Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Προηγμένα Συστήματα Πληροφορικής»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Βιβλιογραφική Επισκόπηση πρόβλεψης τιμών Bitcoin με χρήση μεθόδων Μηχανικής Μάθησης.** **A Literature Review on Machine Learning Techniques for the Prediction of Bitcoin Prices.**
Ονοματεπώνυμο Φοιτητή	**Σταυροπούλου Χρυσάνθη**
Πατρώνυμο	**Χρήστος**
Αριθμός Μητρώου	**ΜΠΣΠ 17063**
Επιβλέπων	**Διονύσιος Σωτηρόπουλος,** **Επίκουρος Καθηγητής**

Ημερομηνία Παράδοσης **Ιούλιος 2020**

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Σωτηρόπουλος Διονύσιος Επίκουρος Καθηγητής	Τσιχριντζής Γεώργιος Καθηγητής	Αλέπης Ευθύμιος Αναπληρωτής Καθηγητής

ABSTRACT

Bitcoin is a crypto-currency based on open source technology that operates in a peer-to –peer grid protocol as a mechanism to facilitate private payments. This protocol operates with a sophisticated cryptography procedure supported by a network of users. Our study reviews the current literature and tries to provide information about the attributes of the bitcoin based on the latest researches. Bitcoin seem to have a number of advantages and disadvantages and creates unique challenges in the financial community. One of these challenges is the bitcoin's price prediction. We present a number of machine learning algorithms that focus on predicting the biotin price and compare them in terms of efficiency. Finally, this study provides an insight in the potential of bitcoin, and also highlights the prerequisites, needs, implications and challenges faced by bitcoin in processing business transactions.

Keywords: Bitcoin, machine learning, cryptocurrency, price prediction, bitcoin mining

ΠΕΡΙΛΗΨΗ

Το Bitcoin βασίζεται σε τεχνολογία ανοικτού κώδικα η οποία δουλεύει με διότιμο πρωτόκολλο, ώστε να διευκολύνει τις ιδιωτικές πληρωμές. Το συγκεκριμένο πρωτόκολλο βασίζεται σε μια εξειδικευμένη διαδικασία κρυπτογράφησης, η οποία υποστηρίζεται από ένα δίκτυο χρηστών. Η συγκεκριμένη μελέτη χρησιμοποίησε την πιο πρόσφατη βιβλιογραφία για να παρέχει λεπτομέρειες για τη λειτουργία του bitcoin όπως αυτή αποτυπώνεται στις πρόσφατες μελέτες. Το Bitcoin φαίνεται ότι έχει τόσο πλεονεκτήματα όσο και μειονεκτήματα, ενώ δημιουργεί έναν αριθμό από μοναδικές προκλήσεις στην κοινότητα των οικονομολόγων. Μία από αυτές τις προκλήσεις είναι η πρόβλεψη των τιμών του Bitcoin. Στην παρούσα διατριβή αναλύουμε μια σειρά από αλγόριθμους μηχανικής μάθησης οι οποίοι επικεντρώνονται στην πρόβλεψη των τιμών του bitcoin και τους συγκρίνουμε αναφορικά με την απόδοσή τους. Τέλος, στην μέλέτη αυτή προσπαθούμε να διερευνήσουμε τις προαπαιτήσεις, τις ανάγκες, τις επιπτώσεις και τις δυσκολίες που προκαλεί το bitcoin στις εμπορικές συναλλαγές.

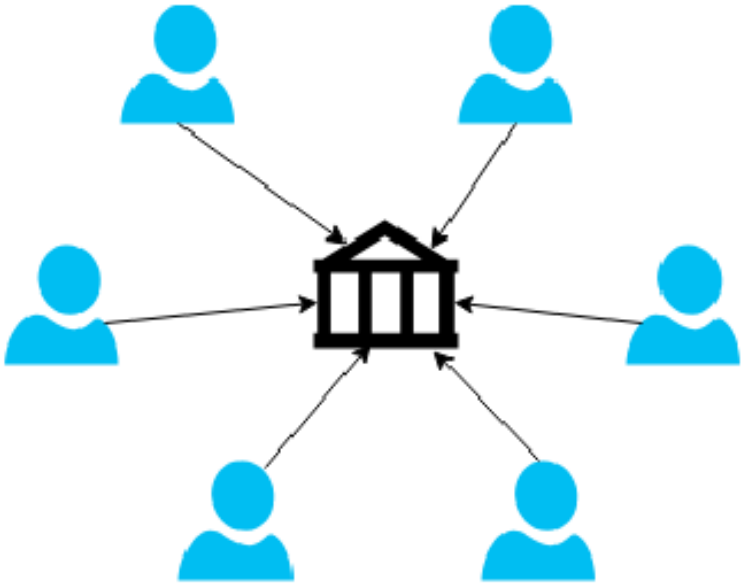
Περιεχόμενα

1. Εισαγωγή

Τα ψηφιακά νομίσματα είναι πολύ διαδεδομένα στην εποχή μας. Το πιο δημοφιλές ψηφιακό νόμισμα είναι το bitcoin το οποίο έχει συνολική κεφαλαιοποίηση 71.882.552.340 δολάρια ΗΠΑ. Είναι , ουσιαστικά ένα αποκεντρωμένο, κατανεμημένο και διομότιμο ψηφιακό νόμισμα που είναι γνωστό και σαν κρυπτονόμισμα (cryptocurrency) (Chatterjee et al., 2018). Ο δημιουργός του bitcoin είναι γνωστός με το ψευδώνυμο Satoshi Nakamoto, και η πραγματική του ταυτότητα παραμένει άγνωστη ακόμη και σήμερα. Λόγω της αποκεντρωμένης του ιδιότητας, δεν έχει κάποιον κεντρικό έλεγχο, όπως έχουν είναι οι τράπεζες στα συμβατικά νομίσματα. Η μεταφορά του νομίσματος από τον έναν χρήστη στον άλλον, δεν εξαρτάται από κανέναν τρίτο. Το bitcoin επιτρέπει στους χρήστες να μεταφέρουν χρήματα ο ένας στο άλλον με τρόπο τόσο απλό όσο να στέλνουν ένα email (Dimitri et al., 2017).

1.1 Κεντρικό Σύστημα

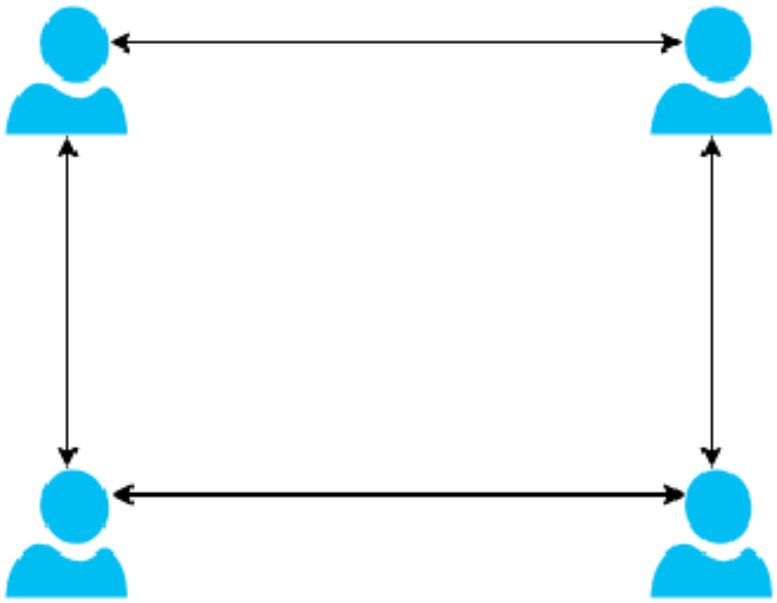
Όπως υποδηλώνει και η λέξη κεντρική διαχείριση είναι η περίπτωση της συγκέντρωσης του ελέγχου ενός οργανισμού ή μιας δραστηριότητας κάτω από μια μόνο αρχή. Τα νομίσματα που χρησιμοποιούμε σήμερα είναι ουσιαστικά παραστατικά νομισμάτων τα οποία μεταφέρονται ανάμεσα στους ανθρώπους μέσω ενός κεντρικού συστήματος. Όταν δύο άτομα θέλουν να μεταφέρουν ένα συγκεκριμένο αριθμό χρημάτων η συναλλαγή πρέπει να περάσει μέσω ενός τρίτου μέλους το οποίο ξεκινάει τη διαδικασία και επιβεβαιώνει τη συναλλαγή. Αν ο χρήστης Α, θέλει να μεταφέρει χρήματα στο χρήστη Β, τότε η διαδικασία ξεκινάει από το χρήστη Α και στη συνέχεια το τρίτο μέλος (στην περίπτωση αυτή η τράπεζα), λαμβάνει την ειδοποίηση της συναλλαγής, επαληθεύει την ορθότητα της συναλλαγής και την εγκρίνει αν τα δεδομένα είναι σωστά. Μετά την έγκριση, το ποσό μεταφέρεται στο χρήστη Β. Για τη διαδικασία αυτή καταναλώνεται ένα συγκεκριμένο χρονικό διάστημα, και η τράπεζα παίρνει ένα ποσό σαν τέλος μεταφοράς (Εικόνα 1) (Ziegeldorf et al., 2018).



Εικόνα 1. Το κεντρικό σύστημα διαχείρισης των νομισμάτων

1.2 Αποκεντρωμένο σύστημα

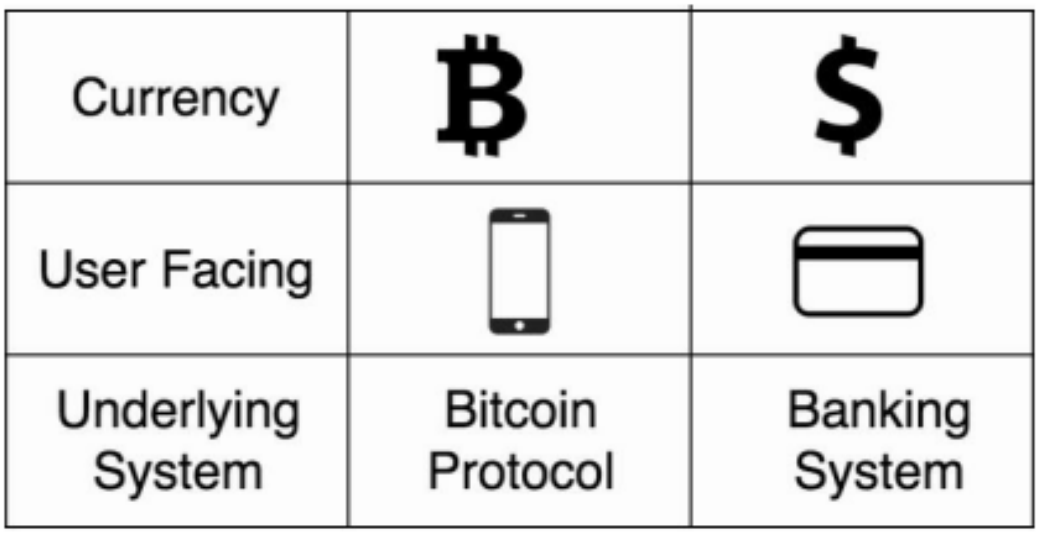
Η εργασία που απαιτείται για τη μεταφορά του bitcoin διαμοιράζεται ανάμεσα σε κάθε χρήστη του δικτύου. Αυτό, σημαίνει ότι τα δεδομένα δε χρειάζεται να περάσουν μέσα από κάποιο κεντρικό διακομιστή ή κάποιον κεντρικό κόμβο. Στην περίπτωση αυτή, κάθε χρήστης που είναι συνδεδεμένος στο δίκτυο Bitcoin, έχει μια δημόσια βάση συναλλαγών για κάθε συναλλαγή του. Οι χρήστες ταυτοποιούν τις συναλλαγές μόνοι τους και εγκρίνουν τη συναλλαγή, αν αυτή είναι έγκυρη. Αν όλοι οι χρήστες του δικτύου εγκρίνουν τη συναλλαγή τότε η συναλλαγή είναι έγκυρη και το ποσό μεταφέρεται από τον χρήση Α στο χρήστη Β. Η διαδικασία αυτή δε χρειάζεται μεγάλο χρονικό διάστημα και έχει ελάχιστο τέλος μεταφοράς σε σχέση με το κεντρικό σύστημα (Εικόνα 2) (Jin et al., 2017).



Εικόνα 2. Το αποκεντρωμένο σύστημα

1.3 Το σύστημα bitcoin σε σύγκριση με το τυπικό σύστημα

Το σύστημα του bitcoin διαφέρει σε σχέση με το υπάρχον σύστημα νομισμάτων. Από την Εικόνα 3 μπορούμε να διακρίνουμε τις διαφορές που έχει σε σχέση με το υπάρχον τραπεζικό σύστημα. Το νομισματικό σύστημα χρησιμοποιεί ένα επικεντρωμένο σύστημα το οποίο ουσιαστικά είναι το τραπεζικό σύστημα. Δέχεται τα νομίσματα σαν μέθοδο πληρωμής (USD, ASD, NPR, INR κλπ). Από την άλλη μεριά, το πρωτόκολλο του bitcoin χρησιμοποιεί ένα αποκεντρωμένο σύστημα το οποίο δέχεται εικονικά νομίσματα σαν μέθοδο πληρωμής (Bitcoin). Το πρωτόκολλο το οποίο βρίσκεται πίσω από το bitcoin και τα υπόλοιπα κρυπτονομίσματα είναι το blockchain (αλυσίδα επιβεβαιωμένων ομάδων συναλλαγών που ξεκινά από την πρώτη μέχρι την πιο πρόσφατη έγκυρη ομάδα) (Crosby et al., 2016).



Εικόνα 3. Το σύστημα του bitcoin σε σύγκριση με το σύστημα που εφαρμόζεται τυπικά

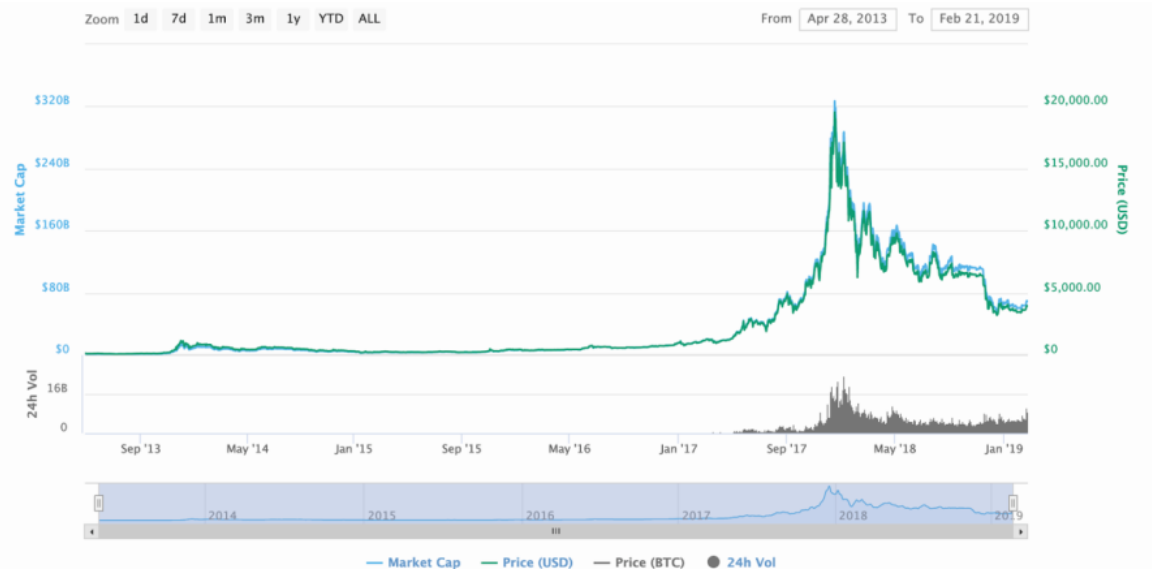
1.4 Ιστορική αναδρομή του Bitcoin

Πολλές ήταν οι ημερομηνίες που υπήρξαν σταθμοί για την πορεία και την εξέλιξη του Bitcoin:

- Στις 11 Ιανουαρίου 2009 , δημιουργήθηκε το πρώτο Block της αλυσίδας των Blocks.
- Στις 12 Ιανουαρίου 2009 , σημειώθηκε η πρώτη συναλλαγή με Bitcoin από τον δημιουργό του Satoshi Nakamoto προς τον προγραμματιστή που το είχε δημιουργήσει . Τον πρώτο χρόνο οι τιμές ήταν πολύ χαμηλές και οι συναλλαγές γινόταν μόνο ιδιωτικά.
- Στις 5 Οκτωβρίου , έγινε η πρώτη συναλλαγματική ισοτιμία δολαρίου των ΗΠΑ και του Bitcoin από την New Liberty Standard. Η ισοτιμία ήταν 1 δολάριο ισάξιο με 1309 bitcoins.
- Τον Ιούλιο του 2010 φτιάχτηκε το πρώτο ανταλλακτήριο για Bitcoins , εν ονόματι Mt.Gox , το οποίο ακολούθησαν πολλά άλλα ιδιωτικά. Παρ' όλα αυτά το πρώτο ανταλλακτήριο συνέχισε να είναι το πιο ανεπτυγμένο, εφόσον το 70% των συναλλαγών σε Bitcoin γινόταν από αυτό.

- Τον Δεκέμβριο του 2012 , δημιουργείται η πρώτη παγκόσμια τράπεζα Bitcoin από το ανταλλακτήριο Bitcoin – Central σε συνεργασία με την γαλλική τράπεζα Credit Mutuel.
- Τον Φεβρουάριο του 2014 , το Mt.Gox κλείνει την ιστοσελίδα του επειδή δέχεται επίθεση από hackers , χάνοντας έτσι 744.408 bitcoins , μη μπορώντας ποτέ να τα πάρει πίσω.
- Τον Μάρτιο του 2017 για πρώτη φορά η τιμή του Bitcoin ξεπερνά την τιμή του χρυσού και φτάνει τα 1268 δολάρια Αμερικής , ενώ η τιμή μιας ουγκιάς χρυσού ήταν 1233 δολάρια.
- Τον Δεκέμβριο του 2017 το Bitcoin έφτασε την μέγιστη τιμή του έως σήμερα, τα 19.290 δολάρια.
- Σήμερα το bitcoin ξεπερνάει τα 89.000 $.

Η αγοραστική αξία της τιμής του Bitcoin φαίνεται στην Εικόνα 4.



Εικόνα 4. Ιστορία της τιμής του bitcoin

Από την Εικόνα μπορούμε να καταλάβουμε τις αλλαγές στην αγοραστική αξία του κρυτπονομίσματος, ειδικά τον Ιανουάριο του 2017. Σε αυτό το χρονικό σημείο, το bitcoin έγινε το πιο δημοφιλές κρυπτονόμισμα. Η αρχική τιμή του ήταν 0.00078 $ ανά νόμισμα. Η τιμή του bitcoin διακυμαίνεται λόγω της παρουσίας του στην αγορά συναλλάγματος και βασίζεται στην αλυσίδα προσφοράς και ζήτησης που υπάρχει εκεί (Gerlach et al., 2019).

1.5 Μεταφορά bitcoin

Το bitcoin μπορεί να μεταφερθεί από το ένα άτομο στο άλλο τόσο εύκολα όσο στέλνουμε ένα μήνυμα. Ωστόσο, για να γίνει η μεταφορά αυτή είναι απαραίτητη μια διεύθυνση (bircoin address), ένα πορτοφόλι (bitcoin wallet) και το ίδιο το κρυπτονόμισμα. Η μικρότερη υπομονάδα του bitcoin ονομάζεται Satoshi και είναι διαιρέσιμο μέχρι το 8^{ο} δεκαδικό ψηφείο, μπορεί δηλαδή να χωριστεί σε 100.000.000 μονάδες (Sorgente et al., 2014).

1 BTC = 1.000.000 Satoshi

Η διεύθυνση του Bitcoin χρησιμοποιείται για να γίνει μεταφορά του κρυπτονομίσματος ανάμεσα σε δύο άτομα. Η διεύθυνση αυτή έχει την ιδιότητα του τραπεζικού λογαριασμού στο τραπεζικό σύστημα. Αν ένα άτομο έχει μια διεύθυνση bitcoin, μπορεί να στείλει και να δεχτεί το νόμισμα σε οποιονδήποτε χρησιμοποιώντας έναν υπολογιστή ή ένα smartphone. Η διεύθυνση αντιπροσωπεύεται από μια ακολουθία 26-25 αλφαριθμιτικών χαρακτήρων και μπορεί να έχει τις τρεις ακόλουθες μορφές:

- Μορφή Α: P2PKH. Στη συγκεκριμένη μορφή, η διεύθυνση ξεκινάει με τον αριθμό 1.

Παράδειγμα: 1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX

- Μορφή Β: P2SH. Στη συγκεκριμένη μορφή, η διεύθυνση ξεκινάει με τον αριθμό 3.

Παράδειγμα: 3CfCfnj6bfmCVqfQAqinK7mB1tYJM5Qrnt

- Μορφή Γ: Bech32. Στη συγκεκριμένη μορφή. η διεύθυνση ξεκινάει με το γράμμα «bcl».

Παράδειγμα: bc1qldx8hs6y0m6cxy3ucf9kasvd3vlxky7ypsp233

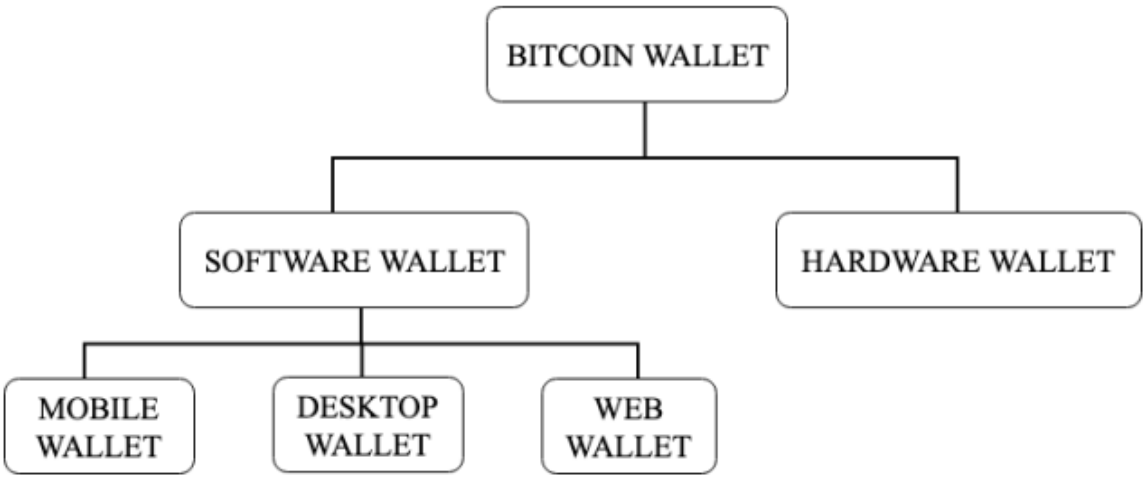
Το πορτοφόλι bitcoin είναι ένα ψηφιακό πορτοφόλι παρόμοιο με τον τραπεζικό λογαριασμό και χρησιμοποιείται για να αποθηκεύσει το νόμισμα. Το λογισμικό, επιτρέπει την ασφαλή μεταφορά, λήψη και αποθήκευση του κρυπτονομίσματος στο δίκτυο. Υπάρχουν δύο βασικές μορφές πορτοφολιού, το πορτοφόλι λογισμικού και το πορτοφόλι με ηλεκτρονική συσκευή (Fan et al., 2019).

Τα πορτοφόλια λογισμικού είναι προγράμματα τα οποία εγκαθίστανται στον υπολογιστή μέσω ασφάλειας κρυπτογράφησης. Τα πορτοφόλια λογισμικού διαιρούνται περαιτέρω σε τρεις κατηγορίες: τα κινητά πορτοφόλια, τα πορτοφόλια ιστοθέσεων και τα πορτοφόλια επιφάνειας εργασίας. Τα κινητά πορτοφόλια μπορούν να εγκατασταθούν σε οποιαδήποτε κινητή συσκευή (συνήθως smartphone με λειτουργικό Android/iOS). Αντίστοιχα τα πορτοφόλια επιφάνειας εργασίας μπορούν να εγκατασταθούν σε ένα σταθερό υπολογιστή (με λειτουργικό σύστημα Windows/Mac/Linux). Επιτρέπουν στο χρήστη να δημιουργήσει μια διεύθυνση Bitcoin για να στέλνει και να λαμβάνει

κρυπτονομίσματα. Τέλος, στα πορτοφόλια ιστοθέσεων, οι χρήστες μπορούν να έχουν πρόσβαση από οποιαδήποτε συσκευή που διαθέτει πρόγραμμα φυλομετρητή (Volety et al., 2019).

Τα πορτοφόλια ηλεκτρονικού εξοπλισμού είναι παρόμοια με ένα εξωτερικό σκληρό δίσκο. Είναι φυσικές συσκευές που μπορούν να συνδεθούν με τον υπολογιστή και να αποθηκεύσουν Bitcoin. Είναι οι πιο ασφαλείς μέθοδοι αποθήκευσης κρυπτονομισμάτων αφού έχει πολύ λιγότερη έκθεση στον υπολογιστή και είναι δύσκολο να παραβιαστούν τα δεδομένα που περιέχουν (Εικόνα 5) (Biryukov et al., 2019).

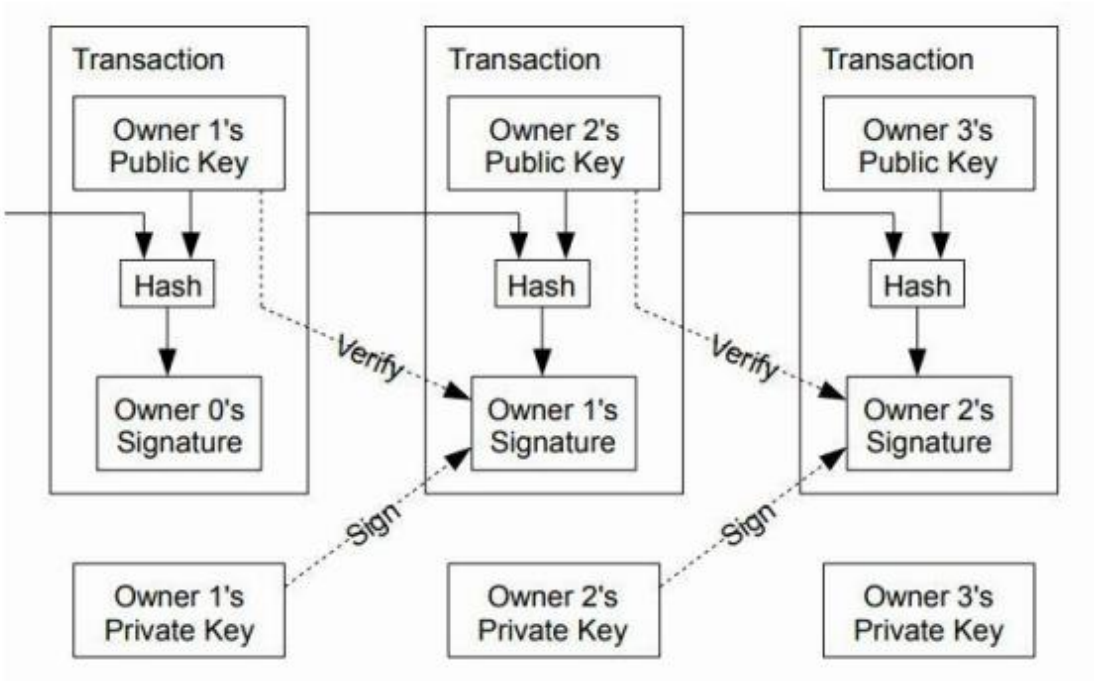
.



Εικόνα 5. Τα είδη των πορτοφολιών Bitcoin

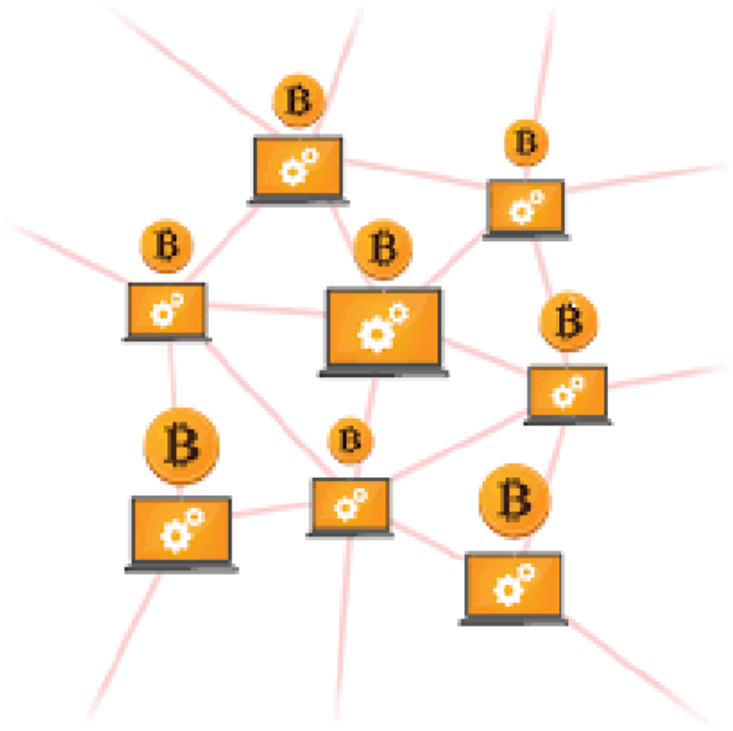
Τα πρωτόκολλα Bitcoin βασίζονται στην δημόσια κρυπτογράφηση. Ο ιδιοκτήτης του κρυπτονομίσματος έχει δύο κλειδιά: ένα δημόσιο και ένα ιδιωτικό. Μπορούμε να αντιστοιχίσουμε περίπου το όνομα χρήστη με το δημόσιο κλειδί και τον κωδικό με το ιδιωτικό. Με παρόμοιο τρόπο, ο κατακερματισμός ενός δημοσίου κλειδιού, είναι μια διεύθυνση για Bitcoin, και για το λόγο αυτό, υπάρχει πάντα ένα

ιδιωτικό κλειδί που συσχετίζεται με ένα δημόσιο κλειδί. Τα ιδιωτικά κλειδιά χρησιμοποιούνται για να δημιουργήσουν μια υπογραφή και τα δημόσια κλειδιά για να επιβεβαιώσουν την υπογραφή αυτή. Στο σύστημα το Bitcoin, αν κάποιος θέλει να κάνει μια συνδιαλλαγή, κάθε κάτοχος του νομίσματος μπορεί να το μεταφέρει σε κάποιον άλλο χρήστη, υπογράφοντας ψηφιακά τον κατακερματισμό μιας προηγούμενης συνδιαλλαγής και του δημοσίου κλειδιού του επόμενου κατόχου των χρημάτων. Ο αλγόριθμος που χρησιμοποιείται ονομάζεται Elliptic Curve Digital Signature Algorithm (ECDSA) και βασίζεται κυρίως στα μαθηματικά (Εικόνα 6) (Eskandari et al., 2018).



Εικόνα 6. Συνδιαλλαγή με bitcoin

Επειδή το Bitcoin είναι ουσιαστικά ένα αποκεντρωμένο δίκτυο, η ανταλλαγή πληροφοριών διαμοιράζεται ανάμεσα στους χρήστες του δικτύου. Στην συγκεκριμένη περίπτωση δικτύου, οι πληροφορίες, αναφέρονται σε συναλλαγές που γίνονται είτε κατά την αγορά είτε κατά την πώληση των κρυπτονομισμάτων (Εικόνα 7).



Εικόνα 7. Διμότιμο δίκτυο Bitcoin

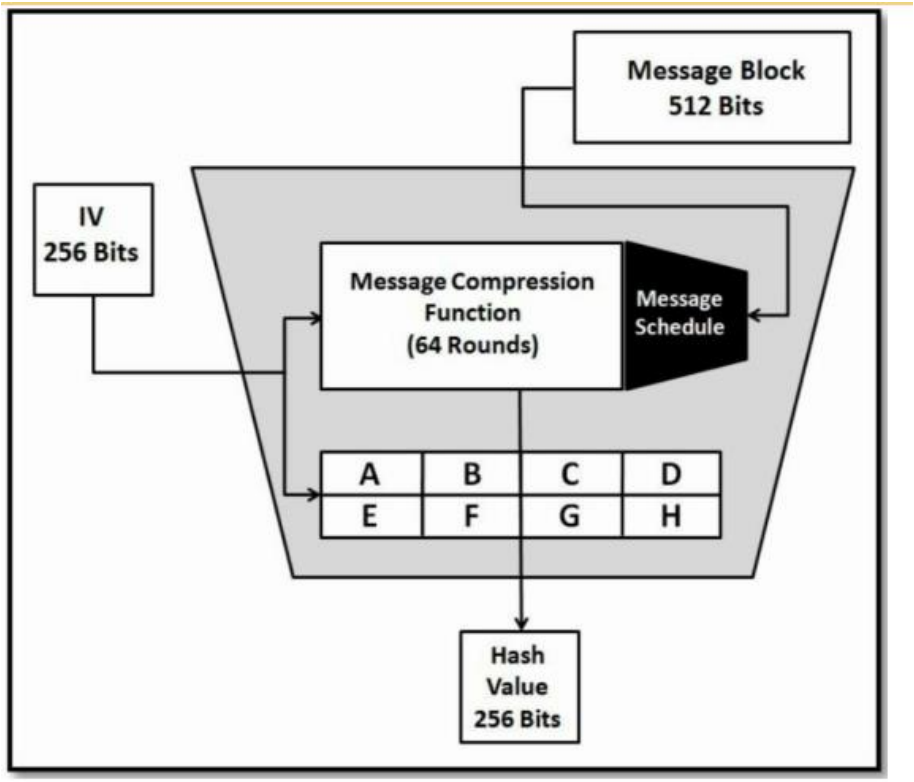
Στο πρωτόκολλο Bitcoin, οι κρυπτογραφικές λειτουργίες κατακερματισμού, χρησιμοποιούνται για τον κερματισμό των συναλλαγών του κρυπτονομίσματος. Ο κατακερματισμός είναι η διαδικασία με την οποία γίνεται ψηφιακή χαρτογράφηση των δεδομένων οποιουδήποτε αυθαίρετου μεγέθους σε ένα προκαθορισμένο μέγεθος (Ding et al., 2019). Με άλλα λόγια, ο κατακερματισμός είναι η ψηφιακή υπογραφή οποιωνδήποτε δεδομένων. Είναι η διαδικασία της λήψης κάποιον αναγνώσιμων πληροφοριών και η μετατροπή τους σε κάτι που δεν βγάζει κανένα νόημα. Κάθε αλγόριθμος κατακερματισμού, πρέπει να έχει μια σειρά από προϋποθέσεις:

- Συγκεκριμένο αποτέλεσμα κατακερματισμού
- Οποιαδήποτε αλλαγή στην είσοδο του αλγόριθμου πρέπει να αποφέρει ένα απολύτως διαφορετικό αποτέλεσμα.
- Η ίδια είσοδος, επιφέρει το ίδιο αποτέλεσμα
- Ο υπολογισμός της τιμής εισόδου από την τιμή εξόδου πρέπει να είναι αδύνατος (αντίστροφη διαδικασία).

- Η διαδικασία του κατακερματισμού πρέπει να είναι πολύ γρήγορη (Cheng et al., 2018)

Ο αλγόριθμος Secure Hash Algorithm (SHA) είναι ένα σύνολο κρυπτογραφικών εξισώσεων που έχει δημοσιευτεί από το NIST (National Institue of Science and Technology). Στο σύστημα του Bitcoin, χρησιμοποιείται ο αλγόριθμος κατακερματισμού SHA-256. Ο αλγόριθμος αυτός έχει σαν έξοδο έναν αριθμό 256 bit ο οποίος αναπαρίσταται στο δεκαεξαδικό αριθμητικό σύστημα. Το SHA σύνολο αποτελείται από 4 υπό-ομάδες τις SHA-0, SHA-1, SHA-2 και SHA-3 (Suresh et al., 2018).

Ο δημιουργός του bitcoin χρησιμοποίησε διπλό κατακερματισμό στο πρωτόκολλο του κρυπτονομίσματος για να κάνει τη διαδικασία του κατακερματισμού πιο άρτια αλλά και να αποφύγει επιθέσεις από κακόβουλο λογισμικό, όπως την επίθεση birthday. Η επίθεση birthday, είναι ένα σενάριο επίθεσης βάση του οποίου κάποιος χρήστης μπορεί να επιτύχει τον ίδιο ακριβώς κατακερματισμό χρησιμοποιώντας διαφορετική είσοδο στον αλγόριθμο. Το γεγονός αυτό, απαλείφει την μοναδική ιδιότητα του κατακερματισμού. Χωρίς, την ιδιότητα αυτή, δυο διαφορετικά μπλοκ bitcoin μπορεί να αναπαρίστανται από τον ίδιο κατακερματισμό, επιτρέποντας σε κάποιο χρήστη που επιτίθεται να μπορεί να αλλάξει τα blocks μεταξύ τους (Εικόνα 8)(Ghimire et al., 2018).



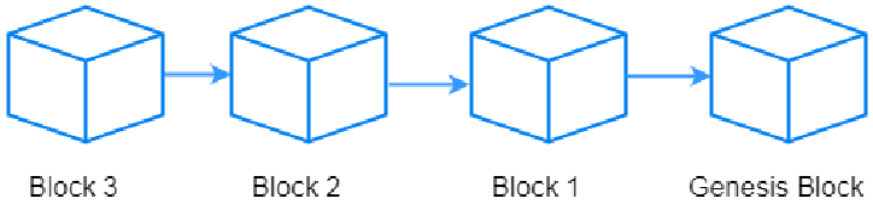
Εικόνα 8. Το διάγραμμα του SHA - 256

1.6 Block and blockchain

Το blockchain (τεχνολογία συστοιχιών) είναι μία από τις σημαντικότερες εγευρέσεις του 21ου αιώνα. Τεχνικά, το blockchain είναι μια χρονολογημένη αλληλουχία αμετάβλητων δεδομένων που διαχειρίζεται από μια συστοιχία υπολογιστών που δεν είναι ιδιοκτησία ενός χρήστη ή μια οντότητας. Κάθε μία από αυτές τις καταγραφές δεδομένων, η οποία ονομάζεται συστοιχία ασφαλίζεται και συνδέεται με μία άλλη καταγραφή χρησιμοποιώντας κρυπτογραφικές εξισώσεις (Vucicic et al., 2018). Η τεχνολογία αυτή περιγράφηκε αρχικά από μια επιστημονική ομάδα το 1991. Ο βασικός της ρόλος ήταν η χρονοσήμανση ψηφιακών δεδομένων ώστε να είναι σχεδόν αδύνατη η προνοχρονολόγηση τους.

Το Bitcoin, αργότερα χρησιμοποίησε την τεχνολογία αυτή και εισήγαγε τα κρυπτονομίσματα που βασίζονται στην τεχνολογία συστοιχιών. Σήμερα, οι δυνατότητες

του blockchain χρησιμοποιούνται και στην έρευνα σε άλλους επιστημονικούς τομείς. Υπάρχει μεγάλη τάση τόσο στους χρήστες όσο και στην επιστημονική κοινότητα ότι το blockchain είναι η τεχνολογία του μέλλοντος. Η τεχνολογία αυτή, είναι ουσιαστικά κατανεμημένο καθολικό το οποίο είναι προσβάσιμο από όλους. Είναι ένα δίκτυο υπολογιστών (ονομάζονται κόμβοι) που περιέχει το ίδιο ιστορικό συναλλαγών και επικυρώνεται από κάθε νέο υπολογιστή που θέλει να γίνει μέλος του δικτύου αυτού. Το blockcain έχει τη μορφή που απεικονίζεται στην Εικόνα 9.



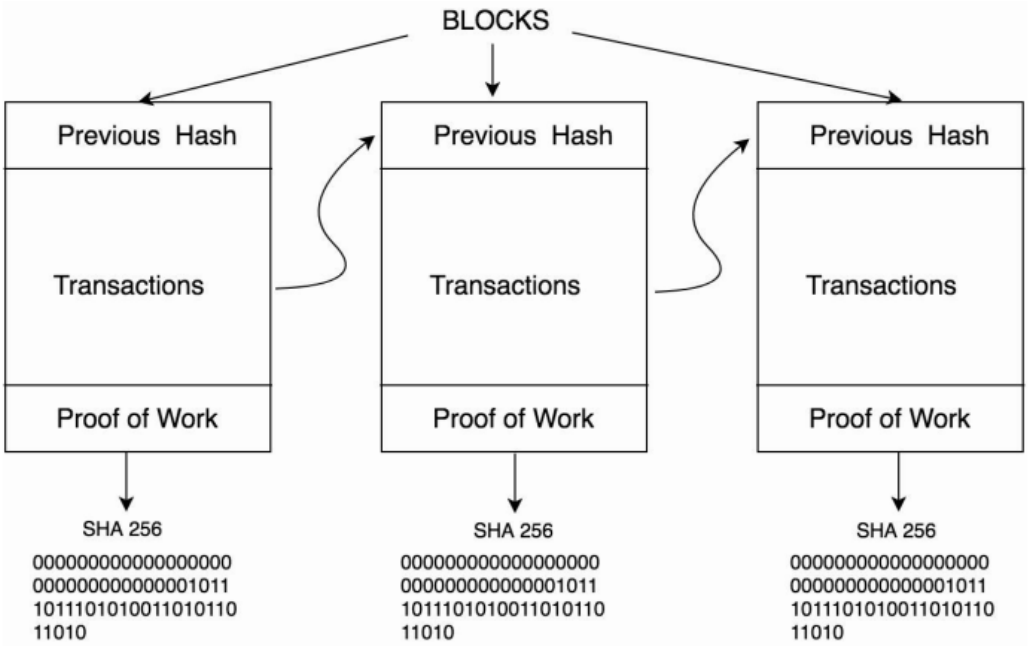
Εικόνα 9. η μορφή του blockchain.

Το bitcoin αποτελείται από αλυσίδες από blocks που είναι συνδεδεμένες μαζί η μία με την άλλη. Κάθε ένα από τα block δρα σαν δομικό υλικό για το blockchain. Το πρώτο block Που δημιουργήθηκε για το Bitcoin ονομάζεται genesis chain block, και έχει ύψος 0. Κάθε block που προστίθεται πάνω από το genesis block ψηλώνει το block chain κατά 1 μονάδα. Κάθε block περιέχει συγκεκριμένες πληροφορίες, όπως το μέγεθός του, το συνολικό ποσό συναλλαγών, το συναλλαγή καθεαυτού και το μπλοκ κεφαλίδας. Η δομή ενός block φαίνεται στον Πίνακα 1 (Zheng et al., 2017).

Πίνακας 1. Η δομή ενός μπλοκ

Αντικείμενο	Περιγραφή
Μέγεθος μπλοκ	Το Μέγεθος του μπλοκ σε bytes
Κεφαλίδα μπλοκ	Κεφαλίδα για διάφορους τομείς
Μετρητής	Μετράει τις συνολικές συναλλαγές
Συναλλαγές	Οι συναλλαγές του μπλοκ

Κάθε μπλοκ αποτελείται από μια κεφαλίδα μπλοκ η οποία είναι η σύνοψη όλων των περιεχομένων του μπλοκ. Η κεφαλίδα περιέχει 6 διαφορετικά στοιχεία που δίνουν πληροφορίες για τα περιεχόμενα του μπλοκ. Στην περίπτωση του bitcoin, η ρίζα της κεφαλίδας είναι μια χρήσιμη περιγραφή κάθε συναλλαγής που έχει γίνει στο μπλοκ. Τα μπλοκ σε ένα blockchain συνδέονται μεταξύ τους με τέτοιο τρόπο ώστε το ισχύον μπλοκ να έχει την εξίσωση κατακερματισμού του προηγούμενου block. Επειδή κάθε μπλοκ συνδέεται με ένα άλλο στην αλυσίδα, μπορούμε να ιχνηλατήσουμε την πορεία του καθενός μέχρι πίσω στο genesis block. Η εξάρτηση και το δέσιμο των μπλοκ μεταξύ τους τα κάνει αποτελεσματικά σε επιθέσεις χάκερ. Πιο αναλυτικά η αλλαγή της πληροφορίας σε ένα μπλοκ, έχει σαν αποτέλεσμα την αλλαγή στην εξίσωση κατακερματισμού του συγκεκριμένου μπλοκ προκαλώντας σφάλμα σε όλα τα προηγούμενα μπλοκ, μέχρι το αρχικό. Η συνολική δομή ενός μπλοκ φαίνεται στην Εικόνα 10 (Ahram et al., 2017).

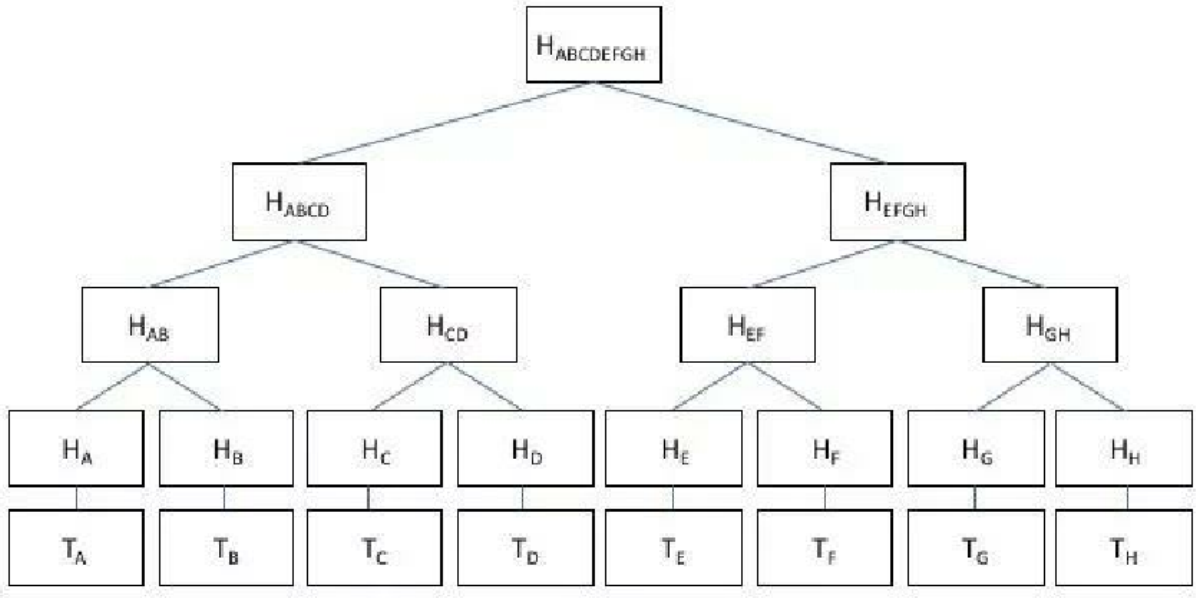


Εικόνα 10. Η αλυσίδα των μπλοκ στο blockchain

1.7 Το δέντρο Merkle

Το δέντρο Merkle είναι μια δυαδική δομή δεδομένων κατακερματισμού. Τα φύλλα του δέντρου περιέχουν τα δεδομένα (τις συναλλαγές δηλαδή). Ο αρχικός κόμβος που είναι ένα επίπεδο του δέντρου, έχει τον κατακερματισμό των δεδομένων αυτών και συνδέεται με ακόμη έναν κόμβο. Με αυτόν τον τρόπο σύνδεση συνεχίζει μέχρι τη βάση (ρίζες) του δέντρου. Ο κατακερματισμός των ριζών του δέντρου χρησιμοποιείται δημόσια και είναι εύκολο να επιβεβαιωθεί αν συγκεκριμένα δεδομένα κατακερματισμού ανήκουν στο δέντρο. Αυτό γίνεται εξετάζοντας μόνο το μπλοκ δεδομένων σε ένα φύλο και τη διαδρομή που ακολουθεί μέχρι τη ρίζα. Αν όλοι οι κατακερματισμοί είναι σωστοί, τότε το μπλοκ δεδομένων συμπεριλαμβάνεται στο δέντρο. Στην περίπτωση που υπάρχουν n κόμβοι σε ένα δέντρο, χρειάζεται περίπου log(n) χρόνος για να εξεταστούν τα μπλοκ δεδομένων (Dhumwald et al., 2017).

Στην Εικόνα 11, συμβολίζεται σαν H ο κατακερματισμός και σαν Τα η συνδιαλλαγή. Ο πρώτος κατακερματισμός αναφέρεται σαν ρίζα και οι ενδιάμεσοι κατακερματισμοί αναφέρονται σαν κλαδιά. Οι κατακερματισμοί στο κάτω μέρος της εικόνας είναι τα φύλλα.



Εικόνα 11. Το δέντρο Merkle

2. Εξόρυξη Bitcoin

Με τη λέξη εξόρυξη εννοούμε την διαδικασία παραγωγής bitcoin η οποία είναι λύση μαθηματικών γρίφων χρησιμοποιώντας hardware. Για την παραγωγή bitcoin χρησιμοποιούνται διαφορετικοί τύποι εξοπλισμού και χρειάζεται χρόνος. Αρχικά χρησιμοποιούνταν CPU όμως στη συνέχεια χρησιμοποιήθηκε και άλλος εξοπλισμός όπως GPU, FPGA και ASIC. Οι κεντρικές μονάδες επεξεργασίας (CPU) είναι ουσιαστικά η πρώτη γενιά εξοπλισμού που χρησιμοποιήθηκε για εξόρυξη κρυπτονομισμάτων, και η διαδικασία έτρεχε έναν κώδικα που υπολόγιζε το SHA-256 μέσω λογισμικού, ελέγχοντας αν το αποτέλεσμα είναι ένα έγκυρο block. Σε έναν προσωπικό υπολογιστή τελευταίας γενιάς, μπορεί να χρειαστεί αρκετά χρόνια για να βρεθεί ένα έγκυρο μπλοκ (Beck et al., 2018).

Για να ξεκινήσει κάποιος την εξόρυξη Bitcoin είναι υποχρεωτικό να συνδεθεί τόσο με το δίκτυο του κρυπτονομίσματος όσο και με άλλους κόμβους. Ουσιαστικά η εξόρυξη περιλαμβάνει 6 βασικές εργασίες:

1. Ο χρήστης που επιτελεί εξόρυξη ανιχνεύει τις συναλλαγές που γίνονται στο δίκτυο του οποίου είναι μέλος. Οι συναλλαγές αυτές θα πρέπει να επιβεβαιώνονται ελέγχοντας την ορθότητα των υπογραφών. Το βήμα αυτό γίνεται για να μετριάσει τις πιθανότητες για διπλές δαπάνες.
2. Πριν γίνουν μέλος του δικτύου bitcoin, τα άτομα που κάνουν εξόρυξη, πρέπει να διαθέτουν όλα τα προηγούμενα block που αποτελούν τμήμα του blockchain. Στη συνέχεια πρέπει να επικυρώσουν κάθε block, επικυρώνοντας κάθε συναλλαγή μέσα σε αυτό.
3. Τη χρονική στιγμή που ο χρήστης εξόρυξης διαθέτει την τελευταία έκδοση του blockchain, μπορεί να ξεκινήσει να δημιουργεί τα δικά του blocks. Για να γίνει αυτό, κατηγοριοποιούνται οι συναλλαγές σε ένα νέο block, το οποίο αποτελεί προέκταση του τελευταίου block.

4. Στη συνέχεια ο χρήστης πρέπει να βρει ένα κρυπτογράφημα, το οποίο να κάνει το block έγκυρο.
5. Αν υποθέσουμε ότι το block γίνεται δεκτό αφού βρεθεί ένα κρυπτογράφημα, δεν υπάρχει κάποια εγγύηση ότι το block αυτό θα είναι τμήμα της αλυσίδας συναίνεσης. Μόνο στην περίπτωση που και οι υπόλοιποι χρήστες δεχτούν το ίδιο block, το block αυτό γίνεται μέλος της αλυσίδας συναίνεσης (Eyal et al., 2014).

Η ανταμοιβή για την εξόρυξη Bitcoin, μειώνεται με την αύξηση των αριθμών Bitcoin που ανακαλύπτονται. Ο συνολικός αριθμός των Bitcoin που ανακαλύπτονται έχει ένα όριο (21 εκατομμύρια). Η ανταμοιβή αυτή, μειώνεται στο μισό κάθε φορά που εξορύσσονται 210.000 blocks. Η χρονική περίοδος που χρειάζεται να παρέλθει για την εξόρυξη των 210.000 block είναι περίπου 4 χρόνια. Στην παρούσα κατάσταση, η εξόρυξη για το χρονικό αυτό διάστημα ισοδυναμεί με 12.5 Bitcoin. Αρχικά, η ανταμοιβή για την εξόρυξη ήταν περίπου 50 Bitcoin (Kroll et al., 2013).

Εκτός όμως από την ανταμοιβή των χρηστών που επιτελούν εξόρυξη, οι χρήστες λαμβάνουν και το ποσό των συναλλαγών για κάθε επιτυχή προσθήκη συναλλαγής στο blockchain (Kroll et al., 2013). Γενικά, η προμήθεια συναλλαγής είναι περίπου το 1% της ανταμοιβής του block. Στην Εικόνα 12 μπορούμε να δούμε την μείωση στην ανταμοιβή των bitcoin μετά από την επιτυχή εξόρυξη 210.000 blocks ή μετά το πέρας της τετραετίας. Επειδή η μείωση αυτή είναι γεωμετρική, δεν μπορεί να υπάρχουν περισσότερα από 21 εκατομμύρια Bitcoin.

$$210{,}000\ (\ 50 + 25 + 12.5 + 6.25 + 3.125 + \ldots\ldots\ )\ \sim approx.\ 21{,}000{,}000\ Bitcoins$$

Time	BTC Reward
Jan 2009 - Nov 2012	50 BTC
Nov 2012 - Jul 2016	25 BTC
Jul 2016 - Feb 2020	12.5 BTC
Feb 2020 - Sep 2023	6.25 BTC

Εικόνα 12. Η μείωση των ανταμοιβών από την εξόρυξη bitcoin

Η δυσκολία της εξόρυξης bitcoin αλλάζει κάθε 2016 block. Ο χρόνος που απαιτείται για την εξόρυξη των block αυτών είναι περίπου 2 εβδομάδες. Από το γεγονός αυτό, φαίνεται ότι η δυσκολία της εξόρυξης bitcoin επαναυπολογίζεται μία φορά κάθε δύο εβδομάδες, Η εξίσωση υπολογισμού της δυσκολίας εξόρυξης Bitcoin είναι:

$$new\_difficulty = (old\_difficulty * 2016 * 10\ min) / (total\ time\ to\ mine\ previous\ 2016\ blocks)$$

Επομένως θα πάρει περίπου δύο εβδομάδες να γίνει εξόρυξη 2016 block αν ένα block παράγεται ακριβώς κάθε 10 λεπτά. Η δυσκολία της διαδικασίας εξόρυξης παραμετροποιείται ανάλογα με τη δύναμη εξόρυξης του δικτύου. Αν στο δίκτυο συνδεθούν περισσότεροι χρήστες εξόρυξης, η δυσκολία αυξάνεται και η λύση του προβλήματος είναι πιο δύσκολη. Αντίστοιχα, στην περίπτωση που πολλοί χρήστες αποσυνδεθού, η δυσκολία μειώνεται. Η αυξομείωση της δυσκολίας γίνεται για να ελέγχεται η ταχύτητα δημιουργίας των καινούριων block (Lewenberg et al., 2018).

2.1 Εξοπλισμός για εξόρυξη κρυπτονομισμάτων

Η εξόρυξη του Bitcoin είναι η διαδικασία δημιουργίας κρυπτονομισμάτων λύνοντας μια σειρά από πολύπλοκες μαθηματικές εξισώσεις χρησιμοποιώντας ειδικό εξοπλισμό. Πρέπει να ξεκαθαρίσουμε ότι για την εξόρυξη bitcoin απαιτείται εξοπλισμός (hardware). Υπάρχουν διάφορα είδη εξοπλισμών που χρησιμοποιούνται για τη διαδικασία αυτή ώστε με την πάροδο του χρόνου να ανακαλύψουν τμήματα Bitcoin, όμως αρχικά η εξόρυξη γινόταν με CPU.

2.2 Εξόρυξη με CPU

Οι κεντρικές υπολογιστικές μονάδες (Central Processing Units – CPUs) χρησιμοποιήθηκαν στην εξόρυξη του Bitcoin στα αρχικά στάδια. Θεωρείται σαν η πρώτη γενιά εξοπλισμού και η εξόρυξη ήταν τόσο απλή όσο να «τρέξει» η CPU έναν κώδικα όπως ο παρακάτω. Ο κώδικας ψάχνει για ένα κρυπτογράφημα με γραμμικό τρόπο και μετά υπολογίζει το SHA-256 με λογισμικό, ενώ τελικά ελέγχει αν το αποτέλεσμα είναι ένα έγκυρο τμήμα κρυπτονομίσματος. Το SHA-256 εφαρμόζεται στον κώδικα 2 φορές (Dev et al., 2014).

```
target  = ( 65535 << 208 ) / difficulty ;
coinbase_nonce = 0;
while ( 1 ) {
        header = blockHeader (transactions,coinbase_nonce);
        for ( header_nonce = 0 ; header_nonce < ( 1 << 32 ) ; header_nonce++ ) {
                if  ( SHA256 ( SHA256 ( blockHeader ( header , header_nonce ) ) ) <  target )
                        Break;      // block is found
        }
 coinbase_nonce++;
}
```

Σε έναν υπολογιστή με υψηλές προδιαγραφές η υπολογιστική ικανότητα φτάνει περίπου τους 20 εκατομμύρια κατακερματισμούς το δευτερόλεπτο (M/s). Με αυτήν την ταχύτητα χρειάζεται αρκετά χρόνια, κατά μέσο όρο, για να ανακαλυφτεί ένα τμήμα που είναι έγκυρο.

2.3 Εξόρυξη με GPU

Η εξόρυξη με τη βοήθεια GPU θεωρείται σαν εξόρυξη Bitcoin δεύτερης γενιάς. Η εξόρυξη με GPU ξεκίνησε λόγω της χαμηλής υπολογιστικής ικανότητας των CPU. Το βασικότερο πλεονέκτημα της εξόρυξης με αυτό τον εξοπλισμό, είναι ότι η GPU έχει καλύτερες επιδόσεις σε σχέση με το χρόνο αλλά δεν μπορεί να ανταποκριθεί στην αυξανόμενη δυσκολία των εξισώσεων με την πάροδο του χρόνου. Επίσης, κατά την εξόρυξη με GPU παρατηρείται υπερθέρμανση και χρήση του εξοπλισμού στον μέγιστο βαθμό με αποτέλεσμα την ταχύτερη φθορά του (Taylor et al., 2017).

2.4 Εξόρυξη με FPGA

Η εξόρυξη με FPGA θεωρείται ως η τρίτη γενιά εξόρυξης Bitcoin. Μετά την υλοποίηση στον εξοπλισμό με το όνομα Verilog, αρκετοί χρήστες που χρησιμοποιούσαν GPU άλλαξαν τον εξοπλισμό τους σε FPGA. Η υπολογιστική ισχύς του FPGA ήταν πολύ καλύτερη από τις δύο προηγούμενες μεθόδους. Αργότερα, ωστόσο, ο αριθμός των χρηστών που έκαναν εξόρυξη αυξήθηκε, με αποτέλεσμα να αυξηθεί και η δυσκολία του δικτύου. Λόγω αύξησης στη δυσκολία της εξόρυξης τμημάτων του κρυπτονομίσματος, η συγκεκριμένη μέθοδος δεν ανταποκρινόταν στις απαιτήσεις των χρηστών (Εικόνα 12) (Oliveira et al., 2012).

Εικόνα 12. Εξόρυξη bitcoin με τη χρήση πολλαπλών FPGAs

2.5 Εξόρυξη με ASIC.

Η εξόρυξη με τη μέθοδο ASIC είναι η τέταρτη γενιά εξόρυξης κρυπτονομισμάτων. Είναι η μέθοδος που κυριαρχεί σήμερα στα δίκτυα κρυπτονομισμάτων. Ο κύριος λόγος που συμβαίνει αυτό, είναι γιατί τα ολοκληρωμένα κυκλώματα των ASIC σχεδιάζονται, κατασκευάζονται και βελτιστοποιούνται για τον αποκλειστικό σκοπό της εξόρυξης Bitcoin. Υπάρχουν ορισμένοι μεγάλοι προμηθευτές οι οποίοι παράγουν και προμηθεύουν σε πελάτες εξοπλισμό αυτής της μορφής. Μερικά παραδείγματα από εξοπλισμούς ASIC που χρησιμοποιούνται σήμερα είναι Antminer S9, Terminator T3, Dragonmint T1 (Εικόνα 13) (Magaki et al., 2016).

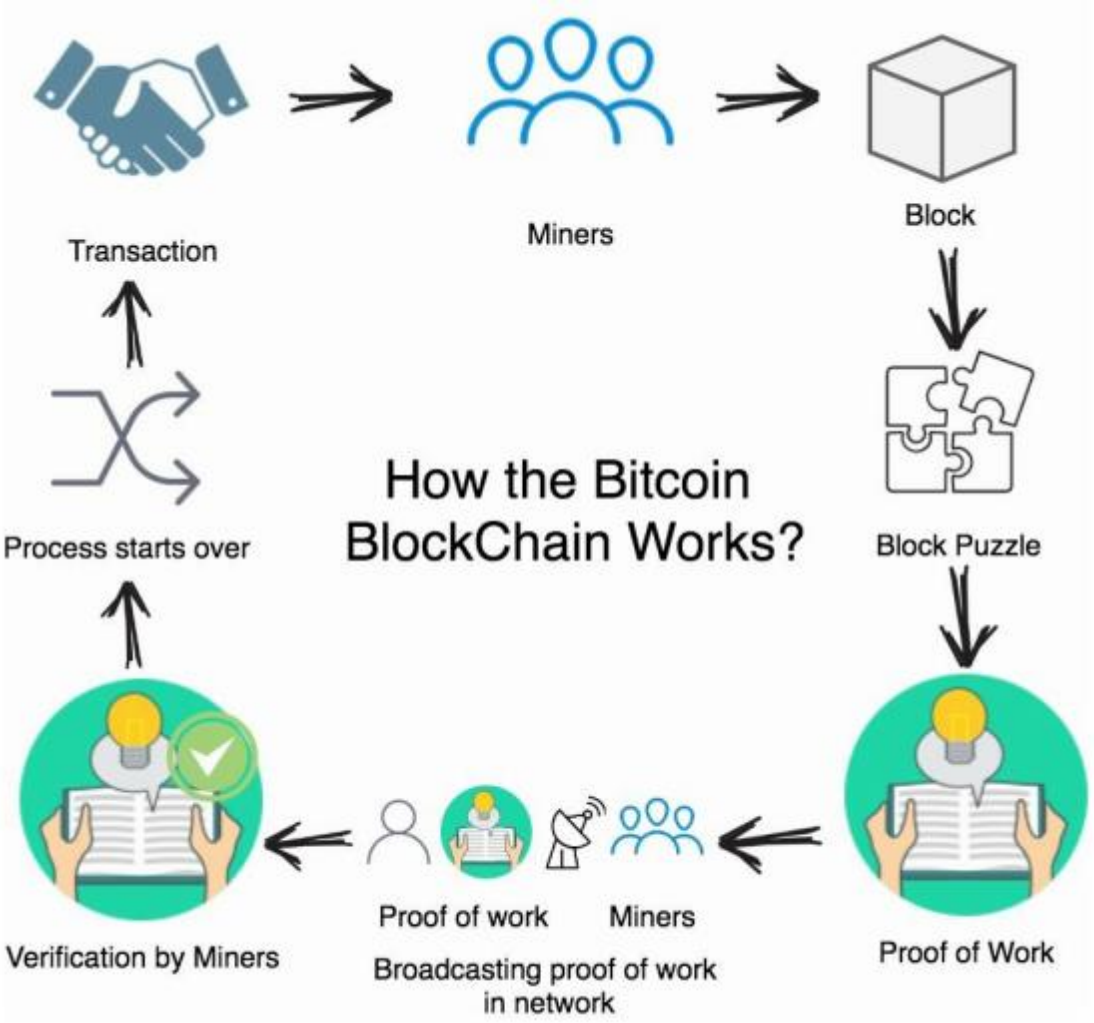
Εικόνα 13. το Antiminer S9 (ASIC εξοπλισμός για bitcoin)

Κατά τη διαδικασία της εξόρυξης, ο κάθε χρήστης πρέπει να αντιμετωπίσει το υψηλό κόστος της ενέργειας που καταναλώνει και την υπερβολική ζέστη που παράγει ο εξοπλισμός. Η εναλλακτική για την αντιμετώπιση αυτών των προβλημάτων είναι η χρήση cloud mining. Ωστόσο, και αυτός ο τρόπος έχει διάφορους περιορισμούς όπως το ρίσκο για απάτη, το χαμηλότερο κέρδος και η έλλειψη ελέγχου και ευελιξίας. Καθώς η εξόρυξη εξελίσσεται, όλο και περισσότερες εταιρείες ξεκινούν την κατασκευή εξοπλισμού που είναι εξειδικευμένος στην εξόρυξη κρυπτονομισμάτων. Τα πιο δημοφιλή μηχανήματα εξόρυξης στην αγορά αυτή τη στιγμή είναι τα:EBIT E11++, Terminator T3, Antminer S15, DragonMint T1, Antiminer S9, Avalonminer 841. Τα τεχνικά χαρακτηριστικά των μηχανημάτων αυτών φαίνεται στον παρακάτω Πίνακα (Derk et al., 2018).

Πίνακας 2. Τα τεχνικά χαρακτηριστικά του εξοπλισμού εξόρυξης Bitcoin.

SN	BTC Miner	Manufacturer	Power consumption	Hash rate	Efficiency	Chip process	Noise level
1	Ebit E11++	Ebang	2000W	44TH/s	0.096 J/GH	10nm	75db
2	Terminator T3	Innosilicon	2100W	43TH/s	0.098J/Gh	10nm	75db
3.	Antminer S15	Bitmain	1600W	28TH/s		7nm	75db
4	DragonMint T1	Halong Mining	1480W	16TH/s	0.0925J/GH	10nm	75db
5	Antminer	Bitmain	1350W	14.5TH/s	0.093J/GH	16nm	76db
6	AvalonMiner 841	Canaan	1290W	13.6TH/s	0.099J/GH	16nm	65db

Ο χρήστης ο οποίος κάνει εξόρυξη, χρησιμοποιεί τη υπολογιστική δύναμη του εξοπλισμού του προκειμένου να λύσει ένα πολύπλοκο μαθηματικό γρίφο και να επικυρώσει το τμήμα του κρυπτονομίσματος που ανακαλύπτει. Η εξόρυξη bitcoin είναι η διαδικασία πρόσθεσης συναλλαγών σε ένα αρχείο ορατό από τους άλλους χρήστες (δημόσιο αρχείο). Μια συναλλαγή θεωρείται έγκυρη όταν ο χρήστης την έχει υπογράψει. Για το λόγο αυτό, η δυσκολία εξόρυξης δυσκολεύει όσο περισσότεροι χρήστες εισέρχονται στο δίκτυο. Το πρωτόκολλο Bitcoin, διαφοροποιείται με τέτοιον τρόπο ώστε κάθε τμήμα να επαληθεύεται και να προστίθεται στην blockchain κάθε δέκα περίπου λεφτά. Η ανταμοιβή παρέχεται στο χρήση ο οποίος εξορίσει με επιτυχία ένα τμήμα bitcoin. Το τμήμα το οποίο έχει Proof of Work θεωρείται ότι είναι έγκυρο. Οι χρήστες που κάνουν εξόρυξη ανταμείβονται με ένα bitcoin (στην παρούσα φάση είναι 12.5 Bitcoin ανά τμήμα) για την εργασία τους της επαλήθευσης ενός τμήματος. Εκτός από την ανταμοιβή αυτή οι χρήστες λαμβάνουν και μια προμήθεια συναλλαγής από όλες τις συναλλαγές που συμπεριλαμβάνονται στο τμήμα αυτό. Αυτό το σύστημα ανταμοιβών ενθαρρύνει τους χρήστες να κάνουν εξόρυξη. Τα γενικό πλάνο εργασίας των χρηστών δείχνεται στην Εικόνα 14 (Wang et al., 2015).



Εικόνα 14. Ο μηχανισμός λειτουργίας του bitcoin blockchain

Τα βήματα με τα οποία τρέχει το δίκτυο είναι τα ακόλουθα:

- Νέες συναλλαγές εκπέμπονται σε όλους τους κόμβους του δικτύου
- ΟΙ χρήστες επιβεβαιώνουν αν οι συναλλαγές αυτές είναι έγκυρες
- Οι καινούριες συναλλαγές κατηγοριοποιούνται σε ένα block από κάθε κόμβο
- Κάθε κόμβος εργάζεται στο να αναζητάει μία έγκυρη proof of work για το κάθε block
- Όταν ο κόμβος βρει μια έγκυρη proof of work μεταδίδει το block σε κάθε κόμβο του δικτύου
- Οι κόμβοι δέχονται το block μόνο αν όλες οι συναλλαγές είναι έγκυρες

- Οι κόμβοι εκφράζουν την αποδοχή στο block δημιουργώντας το επόμενο block στην αλυσίδα, χρησιμοποιώντας το hash του προηγούμενου block (Naik et al., 2013).

2.6 Proof of Work (PoW)

Ο PoW είναι ένας αλγόριθμος συναίνεσης που δημιουργήθηκε για πρώτη φορά από το Bitcoin, αλλά χρησιμοποιείται ευρέως και από άλλα κρυπτονομίσματα. Αποτελείται από ένα πολύπλοκο κρυπτογραφικό μαθηματικό γρίφο. Ο αλγόριθμος ψάχνει μια τιμή που ονομάζεται nonce (number only used once – μοναδικός αριθμός). Ο μοναδικός αυτός αριθμός είναι χρησιμοποιείται στην κεφαλίδα του block, την οποία αλλοιώνουν οι χρήστες με σκοπό να αλλάξουν την τιμή του hash. Η τιμή του μοναδικού αυτού αριθμού ξεκινάει με έναν συγκεκριμένο αριθμό από μηδενικά (Bentof et al., 2016). Η εκθετική παράγωγος του αριθμού των μηδενικών είναι το σωστό hash το οποίο και προσδιορίζει το μέσο όρο του χρόνου που πρέπει να δαπανηθεί για την εξόρυξη ενός συγκεκριμένου τμήματος. Αυτό σημαίνει ότι ο αλγόριθμος PoW περιέχει μεγάλο τμήμα του υπολογισμού που συμβαίνει στη διαδικασία ταυτοποίησης. Αυτή η υπολογιστική εργασία γίνεται από τους χρύστες εξόρυξης οι οποίοι υπολογίζουν το hash ενός block με ένα διαφοροποιούμενο nonce. Πρέπει επίσης να σημειώσουμε ότι δεν υπάρχει ένα συγκεκριμένος τρόπος ή ένα μοτίβο με τον οποίο να διαφοροποιείται το nonce. Αντίθετα, η διαφοροποίησή του γίνεται τυχαία (Beccuti et al., 2017).

2.7 Στόχος

Ο στόχος είναι ένας αριθμός 256 – bit τον οποίο μοιράζονται όλοι οι χρήστες εξόρυξης. Ο στόχος επηρεάζει απ' ευθείας τη δυσκολία του Bitcoin: όσο πιο χαμηλός είναι ο στόχος τόσο πιο δύσκολο είναι να ανακαλύψεις ένα block. Μετά από κάθε hash, ο αριθμός συγκρίνεται με τον αριθμό – στόχο, και αν ο αριθμός αυτός είναι μικρότερος ή ίσος με τον αριθμό στόχο, ο χρήστης ανταμείβεται. Σε διαφορετική περίπτωση, ο μοναδικός αριθμός αυξάνεται και η διαδικασία επαναλαμβάνεται. Στην περίπτωση αυτή οι χρήστες εξόρυξης που είναι πιο γρήγοροι έχουν τις μεγαλύτερες πιθανότητες ανταμοιβής, ωστόσο η διαδικασία είναι τυχαία και για το λόγο αυτό έχουν πιθανότητα και οι χρήστες εξόρυξης που είναι πιο αργοί. Η τιμή στόχος επαναυπολογίζεται μετά από την εξόρυξη 2016 block. Παίρνει περίπου 14 ημέρες για την εξόρυξη 2016 τμημάτων. Ο αλγόριθμος εξόρυξης φαίνεται στην Εικόνα 15 (Gervais et al., 2016).

Algorithm 1: Mining Process

Nonce ← 0

While *nonce* < *232***do**

threshold ← ((216-1) << 208)/ *D(t)*

digest ← SHA - 256 (SHA - 256(*header)*)

if *digest* < *threshold* **then**

return *nonce*

end

else

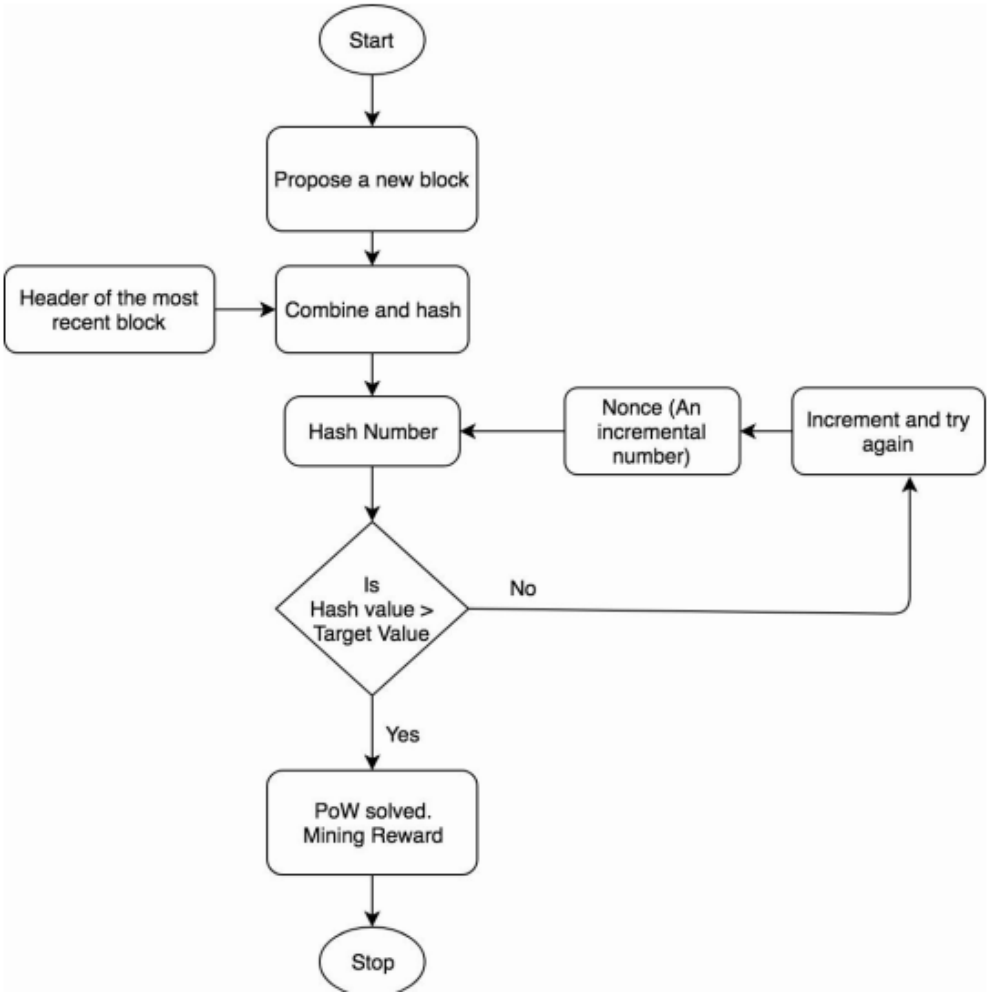
nonce ← *nonce* + 1

end

end

Εικόνα 15. Ο αλγόριθμος εξόρυξης

Το διάγραμμα ροής της διαδικασίας εξόρυξης φαίνεται στην Εικόνα 18.



Εικόνα 16. Το διάγραμμα ροής της διαδικασίας εξόρυξης

2.8 Η διαδικασία εξόρυξης

Για να γίνει κάποιος χρήστης εξόρυξης, η σύνδεση στο δίκτυο bitcoin και η σύνδεση με άλλου κόμβους είναι υποχρεωτική. Υπάρχουν 6 βασικές εργασίες οι οποίες απαιτούνται να εκτελεστούν από τους χρήστες εξόρυξης.

1. Ο χρήστης πρέπει να ανιχνεύει τις συναλλαγές που γίνονται στο δίκτυο. Πρέπει να επαληθεύει τις συναλλαγές αυτές με το να ελέγχει την ορθότητα των υπογραφών. Αυτό γίνεται για να περιοριστεί το πρόβλημα των διπλών δαπανών.
2. Πριν γίνουν μέλη του δικτύου, οι χρήστες πρέπει να διαθέτουν όλα τα προηγούμενα τμήματα που είναι μέρη του blockchain.
3. Όταν οι χρήστες διαθέτουν στην κατοχή τους την τελευταία έκδοση του blockchain μπορούν να ξεκινήσουν να κατασκευάζουν το δικό τους block.
4. Οι χρήστες πρέπει επίσης να βρουν έναν μοναδικό αριθμό που κάνει το block τους έγκυρο
5. Ας υποθέσουμε ότι το block γίνεται αποδεκτό μετά την εύρεση ενός μοναδικού αριθμού. Δεν είναι σίγουρο ότι ο το block αυτό θα είναι τμήμα της αλυσίδας συναίνεσης. Μόνο αν δεχτούν και οι άλλοι χρήστες το ίδιο block και ξεκινήσουν εξόρυξη πάνω σε αυτό, τα γίνει μέρος της αλυσίδας συναίνεσης (Chepurnoy et al., 2017).
6. Αν όλοι οι χρήστες εξόρυξης δεχτούν το block και το προσθέσουν στην δική τους αλυσίδα συναίνεσης, τότε ο χρήστης ο οποίος βρήκε τον μοναδικό αριθμό θα ανταμειφτεί.

2.9 Κατηγορίες εξόρυξης

Υπάρχουν δύο κύριες κατηγορίες εξόρυξης: η κοινή εξόρυξη (pool mining) και η κατ΄ ιδίαν εξόρυξη (solo mining). Η κατ' ιδίαν εξόρυξη, αναφέρεται στην εξόρυξη bitcoin από ένα άτομο χρησιμοποιώντας δικό του εξοπλισμού και δουλεύοντας ανεξάρτητα. Επειδή η κατηγορία αυτή αναφέρεται σε έναν και μόνο χρήστη, απαιτεί πολλούς πόρους, ώστε να ανταγωνιστεί άλλου χρήστες, ώστε τελικά να λύσει το block και να πάρει ο χρήστης την ανταμοιβή. Ωστόσο, η ανταμοιβή συλλέγεται μόνο από το χρήστη και το κέρδος είναι πολύ μεγαλύτερο, αν υπάρχει επαρκής εξοπλισμός. Το σημαντικότερο μειονέκτημα του solo mining είναι ότι μπορεί να πάρει χρόνια να γίνει εξόρυξη ακόμη και ενός μόνο block. Πριν την εισαγωγή της κοινής εξόρυξης, το 2011, όλοι οι χρήστες που ασχολούνταν με τα κρυπτονομίσματα έκανα κατ' ιδίαν εξόρυξη (Salimitary et al., 2017).

Η κοινή εξόρυξη είναι μια μέθοδος με την οποία οι χρήστες μοιράζονται μεταξύ τους τις πηγές, ώστε να παράγουν σταθερές ανταμοιβές. Κάθε κοινή εξόρυξη χρησιμοποιεί ένα μοναδικό ID για την εξόρυξη Bitcoin. Στην κοινή εξόρυξη, όλοι οι χρήστες, συνδυάζουν τον εξοπλισμό τους ώστε να έχουν μεγαλύτερη δύναμη εξόρυξης και η διαδικασία να είναι ταχύτερη σε σχέση με την κατ΄ ιδίαν εξόρυξη. Στη διαδικασία αυτή, η δυσκολία του προβλήματος που καλείται να επιλύσει ο κάθε χρήστης είναι μικρότερη σε σχέση με την κατ' ιδίαν (Recabarren et al., 2017).

3. Σύντομη ανασκόπηση της Βιβλιογραφίας

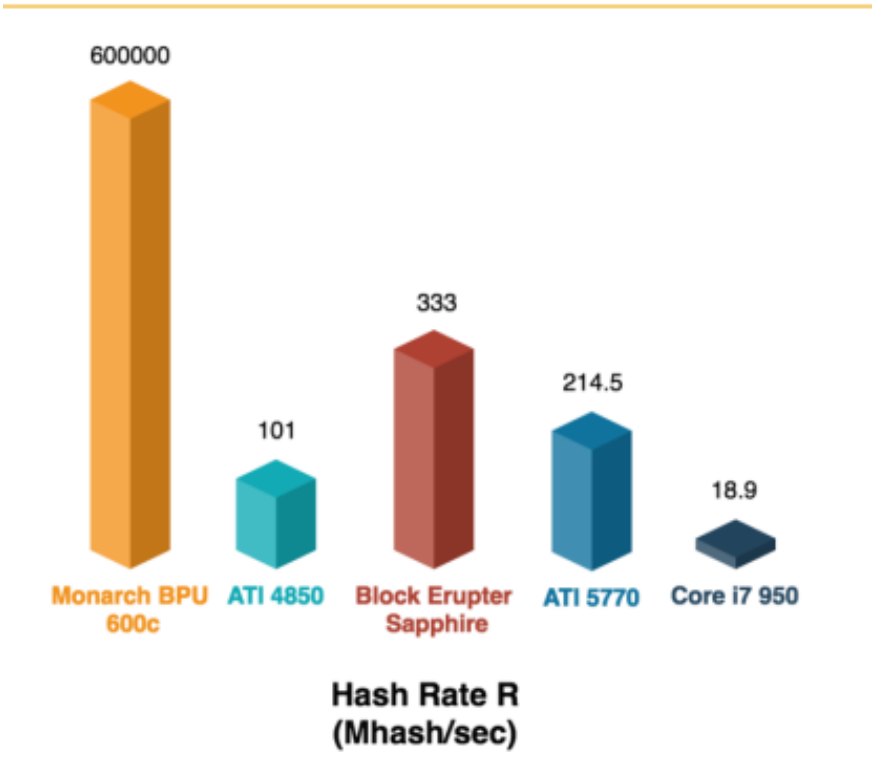
Το κρυπτονόμισμα bitcoin έχει κάνει αντίκτυπο διεθνώς. Τα τελευταία χρόνια, έχει αυξηθεί το ενδιαφέρον της κοινής γνώμης γύρω από το bitcoin και τα κρυπτονομίσματα γενικότερα. Αρκετοί είναι αυτοί που έχουν κάνει την εξόρυξη bitcoin επάγγελμα, αλλά αρκετές είναι και οι εταιρείες οι οποίες χρησιμοποιούν τα Bitcoin σαν μεθόδους συναλλαγής. Επειδή έχει περάσει μικρό χρονικό διάστημα από τη δημιουργία του Bitcoin, η ερευνητική προσπάθεια πάνω στον τομέα αυτό είναι διαρκής. Υπάρχουν κατηγορίες μελετών που αναλύουν διαφορετικές πτυχές του κρυπτονομίσματος όπως είναι η εξόρυξη, η ασφάλεια και οι επιθέσεις στην διαδικασία της κοινής εξόριξης. Οι Nakamoto et al., ανέλυσε με κάθε λεπτομέρεια το πρωτόκολλο του κρυπτονομίσματος στην αρχική του μελέτη το 2009. Αν και το bitcoin ήταν το πρώτο κρυπτονόμισμα η έννοια των κρυπτονομισμάτων προτάθηκε νωρίτερα, το 1983 από τον David Chaum (Fosso et al., 2018).

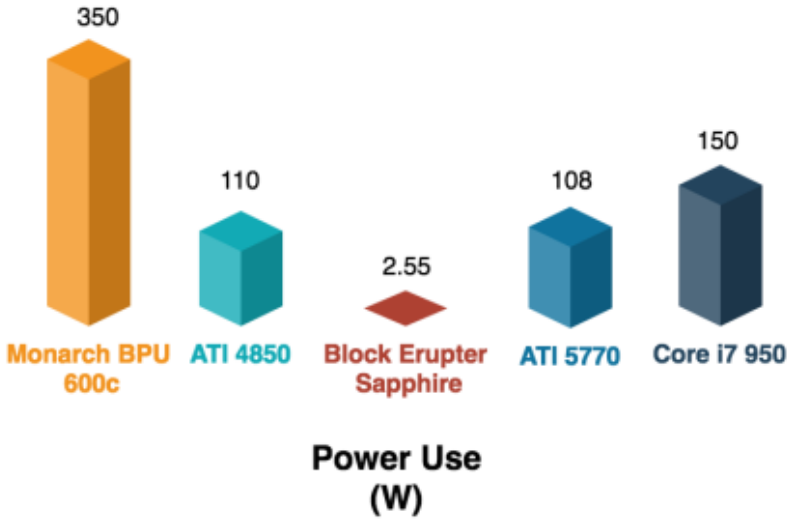
Μετά την πρόταση του Bitcoin, πολλά είναι τα κρυπτονομίσματα τα οποία προτάθηκαν. Τα περισσότερα από αυτά χρησιμοποιούν τον αλγόριθμο «proof of work", ωστόσο προτάθηκαν και μια σειρά από άλλους αλγόριθμους όπως Proof of Stake, Proof of activity, Proof of Capacity και Proof of burn. Ο λόγος της δημιουργίας ενός μεγάλου αριθμού αλγορίθμων ήταν το σημαντικό μειονέκτημα του αλγορίθμου Proof of work , δηλαδή η μεγάλη κατανάλωση ενέργειας. Η εμφάνιση του αλγορίθμου «Proof of Stake», ο οποίος είχε ως στόχο τη μείωση της κατανάλωσης ηλεκτρικής ενέργειας, είχε ως αποτέλεσμα να εμφανιστούν αρκετέ επιπλέον κρυπτονομίσματα όπως τα Peercoin, Dash, Cardano, KuCoin κλπ, τα οποία χρησιμοποιούν τον συγκεκριμένο αλγόριθμο (Kiyayas et al., 2017, Bentov et al., 2014).

Ο αρχικός εξοπλισμός που χρησιμοποιούνταν για την εξόρυξη των Bircoin ήταν ο CUDA miner, και εμφανίστηκε για πρώτη φορά στην αγορά το 2010. Σε σύντομο χρονικό διάστημα, όμως αναπτύχθηκε το κίνημα της ομαδικής εξόρυξης. Στο ανταγωνιστικό αυτό περιβάλλον, η κατ' ιδίαν εξόρυξη δεν είχε καμία αποτελεσματικότητα. Η πιθανότητα ανακάλυψης ενός block σε σχέση με την ενέργεια

που ξοδεύτηκε είναι μη συγκρίσιμη. Η συλλογική εξόρυξη έδωσε τη δυνατότητα στους χρήστες της κατ' ιδίαν εξόρυξης να συνεργαστούν και να συνδυάσουν τη δύναμη των εξοπλισμών τους ώστε να μοιραστούν το αποτέλεσμα. Αρκετές μελέτες εξηγούν γιατί σήμερα, η διαδικασία της κατ' ιδίαν εξόρυξης κρυπτονομισμάτων είναι ουσιαστικά σπατάλη χρόνου, εκτός αν υπάρχει μεγάλο αρχικό κεφάλαιο για την αγορά ASIC εξοπλισμού (Bhaskar et al., 2015, Velner et al., 2017).

Υπάρχουν αρκετές μελέτες γύρω από τον εξοπλισμό που χρησιμοποιείται για την εξόρυξη του Bitcoin. Τα πειράματα που αναφέρονται στις μελέτες αυτές, είναι απαραίτητα ώστε να κατανοήσουμε πως συμπεριφέρονται εξοπλισμοί διαφορετικών τύπων στην εξόρυξη του Bitcoin. Οι παράμετροι οι οποίοι αναλύονται συνήθως είναι ο ρυθμός κατακερματισμού, η αποτελεσματικότητα, η κατανάλωση ρεύματος και το κόστος. Η σύγκριση αυτή απεικονίζεται στην Εικόνα 13 (Stoll et al., 2019).





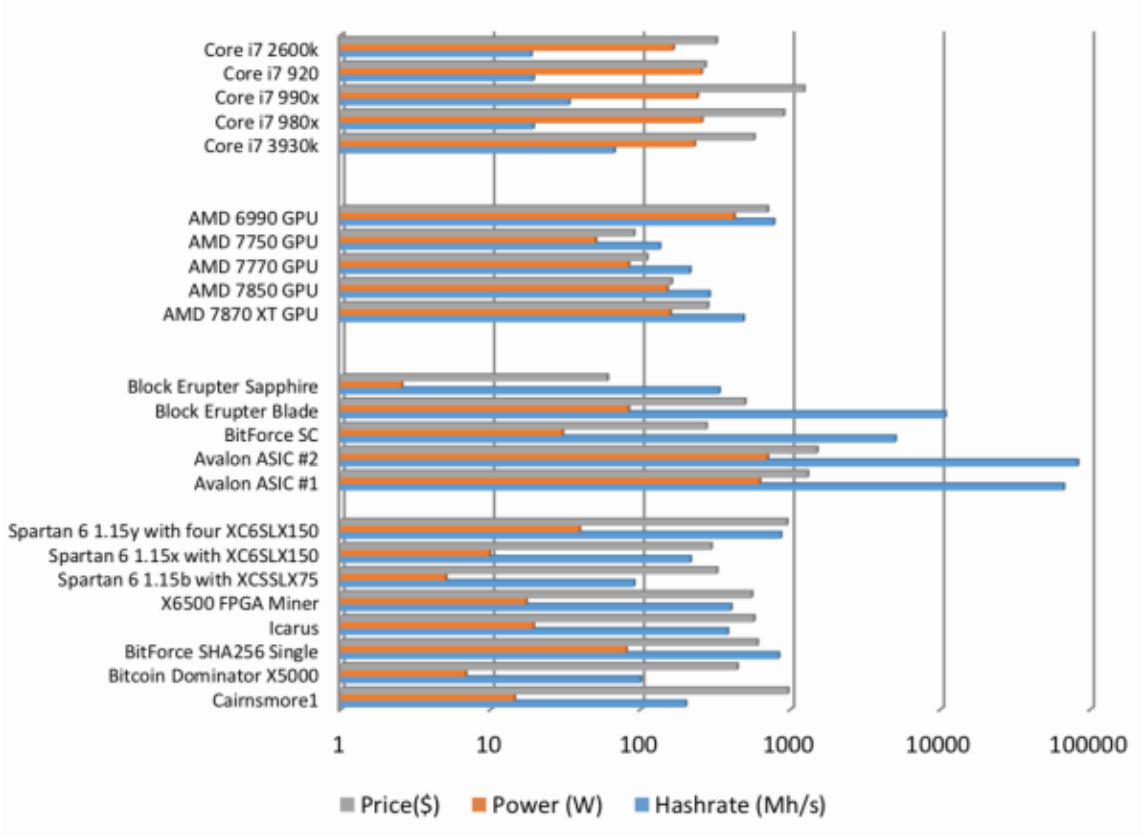
Εικόνα 13. Σύγκριση εξοπλισμού που χρησιμοποιείται για εξόρυξη, σε σχέση με το ρυθμό κατακερματισμού και το ρυθμό κατανάλωσης ενέργειας.

Σύμφωνα με την παραπάνω σύγκριση, ο μέγιστος ρυθμός κατακερματισμού αποδίδεται στο Monarch BPU 600c με 600.000 Mhash/sec, ωστόσο το συγκεκριμένο μηχάνημα καταναλώνει μεγάλα ποσά ενέργειας και έχει υψηλό κόστος. Ωστόσο, το ATI 5770 είναι φτηνό, με απόδοση 214.5 Mhas/sec καταναλώνοντας μόνο 108 wat ενέργειας. Από τη σύγκριση φαίνεται ότι το ATI 5770 είναι και η πιο αποδοτική επιλογή εξοπλισμού σε σχέση με τις υπόλοιπες (Εικόνα 14).

Name	Type	Hash Rate R (Mhash/s)	Power Use P (W)	Energy Efficiency $\mathcal{E}$ (Mhash/J)	Cost ($)
Core i7 950	CPU	18.9	150	0.126	350
Atom N450	CPU	1.6	6.5	0.31	169
Sony Playstation 3	CELL	21.0	60	0.35	296
ATI 4850	GPU	101.0	110	0.918	45
ATI 5770	GPU	214.5	108	1.95	80
Digilent Nexys 2 500K	FPGA	5.0	5	1	189
Monarch BPU 600 C	ASIC	600000.0	350	1714	2196
Block Erupter Sapphire	ASIC	333.0	2.55	130	34.99

Εικόνα 14. Σύγκριση εξοπλισμού για την εξόρυξη bitcoin.

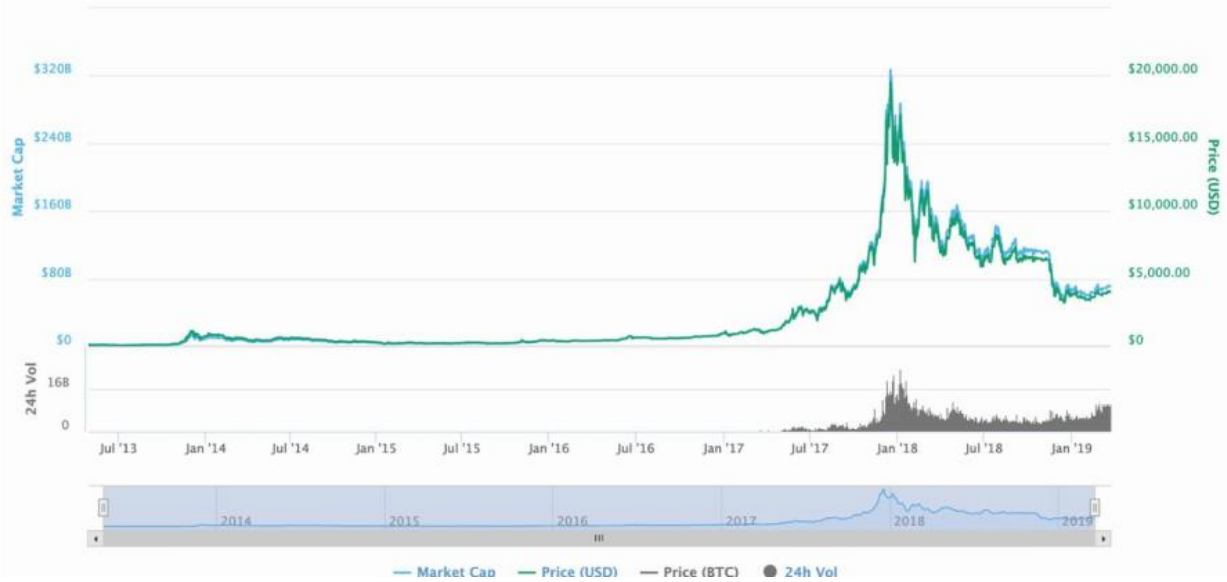
Αρκετές έρευνες έχουν δοκιμάσει την εξόρυξη bitcoin σε διαφορετικούς τύπους εξοπλισμού CPU, GPU και ASIC για να καταλήξουν στον αποδοτικότερο τρόπο. Με το πέρας του χρόνου, ωστόσο, αλλάζει τόσο η ποιότητα του εξοπλισμού, όσο και η ποσότητα των ατόμων που κάνουν εξόρυξη και αυτό αυξομειώνει τον ανταγωνισμό για την εξόρυξη ενός block. Η σύγκριση της τιμής, της δύναμης και του ρυθμού κατακερματισμού του εξοπλισμού εξόρυξης bitcoin κατά την μελέτη των Ho et al., φαίνεται στην Εικόνα 15.



Εικόνα 15. Σύγκριση εξοπλισμού βασιζόμενη στην τιμή, δύναμη και στο ρυθμό κατακερματισμού

4. Τα δεδομένα της αγοράς του Bitcoin.

Η αγορά του Bitcoin μεγαλώνει όλο και περισσότερο. Η κεφαλαιοποίηση της αγοράς είναι περίπου 68.8 δισεκατομμύρια $, με συνολική αξία συναλλαγών την ημέρα που πλησιάζει τα 9 δισεκατομμύρια $. Η κεφαλαιοαγορά του κρυπτονομίσματος φαίνεται από το Σεπτέμβριο του 2013 μέχρι και τον Ιανουάριο του 2019 φαίνεται στην Εικόνα 16 (Jiang et al., 2018).



Εικόνα 16. Η αύξηση της κεφαλαιαγοράς του bitcoin από το 2013 μέχρι το 2019.

Από το γράφημα της παραπάνω εικόνας, μπορούμε να συμπεράνουμε ότι το Ιανουάριο του 2017 η τιμή του Bitcoin ήταν περίπου 200 $. Από εκείνη τη χρονική στιγμή και μετά, υπήρχε μια εκθετική αύξηση της τιμής μέχρι το Δεκέμβριο του 2017, όπου και παρουσιάστηκε νέα μέγιστη τιμή του κρυπτονομίσματος και πιο συγκεκριμένα 1 BTC = 19.000 USD. Από τότε η τιμή έπεσε και αυξομοιώνεται με πιο ομαλούς ρυθμούς (Bariviera et al., 2017).

4.1 Πλεονεκτήματα των Bitcoin

Όπως είδαμε, το Bitcoin είναι ένα πρωτόκολλο που δεν έχει αποκλειστικό σκοπό την αποστολή χρημάτων από ένα σημείο Α σε ένα σημείο Β. Έχει πολλά ιδιαίτερα χαρακτηριστικά και διαφορετικές δυνατότητες πολλές από τις οποίες τώρα ανακαλύπτονται. Ωστόσο, έχει διαμορφωθεί σε προϊόντα και υπηρεσίες. Τα κυριότερα πλεονεκτήματά του είναι τα εξής:

- η προστασία από απάτες. Το πρωτόκολλο του bitcoin έχει εξαιρετικά δυνατό σύστημα ασφάλειας ακόμη και ενάντια στις πιο κακόβουλες επιθέσεις, ενώ κάνει την αντιγραφή των νομισμάτων εξαιρετικά δύσκολη διαδικασία. Οι χρήστες μπορούν να δημιουργήσουν αντίγραφα ασφαλείας του πορτοφολιού τους για να μη χάσουν τα κρυπτονομίσματα (Androulaki et al.., 2013).
- Παγκόσμια απήχηση. Όλες οι πληρωμές μπορεί να είναι διαλειτουργικές. Το Bitcoin επιτρέπει να γίνονται πληρωμές από οποιονδήποτε, οπουδήποτε και οποιαδήποτε ώρα, ανεξάρτητα από αν κάποιος διαθέτει τραπεζικό λογαριασμό ή όχι. Επιπλέον μπορεί να χρησιμοποιηθεί σε χώρες στις οποίες δεν υπάρχει πρόσβαση σε συμβατικές τράπεζες (Vergen et al., 2017)
- Εξοικονόμηση κόστους συναλλαγών. Η κρυπτογραφία ενεργοποιεί τις ασφαλείς πληρωμές και αποφεύγει τη χρήση δαπανηρών μεσαζόντων. Επιπλέον, οι συναλλαγές με bitcoin είναι πιο γρήγορες και πιο φτηνές σε σχέση με τις υπόλοιπες.
- Δωρεές. Το bitcoin μπορεί να αποτελέσει μια αποτελεσματική λύση για δωρεές και φιλοδωρήματα σε πολλές περιπτώσεις. Η πληρωμή μπορεί να γίνει μόνο με ένα click ή με έναν κώδικα QR. Επιπλέον, οι δωρεές μπορεί να είναι ορατές στο κοινό, δημιουργώντας διαφάνεια.
- Συμμετοχική χρηματοδότηση. Το bitcoin μπορεί να αποτελέσει έναν τρόπο χρηματοδότησης όπου χρειάζεται να συγκεντρωθεί ένα συγκεκριμένο ποσό χρημάτων ώστε να επιτευχθεί κάποιος στόχος.

Τέτοιου τύπου συμβόλαια μπορούν να παρατηρηθούν μέσα από το πρωτόκολλο του bitcoin, το οποίο απαγορεύει τις συναλλαγές πριν το συγκεκριμένο στόχο (Grosshoff et al., 2014).

- Εμπιστοσύνη και ακεραιότητα. Το bitcoin παρέχει μια λύση στο πρόβλημα της εμπιστοσύνης το οποίο επηρεάζει τις τράπεζες. Με το πρωτόκολλο του κρυπτονομίσματος, προετοιμάζεται το έδαφος για διαύγεια στις συναλλαγές, συναλλαγές μη αναστρέψιμες και ψηφιακά συμβόλαια. Επίσης μπορεί να χρησιμοποιηθεί και σαν πλατφόρμα εμπιστοσύνης στις τραπεζικές συναλλαγές.
- Αυτοματοποιημένες λύσεις. Συνήθως οι αυτοματοποιημένες λύσεις αναστέλλονται λόγω περιορισμών στο κόστος και λόγω των πληρωμών με πιστωτικές κάρτες. Το Bitcoin μπορεί να χρησιμοποιηθεί στις ηλεκτρονικές υπηρεσίες σαν τρόπος περιορισμού του κόστους λειτουργίας (Vergne et al., 2017).

5. Πρόβλεψη τιμών Bitcoin

Όπως προαναφέραμε, η τιμή του Bitcoin, αυξομοιώνεται όπως ακριβώς συμβαίνει και με τις μετοχές και τα υπόλοιπα νομίσματα. Προκειμένου να προβλεφτεί η τιμή του bitcoin στην αγορά, χρησιμοποιούνται ένας μεγάλος αριθμός από αλγόριθμους. Ωστόσο οι αλγόριθμοι πρόβλεψης των τιμών bitcoin είναι διαφορετικοί σε σχέση με του αλγόριθμους πρόβλεψης των τιμών των υπόλοιπων νομισμάτων ή των μετοχών, επειδή το bitcoin επηρεάζεται από διαφορετικούς παράγοντες. Η πρόβλεψη της τιμής του bitcoin είναι απαραίτητη ώστε να λαμβάνονται οι σωστές αποφάσεις επενδύσεων. Η τιμή του Bitcoin δεν εξαρτάται από επιχειρηματικές εκδηλώσεις ή από την παρεμβαίνουσες αρχές των κυβερνήσεων, όπως γίνεται με το χρηματιστήριο. Επομένως, για να γίνουν οι βέλτιστες προβλέψεις της τιμής, μπορούμε να χρησιμοποιήσουμε την τεχνολογία της μηχανικής μάθησης (McNally et al., 2018).

Η έρευνα σχετικά με την πρόβλεψη της τιμής του bitcoin μέσω μηχανικής μάθησης έχει αρκετά κενά. Έχει χρησιμοποιηθεί μια μέθοδος λανθάνουσας πηγής για την πρόβλεψη της τιμής του Bitcoin η οποία απέδωσε 89% επιστροφή με αναλογία 4:1 (Shah et al., 2014). Υπάρχει επίσης μια μελέτη η οποία χρησιμοποιεί δεδομένα κειμένων από πλατφόρμες κοινωνικών δικτύων και από άλλες πηγές για να προβλέψει την τιμή του συγκεκριμένου κρυπτονομίσματος (Georgoula et al., 2015). Μια παρόμοια έρευνα ανάλυσε την σχέση μεταξύ της τιμής του Bitcoin και των tweets για το bitcoin στην μηχανή αναζήτησης google trend (Matta et al., 2015). Η μεθοδολογία αυτή, αντί να προβλέπει την τιμή, προέβλεπε τον όγκο συναλλαγών. Όλες οι παραπάνω μελέτες είχαν σαν μειονέκτημα το μικρό δείγμα και την ροπή που υπάρχει για λανθασμένες πληροφορίες μέσω των κοινωνικών δικτύων όπως είναι το Twitter και το Reddit. Η λανθασμένες αυτές πληροφορίες είχαν σαν αποτέλεσμα την εικονική αύξηση ή μείωση της πρόβλεψης για την τιμή του κρυπτονομίσματος. Στις συναλλαγές bitcoin η ρευστοποίηση είναι περιορισμένη και για το λόγο αυτό υπάρχει μεγαλύτερο ρίσκο για χειραγώγηση στην αγορά των κρυπτονομισμάτων. Για όλους τους παραπάνω λόγους, οι γνώμες από τα κοινωνικά δίκτυα δεν θεωρούνται πλέον κατάλληλη μέθοδος για την πρόβληςψη τιμών κρυπτονομισμάτων (Gu et al., 2006).

Μια ακόμη μέθοδος ανάλυσης της τιμής του bitcoin είναι οι μηχανές υποστήριξης διανυσμάτων (Support Vector Machines) και τα τεχνητά νευρωνικά δίκτυα (Artificial Neural Networks). Οι μέθοδοι αυτές αναφέρουν επιτυχία πρόβλεψης 55% και χρησιμοποιούν την αλυσίδα συστοιχιών του bitcoin (Greaves et al., 2015). Τα δεδομένα της αλυσίδας συστοιχιών έχουν επίσης χρησιμοποιηθεί σε συνδυασμό με μηχανές διανυσματικής υποστήριξης και μεθοδολογία τυχαίου δάσους με το αποτελέσματα να δείχνουν επιτυχία στις προβλέψεις τιμών της τάξεως του 97% χωρίς όμως να υπάρχει στην μελέτη διασταυρούμενη επαλήθευση (Madan et al., 2015).

Για την πρόβλεψη των τιμών των κρυπτονομισμάτων έχουν επίσης χρησιμοποιηθεί οι κυμματομορφές (wavelets). Οι μέθοδος αυτή χρησιμοποιεί της θετικές συσχετίσεις μεταξύ των αναζητήσεων στις μηχανές αναζήτησης και του ρυθμού κατακερματισμού με την δυσκολία εξόρυξης bitcoin και την τιμή (Kristoufek et al., 2014). Εξάλλου, η πρόβλεψη των τιμών bitcoin Μπορεί να θεωρηθεί ανάλογη της πρόβλεψης των τιμών των μετοχών και της αγοράς συναλλάγματος. Αρκετές μελέτες χρησιμοποιούν τα πολυστρωματικά επίπεδα για την πρόβλεψη της τιμής του συναλλάγματος (MultiLayer Perceptron). Ωστόσο η μεθοδολογία αυτή αναλύει μία μόνο παρατήρηση κάθε φορά. σε αντίθεση, η απόδοση από κάθε στρώμα σε ένα επαναλαμβανόμενο νευρωνικό δίκτυο (recurrent neural network) αποθηκεύεται και χρησιμοποιείται στην είσοδο του επόμενου νευρωνικού δικτύου. Με άλλα λόγια το νευρωνικό δίκτυο, σε αντίθεση με το σύστημα πουστρωματικών επιπέδων, σχηματίζει ένα είδος μνήμης. Το μήκος του δικτύου ονομάζεται και χρονικό διάστημα παράθυρου (Gilles et al., 2001).

Ακόμη μια μορφή επαναλαμβανόμενων νευρωνικών δικτύων είναι και το δίκτυο μακροπρόθεσμης και βραχυπρόθεσμης μνήμης (Long Short Term Memory 0 LSTM). Τα δίκτυα αυτά, εκτός από το γεγονός ότι έχουν μνήμη, μπορούν να επιλέξουν πια δεδομένα θα θυμούνται και ποια δεδομένα θα ξεχνούν, ανάλογα με τη βαρύτητα και την σημασία του κάθε χαρακτηριστικού. Έχουν δημοσιευτεί μοντέλα LSTM για πρόβλεψη χρονοσειρών, απόδοση των οποίων είναι στα ίδια επίπεδα με την απόδοση των νευρωνικών δικτύων. Ένα μειονέκτημα στην εκπαίδευση τόσο των LTSM όσο και των RNN είναι ο σημαντικός χρόνος που απαιτείται για τους υπολογισμούς. Για

παράδειγμα, ένα δίκτυο από 50 κόμβους, συγκρίνεται με την εκπαίδευση 50 ξεχωριστών κόμβων MLP (Gers et al., 2001).

Από το χρονικό σημείο που η NVIDIA ανακάλυψε το πλαίσιο CUDA το 2006, έχει αυξηθεί κατά πολύ η ανάπτυξη εφαρμογών που εκμεταλλεύονται το δυνατότητες παράλληλου υπολογισμού μιας GPU. Στις εφαρμογές αυτές συμπεριλαμβάνονται και εφαρμογές μηχανικής μάθησης (Steinkrau et al., 2005). Για παράδειγμα έχει αναφερθεί ότι η εκπαίδευση ενός νευρωνικού δικτύου γίνεται ακόμη και τρεις φορές πιο γρήγορα, αν χρησιμοποιηθεί μια GPU αντί μιας CPU. Επίσης σε άλλες μελέτες φαίνεται μια αύξηση στην ταχύτητα της ταξινόμησης 80 φορές πιο γρήγορα όταν ένα SVM εφαρμόζεται σε μια GPU σε σχέση με την εφαρμογή ενός SVM σε CPU. Επιπλέον, ο χρόνος εκπαίδευσης του δικτύου όταν εφαρμόζεται σε CPU ήταν 9 φορές μεγαλύτερος (Ciresan et al., 2010).

6. Παραδείγματα πρόβλεψης τιμών bitcoin με μεθόδους μηχανικής μάθησης

Στα παραδείγματα που θα αναλύσουμε στις παρακάτω παραγράφους, χρησιμοποιείται σαν σύνολο δεδομένων οι τιμές του κρυπτονομίσματος bitcoin, σε χρονικά διαστήματα μιας ώρας στις ημερομηνίες από 10 Οκτωβρίου 2015 μέχρι και 01 Μαρτίου του 2019. Ένα δείγμα του συνόλου δεδομένων απεικονίζεται στον Πίνακα 2.

Πίνακας 2. Δείγμα του συνόλου δεδομένων

Ημερομηνία	Άνοιγμα	Κλείσιμο	Χαμηλό	Υψηλό	Όγκος συναλλαγών
25-10-2018 23:00	6405.08	6408.66	6408.66	6408.66	0.04456267
25-10-2018 22:00	6397.5	6408.66	6394.84	6405.08	23.398 52208
25-10-2018 21:00	6396.56	6402.63	6393.99	6397.5	35.453 5606

Τα δεδομένα είναι διαθέσιμα από την ιστοσελίδα cryptodatadownoad.com.

Αρκετά είναι τα μοντέλα τα οποία έχουν προταθεί για την πρόβλεψη της κατεύθυνσης της αλλαγής στην τιμή του Bitcoin. Μοντέλα ταξινόμησης όπως λογιστική παλινδρόμησης (Logistic Regression) και μηχανές υποστήριξης διανυσμάτων (Support Vector Machines). Άλλα μοντέλα στηρίζονται στην φθίνοντες αλγόριθμους (Regression Algorithms) όπως είναι το μοντέλο Αυτοπαλίνδρομου κινητού μέσου όρου (Autorregressive Integrated Moving Average – ARIMA). Τέλος, έχουν προταθεί και εφαρμοστεί μοντέλα που βασίζονται στα επαναλαμβανόμενα νευρωνικά δίκτυα (Karasu et al., 2018,. Indera et al., 2017).

Για όλα τα μοντέλα που θα αναλυθούν σαν παραδείγματα, εξετάστηκε η απόδοση στην πρόβλεψη. Σκοπός είναι να εξετάσουμε πως οι παραδοχές που βρίσκονται πίσω από κάθε μοντέλο, επηρεάζουν την απόδοση των μοντέλων. Η σύνοψη των μεθόδων των μοντέλων αυτών απεικονίζονται παρακάτω:

6.1 Λογιστική παλινδρόμηση

Η λογιστική παλινδρόμηση είναι μια στατιστική μέθοδος που χρησιμοποιείται για την εξέταση ενός συνόλου δεδομένων στο οποίο υπάρχουν μία ή περισσότερες ξεχωριστές μεταβλητές οι οποίες επηρεάζουν το αποτέλεσμα. Το αποτέλεσμα εκφράζεται με μία διαιρεμένη μεταβλητή (υπάρχουν δηλαδή μόνο δύο πιθανά αποτελέσματα). Χρησιμοποιείται για να προβλέψει ένα δυαδικό αποτέλεσμα (1/0, Αλήθεια/ψέματα, ναι/όχι) στηριζόμενο σε ένα σύνολο από ανεξάρτητες μεταβλητές. Είναι ένα μοντέλο πρόβλεψης παλινδρόμησης στο οποίο οι εξαρτημένες μεταβλητές είναι απόλυτες. Χρησιμοποιεί την εκτίμηση μέγιστης πιθανότητας (Maximum Likelihood Estimation) για να αναπτύξει τις πιθανότητες με τις οποίες τα εφαρμοστεί η λογιστική παλινδρόμηση σε συγκεκριμένη κλάση (Madan et al., 2015).

Το μοντέλο απεικονίζεται στην παρακάτω εξίσωση:

$$h_\theta(x) = g(\theta^T x) = \frac{1}{1 + e^{-\theta^T x}}$$

Όπου, x είναι η είσοδος και θ η παράμετρος που πρέπει να μαθευτεί.

6.2 Μηχανές υποστήριξης διανυσμάτων

Όπως και στην περίπτωση της λογιστικής παλινδρόμησης, ο αλγόριθμος μηχανής υποστήριξης διανυσμάτων δίνει ένα αποτέλεσμα δυαδικής φύσης χωρίς να κάνει παραδοχές για το σύνολο των δεδομένων. Ο ταξινομητής λαμβάνεται από την βελτιστοποίηση του:

$$\begin{aligned} \min_{\gamma,w,b} \quad & \frac{1}{2}||w||^2 \\ \text{s.t.} \quad & y^{(i)}(w^T x^{(i)} + b) \geq 1, \; i = 1, \ldots, m \end{aligned}$$

όπου x είναι η είσοδος και w,b είναι οι παράμετροι που πρέπει να μαθευτούν από το σύστημα. Οι προβλέψεις γίνονται αναλύοντας την τιμή του wTx + b (Chen et al., 2020).

6.3 Auto Regressive Integrated Moving Average (ARIMA)

Το ARIMA είναι ένα μοντέλο που χρησιμοποιείται σε ανάλυση χρονολογικών σειρών αλλά και σε προβλέψεις. Οι τιμές του μοντέλου βασίζονται σε δεδομένα από χρονολογικές σειρές οι οποίες μετασχηματίζονται σε στάσιμε χρονολογικές σειρές. Οι προβλέψεις είναι μια γραμμική παλινδρόμηση χαρακτηριστικών όπως οι χρονικές διαφορές, και οι κυλιόμενοι μέσοι όροι. Η υλοποίηση την οποία εξετάζουμε προέρχεται από το στατιστικό πακέτο λογισμικού Statsmodel.

Στο ARIMA τα δεδομένα είναι διαφορετικά, δηλαδή, τα χαρακτηριστικά των τιμών του κρυπτονομίσματος, μετασχηματίζονται στην διαφορά μεταξύ των τιμών.

- p: ο αριθμός των αυτορυθμιζόμενων χαρακτηριστικών
- d: ο αριθμός των μη εποχικών διαφορών που χρειάζονται για τη στατιμότητα
- q: ο αριθμός των σφαλμάτων στην πρόβλεψη που γίνεται από την εξίσωση πρόβλεψης

$$\left(1 - \sum_{k=1}^{p} \alpha_k L^k\right)(1 - L)^d X_t = \left(1 - \sum_{k=1}^{q} \beta_k L^k\right)\epsilon_t$$

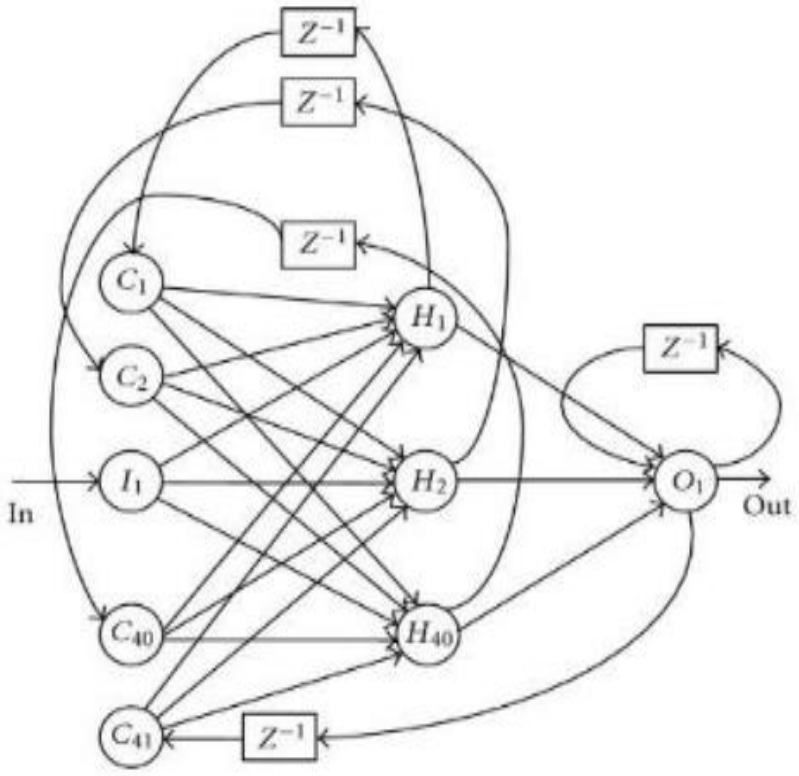
Όπου στην παραπάνω εξίσωση το L είναι τελεστής καθυστέρησης και οι p, d, q είναι υπερ-παράμετροι πάνω στις οποίες βελτιστοποιήθηκε. Για κάθε χρόνο t, εκπαιδεύεται ένα μοντέλο χρησιμοποιώντας το ιστορικό των τιμών για να προβλέψουμε την τιμή στο χρόνο t και για να χρησιμοποιήσουμε το πρόσημο της αλλαγής στην τιμή σαν πρόβλεψη (Rebane et al., 2018).

6.4 Επαναλαμβανόμενα Νευρωνικά δίκτυα

Τα επαναλαμβανόμενα νευρωνικά δίκτυα (Recurrent Neural Network – RNN) αναπτύχθηκαν για πρώτη φορά από τους Elman et al., Ένα RNN είναι παρόμοιο σε δομή με ένα MLP (Multi Layer Perceptron) με την εξαίρεση ότι τα σήματα μπορούν να ταξιδεύουν τόσο προς τα εμπρός όσο και προς τα πίσω με αλληλεπιδραστικό τρόπο. Για να γίνει εκμετάλλευση της αμφίδρομης αυτής ροής, έχει προστεθεί ένα επιπλέον επίπεδο το οποίο ονομάζεται Επίπεδο Πλαισίου. Εκτός ότι υπάρχει διακίνηση πληροφοριών μεταξύ των πλαισίων, η έξοδος κάθε πλαισίου εισάγεται στο Επίπεδο Πλαισίου για να εισαχθεί στο επόμενο επίπεδο με την επόμενη είσοδο. Με αυτή τη λογική, η κατάσταση αντικαθίσταται σε κάθε χρονικό σημείο. Το γεγονός αυτό,

προσφέρει το εξής πλεονέκτημα: επιτρέπει την ανάθεση συγκεκριμένων βαρών σε παραμέτρους που επηρεάζουν το δίκτυο σε σύγκριση με τα MLP, στα οποία τίθεται το ίδιο βάρος σε όλες τις εισόδους (Pant et al., 2018).

Στην συγκεκριμένη υλοποίηση, χρησιμοποιήθηκαν διαφορετικοί αριθμοί και μονάδες για τα επίπεδα, τους χρόνους εκπαίδευσης και τα μεγέθη των δεδομένων. Τα νευρωνικά δίκτυα υλοποιούνται με τις μεθόδους Keras και TensorFlow Στην Εικόνα 17 φαίνεται το διάγραμμα των επαναλαμβανόμενων νευρωνικών δικτύων (Jang et al., 2017).



Εικόνα 17 Διάγραμμα επαναλαμβανόμενων Νευρωνικών Δικτύων

7. Συμπεράσματα

Στα παραπάνω παραδείγματα περιγράφονται 4 μέθοδοι πρόβλεψης τιμής του Bitcoin: λογιστική παλινδρόμηση, μηχανή υποστήριξης διανυσμάτων, επαναλαμβανόμενα νευρωνικά δίκτυα και ARIMA. Οι ακρίβειες της πρόβλεψης για τις 4 αυτές μεθόδους φαίνονται στον Πίνακα 3. Από τις 4 μεθόδους, αυτή που έχει τη μεγαλύτερη ακρίβεια είναι η ARIMA, η οποία αποδίδει καλά για τις προβλέψεις τιμών επόμενης μέρας αλλά δεν έχει καλή απόδοση στις τιμές πρόβλεψης μετά από 5-7 ημέρες. Τα επαναλαμβανόμενα νευρωνικά δίκτυα έχουν καλή απόδοση στις προβλέψεις μέχρι 6 ημέρες.

Πίνακας 3. Πίνακας απόδοσης πρόβλεψης τιμών από διαφορετικές μεθόδους μηχανικής μάθησης

Μέθοδος	Ακρίβεια
Logistic regression	47%
SVM	48%
ARIMA	53%
RNN	50%

8. Συζήτηση

Ο σκοπός της μελέτης αυτής ήταν η ανασκόπηση της βιβλιογραφίας σχετικά με το θέμα των κρυπτονομισμάτων και ειδικότερα του Bitcoin. Βασιζόμενη στην πιοι πρόσφατη βιβλιογραφία, η μελέτη προσπάθησε να δώσει μια σφαιρική προσέγγιση του Bitcoin. Αρχικά, μελετήθηκε η ανάγκη για τη δημιουργία του κρυπτονομίσματος, η απαιτήσεις για την λειτουργία του αλλά και οι επιπτώσεις και οι δυσκολίες στην σύνθεση του πρωτοκόλλου του. Στη συνέχεια, αναλύθηκε η διαδικασία εξόρυξης και περιγράφηκαν οι κατηγορίες εξοπλισμού που δημιουργείται για την εξόρυξη.

Το κυριότερο μειονέκτημα του bitcoin είναι ότι είναι ευάλωτο στην κβαντική πληροφορική. Ωστόσο, οι κβαντικοί υπολογιστές δεν είναι τεχνολογία η οποία έχει αναπτυχθεί. Στην περίπτωση ανάπτυξης και κυκλοφορίας των κβαντικών υπολογιστών, τα κρυπτονομίσματα θα απειληθούν (Walch et al., 2015, Valfells et al., 2016).

Επομένως, οι χρήστες του Bitcoin πρέπει να είναι ιδιαίτερα προσεκτικοί την υιοθέτηση των κρυπτονομισμάτων σαν μέθοδο εμπορικών συναλλαγών. Εξάλλου, πολλοί από τους μελετητές των κρυπτονοισμάτων εκφράζουν προβληματισμούς σχετικά με τη χρήση τους από εγκληματικές και τρομοκρατικές οργανώσεις και την εκμετάλλευση της ανωνυμίας που παρέχει το σύστημα των κρυπτονομισμάτων (Reynolds et al., 2107).

Η τιμές του bitcoin, αυξομειώνονται όπως ακριβώς αυξομειώνονται και οι τιμές των μετιοχών και οι τιμές του συναλλάγματος. Επομένως, οι προβλέψεις των τιμών αυτών μπορούν να χρησιμοποιηθούν για την αύξηση των κεφαλαίων των χρηστών. Για το σκοπό αυτό έχουν προταθεί μια σειρά από αλγόριθμους πρόβλεψης τιμών. Οι αλγόριθμοι αυτοί έχουν διαφορετικά ποσοστά απόδοσης και επιτυχίας στην πρόβλεψη η οποία εξαρτάται και από το διάστημα πρόβλεψης (βραχυπρόθεσμο ή μακρυπρόθεσμο). Στη συγκεκριμένη πτυχιακή περιγράφουμε 4 αλγόριθμους μηχανικής μάθησης οι οποίοι προβλέπουν την τιμή του Bitcoin και συγκρίνουμε τις αποδόσεις τους.

9. Βιβλιογραφία

1. Androulaki, E., Karame, G. O., Roeschlin, M., Scherer, T., & Capkun, S. (2013, April). Evaluating user privacy in bitcoin. In *International Conference on Financial Cryptography and Data Security* (pp. 34-51). Springer, Berlin, Heidelberg.
2. Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., & Amaba, B. (2017, June). Blockchain technology innovations. In *2017 IEEE Technology & Engineering Management Conference (TEMSCON)* (pp. 137-141). IEEE.Biryukov, A., & Tikhomirov, S. (2019). Security and privacy of mobile wallet users in Bitcoin, Dash, Monero, and Zcash. *Pervasive and Mobile Computing*, *59*, 101030.
3. Bariviera, A. F., Basgall, M. J., Hasperué, W., & Naiouf, M. (2017). Some stylized facts of the Bitcoin market. *Physica A: Statistical Mechanics and its Applications*, *484*, 82-90.
4. Bhaskar, N. D., & Chuen, D. L. K. (2015). Bitcoin mining technology. In *Handbook of digital currency* (pp. 45-65). Academic Press.
5. Beck, R. (2018). Beyond bitcoin: The rise of blockchain world. *Computer*, *51*(2), 54-58.
6. Beccuti, J., & Jaag, C. (2017). The bitcoin mining game: On the optimality of honesty in proof-of-work consensus mechanism. *Swiss Economics Working Paper 0060*.
7. Bentov, I., Lee, C., Mizrahi, A., & Rosenfeld, M. (2014). Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract] y. *ACM SIGMETRICS Performance Evaluation Review*, *42*(3), 34-37.

8. Bentov, I., Gabizon, A., & Mizrahi, A. (2016, February). Cryptocurrencies without proof of work. In *International Conference on Financial Cryptography and Data Security* (pp. 142-157). Springer, Berlin, Heidelberg.
9. Chatterjee, J. M., Ghatak, S., Kumar, R., & Khari, M. (2018). BitCoin exclusively informational money: a valuable review from 2010 to 2017. *Quality & Quantity*, *52*(5), 2037-2054.
10. Chepurnoy, A., Duong, T., Fan, L., & Zhou, H. S. (2017). TwinsCoin: A Cryptocurrency via Proof-of-Work and Proof-of-Stake. *IACR Cryptology ePrint Archive*, *2017*, 232.
11. Chen, Z., Li, C., & Sun, W. (2020). Bitcoin price prediction using machine learning: An approach to sample dimension engineering. *Journal of Computational and Applied Mathematics*, *365*, 112395.
12. Cheng, Y., Du, D., & Han, Q. (2018, September). A Hashing Power Allocation Game in Cryptocurrencies. In *International Symposium on Algorithmic Game Theory* (pp. 226-238). Springer, Cham.
13. Cireşan, D. C., Meier, U., Gambardella, L. M., & Schmidhuber, J. (2010). Deep, big, simple neural nets for handwritten digit recognition. *Neural computation*, *22*(12), 3207-3220.
14. Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation*, *2*(6-10), 71.
15. Derks, J., Gordijn, J., & Siegmann, A. (2018). From chaining blocks to breaking even: A study on the profitability of bitcoin mining from 2012 to 2016. *Electronic Markets*, *28*(3), 321-338.

16. Dev, J. A. (2014, May). Bitcoin mining acceleration and performance quantification. In *2014 IEEE 27th Canadian Conference on Electrical and Computer Engineering (CCECE)* (pp. 1-6). IEEE.
17. Dhumwad, S., Sukhadeve, M., Naik, C., Manjunath, K. N., & Prabhu, S. (2017, September). A peer to peer money transfer using SHA256 and Merkle tree. In *2017 23RD Annual International Conference in Advanced Computing and Communications (ADCOM)* (pp. 40-43). IEEE.
18. Dimitri, N. (2017). Bitcoin mining as a contest. *Ledger*, *2*, 31-37.
19. Ding, D., Jiang, X., Wang, J., Wang, H., Zhang, X., & Sun, Y. (2019). Txilm: Lossy Block Compression with Salted Short Hashing. *arXiv preprint arXiv:1906.06500*.
20. Eskandari, S., Clark, J., Barrera, D., & Stobert, E. (2018). A first look at the usability of bitcoin key management. *arXiv preprint arXiv:1802.04351*.
21. Eyal, I., & Sirer, E. G. (2014, March). Majority is not enough: Bitcoin mining is vulnerable. In *International conference on financial cryptography and data security* (pp. 436-454). Springer, Berlin, Heidelberg.
22. Fan, C. I., Tseng, Y. F., Su, H. P., Hsu, R. H., & Kikuchi, H. (2019). Secure hierarchical bitcoin wallet scheme against privilege escalation attacks. *International Journal of Information Security*, 1-11.
23. Fosso Wamba, S., Kala Kamdjoug, J. R., Bawack, R., & G Keogh, J. (2018). Bitcoin, Blockchain, and FinTech: a systematic review and case studies in the supply chain. *Production Planning and Control*, *Forthcoming*.

24. Georgoula, I., Pournarakis, D., Bilanakos, C., Sotiropoulos, D., & Giaglis, G. M. (2015). Using time-series and sentiment analysis to detect the determinants of bitcoin prices. *Available at SSRN 2607167*.
25. Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., & Capkun, S. (2016, October). On the security and performance of proof of work blockchains. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security* (pp. 3-16).
26. Gerlach, J. C., Demos, G., & Sornette, D. (2019). Dissection of Bitcoin's multiscale bubble history from January 2012 to February 2018. *Royal Society open science*, *6*(7), 180643.
27. Gers, F. A., Eck, D., & Schmidhuber, J. (2002). Applying LSTM to time series predictable through time-window approaches. In *Neural Nets WIRN Vietri-01* (pp. 193-200). Springer, London.
28. Ghimire, S., & Selvaraj, H. (2018, December). A survey on bitcoin cryptocurrency and its mining. In *2018 26th International Conference on Systems Engineering (ICSEng)* (pp. 1-6). IEEE.
29. Giles, C. L., Lawrence, S., & Tsoi, A. C. (2001). Noisy time series prediction using recurrent neural networks and grammatical inference. *Machine learning*, *44*(1-2), 161-183.
30. Greaves, A., & Au, B. (2015). Using the bitcoin transaction graph to predict the price of bitcoin. *No Data*.
31. Groshoff, D. (2014). Kickstarter my heart: extraordinary popular delusions and the madness of crowdfunding constraints and bitcoin bubbles. *Wm. & Mary Bus. L. Rev.*, *5*, 489.

32. Gu, B., Konana, P., Liu, A., Rajagopalan, B., & Ghosh, J. (2006). Identifying information in stock message boards and its implications for stock market efficiency. In *Workshop on Information Systems and Economics, Los Angeles, CA*.
33. Indera, N. I., Yassin, I. M., Zabidi, A., & Rizman, Z. I. (2017). Non-linear autoregressive with exogeneous input (NARX) Bitcoin price prediction model using PSO-optimized parameters and moving average technical indicators. *Journal of Fundamental and Applied Sciences*, *9*(3S), 791-808.
34. Jang, H., & Lee, J. (2017). An empirical study on modeling and prediction of bitcoin prices with bayesian neural networks based on blockchain information. *Ieee Access*, *6*, 5427-5437.
35. Jiang, Y., Nie, H., & Ruan, W. (2018). Time-varying long-term memory in Bitcoin market. *Finance Research Letters*, *25*, 280-284.
36. Jin, T., Zhang, X., Liu, Y., & Lei, K. (2017, July). Blockndn: A bitcoin blockchain decentralized system over named data networking. In *2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN)* (pp. 75-80). IEEE.
37. Karasu, S., Altan, A., Saraç, Z., & Hacioğlu, R. (2018, May). Prediction of Bitcoin prices with machine learning methods using time series data. In *2018 26th Signal Processing and Communications Applications Conference (SIU)* (pp. 1-4). IEEE.
38. Kiayias, A., Russell, A., David, B., & Oliynykov, R. (2017, August). Ouroboros: A provably secure proof-of-stake blockchain protocol.

In *Annual International Cryptology Conference* (pp. 357-388). Springer, Cham.

39. Kristoufek, L. (2015). What are the main drivers of the Bitcoin price? Evidence from wavelet coherence analysis. *PloS one*, *10*(4).
40. Kroll, J. A., Davey, I. C., & Felten, E. W. (2013, June). The economics of Bitcoin mining, or Bitcoin in the presence of adversaries. In *Proceedings of WEIS* (Vol. 2013, p. 11).
41. Lewenberg, Y., Bachrach, Y., Sompolinsky, Y., Zohar, A., & Rosenschein, J. S. (2015, May). Bitcoin mining pools: A cooperative game theoretic analysis. In *Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems* (pp. 919-927).
42. Madan, I., Saluja, S., & Zhao, A. (2015). Automated bitcoin trading via machine learning algorithms. *URL: http://cs229. stanford. edu/proj2014/Isaac% 20Madan*, *20*.
43. Magaki, I., Khazraee, M., Gutierrez, L. V., & Taylor, M. B. (2016, June). Asic clouds: Specializing the datacenter. In *2016 ACM/IEEE 43rd Annual International Symposium on Computer Architecture (ISCA)* (pp. 178-190). IEEE.
44. Matta, M., Lunesu, I., & Marchesi, M. (2015, June). Bitcoin Spread Prediction Using Social and Web Search Media. In *UMAP Workshops* (pp. 1-10).
45. McNally, S., Roche, J., & Caton, S. (2018, March). Predicting the price of bitcoin using machine learning. In *2018 26th Euromicro International*

Conference on Parallel, Distributed and Network-based Processing (PDP) (pp. 339-343). IEEE.

46. Naik, R. P., & Courtois, N. T. (2013). Optimising the SHA256 Hashing Algorithm for Faster and More Efficient Bitcoin Mining. *MSc Information Security Department of Computer Science UCL*, 1-65.
47. Oliveira, S., Soares, F., Flach, G., Johann, M., & Reis, R. (2012). Building a bitcoin miner on an FPGA. In *XXVII SIM—South Symposium on Microelectronics*.
48. Pant, D. R., Neupane, P., Poudel, A., Pokhrel, A. K., & Lama, B. K. (2018, October). Recurrent neural network based bitcoin price prediction by twitter sentiment analysis. In *2018 IEEE 3rd International Conference on Computing, Communication and Security (ICCCS)* (pp. 128-132). IEEE.
49. Rebane, J., Karlsson, I., Denic, S., & Papapetrou, P. (2018). Seq2Seq RNNs and ARIMA models for cryptocurrency prediction: A comparative study. *SIGKDD Fintech*, *18*.
50. Recabarren, R., & Carbunar, B. (2017). Hardening stratum, the bitcoin pool mining protocol. *Proceedings on Privacy Enhancing Technologies*, *2017*(3), 57-74.
51. Reynolds, P., & Irwin, A. S. (2017). Tracking digital footprints: anonymity within the bitcoin system. *Journal of Money Laundering Control*.
52. Salimitari, M., Chatterjee, M., Yuksel, M., & Pasiliao, E. (2017, October). Profit maximization for bitcoin pool mining: A prospect theoretic approach. In *2017 IEEE 3rd international conference on collaboration and internet computing (CIC)* (pp. 267-274). IEEE.

53. Shah, D., & Zhang, K. (2014, September). Bayesian regression and Bitcoin. In *2014 52nd annual Allerton conference on communication, control, and computing (Allerton)* (pp. 409-414). IEEE.
54. Sorgente, M., & Cibils, C. (2014). The reaction of a network: Exploring the relationship between the bitcoin network structure and the bitcoin price. *No Data*.
55. Steinkraus, D., Buck, I., & Simard, P. Y. (2005, August). Using GPUs for machine learning algorithms. In *Eighth International Conference on Document Analysis and Recognition (ICDAR'05)* (pp. 1115-1120). IEEE.
56. Stoll, C., Klaaßen, L., & Gallersdörfer, U. (2019). The carbon footprint of bitcoin. *Joule*, *3*(7), 1647-1661.
57. Suresh, V. B., Satpathy, S. K., & Mathew, S. K. (2018). *U.S. Patent No. 10,142,098*. Washington, DC: U.S. Patent and Trademark Office.
58. Taylor, M. B. (2017). The evolution of bitcoin hardware. *Computer*, *50*(9), 58-66.
59. Valfells, S., & Egilsson, J. H. (2016). Minting money with megawatts [point of view]. *Proceedings of the IEEE*, *104*(9), 1674-1678.
60. Velner, Y., Teutsch, J., & Luu, L. (2017, April). Smart contracts make bitcoin mining pools vulnerable. In *International Conference on Financial Cryptography and Data Security* (pp. 298-316). Springer, Cham.
61. Vergne, J. P., & Swain, G. (2017). Categorical anarchy in the UK? The British media's classification of bitcoin and the limits of categorization. In *From categories to categorization: Studies in sociology, organizations and strategy at the crossroads* (pp. 185-222). Emerald Publ. Ltd.

62. Volety, T., Saini, S., McGhin, T., Liu, C. Z., & Choo, K. K. R. (2019). Cracking Bitcoin wallets: I want what you have in the wallets. *Future Generation Computer Systems*, *91*, 136-143.

63. Vujičić, D., Jagodić, D., & Ranđić, S. (2018, March). Blockchain technology, bitcoin, and Ethereum: A brief overview. In *2018 17th international symposium infoteh-jahorina (infoteh)* (pp. 1-6). IEEE.

64. Walch, A. (2015). The bitcoin blockchain as financial market infrastructure: A consideration of operational risk. *NYUJ Legis. & Pub. Pol'y*, *18*, 837.

65. Wang, L., & Liu, Y. (2015, March). Exploring miner evolution in bitcoin network. In *International Conference on Passive and Active Network Measurement* (pp. 290-302). Springer, Cham.

66. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE international congress on big data (BigData congress)* (pp. 557-564). IEEE.

67. Ziegeldorf, J. H., Matzutt, R., Henze, M., Grossmann, F., & Wehrle, K. (2018). Secure and anonymous decentralized Bitcoin mixing. *Future Generation Computer Systems*, *80*, 448-466.