πραγματοποιούν.

Η κατά το ήμισυ ανταμοιβή του Bitcoin έχει προγραμματιστεί να πραγματοποιείται κάθε 210.000 μπλοκ - περίπου κάθε τέσσερα χρόνια - έως ότου δημιουργηθεί η μέγιστη προσφορά των 21 εκατομμυρίων bitcoin από το δίκτυο. Αυτό κάνει τον λόγο Stock-to-Flow (σπανιότητα) υψηλότερο, επομένως θεωρητικά η τιμή θα πρέπει να ανέβει.

Η βασική πηγή δεδομένων για το διάγραμμα Bitcoin Stock-to-Flow είναι το χρονοδιάγραμμα προσφοράς για το Bitcoin. Αυτός είναι ο αριθμός των bitcoin που έχουν εξορυχθεί μέχρι σήμερα και θα εξορυχθούν στο μέλλον. Έως σήμερα, η τιμή του Bitcoin σε κάθε προηγούμενο ανοδικό κύκλο ξεπερνάει την τιμή που ορίζει το Stock-to-Flow. Όμως θα πρέπει να επισημανθεί ότι χρειάζεται προσοχή, γιατί σε κάθε καθοδικό κύκλο η τιμή υποχωρεί σημαντικότερα από την τιμή που ορίζει το μοντέλο Stock-to-Flow.

5.4.2. Το μοντέλο Bitcoin Rainbow

Το Rainbow Chart είναι ένα μακροπρόθεσμο εργαλείο αποτίμησης για το Bitcoin. Χρησιμοποιεί μια λογαριθμική καμπύλη ανάπτυξης για να προβλέψει την πιθανή μελλοντική κατεύθυνση των τιμών του Bitcoin. Επικαλύπτει τις χρωματικές ζώνες του ουράνιου τόξου πάνω από το κανάλι της λογαριθμικής καμπύλης ανάπτυξης σε μια προσπάθεια να τονίσει το συναίσθημα της αγοράς σε κάθε στάδιο χρώματος ουράνιου τόξου καθώς η τιμή κινείται μέσα από αυτό. Ως εκ τούτου, το μοντέλο, επισημαίνει και προτείνει πιθανές ευκαιρίες για αγορά ή πώληση. Με βάση το εν λόγω μοντέλο, έως σήμερα, η τιμή του bitcoin συνέχισε να παραμένει εντός των χρωμάτων του ουράνιου τόξου του καναλιού λογαριθμικής ανάπτυξης (Alex & Au, 2015).

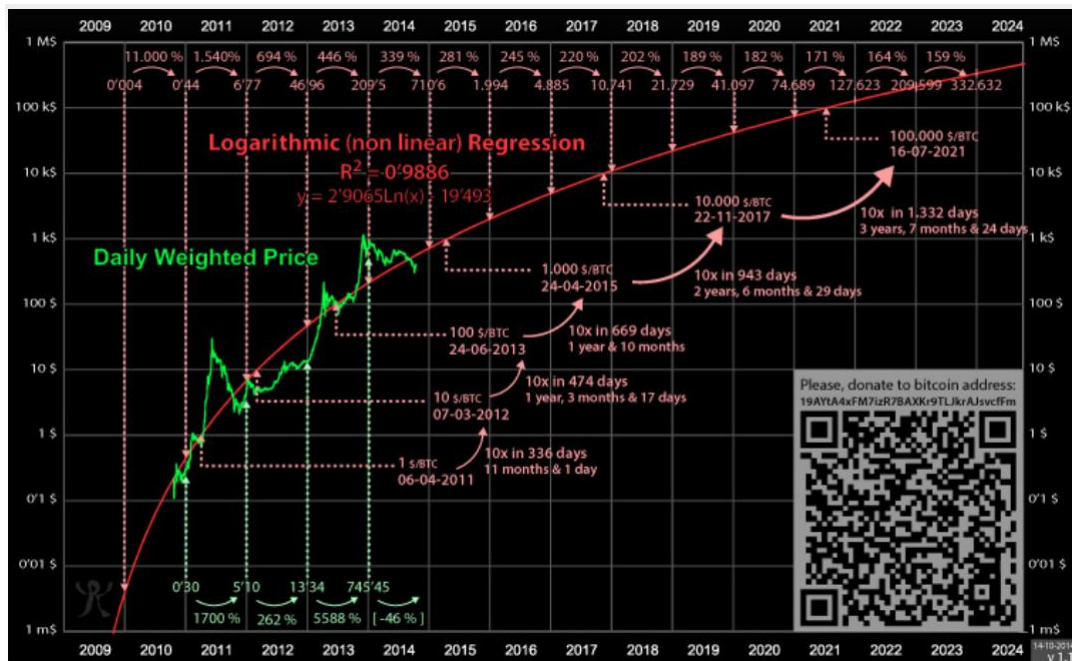
Επειδή το Bitcoin εξακολουθεί να είναι μια σχετικά νέα κατηγορία περιουσιακών στοιχείων, οι κινήσεις των τιμών του είναι εξαιρετικά ασταθείς. Αν και σε ένα μακροχρονοδιάγραμμα υιοθετείται το Bitcoin, το οποίο μπορούμε να δούμε στη γενική ανοδική κίνηση της τιμής, βιώνει κύκλους της αγοράς.. Κατά τη διάρκεια αυτών των κύκλων της αγοράς, η τιμή του Bitcoin μπορεί να αυξηθεί παραβολικά και επίσης να πέσει πολύ γρήγορα. Έχει επίσης πολύ υψηλή ημερήσια αστάθεια την οποία πρέπει να γνωρίζουν οι επενδυτές (Alex & Au, 2015).

Το διάγραμμα Bitcoin Rainbow υπογραμμίζει πού βρίσκεται η τιμή του Bitcoin σε αυτούς τους κύκλους και παρέχει μια άποψη για τη στρατηγική των επενδυτών. Τα πιο ζεστά επάνω χρώματα του γραφήματος του ουράνιου τόξου δείχνουν πότε η αγορά είναι πιθανό να υπερθερμανθεί. Τέτοιες περιόδους έχουν αποδειχθεί ιστορικά ότι είναι καλές στιγμές για τον στρατηγικό επενδυτή να αρχίσει να παίρνει κάποια κέρδη.

Όταν η τιμή πέφτει προς τα πιο ψυχρά χρώματα, το γενικό κλίμα της αγοράς βρίσκεται συνήθως σε ύφεση και πολλοί επενδυτές δεν ενδιαφέρονται για

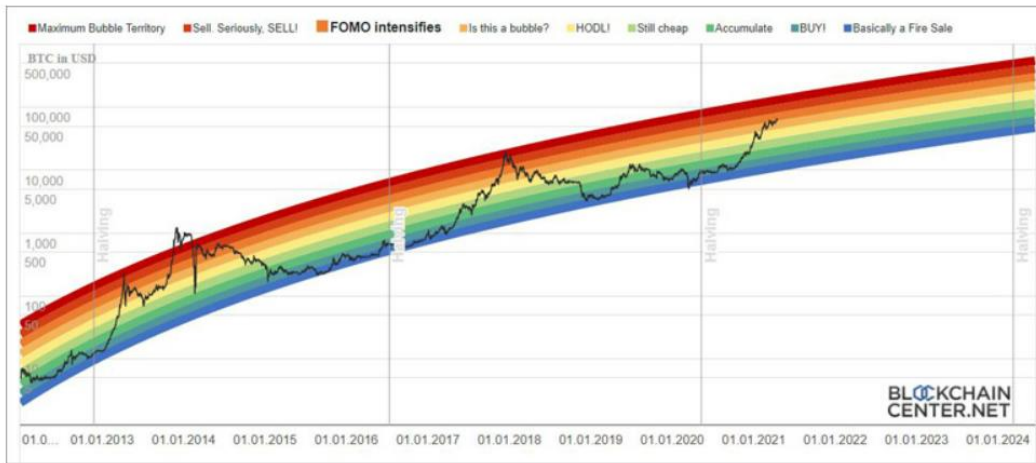
το Bitcoin. Το διάγραμμα Rainbow υπογραμμίζει ότι αυτές οι περιόδους είναι συνήθως εξαιρετικές στιγμές για τον στρατηγικό επενδυτή να συγκεντρώσει περισσότερα Bitcoin.

Το πρώτο παράδειγμα καμπύλης λογαριθμικής παλινδρόμησης για το Bitcoin δημιουργήθηκε από τον χρήστη του Bitcoin Talk trolololo. Αυτό είναι το αρχικό γράφημα, το οποίο δείχνει πώς η τιμή \$BTC θα μπορούσε δυνητικά να εξελιχθεί με την πάροδο του χρόνου χρησιμοποιώντας ανάλυση παλινδρόμησης ανάπτυξης καταγραφής:



Γράφημα 2 Το πρώτο διάγραμμα για την πρόβλεψη της τιμής του Bitcoin που δημιουργήθηκε με το μοντέλο Bitcoin Rainbow

Το επόμενο γράφημα που ακολουθεί είναι ένα λογαριθμικό γράφημα του Bitcoin από τότε που διαθέτουμε στοιχεία για το Bitcoin.



Γράφημα 3 Διάγραμμα για την πρόβλεψη της τιμής του Bitcoin που δημιουργήθηκε με το μοντέλο Bitcoin Rainbow, με βάση όλα τα διαθέσιμα στοιχεία που υπάρχουν για την αγορά του Bitcoin

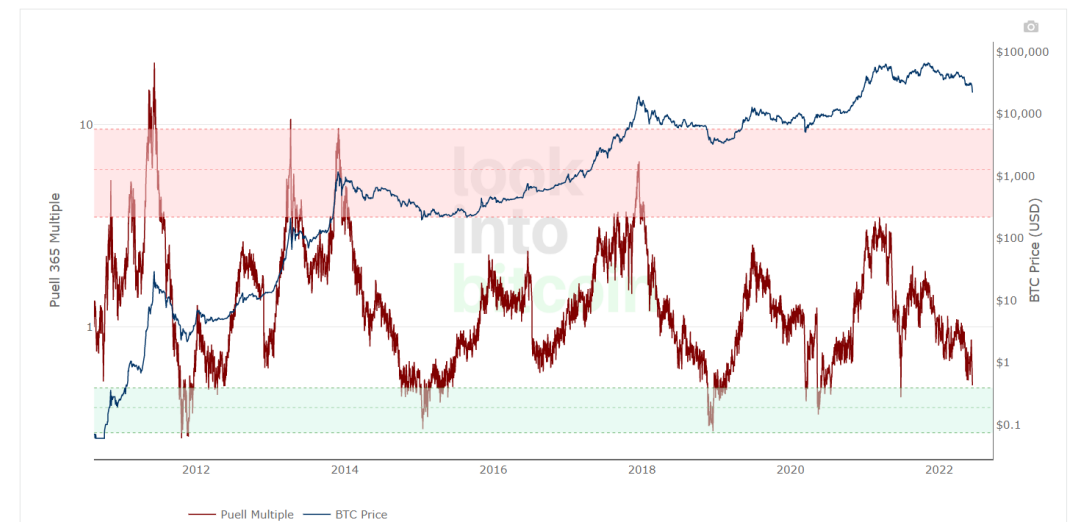
Σύμφωνα με αυτό το μοντέλο, μπορούμε να παρατηρήσουμε ότι σήμερα είμαστε πολύ ψηλά, αλλά πιθανότατα όχι ακόμα πλησίον της κορυφής του ανοδικού κύκλου. Παράλληλα όπως φαίνεται από το διάγραμμα η κορυφή του 2017 σχηματίστηκε σε χαμηλότερο χρωματικό επίπεδο από την προηγούμενη κορυφή του 2013. Μένει να αποδειχθεί εάν η κορυφή του παρόντος ανοδικού κύκλου θα σχηματιστεί σε χαμηλότερο χρωματικό επίπεδο από την κορυφή του 2017. Γεγονός απόλυτα φυσιολογικό, καθώς υπό την παρουσία θεσμικών επενδυτών η μεταβλητότητα της τιμής του Bitcoin ιστορικά βαίνει μειούμενη.

5.4.3. Το Μοντέλο Puell Multiple

Το συγκεκριμένο μοντέλο πρόβλεψης των τιμών του Bitcoin εξετάζει την πλευρά της προσφοράς της οικονομίας του Bitcoin - τους εξορύκτες bitcoin και τα έσοδά τους. Εξερευνά τους κύκλους της αγοράς από την άποψη των εσόδων εξόρυξης. Οι εξορύκτες Bitcoin μερικές φορές αναφέρονται ως υποχρεωτικοί πωλητές λόγω της ανάγκης τους να καλύψουν σταθερό το κόστος υλικού εξόρυξης

σε μια αγορά όπου η τιμή είναι εξαιρετικά ασταθής. Τα έσοδα που παράγουν μπορούν επομένως να επηρεάσουν την τιμή με την πάροδο του χρόνου. Το Puell Multiple υπολογίζεται διαιρώντας την ημερήσια αξία έκδοσης των bitcoin (σε USD) με τον κινητό μέσο όρο 365 ημερών της ημερήσιας αξίας έκδοσης (Phaladisailoed & Numnonda, 2018).

Υπάρχουν χρονικές περιόδους όπου η αξία των bitcoin που εξορύσσονται και εισέρχονται στο οικοσύστημα είναι πολύ μεγάλη ή πολύ μικρή σε σχέση με προγενέστερες αξίες. Η κατανόηση αυτών των χρονικών περιόδων μπορεί να είναι επωφελής για τον στρατηγικό επενδυτή Bitcoin.



Γράφημα 4 Το μοντέλο Puell Multiple

Το παραπάνω διάγραμμα επισημαίνει περιόδους όπου η αξία των Bitcoin που εκδίδονται σε καθημερινή βάση ήταν ιστορικά εξαιρετικά χαμηλή (η Puell Multiple εισέρχεται στο πράσινο πλαίσιο), η οποία παρήγαγε μεγάλες αποδόσεις για τους επενδυτές Bitcoin που αγόρασαν Bitcoin. Δείχνει επίσης περιόδους όπου η ημερήσια αξία έκδοσης ήταν εξαιρετικά υψηλή (το Puell Multiple εισάγει το κόκκινο πλαίσιο), παρέχοντας συμφέρουσα κερδοφορία για τους επενδυτές Bitcoin που πούλησαν στις συγκεκριμένες περιόδους (Phaladisailoed & Numnonda, 2018).

Όσον αφορά την πρόβλεψη τιμών Bitcoin με χρήση αυτού του εργαλείου, το Puell Multiple χρησιμοποιεί την επάνω κόκκινη ζώνη στο γράφημα για να δείξει πότε τα έσοδα των εξορυκτών σε όρους USD είναι σημαντικά υψηλότερα από τα ιστορικά πρότυπα (σε αυτήν την περίπτωση ο κινητός μέσος όρος 365 ημερών). Το μοντέλο διαιρεί την ημερήσια αξία έκδοσης των νέων Bitcoin με τον κινούμενο μέσο όρο έκδοσης των τελευταίων 365 ημερών. Δηλαδή, το Puell Multiple είναι σε θέση να αναγνωρίσει πότε η τιμή του Bitcoin είναι μη βιώσιμα υψηλή ή χαμηλή χρησιμοποιώντας την επάνω κόκκινη ζώνη και την κάτω πράσινη ζώνη. Κατά την πλειονότητα της ύπαρξης των Bitcoin, αυτές οι περίοδοι ήταν όταν η τιμή του \$BTC έφτασε επίσης στα μεγάλα υψηλά της. Έτσι, το Puell Multiple μπορεί να είναι ένα χρήσιμο εργαλείο πρόβλεψης Bitcoin για να προσδιορίσουν οι χρήστες, με βάση αυτή τη μέτρηση εάν η τιμή είναι πολύ υψηλή και πρέπει να πέσει (όταν ο δείκτης βρίσκεται στην κόκκινη ζώνη) ή εάν είναι πολύ χαμηλός και μπορεί να χρειαστεί να αναπηδήσει (όταν ο δείκτης βρίσκεται στην πράσινη ζώνη). (Phaladisailoed & Numnonda, 2018).

5.4.4. Το Μοντέλο Mayer Multiple

Το Mayer Multiple δημιουργήθηκε από την Trace Mayer ως ένας τρόπος ανάλυσης της τιμής του Bitcoin σε ένα ιστορικό πλαίσιο. Δεν λέει αν οι επενδυτές, θα αγοράσουν, θα πουλήσουν, ή θα κρατήσουν. Το μοντέλο Mayer Multiple το οποίο είναι ένα απλό μοντέλο ανάλυσης της ιστορικής τιμής του Bitcoin, υπολογίζει πόσο απέχει η τρέχουσα τιμή από τον κινητό μέσο όρο των 200 ημερών. Όσο μεγαλύτερο το Mayer Multiple τόσο πιο ακριβή είναι η αγορά. Παρατηρώντας το παρελθόν, το μοντέλο είναι χρήσιμο στον εντοπισμό των κορυφών και των πάτων κάθε ανοδικού/καθοδικού κύκλου (Pant, 2018).



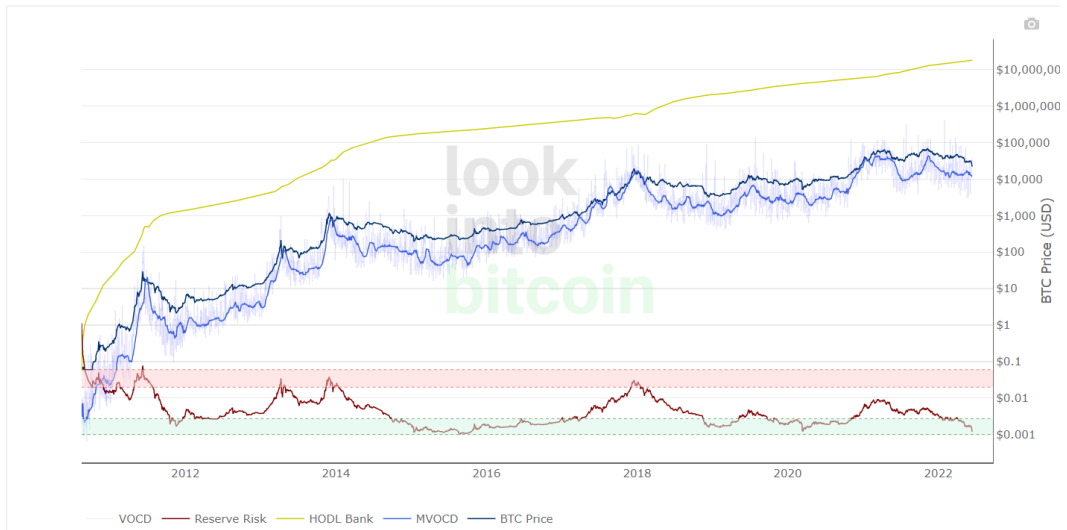
Γράφημα 5 Το μοντέλο Mayer Multiple

Το Mayer Multiple, είναι δηλαδή ένας ένας τρόπος μέτρησης της τρέχουσας τιμής του Bitcoin σε σχέση με τις μακροχρόνιες ιστορικές κινήσεις των τιμών του (κινούμενος μέσος όρος 200 ημερών), και το οποίο τονίζει πότε το Bitcoin υπεραγοράζεται ή υπερπωλείται στο πλαίσιο μεγαλύτερου χρονικού διαστήματος. Αξίζει να σημειωθεί καθώς η αγορά γίνεται μεγαλύτερη και λιγότερο ασταθής, οι κορυφές γίνονται λιγότερο υπερβολικές. Αυτό οφείλεται στο ότι η κύρια γραμμή βάσης του κινούμενου μέσου όρου 200 ημερών είναι ένα στατικό κριτήριο έναντι μιας συνεχώς αναπτυσσόμενης, πιο σταθερής αγοράς Bitcoin (Pant, 2018).

5.4.5.Bitcoin Reserve Risk

Το Bitcoin Reserve Risk είναι ένα διάγραμμα bitcoin που μας επιτρέπει να οπτικοποιήσουμε την εμπιστοσύνη μεταξύ των μακροπρόθεσμων κατόχων bitcoin σε σχέση με την τιμή του Bitcoin σε μια δεδομένη χρονική στιγμή. Όταν η εμπιστοσύνη είναι υψηλή και η τιμή χαμηλή, τότε υπάρχει ένας ελκυστικός κίνδυνος/ανταμοιβή να επενδύσει κανείς σε Bitcoin εκείνη τη στιγμή (πράσινη

ζώνη). Όταν η εμπιστοσύνη είναι χαμηλή και η τιμή είναι υψηλή, τότε το ρίσκο/ανταμοιβή δεν είναι ελκυστικό (κόκκινη ζώνη). Η επένδυση σε Bitcoin σε περιόδους όπου ο κίνδυνος αποθεμάτων βρίσκεται στην πράσινη ζώνη έχει παράγει μεγάλες αποδόσεις με την πάροδο του χρόνου (Munim & Alon, 2019).



Γράφημα 6 Bitcoin Reserve Risk

Τα βήματα που απαιτούνται για τον υπολογισμό του Bitcoin Reserve Risk είναι τα ακόλουθα:

- Bitcoin Days Destroyed (BDD)
- Adjusted Bitcoin Days Destroyed (ABDD)
- Value of Coin (Days) Destroyed (VOCD)
- Median Value of Coin (Days) Destroyed (MVOCD)

- HODL Bank

Τα στοιχεία δείχνουν ότι, γενικά, οι μακροπρόθεσμοι κάτοχοι Bitcoin έχουν μεγαλύτερη γνώση σχετικά με τους κύκλους αγοράς του Bitcoin και τον εντοπισμό των καλών στιγμών για την αγορά και την πώληση Bitcoin. Αυτό δεν αποτελεί έκπληξη, δεδομένου ότι είναι πιο έμπειροι στον χώρο έναντι των νεότερων συμμετεχόντων που μόλις εισέρχονται και μαθαίνουν για το Bitcoin. (Munim & Alon, 2019).

Αυτό μπορεί να οπτικοποιηθεί μέσω των διαδικασιών Bitcoin Days και Bitcoin Days Destroyed:

$\text{Bitcoin Days} = \text{Ποσότητα Bitcoin} * \text{Αριθμός ημερών από τη μετακίνηση των νομισμάτων από το ένα πορτοφόλι χρήστη στο άλλο.}$ Αυτό μας επιτρέπει να αποδώσουμε μεγαλύτερη αξία στα νομίσματα που κατέχουν μακροπρόθεσμοι κάτοχοι – καθώς έχουν στην κατοχή τους νομίσματα που δεν έχουν μετακινηθεί για μεγάλο αριθμό ημερών.

$\text{Bitcoin Days Destroyed} = \text{Όταν ένα bitcoin βρίσκεται σε ένα πορτοφόλι, συγκεντρώνει ημέρες Bitcoin, όταν στη συνέχεια πωλείται, αυτές οι ημέρες "καταστρέφονται"}$ (Munim & Alon, 2019).

5.4.6. Relative Unrealized Profit/Loss

Ο δείκτης μετράει τα κέρδη που έχουν πραγματοποιηθεί αλλά δεν έχουν κατοχυρωθεί ακόμα στο Bitcoin. Όσο μεγαλύτερα είναι τα μη-κατοχυρωμένα κέρδη τόσο πιο πιθανό είναι η αγορά να είναι υπέρ-αγορασμένη. Ειδικότερα ο εν λόγω δείκτης προέρχεται από τον Δείκτη Market Value and Realized Value, η οποία μπορεί να οριστεί ως (Kuhn, 2013):

Market Value - Αγοραία αξία: Η τρέχουσα τιμή του Bitcoin πολλαπλασιαζόμενη με τον αριθμό των κερμάτων σε κυκλοφορία. Αυτό είναι σαν το ανώτατο όριο αγοράς στις παραδοσιακές αγορές, δηλαδή η τιμή της μετοχής πολλαπλασιαζόμενη με τον αριθμό των μετοχών.

Realized Value - Πραγματοποιημένη Αξία: Αντί να παίρνει την τρέχουσα τιμή του Bitcoin, η Πραγματοποιημένη Αξία λαμβάνει την τιμή κάθε Bitcoin κατά την τελευταία μετακίνησή του, δηλαδή την τελευταία φορά που στάλθηκε από το ένα πορτοφόλι σε ένα άλλο πορτοφόλι. Στη συνέχεια, αθροίζει όλες αυτές τις μεμονωμένες τιμές και παίρνει έναν μέσο όρο από αυτές. Στη συνέχεια πολλαπλασιάζει αυτή τη μέση τιμή με τον συνολικό αριθμό των κερμάτων σε κυκλοφορία.

Αφαιρώντας την Πραγματοποιημένη Αξία από την Αγοραία Αξία ο δείκτης υπολογίζει το Μη Πραγματοποιημένο Κέρδος/Ζημιά. Τα μη πραγματοποιηθέντα κέρδη/ζημίες υπολογίζουν τα συνολικά κέρδη/ζημίες σε Bitcoin. Αυτό είναι ενδιαφέρον να το γνωρίζουμε, αλλά μεγαλύτερη αξία έχει να προσδιορίσουμε πώς αυτό αλλάζει σχετικά με την πάροδο του χρόνου. Για να γίνει αυτό, μπορούμε να διαιρέσουμε τα Μη πραγματοποιηθέντα κέρδη/ζημίες με την κεφαλαιοποίηση της αγοράς. Αυτό δημιουργεί Σχετικά Μη Πραγματοποιημένα Κέρδη/Ζημίες που είναι πολύ χρήσιμο για την παρακολούθηση του συναισθήματος των επενδυτών με την πάροδο του χρόνου για το Bitcoin (Kuhn, 2013).



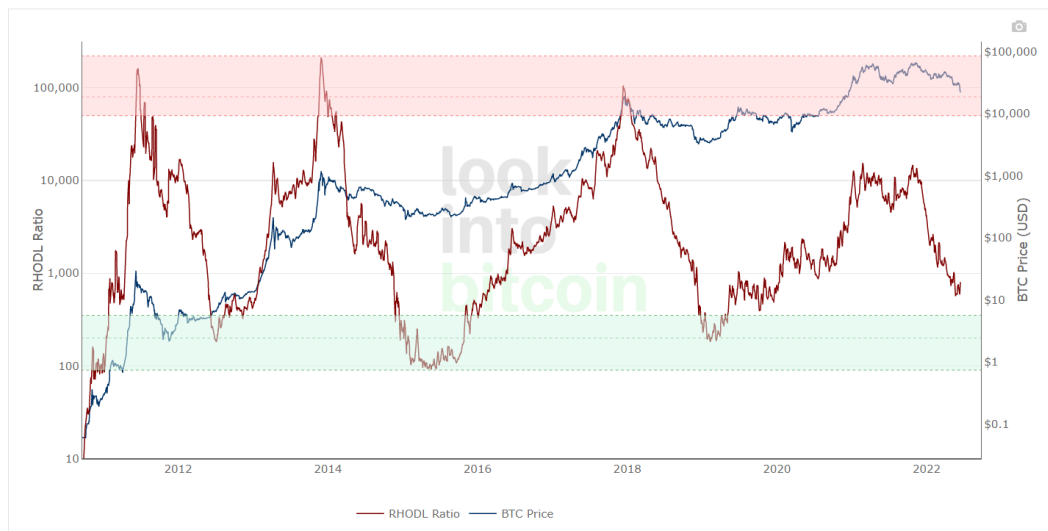
Γράφημα 7 Μοντέλο Relative Unrealized Profit/Loss

Η βασική αρχή αυτού του εργαλείου είναι η αναλογία μεταξύ της κεφαλαιοποίησης της αγοράς και των επενδυτών Bitcoin που λαμβάνουν κέρδη. Όταν η κεφαλαιοποίηση της αγοράς αυξάνεται πολύ πιο γρήγορα από τη λήψη κερδών, βλέπουμε ότι η αγορά υπερθερμαίνεται, θα μπορούσε να πει κανείς λόγω της απληστίας των επενδυτών (κόκκινη ζώνη). Για τον στρατηγικό επενδυτή τέτοιες εποχές ήταν ιστορικά ευνοϊκές για να αποκομίσει κέρδη. Τέλος, μπορούμε να αναλύσουμε διαφορετικά ποσοστά του Σχετικού Μη Πραγματοποιημένου Κέρδους/Ζημίας Bitcoin για να προσδιορίσουμε σε ποιο στάδιο της αγοράς βρισκόμαστε. Αυτό μπορεί να είναι επωφελές για τον μακροπρόθεσμο στρατηγικό επενδυτή (Kuhn, 2013).

5.4.7.RHODL Ratio

Ο δείκτης έχει προσδιορίσει με ακρίβεια την υψηλή τιμή κάθε προηγούμενου μακροοικονομικού κύκλου του Bitcoin, και άρα έχει αρκετό ενδιαφέρον. Ειδικότερα αυτός ο δείκτης χρησιμοποιεί μια αναλογία Realized Value HODL Waves. Συνοπτικά, τα κύματα Realized Value HODL είναι διαφορετικές

ηλικιακές ζώνες των UTXO (νομισμάτων) που σταθμίζονται με την Realized Value των νομισμάτων σε κάθε ζώνη. Η Πραγματοποιημένη Αξία είναι η τιμή των UTXO (νομισμάτων) όταν μεταφέρθηκαν για τελευταία φορά από το ένα πορτοφόλι στο άλλο. Το RHODL Ratio εξετάζει την αναλογία μεταξύ της ζώνης RHODL της 1 εβδομάδας έναντι της ζώνης RHODL των τελευταίων 1-2 ετών. Επίσης, βαθμονομείται για αυξημένη παρακράτηση με την πάροδο του χρόνου και για χαμένα νομίσματα πολλαπλασιάζοντας την αναλογία με την ηλικία της αγοράς σε αριθμό ημερών. Όταν η τιμή της 1 εβδομάδας είναι σημαντικά υψηλότερη από την τιμή του 1-2 έτους είναι ένα σημάδι ότι η αγορά υπερθερμαίνεται (Jang et al., 2018).



Γράφημα 8 RHODL Ratio

Ο δείκτης μπορεί να προσδιορίσει με μεγάλη ακρίβεια την υψηλή τιμή καθενός από τους προηγούμενους μακροοικονομικούς κύκλους του Bitcoin. Επίσης, προσδιορίζει την κορυφή της αγοράς με ακρίβεια εντός λίγων ημερών. Η

αναλογία RHODL που εισέρχεται στην κόκκινη ζώνη σηματοδοτεί ότι η αγορά πλησιάζει στην κορυφή του κύκλου της. Αυτή ήταν ιστορικά μια καλή στιγμή για τους επενδυτές να αποκομίσουν κέρδη σε κάθε κύκλο.

Το RHODL Ratio είναι χρήσιμο για την πρόβλεψη της τιμής του Bitcoin στις ακραίες συνθήκες της αγοράς. Είναι σε θέση να προβλέψει πού μπορεί να χρειαστεί να υποχωρήσει η τιμή του Bitcoin όταν η γραμμή αναλογίας RHODL εισέλθει στην επάνω κόκκινη ζώνη και επίσης πότε η τιμή του \$BTC μπορεί να αυξηθεί μετά από χρόνο που θα περάσει στην κάτω πράσινη ζώνη. Το κάνει αυτό σε υψηλά χρονικά πλαίσια, έτσι έχει ιστορικά εντοπίσει τα μεγάλα υψηλά των τιμών Bitcoin καθ' όλη τη διάρκεια της ύπαρξης των Bitcoin. (Jang et al., 2018).

5.4.8.MVRV Z-Score

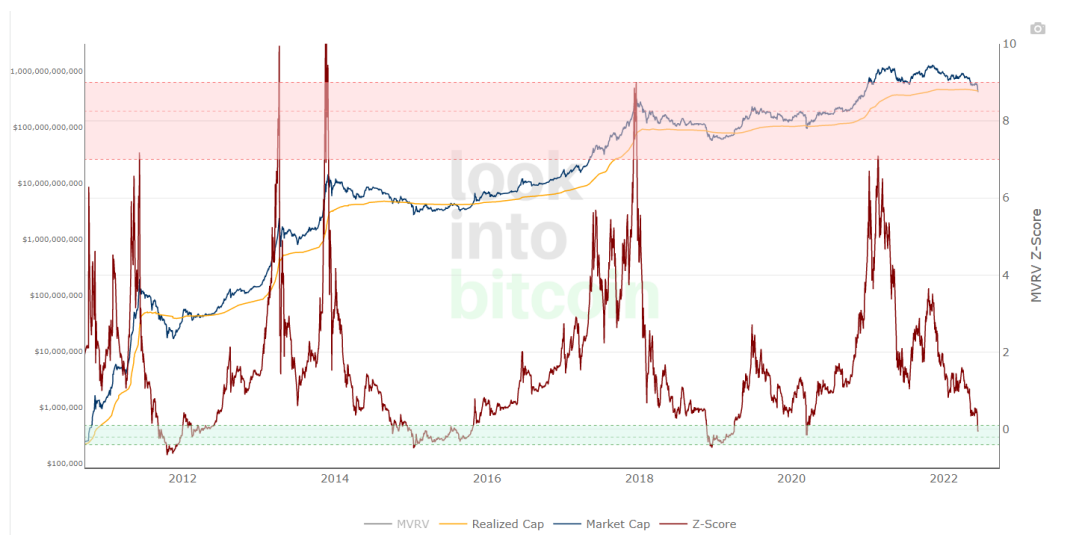
Το MVRV Z-Score είναι ένα διάγραμμα bitcoin που χρησιμοποιεί ανάλυση blockchain για τον εντοπισμό περιόδων όπου το Bitcoin είναι εξαιρετικά υπερτιμημένο ή υποτιμημένο σε σχέση με την «εύλογη αξία» του. Το μοντέλο χρησιμοποιεί τρεις μετρήσεις (Indera et al., 2018):

1. Αγοραία αξία (μπλε γραμμή): Η τρέχουσα τιμή του Bitcoin πολλαπλασιαζόμενη με τον αριθμό των κερμάτων σε κυκλοφορία. Αυτό είναι σαν το ανώτατο όριο αγοράς στις παραδοσιακές αγορές, δηλαδή η τιμή της μετοχής πολλαπλασιαζόμενη με τον αριθμό των μετοχών.

2. Πραγματοποιημένη Αξία (πορτοκαλί γραμμή): Αντί να λαμβάνει την τρέχουσα τιμή του Bitcoin, η Πραγματοποιημένη Αξία λαμβάνει την τιμή κάθε Bitcoin την τελευταία φορά που μετακινήθηκε, δηλαδή την τελευταία φορά που στάλθηκε από ένα πορτοφόλι σε άλλο πορτοφόλι. Στη συνέχεια, αθροίζει όλες αυτές τις μεμονωμένες τιμές και παίρνει έναν μέσο όρο από αυτές. Τέλος, πολλαπλασιάζει αυτή τη μέση τιμή με τον συνολικό αριθμό των κερμάτων σε κυκλοφορία.

Με αυτόν τον τρόπο, αφαιρεί το βραχυπρόθεσμο συναίσθημα της αγοράς που έχουμε στη μέτρηση της Αγοραίας Αξίας. Ως εκ τούτου, μπορεί να θεωρηθεί ως ένα πιο «αληθινό» μακροπρόθεσμο μέτρο της αξίας του Bitcoin, στο οποίο η Αγοραία Αξία κινείται πάνω και κάτω ανάλογα με το κλίμα της αγοράς εκείνη τη στιγμή (Indera et al., 2018).

3. Z-score (κόκκινη γραμμή): Μια δοκιμή τυπικής απόκλισης που εξάγει τα άκρα στα δεδομένα μεταξύ της αγοραίας αξίας και της πραγματοποιηθείσας αξίας.



Γράφημα 9 MVRV Z-Score

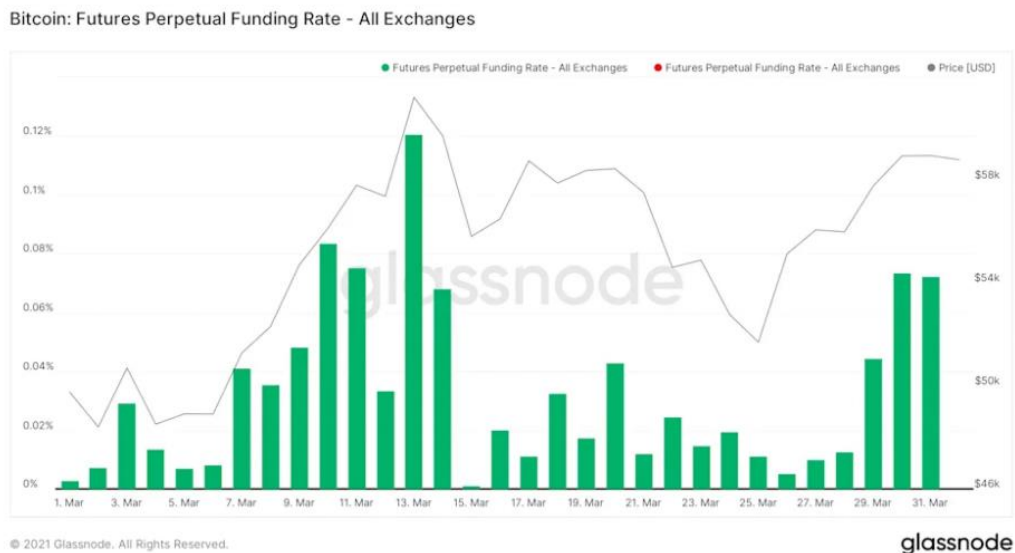
Το MVRV Z-score ήταν ιστορικά πολύ αποτελεσματικό στον εντοπισμό περιόδων όπου η αγοραία αξία κινείται ασυνήθιστα ψηλά πάνω από την πραγματοποιηθείσα αξία. Αυτές οι περιόδους επισημαίνονται με το z-score (κόκκινη γραμμή) που εισάγεται στο ροζ πλαίσιο και υποδεικνύει την κορυφή των κύκλων της αγοράς. (Indera et al., 2018).

Δείχνει επίσης πότε η αγοραία αξία είναι πολύ κάτω από την πραγματοποιηθείσα τιμή, και επισημαίνεται με τη βαθμολογία z που εισάγεται στο πράσινο πλαίσιο. Η αγορά Bitcoin κατά τη διάρκεια αυτών των περιόδων έχει ιστορικά δημιουργήσει μεγάλες αποδόσεις. Το διάγραμμα bitcoin Z-Score MVRV

είναι χρήσιμο για την πρόβλεψη της τιμής του Bitcoin στις ακραίες συνθήκες της αγοράς. Είναι σε θέση να προβλέψει πού μπορεί να χρειαστεί να υποχωρήσει η τιμή του Bitcoin όταν το MVRV Z-score μπει στην επάνω κόκκινη ζώνη, και επίσης πότε η τιμή του \$BTC μπορεί να αυξηθεί αφού περάσει χρόνο στην κάτω πράσινη ζώνη (Indera et al., 2018).

5.4.9.Funding Rates

Το εν λόγω μοντέλο, μετράει το κόστος διατήρησης μιας θέσης long/short. Όταν τα Funding Rates των ανοδικών θέσεων (long) ακριβαίνουν η αγορά θεωρείται υπέρ-αγορασμένη και επικίνδυνη να διορθώσει. Ειδικότερα η μελέτη των δεδομένων on-chain του Bitcoin, συγκεκριμένα στα επιτόκια χρηματοδότησης και στο ανοιχτό ενδιαφέρον, μας επιτρέπει να προσδιορίσουμε πότε οι συνθήκες στη μελλοντική αγορά είναι παράλογες και αναμένεται διόρθωση (Cocco, Tonelli & Marchesi, 2019).

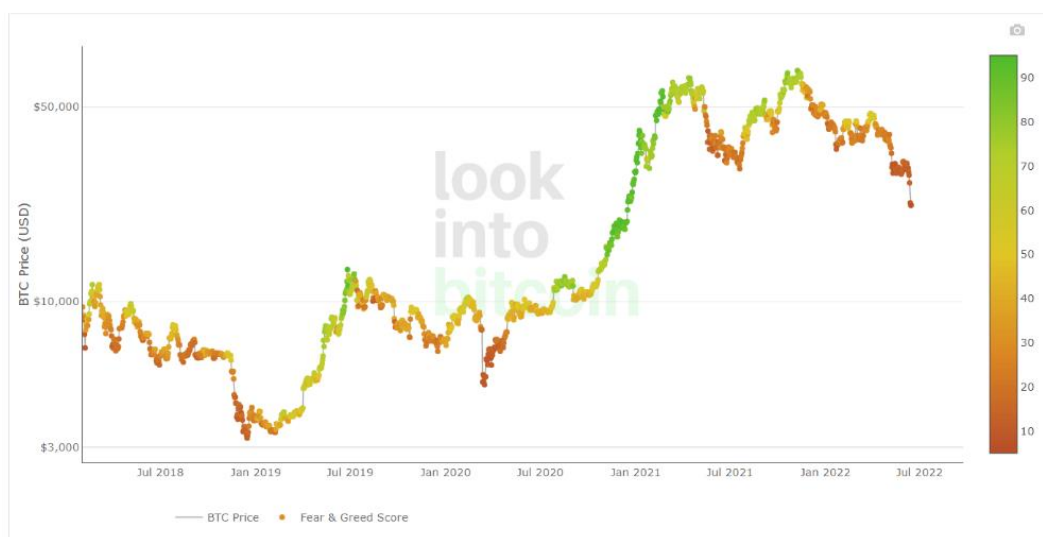


Γράφημα 10 Funding Rates Model

Το μοντέλο υποδεικνύει το επιτόκιο που πρέπει να πληρώσουν (ή να λάβουν οι έμποροι συμβολαίων μελλοντικής εκπλήρωσης) για να διατηρήσουν μια θέση ανοιχτή. Εάν το επιτόκιο χρηματοδότησης είναι θετικό, οι έμποροι με ανοιχτή θέση αγοράς πρέπει να πληρώσουν ένα premium για να διατηρήσουν την αγορά ανοιχτή. Εάν το επιτόκιο χρηματοδότησης είναι αρνητικό, οι έμποροι με μια short θέση πρέπει να πληρώσουν ένα premium για να διατηρήσουν την αγορά ανοιχτή (Cocco, Tonelli & Marchesi, 2019).

5.4.10.Fear & Greed Index

Το εν λόγω μοντέλο, μετράει την απληστία και τον φόβο της αγοράς σε κλίμακα (0-100). Πάνω από 90 δείχνει μια υπέρ-αγορασμένη αγορά, και κάτω από 20 μια υπέρ-πουλημένη αγορά. Ειδικότερα μέσω του μοντέλου, δημιουργείται ένας δείκτης για τη μέτρηση της απληστίας και του φόβου των επενδυτών στην αγορά κρυπτονομισμάτων. Χρησιμοποιείται για την ανάλυση της συμπεριφοράς των επενδυτών στην αγορά κρυπτογράφησης. Όταν συμβαίνουν σημαντικά γεγονότα στην αγορά, είτε θετικά είτε αρνητικά, οι επενδυτές λαμβάνουν ειδήσεις αμέσως και μπορούν να λάβουν αποφάσεις αμέσως χωρίς να χρειάζεται να περιμένουν να ανοίξει η αγορά κατά τις εργάσιμες ώρες (Cocco, Tonelli & Marchesi, 2019).



Γράφημα 11 Fear & Greed Index

Ο δείκτης Crypto Fear and Greed κυμαίνεται από 0 έως 100, όπου το 0 αντιπροσωπεύει την κατάσταση ακραίου φόβου μεταξύ των επενδυτών που μπορεί να προκαλέσει ισχυρή πίεση πωλήσεων. Η τιμή του 100 έχει το αντίθετο νόημα: οι επενδυτές γίνονται εξαιρετικά άπληστοι. Μπορεί ωστόσο να υπάρχει κάποια αγοραστική δυναμική που προκαλείται από το FOMO. Ειδικότερα, παρά τις όποιες θετικές του συνεισφορές το μοντέλο συνδέεται και με κινδύνους αν φανταστεί κανείς τι μπορεί να γίνει καθώς οι επενδυτές σε όλο τον κόσμο λαμβάνουν τα νέα ταυτόχρονα. Αυτό μπορεί να προκαλέσει συμπεριφορά με τον τρόπο «αγοράς FOMO» ή «πώλησης πανικού» πιο εύκολα από άλλες επενδυτικές αγορές. Ωστόσο όταν υπάρχει εισροή ζήτησης για αγορά ή πώληση σε αυτήν την αγορά 24 ώρες το 24ωρο, ο δείκτης Crypto Fear and Greed Index χρησιμοποιείται για την ανάλυση της συμπεριφοράς των επενδυτών για τη βελτίωση της διαδικασίας λήψης αποφάσεων. Ως εκ τούτου, κανείς δεν δεσμεύεται και δεν επηρεάζεται από τη διάθεση της αγοράς που μπορεί κάλλιστα οι επενδυτές να ακολουθήσουν καλύτερα τα επενδυτικά τους σχέδια (Cocco, Tonelli & Marchesi, 2019).

5.4.11. Μοντέλα πρόβλεψης τιμών μέσω των κινήσεων των Μεγάλων Επενδυτών

Ενώ η παραδοσιακή οικονομία είναι σε πολύ μεγάλο βαθμό αδιαφανής, αντίθετα η αγορά των κρυπτονομισμάτων στηρίζεται στην ουσιαστική διαφάνεια των συναλλαγών. Εξάλλου, δεν θα μπορούσε να είναι και διαφορετικά καθώς στην αγορά των κρυπτονομισμάτων, τα πάντα καταγράφονται στην αλυσίδα (blockchain). Έτσι κάθε επενδυτής, είναι σε θέση να δει τι κάνουν οι άλλοι, τόσο σε μεμονωμένη βάση όσο και σε συγκεντρωτική (Chen, Li & Sun, 2020).

1-Bitcoin Rich List

Στην εν λόγω εφαρμογή μπορεί κανείς να δει ανά ημέρα, αλλά και αθροιστικά, τις μεταβολές όλων των πλούσιων κατόχων του Bitcoin.

1. Top 100 Richest Bitcoin Addresses

#	Address	Balance
1	16ftSEQ4ctQFDtVZiUBusQUjRrGhM3JYwe	168,791 BTC
2	3D2oetdNuZUqQHPJmcMDDHYoqkyNVsFk9r	144,467 BTC
3	16rCmCmbuWDhPjWTrpQGau3EPdZF7MTdUk	107,203 BTC
4	3Cbq7aT1tY8kMxWLbitaG7yT6bPbKChq64	98,042 BTC
5	3Nxwenay9Z8Lc9JBiywExpnEFilp6Afp8v	97,848 BTC
6	183hmJGRuTEi2YDCWy5iozY8rZtFwVgahM	85,947 BTC
7	1FeexV6bAHb8ybZjqQMjJrcCrHGw9sb6uF	79,957 BTC
8	18rnfoQgGo1HqvVQaAN4QnxjYE7Sez9eca	73,600 BTC

Γράφημα 12 Bitcoin Rich List

2-Bitcoin WallStreet Treasuries

Το εν λόγω μοντέλο προβλέπει τις τιμές του Bitcoin μέσω μελέτης των εισηγμένων εταιρειών στη WallStreet που επενδύουν στο Bitcoin.

Bitcoin Treasuries

Totals by Category

Category	# of BTC	Value Today	% of 21m
ETFs ↗	828,641	\$17,958,729,779	3.946%
Countries ↗	50,699	\$1,098,774,549	0.241%
Public Companies ↗	268,271	\$5,814,105,742	1.277%
Private Companies ↗	202,068	\$4,379,320,609	0.962%
Totals:	1,359,781	\$29,469,866,368	6.475%

Γράφημα 13 Λίστα των εισηγμένων εταιριών της WallStreet που επενδύουν στο Bitcoin

3-Διαθέσιμο Bitcoin στα Ανταλλακτήρια

Το συγκεκριμένο εργαλείο πρόβλεψης τιμών του Bitcoin βασίζεται στη λογική πως όσο λιγότερο Bitcoin κατέχουν τα ανταλλακτήρια τόσο το καλύτερο. Ειδικότερα όταν αυξάνεται σε μια περίοδο απότομα το Bitcoin στα Ανταλλακτήρια αυτό αποτελεί μια ένδειξη ότι πιθανότατα οι μεγάλοι παίχτες ετοιμάζονται να πουλήσουν.

ΣΥΜΠΕΡΑΣΜΑΤΑ – ΕΠΙΛΟΓΟΣ

Εν όψει των καινοτόμων χαρακτηριστικών της αποκέντρωσης και της ιχνηλασιμότητας του bitcoin, το bitcoin έχει προσελκύσει εκτεταμένη προσοχή από τα μέσα ενημέρωσης και τους επενδυτές. Μετά την άνοδο και την πτώση των τιμών των κρυπτονομισμάτων τα τελευταία χρόνια, το bitcoin θεωρείται όλο και περισσότερο ως επενδυτικό περιουσιακό στοιχείο. Οι επενδυτές βλέπουν το bitcoin ως μια κερδοσκοπική επένδυση, παρόμοια με τις μετοχές του Διαδικτύου του περασμένου αιώνα. Το Bitcoin ως κρυπτονόμισμα εμφανίζεται για μικρό χρονικό διάστημα σε σύγκριση με το κρατικό νόμισμα. Σε αντίθεση με το κρατικό νόμισμα, όμως, το bitcoin είναι ένα αποκεντρωμένο ψηφιακό νόμισμα χωρίς καμία κρατική πιστωτική υποστήριξη, επομένως η τιμή του bitcoin είναι εξαιρετικά ασταθής. Παράγει πολύ μεγαλύτερη μεταβλητότητα από τα κρατικά νομίσματα. Η τιμή του αυξήθηκε από μηδενική αξία όταν ιδρύθηκε το 2009, σε περίπου 13 \$ ανά bitcoin τον Ιανουάριο του 2013 και στη συνέχεια εκτινάχθηκε στα 20.000 \$ ανά bitcoin τον Δεκέμβριο του 2017. Σήμερα βέβαια το Bitcoin, το μεγαλύτερο ψηφιακό νόμισμα στον κόσμο έχει φθάσει τις \$20.824, που είναι το πιο χαμηλό σημείο από τον Δεκέμβριο του 2020 και κάτω από το 1 τρις. δολάρια η παγκόσμια κεφαλαιοποίηση της αγοράς crypto.

Ιδιαίτερος αξιοσημείωτος είναι δε, οι παράγοντες που επηρεάζουν τις τιμές του bitcoin. Εκτός από τους εσωτερικούς παράγοντες όπως το μέγεθος μπλοκ, το ποσοστό κατακερματισμού, η δυσκολία εξόρυξης, ο όγκος συναλλαγών και η αγοραία αξία του bitcoin, άλλοι παράγοντες όπως ο δείκτης αναζήτησης Google και Baidu αποτελούν μεταξύ άλλων παράγοντες, που επηρεάζου το bitcoin, επειδή είναι ένας σημαντικός δείκτης για τη μέτρηση της προσοχής των επενδυτών και της διαφημιστικής εκστρατείας των μέσων ενημέρωσης και αντανακλά το συναίσθημα της άκρως κερδοσκοπικής αγοράς κρυπτονομισμάτων. Δεύτερον, άλλοι παράγοντες όπως τα μεγάλα γεγονότα και το συναίσθημα των επενδυτών που

προκαλούνται από τις οικονομικές πολιτικές επηρεάζουν επίσης επίσης την τιμή του bitcoin. Παράλληλα, υπάρχει καλή αλληλεπίδραση μεταξύ της τιμής του bitcoin και της τιμής του χρυσού. Εξάλλου μελέτες έχουν αποδείξει την ομοιότητα μεταξύ του bitcoin, του χρυσού και του δολαρίου ΗΠΑ μέσω του μοντέλου GARCH. Επομένως τόσο η τιμή του χρυσού όσο και ο δείκτης του δολαρίου αποτελούν παράγοντες που επηρεάζουν την τιμή του bitcoin. Λαμβάνοντας υπόψη τους παραπάνω παράγοντες είναι προφανές ότι το πρόβλημα της απλοποίησης της πρόβλεψης της τιμής του bitcoin αποτελεί ένα ζήτημα αιχμής για τους επενδυτές παγκοσμίως. Από τότε που άρχισε να διαπραγματεύεται το bitcoin, η εξαιρετικά ασταθής φύση του μαστίζει τους επενδυτές και μπορεί να είναι μια φούσκα, που απειλεί τη σταθερότητα του χρηματοπιστωτικού συστήματος. Επομένως, είναι απαραίτητο να γίνει μια καλή πρόβλεψη της τιμής του ειδικού νομίσματος. Η δυνατότητα πρόβλεψης της τάσης των τιμών του bitcoin είναι ένα πρακτικό πρόβλημα. Δεν επηρεάζει μόνο την οικονομική πολιτική μιας χώρας σε μακροοικονομικό επίπεδο, αλλά επηρεάζει επίσης έντονα την απόφαση των επενδυτών να αγοράσουν και να πουλήσουν επενδυτικά μέσα σε μικροεπίπεδο. Μια όσο το δυνατόν ακριβής πρόβλεψη της τιμής του bitcoin όχι μόνο μπορεί να παρέχει υποστήριξη απόφασης στους επενδυτές αλλά επίσης να παρέχει αναφορά στην κυβέρνηση για τη διαμόρφωση ρυθμιστικών πολιτικών.

Υπάρχει σημαντική εξέλιξη όπως αναλύθηκε στο πλαίσιο της παρούσας εργασίας, αναφορικά με τα μοντέλα πρόβλεψης της τιμής του Bitcoin. Παράλληλα ωστόσο είναι γεγονός ότι η πρόβλεψη της τιμής του bitcoin βρίσκεται ακόμη σε αρχικό στάδιο. Αυτό σημαίνει ότι στο σχετικό πεδίο υπάρχει ανάγκη προφανώς να προταθούν στο εγγύς μέλλον κι άλλα μοντέλα, πιο εξελιγμένα από τα ήδη υπάρχοντα τα οποία θα διαθέτουν πλεονεκτήματα στην πρόβλεψη τιμών bitcoin, και που θα βελτιώσουν ενδεχόμενα προβλήματα στα υφιστάμενα μοντέλα στα οποία η ανισορροπία και η κακή ακεραιότητα των σχετικών δεδομένων μπορεί να οδηγήσει σε προβλήματα χαμηλής ακρίβειας, χαμηλής ευρωστίας και εύκολης κατάρρευσης.

Βιβλιογραφικές αναφορές

- Abubakar, Y., Ogunbado, A., & Saidi, M. (2018). Bitcoin and its legality from Shariah point of view. *Seisense Journal of Management*, 1(4), 13-21
- Adhami S, Giudici G, Martinazzi S (2018) Why do businesses go crypto? An empirical analysis of initial coin offerings. *J Econ Bus* 100:64–75
- Akbulaev N., Mammadov I. & Hemdullayeva M. Correlation and Regression Analysis of the Relation between Ethereum Price and Both Its Volume and Bitcoin Price. *The Journal Of Structured Finance*. 26, 46–56 (2020).
- Alex, G. and Au. B. (2015) Using the Bitcoin Transaction Graph to Predict the Price of Bitcoi
- Andolfatto, D., & Spewak, A. (2019). Whither the price of Bitcoin? *Economic Synopses*, 1, 1-2.
- Andolfatto, D., & Spewak, A. (2019). Whither the price of Bitcoin? *Economic Synopses*, 1, 1-2
- Beer et al. Bitcoin — the promise and limits of private innovation in monetary and payment systems *Monet Policy Econ* (2014)
- Blau, B. M. (2017). Price dynamics and speculative trading in bitcoin. *Research in International Business and Finance*, 41:493–499
- Blau, B. M. (2018). Price dynamics and speculative trading in Bitcoin. *Research in International Business and Finance*, 43, 15-21.
- Bornholdt, S., & Sneppen, K. (2014). Do Bitcoins make the world go round? On the dynamics of competing crypto-currencies. *arXiv preprint arXiv:1403.6378*.
- Bouri E., Roubaud D. & Shahzad S. Do Bitcoin and other cryptocurrencies jump together?. *The Quarterly Review Of Economics And Finance*. 76 pp. 396–409 (2020).

- Bradbury, D. (2013). The Problem with Bitcoin. *Computer Fraud & Security*, 2013, 5-8.
- Bunea, Sinziana, Benjamin Kogan, and David Stolin. 2016. Banks vs. fintech—At last, it's official. *Journal of Financial Transformation* 44: 122–31.
- Carrick J. Bitcoin as a complement to emerging market currencies. *Emerging Markets Finance And Trade*. 52, 2321–2334 (2016).
- Casino, F., Dasaklis, T. K., and Patsakis, C. (2018). A systematic literature review of blockchain-based applications: current status, classification and open issues. *Telemat. Informat.* 36, 55–81.
- Catalini, C., and Gans, J. S. (2016). Some Simple Economics of the Blockchain. Rotman School of Management Working Paper No. 2874598, MIT Sloan Research Paper No. 5191-16. Social Science Research Network (SSRN).
- Chen Z, Li C, Sun W. Bitcoin price prediction using machine learning: an approach to sample dimension engineering. *Journal of Computational and Applied Mathematics*. 2020;365(1):112395. doi: 10.1016/j.cam.2019.112395.
- Christidis, K., and Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *IEEE Access* 4, 2292–2303.
- Claessens, Stijn, Jon Frost, Grant Turner, and Feng Zhu. 2018. Fintech Credit Markets around the World: Size, Drivers and Policy Issues. *BIS Quarterly Review*. Basel: BIS, September.
- Cocco L, Tonelli R, Marchesi M. An agent-based artificial market model for studying the bitcoin trading. *IEEE Access*. 2019;7(42908):42920.
- Conley, J. P. (2017). “Blockchain and the economics of crypto-tokens and initial coin offerings,” in Vanderbilt University Department of Economics Working Papers 17-00008.

- Conte de Leon, D., Stalick, A. Q., Jillepalli, A. A., Haney, M. A., & Sheldon, F. T. (2017). Blockchain: properties and misconceptions. *Asia Pacific Journal of Innovation and Entrepreneurship*, 11(3), 286-300.
- Dai, H., Young, H. P., Durant, T. J. S., Gong, G., Kang, M., Krumholz, H. M., et al. (2018). TrialChain: a blockchain-based platform to validate data integrity in large, biomedical research studies. *Comput. Res. Repository*. arxiv: 1807.03662.
- Dell'Erba, M. (2018). Demystifying Technology. Do Smart Contracts Require a New Legal Framework? Regulatory Fragmentation, Self-Regulation, Public Regulation. Philadelphia, PA: University of Pennsylvania Journal of Law & Public Affairs.
- Deshpande, A., Stewart, K., Lepetit, L., and Gunashekar, S. (2017). Distributed Ledger Technologies/Blockchain: Challenges, Opportunities and the Prospects for Standards. Technical report, The British Standards Institution (BSI).
- DeVries, P. D. (2016). An analysis of cryptocurrency, Bitcoin, and the future, *International Journal of Business Management and Commerce*, 1(2), 1-9
- Dierksmeier, C., & Seele, P. (2016). Cryptocurrencies and business ethics. *Journal of Business Ethics*, 152(1), 1-14.
- Donier, J. and Bouchaud, J.-P. (2015). Why do markets crash? bitcoin data offers unprecedented insights. *PLOS ONE*, 10(10):1–11.
- Dos Santos, R. P. (2017). On the Philosophy of Bitcoin/Blockchain Technology: Is it a Chaotic, Complex System? *Metaphilosophy*, 48(5), 620-633.
- Dyhrberg A. Bitcoin, gold and the dollar—A GARCH volatility analysis. *Finance Research Letters*. 16 pp. 85–92 (2016).
- Fang, L., Bouri, E., Gupta, R., & Roubaud, D. (2019). Does global economic uncertainty matter for the volatility and hedging effectiveness of Bitcoin? *International Review of Financial Analysis*, 61, 29-36.

- Fry, J. & Eng-Tuck C. (2016). Negative bubbles and shocks in cryptocurrency markets. *International Review of Financial Analysis*, North-Holland.
- Fry, J., & Cheah, E. T. (2016). Negative bubbles and shocks in cryptocurrency markets. *International Review of Financial Analysis*, 47, 343-352.
- FSB. 2017. *Artificial Intelligence and Machine Learning in Financial Services. Market Developments and Financial Stability Implications*. Basel: FSB, November.
- FSB. 2019. *FinTech and Market Structure in Financial Services: Market Developments and Potential Financial Stability Implications*. Basel: FSB, February.
- Ghimire, Suman, "Analysis of Bitcoin Cryptocurrency and Its Mining Techniques" (2019). UNLV Theses, Dissertations, Professional Papers, and Capstones. 3603.
- Ha, S., & Moon, B. R. (2018). Finding attractive technical patterns in cryptocurrency markets. *Memetic Computing*, 10(3), 301-306.
- Harasim, Janina. 2021. FinTechs, BigTechs and structural changes in capital markets. In *The Digitalization of Financial Markets. The Socioeconomic Impact of Financial Technologies*, 1st ed. Edited by Adam Marszk and Ewa Lechman. London: Routledge, part 2. pp. 81–100.
- Hileman, G. and Rauchs, M. (2017). *Global Cryptocurrency Benchmarking Study*. United Kingdom: University of Cambridge, pp.26–65.
- Hong MY, Yoon JW (2022) The impact of COVID-19 on cryptocurrency markets: A network analysis based on mutual information. *PLoS ONE* 17(2): e0259869.
- Hong, K. (2017). Bitcoin as an alternative investment vehicle. *Information Technology and Management*, 18(4), 265-275
- Hornuf, Lars, Milan Klus, Todor S. Lohwasser, and Armin Schwienbacher. 2021. *How Do Banks Interact with Fintechs? Forms of Alliances and Their*

Impact on Bank Value. CESifo Working Paper No. 7170, Category 14: Economics of Digitalization. Munich: CESifo GmbH.

Ilutinović, M. (2018). Cryptocurrency. *Ekonomika*, 64(1), 105-122.

Indera NI, Yassin I, Zabidi A, Rizman ZI. Non linear autoregressive with exogenous input (narx) bitcoin price prediction model using pso-optimized parameters and moving average technical indicators. *Journal of Fundamental and Applied Sciences*. 2018;9(3S):791–808.

Jang H, Lee J, Ko H, Lee W. Predicting bitcoin prices by using rolling window LSTM model. *Proceedings of KDD Data Science in Fintech Workshop (DSF)*; New York: ACM; 2018. pp. 1–9.

Kajtazi, A., & Moro, A. (2018). The role of Bitcoin in well diversified portfolios: A comparative global study. *SSRN Electronic Journal*.

Kaplanov, N. (2020). Nerdy money: Bitcoin, the private digital currency, and the case against its regulation. *Loyola Consumer Law Review*, 25(1), 111–174.

Kasgar A. K., Agrawal Jitendra, Sahu Santosh, 2012, “New Modified 256-bit MD5 Algorithm with SHA Compression Function”, *IJCA (0975–8887) Volume 42 (12)* , pp47-51.

Katsiampa P., “Volatility estimation for Bitcoin: a comparison of GARCH models,” *Economics Letters*, vol. 158, pp. 3–6, 2017.

Kim, T. (2017). On the transaction cost of Bitcoin. *Finance Research Letters*, 23, 300-305.

Kristoufek, L. Can Google Trends search queries contribute to risk diversification? *Sci. Rep.* 3, 2713 (2013)

Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy*, 41(10), 1027-1038

Kuhn M, Johnson K. *Applied predictive modeling*. New York: Springer-Verlag; 2013.

- Kurihara Y. & Fukushima A. The market efficiency of Bitcoin: a weekly anomaly perspective. *Journal Of Applied Finance And Banking*. 7, 57 (2017).
- Kurihara Y. & Fukushima A. The market efficiency of Bitcoin: a weekly anomaly perspective. *Journal Of Applied Finance And Banking*. 7, 57 (2017).
- Lee, D. K. C., Guo, L., & Wang, Y. (2018). Cryptocurrency: A new investment opportunity? *Journal of Alternative Investments*, 20(3), 16.1
- Liu H., A. Kadir, X. Sun, and Y. Li, "Chaos based adaptive double-image encryption scheme using hash function and S-boxes," *Multimedia Tools and Applications*, vol. 77, no. 1, pp. 1391–1407, 2018.
- Liu, J., Li, W., Karame, G. O., & Asokan, N. (2018). Toward fairness of cryptocurrency payments. *IEEE Security & Privacy*, 16(3), 81-89.
- Luther, W. (2016). Bitcoin and the future of digital payments. *The Independent Review*, 20(3), 397-404.
- Luther, W. J. (2015). Cryptocurrencies, network effects, and switching costs. *Contemporary Economic Policy*, 34(3), 553-571.
- Madey, R. S. (2020). A study of the history of cryptocurrency and associated risks and threats. *Utica College*
- Mnif E., Jarboui A. & Mouakhar K. How the cryptocurrency market has performed during COVID 19? A multifractal analysis. *Finance Research Letters*. 36 pp. 101647 (2020). pmid:32837367
- Morillon, T.G. and Chacon, R.G. (2022), "Dissecting the stock to flow model for Bitcoin", *Studies in Economics and Finance*, Vol. 39 No. 3, pp. 506-523
- Munim, Shakil & Alon (2019) Munim Z, Shakil M, Alon I. Next-day bitcoin price forecast. *Journal of Risk and Financial Management*. 2019;12(2):1–15.
- Nakamoto Bitcoin: A Peer-to-Peer Electronic Cash System (2008)

- Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*. pp. 21260 (2019).
- Osterrieder J., Lorenz J. & Strika M. Bitcoin and cryptocurrencies-not for the faint-hearted. Available At SSRN 2867671. (2016).
- Padilla, Jorge. 2020. BigTech “banks”, financial stability and regulation. *Banquo de España, Financial Stability Review* 38: 11–26.
- Pant et al. (2018) Pant DR, Neupane P, Poudel A, Pokhrel AK, Lama BK. Recurrent neural network based bitcoin price prediction by twitter sentiment analysis. *IEEE 3rd International Conference on Computing, Communication and Security (ICCCS); Kathmandu (Nepal): 2018.*
- Park, S., & Park, H. W. (2019). Diffusion of Cryptocurrencies: Web traffic and social network attributes as indicators of cryptocurrency performance. *Quality & Quantity*
- Pedregosa, F., et al. (2019) Scikit-Learn: Machine Learning in Python. *Journal of machine learning research*, 12, 2825-2830.
- Phaladisailoed & Numnonda (2018) Phaladisailoed T, Numnonda T. Machine learning models comparison for bitcoin price prediction. *10th International Conference on Information Technology and Electrical Engineering (ICITEE); 24–26 July 2018; Indonesia. 2018*
- Pieters, G., & Vivanco, S. (2017). Financial regulations and price inconsistencies across Bitcoin markets. *Information Economics and Policy*, 39, 1-1
- Price Waterhouse Coopers (2016). *Customers in the Spotlight : How FinTech is Reshaping Banking*. P.W.C.
- Schueffel, Patrick. 2016. Taming the beast: A scientific definition of Fintech. *Journal of Innovation Management* 4: 32–54.
- Shi, N. (2016). A new proof-of-work mechanism for bitcoin. *Financial Innovation*, 2(1), 31.

Stallings William, *Cryptography and Network Security: Principles and Practice*, 5th Edition Prentice Hall; 5th edition (2018).

Stulz, René M. 2019. Fintech, bigtech, and the future of banks. *Journal of Applied Corporate Finance* 31: 86–97

Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Communications Surveys & Tutorials*, 18(3), 2084-2123.

Urquhart, A. (2016). The inefficiency of Bitcoin. *Economics Letters*, 148, 80-82.

Warden, S. (2019). Bitcoin. *The Milken Institute Review: A Journal of Economic Policy*, 17(4), 16+

Wheili, C. (2019). *Market Manipulation of Bitcoin: Evidence from Mining the Mt.Gox Transaction Network*. Guangzhou China: Sun Yat-sen University

Xi S. X., W. N. Zhang, Q. L. Zhou, S. XueMing, and B. Li, “High-throughput implementation of SHA512 algorithm based on mimetic computer,” *Computer Engineering and Science*, vol. 40, no. 8, pp. 1344–1350, 2018.

Zavolokina, Liudmila, Mateusz Dolata, and Gerhard Schwabe. (2021) *FinTech—What’s in a name?* Paper presented at Thirty Seventh International Conference on Information Systems, Dublin, Ireland, December 11–14.