



ΙΟΝΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

**ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΣΧΟΛΗ ΕΠΙΣΤΗΜΗΣ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ**

ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΑ ΚΑΙ ΜΗΧΑΝΙΚΗ ΜΑΘΗΣΗ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Γεώργιος Τσουρέκας (Π2015045)

Επιβλέπον : Έξαρχος Θέμης

Κέρκυρα, Ιανουάριος 2022

Copyrights

Περίληψη

Τα τελευταία χρόνια γίνεται ολοένα και πιο έντονη η εμφάνιση των κρυπτονομισμάτων, αυτή τη στιγμή υπάρχουν σε κυκλοφορία περισσότερα από 19000 κρυπτονομίσματα και δεκάδες πλατφόρμες blockchain, τα οποία αποτελούν αντικείμενο συζήτησης αλλά και πηγή εσόδων για πολλούς ανθρώπους. Μία πλατφόρμα blockchain, όπως το Ethereum, είναι η τεχνολογία πάνω στην οποία χτίζονται κάθε ένα από τα κρυπτονομίσματα. Την ανάγκη αυτή για αγοροπωλησίες κρυπτονομισμάτων, εκμεταλλεύτηκαν τα ηλεκτρονικά ανταλλακτήρια, τα οποία έδωσαν τη δυνατότητα στον κόσμο να επενδύει σε κρυπτονομίσματα αγοράζοντας και πουλώντας ποσότητες αυτών. Με τις διακυμάνσεις των τιμών των κρυπτονομισμάτων καθορίζονται και τα κέρδη ή η ζημία των επενδυτών, όπως γίνεται και με το χρηματιστήριο.

Το γεγονός ότι οι διακυμάνσεις στα ποσοστά ανόδου και πτώσης της τιμής στα κρυπτονομίσματα είναι μεγάλες, προσέλκυσε πολλούς επενδυτές οι οποίοι αναζητούν κερδοφόρες στρατηγικές που θα βοηθήσουν στις αγοροπωλησίες τους. Υπάρχουν πολλοί δείκτες οι οποίοι παρέχουν πληροφορίες για την κίνηση της τιμής ενός κρυπτονομίσματος και έτσι στοιχειοθετείται η τεχνική ανάλυση, σύμφωνα με την οποία κάθε επενδυτής προσπαθεί να «προβλέψει» μία ενδεχόμενη άνοδο ή πτώση της τιμής.

Στη συγκεκριμένη εργασία, έγινε η μελέτη για τα κρυπτονομίσματα και για το πως θα μπορούσε να γίνει χρήση της μηχανική μάθησης στην κατασκευή ενός μοντέλου πρόβλεψης της συμπεριφοράς της τιμής ενός κρυπτονομίσματος βασισμένο στα ιστορικά δεδομένα που του δόθηκαν.

Λέξεις Κλειδιά

Κρυπτονομίσματα, ανταλλακτήριο, τεχνική ανάλυση, δείκτης, μηχανική μάθηση

Abstract

In recent years, the appearance of cryptocurrencies has become more and more intense, currently there are more than 19000 cryptocurrencies and dozens of blockchain platforms in circulation, which are a topic of discussion and a source of income for many people. A blockchain platform, such as Ethereum, is the technology upon which each of the cryptocurrencies are built. This need to buy and sell cryptocurrencies, was exploited by electronic exchanges, which enabled people to invest in cryptocurrencies by buying and selling quantities of them. With the fluctuations in the prices of cryptocurrencies, the profit or loss of the investors is determined, as is done with the stock market.

The fact that the fluctuations in the rate of rise and fall in the price of cryptocurrencies are large has attracted many investors who are looking for profitable strategies that will help in their buying and selling. There are many indicators that provide information on the movement of the price of a cryptocurrency, and this is how technical analysis is defined, according to which every investor tries to "predict" a possible rise or fall in price.

In this particular work, the study was done on cryptocurrencies and how machine learning could be used in making a model for predicting the behavior of the price of a cryptocurrency based on the historical data given to it.

Key Words

Cryptocurrency, exchange, technical analysis, indicator, machine learning

Ευχαριστίες

Περιεχόμενα

1	Εισαγωγή	8
1.1	Αντικείμενο της Διπλωματικής.....	9
1.2	Οργάνωση κειμένου.....	9
2	Κρυπτονομίσματα.....	10
2.1.1	Bitcoin [7], [8], [9], [10].....	12
2.1.2	Ιστορικό και εξέλιξη	13
2.1.3	Blockchain και έξυπνα συμβόλαια (Smart contracts).....	17
2.1.4	Τεχνολογία Blockchain	20
2.1.5	Εξόρυξη των Bitcoins (Bitcoin Mining)	23
2.1.6	Πλεονεκτήματα	25
2.1.7	Μειονεκτήματα, ρίσκα και κίνδυνοι.....	31
3	Χρονοσειρές και Πρόβλεψη	35
3.1	Χρονοσειρές [19]	35
3.2	Πρόβλεψη (Forecasting).....	37
3.3	Μηχανική Μάθηση.....	37
3.4	Μέθοδοι μηχανικής μάθησης [20].....	37
3.4.1	Εποπτευόμενη μηχανική εκμάθηση.....	37
3.4.2	Μη εποπτευόμενη μηχανική εκμάθηση	38
3.4.3	Ημι-εποπτευόμενη μάθηση	38
3.5	Το SMOreg (μοντέλο SVM) για παλινδρόμηση.....	39
3.6	Η γραμμική παλινδρόμηση – Linear Regression.	39
3.7	MultilayerPerceptron	40
3.8	Bagging.....	41
3.9	Δέντρα απόφασης.....	41
3.10	Μηχανική Μάθηση - RL	42
3.11	Μηχανική Μάθηση – WEKA [31]	45
3.12	Πρόβλεψη Χρονοσειρών μέσω Weka.....	46
3.13	Ο σχεδιασμός των πειραμάτων.....	46
3.14	Τα δεδομένα των πειραμάτων	47
3.15	Τα πειράματα	51
4	Σύνοψη και συμπεράσματα.....	62
	ΒΙΒΛΙΟΓΡΑΦΙΑ.....	63

Κατάλογος Σχημάτων

Εικόνα 1 Σχηματισμός μπλοκ σε κρυπτογραφική και χρονολογική σειρά αλυσίδας. [12]....	18
Εικόνα 2 Πως λειτουργεί ένα blockchain. [13]	22
Εικόνα 3 Χαρακτηριστικά χρονοσειρών. [19]	36
Εικόνα 4 Οι αγοραπωλησίες του RL αλγορίθμου.....	45
Εικόνα 5 Πληροφορίες για το Bitcoin από το yahoo, στις 26 Ιουλίου 2022	47
Εικόνα 6 Δεδομένα για το Bitcoin του csv αρχείου που χρησιμοποιήθηκαν στα πειράματα. 48	
Εικόνα 7 Γράφημα που δείχνει την ετήσια πορεία του Bitcoin, στις 26 Ιουλίου 2022	49
Εικόνα 8 Ιστορικά δεδομένα του Bitcoin μέσα από τη σελίδα coinmarketcap.com.....	50

1 Εισαγωγή

Από την αρχή του παραστατικού χρήματος, στο οποίο βασίζονται σχεδόν όλα τα σύγχρονα χρηματικά συστήματα, οι άνθρωποι το χρησιμοποιούν για τις καθημερινές τους συναλλαγές. Μετά την παγκόσμια οικονομική κρίση του 2008, έκανε την εμφάνιση του το πρώτο κρυπτονόμισμα, ονομαζόμενο ως Bitcoin. Εν συνεχεία, αναπτύχθηκαν και κυκλοφόρησαν πολλά ακόμα κρυπτονομίσματα βασισμένα στο Bitcoin. Οι ραγδαίοι ρυθμοί εξέλιξης και εμφάνισης των κρυπτονομισμάτων, αποτέλεσαν κίνητρο για πολλούς ανθρώπους να μάθουν περισσότερα γι' αυτά. Περίπου 5 χρόνια αργότερα, ηλεκτρονικές πλατφόρμες εκμεταλλεύτηκαν την ανάγκη των ανθρώπων να αποκτήσουν κρυπτονομίσματα, και δημιουργήθηκαν αποκλειστικά για αγοροπωλησίες και ανταλλαγές κρυπτονομισμάτων με άλλα συναλλάγματα όπως το ευρώ ή το δολάριο.

Αυτή τη στιγμή υπάρχουν σε κυκλοφορία περισσότερα από 19000 κρυπτονομίσματα και δεκάδες πλατφόρμες blockchain, τα οποία αποτελούν αντικείμενο συζήτησης αλλά και πηγή εσόδων για πολλούς ανθρώπους. Με τις διακυμάνσεις των τιμών των κρυπτονομισμάτων καθορίζονται και τα κέρδη ή η ζημία των επενδυτών, όπως γίνεται και με το χρηματιστήριο. Μία πλατφόρμα blockchain, όπως το Ethereum, είναι η τεχνολογία πάνω στην οποία χτίζονται κάθε ένα από τα κρυπτονομίσματα. Η δυνατότητα που έδωσαν στον κόσμο τα ανταλλακτήρια για αγοροπωλησίες και επενδύσεις γύρω από τα κρυπτονομίσματα, ήταν το ξεκίνημα για την εύρεση κερδοφόρων στρατηγικών με τη βοήθεια ήδη υπάρχοντων εργαλείων που χρησιμοποιούνταν για συναλλαγές μετοχών στο χρηματιστήριο.

Το γεγονός ότι οι διακυμάνσεις στα ποσοστά ανόδου και πτώσης της τιμής στα κρυπτονομίσματα είναι μεγάλες, προσέλκυσε πολλούς επενδυτές οι οποίοι αναζητούν κερδοφόρες στρατηγικές που θα βοηθήσουν στις αγοροπωλησίες τους. Υπάρχουν πολλοί δείκτες οι οποίοι παρέχουν πληροφορίες για την κίνηση της τιμής ενός κρυπτονομίσματος και έτσι στοιχειοθετείτε η τεχνική ανάλυση, σύμφωνα με την οποία κάθε επενδυτής προσπαθεί να «προβλέψει» μία ενδεχόμενη άνοδο ή πτώση της τιμής. Στη συγκεκριμένη εργασία, έγινε η μελέτη για τα κρυπτονομίσματα και για το πως θα μπορούσε να γίνει χρήση της μηχανική μάθησης στην κατασκευή ενός μοντέλου πρόβλεψης της συμπεριφοράς της τιμής ενός κρυπτονομίσματος βασισμένο στα ιστορικά δεδομένα που του δόθηκαν.

1.1 Αντικείμενο της Διπλωματικής

Η μεγάλη μεταβλητότητα στις τιμές των κρυπτονομισμάτων και ο χρόνος που απαιτούνταν να αφιερώσει κάποιος για να εκτελέσει αγοροπωλησίες καθημερινά, έστρεψε τους επενδυτές στο Algorithmic trading, μία μέθοδο εκτέλεσης εντολών αγοράς και πώλησης με τη χρήση αυτοματοποιημένων προ-προγραμματισμένων οδηγιών σύμφωνα με ορισμένες μεταβλητές. Με αυτό τον τρόπο η προσπάθεια έχει στραφεί στην εύρεση βελτιστοποιημένων στρατηγικών στις οποίες θα βασιζόταν ο αλγόριθμός αγοροπωλησιών. Στα πλαίσια της εργασίας θα πειραματιστούμε με την βιβλιοθήκη AI Gym Anytrading και μέσω της Ενισχυτικής Μάθησης θα δοκιμαστεί σε αυτοματοποιημένες αγοροπωλησίες bitcoin με στόχο το κέρδος και στη συνέχεια θα επιχειρηθεί η πρόβλεψη της τιμής του bitcoin με διάφορα μοντέλα μηχανικής μάθησης κάτω από διαφορετικές συνθήκες στην αγορά των κρυπτονομισμάτων.

1.2 Οργάνωση κειμένου

Η εργασία ξεκινά με τα κρυπτονομίσματα, την τεχνολογία των Blockchain και τα έξυπνα συμβόλαια. Η εξόρυξη των bitcoins περιγράφεται στη συνέχεια και έπειτα γίνεται αναφορά στα πλεονεκτήματα των κρυπτονομισμάτων, στα μειονεκτήματα, τα ρίσκα και τους κινδύνους που εγκυμονούν.

Στα μοντέλα μηχανική μάθησης που χρησιμοποιήθηκαν γίνεται στη συνέχεια αναφορά, για το SMOReg που είναι μοντέλο SVM για παλινδρόμηση, για τη γραμμική παλινδρόμηση, για το Multilayer Perceptron, για το Bagging και για τα Δέντρα απόφασης. Ακολουθεί αναφορά στην ενισχυτική μάθηση και έπειτα στο WEKA. Το τελευταίο πριν τα πειράματα κείμενο αναφέρεται στις χρονοσειρές και στην πρόβλεψη χρονοσειρών μέσω Weka.

Τα πειράματα και τα συμπεράσματα από την εκτέλεση τους είναι το τελευταίο κομμάτι της εργασίας.

2 Κρυπτονομίσματα

Η αξία των κρυπτονομισμάτων έχει αναπτυχθεί εκθετικά την τελευταία δεκαετία, με τις πιο γρήγορες εξελίξεις που παρατηρούνται τα τελευταία χρόνια, καθώς όλο και περισσότερα μέρη σε όλο τον κόσμο αναγνωρίζουν την αξία της διατήρησης ψηφιακών περιουσιακών στοιχείων στο διαδίκτυο. Τα στατιστικά στοιχεία από το Twitter υποστηρίζουν αυτή τη δήλωση όπου καταγράφονται περίπου 1.500 Tweets μόνο για το Bitcoin ανά ώρα. Κατά συνέπεια, πολλοί άνθρωποι αρχίζουν να συνειδητοποιούν περισσότερο και να αποδέχονται τη φύση των ψηφιακών νομισμάτων, και ειδικότερα οι έμποροι αναζητούν να μάθουν πώς μπορούν να κάνουν επικερδείς συναλλαγές και επενδύσεις κρυπτονομισμάτων. [1]

Για το λόγο αυτό, στις μέρες μας τα κρυπτονομίσματα βρίσκονται στο επίκεντρο του ενδιαφέροντος επενδυτικά, τεχνολογικά, και ακαδημαϊκά. Τα κρυπτονομίσματα αποτελούν ένα είδος ψηφιακού χρήματος που βασίζεται στις αρχές της κρυπτογραφίας, που εγγυάται την ασφάλεια και την ανωνυμία των συναλλαγών. Διαφέρουν από τα συνηθισμένα νομίσματα όπως το ευρώ και το δολάριο καθώς δεν έχουν φυσική υπόσταση. Χρησιμοποιούνται για peer-to-peer συναλλαγές, μεταφορές χρημάτων σε τρίτους αλλά και αποταμιεύσεις/επενδύσεις, ως περιουσιακό στοιχείο. Η βασική τεχνολογία για την κατασκευή του Bitcoin είναι το blockchain, το οποίο προτάθηκε για πρώτη φορά από τον Satoshi Nakamoto το 2008 και εφαρμόστηκε το 2009. Το πρώτο κρυπτόνμισμα που κυκλοφόρησε με επιτυχία είναι το Bitcoin, το 2009.

Το Blockchain θα μπορούσε να θεωρηθεί ως ένα καθολικό που είναι δημόσιο και κάθε συναλλαγή αποθηκεύεται σε μπλοκ. Αυτή η λίστα από μπλοκ, μοιάζει με αλυσίδα και μεγαλώνει καθώς προστίθενται συνεχώς νέα μπλοκ σε αυτήν. Ασύμμετρη κρυπτογραφία και κατανεμημένοι αλγόριθμοι συναίνεσης έχουν εφαρμοστεί για την ασφάλεια των χρηστών και τη συνοχή του καθολικού. Μέχρι το 2011, αυτή η ιδέα σχημάτισε μια αγορά αξίας άνω των 54 εκατομμυρίων. Ως ένα από τα πιο επιτυχημένα κρυπτονομίσματα, το Bitcoin γνώρισε τεράστια επιτυχία με την κεφαλαιαγορά του να φτάνει τα 10 δισεκατομμύρια δολάρια το 2016. Με μια ειδικά σχεδιασμένη δομή αποθήκευσης δεδομένων, οι συναλλαγές στο δίκτυο Bitcoin μπορούν να πραγματοποιηθούν χωρίς τρίτο μέρος (μεσάζοντα). Η μεγάλη απήχηση και το παγκόσμιο ενδιαφέρον για τα κρυπτονομίσματα αποτυπώνεται από την συνολική κεφαλαιοποίηση αγοράς τους, η οποία έχει φτάσει το πρωτοφανές μέγιστο των 2,6 τρις

δολάρια. Με το bitcoin να απογειώνεται, εκατοντάδες εναλλακτικά κρυπτονομίσματα, βασισμένα στον ανοιχτό κώδικα του πρωτοπόρου Bitcoin, σχημάτισαν ένα ξεχωριστό σύστημα αγοράς. Συγχρόνως, πιο προηγμένες, εναλλακτικές μορφές blockchains ξεπηδούν ως αυτόνομες εταιρείες. [2], [3], [4]

Τα κύρια χαρακτηριστικά της αρχιτεκτονικής blockchain που γίνεται όλο και πιο δημοφιλής, είναι η ακεραιότητα των δεδομένων, η αποκέντρωση και η ενισχυμένη ασφάλεια. Τα κρυπτονομίσματα δεν ελέγχονται από καμία κεντρική δημόσια αρχή, από τράπεζες ή κυβερνήσεις και χρησιμοποιούν μία κατανεμημένη βάση δεδομένων, το επονομαζόμενο Blockchain, το οποίο μπορεί να χαρακτηριστεί ως ένα ψηφιακό λογιστικό βιβλίο που καταγράφει συναλλαγές σε συνάρτηση με το χρόνο, χωρίς ποτέ να αλλοιώνει ή καταστρέφει το ιστορικό των παλαιών συναλλαγών. Τα έξυπνα συμβόλαια blockchain έχουν την ικανότητα να διαταράσσουν την αγορά δεδομένων και να κάνουν τις συναλλαγές πιο δημοκρατικές, ασφαλείς, αυτόνομες, διαφανείς και αποτελεσματικές. [5]

Τα κορυφαία 5 κρυπτονομίσματα με βάση την κεφαλαιοποίηση, σύμφωνα με το στο CoinMarketCap, το οποίο είναι ένας από τους πιο δημοφιλείς ιστότοπους για την παρακολούθηση κρυπτονομισμάτων [6]

Στις 5/7/2022 οι τιμές των κρυπτονομισμάτων ήταν [6]:

# ▲	Όνομα	Τιμή	24h %	7d %	Κεφαλαιοποίηση Αγοράς ⓘ	Volume(24h) ⓘ
1	 Bitcoin BTC Αγορά	€19,129.04	▼ 1.26%	▼ 6.91%	€365,605,880,081	€22,793,644,048 1,189,904 BTC
2	 Ethereum ETH Αγορά	€1,072.30	▼ 1.37%	▼ 9.19%	€130,275,791,736	€14,728,085,437 13,727,290 ETH
3	 Tether USDT	€0.9753	▼ 0.71%	▼ 1.56%	€64,413,878,428	€41,235,030,568 42,278,270,735 USDT
4	 USD Coin USDC Αγορά	€0.9761	▼ 0.73%	▼ 1.59%	€54,484,213,437	€4,831,873,690 4,948,793,834 USDC
5	 BNB BNB Αγορά	€220.00	▼ 0.76%	▼ 6.02%	€35,977,751,828	€1,201,220,775 5,451,472 BNB

Στις 8/6/2022 υπήρχαν [6]:

- Κρυπτονομίσματα: 19785
- Ανταλλακτήρια: 527
- Κεφαλαιοποίηση Αγοράς: €1.151.820.652.318
- 24ωρος Όγκος: €81.690.363.906
- Κυρίαρχα κρυπτονομίσματα στις συναλλαγές: BTC: 46.5% ETH: 17.5%

Τα 5 μεγαλύτερα σε κεφαλαιοποίηση κρυπτονομίσματα [6]:

#	Όνομα	Κεφαλαιοποίηση Αγοράς
1	 Bitcoin - BTC	€534,001,362,771
2	 Ethereum - ETH	€201,070,966,240
3	 Tether - USDT	€67,539,702,943
4	 USD Coin USDC	€50,200,362,912
5	 BNB - BNB	€43,660,002,865

Μέσα σε ένα μήνα υπήρξε πτώση της αξίας σημαντική κι αυτό γιατί τα κρυπτονομίσματα ακόμα και τα κορυφαία είναι αναδυόμενα, καινούργια περιουσιακά στοιχεία διαφύλαξης αξίας, αλλά δεν είναι ώριμα. Και αυτό οδηγεί στη μεγάλη μεταβλητότητα σε σχέση με τον χρυσό, που προστατεύεται από την αίγλη των χιλιάδων χρόνων ιστορίας.

2.1.1 Bitcoin [7], [8], [9], [10]

Το Bitcoin είναι το πρώτο αποκεντρωμένο ψηφιακό νόμισμα ανοιχτού κώδικα. Είναι ένα άυλο ψηφιακό νόμισμα το οποίο δεν απαιτεί μία κεντρική τράπεζα για την έκδοση του. Οι συναλλαγές Bitcoin έχουν την μορφή ψηφιακών μεταφορών ανάμεσα στους χρήστες του δικτύου Bitcoin, χωρίς την ύπαρξη μεσάζοντα. Βασίζεται στις αρχές της κρυπτογραφίας με σκοπό να εγγυάται την φερεγγυότητα των συναλλαγών, οι οποίες καταχωρούνται και αποθηκεύονται σε ένα δημόσια καταναμεμημένο αρχείο, το ονομαζόμενο Blockchain. Το Bitcoin εφευρέθηκε το 2008, από ένα άτομο ή μία ομάδα ατόμων με το ψευδώνυμο Satoshi Nakamoto. Η ταυτότητα τους μέχρι και σήμερα είναι άγνωστη αποτελώντας ένα μυστήριο. Η ιδέα δημοσιεύτηκε για πρώτη φορά στον κόσμο στις 31/10/2008 μέσω ενός PDF αρχείου με όνομα «Bitcoin: A peer-to-peer electronic cash system». Το bitcoin έχει κατακριθεί για την χρήση του σε παράνομες

συναλλαγές, την μεγάλη κατανάλωση ηλεκτρικής ενέργειας που απαιτείται για την εξόρυξή τους, τη μεταβλητότητα της τιμής του και για τις υψηλές χρεώσεις για την μετατροπή από και προς άλλα νομίσματα. Μερικοί οικονομολόγοι, συμπεριλαμβανομένων και επιφανών κατόχων του Νόμπελ Οικονομίας, το έχουν χαρακτηρίσει ως χρηματοπιστωτική φούσκα. Το bitcoin έχει χρησιμοποιηθεί και σαν επένδυση, μολονότι διάφοροι επενδυτικοί οίκοι, οίκοι αξιολόγησης και ελεγκτικές αρχές έχουν εκδώσει προειδοποιήσεις προς τους επενδυτές για το bitcoin.

Στις 7 Σεπτεμβρίου 2021 το Ελ Σαλβαδόρ έγινε η πρώτη χώρα στον κόσμο που υιοθέτησε επίσημα για νόμιμες συναλλαγές το Bitcoin.

2.1.2 Ιστορικό και εξέλιξη

2.1.2.1 Ιστορικό

Πριν από την δημοσίευση του Bitcoin, υπήρχαν πολλές τεχνολογίες ψηφιακού χρήματος. Η πρώτη ήταν τα ecash πρωτόκολλα του εκδότη David Chaum και Stefan Brands. Οι κρυπτογράφοι Cynthia Dwork και Moni Naor το 1992, πρότειναν για πρώτη φορά την ιδέα ότι οι λύσεις σε υπολογιστικές εξισώσεις θα μπορούσαν να έχουν μία αξία. Την ιδέα αυτή βρήκε χρήσιμη ο Adam Back, ο οποίος δημιούργησε το hashcash το 1997. Η πρώτες προτάσεις για καταναμεμημένα ψηφιακά νομίσματα που βασίζονται στην σπανιότητα ήταν το b-money του Wei Dai και το bit gold του Nick Szabo.

2.1.2.2 Δημιουργία

Στις 18 Αυγούστου, καταχωρήθηκε το domain name bitcoin.org. Αργότερα, στις 31 Οκτωβρίου, δημοσιεύτηκε ένα άρθρο από κάποιον ή κάποιους με το ψευδώνυμο Satoshi Nakamoto. Το όνομα του άρθρου ήταν “Bitcoin : A Peer-to-Peer Electronic Cash System” και περιείχε μεθόδους χρήσης ενός δικτύου peer-to-peer για τη δημιουργία αυτού που περιγραφικά ως “a system for electronic transactions without relying on trust”. Στις 3 Ιανουαρίου 2009, το δίκτυο Bitcoin εμφανίστηκε με τον Satoshi Nakamoto να παράγει το πρώτο Block γνωστό ως genesis block of bitcoin (block number 0), το οποίο είχε ως ανταμοιβή 50 Bitcoins. Κάποιοι από τους πρώτους υποστηρικτές και συμμετέχοντες στις πρώτες συναλλαγές του δικτύου Bitcoin, ήταν ο προγραμματιστής Hal Finney, ο Wei Dai (δημιουργός του b-money) και ο Nick Szabo (δημιουργός του bit gold). Ο Satoshi Nakamoto, ήταν υπεύθυνος για την δημιουργία του μεγαλύτερου μέρους του λογισμικού Bitcoin και ήταν ενεργός στην

πραγματοποίηση τροποποιήσεων και στη δημοσίευση τεχνικών πληροφοριών στο forum του Bitcoin. Μέχρι να εξαφανιστεί, εκτιμάται ότι είχε παράξει 1 εκατομμύριο Bitcoins.

2.1.2.3 Εξέλιξη

Ακολουθεί πίνακας με την εξέλιξη που σημείωσε το Bitcoin.

Ημερομηνία	Αναλογία δολαρίου / Bitcoin	Στοιχεία
Ιανουάριος 2009 – Μάρτιος 2010	-	Δεν υπήρχαν ανταλλακτήρια και ο κόσμος έστελνε Bitcoins δοκιμαστικά, τα οποία δεν είχαν αξία τότε.
Μάιος 2010	Λιγότερο από \$0.01	Στις 22 Μαΐου 2010, ο Laszlo Hanyecz πραγματοποίησε την πρώτη συναλλαγή, αγοράζοντας δύο πίτσες έναντι 10,000 Bitcoins.
Φεβρουάριος 2011 – Απρίλιος 2011	\$1.00	Το Bitcoin ισοδυναμεί με ένα δολάριο
Νοέμβριος 2013	\$350-\$1,242	Η τιμή αυξάνεται από \$150 τον Οκτώβριο στα \$200 τον Νοέμβριο, φτάνοντας \$1,242 στις 29 Νοεμβρίου 2013
Απρίλιος 2014	\$340-\$530	Η χαμηλότερη τιμή από την Κυπριακή οικονομική κρίση 2012-2013
2-3 Μαρτίου 2017	\$1,290+	Η τιμή ξεπέρασε το προηγούμενο μέγιστο \$1,242 του Νοεμβρίου 2013
20 Μαΐου 2017	\$2,000	Στις 20 Μαΐου η τιμή ξεπερνάει τα \$2,000 για πρώτη φορά
1 Σεπτεμβρίου 2017	\$5,013.91	Η τιμή ξεπερνάει τα \$5,000 για πρώτη φορά
17-20 Νοεμβρίου 2017	\$7,600-\$8,100	Η αύξηση στα \$8,004.59 πιθανόν να συνδέεται με

		το πραξικόπημα της Ζιμπάμπουε 2017
15 Δεκεμβρίου 2017	\$17,900	Η τιμή φτάνει τα \$17,900
17 Δεκεμβρίου 2017	\$19,783.06	Η τιμή αυξάνεται κατά 5% σε 24 ώρες για να φτάσει το νέο πρωτοφανές μέγιστο των \$19,783.06
22 Δεκεμβρίου 2017	\$13,800	Το Bitcoin χάνει το 1/3 της αξίας του σε 24 ώρες
5 Φεβρουαρίου 2018	\$6.200	Η τιμή μειώνεται κατά 50% σε 16 μέρες, κάτω από \$7,000
31 Οκτωβρίου 2018	\$6,300	Στη 10 ^η επέτειο του Bitcoin, η τιμή παραμένει πάνω από τα \$6,000
7 Δεκεμβρίου 2018	\$3,300	Η τιμή του Bitcoin, μειώνεται στα \$3,300, μία πτώση 76% σε σχέση με την προηγούμενη χρονιά
16 Μαρτίου 2020	\$5,000	Η τιμή μειώνεται κατά 50% στις αρχές του 2020 εξαιτίας της πανδημίας COVID-19
27 Ιουλίου 2020	\$10,944	Επανάκτηση της αξίας που έχασε εξαιτίας της πανδημίας
30 Νοεμβρίου 2020	\$19,850.11	Καινούργιο πρωτοφανές μέγιστο στα \$19,850.11
8 Ιανουαρίου 2021	\$41,973	Η τιμή του Bitcoin διαπραγματεύεται σε ψηλά επίπεδα
11 Ιανουαρίου 2021	\$33,400	Η τιμή μειώνεται κατά 26%
8 Φεβρουαρίου 2021	\$44,200	Ο Elon Musk και η Tesla ανακοινώνει ότι επένδυσε στο Bitcoin και το δέχεται ως μέθοδο πληρωμής
16 Φεβρουαρίου 2021	\$50,000	Καινούργιο πρωτοφανές μέγιστο στα \$50,000
10 Απριλίου 2021	\$60,000	Η Coinbase ανακοινώνει ότι εισέρχεται στο stock

		market, η τιμή του Bitcoin αυξάνεται στα \$60,000
14 Απρίλιου 2021	\$64,800	Καινούργιο all-time-high
19 Μαΐου 2021	\$30,000	Καινούργιες αποφάσεις της Κινεζικής κυβέρνησης για τα κρυπτονομίσματα
2 Σεπτεμβρίου 2021	\$50,128	Η τιμή επανέρχεται στα \$50,000 μετά την μεγάλη πτώση
17 Οκτωβρίου 2021	\$62,600	Το Bitcoin διαπραγματεύεται κοντά στο προηγούμενο μέγιστο
20 Οκτωβρίου 2021	\$66,974.77	Η τιμή του Bitcoin φτάνει τα 66,974.77 με καινούργιο πρωτοφανές μέγιστο
22 Ιανουαρίου 2022	\$35,000	Η τιμή του Bitcoin μειώνεται σχεδόν 50% από το προηγούμενο μέγιστο
5 Ιουλίου 2022	\$19,645	Συνέχεια στις πιέσεις που δέχεται το bitcoin και συνολικά η αγορά των κρυπτονομισμάτων τις τελευταίες εβδομάδες. Το δημοφιλέστερο crypto του κόσμου βρίσκεται, προς ώρα, μακριά από τη «βουτιά» στα μέσα Ιουνίου, που έφτασε την τιμή του στα 18.000 δολάρια, αλλά και ακόμα μακρύτερα από το ιστορικό υψηλό του Νοεμβρίου του 2021, όταν είχε φτάσει στην «πόρτα» των 69.000 δολαρίων. Από τότε μέχρι σήμερα, το bitcoin έχει απωλέσει το 1/3 της αξίας του.

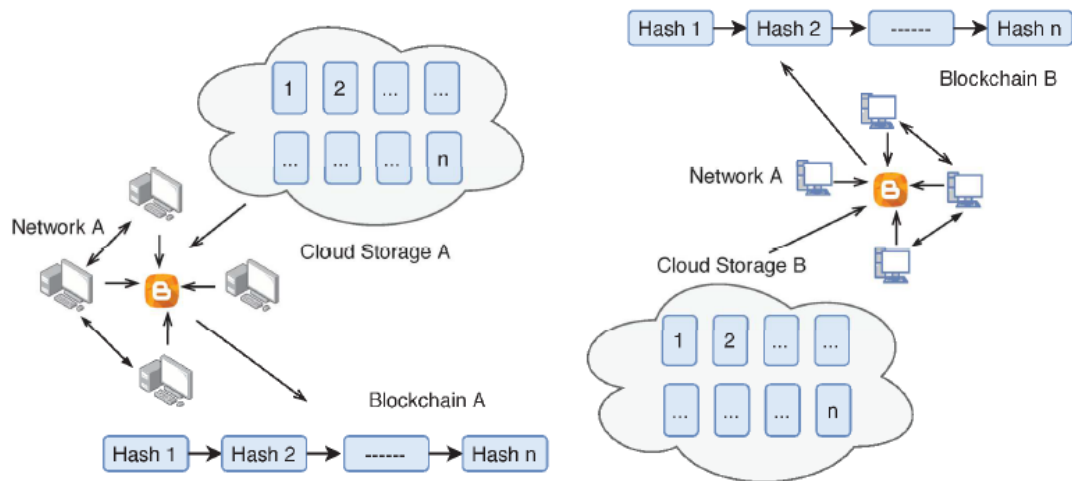
2.1.3 Blockchain και έξυπνα συμβόλαια (Smart contracts)

Το blockchain (αλυσίδα συστοιχιών) είναι μια εφαρμογή της τεχνολογίας κατανεμημένων (καθολικών) μητρώων (Distributed Ledger Technology – DLT), και αναφέρεται στην τεχνολογική υποδομή και πρωτόκολλα που επιτρέπουν την ταυτόχρονη πρόσβαση, επικύρωση και ενημέρωση εγγραφών με αμετάβλητο τρόπο σε ένα δίκτυο που είναι κατανεμημένο σε πολλές οντότητες ή τοποθεσίες.

Το blockchain είναι ένα μητρώο στο οποίο αποθηκεύονται κι επαληθεύονται πληροφορίες και δεδομένα, με τη χρήση κρυπτογραφικών μεθόδων, τα οποία συνήθως ομαδοποιούνται προκειμένου να σχηματίσουν συστοιχίες (blocks) και με τέτοιο τρόπο ώστε να δημιουργείται μία συνεχής αλυσίδα δεδομένων (chain), με χρονολογική σειρά, ενώ κάθε τροποποίηση μίας πληροφορίας που έχει καταγραφεί στο μητρώο να επηρεάζει αναγκαστικά όλες τις μεταγενέστερες καταχωρήσεις. Η αλυσίδα προστατεύεται στο σύνολό της από σύνθετους μαθηματικούς αλγορίθμους με σκοπό να διασφαλίζεται η ακεραιότητα και η ασφάλεια των δεδομένων. Τα μπλοκ συνδέονται με τη συμπερίληψη της κρυπτογραφικής τιμής κατακερματισμού του προηγούμενου μπλοκ στο νεοδημιουργημένο για επόμενο μπλοκ. Αυτή η τεχνική αλυσίδας με συνδεδεμένες τιμές κατακερματισμού αποτρέπει την παραποίηση συναλλαγών χωρίς να εντοπιστεί.

Αποτελεί ουσιαστικά μια βάση δεδομένων για συναλλαγές που, αντί να αποθηκεύεται σε μια κεντρική τοποθεσία, κατανέμεται σε ένα δίκτυο πολλών υπολογιστών. Συνήθως, όλα τα μέλη του δικτύου μπορούν να διαβάσουν τις πληροφορίες και, ανάλογα με τις άδειες που τους έχουν δοθεί, να προσθέτουν στοιχεία.

Μία πλατφόρμα blockchain μπορεί να είναι δημόσια (ανοιχτή) ή ιδιωτική (κλειστή), κατ' αντιστοιχία με τα δημόσια δίκτυα (όπως το διαδίκτυο - internet) και τα εσωτερικά δίκτυα (intranets).



Εικόνα 1 Σχηματισμός μπλοκ σε κρυπτογραφική και χρονολογική σειρά αλυσίδας. [12]

Τα έξυπνα συμβόλαια (Smart Contracts) είναι προγράμματα ηλεκτρονικών υπολογιστών (κώδικας) που χειρίζονται την επιχειρησιακή λογική που είχε προσυμφωνηθεί από τα μέλη του δικτύου. Εκτελούνται στο blockchain και παρέχουν μια διεπαφή για αλληλεπίδραση με τα δεδομένα. Αυτός ο κωδικός είναι διαθέσιμος σε όλα τα μέλη που είναι παρόντα στο δίκτυο (π.χ. παραγγελιοδότες, ομότιμα μέλη). Τα μέλη του blockchain προσθέτουν έξυπνα συμβόλαια στο blockchain με παρόμοιο τρόπο προσθήκης συναλλαγών, επομένως αυτά τα έξυπνα συμβόλαια περιλαμβάνονται σε μπλοκ. Οι συναλλαγές που ενημερώνουν τις καταστάσεις έξυπνων συμβολαίων καταγράφονται επίσης στο επόμενο μπλοκ που δημιουργείται μετά την πραγματοποίηση της αλλαγής. Αυτός ο μηχανισμός καθιστά τα έξυπνα συμβόλαια αμετάβλητα με τον ίδιο τρόπο για τις συναλλαγές. [11], [12]

Το Blockchain έχει σχεδιαστεί ως βάση για εφαρμογές που περιλαμβάνουν συναλλαγές και αλληλεπιδράσεις. Αυτά μπορεί να περιλαμβάνουν έξυπνα συμβόλαια (τα έξυπνα συμβόλαια εκτελούνται αυτόματα όταν πληρούνται μια συγκεκριμένη προϋπόθεση, για παράδειγμα σχετικά με τις συνθήκες των αγαθών ή τις περιβαλλοντικές συνθήκες) ή άλλες έξυπνες εφαρμογές που υποστηρίζουν συγκεκριμένες διαδικασίες Διαδικτύου των πραγμάτων.

Η τεχνολογία Blockchain μπορεί να προσφέρει ένα πιο προηγμένο περιβάλλον ασφαλείας σε σύγκριση με την ασφάλεια της κεντρικής βάσης δεδομένων.

Στην τεχνολογία blockchain, κάθε μπλοκ στην αλυσίδα παρακολουθεί συνεχώς τη λίστα των εγγραφών που συνδέονται με προηγούμενα μπλοκ, χρησιμοποιώντας την

κρυπτογραφική συνάρτηση κατακερματισμού. Είναι επίσης ένα κατανεμημένο ημερολόγιο που διατηρεί αρχείο των συναλλαγών και μπορεί να αποτρέψει παραμορφώσεις.

Το Blockchain διαχειρίζεται πλήρως μέσω του δικτύου και έχει σχεδιαστεί για να αποτρέπει τυχαίες παρεμβολές. Όσον αφορά τη διαχείριση, επιτρέπει την αποτροπή απειλών και επιθέσεων προσανατολισμένων στα δεδομένα. [13]

Στη σύγχρονη εποχή, τα συστήματα cloud (πριν από την τεχνολογία blockchain) δημιούργησαν μια σοβαρή υποδομή και μια αγορά δισεκατομμυρίων δολαρίων. Αυτά τα συστήματα έχουν μελετηθεί για μεγάλο χρονικό διάστημα, καθιστώντας έναν από τους τομείς σοβαρής ανάπτυξης. Κατά κάποιο τρόπο, η τεχνολογία cloud ήταν η πρώτη τεχνολογική λύση που απομακρύνθηκε από τη συγκέντρωση.

Πιο πρόσφατα, αυτή η τεχνολογία έχει δημιουργήσει την ανάγκη για ευρείες δικτυακές συνδέσεις για την υλοποίηση και χρήση των καθημερινών λειτουργιών κρατών, ατόμων και εταιρειών. Ταυτόχρονα, προβλήματα όπως η συντήρηση του δωματίου διακομιστή, η συνεχής ασφάλεια, η στελέχωση, η παροχή ρεύματος, ο εξαιρισμός και οι τακτικές ενημερώσεις επιτάχυναν σε μεγάλο βαθμό αυτές τις διαδικασίες. Έτσι, οι εταιρείες που μετέφεραν τους διακομιστές τους στο Cloud άρχισαν να πραγματοποιούν τις δραστηριότητές τους προς αυτή την κατεύθυνση πιο γρήγορα.

Η τεχνολογία Blockchain έχει προσφέρει στους χρήστες ένα αξιόπιστο και ανεξίτηλο δίκτυο δεδομένων χάρη σε ένα κατανεμημένο, αποκεντρωμένο σύστημα δικτύου παρόμοιο με το Cloud. Από αυτή την άποψη, είναι λάθος να αξιολογούνται οι τεχνολογίες blockchain και cloud ως δύο ξεχωριστές έννοιες. Αν και το καθένα είναι ένα ουσιαστικό σύστημα από μόνο του, η αξιολόγησή τους από κοινού μπορεί να δώσει στους χρήστες εξαιρετικές προοπτικές όσον αφορά την ασφάλεια.

Σε αντίθεση με τη δομή του cloud, ένα αποκεντρωμένο σύστημα blockchain δεν χρειάζεται να αποθηκεύεται σε κάποιον διακομιστή.

Στην τεχνολογία blockchain, οι δομές που ονομάζονται κόμβοι χρησιμεύουν για τη διατήρηση της ακεραιότητας της αλυσίδας μπλοκ. είναι ένα αντίγραφο του blockchain που βρίσκεται στον ίδιο ή διαφορετικούς υπολογιστές. Αυτοί οι κόμβοι συνδέονται μεταξύ τους από διαφορετικά μέρη, κάνοντας το σύστημα να λειτουργεί και την τεχνολογία blockchain πιο αξιόπιστη καθώς μεγαλώνει. Σε αυτό το πλαίσιο, η ταχύτερη

ανάπτυξη της βιομηχανίας cloud με ενσωμάτωση στην τεχνολογία blockchain στο μέλλον είναι αναπόφευκτη.

Η δυνατότητα του blockchain να χρησιμοποιεί την υπολογιστική ισχύ που είναι διαθέσιμη μέσω του Διαδικτύου μας δίνει τη σιγουριά ότι στο μέλλον, η ανθρωπότητα και η οικονομία θα γίνουν μάρτυρες πιο ριζικών αλλαγών από τις προβλεπόμενες, και ότι το cloud θα κάνει το blockchain πιο διαδεδωμένο. Το blockchain θα καταστήσει δυνατή τη διασφάλιση υψηλότερου επιπέδου ασφάλειας στον κυβερνοχώρο στο μέλλον και τη διατήρηση των δεδομένων σε αποκεντρωμένα περιβάλλοντα πιο ασφαλή, και αυτή η δομή θα ενσωματωθεί με διάφορες τεχνολογίες, επισημοποιώντας την έννοια του blockchain-cloud. [13]

2.1.4 Τεχνολογία Blockchain

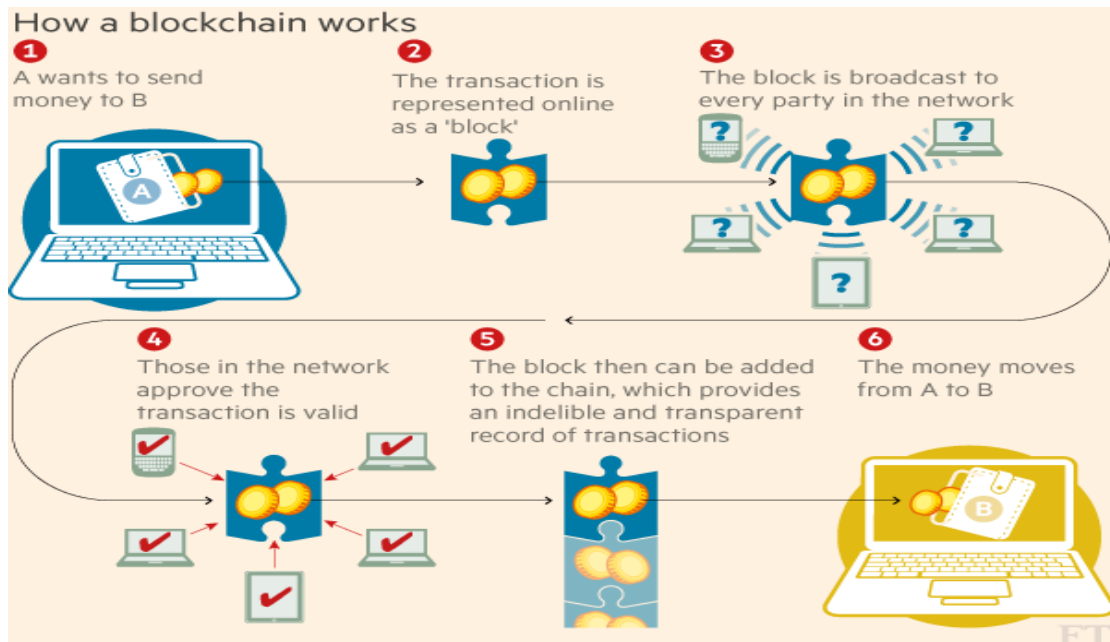
Αναφέρθηκε παραπάνω πως η τεχνολογία του blockchain δεν είναι τίποτα περισσότερο από μια ψηφιακή βάση δεδομένων, η οποία αποτελείται από εγγραφές δεδομένων που ομαδοποιημένα ονομάζονται blocks, και που συνδέονται μεταξύ τους κρυπτογραφικά σε μορφή αλυσίδας δημιουργώντας επομένως αλυσίδα από μπλοκ, δηλαδή blockchain. Η όλη δομή έχει δημιουργηθεί με τέτοιο τρόπο ώστε να μην υπάρχει κανένας κεντρικός έλεγχος ή αρχή, αλλά και ταυτόχρονα η αλλαγή των δεδομένων από μεμονωμένους χρήστες να είναι πρακτικά αδύνατη. Η τεχνολογία του blockchain μπορεί να εξηγηθεί περιγράφοντας πως λειτουργεί το Bitcoin αφού είναι τεχνολογία εγγενώς συνδεδεμένη με το Bitcoin. Στις μέρες μας το εμπόριο μέσω Διαδικτύου αποτελεί μια τεράστια Παγκόσμια αγορά, η οποία συνδέεται αποκλειστικά με τα χρηματοπιστωτικά ιδρύματα που λειτουργούν ως το αξιόπιστο τρίτο μέρος που επεξεργάζεται και διαμεσολαβεί για οποιαδήποτε ηλεκτρονική συναλλαγή. Ο ρόλος του αξιόπιστου τρίτου μέρους είναι να επικυρώνει, να προστατεύει και να διατηρεί τις συναλλαγές. Καθώς ένα ορισμένο ποσοστό απάτης είναι αναπόφευκτο στις διαδικτυακές συναλλαγές, είναι απαραίτητη η μεσολάβηση από οικονομικές συναλλαγές. Αυτό έχει ως αποτέλεσμα υψηλό κόστος συναλλαγής.

Η τεχνολογία blockchain μπορεί να χρησιμοποιηθεί σε οποιαδήποτε διαδικτυακή συναλλαγή. Σε αντιδιαστολή με τον παραδοσιακό trust-in-the-third-party μηχανισμό για μία συναλλαγή που πραγματοποιείται μεταξύ δύο ατόμων στο διαδίκτυο, το Bitcoin χρησιμοποιεί κρυπτογραφική απόδειξη. Κάθε συναλλαγή είναι προστατευμένη μέσω μίας ψηφιακής υπογραφής, μια που είναι σταλμένη στο δημόσιο κλειδί του παραλήπτη

και είναι ψηφιακά υπογεγραμμένη με τη χρήση του ιδιωτικού κλειδιού του αποστολέα. Προκειμένου ο κάτοχος κρυπτονομίσματος να πραγματοποιήσει μία συναλλαγή, χρειάζεται να αποδείξει την κυριότητα του ιδιωτικού κλειδιού. Στη συνέχεια, η οντότητα που λαμβάνει το ψηφιακό νόμισμα επαληθεύει την ψηφιακή υπογραφή, η οποία συνεπάγεται την ιδιοκτησία του αντίστοιχου ιδιωτικού κλειδιού, χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα στην αντίστοιχη συναλλαγή. Κάθε συναλλαγή μεταδίδεται σε κάθε κόμβο του δικτύου Bitcoin και στη συνέχεια αποθηκεύεται σε public ledger μετά από επιβεβαίωση. Όλες οι συναλλαγές πρέπει να επαληθεύονται για εγκυρότητα πριν καταγραφούν στο public ledger. Ο κόμβος που επιβεβαιώνει πρέπει να εξασφαλίσει δύο πράγματα πριν καταγραφεί η οποιαδήποτε συναλλαγή :

1. Ο αποστολέας κατέχει το κρυπτονόμισμα, το οποίο γίνεται μέσω της επαλήθευσης ψηφιακής υπογραφής στη συναλλαγή.
2. Ο αποστολέας έχει επαρκή κρυπτονομίσματα στον λογαριασμό του, το οποίο γίνεται με τον έλεγχο όλων των συναλλαγών που έχει πραγματοποιήσει ή αλλιώς το δημόσιο κλειδί που είναι καταχωρημένο στο ledger. Έτσι, διασφαλίζεται ότι υπάρχει επαρκές υπόλοιπο στο λογαριασμό του αποστολέα για την οριστικοποίηση της συναλλαγής.

Ωστόσο, οι συναλλαγές δεν έρχονται με τη σειρά με την οποία πραγματοποιούνται και έτσι υπάρχει ανάγκη ενός μηχανισμού που επιβεβαιώνει ότι δεν συμβαίνει double spending. Λαμβάνοντας υπόψη ότι οι συναλλαγές περνούν από κόμβο σε κόμβο στο δίκτυο του Bitcoin, δεν εγγυάται κανείς ότι οι συναλλαγές παραλαμβάνονται από τον έναν κόμβο στον άλλον με την σειρά που δημιουργήθηκαν. Το Bitcoin, έλυσε το πρόβλημα αυτό με έναν μηχανισμό που είναι πλέον ευρέως γνωστός ως τεχνολογία Blockchain. Με το μηχανισμό του Bitcoin, οι συναλλαγές τοποθετούνται σε ομάδες και ονομάζονται Blocks. Στη συνέχεια, τα blocks συνδέονται δημιουργώντας μία αλυσίδα block, το blockchain. Οι συναλλαγές σε ένα block θεωρούνται ότι έχουν πραγματοποιηθεί την ίδια στιγμή. Τα blocks αυτά συνδέονται μεταξύ τους με σωστή γραμμική χρονολογική σειρά, με κάθε block που περιέχει τον κατακερματισμό του προηγούμενου block.



Εικόνα 2 Πως λειτουργεί ένα blockchain. [13]

Παραμένει, όμως, ακόμα ένα πρόβλημα. Οποιασδήποτε κόμβος στο δίκτυο μπορεί να συλλέγει μη επιβεβαιωμένες συναλλαγές και να δημιουργεί ένα block το οποίο θα μεταδίδει στο υπόλοιπο δίκτυο ως το επόμενο block που θα προστεθεί στο blockchain. Έτσι, είναι δύσκολο το δίκτυο να αποφασίσει ποιο είναι το επόμενο block πρέπει να προστεθεί στο blockchain. Μπορεί να δημιουργηθούν διαφορετικά blocks από διαφορετικούς κόμβους την ίδια στιγμή και να μην είναι εφικτό να βρεθεί η σωστή σειρά. Το Bitcoin δίνει λύση σε αυτό το πρόβλημα εισάγοντας ένα “μαθηματικό puzzle”. Σύμφωνα με αυτό, κάθε block θα προστίθεται στο blockchain με την προϋπόθεση ότι έχει επιλύσει ένα πολύ ιδιαίτερο μαθηματικό πρόβλημα. Αυτό είναι επίσης γνωστό ως “proof-of-work”, δηλαδή ένας κόμβος που δημιουργεί ένα block πρέπει να αποδείξει ότι έχει την υπολογιστική δύναμη για την επίλυση του μαθηματικού puzzle. Η επίλυση της μαθηματικής εξίσωσης δεν είναι εύκολη και η πολυπλοκότητα του προβλήματος μπορεί να ρυθμιστεί έτσι ώστε να χρειάζονται κατά μέσο όρο δέκα λεπτά για έναν κόμβο του δικτύου να βρει τη λύση και να δημιουργήσει ένα block. Η πιθανότητα να δημιουργηθούν ταυτόχρονα περισσότερα από ένα block είναι εξαιρετικά μικρή. Ο πρώτος κόμβος που θα επιλύσει το πρόβλημα, μεταδίδει το block στο υπόλοιπο δίκτυο. Μετά απ’ αυτό, κάθε κόμβος συμφωνεί σχετικά με τη σειρά των blocks.

Οι κόμβοι που χρησιμοποιούν τους υπολογιστικούς πόρους τους για να επιλύσουν το μαθηματικό πρόβλημα και να δημιουργήσουν block, λέγονται κόμβοι miner και

επιβραβεύονται οικονομικά για την προσπάθεια τους. Το δίκτυο δέχεται μόνο το μεγαλύτερο blockchain ως έγκυρο, έτσι είναι σχεδόν αδύνατο για έναν εισβολέα να εισάγει μία ψευδή συναλλαγή, αφού δεν φτάνει μόνο να δημιουργήσει ένα block, αλλά πρέπει να ανταγωνιστεί τους υπόλοιπους κόμβους του δικτύου και να τους πείσει να αποδεχτούν τη συναλλαγή ως έγκυρη. Μία απάτη στο δίκτυο γίνεται ακόμα πιο απίθανη αφού τα block στο blockchain συνδέονται κρυπτογραφικά μεταξύ τους. [14]

2.1.5 Εξόρυξη των Bitcoins (Bitcoin Mining)

Το bitcoin επειδή είναι αποκεντρωμένο, χρειάζεται τη συνεισφορά τυχαίων υπολογιστών από όλον τον πλανήτη για να επιβεβαιώσει τις συναλλαγές που γίνονται παγκοσμίως. Αυτή η διαδικασία απαιτεί συνολικά τεράστια υπολογιστική δύναμη. Νέα bitcoin εκδίδονται κάθε δέκα λεπτά τα οποία δίνονται ως ανταμοιβή σε αυτούς που συνεισφέρουν στην επιβεβαίωση των συναλλαγών, ανάλογα με τη συνεισφορά του καθενός. Αυτοί που επιβεβαιώνουν συναλλαγές ώστε να εισπράξουν κάποια ανταμοιβή ονομάζονται miners (εξορύκτες) και η διαδικασία mining, αντίστοιχα.

Κάθε συναλλαγή που γίνεται με Bitcoin περνάει από έλεγχο εγκυρότητας και έπειτα τοποθετείται σε ένα block μαζί με άλλες ολοκληρωμένες συναλλαγές. Κάθε μπλοκ που δημιουργείται έχει άμεση σχέση με το αμέσως προηγούμενο άλλα και με όλα τα υπόλοιπα μπλοκ. Με αυτό τον τρόπο δημιουργείται μια αλυσίδα από μπλοκ (block chain). Η σχέση κάθε νέου μπλοκ με τα προηγούμενα καθορίζεται από έναν μαθηματικό αλγόριθμο, ο οποίος όμως είναι δύσκολο να δημιουργηθεί.

Κάθε φορά που δημιουργείται ένα νέο μπλοκ δημιουργείται αυτόματα και ένας αριθμός νέων Bitcoin τα οποία μοιράζονται σε αυτούς που θα έχουν λύσει τον αλγόριθμο ανάλογα με τη συνεισφορά του καθενός. Πολλά κρυπτονομίσματα όπως το Bitcoin, το Ethereum και το Litecoin υιοθετούν τον μηχανισμό PoW ως συναινετικό αλγόριθμο. Στον μηχανισμό PoW, όταν ένας κόμβος λύνει ένα κρυπτογραφικό παζλ, ο κόμβος μπορεί να δημιουργήσει και να διαδώσει ένα έγκυρο μπλοκ. Στη συνέχεια, άλλοι κόμβοι προσαρτούν το μπλοκ που δημιουργείται στην υπάρχουσα αλυσίδα μπλοκ. Το παζλ είναι να βρει την αντίστροφη μιας συνάρτησης κατακερματισμού που ικανοποιεί τη συγκεκριμένη συνθήκη, και έτσι ο κόμβος θα πρέπει να ξοδέψει υπολογιστική ισχύ για να λύσει το κρυπτογραφικό παζλ. Η διαδικασία δημιουργίας ενός μπλοκ ονομάζεται mining και οι κόμβοι που συμμετέχουν στην εξόρυξη ονομάζονται miners. Στα συστήματα, η δυσκολία εξόρυξης προσαρμόζεται ώστε να διατηρείται ο μέσος

χρόνος δημιουργίας ενός μπλοκ. Συγκεκριμένα, η δυσκολία εξόρυξης Bitcoin προσαρμόζεται ώστε να διατηρείται η μέση περίοδος δημιουργίας ενός μπλοκ στα 10 λεπτά. Επιπλέον, για την παροχή κινήτρων για την εξόρυξη, κάθε φορά που ένας miner βρίσκει ένα έγκυρο μπλοκ, ο miner κερδίζει την ανταμοιβή για ένα μπλοκ ως αποζημίωση για την υπολογιστική ισχύ που δαπανάται. Για παράδειγμα, επί του παρόντος, οι miners κερδίζουν την ανταμοιβή μπλοκ των 12,5 νομισμάτων στο σύστημα Bitcoin όταν βρίσκουν ένα μπλοκ. [15]

Όσο μεγαλύτερο ποσοστό της συνολικής υπολογιστικής δύναμης διαθέσει κάποιος για τη λύση του αλγορίθμου τόσο μεγαλύτερο ποσοστό από τα καινούργια bitcoin που δημιουργούνται θα πάρει. Για παράδειγμα, κάποιος που ασχολείται επαγγελματικά με το bitcoin mining και έχει πολλά miners (GPU που έχουν τροποποιηθεί ώστε να λύνουν τον αλγόριθμο) θα πάρει μεγαλύτερο κομμάτι "της πίτας" των καινούργιων bitcoin που βγαίνουν στη κυκλοφορία από κάποιον που έχει μόνο ένα miner. Ο αλγόριθμος που δημιουργείται είναι πάντα τόσο δύσκολος να επιλυθεί ώστε όλη η υπολογιστική δύναμη (όλα τα miners του πλανήτη) που επιδίδονται στη λύση του να χρειάζονται κατά μέσο όρο 10 λεπτά για να τον λύσουν. Κατά συνέπεια με τη πάροδο του χρόνου το σύστημα προσαρμόζει τη λύση του αλγορίθμου και τη κάνει όλο και πιο δύσκολη, μιας και παράλληλα αυξάνεται η συνολική υπολογιστική δύναμη που διατίθεται στη λύση του (με τη πρόοδο της τεχνολογίας και με τη κατασκευή καινούργιων miners). Αυτό μας φέρνει και σε ένα ακόμη συμπέρασμα: Όλα τα miners με τη πάροδο του χρόνου παράγουν όλο και πιο λίγες υποδιαιρέσεις του bitcoin, αφού όσο περνάει ο καιρός αποτελούν ολοένα και μικρότερο ποσοστό της συνολικής υπολογιστικής δύναμης που διατίθεται στη λύση του αλγορίθμου, με αποτέλεσμα έτσι να παίρνουν και πιο μικρό κομμάτι "της πίτας". Όταν ένα miner αναπόφευκτα φτάσει σε σημείο να καταναλώνει περισσότερα χρήματα σε ηλεκτρικό απ' όσα παράγει σε bitcoin τότε δεν έχει νόημα να λειτουργεί πλέον και πρέπει να αντικατασταθεί. Αντίστροφα, εάν μειωθεί η συνολική παγκόσμια υπολογιστική δύναμη των miners (π.χ. με την απαγόρευση εξόρυξεως σε ορισμένες χώρες) τότε αυξάνεται και το μερίδιο της πίτας που λαμβάνουν ξεχωριστά οι εναπομείναντες miner, δίνοντας έτσι κίνητρο σε νέους παίκτες να εισέλθουν στην αγορά και ενδεχομένως επιτρέποντας σε παλιότερους miner να επαναλειτουργήσουν. Ωστόσο, φυσικά η κερδοφορία καθορίζεται όχι μόνο από τον αριθμό bitcoin που εξορύχθηκαν, αλλά και από την τιμή στην οποία αυτά διαπραγματεύονται.

Ο αριθμός των bitcoin που δημιουργούνται με κάθε νέο block μειώνεται πολύ ελαφρά κάθε φορά. Μέσα σε 4 χρόνια τα bitcoin που δημιουργούνται με κάθε νέο block πέφτουν στο μισό. Τα τελευταία bitcoin θα δημιουργηθούν το 2140. Τότε ο συνολικός αριθμός των bitcoin που υπάρχουν θα είναι 21 εκατομμύρια.

Πολλοί άνθρωποι έχουν ασχοληθεί με την εξόρυξη λόγω του κινήτρου για εξόρυξη και έχει εμφανιστεί εξειδικευμένο υλικό για αποτελεσματική εξόρυξη, όπως ολοκληρωμένα κυκλώματα για συγκεκριμένες εφαρμογές (ASIC). Με βάση τους παραπάνω λόγους, η τεράστια υπολογιστική ισχύς χρησιμοποιείται για εξόρυξη και η δυσκολία εξόρυξης έχει αυξηθεί σημαντικά. Επομένως, ένας solo miner, ο οποίος κάνει εξόρυξη μόνος του, θα πρέπει να πάρει πολύ χρόνο για να βρει ένα έγκυρο μπλοκ, και αυτό κάνει τους solo miners να περιμένουν για μεγάλο χρονικό διάστημα για να κερδίσουν ανταμοιβές μπλοκ. Για να μειωθεί όχι μόνο το κόστος των κόμβων αλλά και η διακύμανση των ανταμοιβών τους, έχουν οργανωθεί δεξαμενές εξόρυξης (mining pools) όπου συγκεντρώνονται οι miners για εξόρυξη. Οι περισσότερες mining pools αποτελούνται από εργάτες και έναν διευθυντή. Ο διευθυντής δίνει παζλ στους εργάτες και αυτοί λύνουν τους γρίφους. Εάν ένας εργαζόμενος λύσει ένα δεδομένο παζλ, η ανταμοιβή μπλοκ διανέμεται και στους υπόλοιπους εργαζόμενους του mining pool. [15]

2.1.6 Πλεονεκτήματα

Οι επιτυχημένες καινοτομίες λύνουν σημαντικά προβλήματα. Τα ακόλουθα είναι μερικά από τα προβλήματα που λύνουν τα bitcoin και μερικά από τα κύρια πλεονεκτήματα της χρήσης Bitcoin έναντι άλλων νομισματικών συστημάτων:

- Τα Bitcoin επιτρέπουν ηλεκτρονικές συναλλαγές χωρίς να υπάρχει ανησυχία ότι τα **προσωπικά δεδομένα** (όπως στοιχεία πιστωτικής κάρτας ή τραπεζικού λογαριασμού) θα παραβιαστούν.
- **Ανωνυμία.** Είναι εντελώς ανώνυμο και ταυτόχρονα πλήρως διαφανές. Οποιαδήποτε εταιρεία μπορεί να δημιουργήσει έναν άπειρο αριθμό διευθύνσεων bitcoin χωρίς αναφορά στο όνομα, τη διεύθυνση ή οποιαδήποτε άλλη πληροφορία.
- **Εύκολο στη χρήση.** Οποιοσδήποτε έχει κινητό τηλέφωνο ή σύνδεση στο Διαδίκτυο μπορεί να εκτελεί απρόσκοπτες συναλλαγές, ακόμη και σε ποσά μικρότερα από μια δεκάρα. Αυτό είναι σημαντικό για πολλούς που δεν έχουν **πρόσβαση** σε τράπεζες, ειδικά στον αναπτυσσόμενο κόσμο. Οι συναλλαγές σε

bitcoin συμβαίνουν άμεσα και ανακοινώνονται ταυτόχρονα σε όλο το δίκτυο ανά τον πλανήτη.

- Λαμβάνοντας υπόψη ότι η διαδικασία ανοίγματος ενός τραπεζικού λογαριασμού στις περισσότερες χώρες είναι υπερβολικά περίπλοκη και μπορεί να απορριφθεί χωρίς εξήγηση, η χρήση BTC είναι **βολική για τις εταιρείες**. Μια εταιρεία χρειάζεται περίπου 5 λεπτά για να δημιουργήσει ένα πορτοφόλι BTC και αμέσως ξεκινά να το χρησιμοποιεί χωρίς ερωτήσεις και προμήθειες.
- **Απεριόριστες δυνατότητες συναλλαγών.** Καθένας από τους κατόχους πορτοφολιού μπορεί να πληρώσει σε οποιονδήποτε, οπουδήποτε και οποιοδήποτε ποσό. Η συναλλαγή δεν μπορεί να ελεγχθεί ή να αποτραπεί, επομένως είναι εφικτό να γίνονται μεταφορές οπουδήποτε στον κόσμο όπου κι αν βρίσκεται ένας άλλος χρήστης με πορτοφόλι Bitcoin.
- Οι πληρωμές που γίνονται σε αυτό το σύστημα είναι αδύνατο να ακυρωθούν. Τα νομίσματα δεν μπορούν να παραποιηθούν, να αντιγραφούν ή να δαπανηθούν δύο φορές. Αυτές οι δυνατότητες εγγυώνται την ακεραιότητα ολόκληρου του συστήματος. Κάθε μήνα ο αριθμός των ηλεκτρονικών καταστημάτων, των πόρων και των εταιρειών που δέχονται BTC διευρύνεται.
- **Το εξαιρετικά χαμηλό κόστος λειτουργίας BTC.** Το κρυπτονόμισμα BTC λειτουργεί ως φυσικά μετρητά, συνδυάζοντας τις λειτουργίες του ηλεκτρονικού εμπορίου. Δεν χρειάζεται να πληρώσετε προμήθειες σε τράπεζες και άλλους οργανισμούς. Το κύριο μέρος μιας τέτοιας διαδικασίας είναι τα μαθηματικά, που δεν χρειάζονται χρήματα. Η προμήθεια σε αυτό το σύστημα είναι χαμηλότερη από οποιοδήποτε άλλο. Ανέρχεται στο 0,1% του ποσού της συναλλαγής. Οι χρεώσεις τόκων λειτουργίας πηγαίνουν στα πορτοφόλια του κατόχου BTC, που εκτελούν τους ελέγχους των συναλλαγών και την επιβεβαίωση της αντικειμενικότητάς του, ως αμοιβή για την επεξεργαστική ισχύ που επενδύουν στην προστασία του δικτύου από κακόβουλες επιθέσεις. Η αποστολή και η λήψη Bitcoin απαιτεί από τους χρήστες να διατηρούν μια εφαρμογή πελάτη του Bitcoin σε λειτουργία και συνδεδεμένο με άλλους κόμβους. Ουσιαστικά, με τη χρήση bitcoin, οι χρήστες θα συνεισφέρουν στο δίκτυο και έτσι θα μοιράζονται το βάρος της εξουσιοδότησης συναλλαγών. Η κοινή χρήση αυτής της εργασίας μειώνει σημαντικά το κόστος συναλλαγής και, κατά συνέπεια, το κόστος συναλλαγής είναι αμελητέο.

- Τα διεθνή εμβάσματα έχουν ασήμαντες χρεώσεις σε σύγκριση με το 10% που χρεώνουν οι τρέχουσες εταιρείες σε αυτόν τον χώρο.
- Οι προμήθειες συναλλαγών για τους εμπόρους είναι ελάχιστες, σε σύγκριση με τις προμήθειες πιστωτικών καρτών, κάτι που είναι καλό για εμπόρους λιανικής με στενά περιθώρια.
- **Δεν υπάρχει κίνδυνος πληθωρισμού.** Κι αυτό γιατί ο μέγιστος αριθμός νομισμάτων περιορίζεται αυστηρά κατά 21 εκατομμύρια Bitcoin. Καθώς δεν υπάρχουν ούτε πολιτικές δυνάμεις ούτε εταιρείες ικανές να αλλάξουν αυτή τη σειρά, δεν υπάρχει δυνατότητα ανάπτυξης πληθωρισμού στο σύστημα. Ο ρυθμός με τον οποίο δημιουργούνται τα bitcoin είναι αργός και το σύνολο των νομισμάτων που μπορούν να δημιουργηθούν είναι περιορισμένο, σύμφωνα με τις μαθηματικές επιταγές του συστήματος. Το Bitcoin παρέχει έναν εναλλακτικό τρόπο συναλλαγών για χώρες που αντιμετωπίζουν οικονομικό ή πολιτικό στρες.
- **Ο ανοιχτός κώδικας για την εξόρυξη κρυπτονομισμάτων.** Το BTC εφαρμόζει τους ίδιους αλγόριθμους που χρησιμοποιούνται στην ηλεκτρονική τραπεζική. Η μόνη διαφορά της διαδικτυακής τραπεζικής είναι η αποκάλυψη πληροφοριών σχετικά με τους χρήστες. Όλες οι πληροφορίες σχετικά με τη συναλλαγή στο δίκτυο BTC κοινοποιούνται (πώς, πότε), αλλά δεν υπάρχουν δεδομένα σχετικά με τον παραλήπτη ή τον αποστολέα των νομισμάτων (δεν υπάρχει πρόσβαση στα προσωπικά στοιχεία του πορτοφολιού του ιδιοκτήτη).
- **Υποδιαιρέσεις επιτρέποντας μικρο-συναλλαγές.** Κάθε bitcoin είναι υποδιαιρέσιμο έως 8 δεκαδικά ψηφία (έως 0,00000001) που ονομάζονται Satoshi, επιτρέποντας μικρο-συναλλαγές που δεν είναι δυνατές με άλλα μέσα ή συμβατικά νομίσματα. Η προσθήκη περισσότερων ακόμα δεκαδικών επαφίεται στην συναίνεση του δικτύου αν αυτό χρειαστεί στο μέλλον.
- **Αποκεντρωμένη Φύση.** Δεν υπάρχει κεντρική αρχή ελέγχου στο δίκτυο, το δίκτυο διανέμεται σε όλους τους συμμετέχοντες, κάθε υπολογιστής εξόρυξης bitcoin είναι μέλος αυτού του συστήματος. Αυτό σημαίνει ότι η κεντρική αρχή δεν έχει εξουσία να υπαγορεύει κανόνες για τους κατόχους bitcoin. Και ακόμα κι αν κάποιο τμήμα του δικτύου βγει εκτός σύνδεσης, το σύστημα πληρωμών θα συνεχίσει να λειτουργεί σταθερά. Αρκεί μόνο ένας υπολογιστής που περιέχει το αρχείο της αλυσίδας των προηγούμενων συναλλαγών να παραμείνει συνδεδεμένος στο δίκτυο.

- **Το κατακευκμένο Δίκτυο (peer-to-peer) κρυπτονομισμάτων.** Σε τέτοια δίκτυα δεν υπάρχει κύριος διακομιστής, ο οποίος είναι υπεύθυνος για όλες τις λειτουργίες. Η ανταλλαγή πληροφοριών (εδώ τα χρήματα) γίνεται μεταξύ 2-3 ή περισσότερων κόμβων (πελατών λογισμικού πορτοφολιών) του δικτύου. Όλα τα προγράμματα-πορτοφόλια που εγκαθίστανται από τους χρήστες αποτελούν μέρος ενός δικτύου bitcoin. Κάθε πελάτης αποθηκεύει ένα αρχείο όλων των δεσμευμένων συναλλαγών και τον αριθμό των bitcoin σε κάθε πορτοφόλι. Οι συναλλαγές πραγματοποιούνται από εκατοντάδες κατακευκμένους διακομιστές. Ούτε οι τράπεζες ούτε οι φόροι, ούτε οι κυβερνήσεις μπορούν να ελέγξουν την ανταλλαγή χρημάτων μεταξύ τους.
- **Διαφάνεια.** Όλες οι συναλλαγές που έχουν εκτελεστεί ποτέ στο δίκτυο είναι δημόσια διαθέσιμες και διαφανείς. Όλες οι συναλλαγές που έχουν εκτελεστεί ποτέ στο δίκτυο είναι δημόσια διαθέσιμες και διαφανείς. Η αλυσίδα μπλοκ διατηρεί πληροφορίες για τα πάντα. Έτσι, οποιοσδήποτε μπορεί να εξετάσει οποιαδήποτε διεύθυνση και να δει τις προηγούμενες συναλλαγές που έχουν εκτελεστεί με αυτήν, το πλήθος των bitcoin που έχουν μετακινηθεί, όπως και το που έχουν σταλεί. Αυτό ισχύει για όλες τις συναλλαγές που έχουν εκτελεστεί ποτέ στο δίκτυο έως την πρώτη. Το ίδιο ακριβώς ισχύει για όλους τους κανόνες σύμφωνα με τους οποίους δουλεύει το λογισμικό και στο οποίο συναινούν οι χρήστες. Δεν υπάρχει κανένας κρυφός κανόνας μέσα στο λογισμικό, και δεν είναι δυνατόν να υπάρξει, καθώς οι χρήστες δεν θα το αποδέχονταν. Έτσι, εάν η εταιρεία έχει χρησιμοποιήσει δημόσια τη διεύθυνση BTC, τότε ο καθένας μπορεί να δει πόσα BTC κατέχει. Εάν η διεύθυνση της εταιρείας δεν επιβεβαιωθεί δημόσια, τότε κανείς δεν θα μάθει ποτέ ότι ανήκει σε αυτήν την εταιρεία. Για πλήρη ανωνυμία, οι εταιρείες συνήθως χρησιμοποιούν τη μοναδική διεύθυνση BTC για κάθε συναλλαγή.
- **Ταχύτητα συναλλαγής.** Η δυνατότητα αποστολής χρημάτων οπουδήποτε και σε οποιονδήποτε μέσα σε λίγα λεπτά μετά το δίκτυο BTC θα επεξεργαστεί την πληρωμή.
- **Ανήκει μόνο στον κάτοχο του πορτοφολιού.** Υπάρχει ένα μοναδικό σύστημα ηλεκτρονικών πληρωμών όπου ο λογαριασμός ανήκει μόνο στον ιδιοκτήτη. Για παράδειγμα, στο PayPal εάν για οποιονδήποτε λόγο η εταιρεία αποφασίσει ότι ο κάτοχος χρησιμοποιεί με κάποιο τρόπο τον λογαριασμό με λάθος τρόπο, το σύστημα έχει το δικαίωμα να δεσμεύσει όλα τα χρήματα στον λογαριασμό χωρίς καν να προειδοποιήσει τον ιδιοκτήτη σχετικά. Η επαλήθευση της σωστής χρήσης

του λογαριασμού είναι συνολική ευθύνη του ιδιοκτήτη. Με το BTC, ο κάτοχος έχει ένα ιδιωτικό κλειδί και ένα αντίστοιχο δημόσιο κλειδί, το οποίο είναι η διεύθυνση στο πορτοφόλι BTC. Κανείς εκτός από τον ιδιοκτήτη δεν μπορεί να κάνει ανάληψη bitcoin.

- **Καμία κατάσχεση από τρίτους.** Δεδομένου ότι υπάρχουν πολλά περιττά αντίγραφα της βάσης δεδομένων συναλλαγών, κανείς δεν μπορεί να κατασχέσει τα bitcoins. Το περισσότερο που μπορεί να κάνει κάποιος είναι να αναγκάσει τον χρήστη, με άλλα μέσα, να στείλει τα bitcoin σε κάποιον άλλο. Αυτό σημαίνει ότι οι κυβερνήσεις δεν μπορούν να παγώσουν τον πλούτο κάποιου και έτσι οι χρήστες Bitcoins θα έχουν απόλυτη ελευθερία να κάνουν ό,τι θέλουν με τα χρήματά τους.
- **Χωρίς φόρους.** Δεν υπάρχει τρόπος για ένα τρίτο μέρος να υποκλέψει συναλλαγές Bitcoin, και επομένως δεν υπάρχει βιώσιμος τρόπος για την εφαρμογή ενός συστήματος φορολογίας Bitcoin. Ο μόνος τρόπος πληρωμής φόρου θα ήταν, εάν κάποιος αποστέλλει οικειοθελώς ένα ποσοστό του ποσού που αποστέλλεται ως φόρος.
- **Χωρίς εντοπισμό.** Αν οι χρήστες δεν δημοσιοποιήσουν τις διευθύνσεις του πορτοφολιού τους δημόσια, κανείς δεν μπορεί να εντοπίσει τις συναλλαγές σε αυτούς. Κανείς, εκτός από τους κατόχους πορτοφολιών, δεν θα ξέρει πόσα Bitcoins έχουν. Ακόμα κι αν η διεύθυνση του πορτοφολιού δημοσιοποιήθηκε, μπορεί εύκολα να δημιουργηθεί μια νέα διεύθυνση πορτοφολιού. Αυτό αυξάνει σημαντικά το απόρρητο σε σύγκριση με τα παραδοσιακά νομισματικά συστήματα, όπου τρίτα μέρη έχουν δυνητικά πρόσβαση σε προσωπικά οικονομικά δεδομένα.
- **Κανένας κίνδυνος «επιστροφής χρεώσεων».** Μόλις αποσταλούν Bitcoin, η συναλλαγή είναι τελική και μη αντιστρέψιμη. Αυτό έχει το επιπλέον πλεονέκτημα προς όσους διαθέτουν προϊόντα για bitcoin ότι δεν είναι δυνατόν να ανακληθούν συναλλαγές όπως π.χ. είθισται στις απάτες με πιστωτικές κάρτες. Αυτό συνήθως δίνει επιπλέον κίνητρα σε επιχειρήσεις να προσφέρουν τα προϊόντα τους σε χαμηλότερες τιμές, εξαιτίας της άμεσης και αμετάκλητης πληρωμής. Από την άλλη, οι χρήστες που εκτελούν αγορές με bitcoin πρέπει να είναι προσεκτικοί στις επιλογές τους, καθώς ένας πάροχος προϊόντων ή υπηρεσιών που δεν έχει ιστορικό κινήσεων ή έμπιστη παρουσία στην αγορά μπορεί να μην είναι αυτό που δείχνει. Εφόσον μόνο ο νέος κάτοχος έχει το συσχετισμένο ιδιωτικό κλειδί, μόνο

αυτός/αυτή μπορεί να αλλάξει την ιδιοκτησία των νομισμάτων. Αυτό διασφαλίζει ότι δεν υπάρχει κίνδυνος κατά τη λήψη Bitcoin.

- **Τα Bitcoins δεν μπορούν να κλαπούν.** Η διεύθυνση ιδιοκτησίας των Bitcoins μπορεί να αλλάξει μόνο από τον κάτοχο. Κανείς δεν μπορεί να κλέψει Bitcoins εκτός εάν έχει φυσική πρόσβαση στον υπολογιστή ενός χρήστη και στέλνει τα bitcoin στον λογαριασμό του. Σε αντίθεση με τα συμβατικά συστήματα νομισμάτων, όπου απαιτούνται μόνο μερικές λεπτομέρειες ελέγχου ταυτότητας για να αποκτήσετε πρόσβαση στα οικονομικά, αυτό το σύστημα απαιτεί φυσική πρόσβαση, γεγονός που καθιστά πολύ πιο δύσκολη την κλοπή.
- **Ιδιωτικότητα συναλλαγών:** Κάθε χρήστης μπορεί να δημιουργήσει, μέσω του λογισμικού, σχεδόν απεριόριστο αριθμό διευθύνσεων μέσω των οποίων να εκτελέσει τις συναλλαγές του. Αυτές οι διευθύνσεις είναι ψευδώνυμες, δεν έχουν δηλαδή κάποια άμεση σχέση με τα πραγματικά στοιχεία ή την τοποθεσία του χρήστη, παρόλο που έχουν αναγνωρίσιμα χαρακτηριστικά ώστε να εντοπίζονται από το δίκτυο. Με αυτό τον τρόπο μπορεί ο χρήστης να διατηρήσει την ιδιωτικότητά του απομπλέκοντας τις συναλλαγές του από τα προσωπικά του στοιχεία. Αυτό δεν συνεπάγεται εξ' ορισμού ανωνυμία συναλλαγών καθώς όλες οι συναλλαγές δημοσιεύονται, και έστω και μία συναλλαγή να έχει γνωστό (δημόσιο) αποδέκτη, ίσως μπορεί να εξαχθεί από συμπληρωματικά στοιχεία η ταυτότητα του χρήστη. Αυτός είναι και ο κύριος λόγος για τον οποίο η χρήση bitcoins δεν ενδείκνυται για συναλλαγές παράνομων δραστηριοτήτων, ιδιαίτερα μεγάλης κλίμακας, καθώς το ίχνος των συναλλαγών όχι μόνο δεν διαγράφεται με το πέρασμα του χρόνου, αλλά παραμένει διαθέσιμο για εξέταση από όλους, για πάντα.
- **Δεν υπάρχουν πιθανότητες να χρησιμοποιηθούν ορισμένα προσωπικά δεδομένα για απάτη.** Αυτό είναι ένα σημαντικό σημείο. Σήμερα οι περισσότερες αγορές γίνονται με πιστωτικές κάρτες. Είναι αναξιόπιστοι. Συμπληρώνοντας φόρμες σε ιστοσελίδες, οι πελάτες υποχρεούνται να εισάγουν τα ακόλουθα στοιχεία: αριθμό κάρτας, ημερομηνία λήξης και κωδικό. Κι αυτό δεν αποτελεί ασφαλή τρόπο πληρωμής. Ως εκ τούτου, οι πιστωτικές κάρτες κλέβονται πολύ συχνά. Οι συναλλαγές BTC δεν απαιτούν αποκάλυψη προσωπικών δεδομένων. Αντίθετα, χρησιμοποιεί δύο κλειδιά: δημόσιο και ιδιωτικό. Το δημόσιο είναι διαθέσιμο σε όλους (δηλαδή η διεύθυνση του πορτοφολιού BTC), αλλά το ιδιωτικό κλειδί είναι γνωστό μόνο στον κάτοχο. Η συναλλαγή πρέπει να υπογραφεί με

αλληλεπίδραση ιδιωτικών κλειδιών και εφαρμογή μιας μαθηματικής συνάρτησης. Αυτό δημιουργεί στοιχεία ότι η συναλλαγή πραγματοποιείται από τον ιδιοκτήτη. [16], [17], [18]

2.1.7 Μειονεκτήματα, ρίσκα και κίνδυνοι

Τα τελευταία χρόνια, υπήρξαν πολλές επιθέσεις και προβλήματα με συστήματα κρυπτονομισμάτων, και αυτές οι επιθέσεις ή προβλήματα έχουν προκαλέσει ακόμη και τη διάσπαση των συστημάτων κρυπτονομισμάτων. Για παράδειγμα, επειδή το Bitcoin έχει γίνει ένα δημοφιλές κρυπτονόμισμα, το σύστημα πρέπει να παρέχει υψηλή απόδοση συναλλαγών. Για να αντιμετωπιστεί το ζήτημα της επεκτασιμότητας, έχουν προταθεί διάφορες λύσεις, όπως το Segregated Witness και το απεριόριστο μέγεθος μπλοκ. Λόγω της συζήτησης για τις προτεινόμενες λύσεις, το Bitcoin τελικά χωρίστηκε στο αρχικό Bitcoin (BTC) και στο Bitcoin Cash (BCH) στις αρχές Αυγούστου 2017. Παρόλο που το BCH επέλεξε να αυξήσει το όριο μεγέθους μπλοκ προκειμένου να επιτρέψει περισσότερες συναλλαγές ανά μπλοκ, το πρωτόκολλο εξόρυξης του BCH σχεδιάστηκε για να είναι συμβατό με αυτό του BTC. Επομένως, οι εξορύκτες μπορούν να διεξάγουν εξόρυξη BTC και BCH με μία συσκευή υλικού. [15]

Όπως κάθε νόμισμα, υπάρχουν μειονεκτήματα που σχετίζονται με τη χρήση του Bitcoin:

- **Τα Bitcoins δεν γίνονται ευρέως αποδεκτά.** Τα Bitcoin εξακολουθούν να γίνονται αποδεκτά μόνο από μια πολύ μικρή ομάδα διαδικτυακών εμπόρων. Αυτό καθιστά ανέφικτο να βασίζεστε πλήρως στα Bitcoins ως νόμισμα. Υπάρχει επίσης η πιθανότητα οι κυβερνήσεις να αναγκάσουν τους εμπόρους να μην χρησιμοποιούν Bitcoin για να διασφαλίσουν ότι οι συναλλαγές των χρηστών μπορούν να παρακολουθούνται.
- **Τα πορτοφόλια μπορούν να χαθούν.** Εάν ένας σκληρός δίσκος καταρρεύσει ή ένας ιός καταστρέψει τα δεδομένα και το αρχείο του πορτοφολιού είναι κατεστραμμένο, τα Bitcoins έχουν ουσιαστικά «χαθεί». Δεν υπάρχει τίποτα που μπορεί να γίνει για να το ανακτήσει. Αυτά τα νομίσματα θα μείνουν για πάντα ορφανά στο σύστημα. Αυτό μπορεί να χρεοκοπήσει έναν πλούσιο επενδυτή Bitcoin μέσα σε λίγα δευτερόλεπτα χωρίς καμία μορφή ανάκαμψης. Τα νομίσματα που κατείχε ο επενδυτής θα μείνουν επίσης οριστικά ορφανά.

- **Η αποτίμηση του Bitcoin παρουσιάζει διακυμάνσεις.** Έντονη αστάθεια – σχεδόν όλα τα σκαμπανεβάσματα της τιμής του BTC εξαρτώνται άμεσα από τις δηλώσεις των κυβερνήσεων διαφορετικών χωρών. Καθώς τα bitcoin δεν έχουν κάποια κεντρική αρχή να παρεμβαίνει στις διακυμάνσεις στην προσφορά και την ζήτηση όπως συμβαίνει με π.χ. τα κρατικά νομίσματα, είναι επιρρεπές σε μεγαλύτερες διακυμάνσεις της ισοτιμίας του με τα περισσότερα νομίσματα. Αυτή η αστάθεια δημιουργεί το πρόβλημα βραχυπρόθεσμα. Επίσης η αξία των Bitcoin κυμαίνεται συνεχώς ανάλογα με τη ζήτηση. Από τις 2 Ιουνίου 2011, ένα Bitcoin αποτιμήθηκε στα 9,9\$ σε μια δημοφιλή τοποθεσία ανταλλαγής bitcoin. Υπολογίστηκε ότι ήταν λιγότερο από \$1 μόλις πριν από 6 μήνες. Αυτή η συνεχής διακύμανση θα κάνει τους ιστότοπους που δέχονται Bitcoin να αλλάζουν συνεχώς τις τιμές. Θα προκαλέσει επίσης μεγάλη σύγχυση εάν γίνει επιστροφή χρημάτων για ένα προϊόν. Για παράδειγμα, εάν ένα μπλουζάκι αγοράστηκε αρχικά για 1,5 BTC και επιστραφεί μια εβδομάδα αργότερα, θα πρέπει να επιστραφεί 1,5 BTC, παρόλο που η αποτίμηση έχει αυξηθεί ή θα πρέπει να σταλεί το νέο ποσό (υπολογισμένο σύμφωνα με την τρέχουσα αποτίμηση); Με ποιο νόμισμα πρέπει να συνδέεται το BTC κατά τη σύγκριση της αποτίμησης; Αυτά είναι ακόμα σημαντικά ερωτήματα για τα οποία η κοινότητα του Bitcoin εξακολουθεί να μην έχει συναίνεση.
- **Ενσωματωμένο ξεφούσκωμα.** Δεδομένου ότι ο συνολικός αριθμός των bitcoin περιορίζεται στα 21 εκατομμύρια, θα προκαλέσει αποπληθωρισμό. Κάθε bitcoin θα αξίζει όλο και περισσότερο καθώς ο συνολικός αριθμός των Bitcoin μεγιστοποιείται. Αυτό το σύστημα έχει σχεδιαστεί για να ανταμείβει τους πρώιμους χρήστες. Δεδομένου ότι κάθε bitcoin θα αποτιμάται υψηλότερα κάθε μέρα που περνά, το ερώτημα του πότε να ξοδέψετε γίνεται σημαντικό. Αυτό μπορεί να προκαλέσει αυξήσεις δαπανών που θα προκαλέσουν τις διακυμάνσεις της οικονομίας του Bitcoin πολύ γρήγορα και απρόβλεπτα.
- **Χωρίς προστασία αγοραστή.** Όταν τα αγαθά αγοράζονται με Bitcoin και ο πωλητής δεν στέλνει τα υποσχόμενα αγαθά, δεν μπορεί να γίνει τίποτα για να αντιστραφεί η συναλλαγή. Αυτό το πρόβλημα μπορεί να λυθεί χρησιμοποιώντας μια υπηρεσία μεσεγγύησης τρίτου μέρους όπως το ClearCoin, αλλά στη συνέχεια, οι υπηρεσίες μεσεγγύησης θα αναλάμβαναν το ρόλο των τραπεζών, κάτι που θα έκανε τα Bitcoin να είναι παρόμοια με ένα πιο παραδοσιακό νόμισμα.

- **Κίνδυνος άγνωστων τεχνικών ελαττωμάτων.** Το σύστημα Bitcoin θα μπορούσε να περιέχει ανεκμετάλλευτα ελαττώματα. Καθώς πρόκειται για ένα αρκετά νέο σύστημα, εάν τα Bitcoin υιοθετούνταν ευρέως και διαπιστωθεί ένα ελάττωμα, θα μπορούσε να δώσει τεράστιο πλούτο στον εκμεταλλευτή σε βάρος της καταστροφής της οικονομίας του Bitcoin.
- **Απώλεια ιδιωτικών κλειδιών - οι κίνδυνοι hacking:** Είναι κρίσιμο να μην περιέλθει το ιδιωτικό κλειδί σε χέρια κακόβουλα. Αν και το λογισμικό παρέχει ικανή προστασία για το μέσο χρήστη, είναι επιβεβλημένη η στρατηγική προστασίας των ιδιωτικών κλειδιών, απέναντι σε κακόβουλο λογισμικό ή κάποιου άλλου είδους παραβιάσεις τόσο φυσικές όσο και ψηφιακές.
- **Η έλλειψη κεντρικού εκδότη.** Μια ανάγνωση αυτής της αρχιτεκτονικής μπορεί να σημαίνει και ότι δεν υπάρχει νομική επίσημη οντότητα για εγγύηση σε περίπτωση πτώχευσης.
- **Χωρίς εγγύηση αποτίμησης.** Δεδομένου ότι δεν υπάρχει κεντρική αρχή που να διέπει τα Bitcoin, κανείς δεν μπορεί να εγγυηθεί την ελάχιστη αποτίμησή τους. Εάν μια μεγάλη ομάδα εμπόρων αποφασίσει να «ρίξει» τα Bitcoins και να εγκαταλείψει το σύστημα, η αποτίμησή του θα μειωθεί πολύ, κάτι που θα βλάψει πάρα πολύ τους χρήστες που έχουν επενδύσει μεγάλο ποσό πλούτου σε Bitcoin. Η αποκεντρωμένη φύση του bitcoin είναι ταυτόχρονα κατάρρα και ευλογία.
- **Χωρίς φυσική μορφή.** Δεδομένου ότι τα Bitcoin δεν έχουν φυσική μορφή, δεν μπορούν να χρησιμοποιηθούν σε φυσικά καταστήματα. Θα έπρεπε πάντα να μετατρέπεται σε άλλα νομίσματα. Έχουν προταθεί κάρτες με πληροφορίες πορτοφολιού Bitcoin που είναι αποθηκευμένες σε αυτές, αλλά δεν υπάρχει συναίνεση για ένα συγκεκριμένο σύστημα. Δεδομένου ότι θα υπήρχαν πολλά ανταγωνιστικά συστήματα, οι έμποροι θα θεωρούσαν αδύνατο να υποστηρίξουν όλες τις κάρτες Bitcoin και επομένως οι χρήστες θα αναγκάζονταν να μετατρέψουν Bitcoins ούτως ή άλλως, εκτός εάν προταθεί και εφαρμοστεί ένα καθολικό σύστημα.
- **Ασαφές νομικό πλαίσιο:** Η φύση των bitcoin τα καθιστά δύσκολα στην αντιμετώπιση τους ενιαία από όλες τις χώρες. Η ευρωπαϊκή νομοθεσία έχει λάβει μέτρα για τη θέσπιση όρων σε ότι αφορά κεντρικά ελεγχόμενα ή εκδιδόμενα ψηφιακά νομίσματα. Η Γερμανία τα έχει καθορίσει ως "ιδιωτικά χρήματα" (privates Geld), ενώ η Ολλανδία ως κάτι στο οποίο δεν χρειάζεται ο έλεγχος της

κεντρικής τράπεζας της χώρας. Στην Ελλάδα το bitcoin χαρακτηρίζεται ως χρήμα και έτσι όλες οι συναλλαγές σε bitcoin θα πρέπει να αντιμετωπίζονται ως χρηματικές. Στις ΗΠΑ, η κύρια επίσημη οδηγία (FINCEN) έχει στόχευση στην προσπάθεια αποφυγής εγκληματικών οικονομικών δραστηριοτήτων με τη χρήση bitcoins, με αμφισβητούμενη ως τώρα επιτυχία, πέρα από την επιβράδυνση και δυσχέραση των επιχειρηματικών δραστηριοτήτων που σχετίζονται με bitcoin και αφορούν πελάτες από τις ΗΠΑ. Θεωρείται απίθανο κάποια χώρα να απαγορέψει ολοκληρωτικά τις συναλλαγές με bitcoin, και κάτι τέτοιο είναι εξαιρετικά δύσκολο (έως αδύνατο) να εφαρμοστεί πρακτικά. Δεν αποκλείεται στην προσπάθεια διερεύνησης του περιβάλλοντος όμως, να ισχύσουν οδηγίες με αναδρομική ισχύ που να αλλάζουν το τοπίο, κυρίως επηρεάζοντας τις απαιτήσεις από τις επιχειρήσεις αλλά όχι τόσο τους χρήστες και την ιδιοκτησία τους. Το κύριο σημείο στο οποίο προβλέπεται ότι θα ασκηθεί κρατική επίβλεψη είναι το σημείο ανταλλαγής με τα κρατικά νομίσματα. [17], [18]

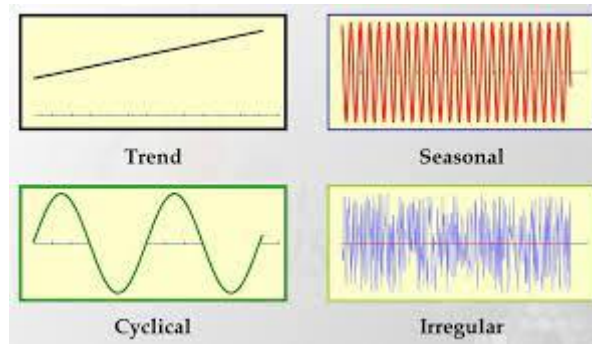
3 Χρονοσειρές και Πρόβλεψη

3.1 Χρονοσειρές [19]

Με τον όρο χρονολογική σειρά ή χρονοσειρά ορίζουμε μια σειρά δεδομένων με κύριο χαρακτηριστικό τη διατεταγμένη χρονική διάταξη των παρατηρήσεων της σειράς. Πρόκειται δηλαδή για ένα σύνολο από δεδομένα που δίνονται με χρονική διάταξη όπως η τιμή της μετοχής μιας εταιρίας στο χρηματιστήριο ή η τιμή του Bitcoin που αποτελεί και το ερευνητικό αντικείμενο της εργασίας.

Ανάλογα με το είδος της παραμέτρου του χρόνου οι χρονοσειρές χωρίζονται σε κατηγορίες: ως προς τη μέτρηση του χρόνου και ως προς το πλήθος των μεταβλητών που επηρεάζεται από την χρονική εξέλιξη. Έτσι, υπάρχουν χρονοσειρές διακριτού χρόνου (ημερήσιες, μηνιαίες, ετήσιες) και χρονοσειρές συνεχούς χρόνου (που αναφέρονται σε κάθε σημείο του χρόνου), όπως επίσης μονομεταβλητές χρονοσειρές (univariate time series) και πολυμεταβλητές χρονοσειρές (multivariate time series).

Οι χρονοσειρές, εμφανίζουν κάποια κοινά ποιοτικά χαρακτηριστικά όπως την στασιμότητα, όταν οι τιμές κυμαίνονται γύρω από μία μέση τιμή, ή μη στασιμότητα (stationary or non-stationary), την τάση (trend), που αντιπροσωπεύει μια γενική συστηματική γραμμική ή μη γραμμική διαδικασία που αλλάζει με την πάροδο του χρόνου και δεν επαναλαμβάνεται ή τουλάχιστον δεν επαναλαμβάνεται μέσα στα όρια του χρόνου που καλύπτουν τα στοιχεία που έχουμε, την περιοδικότητα που διακρίνεται σε εποχικότητα (seasonality) όταν η χρονοσειρά επαναλαμβάνεται σε συστηματικά διαστήματα με την πάροδο του χρόνου ή κυκλική διακύμανση (cycle) όταν οι τιμές αυξομειώνονται, αλλά όχι σε σταθερές περιόδους, τα κατάλοιπα (residuals), τις ασυνέχειες (Discontinuity), τις ασυνήθιστες τιμές (Outliers), την τυχαιότητα (Randomization), όταν έχουμε διακυμάνσεις λόγω τυχαίων γεγονότων, αλλά και την αυτοσυσχέτιση (auto-correlation) και τη συσχέτιση με άλλες χρονοσειρές (cross-correlation). Απομονώνοντας αυτά τα στοιχεία και μετρώντας την προφανή επιρροή του καθενός, είναι πιθανό να προβλέψουμε τις μελλοντικές τιμές της χρονοσειράς.



Εικόνα 3 Χαρακτηριστικά χρονοσειρών. [19]

Στην προσπάθεια μελέτης των ημερήσιων τιμών του Bitcoin θα χρησιμοποιηθούν μονομεταβλητές χρονοσειρές διακριτού χρόνου, επικεντρώνοντας την προσοχή μας στη τιμή κλεισίματος συνεπώς με χρονική μεταβολή μιας ημέρας.

Η ανάλυση των χρονοσειρών περιλαμβάνει τα παρακάτω υποπροβλήματα:

1. Την πρόβλεψη (Prediction)
2. Την μοντελοποίηση (Modeling)
3. Και τον χαρακτηρισμό (Characterization)

Στόχος της πρόβλεψης είναι να υπολογίσει τις μελλοντικές τιμές της μεταβλητής της χρονοσειράς, ενώ μέσω της μοντελοποίησης γίνεται η καταγραφή της συμπεριφοράς της μεταβλητής που μελετάται ιδιότητες και με τον χαρακτηρισμό του συστήματος γίνεται καθορισμός κάποιων θεμελιωδών ιδιοτήτων του συστήματος.

Για την αξιολόγηση της απόδοσης των μοντέλων πρόβλεψης, η κάθε χρονοσειρά χωρίζεται σε δύο τμήματα:

- Το πρώτο σύνολο σημείων χρησιμοποιείται για την εκμάθηση του μοντέλου (δεδομένα εκπαίδευσης - training set). Για τα διάφορα μοντέλα αυτό το σύνολο σημείων δίνει τις απαραίτητες παραμέτρους που θα χρησιμοποιηθούν στην εφαρμογή.
- Το δεύτερο σύνολο σημείων χρησιμοποιείται στην εκτίμηση του λάθους πρόβλεψης (δεδομένα δοκιμής/ελέγχου - test set). Αυτά είναι τα σημεία αναφοράς για τα οποία γίνεται πρόβλεψη και συγκρίνεται με τις πραγματικές παρατηρήσεις.

Είναι σύνηθες στη στατιστική ανάλυση των χρονοσειρών η χρησιμοποίηση του 80% των δεδομένων για την προσαρμογή ή την εκμάθηση του μοντέλου και του 20% για την αξιολόγηση της πρόβλεψης.

3.2 Πρόβλεψη (Forecasting)

Από τις περισσότερες χρήσιμες εφαρμογές της ανάλυσης χρονοσειρών είναι η παρατήρηση της εξέλιξης των μεγεθών που περιγράφουν αυτές και η εκτίμηση της μελλοντικής πορείας της ακολουθίας των παρατηρήσεων. Η πρόβλεψη των μελλοντικών τιμών της μεταβλητής γίνεται με βάση την προηγούμενη συμπεριφορά της. Η διαδικασία αυτή έχει τυποποιηθεί με επιτυχία μέσω μαθηματικών ή ευριστικών μοντέλων, τα οποία είναι γνωστά ως μοντέλα πρόβλεψης. Χωρίς αμφιβολία, το ενδιαφέρον και η σημασία της πρόβλεψης έχει αυξηθεί ραγδαία τα τελευταία χρόνια. Ανάλογα με τη φύση της ακολουθίας των γεγονότων, οι προσεγγίσεις για την εύρεση των λύσεων σε ένα πρόβλημα μπορεί να είναι διαφορετικές.

3.3 Μηχανική Μάθηση

Η μηχανική μάθηση είναι ένας κλάδος της τεχνητής νοημοσύνης (AI) και της επιστήμης των υπολογιστών που εστιάζει στη χρήση δεδομένων και αλγορίθμων για τη μίμηση του τρόπου με τον οποίο μαθαίνουν οι άνθρωποι, βελτιώνοντας σταδιακά την ακρίβειά της.

Η μηχανική μάθηση είναι ένα σημαντικό στοιχείο του αναπτυσσόμενου τομέα της επιστήμης δεδομένων. Μέσω της χρήσης στατιστικών μεθόδων, οι αλγόριθμοι εκπαιδεύονται να κάνουν ταξινομήσεις ή προβλέψεις, αποκαλύπτοντας βασικές γνώσεις στα έργα εξόρυξης δεδομένων. Αυτά οι γνώσεις στη συνέχεια οδηγούν στη λήψη αποφάσεων εντός των εφαρμογών και των επιχειρήσεων, επηρεάζοντας ιδανικά τις βασικές μετρήσεις ανάπτυξης. Καθώς τα μεγάλα δεδομένα συνεχίζουν να επεκτείνονται και να αναπτύσσονται, αποτελεί έναν σημαντικό τομέα στις σύγχρονες κοινωνίες.

3.4 Μέθοδοι μηχανικής μάθησης [20]

Οι ταξινομητές μηχανικής μάθησης εμπίπτουν σε τρεις κύριες κατηγορίες.

3.4.1 Εποπτευόμενη μηχανική εκμάθηση

Η εποπτευόμενη μάθηση, γνωστή και ως εποπτευόμενη μηχανική μάθηση, ορίζεται από τη χρήση επισημασμένων συνόλων δεδομένων για την εκπαίδευση αλγορίθμων

που ταξινομούν δεδομένα ή προβλέπουν τα αποτελέσματα με ακρίβεια. Καθώς τα δεδομένα εισόδου τροφοδοτούνται στο μοντέλο, προσαρμόζει τα βάρη του έως ότου το μοντέλο τοποθετηθεί κατάλληλα. Αυτό συμβαίνει ως μέρος της διαδικασίας πολλαπλής επικύρωσης για να διασφαλιστεί ότι το μοντέλο αποφεύγει την υπερπροσαρμογή ή την υποσυναρμολόγηση. Η εποπτευόμενη μάθηση βοηθά τους οργανισμούς να λύσουν μια ποικιλία πραγματικών προβλημάτων σε κλίμακα, όπως η ταξινόμηση των ανεπιθύμητων μηνυμάτων σε ξεχωριστό φάκελο από τα εισερχόμενά σας. Ορισμένες μέθοδοι που χρησιμοποιούνται στην εποπτευόμενη μάθηση περιλαμβάνουν τα νευρωνικά δίκτυα, τις απλές bayes, τη γραμμική παλινδρόμηση, την λογιστική παλινδρόμηση, το τυχαίο δάσος, τη μηχανή διανυσμάτων υποστήριξης (SVM) και άλλα.

3.4.2 Μη εποπτευόμενη μηχανική εκμάθηση

Η μη εποπτευόμενη μάθηση, γνωστή και ως μη εποπτευόμενη μηχανική μάθηση, χρησιμοποιεί αλγόριθμους μηχανικής μάθησης για την ανάλυση και την ομαδοποίηση συνόλων δεδομένων χωρίς ετικέτα. Αυτοί οι αλγόριθμοι ανακαλύπτουν κρυφά μοτίβα ή ομαδοποιήσεις δεδομένων χωρίς την ανάγκη ανθρώπινης παρέμβασης. Η ικανότητά του να ανακαλύπτει ομοιότητες και διαφορές στις πληροφορίες το καθιστά την ιδανική λύση για διερευνητική ανάλυση δεδομένων, στρατηγικές cross-selling, τμηματοποίηση πελατών, αναγνώριση εικόνας και μοτίβων. Χρησιμοποιείται επίσης για τη μείωση του αριθμού των χαρακτηριστικών σε ένα μοντέλο μέσω της διαδικασίας μείωσης διαστάσεων. Η ανάλυση κύριου συστατικού (PCA) και η αποσύνθεση μονής τιμής (SVD) είναι δύο κοινές προσεγγίσεις για αυτό. Άλλοι αλγόριθμοι που χρησιμοποιούνται στην μάθηση χωρίς επίβλεψη περιλαμβάνουν νευρωνικά δίκτυα, ομαδοποίηση k-means, πιθανοτικές μεθόδους ομαδοποίησης και πολλά άλλα.

3.4.3 Ημι-εποπτευόμενη μάθηση

Η ημι-εποπτευόμενη μάθηση προσφέρει ένα ευχάριστο μέσο μεταξύ εποπτευόμενης και μη εποπτευόμενης μάθησης. Κατά τη διάρκεια της εκπαίδευσης, χρησιμοποιεί ένα μικρότερο σύνολο δεδομένων με ετικέτα για να καθοδηγήσει την ταξινόμηση και την εξαγωγή χαρακτηριστικών από ένα μεγαλύτερο, χωρίς ετικέτα σύνολο δεδομένων. Η ημι-εποπτευόμενη μάθηση μπορεί να λύσει το πρόβλημα της έλλειψης επαρκών ετικετοποιημένων δεδομένων (ή της έλλειψης οικονομικής δυνατότητας για την

επισήμανση επαρκών δεδομένων) για την εκπαίδευση ενός εποπτευόμενου αλγόριθμου μάθησης.

Η ενισχυτική μάθηση (Reinforcement Learning) είναι επίσης ένας τομέας της Μηχανικής Μάθησης. Η ενισχυτική μηχανική μάθηση είναι ένα συμπεριφορικό μοντέλο μηχανικής μάθησης που είναι παρόμοιο με την εποπτευόμενη μάθηση, αλλά ο αλγόριθμος δεν εκπαιδεύεται χρησιμοποιώντας δείγματα δεδομένων. Αυτό το μοντέλο μαθαίνει καθώς προχωρά χρησιμοποιώντας δοκιμή και σφάλμα. Μια σειρά επιτυχών αποτελεσμάτων θα ενισχυθεί για να αναπτυχθεί η καλύτερη σύσταση ή πολιτική για ένα δεδομένο πρόβλημα. [20] Πρόκειται για τη λήψη κατάλληλων μέτρων για τη μεγιστοποίηση της ανταμοιβής σε μια συγκεκριμένη κατάσταση. Χρησιμοποιείται από διάφορα λογισμικά και μηχανήματα για να βρει την καλύτερη δυνατή συμπεριφορά ή διαδρομή που πρέπει να ακολουθήσει σε μια συγκεκριμένη κατάσταση. Η ενισχυτική μάθηση διαφέρει από την εποπτευόμενη μάθηση με τρόπο που στην εποπτευόμενη μάθηση τα δεδομένα εκπαίδευσης έχουν το κλειδί απάντησης, έτσι το μοντέλο εκπαιδεύεται με τη σωστή απάντηση, ενώ στην ενισχυτική μάθηση, δεν υπάρχει απάντηση, αλλά ο ενισχυτικός παράγοντας αποφασίζει τι να κάνει εκτελέσει τη δεδομένη εργασία. Ελλείπει δεδομένων κατάρτισης, είναι βέβαιο ότι θα διδαχθεί από την εμπειρία του. [21]

Στη συνέχεια ακολουθεί μια περιγραφή μοντέλων που χρησιμοποιήθηκαν στα πειράματα.

3.5 To SMOReg (μοντέλο SVM) για παλινδρόμηση.

Το SMOReg που υλοποιεί το μοντέλο SVM - Support Vector Machine για παλινδρόμηση. Εφαρμόζει τον αλγόριθμο διαδοχικής ελάχιστης βελτιστοποίησης των Alex Smola και Bernhard Scholkopf για την εκπαίδευση ενός μοντέλου παλινδρόμησης SVM. Αυτή η υλοποίηση αντικαθιστά συνολικά όλες τις τιμές που λείπουν και μετατρέπει τα ονομαστικά χαρακτηριστικά σε δυαδικά. Επίσης κανονικοποιεί όλα τα χαρακτηριστικά από προεπιλογή. (Σημειώστε ότι οι συντελεστές στην έξοδο βασίζονται στα κανονικοποιημένα/διακριτοποιημένα δεδομένα και όχι στα αρχικά δεδομένα.) [22]

3.6 Η γραμμική παλινδρόμηση – Linear Regression.

Η ανάλυση γραμμικής παλινδρόμησης χρησιμοποιείται για την πρόβλεψη της τιμής μιας μεταβλητής με βάση την τιμή μιας άλλης μεταβλητής. Η μεταβλητή για την οποία

γίνεται η πρόβλεψη ονομάζεται εξαρτημένη μεταβλητή. Η μεταβλητή που χρησιμοποιείτε για την πρόβλεψη της τιμής μιας άλλης μεταβλητής ονομάζεται ανεξάρτητη μεταβλητή.

Αυτή η μορφή ανάλυσης εκτιμά τους συντελεστές της γραμμικής εξίσωσης, που περιλαμβάνει μία ή περισσότερες ανεξάρτητες μεταβλητές που προβλέπουν καλύτερα την τιμή της εξαρτημένης μεταβλητής. Η γραμμική παλινδρόμηση ταιριάζει σε μια ευθεία γραμμή ή επιφάνεια που ελαχιστοποιεί τις αποκλίσεις μεταξύ των προβλεπόμενων και των πραγματικών τιμών εξόδου. Υπάρχουν απλές αριθμομηχανές γραμμικής παλινδρόμησης που χρησιμοποιούν μια μέθοδο «ελάχιστων τετραγώνων» για να ανακαλύψουν την καλύτερη γραμμή για ένα σύνολο ζευγαρωμένων δεδομένων. Στη συνέχεια, γίνεται ο υπολογισμός της τιμής του X (εξαρτώμενη μεταβλητή) από την Y (ανεξάρτητη μεταβλητή). [23]

3.7 Multilayer Perceptron

Το Multilayer Perceptron είναι ένα νευρωνικό δίκτυο που μαθαίνει τη σχέση μεταξύ γραμμικών και μη γραμμικών δεδομένων. Οι αλγόριθμοι Βαθιάς Μάθησης - Deep Learning χρησιμοποιούν τα τεχνητά νευρωνικά δίκτυα ως κύρια δομή τους. Αυτό που τους διαφοροποιεί από άλλους αλγόριθμους είναι ότι δεν απαιτούν τη συμβολή των ειδικών κατά τη φάση σχεδιασμού χαρακτηριστικών και μηχανικής. Τα νευρωνικά δίκτυα μπορούν να μάθουν τα χαρακτηριστικά των δεδομένων.

Οι αλγόριθμοι Deep Learning λαμβάνουν το σύνολο δεδομένων και μαθαίνουν τα μοτίβα του, μαθαίνουν πώς να αντιπροσωπεύουν τα δεδομένα με χαρακτηριστικά που εξάγουν μόνοι τους. Στη συνέχεια συνδυάζουν διαφορετικές αναπαραστάσεις του συνόλου δεδομένων, καθεμία από τις οποίες προσδιορίζει ένα συγκεκριμένο μοτίβο ή χαρακτηριστικό, σε μια πιο αφηρημένη, υψηλού επιπέδου αναπαράσταση του συνόλου δεδομένων. Αυτή η προσέγγιση hands-off, χωρίς μεγάλη ανθρώπινη παρέμβαση στον σχεδιασμό και την εξαγωγή χαρακτηριστικών, επιτρέπει στους αλγόριθμους να προσαρμόζονται πολύ πιο γρήγορα στα διαθέσιμα δεδομένα.

Τα νευρωνικά δίκτυα εμπνέονται από τη δομή του εγκεφάλου, αλλά όχι απαραίτητα ένα ακριβές μοντέλο. Υπάρχουν πολλά που δεν γνωρίζουμε ακόμη για τον εγκέφαλο και τον τρόπο λειτουργίας του, αλλά έχει χρησιμεύσει ως έμπνευση σε πολλούς επιστημονικούς τομείς λόγω της ικανότητάς του να αναπτύσσει νοημοσύνη. Και παρόλο που υπάρχουν νευρωνικά δίκτυα που δημιουργήθηκαν με μοναδικό σκοπό την

κατανόηση του τρόπου λειτουργίας του εγκεφάλου, το Deep Learning όπως το ξέρουμε σήμερα δεν έχει σκοπό να αναπαράγει τον τρόπο λειτουργίας του εγκεφάλου. Αντίθετα, το Deep Learning εστιάζει στην ενεργοποίηση συστημάτων που μαθαίνουν πολλαπλά επίπεδα σύνθεσης προτύπων. [24]

3.8 Bagging

Το Bagging, γνωστό και ως bootstrap aggregation, είναι η μέθοδος εκμάθησης συνόλου που χρησιμοποιείται συνήθως για τη μείωση της διακύμανσης μέσα σε ένα θορυβώδες σύνολο δεδομένων. Στο bagging, ένα τυχαίο δείγμα δεδομένων σε ένα σετ εκπαίδευσης επιλέγεται με αντικατάσταση—που σημαίνει ότι τα μεμονωμένα σημεία δεδομένων μπορούν να επιλεγούν περισσότερες από μία φορές. Αφού δημιουργηθούν πολλά δείγματα δεδομένων, αυτά τα αδύναμα μοντέλα στη συνέχεια εκπαιδεύονται ανεξάρτητα και ανάλογα με τον τύπο της εργασίας - παλινδρόμηση ή ταξινόμηση, για παράδειγμα - ο μέσος όρος ή η πλειονότητα αυτών των προβλέψεων δίνουν μια πιο ακριβή εκτίμηση.

Σημείωση, ο αλγόριθμος του Random Forest που ακολουθεί, θεωρείται επέκταση της μεθόδου bagging, χρησιμοποιώντας τόσο το bagging όσο και την τυχειότητα χαρακτηριστικών για τη δημιουργία ενός μη συσχετισμένου δάσους δέντρων απόφασης. [25]

Το Random Forest είναι ένας ευρέως χρησιμοποιούμενος αλγόριθμος μηχανικής μάθησης με εμπορικό σήμα από τους Leo Breiman και Adele Cutler, ο οποίος συνδυάζει την έξοδο πολλαπλών δέντρων αποφάσεων για να φτάσει σε ένα μόνο αποτέλεσμα. Η ευκολία χρήσης και η ευελιξία του έχουν τροφοδοτήσει την υιοθέτησή του, καθώς αντιμετωπίζει προβλήματα ταξινόμησης και παλινδρόμησης.

3.9 Δέντρα απόφασης

Δεδομένου ότι το μοντέλο Random Forest αποτελείται από πολλαπλά δέντρα αποφάσεων, θα ήταν χρήσιμο να ξεκινήσουμε περιγράφοντας εν συντομία τον αλγόριθμο του δέντρου αποφάσεων. Τα δέντρα απόφασης ξεκινούν με μια βασική ερώτηση, όπως «Πρέπει να σερφάρω;» Από εκεί, μπορείτε να κάνετε μια σειρά από ερωτήσεις για να προσδιορίσετε μια απάντηση, όπως, "Είναι μια μεγάλη περίοδος πρήξιμο;" ή «Είναι ο άνεμος που φυσά στη θάλασσα;». Αυτές οι ερωτήσεις αποτελούν τους κόμβους απόφασης στο δέντρο, λειτουργώντας ως μέσο για τον διαχωρισμό των δεδομένων. Κάθε ερώτηση βοηθά ένα άτομο να καταλήξει σε μια τελική απόφαση, η

οποία θα συμβολίζεται με τον κόμβο φύλλου. Οι παρατηρήσεις που πληρούν τα κριτήρια θα ακολουθήσουν τον κλάδο «Ναι» και όσες δεν πληρούν την εναλλακτική διαδρομή. Τα δέντρα αποφάσεων αναζητούν την εύρεση του καλύτερου διαχωρισμού για υποσύνολο των δεδομένων και συνήθως εκπαιδεύονται μέσω του αλγορίθμου Classification and Regression Tree (CART). Οι μετρήσεις, όπως ο δείκτης Gini που μετρά την ακαθαρσία (impurity) ενός κόμβου, το κέρδος πληροφοριών ή το μέσο τετραγωνικό σφάλμα (MSE), μπορούν να χρησιμοποιηθούν για την αξιολόγηση της ποιότητας του διαχωρισμού. [26]

3.10 Μηχανική Μάθηση - RL

Έγιναν δύο διαφορετικά πειράματα. Το πρώτο πείραμα έγινε στο Colab, στο ανοιχτό περιβάλλον AI Gym Anytrading, που είναι ένα προσαρμοσμένο περιβάλλον συναλλαγών που μπορεί να χρησιμοποιηθεί για την διαπραγμάτευση μετοχών, forex (foreign exchange ή FX), κρυπτονομισμάτων και τίτλων. Χρησιμοποιήθηκαν ιστορικά δεδομένα διακύμανσης της τιμής του bitcoin από το MarketWatch. Συγκεκριμένα συλλέχθηκαν και μελετήθηκαν δεδομένα από τις 20.5.2021 μέχρι 14.6.2022.

Μια αναζήτηση στο Διαδίκτυο για αλγόριθμους συναλλαγών, δείχνει ότι η χρήση πολλών ενεργειών όπως Αγορά, Πώληση, Αναμονή, Εισαγωγή, Έξοδος κ.λπ. Ένας τυπικός πράκτορας RL μπορεί να λύσει μόνο ένα μέρος του κύριου προβλήματος σε αυτόν τον τομέα. Εάν κάποιος εργάζεται σε αγορές συναλλαγών θα μάθει ότι η απόφαση για το αν θα κρατήσει, θα εισαγάγει ή θα εξέλθει από ένα ζεύγος (σε FOREX) ή απόθεμα (σε Μετοχές) είναι μια στατιστική απόφαση που εξαρτάται από πολλές παραμέτρους όπως ο προϋπολογισμός, τα ζεύγη ή οι μετοχές σας, εμπόριο, την πολιτική διανομής χρημάτων σας σε πολλές αγορές, κ.λπ. Είναι τεράστιο βάρος για έναν πράκτορα RL να εξετάσει όλες αυτές τις παραμέτρους και μπορεί να χρειαστούν χρόνια για να αναπτύξει έναν τέτοιο πράκτορα! Σε αυτήν την περίπτωση, κάποιος σίγουρα δεν θα χρησιμοποιήσει αυτό το περιβάλλον αλλά θα επεκτείνει το δικό του/της.

Αυτές οι ενέργειες απλώς κάνουν τα πράγματα περίπλοκα χωρίς πραγματικό θετικό αντίκτυπο. Στην πραγματικότητα, απλώς αυξάνουν τον χρόνο εκμάθησης και μια ενέργεια όπως το Hold μετά βίας θα χρησιμοποιηθεί από έναν καλά εκπαιδευμένο πράκτορα επειδή δεν θέλει να χάσει ούτε μια δεκάρα. Επομένως, δεν χρειάζεται να

υπάρχουν τόσες πολλές ενέργειες και μόνο οι ενέργειες $Sell=0$ και $Buy=1$ είναι επαρκείς για την εκπαίδευση ενός πράκτορα εξίσου καλά.

Τώρα σχετικά με τις θέσεις διαπραγμάτευσης και τι σημαίνουν: Η Long σημαίνει πως κάποιος θέλει να αγοράσει μετοχές όταν οι τιμές είναι χαμηλές και να κερδίζει μένοντας μαζί τους ενώ η αξία τους αυξάνεται και η Short σημαίνει πως κάποιος θέλει να πουλήσει μετοχές με υψηλή αξία και να χρησιμοποιήσει αυτήν την αξία για να αγοράσει μετοχές σε χαμηλότερη αξία, διατηρώντας τη διαφορά ως κέρδος.

Το ανοιχτό περιβάλλον AI Gym Anytrading που χρησιμοποιείται είναι ένα προσαρμοσμένο περιβάλλον συναλλαγών που μπορεί να χρησιμοποιηθεί για την διαπραγμάτευση μετοχών, forex (foreign exchange, FX η αγορά συναλλάγματος), κρυπτονομίσματα, μετοχές και τίτλους.

Στη συνέχεια, ο αλγόριθμος RL που χρησιμοποιήθηκε ήταν ο A2C. Οι εναλλακτικοί αλγόριθμοι RL είναι οι DQN και PPO2.

Ο A2C είναι μια μέθοδος Ενισχυτικής Μάθησης, την οποία μπορούμε να ονομάσουμε «υβριδική μέθοδο»: Actor-Critic (Ηθοποιός-Κριτικός). Ο αλγόριθμος Actor-Critic είναι μία μέθοδος Ενίσχυσης Μάθησης που συνδυάζει προσεγγίσεις βελτιστοποίησης αξίας και βελτιστοποίησης πολιτικής. Πιο συγκεκριμένα, το Actor-Critic συνδυάζει τους αλγόριθμους Q-learning και Policy Gradient (PG). Ο αλγόριθμος που προκύπτει και λαμβάνεται σε υψηλό επίπεδο μοιράζεται χαρακτηριστικά όπως:

Actor: ένας αλγόριθμος PG που αποφασίζει για μια ενέργεια που πρέπει να γίνει. Στους PG αλγόριθμους η αρχή είναι απλή: Παρατηρούμε και ενεργούμε.

Critic: Αλγόριθμος Q-learning που κριτικάρει τη δράση που επέλεξε ο ηθοποιός, παρέχοντας ανατροφοδότηση σχετικά με τον τρόπο προσαρμογής. Μπορεί να επωφεληθεί από κόλπα αποτελεσματικότητας στην Q-learning, όπως η επανάληψη της μνήμης. Η O-learning (Watkins, 1989) είναι μια μορφή ενισχυτικής μάθησης χωρίς μοντέλα. Μπορεί επίσης να θεωρηθεί ως μέθοδος ασύγχρονου δυναμικού προγραμματισμού (DP). Παρέχει στους πράκτορες τη δυνατότητα να μάθουν να ενεργούν βέλτιστα σε μαρκοβιανούς τομείς βιώνοντας τις συνέπειες των ενεργειών, χωρίς να τους απαιτείται να δημιουργήσουν χάρτες των τομέων. [27], [28], [29]

Επίσης χρησιμοποιήθηκαν, ως κύριες βιβλιοθήκες επεξεργασίας οι παρακάτω:

1) Το Pandas χρησιμοποιείται για ανάγνωση των δεδομένων συναλλαγών μας.

2) Το Numpy χρησιμοποιείται στη φάση αξιολόγησης του φροντιστηρίου για την εκτέλεση μαθηματικών.

3) Το matplotlib μας βοηθά να οπτικοποιήσουμε τις συναλλαγές μας.

4) Το OS που χρησιμοποιείται για την εκτέλεση εργασιών λειτουργικού συστήματος

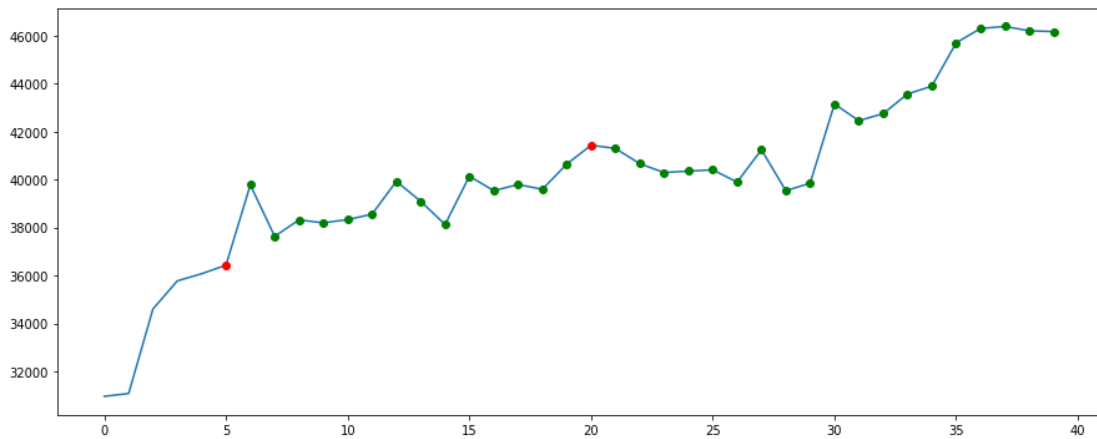
5) Το Google Colab για την προσάρτηση στο περιβάλλον Google Colab του προσωπικού χώρου στο Google drive για πρόσβαση στο σύνολο δεδομένων.

Αφού έγινε προεπεξεργασία για προετοιμασία των δεδομένων ώστε να εισαχθούν στο περιβάλλον Gym Anytrading.

Χρησιμοποιήθηκε η πολιτική MlpLstm, η οποία είναι μια πολιτική ενός βαθύ νευρωνικού δικτύου με επίπεδο LSTM. Είναι μια σημαντική πολιτική, καθώς επιτρέπει σε ένα νευρωνικό δίκτυο να διατηρεί το πλαίσιο και να μαθαίνει για την προηγούμενη ιστορία στους νευρώνες του. Η τελευταία γραμμή κώδικα ξεκινά την εκπαίδευση με 1000000 χρονικά βήματα. Στην ιδανική περίπτωση, αυτό που χρειάζεται να παρατηρηθεί κατά την εκπαίδευση είναι η τιμή της διακύμανσης `explained_variance`. Θέλουμε να είναι όσο πιο ψηλά γίνεται. Εξετάζουμε τιμές μεταξύ 0 και 1. Ένας αριθμός κοντά στο 1 δηλώνει μια υψηλή τιμή ενώ αυτός κοντά στο 0, μια χαμηλή τιμή. Θα πρέπει επίσης να βεβαιωθείτε ότι το `value_loss` είναι όσο το δυνατόν χαμηλότερο. Η εκπαίδευση του μοντέλου μπορεί να διακοπεί όταν η `explained_variance` είναι 0,966. Αυτό δίνει ένα μοντέλο που αποδίδει αρκετά καλά.

Μετά την εκπαίδευση ακολουθεί ο έλεγχος, με κώδικα που είναι παρόμοιος με τη βασική διαφορά ότι, αντί να επιλέγονται τυχαίες ενέργειες, χρησιμοποιείται το μοντέλο μας για να προβλεφθεί ποια ενέργεια πρέπει να λάβει, δηλαδή να αγοράσει ή να πουλήσει.

Total Reward: 1655.000000 ~ Total Profit: 1.129994



Εικόνα 4 Οι αγοραπωλησίες του RL αλγορίθμου

Αυτά είναι τα αποτελέσματα από την εκπαίδευση του πράκτορα μας από την 15η έως την 50η ημέρα. Το μοντέλο μας έχει προβλέψει νέες ενέργειες. Μπορούμε να σημειώσουμε ότι έχει κάνει μερικές καλές συναλλαγές όπως και κακές. Οι πράσινες κουκκίδες αντιπροσωπεύουν την αγορά ενώ οι κόκκινες κουκκίδες αντιπροσωπεύουν την πώληση κρυπτονομισμάτων.

Για παράδειγμα, στην έκτη συναλλαγή του, ήταν ένα τοπικό υψηλό που θα μπορούσε να είχε πουλήσει και να αγοράσει μετά σε χαμηλότερη τιμή. [30]

3.11 Μηχανική Μάθηση – WEKA [31]

Το δεύτερο πείραμα έγινε με τη χρήση του Waika to Environment for Knowledge Analysis (Weka), που είναι μια δημοφιλής σουίτα λογισμικού μηχανικής μάθησης γραμμένο σε Java, που αναπτύχθηκε στο Πανεπιστήμιο του Waikato της Νέα Ζηλανδίας. Είναι ελεύθερο λογισμικό υπό την άδεια GNU General Public License. Αποτελεί ένα εργαλείο χρήσιμο τόσο για πειράματα, όσο και για ενσωμάτωση μηχανισμών μηχανικής μάθησης σε καθημερινές εφαρμογές.

Περιέχει μια συλλογή από εργαλεία για την προεπεξεργασία δεδομένων (Preprocessing Filters), την ταξινόμηση/παλινδρόμηση (Classification/Regression), την συσταδοποίηση (Clustering), τους κανόνες συσχέτισης (Association discovery rules) και την οπτικοποίηση (Visualization) καθώς και αλγορίθμους για την ανάλυση δεδομένων και την προγνωστική μοντελοποίηση, μαζί με γραφικές διεπαφές χρήστη για εύκολη πρόσβαση σε αυτές τις λειτουργίες.

3.12 Πρόβλεψη Χρονοσειρών μέσω Weka

Η ανάλυση χρονοσειρών με το Weka γίνεται με τη χρήση του time series package, το οποίο παρέχει ένα περιβάλλον πρόβλεψης χρονοσειρών για το Weka. Αυτοματοποιεί τη διαδικασία δημιουργίας μεταβλητών με καθυστέρηση και περιοδικών μεταβλητών που προέρχονται από ημερομηνία και παρέχει τη δυνατότητα πρόβλεψης (*prediction, forecasting*) για μελλοντικά γεγονότα με βάση γνωστά παρελθόντα γεγονότα. Είναι η διαδικασία χρήσης στατιστικών τεχνικών για τον υπολογισμό και την εξήγηση μιας χρονικά εξαρτώμενης σειράς δεδομένων. Τα δεδομένα χρονοσειρών έχουν μια φυσική χρονική ακολουθία, αυτό διαφέρει από τις συνήθεις εφαρμογές εξόρυξης δεδομένων/μηχανικής μάθησης όπου κάθε δεδομένο είναι ένα ανεξάρτητο παράδειγμα της έννοιας την οποία πρέπει να μάθει και η ακολουθία δεδομένων μέσα σε ένα σύνολο δεδομένων δεν έχει σημασία.

Στο περιβάλλον του Weka (από την έκδοση $\geq 3.7.3$ και μετά) υπάρχει ένα ειδικό περιβάλλον ανάλυσης χρονοσειρών που επιτρέπει την ανάπτυξη, την αξιολόγηση και την απεικόνιση μοντέλων πρόβλεψης. Είναι ένα πρόσθετο (plugin) στο γραφικό περιβάλλον "Explorer" της Weka και μπορεί να εγκατασταθεί μέσω του διαχειριστή πακέτων. Το πλαίσιο χρονοσειρών της Weka υιοθετεί μια προσέγγιση εκμάθησης μηχανών/εξόρυξης δεδομένων για τη μοντελοποίηση χρονολογικών σειρών μετασχηματίζοντας τα δεδομένα σε μια μορφή που μπορούν να επεξεργαστούν οι τυποποιημένοι αλγόριθμοι προτεινόμενης εκμάθησης. Διάφορα άλλα πεδία υπολογίζονται επίσης αυτόματα για να επιτρέπουν στους αλγόριθμους να διαμορφώνουν τις τάσεις και την εποχικότητα. Αφού μετασχηματιστούν τα δεδομένα, οποιοσδήποτε αλγόριθμος παλινδρόμησης της Weka μπορεί να εφαρμοστεί για να μάθει ένα μοντέλο.

3.13 Ο σχεδιασμός των πειραμάτων

Για τα καλύτερα δυνατά αποτελέσματα δοκιμάστηκαν όλα τα διαθέσιμα μοντέλα που υποστηρίζει το Weka για πρόβλεψη της τιμής (πρόβλεψη χρονοσειρών - timeseries forecasting). Αρχικά έγινε μελέτη των αποτελεσμάτων πρόβλεψης. Γνωρίζουμε πως υπάρχει αβεβαιότητα στη διαδικασία της πρόβλεψης ή της εκτίμησης λόγω πλήθους τυχαίων μεταβλητών. Στη συνέχεια κάποιος που θέλει να επενδύσει σε Bitcoin, λαμβάνει την απόφασή του με βάση τον κίνδυνο που είναι διατεθειμένος να αναλάβει για να πάρει το αποτέλεσμα που θέλει ή χρειάζεται.

Στα πειράματα, χρησιμοποιήθηκαν οι παρακάτω τύποι:

$$\text{Percentage Error} = \frac{(\text{Actual} - \text{Forecast})}{\text{Actual}} \times 100$$

Δηλαδή η Ακρίβεια πρόβλεψης ισούται με:

$$\text{Forecast Accuracy (\%)} = (\text{Actual Value} - \text{Forecast Value}) \div (\text{Actual Value}) \times 100$$

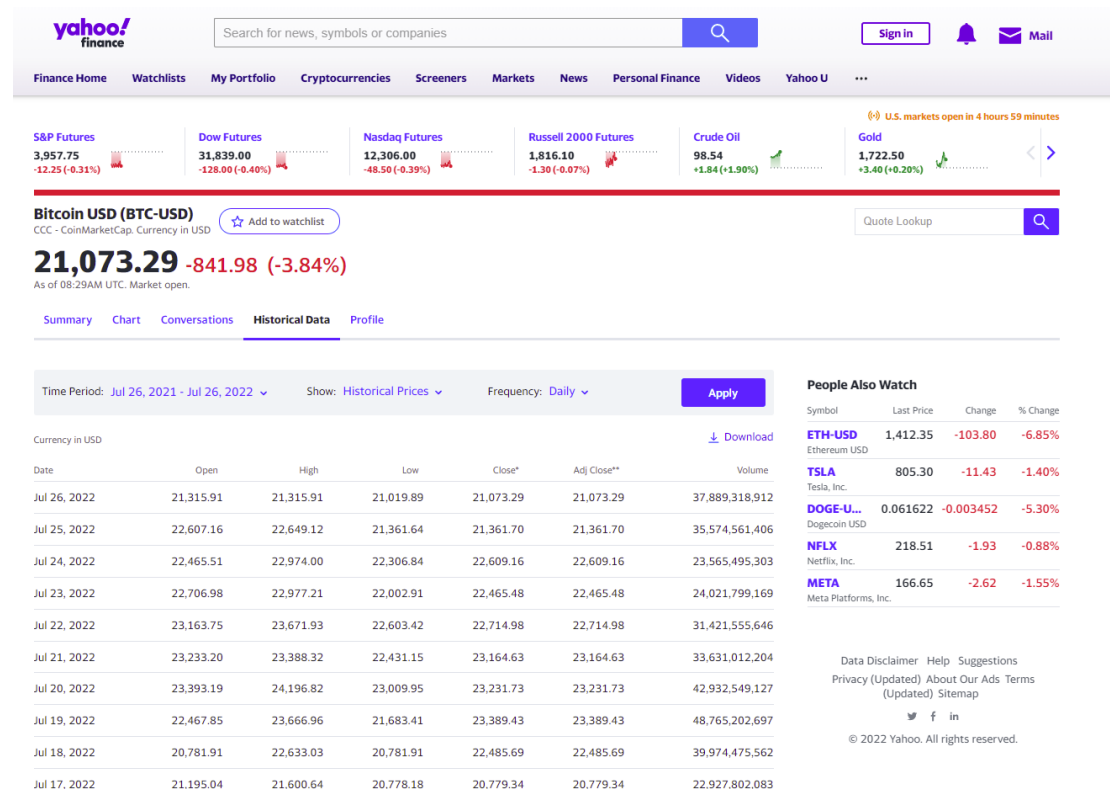
(όπου Actual Value η πραγματική τιμή και Forecast Value η τιμή της πρόβλεψης).

3.14 Τα δεδομένα των πειραμάτων

Δεδομένα για το bitcoin υπάρχουν διαθέσιμα σε ελεύθερη μορφή σε διάφορες σελίδες.

Τα δεδομένα των πειραμάτων κατέβηκαν σε csv μορφή από την σελίδα

<https://finance.yahoo.com/quote/BTC-USD/history?p=BTC-USD>



Εικόνα 5 Πληροφορίες για το Bitcoin από το yahoo, στις 26 Ιουλίου 2022

Τα δεδομένα που χρησιμοποιήθηκαν κατέβηκαν στις 21.5.2022 και ήταν δεδομένα ενός χρόνου από τις 20.5.2021 μέχρι τις 20.5.2022. Το αρχείο csv περιέχει 5 στήλες με τα εξής δεδομένα: ημερομηνία, τιμή ανοίγματος, υψηλότερη τιμή της ημέρας, χαμηλότερη τιμή της ημέρας και τιμή κλεισίματος.

BTCUSD.csv - LibreOffice Calc

Αρχείο Επεξεργασία Προβολή Εισαγωγή Μορφή Τεχνοτροπίες Φύλλο Δεδομένα Εργαλεία Παρά

Liberation Sans 10 στ B I U A

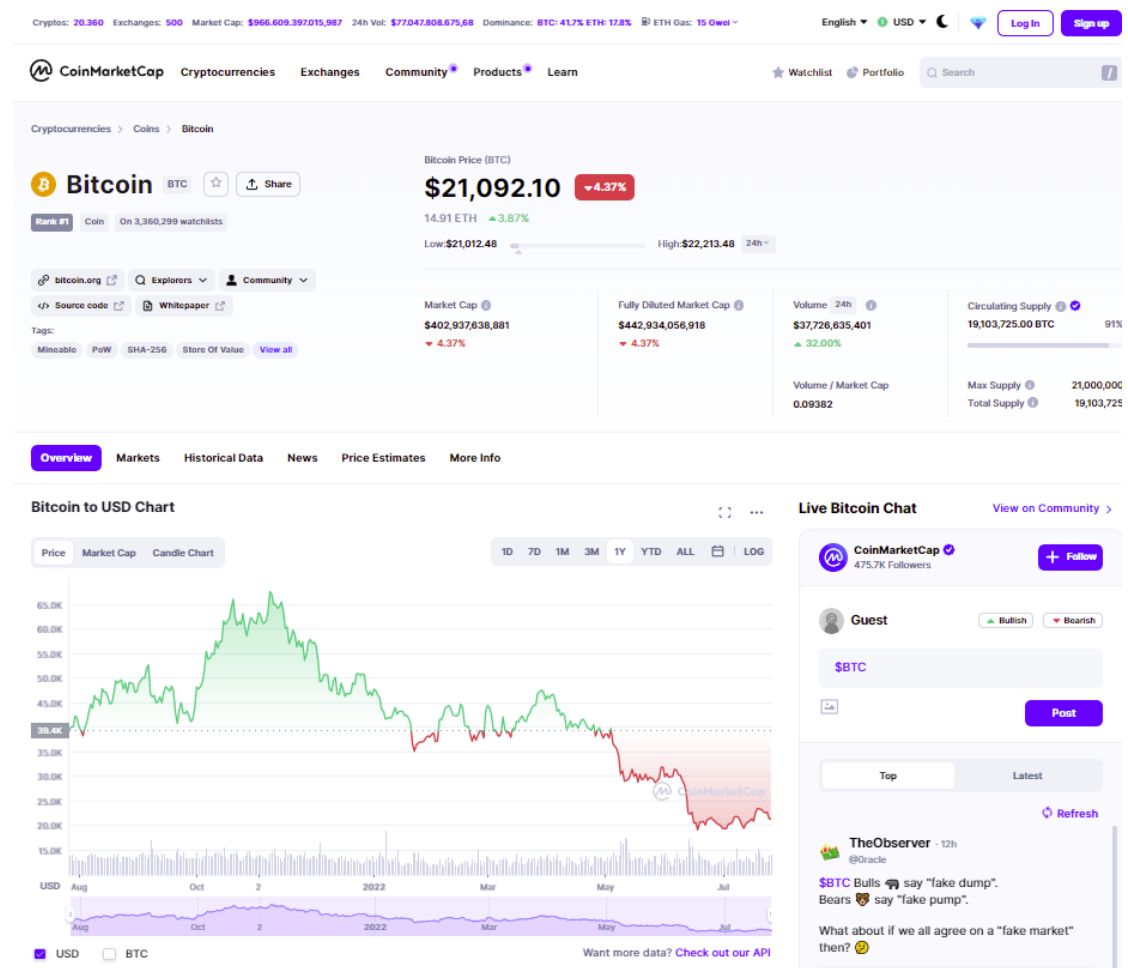
H32 fx Σ =

	A	B	C	D	E	F	G
1	Date	Open	High	Low	Close		
2	05/20/2022	30214	30700	28714	29121		
3	05/19/2022	29205	30483	28637	30214		
4	05/18/2022	30081	30664	28749	29205		
5	05/17/2022	29880	30721	29465	30081		
6	05/16/2022	30991	31346	29179	29880		
7	05/15/2022	29370	31061	29345	30991		
8	05/14/2022	29800	30079	28661	29370		
9	05/13/2022	28572	30994	27968	29800		
10	05/12/2022	28315	30079	25805	28572		
11	05/11/2022	30960	32075	28233	28315		
12	05/10/2022	31076	32624	29842	30960		
13	05/09/2022	34604	34604	30416	31076		
14	05/08/2022	35775	35816	33766	34604		
15	05/07/2022	36074	36140	35749	35775		
16	05/06/2022	36432	36648	35387	36074		
17	05/05/2022	39780	39860	35690	36432		
18	05/04/2022	37633	39890	37633	39780		
19	05/03/2022	38321	38854	37543	37633		
20	05/02/2022	38196	39108	38102	38321		
21	05/01/2022	38332	38660	37510	38196		
22	04/30/2022	38559	38776	38201	38332		
23	04/29/2022	39928	39989	38213	38559		
24	04/28/2022	39095	40338	38877	39928		
25	04/27/2022	38128	39451	37746	39095		
26	04/26/2022	40140	40748	37757	38128		
27	04/25/2022	39539	40316	38292	40140		
28	04/24/2022	39794	39937	39046	39539		
29	04/23/2022	39597	39974	39331	39794		
30	04/22/2022	40647	40842	39214	39597		
31	04/21/2022	41435	42949	40647	40647		
32	04/20/2022	41300	42202	40935	41435		
33	04/19/2022	40665	41750	40609	41300		
34	04/18/2022	40295	40911	38639	40665		
35	04/17/2022	40356	40712	39927	40295		

BTUSD

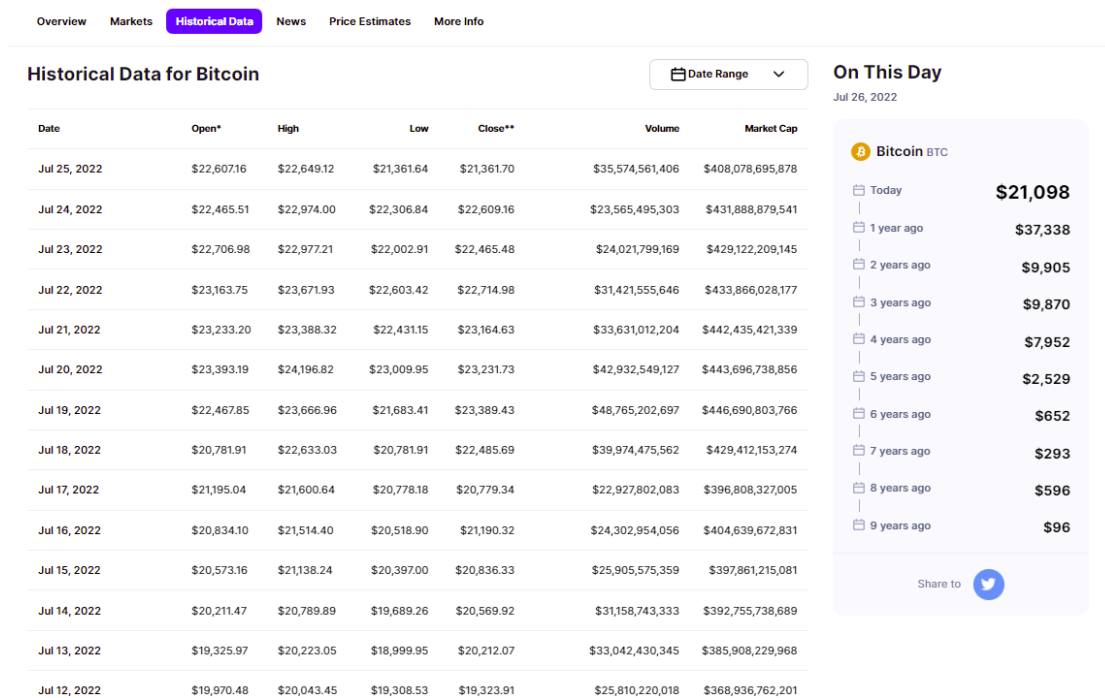
Εικόνα 6 Δεδομένα για το Bitcoin του csv αρχείου που χρησιμοποιήθηκαν στα πειράματα

Στην σελίδα <https://coinmarketcap.com/currencies/bitcoin/> επίσης υπάρχουν δεδομένα που μπορεί κανείς να διαβάσει και να χρησιμοποιήσει.



Εικόνα 7 Γράφημα που δείχνει την ετήσια πορεία του Bitcoin, στις 26 Ιουλίου 2022

Τα ιστορικά δεδομένα περιέχουν 7 στήλες: τις 5 που υπάρχουν και στη σελίδα του yahoo και επιπρόσθετα ο ημερήσιος όγκος συναλλαγών και η συνολική κεφαλαιοποίηση του bitcoin. Δοκιμάστηκαν στα πειράματα και αυτά τα δεδομένα και αποδείχθηκε πως οι 2 επιπρόσθετες στήλες δεν δίνουν καλύτερα αποτελέσματα. Έτσι χρησιμοποιήθηκαν τα δεδομένα με τις 5 στήλες από το yahoo.



Εικόνα 8 Ιστορικά δεδομένα του Bitcoin μέσα από τη σελίδα coinmarketcap.com

Με βάση την πορεία της τιμής του bitcoin επιλέχθηκαν συγκεκριμένες ημερομηνίες για να εξεταστεί η εγκυρότητα της πρόβλεψης της τιμής του. Τα δεδομένα των δοκιμών για κάθε σενάριο ήταν από τις 20.5.2021 (η πρώτη μέρα των δεδομένων μας στο αρχείο που κατέβηκε) μέχρι την ημέρα που επιλέχθηκε για το κάθε σενάριο. Για παράδειγμα για το πρώτο σενάριο που ήταν στις 21.5.2022 το μοντέλο εκπαίδευσης δέχθηκε δεδομένα μέχρι τις 20.5.2022 ενώ για το δεύτερο που ήταν στις 28.2.2022 τα δεδομένα ελέγχου ήταν από τις 20.5.2021 μέχρι τις 27.2.2022.

Συνεπώς, μια που το τρέχουμε με δεδομένα του πρόσφατου παρελθόντος, ο έλεγχος της εκτίμησης του μοντέλου γίνεται με την τιμή που γνωρίζουμε πως είχε το BTC εκείνη την ημέρα.

3.15 Τα πειράματα

Τα σενάρια δοκιμών επιλέχθηκαν με βάση τη συμπεριφορά της τιμής του bitcoin πριν από την ημέρα που επιλέχθηκε και της τιμής που είχε τελικά για να διαπιστωθεί η ακρίβεια της πρόβλεψης.

Στις 21.5.2022 η τιμή μετά από συνεχόμενη καθοδική πορεία για 10 μέρες παρέμεινε σταθερή όπως και παρέμεινε τελικά και στις 21.5. Τρέχοντας τα πειράματα παρήχθησαν τα παρακάτω αποτελέσματα για την τιμή ανοίγματος (open), την υψηλότερη τιμή (high), τη χαμηλότερη τιμή (low) και την τιμή κλεισίματος (close):

SMOreg			
Open	High	Low	Close
0,158845	-1,71776	0,544418	0,131643

LinearRegression			
Open	High	Low	Close
-1,860816	-2,163379	-1,17195	-0,6761873

MultilayerPerceptron			
Open	High	Low	Close
-0,59891	1,145769	2,723948	3,718444

bagging			
Open	High	Low	Close
-1,40924	-4,57625	0,834195	-1,41029

RandomForest			
Open	High	Low	Close
1,715889	3,937749	-0,65983	1,355891

Το Μέσο Ποσοστό σφάλματος των Προβλέψεων από τα 5 μοντέλα

Open	High	Low	Close
-1,085201	-2,24987483	0,718089	0,08154353

Τα αποτελέσματα ήταν εξαιρετικά.

Επικεντρωθήκαμε στη τιμή κλεισίματος και μετά το πρώτο πείραμα δοκιμάσαμε και σε διαφορετικές συνθήκες της πορείας της τιμής για να παρατηρήσουμε την ακρίβεια της πρόβλεψης.

Στο 2^ο πείραμα επιλέχθηκε η 28.02.2021 που είχε ανοδική πορεία της προηγούμενες μέρες από τις 37700 στις 43000 και την επόμενη μέρα ξανανέβηκε.

SMOreg			
Open	High	Low	Close
-0,16401	2,633598	0,829907281	3,435236385

LinearRegression			
Open	High	Low	Close
1,3251568	4,409309129	2,142014312	2,39679298

MultilayerPerceptron			
Open	High	Low	Close
-0,74146	1,946910346	-1,7550111	-2,45615377

bagging			
Open	High	Low	Close
-0,27518	1,785639768	3,70687562	3,314269325

RandomForest			
Open	High	Low	Close
-6,22079	-6,45598	-7,361567805	-7,803971073

Το Μέσο Ποσοστό σφάλματος των Προβλέψεων από τα 5 μοντέλα

Open	High	Low	Close
1,273057	3,446286811	2,457070779	2,8988232

Το μέσο σφάλμα βρέθηκε κοντά στο 3%.

Στο 3^ο πείραμα πρόβλεψης, επιλέχθηκε η ημερομηνία 4/12/2021 όπου τις προηγούμενες μέρες η τιμή ήταν σταθερή αλλά μια μέρα πριν έπεσε. Είχε ενδιαφέρον να βρεθεί πως θα κινηθεί η τιμή του Bitcoin.

SMOreg			
Open	High	Low	Close
-0,18144	-2,50989	-22,85291311	-10,58583423

LinearRegression			
Open	High	Low	Close
-5,325609	-2,59868572	-26,6125677	-9,7843658

MultilayerPerceptron			
Open	High	Low	Close
0,614696	-2,058753189	-23,288703	-9,24056728

bagging			
Open	High	Low	Close
-3,06902	-6,507790849	-27,522286	-14,12611616

RandomForest			
Open	High	Low	Close
5,300924	7,795584	27,61645908	12,97967015

Το Μέσο Ποσοστό σφάλματος των Προβλέψεων από τα 5 μοντέλα

Open	High	Low	Close
-2,652459	-4,29413996	-25,5785858	-11,343311

Η πρόβλεψη ήταν πολύ κακή.

Η επόμενη ημερομηνία που επιλέχθηκε ήταν η 11/5/2022, όπου τις προηγούμενες μέρες έπεφτε αλλά μια μέρα πριν η πτώση σταμάτησε.

SMOreg			
Open	High	Low	Close
0,051459	-0,14005	-8,300067694	-9,369682488

LinearRegression			
Open	High	Low	Close
-1,684862	2,733172921	-7,41165796	-5,1678942

MultilayerPerceptron			
Open	High	Low	Close
-3,36394	-8,005344226	-10,844909	-16,7651926

bagging			
Open	High	Low	Close
0,775675	-2,382674131	-7,7127955	-10,17606842

RandomForest			
Open	High	Low	Close
2,674574	5,329099	11,3978042	10,42715118

Το Μέσο Ποσοστό σφάλματος των Προβλέψεων από τα 5 μοντέλα

Open	High	Low	Close
-1,379248	-2,6247981	-9,13344685	-10,381198

Όπως και στο προηγούμενο πείραμα η πρόβλεψη ήταν κακή.

Το 5^ο πείραμα ήταν για τις 15/10/2021 όπου σταδιακά η τιμή ανέβηκε το διάστημα που προηγήθηκε στη συνέχεια τις προηγούμενες τρεις ημέρες ήταν σταθερή. Έχει ενδιαφέρον να δούμε την πρόβλεψη.

SMOreg			
Open	High	Low	Close
0,163257	6,694279	1,198486845	6,901105341

LinearRegression			
Open	High	Low	Close
0,1742078	7,10985299	2,212904151	6,18653986

MultilayerPerceptron			
Open	High	Low	Close
0,781908	9,179134078	2,84800646	7,000794678

bagging			
Open	High	Low	Close
2,835659	9,05113619	4,55321297	9,284793217

RandomForest			
Open	High	Low	Close
-1,1183	-7,53097	-1,896068774	-7,596766368

Το Μέσο Ποσοστό σφάλματος των Προβλέψεων από τα 5 μοντέλα

Open	High	Low	Close
1,0146672	7,913074375	2,54173584	7,39399989

Η πρόβλεψη ήταν 7,4% λανθασμένη.

Το τελευταίο πείραμα επιλέχθηκε για τις 28/7/2021 με την τιμή να έχει ανεβεί τις προηγούμενες μέρες. Στις επόμενες μέρες θα είναι σταθερή. Γι' αυτό επιλέχθηκε για να φανεί εάν αυτό μπορεί να προβλεφθεί από τα μοντέλα πρόβλεψης.

SMOreg			
Open	High	Low	Close
0,293136	-0,57958	3,448807862	-2,188477352

LinearRegression			
Open	High	Low	Close
-0,978792	0,601952641	0,499355966	-0,8215842

MultilayerPerceptron			
Open	High	Low	Close
0,935441	2,94446992	5,28153387	3,539148585

bagging			
Open	High	Low	Close
0,957917	7,735319664	5,41574882	8,505809391

RandomForest			
Open	High	Low	Close
-6,73097	-6,8106	-9,14107279	-6,834868381

Το Μέσο Ποσοστό σφάλματος των Προβλέψεων από τα 5 μοντέλα

Open	High	Low	Close
1,5877346	3,502552554	4,757303862	3,17395296

Κοντά στο 3% το σφάλμα αυτή τη φορά της πρόβλεψης.

Επειδή τα αποτελέσματα έχουν διακυμάνσεις στις προβλέψεις που παρήχθησαν δοκιμάστηκε και μία άλλη τεχνική γνωστή ως Monte Carlo. Η προσομοίωση Monte Carlo, γνωστή και ως μέθοδος Monte Carlo ή προσομοίωση πολλαπλών πιθανοτήτων, είναι μια μαθηματική τεχνική, η οποία χρησιμοποιείται για την εκτίμηση των πιθανών αποτελεσμάτων ενός αβέβαιου γεγονότος. Η μέθοδος του Μόντε Κάρλο επινοήθηκε από τους John von Neumann και Stanislaw Ulam κατά τη διάρκεια του Β' Παγκοσμίου Πολέμου για να βελτιώσει τη λήψη αποφάσεων κάτω από αβέβαιες συνθήκες. Συγκεκριμένα, χρησιμοποιείται για τη μοντελοποίηση της πιθανότητας διαφορετικών αποτελεσμάτων σε μια διαδικασία που δεν μπορεί εύκολα να προβλεφθεί λόγω της παρέμβασης τυχαίων μεταβλητών. Είναι μια τεχνική που χρησιμοποιείται για την κατανόηση της επίδρασης του κινδύνου και της αβεβαιότητας στα μοντέλα πρόβλεψης. Πήρε το όνομά της από μια γνωστή πόλη καζίνο, που ονομάζεται Μονακό, καθώς το στοιχείο της τύχης είναι ο πυρήνας της προσέγγισης μοντελοποίησης, παρόμοιο με ένα παιχνίδι ρουλέτας.

Μια προσομοίωση Monte Carlo μπορεί να αξιολογήσει τον αντίκτυπο του κινδύνου σε πολλά σενάρια της πραγματικής ζωής, όπως στην τεχνητή νοημοσύνη, τις τιμές των μετοχών, την πρόβλεψη πωλήσεων, τη διαχείριση έργων και την τιμολόγηση. Παρέχουν επίσης μια σειρά από πλεονεκτήματα έναντι των προγνωστικών μοντέλων με σταθερές εισόδους, όπως η ικανότητα διεξαγωγής ανάλυσης ευαισθησίας ή υπολογισμού της συσχέτισης των εισροών. Η ανάλυση ευαισθησίας επιτρέπει στους λήπτες αποφάσεων να δουν τον αντίκτυπο των μεμονωμένων εισροών σε ένα δεδομένο αποτέλεσμα και η συσχέτιση τους επιτρέπει να κατανοήσουν τις σχέσεις μεταξύ οποιωνδήποτε μεταβλητών εισόδου. [32], [33]

Αρχικά υπολογίστηκε η ημερήσια απόδοση σύμφωνα με τον παρακάτω τύπο:

$$\text{Ημερήσια Απόδοση} = \ln(\text{Τιμή ημέρας} / \text{Τιμή προηγούμενης ημέρας})$$

$$(\text{Daily Return} = \ln(\text{Day's Price} / \text{Previous Day's Price}))$$

Στη συνέχεια υπολογίστηκε η τάση ως εξής:

$$\text{Τάση} = \text{Μέση Ημερήσια Απόδοση} - (\text{Τυπική απόκλιση} / 2)$$

$$(\text{Drift} = \text{Average Daily Return} - (\text{Standard Deviation} / 2))$$

Όπου αντί της Variance – Διαφορά, που παράγεται από τη Συνάρτηση VAR.P του excel από τα δεδομένα των ημερήσιων αποδόσεων (daily returns series), μπήκε η Standard Deviation – Τυπική απόκλιση, που υπολογίζεται από τη συνάρτηση του Excel STDEV.P, κι αυτό γιατί μετά από δοκιμές βρέθηκε να δίνει καλύτερα αποτελέσματα.

Η Average Daily Return - Μέση Ημερήσια Απόδοση, παράγεται από τη συνάρτηση του Excel AVERAGE από τις τιμές της ημερήσιας απόδοσης.

Η τιμή της επόμενης ημέρας υπολογίστηκε από τον τύπο:

Τιμή επόμενης ημέρας = τιμή τρέχουσας ημέρας * $e^{(τάση+τυχαία\ τιμή)}$

(Next Day's Price=Today's Price $\times e^{(Drift+Random\ Value)}$)

Κανονικά χρειάζεται μια τυχαία τιμή η οποία θα έπρεπε να παραχθεί από την Random Value= $\sigma \times \text{NORMSINV}(\text{RAND}())$ όπου: σ = τυπική απόκλιση - Standard deviation, που παράγεται από τη συνάρτηση του Excel STDEV.P και από την Ημερήσια Απόδοση (daily returns series) και τις NORMSINV και RAND που είναι συναρτήσεις του Excel.

Θέλοντας να χρησιμοποιήσουμε το μοντέλο Monte Carlo αλλά να αφαιρέσουμε την τυχειότητα που προκύπτει με τη χρήση της rand(), αλλά να προσθέσουμε βαρύτητα στην τάση που δείχνει η αγορά προς το bitcoin, χρησιμοποιήθηκε σαν τυχαία τιμή ένας συνδυασμός της τυπικής απόκλισης.

Καταρχήν υπολογίστηκε η τυπική απόκλιση (σ) του τελευταίου έτους, των τελευταίων 20 ημερών και της τελευταίας εβδομάδας. Δώσαμε από βαρύτητα 25% στο σ της τελευταίας εβδομάδας και στο σ των τελευταίων 20 ημερών και 50% βαρύτητα στο σ του τελευταίου έτους. Έτσι ο συντελεστής για τον υπολογισμό της τυχαίας τιμής ήταν ο συνδυασμός των σ : τυχαία τιμή = $(\sigma_{\text{έτους}} + (\sigma_{\text{εβδομάδας}} + \sigma_{20\text{ημερών}})/2)/2$

Ακολουθούν τα αποτελέσματα που παρήχθησαν:

Για 21/5/2022

average daily return (close)	-0,00091525
variance	0,03688604
drift	-0,01935827

σ derived from avg	0,03688604
σ from last 7 days	0,04228462
σ from last 20 days	0,04508663

Random value = 0,04028583

Next day 21.05.22	29818,2799
ML Forecast Avg	29408,2309

Actual value

29432,23

MC Percentage error	-1,311653502
ML Forecast error	0,08154353

Για 4/12/2021

ML Forecast Avg	54781,69
-----------------	----------

Next day 4.12.21	54488,8156
------------------	------------

average (close) daily return	0,001387094
variance	0,03847127
drift	-0,017848542

σ derived from avg	0,03847127
σ last 7 days	0,02836642
σ last 20 days	0,032001676

Random value = 0,03432766

Actual value

49200,70313

MC Percentage error	-10,74804257
ML Forecast error	-11,343311

Για 1/3/2022

ML Forecast Avg 43068,87

Next day 1.3.22 47985,8022

average (close) daily return 0,000202201
variance 0,037563202
drift -0,0185794

σ derived from avg 0,037563202
last 7 days 0,052662504
last 20 days 0,04244977

Random value = 0,04255967

Actual value
49200,70313

MC Percentage error 2,4692755
ML Forecast error 2,8988232

Για 11/5/2022

ML Forecast Avg 31940,30

Next day 11.5.22 29527,0455

average (close) daily return -0,000963933
variance 0,036871691
drift -0,019399779

σ derived from avg 0,036871691
last 7 days 0,044248003
last 20 days 0,040439166

Random value = 0,03960764

Actual value
28936,35547

MC Percentage error -2,041342043
ML Forecast error -10,381198

Για 15/10/2021

ML Forecast Avg 57039,69

Next day 15.10.21 58247,5504

average (close) daily return 0,002315764

variance 0,040653548
drift -0,01801101

σ derived from avg 0,040653548
last 7 days 0,02187123
last 20 days 0,032969149

Random value = 0,03403687

Actual value
61593,94922

MC Percentage error
5,432999219

ML Forecast error
7,39399989

Για 28/7/2021

ML Forecast Avg 38726,46

Next day 28.07.21 39911,2902

average (close) daily return -0,000504661

variance 0,045203058
drift -0,02310619

σ derived from avg 0,045203058
last 7 days 0,021349266
last 20 days 0,031538446

Random value = 0,03582346

Actual value
39995,90625

MC Percentage error
0,211561815

ML Forecast error
3,17395296

Παρατηρούμε πως η προσομοίωση Monte Carlo δίνει πολύ καλύτερα αποτελέσματα σε σχέση με την πρόβλεψη των Μοντέλων Μηχανικής Μάθησης.

4 Σύνοψη και συμπεράσματα

Τα κρυπτονομίσματα έχουν αρκετά σημαντική θέση στην παγκόσμια οικονομία και έχουν την προσοχή από ένα αυξανόμενο αριθμό επενδυτών. Γύρω από τα κρυπτονομίσματα υπάρχουν τεχνολογίες αιχμής όπως η τεχνολογία blockchain. Σε κάποιους προκαλεί εναλλακτικό επενδυτικό ενδιαφέρον, σε άλλους όμως προκαλεί κερδοσκοπικό ενδιαφέρον οπότε σε αυτή την ταχέως ανερχόμενη αγορά με πολλές μελλοντικές προοπτικές, αλλά και πολλές αδυναμίες όπως ότι είναι ανώριμη, είναι μικρός ο όγκος συναλλαγών σε σχέση με άλλες κατηγορίες περιουσιακών στοιχείων η επένδυση σε κρυπτονομίσματα κατατάσσεται στις ριψοκίνδυνες απομακρύνοντας επενδυτές και προκαλώντας πτώση της τιμής τους. Τα νέα μέσα και οι τεχνολογίες αλλάζουν τη ζωή μας και η χρήση μοντέλων πρόβλεψης της τιμής των κρυπτονομισμάτων αποτελούν ένα ερευνητικό πεδίο με πολύ μεγάλο ενδιαφέρον. Δεν είναι εύκολο ένα μοντέλο να βασίζεται σε ιστορικά δεδομένα και να δώσει αξιόπιστες προβλέψεις όταν η αγορά κλονίζεται. Όσο οι συνθήκες είναι φυσιολογικές μπορούν οι προβλέψεις να επαληθευτούν και ένας επενδυτής να βοηθηθεί για τον καλύτερο σχεδιασμό των επενδύσεων του. Σε περιόδους αστάθειας βρέθηκε μια παραλλαγή της μεθόδου Monte Carlo που προσεγγίζει καλύτερα την τιμή από τις προβλέψεις των μοντέλων της Μηχανικής Μάθησης που δοκιμάστηκαν.

ΒΙΒΛΙΟΓΡΑΦΙΑ

- [1]. M. Wimalagunaratne and G. Poravi, "A Predictive Model for the Global Cryptocurrency Market: A Holistic Approach to Predicting Cryptocurrency Prices," 2018 8th International Conference on Intelligent Systems, Modelling and Simulation (ISMS), 2018, pp. 78-83, doi: 10.1109/ISMS.2018.00024.
- [2]. Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," Proc. - 2017 IEEE 6th Int. Congr. Big Data, BigData Congr. 2017, no. October, pp. 557–564, 2017.
- [3]. V. Shrivastava and S. Kumar, "Utilizing Block Chain Technology in Various Application Areas of Machine Learning," 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon), 2019, pp. 167-171, doi: 10.1109/COMITCon.2019.8862203.
- [4]. Q. Wang, "Cryptocurrencies asset pricing via machine learning: Extended abstract," 2020 IEEE 7th International Conference on Data Science and Advanced Analytics (DSAA), 2020, pp. 789-790, doi: 10.1109/DSAA49011.2020.00118.
- [5]. P. Gupta, V. Dedeoglu, S. S. Kanhere and R. Jurdak, "Towards a blockchain powered IoT data marketplace," 2021 International Conference on COMMunication Systems & NETworkS (COMSNETS), 2021, pp. 366-368, doi: 10.1109/COMSNETS51098.2021.9352865.
- [6]. "Τιμές κρυπτονομισμάτων, γραφήματα και κεφαλαιοποιήσεις αγοράς | CoinMarketCap," *CoinMarketCap*. <https://coinmarketcap.com/el/> (accessed Jul. 05, 2022).
- [7]. Jerry Brito; Andrea Castillo (2013). "Bitcoin: A Primer for Policymakers" (PDF). *Mercatus Center*. George Mason University. Retrieved 5 May 2022.
- [8]. U. W. Chohan, "A History of Bitcoin," Monetary Economics: International Financial Flows, Financial Crises, Regulation & Supervision eJournal. Social Science Research Network (SSRN), papers.ssrn.com, Sep. 30, 2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3047875. Accessed 8 May 2022.
- [9]. W. Dai, "B-money," Weidai.com, 2019. <http://www.weidai.com/bmoney.txt>. Retrieved 5 May 2022.
- [10]. N. Szabo, "Bit gold," Blogspot.com, Jan. 28, 2020. <http://unenumerated.blogspot.com/2005/12/bit-gold.html> Retrieved 5 December 2013.
- [11]. H. T. T. Truong, M. Almeida, G. Karame and C. Soriente, "Towards Secure and Decentralized Sharing of IoT Data," 2019 IEEE International Conference on Blockchain (Blockchain), 2019, pp. 176-183, doi: 10.1109/Blockchain.2019.00031.
- [12]. European Central Bank, "Πώς μπορεί η νέα τεχνολογία να μεταμορφώσει τις χρηματοπιστωτικές αγορές;," European Central Bank, 18-Nov-2021. [Online]. Available: https://www.ecb.europa.eu/ecb/educational/explainers/tell-me-more/html/distributed_ledger_technology.el.html. [Accessed: 20-Jan-2022].
- [13]. S. Daley, "Blockchain and IOT: 8 examples making our future smarter," Built In, 27-Dec-2021. [Online]. Available: <https://builtin.com/blockchain/blockchain-iot-examples>. [Accessed: 20-Jan-2022].
- [14]. "AIR Applied Innovation Review," 2016. [Online]. Available: <https://j2-capital.com/wp-content/uploads/2017/11/AIR-2016-Blockchain.pdf>

- [15].Y. Kwon, H. Kim, J. Shin and Y. Kim, "Bitcoin vs. Bitcoin Cash: Coexistence or Downfall of Bitcoin Cash?," 2019 IEEE Symposium on Security and Privacy (SP), 2019, pp. 935-951, doi: 10.1109/SP.2019.00075.
- [16].“Do Cryptocurrencies Such as Bitcoin Have a Future?,” Wall Street Journal, Mar. 02, 2015. [Online]. Available: <https://www.wsj.com/articles/do-cryptocurrencies-such-as-bitcoin-have-a-future-1425269375>
- [17].“Advantages | Bitcoin,” Stanford.edu, 2010.
<https://cs.stanford.edu/people/eroberts/cs201/projects/2010-11/DigitalCurrencies/advantages/index.html>
- [18].F. Bunjaku, O. Gjorgieva-Trajkovska, and E. Miteva-Kacarski, “CRYPTOCURRENCIES -ADVANTAGES AND DISADVANTAGES.” [Online]. Available: <https://eprints.ugd.edu.mk/18707/1/Cryptocurrencies.pdf>
- [19].Τσαούση Δημ. (2018). Ανάλυση Χρηματοοικονομικών Χρονοσειρών και Πρόβλεψη με Γραμμικά Μοντέλα, Τμήματα Πληροφορικής και Οικονομικών Επιστημών, Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης,, Θεσσαλονίκη. Ανακτήθηκε: <http://ikee.lib.auth.gr/record/297900/files/GRI-2018-21573.pdf>
- [20].IBM Cloud Education, “What is Machine Learning?,” IBM, Jul. 15, 2020. <https://www.ibm.com/cloud/learn/machine-learning>
- [21].“Reinforcement learning - GeeksforGeeks,” GeeksforGeeks, Apr. 25, 2018. <https://www.geeksforgeeks.org/what-is-reinforcement-learning/> [Accessed 5 July 2022].
- [22].“SMOreg,” sci2s.ugr.es.
<https://sci2s.ugr.es/keel/javadoc/keel/Algorithms/SVM/SMO/SMOreg.html> (accessed Jul. 05, 2022).
- [23].IBM Cloud Education, “About Linear Regression | IBM,” [www.ibm.com](https://www.ibm.com/topics/linear-regression). <https://www.ibm.com/topics/linear-regression> [Accessed 5 July 2022].
- [24].C. Bento, “Multilayer Perceptron Explained with a Real-Life Example and Python Code: Sentiment Analysis,” Medium, Sep. 30, 2021. <https://towardsdatascience.com/multilayer-perceptron-explained-with-a-real-life-example-and-python-code-sentiment-analysis-cb408ee93141> [Accessed 5 July 2022].
- [25].IBM Cloud Education, “What is Bagging?,” [www.ibm.com](https://www.ibm.com/cloud/learn/bagging). <https://www.ibm.com/cloud/learn/bagging> [Accessed 5 July 2022].
- [26].IBM Cloud Education, “What is Random Forest?,” [www.ibm.com](https://www.ibm.com/cloud/learn/random-forest), Dec. 07, 2020. <https://www.ibm.com/cloud/learn/random-forest> [Accessed 5 July 2022].
- [27].Link.springer.com. 2022. [online] Available at:
<<https://link.springer.com/content/pdf/10.1007/BF00992698.pdf>> [Accessed 5 July 2022].
- [28].R. Balsys, “An Introduction to Advantage Actor-Critic method (A2C),” Medium, Nov. 18, 2021. <https://python.plainenglish.io/introduction-to-advantage-actor-critic-method-a2c-8efe2b67a7e9> (accessed Jul. 05, 2022).
- [29].J. Hui, “RL — Policy Gradient Explained,” Medium, Aug. 27, 2020. <https://jonathan-hui.medium.com/rl-policy-gradients-explained-9b13b688b146>
- [30].“Reinforcement Learning for Trading Tutorial | \$GME RL Python Trading,” [www.youtube.com](https://www.youtube.com/watch?v=D9sU1hLT0QY&ab_channel=NicholasRenotte).
https://www.youtube.com/watch?v=D9sU1hLT0QY&ab_channel=NicholasRenotte (accessed Jul. 05, 2022).
- [31].“Weka 3 - Data Mining with Open Source Machine Learning Software in Java,” Waikato.ac.nz, 2019. <https://www.cs.waikato.ac.nz/ml/weka/>

- [32].Investopedia. 2022. What Is a Monte Carlo Simulation?. [online] Available at: <<https://www.investopedia.com/terms/m/montecarlosimulation.asp>> [Accessed 5 July 2022].
- [33].IBM Cloud Education, “What is Monte Carlo Simulation?,” [www.ibm.com](https://www.ibm.com/cloud/learn/monte-carlo-simulation), Aug. 24, 2020. <https://www.ibm.com/cloud/learn/monte-carlo-simulation>. [Accessed 5 July 2022].