



ΠΑΝΕΠΙΣΤΗΜΙΟ
ΠΑΤΡΩΝ
UNIVERSITY OF PATRAS

Μέθοδοι Εκτίμησης Ενεργειακής Κατανάλωσης στα Πλαίσια Κρυπτονομισμάτων

ΚΕΦΑΛΑΣ ΚΩΝΣΤΑΝΤΙΝΟΣ

Διπλωματική Εργασία που υπεβλήθη για τη μερική ικανοποίηση των απαιτήσεων για
την απόκτηση Μεταπτυχιακού Διπλώματος Ειδίκευσης

Σχολή Οργάνωσης και Διοίκησης Επιχειρήσεων
Τμήμα Οικονομικών Επιστημών

Μεταπτυχιακό Δίπλωμα Ειδίκευσης στην
«Εφαρμοσμένη Οικονομική και Ανάλυση Δεδομένων»

Ιούνιος 2021

Πανεπιστήμιο Πατρών, Τμήμα Οικονομικών Επιστημών
Κεφαλάς Κωνσταντίνος
2021 - Με την επιφύλαξη παντός δικαιώματος

Τριμελής Επιτροπή Επίβλεψης Διπλωματικής Εργασίας

Επιβλέπων : Μανώλης Τζαγγαράκης Επίκουρος Καθηγητής

Μέλος Επιτροπής: Σόγιακας Βασίλειος Αναπληρωτής Καθηγητής

Μέλος Επιτροπής: Κουνετάς Κωνσταντίνος Επίκουρος Καθηγητής

Η παρούσα διπλωματική εργασία με τίτλο

«Μέθοδοι Εκτίμησης Ενεργειακής Κατανάλωσης στα Πλαίσια Κρυπτονομισμάτων»

εκπονήθηκε από τον **Κωνσταντίνο Κεφαλά, Α.Μ 1017189**, για τη μερική ικανοποίηση των απαιτήσεων για την απόκτηση Μεταπτυχιακού Διπλώματος Ειδίκευσης στην «Εφαρμοσμένη Οικονομική και Ανάλυση Δεδομένων» από το Πανεπιστήμιο Πατρών και εγκρίθηκε από τα μέλη της τριμελούς επιβλέπουσας επιτροπής.

«Ποιο είναι το καλύτερο πρότυπο ανθρώπου;
Γενναίος και Άγιος! - Νίκος Καζαντζάκης (Αναφορά στο Γκρέκο).»

Η παρούσα διπλωματική εργασία αφιερώνεται στη μητέρα μου. Στον άνθρωπο που μου έδωσε το ζην και το εύ ζην. Χωρίς αυτήν δεν θα είχα φτάσει ως εδώ.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω αρχικά τον καθηγητή μου στο ΠΜΣ "Εφαρμοσμένη Οικονομική και Ανάλυση Δεδομένων" τον κύριο Μανώλη Τζαγγαράκη για την αμέριστη βοήθεια του στην ολοκλήρωσή της διπλωματικής μου εργασίας. Επίσης, θα ήθελα να ευχαριστήσω την μητέρα μου Αικατερίνη Κεφαλά και τις δύο μεγαλύτερες αδερφές μου, Σωτηρία και Ευαγγελία για την βοήθειά τους όλα αυτά τα χρόνια. Τέλος, θα ήθελα να ευχαριστήσω όλα τα παιδιά, τις συμφοιτήτριες και τους συμφοιτητές μου που γνώρισα στη σχολή και βοηθήσαμε ο ένας τον άλλον στην ολοκλήρωση των εργασιών μας. Ονομάζομαι Κεφαλάς Κωνσταντίνος, γεννήθηκα τον Αύγουστο του 1990 στη πρωτεύουσα της Ρούμελης, την Λαμία. Αποφοίτησα από το προπτυχιακό του τμήματος Οικονομικών Επιστημών του Πανεπιστημίου Πατρών τον Σεπτέμβρη του 2013, παιδί 23 χρονών, επέστρεψα σχεδόν 31. Δεν ξέρω πως τα κατάφερα να φτάσω ως εδώ, αλλά όλα στο τέλος άξιζαν και με το παραπάνω.

Περίληψη

Σήμερα και με την τεχνολογία που έχουμε, κάποια πράγματα που πριν κάποια χρόνια φαινόταν μακρινά όνειρα, κατά κάποιο τρόπο σήμερα τα βλέπουμε όχι μόνο να τα χρησιμοποιούμε στη καθημερινότητά μας, αλλά και να μπαίνουν στις συζητήσεις της ακαδημαϊκής κοινότητας. Ένα από αυτά τα επιτεύγματα της τεχνολογίας είναι και τα κρυπτονομίσματα. Όταν λέμε κρυπτονόμισμα, εννοούμε ένα ψηφιακό νόμισμα, το οποίο δεν έχει κάποια ύλη, δημιουργείται από έναν αλγόριθμο σε ένα υπολογιστή και σκοπός του είναι να διασφαλίσει την ασφάλεια των συναλλαγών για τις οποίες χρησιμοποιείται. Μετά το 2008 και ουσιαστικά την δημιουργία του bitcoin από τον Satoshi Nakamoto, τα κρυπτονομίσματα με βάση την τεχνολογία του blockchain και των αλγορίθμων τύπου PoW που χρησιμοποιούν έχουν γίνει αντικείμενο μελέτης από πολλούς επιστήμονες. Ένα σημαντικό ζήτημα που προκύπτει στη διαδικασία εξόρυξής τους (mining), είναι και η ενέργεια που καταναλώνουν. Και αυτό ακριβώς το ζήτημα θα προσπαθήσουμε να ερευνήσουμε στη συγκεκριμένη διπλωματική εργασία. Γενικά η τεχνολογία του blockchain θεωρείται αρκετά πρωτοποριακή διότι εξασφαλίζει σε μεγάλο βαθμό την ανωνυμία και επιπρόσθετα δεν χρειάζεται μία κεντρική αρχή για την επίβλεψη των όποιων συναλλαγών. Το ζήτημα όμως της κατανάλωσης ενέργειας, εγείρει σημαντικά ερωτήματα με αποτέλεσμα να αναστέλλει την ταχύτερη υιοθέτηση της. Μπορούμε να δούμε πόσο μεγάλη απήχηση είχε η εφαρμογή της τεχνολογίας του blockchain μέσω του bitcoin αν σκεφτούμε ότι σήμερα το συγκεκριμένο κρυπτονόμισμα παρουσιάζει κεφαλαιοποίηση αγοράς αρκετών δεκάδων δισεκατομμυρίων δολαρίων. Βέβαια η τεχνολογία του blockchain δεν εφαρμόζεται μόνο στη δημιουργία κρυπτονομισμάτων, αλλά μπορεί να χρησιμοποιηθεί και στο βιομηχανικό και στο δημόσιο τομέα καθώς προσφέρει ασφαλείς συναλλαγές. Η πιο γνωστή όμως εφαρμογή της τεχνολογίας του blockchain συνεχίζει να είναι ψηφιακό νόμισμα του bitcoin. Το σημαντικό ζήτημα όμως όπως ειπώθηκε και παραπάνω είναι τα τεράστια ποσά ενέργειας που χρειάζεται η τεχνολογία του blockchain με αποτέλεσμα τον προβληματισμό αρκετών ακόμα και το αν η εφαρμογή της είναι φιλική προς το περιβάλλον.

Λέξεις κλειδιά : κρυπτονόμισμα, blockchain, PoW, bitcoin

Summary

Today and with the technology we have, some things that some years ago seemed distant dreams, in a way today we see them not only to use them in our daily lives, but also to enter the discussions of the academic community. One of these advances in technology is cryptocurrencies. When we say cryptocurrency, we mean a digital currency, which has no material, is created by an algorithm on a computer and its purpose is to ensure the security of the transactions for which it is used. After the creation of bitcoin by Satoshi Nakamoto in 2008, cryptocurrencies based on blockchain technology and the PoW algorithms they use have been the subject of study by many scientists. An important issue that arises in their mining process is the energy they consume. And this is exactly the issue we will try to investigate in this dissertation. In general, blockchain technology is considered quite innovative because it largely ensures anonymity and in addition does not need a central authority to oversee any transactions. The issue of energy consumption, however, raises important questions, as a result of which it suspends its faster adoption. We can see how popular the application of blockchain technology through bitcoin was if we consider that today this cryptocurrency has a market capitalization of several tens of billions of dollars. Of course, blockchain technology is not only applied to the creation of cryptocurrencies, but can also be used in the industrial and public sectors as it offers secure transactions. But the most popular application of blockchain technology continues to be bitcoin digital currency. The important issue, however, as mentioned above, is the huge amounts of energy that blockchain technology needs, resulting in the concern of many even if its application is environmentally friendly.

Keywords: cryptocurrency, blockchain, PoW, bitcoin

Contents

1	Εισαγωγή	9
2	Bitcoin και άλλα κρυπτονομίσματα με βάση τον αλγόριθμο PoW	10
2.0.1	Σκοπός διπλωματικής εργασίας	10
2.0.2	Τί είναι το bitcoin και πως ξεκίνησε	10
2.0.3	Τρόπος λειτουργίας του bitcoin	13
2.0.4	Το πρόβλημα των double spend attack	15
2.0.5	Διαδικασία του mining	17
2.0.6	Πλεονεκτήματα και μειονεκτήματα του bitcoin	28
2.0.7	Άλλα κρυπτονομίσματα που βασίζονται στον αλγόριθμο PoW	31
2.0.8	Ο αλγόριθμος PoW και πως λειτουργεί	38
3	Επισκόπηση Βιβλιογραφίας	41
3.0.1	Βιβλιογραφική αναφορά των άρθρων και των αλγορίθμων μέτρησης κατανάλωσης ενέργειας που βασίστηκε η έρευνα	41
3.0.2	Καταγραφή των βάσεων δεδομένων για την αναζήτηση των αλ- γορίθμων μέτρησης της κατανάλωσης της ενέργειας στα κρυπτονομί- σματα.	46
3.0.3	Αριθμός των δημοσιεύσεων σε κάθε βάση δεδομένων	47
3.0.4	Καταγραφή των μεθόδων εκτίμησης της κατανάλωσης ενέργειας	48
4	Ανάλυση των δεδομένων	51
4.0.1	Ανάλυση των δεδομένων των αλγορίθμων εκτίμησης κατανάλ- ωσης ενέργειας - Συμπεράσματα ως προς τις μεθόδους και τα αποτελέσματα	51
4.0.2	Εκτίμηση κατανάλωσης ενέργειας μέσω του προγραμματιστικού περιβάλλοντος της Python	54
5	Συμπεράσματα	60

1 Εισαγωγή

Όσο αυξάνεται η ζήτηση των κρυπτονομισμάτων και παρόλο υψηλή μεταβλητότητα που έχουν αρκετές εταιρείες αλλά και ιδιώτες ενστερνίζονται αυτόν τον τρόπο πληρωμής, και σε νόμιμες αλλά και σε παράνομες συναλλαγές. Τα κρυπτονομίσματα είτε αυτό είναι το bitcoin, είτε είναι το Litecoin, είτε το Ethereum, ανά καιρούς έχουν αποκτήσει πολύ μεγάλες αποδόσεις, με το ερώτημα του κατά πόσο είναι σταθερά όσον αφορά την αξιοπιστία τους να είναι πάντα στο προσκήνιο. Μάλιστα έχουν γραφτεί και άρθρα όπως των Χαλβατζή και Συμίτη (2018) που ερευνούν το κατά πόσο είναι ευμετάβλητα και τί αποδόσεις μπορεί να έχουν για τις εταιρείες τεχνολογίες, με άλλα άρθρα να προσπαθούν να εντοπίσουν αν τα κρυπτονομίσματα μπορούν να λειτουργήσουν ως μία ασφαλής επένδυση και σταθεροποιητικός παράγοντας όπως είναι ο χρυσός (Bouri, Jalkh, Molnár, Roubaud, 2017). Με τον όρο κρυπτονομίσμα αυτό που εννοούμε είναι ένα ψηφιακό νόμισμα, για την ακρίβεια μία ψηφιακή περιουσία το οποίο προκύπτει μέσω ενός αλγορίθμου (PoW όπως το bitcoin) και μέσω μίας διαδικασίας κρυπτογράφησης είναι σε θέση να εξασφαλίσει τις συναλλαγές που γίνονται με βάση αυτό. Η δυσκολία της αντιγραφής ενός κρυπτονομίσματος (πάντα βέβαια ελοχεύουν κίνδυνοι όπως η περίπτωση του double spend attack) έγκειται στον αλγόριθμο κρυπτογράφησης που βασίζεται (τύπου SHA-256). Ένα ακόμη βασικό χαρακτηριστικό των κρυπτονομισμάτων και μία από τις βασικές διαφορές σε σχέση με τα κλασικά νομίσματα, είναι η απουσία κάποιας ρυθμιστικής αρχής για τον έλεγχο των συναλλαγών. Δηλαδή δεν υπάρχει κάποια ρυθμιστική αρχή όπως είναι η κεντρική Τράπεζα αλλά το δίκτυο του κάθε κρυπτονομίσματος ελέγχεται από το ίδιο το δίκτυό του μέσω της τεχνολογίας της αλυσίδας του blockchain που χρησιμοποιούν. Η συγκεκριμένη διπλωματική εργασία μελετά αλγορίθμους που υπολογίζουν την ενεργειακή κατανάλωση στα κρυπτονομίσματα και γίνεται αναφορά σε πάνω από 20 τρόπους εκτίμησης της ενέργειας. Μπορούμε να αναλογιστούμε μόνο ότι το δίκτυο του Bitcoin υπολογίζεται ότι καταναλώσει σε GJ όσο ενέργεια χρειάζεται περίπου χώρες σαν τη Δανία ή την Ισλανδία. Στη συνέχεια, στο τελευταίο μέρος της έρευνας παρουσιάζεται κάποιες εκτιμήσεις για την ενεργειακή κατανάλωση του ψηφιακού νομίσματος του Ethereum από το 2013 μέχρι και το 2021.

2 Bitcoin και άλλα κρυπτονομίσματα με βάση τον αλγόριθμο PoW

2.0.1 Σκοπός διπλωματικής εργασίας

Ο σκοπός για τον οποίο δημιουργείται η συγκεκριμένη διπλωματική εργασία είναι για να ρίξει φως, στα ζητήματα που αφορούν τους αλγόριθμους με τους οποίους υπολογίζεται η κατανάλωση ενέργειας στη διαδικασία δημιουργίας των κρυπτονομισμάτων. Από εκεί και πέρα θα παρουσιαστούν τα κρυπτονομίσματα τα οποία βασίζονται επάνω στον αλγόριθμο Proof of Work (PoW), θα δούμε τί είναι ο αλγόριθμος PoW και πως λειτουργεί. Επιμέρους σκοποί αυτής της διπλωματικής εργασίας είναι :

- Να παρουσιαστεί η σχετική βιβλιογραφία με βάση την οποία ερευνούμε και τους αλγόριθμους που υπολογίζουν και εκτιμούν την κατανάλωση ενέργειας στα κρυπτονομίσματα.
- Να παρουσιαστούν οι βάσεις δεδομένων από τις οποίες αντλήθηκε η σχετική βιβλιογραφία για το συγκεκριμένο θέμα που πραγματεύεται η διπλωματική εργασία.
- Να εξεταστεί ένας αλγόριθμος στο προγραμματιστικό περιβάλλον της Python που θα αναλύσει δεδομένα σχετικά με την κατανάλωση ενέργειας στα κρυπτονομίσματα

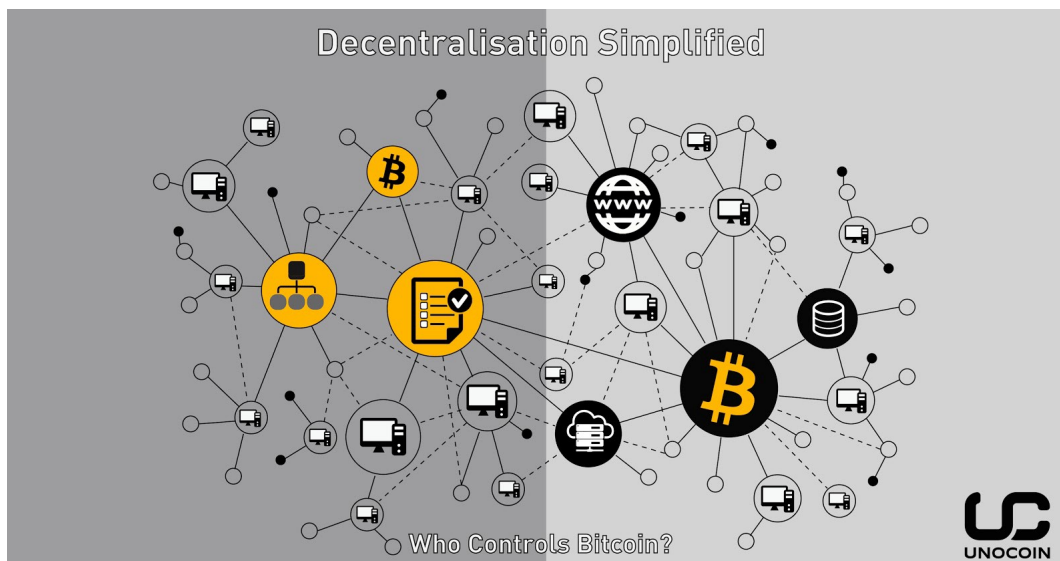
2.0.2 Τί είναι το bitcoin και πως ξεκίνησε

Μπορούμε να πούμε ότι γενικά τα κρυπτονομίσματα είναι μία τεχνολογική δημιουργία η οποία συγκεντρώνει πάρα πολλούς ανθρώπους οι οποίοι ασχολούνται με αυτό το θέμα, είτε θέλοντας να επενδύσουν σε ένα κρυπτονόμισμα, είτε θέλοντας να συμμετέχουν στη διαδικασία εξόρυξης ενός κρυπτονομίσματος, τα τελευταία χρόνια. Δηλαδή, το θέμα των κρυπτονομισμάτων είναι τέτοιας σημασίας που απορροφά μεγάλο ενδιαφέρον όχι μόνο μεμονωμένων ανθρώπων, αλλά ακόμα και μεγάλων βιομηχανιών και κυβερνήσεων. Σαφέστατα, δεν μπορεί να υπάρξει αντίλογος σε αυτό ότι το πιο δημοφιλές και πιο γνωστό κρυπτονόμισμα είναι το bitcoin.



(πηγή : Bloomberg.com)

Τί είναι όμως ένα κρυπτονόμισμα όπως το bitcoin; Ένα ψηφιακό νόμισμα λοιπόν είναι μία μορφή νομίσματος, που δεν αποτελείται από κάποιο υλικό, δεν είναι δηλαδή φτιαγμένο από κάποιο ειδικό χαρτί ή κάποιο μέταλλο όπως τα συμβατικά νομίσματα που γνωρίζουμε όλοι, αλλά είναι άυλο, είναι εντελώς ψηφιακό αλλά δεν υποστηρίζεται από καμία κυβέρνηση ή κάποιο άλλο τρίτο μέρος (<http://bitcoin.org>). Ο πρώτος που ξεκίνησε το bitcoin είναι ο Satoshi Nakamoto που στο άρθρο του το 2008 Bitcoin: A Peer-to-Peer Electronic Cash System, εισήγαγε το αυτό το κρυπτονόμισμα (ακόμα δεν γνωρίζουμε από την υπάρχουσα βιβλιογραφία αν είναι πραγματικό όνομα, αν είναι κάποιο ψευδώνυμο αν είναι ένας άνθρωπος ή μία ομάδα ατόμων και μάλιστα το 2011 ήταν η τελευταία χρονιά που ο Satoshi Nakamoto είχε μία επικοινωνία με το δίκτυο του bitcoin). Στο σημείο αυτό αξίζει να αναφέρουμε ότι η κάθε τιμή του κάθε κρυπτονομίσματος μπορεί να είναι διαφορετική και να αλλάζει με διαφορά λεπτού (Hayes, 2015). Για παράδειγμα το bitcoin και ειδικότερα η τιμή του το Σεπτέμβριο του 2017 ήταν 3700 δολάρια ανά κέρμα, ενώ το Δεκέμβριο του ίδιου χρόνου η τιμή του ανά κέρμα κυμαίνονταν σε σχεδόν 19000 δολάρια. Στην ουσία το bitcoin είναι ένα ψηφιακό όπως αναφέρθηκε παραπάνω ψηφιακό νόμισμα το οποίο μπορεί να γίνει μέσο ανταλλαγής μέσα σε ένα αποθηκευτικό χώρο σαν μητρώο που ονομάζεται ledger. Το συγκεκριμένο μητρώο δεν είναι ιδιωτικό με την έννοια ότι δεν μπορούν να το δούνε ή να έχουν πρόσβαση όλοι, αντιθέτως είναι ένα δημόσιο μητρώο μέσα στο οποίο μπορεί ο καθένας να ανατρέξει και να δει ότι πληροφορία θέλει. Το συγκεκριμένο κρυπτονόμισμα δεν τυπώνεται από κάποια Κεντρική Τράπεζα (πχ Ευρωπαϊκή Κεντρική Τράπεζα) ή από κάποιον άλλο φορέα, αλλά δημιουργείται μέσα στο δίκτυο του bitcoin και οι συναλλαγές γίνονται μέσα στο δίκτυο του blockchain χωρίς να υπάρχει κάποια επίβλεψη από κάποιον τρίτο φορέα (Das, Dutta, 2020).



(πηγή : Unocoin.com)

Με λίγα λόγια το δίκτυο του bitcoin είναι πλήρως αποκεντρωμένο από την ουσία που δεν υπάρχει κάποια άλλη αρχή να το εποπτεύει. Αν θέλουμε να το συγκρίνουμε με μία παραδοσιακή τράπεζα που στη περίπτωση της θα πρέπει να καταγράφει όλες τις συναλλαγές σε ένα μητρώο σε ψηφιακή μορφή και μόνο όσοι είναι μέλη των ρυθμιστικών αρχών θα μπορούν να παρακολουθούν αυτά τα δεδομένα, στο δίκτυο του Bitcoin που είναι πλήρως αποκεντρωμένο, υπάρχει η δυνατότητα που ο οποιοσδήποτε μπορεί να βλέπει τις συναλλαγές σε real time. Δηλαδή δεν υπάρχει κάποιος περιορισμός σε αυτό. Βέβαια όλα αυτά συμβαίνουν με μία υποσημείωση ότι, αυτό που δεν υπάρχει δυνατότητα να δεις είναι τα μέλη μίας συνδιαλλαγής και το ποιος κατέχει ένα ποσό. Με λίγα λόγια το δίκτυο του bitcoin προσφέρει μία κάποια ανωνυμία, δεν προσφέρει εντελώς το χαρακτηριστικό της ανωνυμίας. Δηλαδή αυτό που θα μπορείς και είσαι σε θέση να δεις είναι απλά διευθύνσεις και όχι τα ονόματα αυτών που κατέχουν αυτά τα χρήματα (Sedlmeir, Buhl, Fridgen, Keller, 2020). Συμπερασματικά και με απλά λόγια, το δίκτυο του Blockchain εμπεριέχει μία σειρά από στοιχεία που είναι ελεύθερα και προσβάσιμα από όλο το δίκτυο. Μέσα σε αυτή τη βάση κάθε στιγμή που περνά καταχωρούνται όλα τα δεδομένα και η κάθε μία συνδιαλλαγή εξασφαλίζοντας όχι τη πλήρη ανωνυμία αλλά ένα μέρος από αυτή (έχουν βρεθεί και αλγόριθμοι που κατά κάποιο τρόπο σπάνε την ανωνυμία). Εδώ η μεγάλη διαφορά είναι ότι στο δίκτυο του bitcoin τα δεδομένα δεν αποθηκεύονται σε μία κεντρική αρχή ή έναν κεντρικό υπολογιστή αλλά αποθηκεύονται σε περισσότερες συσκευές. Και για αυτό ακριβώς τον λόγο ονομάζεται και αλυσίδα γιατί αποθηκεύονται με τέτοιο τρόπο που είναι σαν να σχηματίζουν μία νοητή αλυσίδα. Αξίζει να αναφερθούν μερικές ημερομηνίες που έμειναν στην ιστορία του δικτύου του Bitcoin :

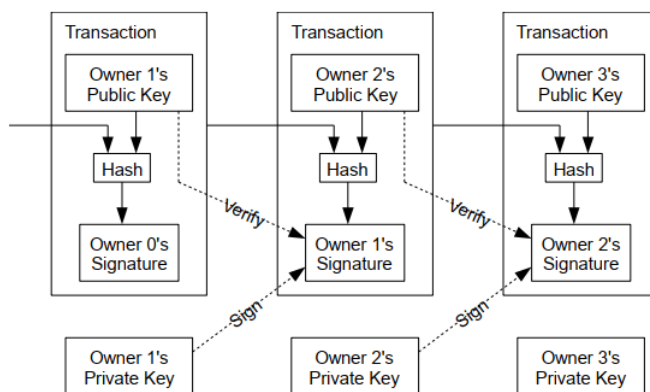
- Τον Νοέμβριο του 2013 η τιμή του bitcoin πέφτει για πρώτη φορά από τα 1213 δολάρια στα 600 δολάρια
- Τον Οκτώβριο του 2017 η Κίνα απαγορεύει για πρώτη φορά την συνδιαλλαγές με bitcoin
- Στα τέλη του Οκτωβρίου του 2018 το Bitcoin γιορτάζει τα δέκα χρόνια από την

πρώτη φορά που εμφανίστηκε.

- Τον Ιούνιο του 2015 εμφανίζεται ένα από τα σημαντικότερους κανόνες για το δίκτυο του bitcoin το λεγόμενο bitlicense.
- Τον Νοέμβριο του 2010 η κεφαλοποίηση αγοράς του bitcoin ξεπερνά το 1.000.000 δολάρια
- Τον Οκτώβριο του 2008 δημοσιεύεται το άρθρο του Satoshi Nakamoto και από εκεί ξεκίνησαν όλα.

2.0.3 Τρόπος λειτουργίας του bitcoin

Ας δούμε λίγο τώρα πως λειτουργεί το κρυπτονόμισμα του bitcoin. Ουσιαστικά αναφερόμαστε σε ένα μηχανισμό peer to peer που δίνει τη δυνατότητα μέσω του διαδικτύου σε ηλεκτρονικές πληρωμές που θα έχουν ένα κοινό χαρακτηριστικό, δεν θα εποπτεύονται από καμία ρυθμιστική αρχή. Για να λυθεί το ζήτημα όμως το να υπάρξουν ψηφιακά νομίσματα τα οποία έχουν ήδη δαπανηθεί και επαναχρησιμοποιούνται (το ζήτημα των double spending attacks) , το δίκτυο του bitcoin συλλέγει τις ψηφιακές υπογραφές. Βέβαια στο σημείο αυτό να αναφέρουμε ότι μέσω των ψηφιακών υπογραφών μπορεί να λυθεί σε ένα σημαντικό ποσοστό το ζήτημα, αλλά δεν είναι αυτή η ενδεδειγμένη λύση λόγω του ότι χάνονται ένα σημαντικό κομμάτι των οφελών όταν πρέπει να υπάρξει ένα τρίτο πρόσωπο εμπιστοσύνης (trusted third person, όπως επισημαίνει ο Nakamoto) για να επιβεβαιώσει τη συναλλαγή και να αποφευχθεί πιθανό double spending problem. Ο Nakamoto το 2008 πρότεινε μέσω της τεχνολογίας του blockchain προτείνει ένα δίκτυο peer to peer όπως αναφέραμε και προηγουμένως, όπου όλες οι συναλλαγές θα καταγράφονται σε ένα μητρώο θα κατακερματίζονται μέσω αλγορίθμων κρυπτογράφησης και θα τοποθετούνται σε μία συνεχιζόμενη αλυσίδα (η οποία βασίζεται στον αλγόριθμο PoW) και θα δημιουργείται ένα αρχείο το οποίο δεν μπορεί να αλλαχθεί εάν δεν επαναλάβουμε τον αλγόριθμο PoW. Με αυτό λοιπόν τον τρόπο δημιουργείται μία αλυσίδα και αυτή που έχει το μεγαλύτερο μήκος σημαίνει ότι έχει «επιβεβαιωθεί» από τους περισσότερους κόμβους του δικτύου του bitcoin. Ένας κόμβος στο δίκτυο του bitcoin στην ουσία αποτελεί και έναν miner, δηλαδή αυτός που κάνει την εξόρυξη των κρυπτονομισμάτων (Biryukov, Khovratovich, 2017). Έτσι η αλυσίδα με το μεγαλύτερο μήκος θεωρείται ότι είναι και η πιο ασφαλή. Βέβαια ακόμα και η πιο μεγάλη αλυσίδα δεν είναι πάντα σίγουρο ότι θα είναι και η πιο αξιόπιστη.



(πηγή : Nakamoto,2008)

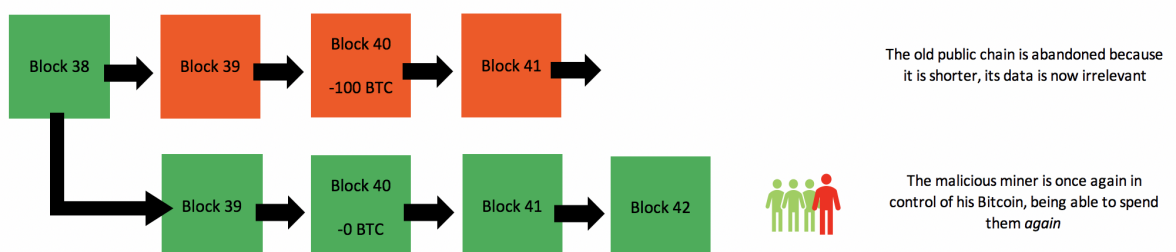
Γενικά μπορούμε να σημειώσουμε ότι το εμπόριο που γίνεται μέσω του διαδικτύου βασίζεται σε πολύ μεγάλο βαθμό στην ύπαρξη κάποιων έμπιστων τρίτων προσώπων (πχ τα χρηματοπιστωτικά ιδρύματα) τα οποία ελέγχουν τη διαδικασία των πληρωμών. Το bitcoin ανέτρεψε αυτή την λογική και πρότεινε μία ριζοσπαστική ιδέα για ηλεκτρονικές πληρωμές, δηλαδή να μην υπάρχει καμία αρχή που να επιβλέπει τις πληρωμές. Στην ουσία το bitcoin πρότεινε ένα ηλεκτρονικό σύστημα πληρωμών το οποίο θα έχει σαν βάση αποδείξεις οι οποίες θα είναι κρυπτογραφημένες, και θα επιτρέπουν σε δύο συναλλασσόμενους να έχουν μία συνδιαλλαγή χωρίς να υπάρχει κάποιο τρίτο πρόσωπο για να ελέγχει κατά κάποιο τρόπο τη διαδικασία (Hileman, Rauchs, 2017) . Το σύστημα αυτό θα συνεχίζει να είναι ασφαλές και να μην υπάρχουν επιθέσεις double spending όσο οι περισσότεροι και «έντιμοι» κόμβοι ελέγχουν μεγαλύτερη ισχύ μέσα στο δίκτυο από την όποια ομάδα «κακόβουλων» κόμβων που θέλουν να κάνουν επιθέσεις double spending στο δίκτυο και στην ουσία να εξαπατήσουν τους χρήστες του δικτύου και να βλάψουν την αξιοπιστία όλου του δικτύου του Bitcoin.

Είπαμε και προηγουμένως ότι ένα κρυπτονόμισμα είναι στην ουσία μία αλυσίδα που αποτελείται από ψηφιακές υπογραφές. Ένα ψηφιακό νόμισμα αποτελείται από το δημόσιο κλειδί (public key) το οποίο μπορεί να το δει ο οποιοσδήποτε, γιατί στην ουσία αντικατοπτρίζει την διεύθυνση μας μέσα στο δίκτυο, και το ιδιωτικό κλειδί (private key) που δημιουργεί το δημόσιο κλειδί. Το private key μπορούμε να το ξέρουμε μόνο εμείς γιατί όποιος ξέρει το ιδιωτικό κλειδί ελέγχει και τα χρήματα τα οποία είναι συνδεδεμένα με τη διεύθυνση στο δίκτυο του blockchain (Kent, Bain, 2020). Αυτό που γίνεται με τις δημόσια και τα ιδιωτικά κλειδιά μέσα στο δίκτυο είναι ότι ο κάθε κάτοχος μεταφέρει το νόμισμα στον επόμενο βάζοντας την ηλεκτρονική του υπογραφή στη προηγούμενη συναλλαγή και στο public key του επόμενου που θα έχει αυτό το ψηφιακό νόμισμα. Με αυτό τον τρόπο προστίθενται όλα στο τέλος του νομίσματος και αυτός που έχει το νόμισμα στο τέλος έπειτα από τις συνδιαλλαγές μπορεί να επαληθεύσει τις υπογραφές και να ελέγξει την αξιοπιστία του όλης της αλυσίδας. Σε προηγούμενα μοντέλα εκτός του bitcoin έπρεπε να υπάρχει μία κεντρική αρχή που θα επέβλεπε αν όλες οι συναλλαγές ήταν αξιόπιστες. Στο δίκτυο του bitcoin χρειαζόμαστε έναν τρόπο για να αποφύγουμε τη περίπτωση κάποιος να έχει ήδη σπαταλήσει το νόμισμα και αυτή η συναλλαγή να μην πέρασε μέσα στο δίκτυο (double spend attack). Για αυτό το λόγο αυτό που μας ενδιαφέρει κατά κύριο λόγο είναι η παλαιότερη συναλλαγή. Για να πετύχουμε και να ελαχιστοποιήσουμε την πιθανότητα των double spend attack, οι

συναλλαγές ανακοινώνονται σε όλους τους χρήστες του δικτύου και ο κάθε ένας που θα δικαιούται ένα νόμισμα του bitcoin, απλά θα πρέπει να έχει ένα αποδεικτικό ότι κάθε στιγμή που πραγματοποιείται η κάθε μία συναλλαγή, οι περισσότεροι κόμβοι να έχουν ήδη συμφωνήσει ότι το νόμισμα αυτό δεν έχει υπάρξει σε κάποια άλλη συναλλαγή (Chiu, Koeppl, 2018).

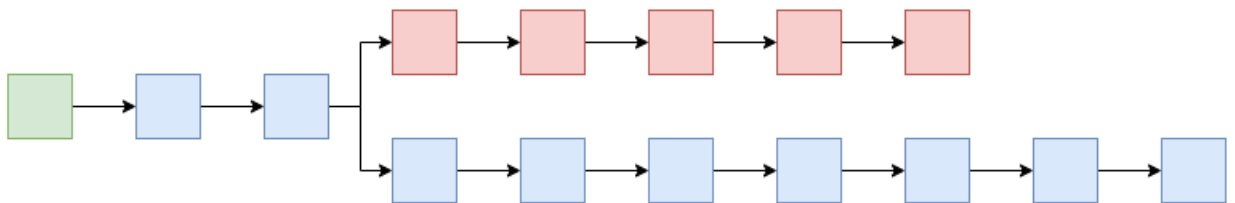
2.0.4 Το πρόβλημα των double spend attack

Ας προσπαθήσουμε να καταλάβουμε με το παρακάτω παράδειγμα πληρωμής μίας υπηρεσίας που θέλουμε, πως μπορεί να γίνει μία επίθεση double-spend. Ας υποθέσουμε ότι θέλουμε να γίνουμε μέλη ενός γυμναστηρίου που δέχεται πληρωμές με bitcoin στο site του γυμναστηρίου στο internet. Οπότε εμείς για να πληρώσουμε το γυμναστήριο δημιουργούμε μια συνδιαλλαγή με bitcoin από τη διεύθυνσή μας στη διεύθυνση του γυμναστηρίου και τη μεταδίδουμε σε όλο το δίκτυο του bitcoin. Ας υποθέσουμε ότι υπάρχουν κάποιοι «έντιμοι» κόμβοι που δημιουργούν το επόμενο μπλοκ και συμπεριλαμβάνουν αυτή την συνδιαλλαγή που κάναμε μέσα στο μπλοκ αυτό. Οπότε τώρα υπάρχει ένα καινούργιο μπλοκ στο δίκτυο που δημιουργήθηκε από έναν έντιμο κόμβο και εμπεριέχει αυτή τη συνδιαλλαγή που αντιπροσωπεύει την πληρωμή που κάναμε για την ετήσια συνδρομή μας στο γυμναστήριο. Ας σημειώσουμε ότι αυτή η συνδιαλλαγή ουσιαστικά είναι ένα κατασκεύασμα από δεδομένα που περιέχουν την ηλεκτρονική υπογραφή μας, μία εντολή πληρωμής, το δημόσιο κλειδί του γυμναστηρίου (ουσιαστικά είναι η διεύθυνση του μέσα στο δίκτυο του bitcoin), και μία συνάρτηση κρυπτογράφησης hash function. Αυτό ακριβώς το hash αντιπροσωπεύει έναν δείκτη που μας πληροφορεί για μία προηγούμενη συνδιαλλαγή που λάβαμε και που τώρα αυτά τα λεφτά που πήραμε τα ξοδεύουμε για να πληρώσουμε το γυμναστήριο. Αυτός ο δείκτης με λίγα λόγια θα πρέπει να δείχνει μία συνδιαλλαγή που είχε συμπεριληφθεί σε προηγούμενο μπλοκ μέσα στο blockchain. Όπως είπαμε, το τελευταίο μπλοκ που δημιουργήθηκε από έναν «έντιμο» κόμβο περιέχει τη συνδιαλλαγή που πληρώσαμε το γυμναστήριο. Από την στιγμή που θα δει το γυμναστήριο ότι αυτή η πληρωμή συμπεριλήφθηκε στο blockchain, το γυμναστήριο θα καταλάβει ότι το έχουμε πληρώσει και θα μας αφήσει να έχουμε πρόσβαση στην ετήσια συνδρομή. Αν υποθέσουμε ότι ο επόμενος τυχαίος κόμβος που θα δημιουργηθεί μέσα στο δίκτυο του bitcoin ελέγχεται από εμάς.



(πηγή :www.medium.com)

Έτσι εμείς στο επόμενο μπλοκ με τις συνδιαλλαγές που θα προτείνουμε, μπορούμε να μην συμπεριλάβουμε την πληρωμή μας στο γυμναστήριο και να συμπεριλάβουμε τον δείκτη που είχαμε λάβει από το προηγούμενο μπλοκ. Εμείς λοιπόν μπορούμε να συμπεριλάβουμε μία συνδιαλλαγή στο επόμενο μπλοκ που το ελέγχουμε εμείς, με τα νομίσματα που έχουμε ήδη στείλει στο γυμναστήριο σε μία διαφορετική διεύθυνση την οποία ελέγχουμε εμείς. Αυτό είναι μία κλασική περίπτωση double spend. Από τη στιγμή που οι δύο συνδιαλλαγές εμπεριέχουν τα ίδια νομίσματα, μόνο μία από αυτές μπορεί να μπει μέσα στο blockchain. Αν εμείς μπορέσουμε να συμπεριλάβουμε την συνδιαλλαγή από τη δική μας διεύθυνση μέσα στο δίκτυο του block chain τότε η πληρωμή που έχουμε κάνει για το γυμναστήριο δεν θα έχει καμία ισχύ, γιατί δεν θα συμπεριληφθεί σε κανένα από τα επόμενα μπλοκ της αλυσίδας, με αποτέλεσμα να έχουμε καταφέρει να «κοροϊδέψουμε» το δίκτυο του bitcoin. Από τέτοιες ενέργειες πλήττεται σε μεγάλο βαθμό η αξιοπιστία του δικτύου. Από τί εξαρτάται δηλαδή το αποτέλεσμα μιας τέτοιας κακόβουλης επίθεσης απέναντι στο δίκτυο του bitcoin; Αυτό εξαρτάται από ποιο μπλοκ θα καταλήξει στην μεγάλη αλυσίδα του δικτύου. Αν καταλήξει το μπλοκ που εμπεριέχει την πληρωμή μας από το εμάς προς το γυμναστήριο ή αν καταλήξει το μπλοκ που περιέχει την συνδιαλλαγή από εμάς προς εμάς. Τι καθορίζει όμως ποιο μπλοκ θα συμπεριληφθεί στην αλυσίδα; Αυτό που γίνεται είναι ότι οι πιο πολλοί «έντιμοι» κόμβοι θα συμπεριλάβουν τα μπλοκ που προέρχονται από τη πιο μεγάλη αλυσίδα. Στην ερώτηση αυτή δεν υπάρχει κάποια σαφή απάντηση διότι στο σημείο που είμαστε οι δύο αλυσίδες έχουν ακριβώς το ίδιο μέγεθος και διαφέρουν ως προς το τελευταίο μπλοκ, που και οι δύο αλυσίδες είναι έγκυρες. Ο κόμβος που θα επιλέξει σε ποιο από τα δύο μπλοκ θα επιλέξει να χτίσει, θα καθορίσει και την έκβαση της προσπάθειάς μας να κάνουμε επίθεση double spend.



(πηγή :www.chowles.com)

Ας πάμε να δούμε στο παράδειγμά μας τι γίνεται από τη πλευρά του γυμναστηρίου και ποιες κινήσεις μπορεί να κάνει για να προστατευθεί; Έτσι θα δούμε και το επίπεδο ασφάλειας που έχει το bitcoin. Όταν εμείς διαδώσαμε την πληρωμή μας στο γυμναστήριο σε όλο το δίκτυο, το γυμναστήριο είχε καταλάβει αυτή τη πληρωμή πολύ πριν τη δημιουργία του επόμενου μπλοκ. Αν το γυμναστήριο με το που καταλάβαινε ή άκουγε τη πληρωμή από το δίκτυο μας έδινε το ελεύθερο εκείνη τη στιγμή να έχουμε πρόσβαση στην ετήσια συνδρομή τότε αυτό ονομάζεται συνδιαλλαγή μηδενικής επιβεβαίωσης. Βέβαια το γυμναστήριο έπρεπε να είναι πιο προσεκτικό και να μην έδινε αμέσως πρόσβαση ακόμα και όταν η συνδιαλλαγή που στείλαμε συμπεριλαμβανόταν σε ένα μπλοκ. Θα έπρεπε να επιλέξει να περιμένει. Αν το γυμναστήριο έβλεπε ότι εμείς πάμε να ξεκινήσουμε μία επίθεση double spend και θα είχε αντιληφθεί ότι το

μπλοκ στο οποίο είχε συμπεριληφθεί η συνδιαλλαγή που αφορούσε την πληρωμή του θα ήταν «άκυρο». Τότε το γυμναστήριο θα προχωρούσε σε ουσιαστική ακύρωση της συνδιαλλαγής και δεν θα μας άφηνε να έχουμε πρόσβαση στην ετήσια συνδρομή του. Γενικά εδώ πρέπει να σημειώσουμε ότι όσες περισσότερες επιβεβαιώσεις πάρει μία συνδιαλλαγή τότε αυξάνονται ακόμα παραπάνω το μπλοκ που εμπεριέχει αυτή τη συνδιαλλαγή να καταλήξει στην «έντιμη» και μεγαλύτερη αλυσίδα. Γενικά έχει παρατηρηθεί ότι η πιθανότητα να συμβεί μία double spend επίθεση μειώνεται όσο αυξάνεται ο αριθμός των επιβεβαιώσεων που έχει ένα μπλοκ που περιέχει συνδιαλλαγές (Miller, Goldfeder, Felten, Bonneau, Narayanan, 2016).

2.0.5 Διαδικασία του mining

Η διαδικασία της εξόρυξης (δηλαδή του mining) των κρυπτονομισμάτων όπως είναι το bitcoin στηρίζεται στους miners. Οι miners είναι αυτοί που έχουν την αποκλειστική ευθύνη να επιβεβαιώνουν οποιαδήποτε συναλλαγή συμβαίνει μέσα στο δίκτυο του κρυπτονομίσματος, αλλά και να κατασκευάζουν ένα μπλοκ και να τα αποθηκεύουν στην αλυσίδα του blockchain. Παρακάτω υπογραμμίζουμε ποια είναι τα πιο σημαντικά πράγματα που πρέπει να είναι σε θέση να κάνει ένας που θέλει να γίνει miner :

- Αρχικά, ένας miner θα πρέπει να είναι σε θέση να αντιλαμβάνεται τις συνδιαλλαγές που γίνονται μέσα στο δίκτυο, δηλαδή θα πρέπει να παρακολουθεί τον όγκο αυτών των συναλλαγών, να μπορεί να ελέγχει τις ηλεκτρονικές υπογραφές εάν είναι όντως οι κατάλληλες, έτσι ώστε να γνωρίζει και να αποτρέπει συναλλαγές με κρυπτονομίσματα που έχουν χρησιμοποιηθεί. Με λίγα λόγια με αυτή τη διαδικασία του ελέγχου των ηλεκτρονικών υπογραφών μπορεί να αποτρέψει τις επιθέσεις double spend που περιγράψαμε παραπάνω.
- Δεύτερον , ένας miner πρέπει να διατηρεί την αλυσίδα των μπλοκ. Παίρνει όλα τα δεδομένα των μπλοκ και από άλλους κόμβους που ήδη υπάρχουν μέσα στην αλυσίδα των μπλοκ. Αυτή η ανταλλαγή των δεδομένων γίνεται από την πλευρά των miner πριν γίνουν μέλη του δικτύου.
- Τρίτον, αφού γίνουν μέλη του δικτύου ακολουθούν τα πιο πρακτικά κομμάτια που έχουν να κάνουν με τη δυνατότητα των miner να συνθέσουν ένα μπλοκ. Αφού πάρουν στα χέρια τους ένα copy από όλη την αλυσίδα θα πρέπει να αρχίσουν με τη σειρά τους να συνθέτουν τα δικά τους μπλοκ. Ακόμα όπως είπαμε και προηγουμένως, οι miner έχουν την υποχρέωση και εξασφαλίζουν ότι η οποιαδήποτε συνδιαλλαγή που εμπεριέχεται στο δικό τους το μπλοκ να είναι έγκυρη.
- Τέταρτον, θα πρέπει να βρούνε κόμβους οι οποίοι θα κάνουν το μπλοκ τους να έχει μία εγκυρότητα. Αυτό είναι εξαιρετικά σημαντικό γιατί ένα τα μπλοκ των miner δεν περιέχουν συναλλαγές που είναι έγκυρες, τότε αυτό αυτόματα θα πλήξει την αξιοπιστία του δικτύου με αποτέλεσμα αρκετοί χρήστες να αποχωρήσουν από αυτό.
- Αφού γίνουν όλα αυτά τα βήματα, και αφού δημιουργηθεί ένα μπλοκ από έναν miner θα πρέπει αυτό το μπλοκ να το δεχθούν και οι άλλοι miner έτσι ώστε

να γίνει μέρος της αλυσίδας που έχει βεβαιωθεί ως η πιο έγκυρη. Αυτό βέβαια δεν είναι πάντα σίγουρο ότι θα γίνει. Η αλήθεια είναι ότι σε αυτό το βήμα, ο παράγοντας της τύχης παίζει έναν ρόλο.

- Τελευταίο και ίσως και πιο σημαντικό είναι το ζήτημα του κέρδους. Ένας miner και αφού έχουν γίνει και τα πέντε βήματα από τους υπόλοιπους miner, αυτό θα σημαίνει ότι το μπλοκ που έχει δημιουργηθεί είναι αποδεκτό και γίνεται κομμάτι της αλυσίδας στην οποία έχουν συναινέσει όλοι και έτσι υπάρχει κέρδος. Όσα περισσότερα μπλοκ δημιουργήσει ένας miner τόσο περισσότερο κέρδος θα έχει.



(πηγή :www.CNBC.com - "Εξόρυξη" ενός bitcoin)

Με βάση τα έξι βήματα που είπαμε παραπάνω, μπορούμε να εξάγουμε το εξής συμπέρασμα, ότι γενικά οι ενέργειες που πρέπει να κάνουν οι miners χωρίζονται σε δύο μεγάλες κατηγορίες : Η πρώτη αφορά διεργασίες οι οποίες αφορούν την επιβεβαίωση των συνδιαλλαγών του δικτύου και οι οποίες είναι εξαιρετικές για την ύπαρξή του. Από την άλλη μεριά η δεύτερη κατηγορία αφορά την δημιουργία των μπλοκ και το κέρδος του κάθε miner. Βέβαια η δεύτερη κατηγορία δεν αφορά καθαρά το δίκτυο του bitcoin, αλλά θα μπορούσαμε να πούμε ότι το κέρδος του κάθε miner λειτουργεί πιο πολύ σαν κίνητρο για να υπάρχει μία εύρυθμη και σωστή λειτουργία του ίδιου του δικτύου. Δηλαδή το κέρδος από τη δημιουργία των μπλοκ αποσκοπεί στην αποτροπή των miner να συμπεριφέρονται κατά του δικτύου του κρυπτονομίσματος. Όσο πιο έντιμα συμπεριφέρονται οι miner τόσο πιο αξιόπιστο φαίνεται το ίδιο το δίκτυο. Έχουμε αναφέρει και παραπάνω ότι το bitcoin λειτουργεί με τον αλγόριθμο του Proof of Work. Αυτό πρακτικά σημαίνει ότι, για να δημιουργήσει ένα μπλοκ ένας miner θα πρέπει να λύσει ένα υπολογιστικό πρόβλημα το οποίο είναι το ίδιο για όλο το δίκτυο και το οποίο αλλάζει κάθε δέκα λεπτά. Βέβαια, με βάση αυτό μπορεί κάποιος εύλογα να καταλήξει στο συμπέρασμα ότι αφού όλοι οι miner λύνουν το ίδιο παζλ, τότε ο miner που θα είναι ο πιο γρήγορος θα κερδίσει. Αυτό είναι ένα εύκολο συμπέρασμα το

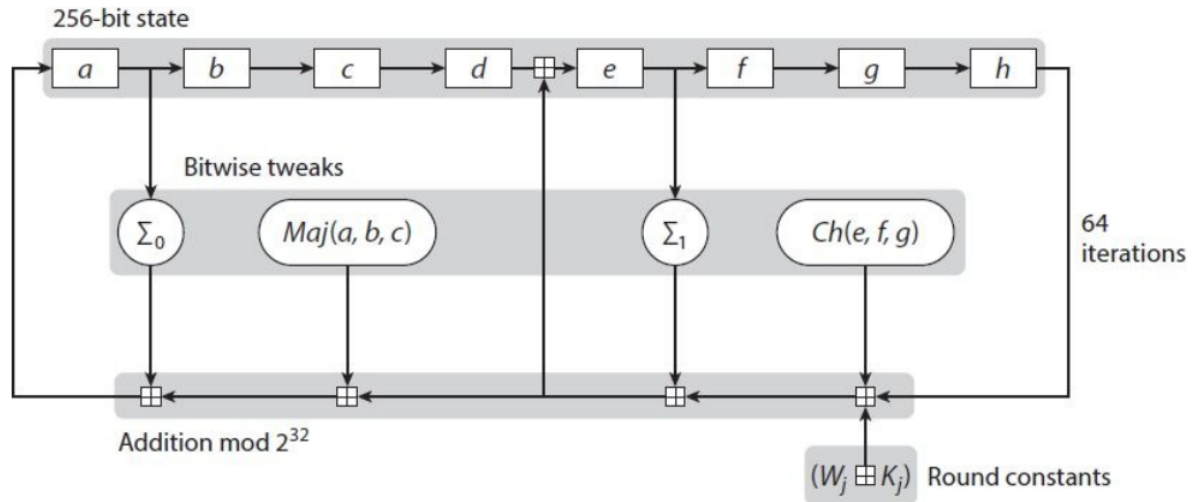
οποίο όμως είναι λάθος. Και είναι λάθος γιατί είναι σχεδόν απίθανο όλοι οι miner του δικτύου, να προσπαθούν να φτιάξουν ακριβώς το ίδιο μπλοκ, γιατί ο εκάστοτε miner στο μπλοκ του θα εμπεριέχει ένα διαφορετικό σύνολο συναλλαγών σε σχέση με τους άλλους και με διαφορετική σειρά. Υπάρχει όμως και μία πιθανότητα οι miner να εργάζονται ακριβώς επάνω στο ίδιο μπλοκ. Αυτό το γεγονός θα συνέβαινε εάν και μόνο αν οι miner μοιράζονταν το ίδιο δημόσιο κλειδί, δηλαδή είχαν την ίδια διεύθυνση και θα έπρεπε να μιλήσουν μεταξύ τους για να διαφοροποιηθούν μεταξύ τους και να συμπεριλάβουν έναν διαφορετικό κόμβο στη συνδιαλλαγή τους. (Η πιθανότητα να έχουν την ίδια διεύθυνση δύο miner συμβαίνει όταν ανήκουν και οι δύο στο ίδιο mining pool).

Το κατά πόσο δύσκολο θα είναι κάθε φορά η εξόρυξη ενός bitcoin καθορίζεται με βάση την αποτελεσματικότητα που είχαν οι miner στα προηγούμενα 2016 μπλοκ. Με λίγα λόγια η δυσκολία μεταβάλλεται κάθε 2016 μπλοκ και θα πρέπει να είναι σε τέτοιο βαθμό που το κάθε μπλοκ σε σχέση με το επόμενο που θα δημιουργηθεί να απέχουν χρονικά 10 λεπτά. Αν η δυσκολία εξόρυξης είναι πολύ μεγάλη και η χρονική απόσταση είναι πολύ περισσότερη των 10 λεπτών, τότε χαμηλώνει ο δείκτης δυσκολίας. Αντίθετα, αν η δυσκολία εξόρυξης είναι πολύ εύκολη και η χρονική απόσταση είναι μικρότερη των 10 λεπτών τότε, ο δείκτης δυσκολίας ανεβαίνει με σκοπό να διατηρείται η χρονική απόσταση των δέκα λεπτών. Ο τύπος που καθορίζει την δυσκολία των επόμενων 2016 μπλοκ είναι :

$$\text{Επόμενη δυσκολία} = (\text{Προηγούμενη δυσκολία} * 2016 * 10 \text{ λεπτά}) / (\text{Χρόνος εξόρυξης των τελευταίων 2016 μπλοκ})$$

((Miller, Goldfeder, Felten, Bonneau, Narayanan, 2016). Αυτό που κάνει αυτός ο τύπος σύμφωνα με τους συγγραφείς από το Πανεπιστήμιο του Πρίνστον είναι η τροποποίηση της δυσκολίας ώστε το δίκτυο να διατηρεί την ισορροπία των δέκα λεπτών στη δημιουργία των μπλοκ. Γενικά ο κάθε miner υπολογίζει αυτός την δυσκολία που θα έχει στη διαδικασία δημιουργίας του δικού του μπλοκ και με τη σειρά του δέχεται μπλοκ με βάση την δυσκολία που έχει αυτός υπολογίσει. Η συναίνεση επιτυγχάνεται όταν υπάρξουν δύο miner που βρίσκονται πάνω από το ίδιο μπλοκ και συμφωνούν όσον αφορά το επίπεδο δυσκολίας. Οι miner όπως αναφέραμε στη προσπάθειά τους να λύσουν το υπολογιστικό πρόβλημα και να καταφέρουν να φτάσουν στη δημιουργία των bitcoin, χρησιμοποιούν κάποιους αλγόριθμους. Η βάση των υπολογιστικών προβλημάτων που καλούνται να λύσουν είναι οι συναρτήσεις κρυπτογράφησης και συγκεκριμένα η συνάρτηση SHA-256. Η συνάρτηση αυτή είναι μία συνάρτηση κρυπτογράφησης και ανήκει σε μία μεγαλύτερη ομάδα συναρτήσεων κρυπτογράφησης οι οποίες τυποποιήθηκαν το 2001 και τα αρχικά SHA σημαίνουν Secure Hash Algorithm. Εύκολα κάποιος μπορεί να αναρωτηθεί γιατί επιλέχθηκε η συγκεκριμένη συνάρτηση κρυπτογράφησης στη δημιουργία των Bitcoin και η απάντηση είναι ότι όταν πρωτοξεκίνησε το bitcoin το 2008 από τον Satoshi Nakamoto, αυτή η συνάρτηση θεωρούνταν η ισχυρότερη συνάρτηση όσον αφορά ζητήματα κρυπτογράφησης. Επίσης η SHA-256 προέρχεται από μία ομάδα συναρτήσεων κρυπτογράφησης, την ομάδα SHA-2, που συμπεριλαμβάνει και την συνάρτηση SHA-512 η οποία θεωρείται ακόμα πιο δυνατή όσον αφορά την κρυπτογράφηση της. Επιπρόσθετα, μπορούμε να αναφέρουμε την ομάδα των συναρτήσεων SHA-1, η οποία είναι προηγούμενης γενιάς και είχε ένα output 160 bit (σε σύγκριση με την SHA-256 που έχει 256 bit), που σήμερα βέβαια θεωρείται μη ασφαλής κρυπτογραφικά, μολονότι συμπεριλαμβάνεται μέσα στο δίκτυο του Bitcoin. Πλέον η νέα γενιά συναρτήσεων κρυπτογράφησης αφορά την ομάδα των SHA-3 που είναι υπό την εποπτεία της Αμερικανικού Ινστιτούτου για την τεχνολογία, οι οποίες θεωρούνται τρομερά ασφαλείς συναρτήσεις

κρυπτογράφησης αλλά δυστυχώς όταν το bitcoin δημιουργούνταν δεν ήταν γνωστές. Η εικόνα που ακολουθεί δείχνει την λειτουργία μιας συνάρτησης SHA-256.



(πηγή : Bitcoin And Cryptocurrency Technologies, A Comprehensive Introduction, 2016)

Στις αρχικές μορφές της εξόρυξης των bitcoin, η διαδικασία του mining γινόταν με τους απλούς υπολογιστές όπως τους ξέρουμε και σήμερα και δεν υπήρχε η ανάγκη για πολύ ισχυρούς και πολύπλοκους επεξεργαστές όπως γίνεται σήμερα. Στην εικόνα που ακολουθεί βλέπουμε έναν από τους πρώτους κώδικες εξόρυξης των bitcoin. Θα παρατηρήσουμε ότι και ο κώδικας είναι αρκετά απλός, όσο ήταν δηλαδή η συνολική διαδικασία του mining στα αρχικά στάδιά του.

```
TARGET = (65535 << 208) / DIFFICULTY;
coinbase_nonce = 0;
while (1) {
    header = makeBlockHeader(transactions, coinbase_nonce);
    for (header_nonce = 0; header_nonce < (1 << 32); header_nonce++){
        if (SHA256(SHA256(makeBlock(header, header_nonce))) < TARGET)
            break; //block found!
    }
    coinbase_nonce++;
}
```

(πηγή : Bitcoin And Cryptocurrency Technologies, A Comprehensive Introduction, 2016)

Βέβαια, πλέον και με τη δυσκολία που έχει η διαδικασία της εξόρυξης είναι τεχνικά αδύνατο να θες να δημιουργήσεις ένα μπλοκ με bitcoin με μία απλή μονάδα CPU. Ας σκεφτούμε απλά ότι με έναν απλό υπολογιστή στις αρχές του 2015 και με τη δυσκολία στη διαδικασία εξόρυξης στο δίκτυο του bitcoin θα χρειαζόμασταν κάποιες χιλιάδες χρόνια για να βρούμε ένα μπλοκ. Σήμερα είναι ανέφικτο και πρακτικά, αλλά και από άποψη κόστους εξαιρετικά ανώφελο να προσπαθήσουμε να δημιουργήσουμε bitcoin με μία απλή μονάδα CPU.



(Ένα "δαχτυλίδι" εξόρυξης αποτελούμενο από 6 κάρτες γραφικών.
Πηγή : coinminingrings.com)

Η συνέχεια της διαδικασίας της εξόρυξης έγινε με τη χρήση των GPUs, δηλαδή οι miner όταν συνειδητοποίησαν ότι με τα CPU ήταν αδύνατο να προχωρήσουν λόγω της πολύ αργής ταχύτητάς τους, πήραν τις κάρτες γραφικών και τις προσαρμόσαν για να μπορούν να είναι κατάλληλες για το mining. Με την προσθήκη της γλώσσας OpenCL που βοηθά στο να γίνουν πράγματα πολύ πιο γρήγορα και να γίνονται υπολογισμοί σε πολύ μικρότερο χρόνο χρησιμοποιώντας τις κάρτες γραφικών, σε σχέση με τους υπολογισμούς που μπορούσαν να γίνουν στα CPU, η εξόρυξη των bitcoin δέχτηκε ένα boost. Οι μονάδες GPUs είχαν κάποια πλεονεκτήματα που τα αναφέρουμε παρακάτω :

- Πρώτον, ήταν αρκετά εύκολο ειδικά για νέους miner να μπορούν να τις στήσουν αλλά και εύκολα να τις βρει κάποιος αν ήθελε. Μπορούσε ο οποιοσδήποτε να παραγγείλει και να αγοράσει κάρτες γραφικών από καταστήματα πχ στο ίντερνετ.
- Επιπλέον είναι σχεδιασμένες έτσι οι κάρτες γραφικών που μπορούν να κάνουν πολλούς υπολογισμούς παράλληλα οπότε έχουν αρκετές δυνατότητες στο να κάνουν ταυτόχρονους αριθμητικούς υπολογισμούς που απαιτεί η εξόρυξη των bitcoin.
- Επίσης μπορείς να τις προγραμματίσεις έτσι να μπορούν να κάνουν τους υπολογισμούς ακόμα πιο γρήγορα από ότι είναι ήδη προγραμματισμένες να κάνουν.

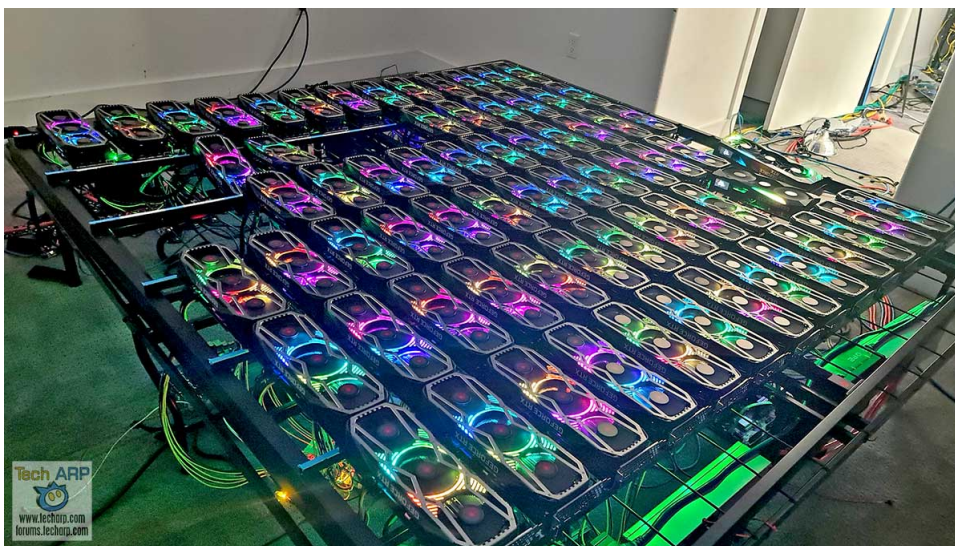
Έχει υπολογιστεί ότι μπορεί να κερδίσεις μέχρι και πέντε τοις εκατό παραπάνω στα κέρδη σου, αν προγραμματίσεις κατάλληλα τις κάρτες γραφικών να «τρέχουν» πιο γρήγορα από το κανονικό τους.

- Τέλος, μπορείς να ελέγχεις παραπάνω από μία κάρτες γραφικών από μία κεντρική μονάδα. Έτσι μπορείς να προσαρμόσεις περισσότερες από μία κάρτες γραφικών στον υπολογιστή σου που είναι προγραμματισμένος για τη διαδικασία του mining.

Ένα ζήτημα που προέκυψε με την ξαφνική αύξηση της ζήτησης για κάρτες γραφικών που χρησίμευαν στη διαδικασία της εξόρυξης, ήταν η δημιουργία μιας διαμάχης ανάμεσα στους miner και στους παίκτες παιχνιδιών που έψαχναν να βρουν κάρτες γραφικών να γίνουν πιο αποδοτικοί στις ταχύτητές τους στα on line παιχνίδια και δεν μπορούσαν. Αποτέλεσμα αυτού του γεγονότος, αρκετοί παίκτες παιχνιδιών έγιναν οι ίδιοι χρήστες του δικτύου του bitcoin και ξεκίνησαν να κάνουν εξόρυξη των bitcoin.

Από την άλλη μεριά, η χρήση των καρτών γραφικών έχει κάποια και κάποια μειονεκτήματα.

- Σε μία πρώτη ανάγνωση των άρθρων μπορούμε να δούμε ότι οι κάρτες γραφικών, έχουν κάποια hardware κομμάτια που δεν χρησιμεύουν στην εξόρυξη των bitcoin.
- Επίσης οι κάρτες γραφικών έχουν ένα θέμα με την θερμοκρασία. Όταν κολλήσουν αρκετές μαζί μπορεί να παρουσιαστεί φαινόμενο υπερθέρμανσης.
- Ακόμα οι κάρτες γραφικών δεν είναι σχεδιασμένες για να λειτουργούν η μία δίπλα στην άλλη, αλλά είναι σχεδιασμένες να δουλεύει η κάθε μία ξεχωριστά για ένα υπολογιστή.
- Ένα ακόμα θέμα προκύπτει με την κατανάλωση ενέργειας. Οι κάρτες γραφικών καταναλώνουν αρκετά μεγάλη ποσότητα ρεύματος, με συνέπεια να φέρουν πολύ μεγαλύτερο κόστος σε σχέση με τους απλούς υπολογιστές.



(Μία κατασκευή από 72 κάρτες γραφικών GeForce για την εξόρυξη bitcoin.
Πηγή : wccfttech.com)

Κάποιοι miner ωστόσο ξεκίνησαν τη διαδικασία της εξόρυξης των Bitcoin στις αρχές της δεκαετίας του 2010 με τη χρήση των FPGAs. Χρησιμοποιήθηκε μια ειδικά γλώσσα προγραμματισμού για να μπορέσουν να προγραμματίσουν τα FPGAs (Field Programmable Gate Arrays). Η λογική πίσω από τον τρόπο αυτόν είναι να πιάσει κατά προσέγγιση την απόδοση του custom hardware καθώς ο κάθε χρήστης του λογισμικού αυτού μπορεί να το επαναπρογραμματίσει μέσα στο πεδίο (μέσα στο field). Τα πλεονεκτήματα σε σχέση με τα GPUs είναι :

- Έχουν πολύ καλύτερη απόδοση σε σχέση με τα GPUs και τα τσιπ τα συγκεκριμένα μπορούν και κάνουν πολύ πιο γρήγορα τους υπολογισμούς που χρειάζεται η διαδικασία της εξόρυξης.
- Η διαδικασία της ψύξης είναι πολύ καλύτερη και πολύ πιο εύκολη για το λογισμικό αυτό σε σχέση με τα GPUs.
- Ακόμα μπορούμε να χρησιμοποιήσουμε όλα τα διαθέσιμα τρανζίστορ που υπάρχουν μέσα στο τσιπ για τη δημιουργία των bitcoin.
- Τέλος, είναι πολύ πιο εύκολο να στήσεις μία κατασκευή και να τακτοποιήσεις μία συστοιχία από FPGAs σε σχέση με μία συστοιχία από τα GPUs.

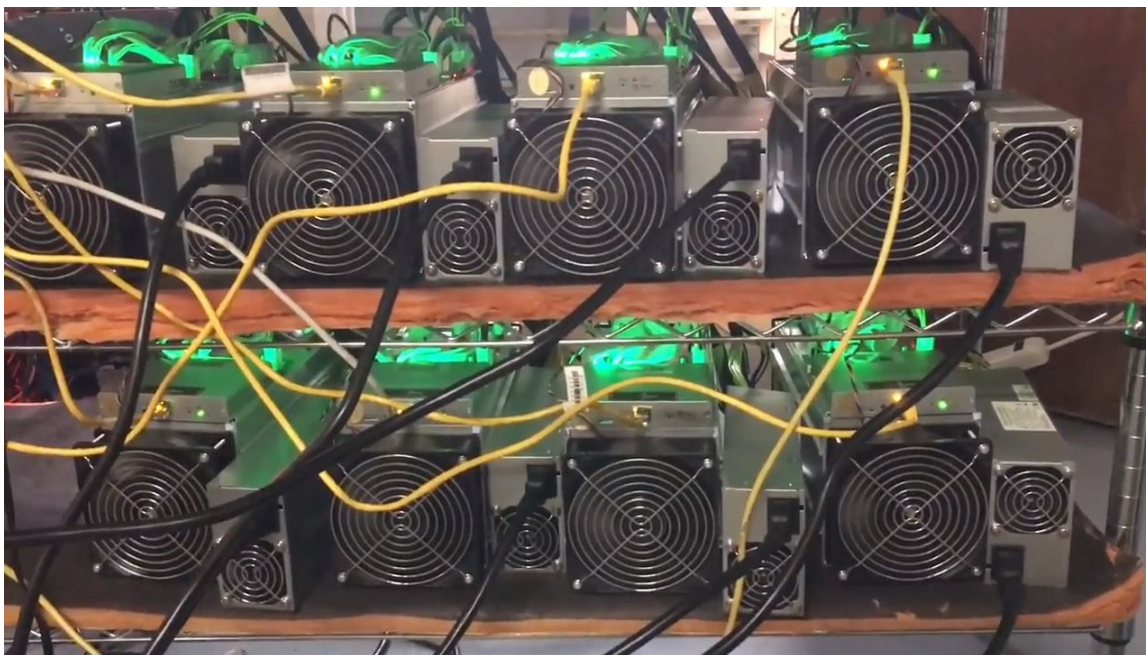


(Μία κατασκευή από 8 FPGAs για την εξόρυξη bitcoin.
Πηγή : BitcoinExchangeguide.com)

Για να αντιληφθούμε την τρομακτική δυσκολία της διαδικασίας της εξόρυξης των bitcoin όπως έχει γίνει σήμερα, αρκεί να σκεφτούμε ότι εάν χρησιμοποιήσουμε ένα hardware σαν το FPGAs με μία πολύ καλή χρήση του, μπορούμε να έχουμε μέχρι και 1 gigahash ανά δευτερόλεπτο. Αλλά ακόμα και να είχαμε δεκάδες hardware (όπως συνέβαινε και τις κάρτες γραφικών GPUs) θα μας έπαιρνε κάποιες δεκάδες χρόνια μέχρι να δημιουργήσουμε ένα μπλοκ στο δίκτυο του bitcoin. Τα μειονεκτήματα που είχε η συγκεκριμένη μέθοδος εξόρυξης ήταν ότι :

- Λόγω του γεγονότος ότι οι miner τα συγκεκριμένα hardware όπως και τα GPUs τα προγραμματίζουν με τέτοιο τρόπο ώστε να δουλεύουν πολύ παραπάνω από το κανονικό τους, πολύ συχνά παρατηρήθηκαν φαινόμενα με λάθος υπολογισμούς στη διαδικασία της δημιουργίας των καινούργιων μπλοκ.
- Επίσης ένα σημαντικό μειονέκτημα είναι ότι δεν είναι τόσο εύκολο να βρεις τα συγκεκριμένα hardware σε κάποιο κατάστημα σε σχέση με τα GPUs.
- Λιγότεροι άνθρωποι σε σχέση με τις GPUs μπορούν να στήσουν και να προγραμματίσουν τα FPGAs.
- Τέλος και πιο σημαντικό το κόστος λειτουργίας του συγκεκριμένου hardware ήταν απλά οριακά καλύτερο σε σχέση με τα GPUs οπότε ούτε η χρήση τους στη διαδικασία της εξόρυξης κράτησε για πολύ καιρό, μερικούς μήνες κυρίως.

Σήμερα και μετά από τις δύο προηγούμενες γενιές των hardware με τα οποία γινόταν η διαδικασία της εξόρυξης, έρχεται η τρίτη γενιά των hardware τα οποία είναι τα ASICs (Application-Specific Integrated Circuits) και έχουν κυριεύσει ως ο πλέον κατάλληλος εξοπλισμός, τον οποίο χρειάζεται ένας miner. Στην ουσία αυτά είναι εξοπλισμοί που έχουν κατασκευαστεί αποκλειστικά και μόνο για τη διαδικασία της εξόρυξης των bitcoin. Υπάρχουν κάποιοι μεγάλοι προμηθευτές οι οποίοι με τη σειρά τους προμηθεύουν τους miner με αυτά τα τσιπ ενώ διαφέρουν ανάλογα με το μέγεθός τους, το κόστος τους και την ενέργεια που χρειάζονται. Λόγω και της αναγκαιότητας και της μεγάλης ζήτησης, τα συγκεκριμένα τσιπ μπορούμε να πούμε ότι σχεδιάστηκαν και αναπτύχθηκαν πολύ γρήγορα, ενώ και ο χρόνος που άντεχαν συνήθως λόγω και της συνεχόμενης και καθημερινής λειτουργίας, ήταν οι έξι μήνες περίπου. Αξίζει να αναφέρουμε όμως ότι οι πρώτες γενιές των ASICs δεν προσέφεραν τις αναμενόμενες αποδόσεις, αλλά σίγουρα από τότε οι συσκευές αυτές έχουν αλλάξει χαρακτηριστικά και έχουν σαφώς καλύτερες επιδόσεις.



(Μία κατασκευή από ASICs κατάλληλα για την εξόρυξη bitcoin.
Πηγή : Cryptoage.com)

Πλέον στις μέρες μας, η διαδικασία της εξόρυξης έχει αλλάξει και γίνεται σε μεγάλες εγκαταστάσεις τα λεγόμενα mining farm. Δηλαδή η εξόρυξη των bitcoin σήμερα, έχει απομακρυνθεί από τους μικρούς ιδιώτες, που μπορούσαν με μία απλή κεντρική μονάδα CPU να δημιουργούσαν μπλοκ, και έχει περάσει στα χέρια των μεγάλων εταιρειών που έχουν την δυνατότητα να αγοράσουν αρκετά μεγάλο εξοπλισμό, ικανό να μπορεί να ανταποκριθεί στη τεράστια δυσκολία που παρουσιάζει σήμερα το mining. Αρκετές πληροφορίες για το πόσο και τί ακριβώς εξοπλισμό χρησιμοποιούν αυτά τα mining center δεν έχουμε αλλά αυτό γίνεται μάλλον γιατί αυτά τα center προφανώς θέλουν να προστατευτούν από τον ανταγωνισμό και να διατηρήσουν αν μπορούν κάποιο πλεονέκτημα. Όπως όμως βλέπουμε από την βιβλιογραφία, λογικά χρησιμοποιούνται κάποια πιο ειδικά τσιπ ASIC τα οποία είναι αρκετά εξειδικευμένα και δεν μπορούν να αγοραστούν εύκολα από έναν απλό ιδιώτη. Αυτά τα κέντρα εξόρυξης, πιο πολύ εντοπίζουν τρεις βασικές συνθήκες που θέλουν να είναι όσο το δυνατόν καλύτερες προς αυτά. Αυτές οι τρεις συνθήκες είναι :

- Τις κλιματολογικές συνθήκες που επικρατούν στη περιοχή εγκατάστασης του mining center.
- Το κόστος της ηλεκτρικής ενέργειας που είναι απαραίτητο για τη λειτουργία των υπολογιστών.
- Την ταχύτητα του δικτύου του ίντερνετ της περιοχής εγκατάστασης.

Προφανώς όσον αφορά τις κλιματολογικές συνθήκες οι εταιρείες αυτές θέλουν να είναι όσο το δυνατόν πιο χειμωνιάτικες για να μην υπερθερμαίνονται τα συστήματά τους. Το θέμα του κόστους της ηλεκτρικής ενέργειας είναι επίσης ένα σημαντικό ζήτημα γιατί η διαδικασία της εξόρυξης των Bitcoin απαιτεί τεράστια ποσά ενέργειας και όσο πιο φτηνό ρεύμα βρεί μία εταιρεία που έχει το mining farm τόσο λιγότερα τα έξοδα για εκείνη. Και τέλος σίγουρα έχουμε ανάγκη από πολύ γρήγορες ταχύτητες για να έχουμε πολύ καλύτερες αποδόσεις στην εξόρυξη των bitcoin. Η αλήθεια είναι ότι χώρες όπως η Γεωργία και η Ισλανδία είναι πολύ δημοφιλείς προορισμοί για να εγκαταστήσει κάποιος μεγάλα κέντρα εξειδικευμένα στην εξόρυξη των bitcoin.



(Κέντρο εξόρυξης bitcoin στη Σιβηρία.
Πηγή : coindesk.com)

Όπως φαίνεται, hardware σαν το ASIC, είναι το μόνο που ανταποκρίνεται όχι μόνο στις δυσκολίες της εξόρυξης που παρουσιάζει σήμερα το bitcoin, σε αντίθεση με τα hardware τύπου GPU και CPU, αλλά και στο κομμάτι του κέρδους.

Η ανάπτυξη των μεγάλων κέντρων εξόρυξης bitcoin μπορεί να εγείρει ζητήματα που αφορούν το εάν και κατά πόσο οι μεμονωμένοι miner απομονώνονται με αποτέλεσμα, η εξόρυξη των Bitcoin να πηγαίνει προς τη μεριά αποκλειστικά και μόνο στις τεράστιες εγκαταστάσεις που βλέπουμε σε χώρες όπως η Σιβηρία, η Ισλανδία και η Γεωργία. Μην ξεχνάμε ότι η κεντρική ιδέα του Νακαμότο, το 2008 ήταν οι μικροί μεμονωμένοι miner να μπορούν να κάνουν την εξόρυξη των bitcoin από το σπίτι τους (Nakamoto,2008).

Ένα από τα πιο σημαντικά κομμάτια και μπορεί και το πιο σημαντικό στη διαδικασία της εξόρυξης των bitcoin είναι η κατανάλωση ενέργειας. Υπάρχουν τρία είδη ενέργειας στην όλη διαδικασία που πολλές φορές μπορεί και να μην είναι τόσο προφανή :

- Υπάρχει η ενέργεια που καταναλώνεται η οποία σχετίζεται με την δημιουργία των hardware τα οποία είναι εξειδικευμένα στην εξόρυξη των bitcoin. Ακόμα μπορούμε να συμπεριλάβουμε την ενέργεια που χρειάζονται αυτά τα υλικά από τη στιγμή που θα τα παραγγείλουμε μέχρι την στιγμή που θα έρθουν σε εμάς. Η ενέργεια αυτή υπάρχουν σχέψεις ότι μπορεί να μειώνεται όσο λιγότεροι άνθρωποι παραγγέλνουν μέσω διαδικτύου τα υλικά που χρειάζονται για τη κατασκευή ενός ASIC.
- Δεύτερον, έχουμε την ηλεκτρική ενέργεια. Από τη στιγμή που τα μηχανήματα εξόρυξης όπως τα ASIC τεθούν σε λειτουργία, καταναλώνουν ηλεκτρική ενέργεια. Το δίκτυο του bitcoin καταναλώνει συνολικά τρομακτικά επίπεδα ενέργειας, που μπορούν να συγκριθούν με επίπεδα κατανάλωσης χωρών όπως η Δανία. Ακόμα έχουν υπάρξει σημαντικές ειδοποιήσεις επιστημόνων που λένε ότι η κατανάλωση ενέργειας στα κρυπτονομίσματα μπορεί να οδηγήσουν σε αύξηση της παγκόσμιας θερμοκρασίας. Για αυτό το λόγο γίνονται προσπάθειες έτσι ώστε να γίνεται χρήση ενέργειας η οποία είναι πιο φιλική προς το περιβάλλον.
- Τρίτο και τελευταίο είδος που υπάρχει στη διαδικασία της εξόρυξης είναι η ενέργεια που χρειάζεται για την ψύξη των μηχανημάτων. Γενικά μπορούμε να πούμε 'τι το είδος της ενέργειας που χρειάζεται για την ψύξη των μηχανημάτων είναι η ηλεκτρική ενέργεια. Εδώ πολλές κέντρα εξόρυξης κρυπτονομισμάτων επιλέγουν τόπους όπως αναφέραμε παραπάνω που το κλίμα είναι ιδιαίτερα ψυχρό έτσι ώστε και το κόστος της ψύξης των μηχανημάτων να μπορούν να το περι-ορίζουν.

Συμπερασματικά, κλείνοντας το κομμάτι της εξόρυξης των bitcoin, αξίζει να αναφέρουμε κάποιες σημαντικές αποφάσεις που θα πρέπει ο κάθε miner να πάρει :

- Θα πρέπει να αποφασίσει ποιες συνδιαλλαγές θα συμπεριλάβει μέσα στα μπλοκ που θα δημιουργήσει.
- Θα πρέπει να δει ποιο είναι το μπλοκ που θα επιλέξει έτσι ώστε να επεκτείνει τη πιο μεγάλη αλυσίδα.
- Αν δύο μπλοκ ανακοινωθούν την ίδια στιγμή, η στρατηγική του miner θα πρέπει να είναι να επιλέξει να «χτίσει» επάνω στο μπλοκ που «άκουσε» πρώτο.

- Θα πρέπει να επιλέξει τη χρονική στιγμή που θα ανακοινώσει τα νέα μπλοκ το δίκτυο του bitcoin. Κανονικά θα έπρεπε να τα ανακοινώσει την ίδια στιγμή που θα τα δημιουργήσει αλλά καλό είναι να περιμένει λίγο για να είναι σε θέση να αμυνθεί από επιθέσεις double-spend.

2.0.6 Πλεονεκτήματα και μειονεκτήματα του bitcoin

Σε αυτό το κομμάτι της εργασίας θα αναφερθούμε στα πλεονεκτήματα και στα μειονεκτήματα που παρουσιάζει το κρυπτονομίσμα του bitcoin. Όπως έχουμε αναφέρει και προηγουμένως, τα bitcoin και γενικά τα κρυπτονομίσματα, είναι από τα ζητήματα που απασχολούν και τους αναλυτές και τους επενδυτές σε παγκόσμιο επίπεδο. Με τον όρο κρυπτονομίσμα εννοούμε ένα ψηφιακό είδος χρήματος το οποίο όμως για να χρησιμοποιηθεί και να κατασκευαστεί χρησιμοποιεί αλγορίθμους κρυπτογράφησης. Το σημαντικό με τα κρυπτονομίσματα και αυτό που τα κάνει να διαφέρουν από τα κλασικά νομίσματα όπως τα γνωρίζουμε, είναι ότι δεν εκδίδονται από καμία Κεντρική Τράπεζα, αλλά ούτε υπάρχει μία ρυθμιστική Αρχή η οποία να είναι υπεύθυνη πχ για τη κυκλοφορία του εκάστοτε κρυπτονομίσματος, όπως είναι η Ευρωπαϊκή Κεντρική Τράπεζα που είναι υπεύθυνη για τη κυκλοφορία του Ευρώ. Από αυτή την άποψη θα μπορούσαμε να πούμε ότι τα κρυπτονομίσματα έφεραν μία κάποια επανάσταση στο χώρο του νομίσματος με αυτά τα χαρακτηριστικά που διαθέτει (Stegaroιu,2018). Το bitcoin μπορούμε να πούμε ότι είναι το πιο γνωστό ψηφιακό νόμισμα στο κόσμο από τη στιγμή που ο Satoshi Nakamoto το σύστησε πρώτη φορά στο κόσμο το 2008. Βέβαια και αυτό έχει και τα πλεονεκτήματα και τα μειονεκτήματά του. Ουσιαστικά, το πιο σημαντικό πλεονέκτημα του Bitcoin είναι ότι διευκολύνει σε τεράστιο βαθμό αλλά και με πολύ μεγάλη ασφάλεια την συνδιαλλαγή μεταξύ δύο μερών. Παρακάτω στο κομμάτι που ακολουθεί θα καταγράψουμε τα κυριότερα πλεονεκτήματα και μειονεκτήματα που εμφανίζουν τα bitcoin, με πρώτα που θα καταγράψουμε να είναι τα πλεονεκτήματα :

- Πρώτο και κύριο πλεονέκτημα του Bitcoin είναι ότι δίνει τη δυνατότητα στους χρήστες του να απολαμβάνουν μία τεράστια ελευθερία στις πληρωμές τους. Ένας χρήστης του bitcoin μπορεί να στείλει και να δεχθεί χρήματα χωρίς κανέναν απολύτως περιορισμό.
- Ένα δεύτερο πλεονέκτημα είναι ότι η ασφάλεια που προκύπτει από τη χρήση του. Λόγω του γεγονότος ότι οι χρήστες του, μπορούν να παρακολουθούν τις συνδιαλλαγές τους, αυτό αυτόματα βοηθά όλο το δίκτυο να παραμείνει ασφαλές. Δηλαδή από τη στιγμή που κάποιος χρήστης, θα χρεώσει παραπάνω κάποιον άλλον χρήστη για μία συνδιαλλαγή αυτό θα φανεί αμέσως στο δίκτυο.
- Επίσης το δίκτυο του bitcoin, προσφέρει σαφώς μία μεγάλη ανωνυμία διότι οι συναλλαγές που περιλαμβάνονται σε αυτό δεν περιλαμβάνουν προσωπικές πληροφορίες. Με αυτό το τρόπο εξασφαλίζεται ότι η ταυτότητα του κάθε χρήστη δεν θα αποκαλυφθεί.
- Ένα ακόμα πλεονέκτημα είναι ότι όλες οι συνδιαλλαγές είναι ανοικτές στον καθένα που θέλει να τις παρακολουθήσει. Δηλαδή ο καθένας μπορεί όποια ώρα θέλει να παρακολουθήσει τις συνδιαλλαγές στην αλυσίδα του δικτύου.

- Το πρωτόκολλο του δικτύου του bitcoin δεν μπορεί να χειραγωγηθεί από τον καθένα διότι είναι απόλυτα κρυπτογραφημένο μέσω των αλγορίθμων κρυπτογράφησης που χρησιμοποιεί.
- Ένα ακόμη πλεονέκτημα που έχει η χρήση των bitcoin είναι οι πολύ μικρές προμήθειες που υπάρχουν στις συναλλαγές.
- Επίσης το δίκτυο του bitcoin περιλαμβάνει διαδικασίες οι οποίες έχουν πολύ χαμηλότερες χρεώσεις σε σχέση με άλλα συστήματα πληρωμών όπως είναι οι πιστωτικές κάρτες ή το PayPal.
- Το δίκτυο του bitcoin προστατεύει σε πολύ μεγάλο βαθμό τους χρήστες του από ενδεχόμενες απάτες και κυρίως από επιθέσεις double-spend.
- Το δίκτυο του bitcoin χρησιμοποιεί ουσιαστικά εφαρμόζει τους ίδιους αλγόριθμους που χρησιμοποιούνται και από τις τράπεζες για το δίκτυο του on-line banking.
- Ένα ακόμη πλεονέκτημα που προκύπτει από τη χρήση του bitcoin είναι η απουσία του πληθωρισμού. Από τη κλασική μακροοικονομία γνωρίζουμε ότι ο πληθωρισμός υπάρχει σαν φαινόμενο και είναι έως αδύνατο να εξαλειφθεί. Η προσφορά όμως των Bitcoin είναι δεδομένη και υπολογίζεται στα 21 δισεκατομμύρια bitcoin. Εάν δεν αλλάξει κάτι σε αυτό τότε δεν υπάρχει πιθανότητα εμφάνισης πληθωρισμού.
- Ένα πολύ σημαντικό πλεονέκτημα του bitcoin είναι η αποκέντρωση όπως έχουμε αναφέρει και παραπάνω. Η απουσία δηλαδή μίας κεντρικής αρχής που ουσιαστικά θα επιβλέπει τις διαδικασίες μέσα στο δίκτυο.
- Το δίκτυο γενικά είναι εύκολο στη χρήση. Υπολογίζεται ότι χρειάζεται περίπου 5 λεπτά να κάνει κάποιος ένα ηλεκτρονικό πορτοφόλι και να το χρησιμοποιήσει αμέσως χωρίς κάποια παραπάνω δυσκολία ή να πρέπει να πληρώσει κάποια προμήθεια.
- Το δίκτυο του bitcoin εκτός των άλλων που αναφερθήκαμε προηγουμένως εξασφαλίζει ταχύτητα στις συναλλαγές του. Δηλαδή το να μπορείς να στείλεις χρήματα οπουδήποτε σε πολύ μικρό χρονικό διάστημα είναι ένα τεράστιο πλεονέκτημα που σου δίνει το δίκτυο της αλυσίδας του bitcoin.
- Σαν τελευταίο πλεονέκτημα θα μπορούσαμε να αναφέρουμε τη δυνατότητα που δίνει το δίκτυο του bitcoin να επενδύσεις σε επικερδείς πηγές.

Από τη στιγμή που υπάρχουν κάποια πλεονεκτήματα που αναφέρθηκαν παραπάνω, θα πρέπει να αναφέρουμε και τα αντίστοιχα μειονεκτήματα για να είναι η ανάλυσή μας, όσο το δυνατόν καλύτερη και πιο εμπεριστατωμένη. Το μεγαλύτερο μειονέκτημα γενικά που μπορούμε να πούμε είναι ότι πολλές χώρες δεν αναγνωρίζουν το bitcoin σαν νόμισμα συναλλαγής που μπορεί να χρησιμοποιηθεί ευρέως σε όλες τις εκφάνσεις της οικονομικής δραστηριότητας. Παρακάτω αναφέρουμε χαρακτηριστικά τα μειονεκτήματα όπως έχουν βρεθεί από την διεθνή βιβλιογραφία.

- Ο αριθμός των εταιρειών, των οργανισμών ακόμα και των κρατών που αναγνωρίζουν τα όποια οφέλη από τη χρήση του bitcoin, είναι πολύ μικρότερος σε σχέση με τον αριθμό αυτών που χρησιμοποιούν και αναγνωρίζουν ως μέσο συναλλαγής τα φυσικά νομίσματα.
- Πολλές φορές προκύπτει ένα κόστος εκπαίδευσης από την μεριά των εταιρειών προς τους εργαζόμενους, διότι το προσωπικό πρέπει να εκπαιδευτεί κατάλληλα για το πως θα βοηθήσει τους πελάτες, στη χρήση των bitcoin που αφορούν τις συναλλαγές τους.
- Επιπλέον ένα ακόμα μειονέκτημα των bitcoin είναι το ρίσκο και το πόσο ευμετάβλητες είναι οι τιμές τους. Αυτό η ευαισθησία προκύπτει από τη τεράστια ζήτηση που έχουν μέρα με τη μέρα και το ότι η προσφορά όπως εξηγήσαμε παραπάνω είναι συγκεκριμένη. Αν και αυτή η μεταβλητότητα αναμένεται να μειωθεί όσο ο αριθμός των εταιρειών και των καταστημάτων που δέχονται τα Bitcoin ως μέσο συναλλαγής αυξάνεται.
- Επιπλέον, θα πρέπει να σκεφτούμε ότι το bitcoin ως νόμισμα είναι ακόμα στην αρχή του, έτσι όπως και με όλα τα νομίσματα που είναι στην αρχή τους, υπάρχουν ακόμα διαδικασίες που πρέπει να γίνουν και γίνονται, έτσι ώστε να είναι όλο και πιο ασφαλές.
- Τέλος ένα σημαντικό μειονέκτημα είναι ότι εγείρονται συζητήσεις που αφορούν το γεγονός ότι διάφορα κέντρα μπορούν να εκμεταλλευτούν τη τεχνολογία που κρύβεται πίσω από το bitcoin και την ανωνυμία του, με σκοπό την προώθηση μη νόμιμων διαδικασιών όπως το ξέπλυμα μαύρου χρήματος είτε την προώθηση άλλως εγκληματικών ενεργειών μέσω του δικτύου της αλυσίδας του συγκεκριμένου κρυπτονομίσματος.

Κλείνοντας αυτό το κομμάτι αξίζει να αναφέρουμε ότι το bitcoin όπως και άλλα κρυπτονομίσματα, με όλα τα πλεονεκτήματα και τα μειονεκτήματά τους, να αντικαταστήσουν μελλοντικά τα υπάρχοντα φυσικά νομίσματα. Βέβαια για να γίνει αυτό θα πρέπει να προσπεράσουν προφανώς με τη βοήθεια της τεχνολογίας τα όποια κρίσιμα ζητήματα προκύπτουν. Αυτό βέβαια είναι μάλλον πολύ δύσκολο έως απίθανο να συμβεί στο κοντινό μέλλον (Bunjaku, Trajkovska, Kacarski, 2018) .

2.0.7 Άλλα κρυπτονομίσματα που βασίζονται στον αλγόριθμο PoW

Σε αυτό το κομμάτι της εργασίας θα ασχοληθούμε με κάποια άλλα κρυπτονομίσματα, που όπως και το bitcoin χρησιμοποιούν τον αλγόριθμο του Proof of Work. Πρώτα θα ασχοληθούμε με το κρυπτόνισμα του Ethereum.

Ethereum

Γενικά αυτό που ξέρουμε από την ανάπτυξη της τεχνολογίας είναι ότι οτιδήποτε καινούριο δημιουργείται από την τεχνολογία, δημιουργείται γιατί θα μας λύσει ένα πρόβλημα. Έτσι και το Ethereum δεν μπορούσε να αποτελέσει κάτι διαφορετικό από αυτό. Το Ethereum δημιουργήθηκε σε μία εποχή, που οι άνθρωποι γενικότερα είχαν δει και είχαν πειστεί ότι το δίκτυο του bitcoin φέρει μαζί του μία τεράστια δύναμη και μία εξέλιξη στη κυκλοφορία του χρήματος και στις παραδοσιακές συναλλαγές όπως τις γνωρίζαμε μέχρι τότε. Με μία διαφορά, κάποιοι θέλανε να πάνε ένα βήμα ακόμα παρακάτω σε σχέση με τις εφαρμογές που πρόσφερε το δίκτυο του bitcoin μέχρι τότε. Οι προγραμματιστές λοιπόν ήρθαν αντιμέτωποι με ένα ζήτημα που ήταν το εξής : Θα έπρεπε να διαλέξουν εάν θα βασίζονταν επάνω στο δίκτυο του bitcoin ή θα έπρεπε να δημιουργήσουν από την αρχή μία καινούργια αλυσίδα. (Αντωνόπουλος, Wood, 2018) Για περιπτώσεις όμως που οι χρήστες χρειαζόντουσαν περισσότερη ελευθερία αλλά και μία δυνατότητα επέκτασης και σε άλλες εφαρμογές, η ιδέα μία καινούργιας αλυσίδας, βασιζόμενη στην αλυσίδα του bitcoin, έμοιαζε η μόνη λύση. Αυτό όπως προφανώς δεν ήταν κάτι εύκολο, απαιτούσε πολύ μεγάλη προσπάθεια και αρκετό προγραμματισμό με μία πολύ δύσκολη κωδικοποίηση. Το 2013 λοιπόν, ο Vitalik Buterin, ένας προγραμματιστής αλλά και υπέρμαχος της τεχνολογίας που συνόδευε το Bitcoin, σκέφτηκε να μεγαλώσει τις δυνατότητες που προσέφερε το bitcoin μέχρι εκείνη τη στιγμή. Στα τέλη του ίδιου χρόνου ο Vitalik ανακοίνωσε μέσω ενός paper και υπογράμμιζε την όλη του ιδέα που έδειχνε το Ethereum. Βέβαια εκείνη την εποχή λίγοι άνθρωποι έδωσαν σημασία στη δουλειά του και θέλησαν να βοηθήσουν. Έτσι ο Vitalik μαζί με έναν άλλο προγραμματιστή τον Gavin, εξέλιξαν την ιδέα που είχε αρχικά ο Vitalik και δημιούργησαν από κοινού ένα πρωτόκολλο που αργότερα έγινε με βάση αυτό το κρυπτόνισμα του Ethereum (Wood 2019). Έτσι οι προγραμματιστές του Ethereum σκεφτόντουσαν να δημιουργήσουν μία αλυσίδα από μπλοκ που να μην έχουν κάποιον σαφή σκοπό, αλλά με το κατάλληλο προγραμματισμό που μπορούσε να υποστηρίξει μία πληθώρα από επιλογές. Με λίγα λόγια ένα προγραμματιστής χρησιμοποιώντας τη βάση του Ethereum, μπορούσε να προγραμματίσει τις ξεχωριστές εφαρμογές που ήθελε, χωρίς να χρειάζεται να πρέπει να εφαρμόσει όλους τους μηχανισμούς του δικτύου peer to peer και των αλγορίθμων συναίνεσης, προσφέροντας όμως ένα ασφαλές περιβάλλον για αποκεντρωμένες εφαρμογές πάνω στην αλυσίδα των μπλοκ. Ο Vitalik και ο Gavin δεν ανακάλυψαν κάποια καινούργια τεχνολογία, απλά «έμπλεξαν» κάποιες

ιδέες που είχαν με τεχνολογίες που ήταν ήδη γνωστές μέχρι τότε (όπως η τεχνολογία του blockchain) και δημιούργησαν το κώδικα του Ethereum.

Το κρυπτονόμισμα του Ethereum έχει τέσσερα βασικά επίπεδα ανάπτυξης, τα οποία παρουσιάζονται παρακάτω :

- Frontier, το οποίο θεωρείται και το αρχικό στάδιο του Ethereum του οποίου η χρονική διάρκεια κράτησε από τον Ιούλιο του 2015 έως και τον Μάρτιο του 2016.
- Homestead, το οποίο θεωρείται και το δεύτερο στάδιο ανάπτυξης του συγκεκριμένου κρυπτονομίσματος και ξεκίνησε από τον Μάρτιο του 2016 (όταν τελείωσε δηλαδή το πρώτο βασικό στάδιο ανάπτυξης).
- Metropolis, που θεωρείται το τρίτο βασικό στάδιο ανάπτυξης και ξεκίνησε τον Οκτώβρη του 2017.
- Serenity, που είναι ουσιαστικά το τελικό στάδιο ανάπτυξης του Ethereum.



(Το σήμα του κρυπτονομίσματος Ethereum.

Πηγή : Forbes.com)

Bitcoin Cash

Όπως αναφέρθηκε και προηγουμένως, τα ψηφιακά νομίσματα έκαναν δυναμική είσοδο στην αγορά μετά το 2010. Πολλές φορές η τεχνολογία δεν οδηγεί πάντα στη δημιουργία καινούργιων κρυπτονομισμάτων, αλλά αντίθετα έχουμε διαχωρισμό ενός νομίσματος. Ο διαχωρισμός των κρυπτονομισμάτων οφείλεται στη τεχνολογία. Τεχνολογικές διαφοροποιήσεις που σχετίζονταν και με την ασφάλεια έχουν παρουσιάσει από καιρό στο bitcoin (Yi, Cho, Sohn, Ahn, 2020). Παρόλα αυτά οι χρήστες του δικτύου δικτύου δεν είχαν βρει μία λύση η οποία θα ήταν ενδεδειγμένη στα ζητήματα της ασφάλειας.

Ο πρώτος διαχωρισμός λοιπόν του Bitcoin έγινε με τη δημιουργία του Bitcoin Cash. Αυτό ο διαχωρισμός έγινε από το mining pool με το όνομα Bitmain το 2017. Στην ουσία κάθε pool μπορεί να διαχωρίσει το κρυπτονόμισμα σε άλλο νόμισμα για να ικανοποιήσει τους στόχους που το ίδιο έχει θέσει. Έτσι στην οικογένεια των Bitcoin, εκτός από το Bitcoin Cash, έχει προστεθεί το Bitcoin Gold, το Bitcoin Diamond και το Bitcoin SV.



(Το σήμα του κρυπτονομίσματος Bitcoin Cash.
Πηγή : bitcoincash.org)

Στην ουσία το Bitcoin Cash δημιουργήθηκε τον Αύγουστο του 2017 με σκοπό να γίνουν ευκολότερες οι συνδιαλλαγές αυξάνοντας τον αριθμό των μπλοκ στην αλυσίδα του Bitcoin. Το συγκεκριμένο κρυπτονόμισμα είναι βασίζεται στην ίδια φιλοσοφία που βασίζεται το bitcoin, δηλαδή είναι ένα κρυπτονόμισμα το οποίο χρησιμοποιεί ένα δίκτυο peer to peer για τις συνδιαλλαγές του. Όσο όμως η αξία του Bitcoin ανέβαινε σε πολύ μεγάλα ύψη, η χρησιμοποίηση του Bitcoin έμοιαζε πιο πολύ με επένδυση παρά με χρήση ενός συνηθισμένου νομίσματος. Κάπως έτσι δημιουργήθηκε το Bitcoin Cash. Η βασική διαφορά ενός Bitcoin με ένα Bitcoin Cash έγκειται στο μέγεθος του μπλοκ στην αλυσίδα. Το μέγεθος του μπλοκ ουσιαστικά καθορίζει πόσες συνδιαλλαγές χωράνε μέσα στο ίδιο το μπλοκ. Αυτό σήμερα σημαίνει ότι το μέγεθος ενός μπλοκ στο Bitcoin ισούται με ένα MB ενώ το μέγεθος ενός μπλοκ στο Bitcoin Cash είναι τριάντα δύο MB. Δηλαδή στο μπλοκ του Bitcoin χωράνε επτά μόνο συναλλαγές ενώ στο μπλοκ του Bitcoin Cash χωράνε 200 συναλλαγές.

Litecoin

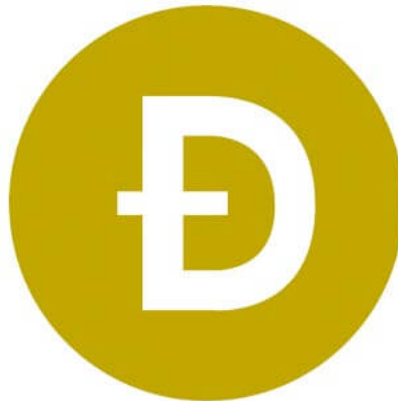
Το κρυπτονόμισμα του Litecoin είναι το δεύτερο πιο παλιό στη σειρά μετά το Bitcoin. Παρουσιάστηκε πρώτη φορά το 2011 και η αρχικές εκτιμήσεις έλεγαν ότι θα είναι μία πολύ πιο δυνατή και ανώτερη έκδοση σε σχέση με το Bitcoin (Barysevich, Solad, 2018). Η τεχνολογία που χρησιμοποιεί το Litecoin είναι σχεδόν η ίδια με αυτή του Bitcoin αλλά σε πολλές περιπτώσεις ακόμα καλύτερη, πράγμα που επέτρεπε εφαρμογές όπως η μεταφορά χρημάτων να γίνεται σε πολύ μικρότερο χρόνο και με πολύ μεγαλύτερη ταχύτητα. Ακόμα το συγκεκριμένο κρυπτονόμισμα επέτρεπε το να υπάρχουν πολύ μικρότερες χρεώσεις σε προμήθειες στις συναλλαγές αλλά έδινε και τη δυνατότητα να μπορεί να γίνεται εξόρυξη πολλών περισσότερων κρυπτονομισμάτων σε σχέση με το Bitcoin. Βέβαια ακόμα και με όλα αυτά τα πλεονεκτήματά του, το Litecoin δεν προσφέρει μεγαλύτερη ασφάλεια στις συναλλαγές σε σχέση με το Bitcoin. Το Litecoin λοιπόν είναι ένας ισχυρός αντίπαλος για το BTC και ο σκοπός της δημιουργίας του ήταν να μπορέσει να εξασφαλίσει μικρότερης αξίας συναλλαγές σε μικρότερο χρόνο σε σχέση με το BTC. Σύμφωνα με τον ιδρυτή του Charles Lee το LTC είναι το ασημένιο μετάλλιο ενώ το BTC είναι το χρυσό. Η κύρια διαφορά τους είναι ότι για να κάνεις εξόρυξη κρυπτονομισμάτων BTC χρειάζεσαι μεγάλο και ακριβό εξοπλισμό ενώ σε αντίθεση με το LTC χρειάζεσαι απλά τον υπολογιστή του σπιτιού σου με πολύ μικρότερη υπολογιστική ισχύ. Αυτή τη στιγμή υπολογίζεται ότι υπάρχουν 84 εκατομμύρια LTC σε σχέση με τα 21 εκατομμύρια BTC που κυκλοφορούν, ενώ ο χρόνος συναλλαγής για τα LTC είναι περίπου 2,5 λεπτά σε σχέση με τα 10 λεπτά που είναι στα BTC (Bhosale, Mavale, 2018).



(Το σήμα του κρυπτονομίσματος Litecoin.
Πηγή : cryptoslate.com)

Dogecoin

Άλλο ένα κρυπτονόμισμα που χρησιμοποιεί τον αλγόριθμο του Proof of Work είναι το Dogecoin. Αρχικά ε Το συγκεκριμένο ψηφιακό νόμισμα δημιουργήθηκε από τον Billy Markous και τον Jackson Palmer. Συχνά έχει επισημανθεί σαν το νόμισμα του διαδικτύου αλλά όπως γράφει και η επίσημη σελίδα του το dogecoin είναι ένα κρυπτονόμισμα που βασίζεται στην αποκέντρωση (όπως και το bitcoin), στην επικοινωνία peer to peer που βοηθά το χρήστη να στέλνει χρήματα με πολύ εύκολο τρόπο. Μία βασική διαφορά του με το BTC είναι ότι καθώς το bitcoin έχει αρκετές εφαρμογές το Dogecoin έχει μία εφαρμογή σχεδόν αποκλειστική θα έλεγε κάποιος στο τομέα του crowdfunding, με αποτέλεσμα η κοινότητα του Dogecoin να είναι χορηγός σε αγώνες ράλι τύπου ΝΑΣΚΑΡ, χορηγός εθνικών ομάδων σε χειμερινούς Ολυμπιακούς αγώνες. Το Dogecoin είναι επίσης διαφορετικό σε σχέση με το BTC γιατί δεν χρησιμοποιεί την συνάρτηση SHA για κρυπτογράφηση αλλά βασίζεται σε έναν αλγόριθμο «σκληρής μνήμης» (Young,2018). Μέχρι τον Φεβρουάριο του 2021 η κεφαλαιοποίηση του υπολογιζόταν στα 10 δισεκατομμύρια δολάρια ενώ το 2014 η κεφαλαιοποίηση του άγγιζε τα 60 εκατομμύρια δολάρια. Σε αντίθεση με άλλα ψηφιακά νομίσματα το Dogecoin είχε μία πολλή μεγάλη αύξηση στη παραγωγή των κρυπτονομισμάτων του, που το 2015 άγγιζε τα 100 δισεκατομμύρια δολάρια, ενώ είχε μία πρόσθετη παραγωγή 5,5 σχεδόν δισεκατομμυρίων ψηφιακών νομισμάτων κάθε χρόνο (Chohan, 2021). Μπορεί στην αρχή οι ιδρυτές του Dogecoin να το εισήγαγαν σαν ένα «αστείο» κρυπτονόμισμα αλλά σύντομα εξελίχθηκε σε έναν πολύ σοβαρό αντίπαλο για το Bitcoin. Η δομή του Dogecoin βασίστηκε σε ένα κρυπτονόμισμα της εποχής, το Luckycoin που αυτό με τη σειρά του είχε βασιστεί στο Litecoin.



(Το σήμα του κρυπτονομίσματος Dogecoin.
Πηγή : Usethebitcoin.com)

Monero

Ακόμα ένα ψηφιακό νόμισμα που χρησιμοποιεί τον αλγόριθμο PoW είναι το Monero. Το συγκεκριμένο κρυπτονόμισμα έχει μία ιδιαιτερότητα : δίνει τη δυνατότητα στο χρήστη να αποκρύπτει το γράφημα των συναλλαγών του, συμπεριλαμβάνοντας κάποια νομίσματα που τα ονομάζει «mixins» μαζί όμως με τα πραγματικά νομίσματα που ξοδεύει (Miller, Moser, Lee, Narayanan, 2017). Το κρυπτονόμισμα του Monero βασίζεται επάνω στο πρωτόκολλο Cryptonote. Το Monero με τη χρήση αυτού του πρωτοκόλλου μπορεί και αποκρύπτει τα γραφήματα των συναλλαγών όπως είπαμε και παραπάνω, ενώ το κάθε καινούργιο μπλοκ μπορεί να δημιουργηθεί ανά δύο λεπτά. Το συγκεκριμένο ψηφιακό νόμισμα έκανε την εμφάνισή του το 2014. Μία σημαντική διαφορά του σε σχέση με τα άλλα κρυπτονομίσματα είναι ότι μπορείς να στείλεις και να λάβεις συναλλαγές χωρίς όμως να γίνεται αυτό γνωστό σε όσους να εξετάσουν την αλυσίδα του blockchain. Το λογισμικό που χρησιμοποιείται εδώ έχει προγραμματιστεί εξ αρχής να ανανεώνεται κάθε έξι μήνες, γεγονός που έχει βοηθήσει σε πολύ μεγάλο βαθμό να προστίθενται νέες εφαρμογές χωρίς μεγάλη αμφισβήτηση επάνω σε αυτές. Ο τρόπος αυτός που στην ουσία επαναπρογραμματίζει το τρόπο λειτουργίας του συγκεκριμένου κρυπτονομίσματος, έχει οδηγήσει στην παρουσίαση νέων λειτουργιών προς τους χρήστες όπως είναι η λειτουργία “stealth addresses”, που δίνει τη δυνατότητα στους χρήστες να δημιουργήσουν one-time διεύθυνση όπως και τη λειτουργία “ring confidential transactions” για να αποκρύπτουν το μέγεθος των συναλλαγών τους (Noether, 2015).























(Το σήμα του κρυπτονομίσματος Monero.
Πηγή : CrazyMining.com)

Zcash

Ανάμεσα από τα δεκάδες κρυπτονομίσματα που βασίστηκαν στο BTC, το ψηφιακό νόμισμα του Zcash, είναι αυτό που είναι περισσότερο γνωστό για την εξασφάλιση της ανωνυμίας του χρήστη και αυτό το οφείλει στη πολύ καλή κρυπτογραφική μέθοδο που έχει. Ο στόχος του ως εναλλακτικό κρυπτονόμισμα απέναντι στο Bitcoin ήταν να σπάσει τη σχέση που υπάρχει ανάμεσα στον αποστολέα και στο δέκτη του νομίσματος (Kappos, Yousaf, Maller, Meiklejohn, 2018). Στο δίκτυο του Bitcoin οι αποδέκτες των νομισμάτων δέχονται τα νομίσματα σε διευθύνσεις και όταν τα σπαταλούν αυτά τα νομίσματα, τα σπαταλούν από τις διευθύνσεις αυτές. Αυτή η κατανάλωση των νομισμάτων δημιουργεί ένα σύνδεσμο ανάμεσα στον αποδέκτη και τον αποστολέα. Και αυτές τις σχέσεις στο δίκτυο της αλυσίδας του Bitcoin μπορείς να ανιχνεύσεις οποιοδήποτε νόμισμα από την δημιουργία του μέχρι και το τωρινό του κάτοχο. Και αυτή τη σχέση με βάση τον προγραμματισμό του, κατάφερε και έσπασε το νόμισμα του Zcash μέσω του shielded pool. Δηλαδή στο δίκτυο του Zcash κάθε συναλλαγή που έχει σχέση με το αυτό το pool, μπορούμε να πούμε ότι διαχωρίζεται σε δύο μέρη που βοηθά να ξέρουμε από ποιον έρχονται τα νομίσματα και που πάνε. Για να δεχθεί κάποιος χρήστης του δικτύου νομίσματα θα πρέπει να δείξει μία διεύθυνση που μπορούν να τη δουν όλοι την t διεύθυνση, ή μία μυστική διεύθυνση την z διεύθυνση. Τα νομίσματα που κρατούνται στη διεύθυνση z λέμε ότι βρίσκονται στο shielded pool. Για να εξειδικεύσουμε που κατευθύνονται τα νομίσματα ο διαχωρισμός που γίνεται περιέχει μία λίστα από t διευθύνσεις με τα χρήματα που τις συνοδεύουν που τις ονομάζουμε zOut, δύο «θωρακισμένα» output και ένα κρυπτογραφημένο σημείωμα (Ramos, Zanko, 2018).



(Το σήμα του κρυπτονομίσματος Zcash.
Πηγή : FixedFloat.com)

#	Name	Algorithm	Block Time	Marketcap	Price	24h Volume	Change 24h	Change 7d
1	 Bitcoin #1 BTC	 SHA256	10 minutes	\$625.87B	\$33,376.03	\$26,403,017,477	+1.64%	-0.13%
2	 Ethereum #2 ETH	 Ethash	~14 seconds	\$248.71B	\$2,132.55	\$23,073,605,805	-0.98%	+1.76%
3	 Dogecoin #7 DOGE	 Scrypt	60 Seconds	\$28.51B	\$0.21872	\$3,068,073,067	+2.44%	-9.65%
4	 Bitcoin Cash #12 BCH	 SHA256	10 minutes	\$9.42B	\$501.221	\$1,357,031,811	+1.31%	+3.03%
5	 Litecoin #14 LTC	 Scrypt	~2.5 minutes	\$8.92B	\$133.670	\$1,531,805,703	+0.9%	-0.28%
6	 Ethereum Classic #19 ETC	 Ethash	N/A	\$5.8B	\$49.8306	\$2,543,264,859	-0.79%	-4.82%
7	 Monero #28 XMR	 CryptoNight	120 seconds	\$3.78B	\$210.356	\$153,110,499	+1.93%	+2.36%
8	 Bitcoin SV #38 BSV	 SHA256	10 minutes	\$2.6B	\$138.357	\$519,381,883	-1.46%	-2.83%
9	 Decred #53 DCR	 Blake (14r)	5 minutes	\$1.66B	\$126.765	\$79,010,083	+3.69%	-6.13%
10	 Zcash #62 ZEC	 Equihash	2.5 minutes	\$1.35B	\$110.956	\$265,488,163	-1.24%	-3.52%

(Τα δέκα πρώτα κρυπτονομίσματα που χρησιμοποιούν τον αλγόριθμο PoW. Πηγή : <https://cryptoslate.com/cryptos/proof-of-work>)

2.0.8 Ο αλγόριθμος PoW και πως λειτουργεί

Στο σημείο αυτό της εργασίας θα αναφερθούμε στον αλγόριθμο Proof of Work (PoW) και στο τρόπο λειτουργίας του. Παραπάνω, αναφερθήκαμε στα κρυπτονομίσματα που βασίζεται ο τρόπος λειτουργίας τους σε αυτόν τον αλγόριθμο. Τώρα θα δούμε με περισσότερες λεπτομέρειες τι κάνει αυτός ο αλγόριθμος και γιατί επιλέγεται από αρκετά κρυπτονομίσματα. Στην ουσία ο συγκεκριμένος αλγόριθμος αποτελεί μία κεντρική ιδέα στα σύγχρονα ψηφιακά νομίσματα ανάμεσα τους και το κυρίαρχο όλων που είναι το Bitcoin. Οι χρήστες του δικτύου που θέλουν να κάνουν εξόρυξη στα κρυπτονομίσματα πρέπει να λύσουν κάτι σαν ένα παζλ, που στη πραγματικότητα είναι μία κρυπτογραφική συνάρτηση η οποία όμως απαιτεί για την λύση της συγκεκριμένο χρόνο και υπολογιστική ισχύ (Ma, Gans, Tourky, 2018). Αυτό το υπολογιστικό πρόβλημα (παζλ όπως αναφέρθηκε προηγουμένως), δεν είναι κάτι καινούργιο, βασίζεται στον Back που το πρότεινε το 2002 ως μία λύση για να αποτρέψει πολλούς να στέλνουν spam email και να υπερφορτώνουν το σύστημα. Δηλαδή για να στείλεις ένα email, θα έπρεπε πρώτα να λύσεις ένα proof of work για να αποδείξεις ότι το email σου είναι κανονικό και όχι spam και αποτελεί κομμάτι του Hashcash proof of work. Η υπολογιστική δύναμη που θα χρειαστείς και το κόστος ηλεκτρικής ενέργειας για να λύσεις αυτό το υπολογιστικό πρόβλημα θα είναι κάτι σαν απόδειξη ότι δεν θες να γεμίσεις με spam email το σύστημα. Στη διαδικασία του mining όμως και ειδικότερα το Bitcoin χρησιμοποιεί ένα κομμάτι του Hashcash Proof of Work για να μπορεί να επαληθεύει το δίκτυο τις συναλλαγές και να ασφαρίζει την αλυσίδα των μπλοκ. Το Hashcash proof of work αποτελεί μία συνάρτηση κόστους η οποία μας δείχνει πόση προσπάθεια χρειάζεται για να λύσουμε ένα υπολογιστικό πρόβλημα (Biryukov, Khovratovich, 2017). Στο Bitcoin για παράδειγμα η συνάρτηση αυτή μας δείχνει πόσους υπολογισμούς πρέπει να κάνουμε πριν μπορέσουμε να λύσουμε αυτό το παζλ. Η συνάρτηση δέχεται μία είσοδο χωρίς

προκαθορισμένο μέγεθος και το τοποθετεί σε μία έξοδο με συγκεκριμένο μέγεθος που το ονομάζουμε hash. Αυτή η συνάρτηση κόστους έχει κάποιες ιδιαιτερότητες :

- Είναι σχεδόν αδύνατον έως και απίθανο να μπορέσει κάποιος αυτή τη συνάρτηση να την αντιστρέψει.
- Το ποια θα είναι η έξοδος για την συνάρτησης είναι καθαρά τυχαίο γεγονός.
- Η λύση του παζλ θα δεν θα βρεθεί με εύκολο τρόπο αλλά θα μπορεί εύκολα να την επιβεβαιώσει κάποιος.

Αν υποθέσουμε ότι έχουμε μία έξοδο σε μία συνάρτηση k , τότε το υπολογιστικό πρόβλημα proof of work για να το λύσουμε πρέπει να βρούμε μία είσοδο n τέτοια ώστε να ισχύει η εξίσωση, $k(n)=k$. Για παράδειγμα στο δίκτυο του Bitcoin κάθε μπλοκ της περιέχει την έξοδο k από το προηγούμενο μπλοκ. Με αυτό το τρόπο κιόλας όλα τα μπλοκ συνδέονται μεταξύ τους και χρονολογικά. Οι χρήστες λοιπόν του δικτύου θα πρέπει να συναγωνιστούν μεταξύ τους για το ποιος θα είναι ο πρώτος που θα βρει την τιμή του n από τη συνάρτησης κόστους τέτοιο ώστε $k(n)=k$. Όπως είπαμε και σε προηγούμενο κομμάτι της εργασίας το δίκτυο του bitcoin χρησιμοποιεί τη συνάρτησης κρυπτογράφησης SHA-256 η οποία δίνει μία έξοδο 256 bit. Η έξοδος k αποτελείται και από μηδενικά και ο αριθμός των μηδενικών μας δείχνει και το βαθμό δυσκολίας του υπολογιστικού προβλήματος. Η συνάρτησης κόστους θα μας επιστρέψει έναν τυχαίο αριθμό μεταξύ 0 και 256 bit για κάθε υπολογισμό που κάνει. Από τη στιγμή που ένας χρήστης που θέλει να κάνει εξόρυξη των bitcoin βρεί μία έξοδο της συνάρτησης που προηγείται από τα απαιτούμενα μηδενικά, τότε θα έχει λύσει το υπολογιστικό πρόβλημα. Γνωρίζουμε ότι για να βρούμε μία έξοδο της συνάρτησης που προηγείται από n μηδενικά πχ θα χρειαστούμε 2^n υπολογισμούς κατά μέσο όρο για να λύσουμε το πάζλ.

Πάμε να δούμε μερικά πλεονεκτήματα που προκύπτουν από τη χρήση του αλγορίθμου αυτού.

- Το κύριο πλεονέκτημα έναντι όλων είναι ότι ο συγκεκριμένος αλγόριθμος δουλεύει σε σχέση με άλλους. Κανένας άλλος αλγόριθμος που βασίζεται στη συναίνεση δεν μπορεί να διατηρήσει σε τόσο μεγάλο βαθμό ασφαλές το αρχείο του.
- Επίσης ο PoW αλγόριθμος αποτρέπει τους κακόβουλους χρήστες να πάρουν θέση στο δίκτυο και να ετοιμάζουν επιθέσεις απέναντι στους άλλους χρήστες.
- Λόγω των πολλών χρηστών η δύναμη διαμοιράζεται. Δηλαδή δεν έχει σημασία πόσα νομίσματα έχει ο καθένας αλλά σημασία έχει πόσο υπολογιστική ισχύ έχει.

Από την άλλη μεριά υπάρχουν και τα αντίστοιχα μειονεκτήματα από τη λειτουργία του συγκεκριμένου αλγορίθμου.

- Πρώτο και σημαντικό μειονέκτημα είναι οι πηγές που χρειαζόμαστε για να μπορέσουμε να λύσουμε το πάζλ. Στο επίπεδο δυσκολίας που έχει φτάσει σήμερα πχ η εξόρυξη ενός bitcoin θα πρέπει να καταναλώσουμε μεγάλες ποσότητες ηλεκτρικής ενέργειας αλλά και να έχουμε στη κατοχή μας ακριβό εξοπλισμό, για να μπορέσουμε να λύσουμε πρώτοι το πάζλ. Αν αναλογιστούμε ότι όλο το δίκτυο του bitcoin πχ καταναλώνει την ηλεκτρική ενέργεια που καταναλώνουν χώρες όπως η Ισλανδία και η Σλοβενία.
- Ένα ακόμα μειονέκτημα είναι ότι με τη πάροδο του χρόνου η χρησιμοποίηση αυτού του αλγορίθμου μπορεί να οδηγήσει σε κεντροποίηση του συστήματος και η συγκέντρωση της δύναμης σε λίγους.
- Τελευταίο μειονέκτημα είναι ότι μπορείς να κάνεις χιλιάδες υπολογισμούς χωρίς να καταφέρεις να λύσεις το πάζλ πρώτος, και να μην έχεις και τίποτα να κερδίσεις από όλη αυτή την προσπάθεια που έπεσε ουσιαστικά στο κενό. Μένει μόνο να ξαναπροσπαθήσεις μήπως και λύσεις το επόμενο. Όποτε εδώ κάποιοι βλέπουν κάποιο χαμένο χρόνο αλλά και σπατάλη ηλεκτρικής ενέργειας χωρίς έστω κάποιο μικρό όφελος (Kent, Bain, 2020).

3 Επισκόπηση Βιβλιογραφίας

3.0.1 Βιβλιογραφική αναφορά των άρθρων και των αλγορίθμων μέτρησης κατανάλωσης ενέργειας που βασίστηκε η έρευνα

Σε αυτό το σημείο θα δώσουμε έμφαση στα άρθρα των ερευνητών αλλά και των αλγορίθμων που χρησιμοποίησαν έτσι ώστε να μετρήσουν την κατανάλωση ενέργειας στην εξόρυξη των κρυπτονομισμάτων.

- **Isaac R. Cason, Aaron Morris, Brandon Habig, Wenying Sun (2018).**
Προσπάθησαν να μετρήσουν την ενεργειακή κατανάλωση των τριών κρυπτονομισμάτων όπως είναι το Monero, το Ethereum και το ZCash. Τα τρία αυτά κρυπτονομίσματα χρησιμοποιούν τους αλγόριθμους Cryptonight (Monero), Ethash(Ethereum) και τον Equihash που χρησιμοποιεί το Zcash. Δημιουργήθηκαν τρεις πανομοιότυπες υπολογιστικές μηχανές που έδειξαν ότι ο αλγόριθμος Cryptonight V7 του Monero είναι ενεργειακά οικονομικότερος σε σχέση με τους άλλους δύο αλγόριθμους. Χρησιμοποίησαν για τη μέθοδο τους την οριακή ενέργεια (Marginal power), την συνολική ενέργεια (Total power) και την ενέργεια που καταναλώνει ο υπολογιστής όταν είναι σε αδράνεια (Baseline power). Όπου $\text{Marginal power} = \text{Total power} - \text{Baseline power}$. Οι υπολογιστές που χρησιμοποιήθηκαν διαθέτουν 4 GB RAM, λειτουργικό σύστημα Inubu Linux. Η ενεργειακή κατανάλωση P μετριέται ως $P=I \cdot E$ όπου I είναι η ένταση του ρεύματος και το E είναι δύναμη ηλεκτροκινητήρα σε volt, ενώ η ένταση της ισχύος τη μετράμε σε kilowatt ανά ώρα. Επίσης και στους τρεις υπολογιστές εγκαταστάθηκε το λογισμικό Claymore GPU Miner Software. Η στατιστική ανάλυση πραγματοποιήθηκε μέσω της μεθόδου ANOVA.
- **Oscar Delgado-Mohatar, Marta Felis-Rota , Carlos Fernández-Herraiz (2019).**
Η ανάλυση τους έδειξε ότι η εξόρυξη κρυπτονομισμάτων είναι πιο επικερδής ότι γίνεται από επαγγελματίες miners σε χώρες που η ηλεκτρική ενέργεια κοστίζει λιγότερο από 0,14 δολάρια/KWh. Η έρευνα τους έδειξε ότι το οριακό κόστος του Bitcoin ανέρχεται περίπου σε 1952 δολάρια, ενώ μετά την 23η Ιουνίου του 2018 η παραγωγή του bitcoin δεν είναι συμφέρουσα για ερασιτέχνες miners που βρίσκονται εκτός της Κίνας. Μάλιστα οι συγγραφείς προβλέπουν ότι στο μέλλον θα αυξηθεί η συγκέντρωση των miners στη Κίνα λόγω του ενεργειακού κόστους. Υπολόγισαν το μεταβλητό κόστος της παραγωγής ενός bitcoin ως $\text{BTC} = \text{number of Hashes/per block} * \text{Chash}$. Το κόστος ηλεκτρικής ενέργειας είναι το k ενώ η αποτελεσματικότητα με ϵ . Το $\text{Chash} = k \cdot \epsilon$ που δείχνει πόσο κοστίζει ένα hashrate.

- **Shaen Corbet, Brian Lucey, Larisa Yarovaya (2021).**

Οι συγγραφείς για να διερευνήσουν την σχέση μεταξύ της μεταβλητότητας των τιμών του bitcoin και των δυναμικών χαρακτηριστικών της εξόρυξης των κρυπτονομισμάτων, έλεγξαν τη δυσκολία της εξόρυξης, τα hashrate, τον ημερήσιο αριθμό των συναλλαγών και των αριθμό των μοναδικών διευθύνσεων από τους miners και το μέγεθος των block . Το hashrate ουσιαστικά είναι η ταχύτητα με την οποία ένας υπολογιστής ολοκληρώνει μία λειτουργία στο κώδικα του bitcoin. Οι συγγραφείς πήραν δεδομένα από το Bitfinex exchange για Bitcoin. Χρησιμοποιήθηκε η μέθοδος DCC-GARCH και έδειξε ότι η συνεχόμενη χρήση ενέργειας για τη παραγωγή των κρυπτονομισμάτων συνδέεται άμεσα με την αύξηση των τιμών στις αγορές ηλεκτρικής ενέργειας.

- **Li, Li, Peng, Cui, Wu (2018).**

Εδώ οι συγγραφείς ανέλυσαν 9 κρυπτονομίσματα που χρησιμοποιούν τη Proof Of Work και τα αποτελέσματα έδειξαν ότι η αποτελεσματικότητα της εξόρυξης εξαρτάται από τον αλγόριθμο. Στη συνέχεια η στατιστική ανάλυση μέσω της δι-αδικασίας benchmark έδειξε ότι υπάρχει μία γραμμική σχέση μεταξύ της ενέργειας που χρειάζεται η εξόρυξης και των hashrate. Στο τέλος της ανάλυσης τους έδειξαν ότι η το δίκτυο του Monero χρειάζεται 645,62 GWh ηλεκτρικής ενέργειας για όλο το 2018 με την κατανάλωση στη Κίνα να ανέρχεται σε 30,34 GWh, δηλαδή για το 4,7 τοις εκατό. Οι τόνοι διοξειδίου του άνθρακα υπολογίζονται σε 19,12 με 19,42 χιλιάδες μετά τον Απρίλιο του 2018 για την περιοχή της Κίνας.

- **Yaser Sobhanifard , Seyedjavad Sadatfarizani (2019).**

Η μελέτη αυτή αφορά τους παράγοντες που επηρεάζουν και προωθούν τη χρήση των κρυπτονομισμάτων. Όπως επισημαίνουν οι συγγραφείς τριάντα ένας παράγοντες που επηρεάζουν τη χρήση των κρυπτονομισμάτων. Επίσης τρεις παράγοντες έχουν θετική σχέση όσον αφορά τη χρήση των κρυπτονομισμάτων, είναι η τεχνολογικές δεξιότητες, η τεχνολογική ασάφεια και τα τεχνολογικά πλεονεκτήματα. Η μέθοδος που χρησιμοποιήθηκε ήταν η EFA, που χρησιμοποιείται ευρέως σε μεθόδους για τη διερεύνηση παραγόντων που επηρεάζουν μεταβλητές αλλά και το Fridman test.

- **Adam S. Hayes (2016).**

Εδώ ο συγγραφέας χρησιμοποίησε δεδομένα cross-sectional data από 66 κρυπτονομίσματα, δημιουργώντας ένα μοντέλο παλινδρόμησης έως και το 2016 που έγινε η μελέτη, και βρήκε τους τρεις κύριους παράγοντες που επηρεάζουν την αξία του κρυπτονομίσματος. Οι τρεις παράγοντες είναι οι εξής : το επίπεδο του ανταγωνισμού των miners μέσα στο δίκτυο του κρυπτονομίσματος, το ποσοστό της παραγωγής του κάθε miner και τη δυσκολία του αλγόριθμου που ο κάθε miner χρησιμοποιεί.

- **Vranken (2017).**

Εδώ ο συγγραφέας χρησιμοποιεί δεδομένα από το Blockchain.info και προσπαθεί να βρει τη κατανάλωση ενέργειας που χρειάζεται για τη παραγωγή των bitcoin. Καταλήγει στο συμπέρασμα ότι η εξέλιξη της τεχνολογίας από το mining hardware των GPU στα ASIC έχει αυξήσει και την αποτελεσματικότητα της ενεργειακής κατανάλωσης. Ο συγγραφέας υπολόγισε ότι η τάξη μεγέθους που απαιτείται για τη παραγωγή bitcoin με τα σύγχρονα μέσα είναι 100 MW. Στο τέλος μας λέει ότι όσο η διαδικασία της παραγωγής των κρυπτονομισμάτων γίνεται και πιο απαιτητική, αυτοί που θα “επιζήσουν” από τους miners θα είναι αυτοί που θα μπορέσουν να έχουν τα πιο ανταγωνιστικά hardware και να μπορούν να επωφεληθούν από τα χαμηλά κόστη της ηλεκτρικής ενέργειας.

- **Pierce Greenberg, Dylan Bugden (2018).**

Οι συγγραφείς εδώ προσπαθούν να βρουν ποιες θα είναι οι μακροπρόθεσμες προβλέψεις όσον αφορά τη κρυπτογράφησης, τη τεχνολογία του blockchain αλλά και τη γενικότερη αποθήκευση δεδομένων και την επεξεργασία τους που θα οδηγούσαν υπό προϋποθέσεις σε μία έκρηξη κατανάλωσης ενέργειας στις Ηνωμένες Πολιτείες της Αμερικής.

- **Valeriia Denisova, Alexey Mikhaylov, Evgeny Lopatin (2019).**

Οι συγγραφείς εδώ προβλέπουν ότι το ψηφιακό νόμισμα θα είναι το τρίτο στοιχείο της νομισματικής βάσης. Προβλέπουν πάντως ότι οι τεχνολογίες Blockchain θα επιφέρουν αρκετές αλλαγές στο χρηματοπιστωτικό τομέα. Χρησιμοποιούν το δείκτη του Herfindall index αλλά και το CR4 για να υπολογίσουν την συγκέντρωση στην αγορά. Τα δεδομένα για την κατανάλωση ενέργειας έχουν αποκτηθεί από τις ιστοσελίδες <https://coinmarketcap.com> και <https://eneroutlook.enerdata.net>.

- **Christophe Schinckus, Canh Phuc Nguyen, Felicia Chong Hui Ling (2019).**

Η μελέτη αυτή αφορά τη σχέση των περιβαλλοντικών επιπτώσεων και της κατανάλωσης ενέργειας από τα bitcoin. Τα δεδομένα που εξετάστηκαν αφορούν τις χρονικές περιόδους από το πρώτο μήνα του 2014 μέχρι το δωδέκατο μήνα του 2017. Αναλύθηκαν χρονοσειρές με τη μέθοδο των μοντέλων ARDL.

- **Mikhail Bondarev (2020).**

Ο συγγραφέας μας λέει ότι η εξόρυξη των bitcoin καταναλώνουν μεγάλες ποσότητες ηλεκτρικής ενέργειας. Τα έξοδα τους για το κόστος της ηλεκτρικής ενέργειας υπολογίζονται στο 30 τοις εκατό των εσόδων τους. Παράγοντες όπως η αξιοπιστία, η αποδοτικότητα και η απόδοση των μεθόδων εξόρυξης εξαρτώνται πολύ άμεσα από τη ποιότητα της ισχύος της ενέργειας που λαμβάνουν. Η απόδοση της εξόρυξης εξαρτάται επίσης από το πόσο καλά παίρνουν τη θερμότητα από τα θερμικά στοιχεία. Η μέθοδος που ακολουθεί ο συγγραφέας βασίζεται στη μελέτη του τριγώνου ενέργειας που αποτελείται από την ενεργή ενέργεια P, την δύναμη αντίδρασης Q και την εμφανή ενέργεια S (Dayong, 2020).

- **Roberto Leonardo Rana, Pasquale Giungato, Angela Tarabella and Caterina Tricase (2019).**

Οι συγγραφείς εδώ τονίζουν το γεγονός για την επιστημονική κοινότητα ότι το blockchain λαμβάνει αυξανόμενη προσοχή στην επιστημονική κοινότητα αλλά και στις τεχνολογικές εταιρείες στη κοινή χρήση ιατρικών δεδομένων.

- **Alex de Vries (2018).**

Η έρευνα στοχεύει στο καθορισμό της τωρινής αλλά και της μελλοντικής κατανάλωσης της ηλεκτρικής ενέργειας που καταναλώνει το δίκτυο του Bitcoin. Η έρευνα υπογραμμίζει ότι κατά μέσο όρο χρειάζεται 300 kWh για μία συνδιαλλαγή στο δίκτυο του Bitcoin. Η μέθοδος ανάλυσης του άρθρου είναι η στατιστική ανάλυση χρησιμοποιώντας μέσους όρους για τα hashrate, τα KWh, Mega Joule, από δεδομένα για τη κατανάλωση του δικτύου του bitcoin από bitmain, bitfury, blockchain.info

- **Kufeoglou, Ozkuran (2019).**

Για την ανάλυση τους οι συγγραφείς χρησιμοποίησαν 160 GB data από blockchain από 269 διαφορετικά hardware models (GPU, CPU, FPGA και ASIC) τα οποία χρησιμοποιούνται για τη διαδικασία εξόρυξης. Οι συγγραφείς ορίζουν δύο μέτρα για να μετρήσουν τη κατανάλωση ενέργειας, το πρώτο μέτρο διαλέγει το πιο αποτελεσματικό hardware στη διαδικασία της εξόρυξης και το άλλο μέτρο μετράει το κόστος της ηλεκτρικής ενέργειας και διαλέγουν το χειρότερο hardware από μεριάς της κατανάλωσης που κυκλοφορεί στην αγορά.

- **Polemis , Tsionas (2020).**

Η ανάλυση έγινε με τη με βάση τη Bayesian analysis και ένα quantile CQVAR μοντέλο που και οι συγγραφείς κατέληξαν ότι υπάρχει σημαντική σχέση μεταξύ της εκπομπής διοξειδίου του άνθρακα και της κατανάλωσης ενέργειας για τη παραγωγή του bitcoin.

- **June Ma, Joshua S. Gans, Rabee Tourky (2018).**

Το άρθρο βασίζεται στο πως μπορεί να διαμορφωθεί η αγορά του bitcoin. Λόγω της μεγάλης ενέργειας που καταναλώνεται από το δίκτυο του συγκεκριμένου κρυπτονομίσματος υπάρχει πολύ μεγάλο ενδιαφέρον από πολλούς ερευνητές. Οι συγγραφείς καταλήγουν ότι ο ρόλος του ανταγωνισμού μπορεί να είναι τέτοιος που αν δεν προκύπτουν ξεκάθαρα οφέλη από τον ανταγωνισμό, οι πόροι που θα δαπανούν οι miners μέσα στο ίδιο το σύστημα του bitcoin δεν θα αποφέρουν τα αναμενόμενα οφέλη.

- **Klaaben, Stoll, Gellersdofer (2020).**

Οι συγγραφείς χρησιμοποιώντας την μεθοδολογία της μέτρησης των hashrate, δηλαδή της ταχύτητας με την οποία η κάθε συσκευή ανά δευτερόλεπτο μπορεί να δημιουργήσει αλγόριθμους ικανούς να λύσουν το υπολογιστικό πρόβλημα και να δημιουργήσουν ένα block στην αλυσίδα του blockchain. Οι συγγραφείς καταλήγουν στο συμπέρασμα ότι το δίκτυο του Bitcoin ευθύνεται για τα 2/3 της παγκόσμιας κατανάλωσης ενέργειας ενώ τα υπόλοιπα κρυπτονομίσματα ευθύνονται για το υπόλοιπο 1/3. Επίσης επισημαίνουν ότι μόνο του το δίκτυο του Bitcoin μπορεί να προκαλέσει αρκετά μεγάλη ζημιά στο περιβάλλον με τη τεράστια κατανάλωση ενέργειας που καταναλώνει.

- **Johannes Sedlmeir, Hans Ulrich Buhl, Gilbert Fridgen, Robert Keller (2020).**

Στο άρθρο αυτό οι συγγραφείς συλλέγουν στοιχεία από το Coinmarketcap και από το Coinswitch και υπολογίζουν την ενεργειακή κατανάλωση με βάση τα hashrate.

- **Stachovski (2021).**

Σε αυτό το άρθρο μετρίεται η κατανάλωση ενέργειας μέσω ενός loop με τη βοήθεια της NVML βιβλιοθήκης για τους αλγόριθμους που τρέχουν τρία γνωστά κρυπτονομίσματα, το Ethereum, το Monero και το Zcash. Τα δεδομένα μετريούνται για ένα συγκεκριμένο χρόνο και αποθηκεύονται μέσα σε ένα φάκελο από τα οποία παίρνουν οι συγγραφείς τη μέση τιμή.

- **Oluwaseun Fadeyi , Ondrej Krejcar , Petra Maresova , Kamil Kuca , Peter Brida and Ali Selamat (2019).**

Εδώ οι συγγραφείς μελετούν τη κατανάλωση του bitcoin αντλώντας δεδομένα από το δίκτυο του bitcoin και μετρώντας τα hashrate υπολογίζουν στη συνέχεια και τη κατανάλωση ενέργειας.

- **Gustavo Pinto, Fernando Castor, Yu David Liu (2014).**

Εδώ οι συγγραφείς συγκέντρωσαν ερωτήσεις από το δίκτυο του StackOverflow που ήταν σχετικές με την κατανάλωση ενέργειας σε λογισμικά. Παρατήρησαν ότι οι ερωτήσεις οι οποίες ήταν σχετικές με τη κατανάλωση ενέργειας, ήταν πιο ενδιαφέρουσες για τους χρήστες και πιο δύσκολες από τη μέση ερώτηση που γινόταν στο δίκτυο αυτό. Παρατήρησαν ότι τα βασικά θέματα που σχετίζονταν με τη κατανάλωση ενέργειας στα κρύπτο ήταν σχετικά με τη : μέτρηση, Γενικές Γνώσεις, Σχεδιασμός κώδικα, Συγκεκριμένο περιβάλλον και Θόρυβος. Οι ερωτήσεις επίσης που αφορούν την τροποποίηση του κώδικα έχουν και τη περισσότερη προσοχή. Τα αποτελέσματα βασίστηκαν με τη μέθοδο της απλής γραμμικής παλινδρόμησης.

- **Debojyoti Das , Anupam Dutta (2019).**

Εδώ οι συγγραφείς μαζεύοντας δεδομένα από το δίκτυο του digieconomist και της βάσης δεδομένων Quandl και χρησιμοποιώντας τη μέθοδο παλινδρόμησης QR καταλήγουν στο συμπέρασμα ότι οι μεταβλητές της ενεργειακής κατανάλωσης του bitcoin και τα έσοδα των Miner έχουν αρνητική σχέση. Η αρνητική αυτή σχέση είναι αρκετά ισχυρή ειδικά όταν τα έσοδα των miner είναι χαμηλά και ευμετάβλητα. Η εξόρυξη των Bitcoin δεν είναι βιώσιμη εκτός και αν υπάρχει πρόσβαση σε φτηνές πηγές ενέργειας και αποτελεσματικό hardware.

3.0.2 Καταγραφή των βάσεων δεδομένων για την αναζήτηση των αλγορίθμων μέτρησης της κατανάλωσης της ενέργειας στα κρυπτονομίσματα.

Στην προσπάθεια υλοποίησης αυτής της διπλωματικής εργασίας σίγουρα χρειάστηκε η αναζήτηση αξιόπιστων πηγών από τις οποίες αντλήθηκαν πολύτιμες πληροφορίες από τις επιστημονικές έρευνες διάφορων επιστημών ανά τον κόσμο. Από την Αμερικανική Οικονομική Ένωση μέχρι το Διεθνές Γραφείο Οικονομικών Ερευνών, όλες οι βάσεις δεδομένων στάθηκαν αξιόπιστοι αρωγοί στην αναζήτηση των αλγορίθμων εκτίμησης της κατανάλωσης της ενέργειας που είναι και το θέμα αυτής της εργασίας. Παρακάτω αναφέρεται αναλυτικά και με τον ιστότοπό της κάθε βάση δεδομένων που χρησιμοποιήθηκε :

- American Economic Association, <https://www.aeaweb.org/econlit/>
- SSRN, <https://www.ssrn.com/index.cfm/en/>
- Cornell University, <https://arxiv.org/>
- EconPapers, <https://econpapers.repec.org/>
- National Bureau of Economic Research, <https://www.nber.org/>
- Google Scholar, <https://scholar.google.com/>
- Βιβλιοθήκη Πανεπιστημίου Κύπρου, <http://library.ucy.ac.cy/el/services/library-guides/article-search>
- Βιβλιοθήκη Ακαδημίας Αθηνών, <http://www.academyofathens.gr/el/library/collections/online>
- Βιβλιοθήκη Scopus, <https://www.scopus.com/home.uri?zone=headerorigin=>
- Βιβλιοθήκη Ινστιτούτο ERIC, <https://eric.ed.gov/?>

3.0.3 Αριθμός των δημοσιεύσεων σε κάθε βάση δεδομένων

Ενδεικτικά θα αναφέρουμε τον αριθμό δημοσιεύσεων σε κάποιες από τις βάσεις δεδομένων που χρησιμοποιήσαμε. Από την βάση δεδομένων της Αμερικανικής Ένωσης Οικονομολόγων που ιδρύθηκε το 1885, έχει μή κερδοσκοπικό χαρακτήρα και είναι αφοσιωμένη στη συζήτηση, αλλά και στη δημοσίευση της οικονομικής έρευνας, αντλήσαμε 7 άρθρα τα οποία δεν είναι απαραίτητα σχετικά με αλγόριθμους κατανάλωσης ενέργειας, αλλά σχετίζονται με το κρυπτονόμισμα του bitcoin γενικότερα. Οι λέξεις κλειδιά ή οι φράσεις που χρησιμοποιήθηκαν είναι οι κάτωθι:

- bitcoins
- cryptocurrencies
- Algorithms for energy consumption in cryptocurrencies
- Energy consumption of blockchain technology

Από τη βάση δεδομένων SSRN βλέπουμε ότι έχουν κατατεθεί 950.733 abstract, 816.075 επιστημονικά άρθρα, ενώ είναι διαθέσιμοι 503.172 συγγραφείς. Τα επιστημονικά άρθρα που έχουν εισαχθεί μέσα στο 2021 είναι 74.740. Μέχρι σήμερα παρατηρούμε ότι οι χρήστες της συγκεκριμένης βάσης έχουν κατεβάσει 154.585.947 papers, τους τελευταίους 12 μήνες 15.965.798, ενώ το τελευταίο μήνα 1.328.896. Όσον αφορά το θέμα της εργασίας παρατηρούμε ότι για τους τελευταίους :

- 6 μήνες - 3 paper που αφορούν τη κατανάλωση ενέργειας στα bitcoin.
- 3 μήνες - 2 paper που αφορούν τη κατανάλωση ενέργειας στα bitcoin.

ενώ για το τελευταίο μήνα δεν εισήχθη κάποιο paper που αφορά τη κατανάλωση ενέργειας στα bitcoin. Επιπλέον βρήκαμε 21 άρθρα το τελευταίο μήνα που αφορά το bitcoin γενικά, 75 άρθρα τους τελευταίους 3 μήνες και 174 άρθρα τους τελευταίους έξι μήνες. Οι λέξεις κλειδιά που χρησιμοποιήσαμε είναι :

- bitcoins
- cryptocurrencies
- Algorithms for energy consumption in cryptocurrencies
- Energy consumption of blockchain technology

Όσον αφορά τη βάση δεδομένων arXiv.org από τα διαθέσιμα στοιχεία που μπορούσαμε να βρούμε και με βάση τις αναζητήσεις μας με τις ίδιες λέξεις ή φράσεις κλειδιά, βρήκαμε 65 άρθρα για τα κρυπτονομίσματα αλλά δεν ήταν όλα σχετικά με το θέμα μας. Όλα βεβαίως ήταν αρκετά βοηθητικά για τη κατανόηση του συστήματος των κρυπτονομισμάτων.

Τέλος, για τη βάση δεδομένων EconPapers, πρέπει να πούμε ότι έχει τα περισσότερα άρθρα και τα πιο σχετικά σε σχέση με τις άλλες βάσεις δεδομένων. Γι αυτό το λόγο ενώ στις προηγούμενες βάσεις οι αναζητήσεις με τις λέξεις κλειδιά έφεραν σχετικά τα ίδια αποτελέσματα εδώ, εδώ κάθε λέξη που αλλάζαμε έφερνε και διαφορετικό αποτέλεσμα. Δηλαδή η αναζήτηση με τη λέξη cryptocurrencies για το τελευταίο μήνα μας έδωσε 40 άρθρα το τελευταίο μήνα από τα οποία αντλήσαμε πολλές πληροφορίες για τη κατανάλωση ενέργειας των bitcoin, ενώ για τους τελευταίους 3 μήνες μας επέστρεψε 177 άρθρα και για τους έξι μήνες 405. Η φράση "Energy and Cryptocurrencies" μας επέστρεψε 1 άρθρα τον τελευταίο μήνα της έρευνάς μας, 3 για τους τελευταίους μήνες ενώ 10 άρθρα για τους έξι. Τέλος η αναζήτηση της φράσης "Energy Algorithms of Cryptocurrencies" μας επέστρεψε πάνω από 2000 άρθρα, από τα οποία όμως ελάχιστα ήταν σχετικά με το θέμα μας, ενώ για τους τελευταίους 3 μήνες η αναζήτηση αυτή μας έδωσε πάνω από 10000 άρθρα από τα οποία όμως ούτε το 1 τοις εκατό από αυτά μας αφορούσε. Πιο πολλά και σχετικά άρθρα μας έδωσε η αναζήτηση με τη λέξη "Bitcoin" που τον τελευταίο μήνα μας επέστρεψε 34 άρθρα, τους τελευταίους 3 μήνες 152 και στους έξι μήνες 353.

3.0.4 Καταγραφή των μεθόδων εκτίμησης της κατανάλωσης ενέργειας

Στο πίνακα που ακολουθεί (Πίνακας 1) παρουσιάζονται συνολικά οι 21 αλγόριθμοι που εξετάσαμε με τον κάθε ερευνητή ή την κάθε ομάδα ερευνητών να προτείνουν ως προς την μέτρηση της ενεργειακής κατανάλωσης των κρυπτονομισμάτων.

Πίνακας 1			
Papers	Μεθοδολογία	Βάσεις από τις οποίες αντλήθηκαν τα δεδομένα	Μεταβλητές που χρησιμοποιήθηκαν για την ανάλυση
Isaac R.Cason, Aaron Morris, Brandon Habig, Wenying Sun (2018)	ANOVA	Δεν χρησιμοποιούν δεδομένα από άλλες βάσεις, τα δημιουργούν τα δεδομένα με τους υπολογισμούς σε κάθε υπολογιστή που χρησιμοποιούν.	Marginal power, Total power, Baseline power, P, I, E,
Oscar Delgado-Mohatar, Marta Felis-Rota, Carlos Fernández-Herraiz (2019)	Hashrates/sec	Quandl, 2018	BTC, number of Hashes/ per block, Chash, k, ε
Shaen Corbet, Brian Lucey, Larisa Yarovaya (2021)	DCC-GARCH	Bitfinex exchange	Difficulty of mining, hashrates, daily number of transactions, block size, number of id
Li, Li, Peng, Cui, Wu (2018)	Benchmark analysis, ARMA	Χρησιμοποιήθηκαν 9 αλγόριθμοι διαφορετικών κρυπτονομισμάτων και έκαναν ανάλυση σε αυτά τα δεδομένα που προέκυψαν	Hashrates, Power usage, air temperature, computer temperature, relative humidity
Yaser Sobhanifard, Seyedjavad Sadatfarizani (2019)	EFA, Friedman test, saturation approach	http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf .	Cryptocurrency, Price USD, Market cap USD,
Adam S. Hayes (2016)	least square multiple regression	bitcoinwisdom, blockchain.info	coinsmined, coins pre minute, algo, price, Giga Hashes/sec
Vranken (2017)	Μέσος όρος, hash rate	Blockchain.info, en.bitcoin.it/wiki/mining_hardware_comparison	P, R, E

Valeriia Denisova, Alexey Mikhaylov, Evgeny Lopatin (2019)	Herfindal index, CR4	https://coinmarketcap.com , https://eneroutlook.enerdata.net .	mined/day, cost/day, power, hashrate, profit per day, Power cost/week, Mined/month, Power cost/year, Profit per year
Christophe Schinckus, Canh Phuc Nguyen, Felicia Chong, Hui Ling (2015)	ARDL, X-12-ARIMA	US Energy Information, www.coinmarketcap.com Administration	Total primary energy consumption (seasonal adjustment) (Quadrillion BTU), Total indigenous electricity production (seasonal adjustment domestic electricity production - TWH), Trading volume of Bitcoin, Total trading volume on Cryptocurrency market
Mikhail Bondarev (2020)	Energy Triangle Method	bitcoinwisdom, blockchain.info	P,Q,S
Roberto Leonardo Rana, Pasquale Giungato, Angela Tarabella, Caterina Tricase (2019)	Geometric series	Adapted after de Vries, 2019a, Digiconomist	Number of bitcoins mined, Electricity
Alex de Vries (2018)	Hash rates	bitmain, bitfury, blockchain.info	Hash rates, Power usage, Electricity cost
Kufeoglou, Ozkuran (2019)	Minimum Energy Consumption, Maximum Energy Consumption	160 GB data από blockchain από 269 διαφορετικά hardware models (GPU, CPU, FPGA και ASIC)	Power demand, Network Hashrate, Efficiency of Hardware
Polemis, Tsionas (2020)	Bayesian analysis, quantile CQVAR	blockchain.info	Energy consumption of BTC, CO emissions
June Ma, Joshua S. Gans, Rabee Tourky (2018)	OLS	blockchain.info	Aggregate hash rate, Market price of BTC
Klaaben, Stoll, Gellersdofer (2020)	Hash rates	blockchain.info	Market capitalization, Energy efficiency, Hashrates, Rated power
Johannes Sedlmeir, Hans Ulrich Buhl, Gilbert Fridgen, Robert Keller (2020)	Hash rates	Coinswitch, Coinmarketcap	Energy consumption of BTC
Stachovski (2021)	Βιβλιοθήκη του NVML, μέσος όρος της κατανάλωσης ενέργειας, Hill Climbing, Simulated Annealing, Nelder-Mead	Τα data ανακτήθηκαν από τα test που έκανα οι μονάδες GPU.	Ethereum, Monero, Zcash
Oluwaseun Fadayi, Ondrej Krejcar, Petra Maresova, Kamil Kuca, Peter Brida, Ali Selamat (2019)	Μέσος όρος των Hash rates	bitcoin.info	Hashrates, Power use, Power efficiency
Gustavo Pinto, Fernando Castor, Yu David Liu (2014)	OLS	Stackoverflow	Questions Answers, S,P,A,F,V
Debojyoti Das, Anupam Dutta (2019)	OLS	digieconomist, Quandl	Energy consumption, Miner's revenue

Ας δούμε παρακάτω λίγα ενδιαφέροντα στοιχεία όσον αφορά τους αλγόριθμους του πίνακα που χρησιμοποιούνται για την εκτίμηση της κατανάλωσης της ενέργειας των κρυπτονομισμάτων.

1. Το 28 τοις εκατό των αλγορίθμων χρησιμοποιούν σαν κοινή μεθοδολογία την μέτρηση των hashrate. Στην ουσία τα hashrate εκφράζουν τον αριθμό των υπολογισμών που γίνεται ανά sec.
2. Το 14 τοις εκατό των αλγορίθμων χρησιμοποιούν σαν κοινή μεθοδολογία την OLS, δηλαδή την μέθοδο των ελαχίστων τετραγώνων.
3. Το 58 τοις εκατό των αλγορίθμων που μελετήθηκαν χρησιμοποιούν διαφορετική μεθοδολογία έναντι των υπολοίπων.
4. Μόνο ο ένας από τους 21 αλγόριθμους δεν αντλεί στοιχεία από συγκεκριμένη βάση αλλά εμφανίζει τα στοιχεία της κατανάλωσης της ενέργειας από τους υπολογισμούς που ο ίδιος κάνει.
5. Το 28 τοις εκατό των αλγορίθμων αντλούν στοιχεία από τη βάση δεδομένων blockchain.info
6. Το 14 τοις εκατό των αλγορίθμων αντλούν στοιχεία από τη βάση δεδομένων coinmarketcap.
7. Το 9 τοις εκατό των αλγορίθμων χρησιμοποιούν στοιχεία από τη βάση δεδομένων bitcoinwisdom.
8. Το 33 τοις εκατό των αλγορίθμων χρησιμοποιεί από κοινού τη μεταβλητή των hashrate για τον υπολογισμό της εκτίμησης της κατανάλωσης της ενέργειας.
9. Το 9 τοις εκατό των αλγορίθμων χρησιμοποιούν από κοινού τη μεταβλητή electricity.
10. Επίσης το 9 τοις εκατό από τους αλγόριθμους που παρουσιάστηκαν παραπάνω χρησιμοποιούν τη μεταβλητή της ενεργειακής κατανάλωσης των bitcoin.
11. Τέλος, το 9 τοις εκατό των αλγορίθμων χρησιμοποιούν τον αριθμό των bitcoin που γίνεται εξόρυξη στις εκτιμήσεις τους.

4 Ανάλυση των δεδομένων

4.0.1 Ανάλυση των δεδομένων των αλγορίθμων εκτίμησης κατανάλωσης ενέργειας - Συμπεράσματα ως προς τις μεθόδους και τα αποτελέσματα

Ο πρώτος αλγόριθμος που μελετήσαμε είναι των Cason, Habig και Sun που το 2018 θέλησαν να μετρήσουν την κατανάλωση ενέργειας ανάμεσα στα τρία κρυπτονομίσματα όπως είναι το Monero, το Zcash και το Ethereum. Στη προσπάθειά τους αυτή μέτρησαν τα δεδομένα κατανάλωσης της ενέργειας μέσα από τρεις ίδιους υπολογιστές και κατέληξαν στο συμπέρασμα ότι ο αλγόριθμος που τρέχει το Monero που είναι ο Cryptonight είναι και ο καλύτερος από άποψη ενεργειακής κατανάλωσης. Οι μεταβλητές που χρησιμοποίησαν στους υπολογισμούς τους ήταν : Marginal Power, Total Power και Baseline Power. Η στατιστική ανάλυση των δεδομένων έγινε μέσω της μεθόδου ANOVA.

Στη συνέχεια είδαμε τον αλγόριθμο των Mohatar, Rota και Herraiz που χρησιμοποιώντας τις μεταβλητές Chash, Hashesblock, k,ε, κατέληξαν στο συμπέρασμα ότι η εξόρυξη των κρυπτονομισμάτων έχει μεγαλύτερο κέρδος όταν γίνεται από επαγγελματίες miners σε χώρες όπου το κόστος της ηλεκτρικής ενέργειας κοστίζει λιγότερο από 0,14 δολάρια / KWh.

Οι Corbet, Lucey και Yarovaya το 2021 έχοντας δεδομένα από το Bitfinex exchange και χρησιμοποιώντας τη μέθοδο DCC-GARCH απέδειξαν ότι η συνεχόμενη χρησιμοποίηση ενέργειας για την εξόρυξη των κρυπτονομισμάτων συνδέεται πολύ ισχυρά με την άνοδο των τιμών στην ηλεκτρική ενέργεια. Στην ανάλυσή τους αυτή χρησιμοποίησαν ως μεταβλητές των αριθμό των block που δημιουργούνται, τα hashrate, τη δυσκολία της εξόρυξης και τον αριθμό των ημερήσιων συναλλαγών.

Οι Li, Li, Peng, Cui, Wu το 2018 απέδειξαν ότι η αποτελεσματικότητα της εξόρυξης και της κατανάλωσης της ενέργειας εξαρτάται από τον αλγόριθμο που χρησιμοποιεί το κάθε κρυπτονόμισμα. Για την έρευνά τους ανέλυσαν 9 κρυπτονομίσματα που χρησιμοποιούν τον αλγόριθμο PoW. Η ανάλυση Benchmark που πραγματοποίησαν έδειξε ότι υπάρχει μία γραμμικότητα στη σχέση μεταξύ της ενέργειας που χρειάζεται η εξόρυξη και των hashrate.

Οι Sobhanifard και Sadatfarizani το 2019 χρησιμοποιώντας το Friedman test και την EFA κατέληξαν στο συμπέρασμα ότι παράγοντες όπως οι τεχνολογικές δεξιότητες του ατόμου και τα τεχνολογικά πλεονεκτήματα επηρεάζουν θετικά τη χρήση των κρυπτονομισμάτων. Συνολικά βρήκαν 31 παράγοντες που επηρεάζουν συνολικά τη χρήση των κρυπτονομισμάτων.

Ο Hayes το 2016 ανέλυσε δεδομένα από 66 κρυπτονομίσματα και δημιούργησε ένα μοντέλο παλινδρόμησης και κατέληξε ότι παράγοντες όπως το επίπεδο του ανταγωνισμού των miner, το ποσοστό της παραγωγής των κρυπτονομισμάτων που έχει ο κάθε miner αλλά και η δυσκολία του αλγορίθμου που χρησιμοποιεί ο κάθε miner, επηρεάζουν την τελική αξία του κρυπτονομίσματος. Τα δεδομένα που συνέλεξε εδώ ο ερευνητής τα ανέλυσε μέσω ενός μοντέλου παλινδρόμησης.

Ο Vranken το 2017 αντλεί δεδομένα από τη βάση δεδομένων του Blockchain.info και καταλήγει στο συμπέρασμα ότι η εξόρυξη που γίνεται με βάση τις μονάδες ASIC είναι πολύ πιο αποτελεσματική σε σχέση με τα άλλα hardware. Ο ερευνητής καταλήγει στο συμπέρασμα ότι οι miner που θα έχουν καλύτερα hardware θα είναι και πιο αποτελεσματικοί στην εξόρυξη των κρυπτονομισμάτων.

Οι Greenberg και Bugden το 2018 προσπάθησαν να ερευνήσουν ποιες θα είναι οι μακροπρόθεσμες προβλέψεις της χρήσης των κρυπτονομισμάτων που θα μπορούσαν να οδηγήσουν σε μία κατακόρυφη άνοδο της κατανάλωσης της ενέργειας στις ΗΠΑ.

Οι Denisova, Mikhaylov και Lopatin το 2019 χρησιμοποιώντας δεδομένα από το coimarket.cap και enerdata.net και του δείκτη συγκέντρωσης Herfindall και του CR4 καταλήγουν στο συμπέρασμα ότι τα κρυπτονομίσματα θα επιφέρουν αρκετές αλλαγές στο χρηματοπιστωτικό σύστημα αλλά και το ότι η κατανάλωση ενέργειας στα κρυπτονομίσματα θα γίνεται πιο αποτελεσματική όσο οι miner χρησιμοποιούν καλύτερα hardware. Οι Schinckus, Nguyen και Ling μέσω ανάλυσης των χρονοσειρών από το 2014 μέχρι και το 2017 χρησιμοποιώντας το μοντέλο ARDL έδειξαν ότι η συνεχόμενη αύξηση της κατανάλωσης της ενέργειας στο κρυπτονόμισμα του bitcoin συνδέεται πολύ ισχυρά με την επιβάρυνση στο περιβάλλον.

Ο Bondarev το 2020 υπολογίζει ότι το κόστος για την κατανάλωση ενέργειας στην εξόρυξη των bitcoin ισοδυναμεί με το 30 τοις εκατό των εσόδων των miner και ότι η εξόρυξη ειδικά των Bitcoin απαιτεί πολύ μεγάλες ποσότητες ηλεκτρικής ενέργειας. Επίσης καταλήγει στο συμπέρασμα ότι παράγοντες η αποδοτικότητα και η απόδοση των μεθόδων εξόρυξης συνδέονται πολύ ισχυρά από την ποιότητα της ισχύος που λαμβάνουν. Οι μεταβλητές που χρησιμοποιεί είναι η ενεργή ενέργεια P , η δύναμη αντίδρασης Q και η εμφανή ενέργεια S .

Οι Rana, Giungato, Tarabella και Tricase το 2019 μέσω από την έρευνά τους καταλήγουν στο συμπέρασμα ότι οι τεχνολογίες όπως το Blockchain που στηρίζεται το bitcoin έχει ολοένα και μεγαλύτερη χρήση από τις εταιρείες τεχνολογίας προσπαθώντας οι ίδιες παράλληλα να βρουν, όσο το δυνατόν φιλικότερες πηγές ενέργειας για το δίκτυο εξόρυξης των κρυπτονομισμάτων.

Ο Vries το 2018 προσπαθεί να εκτιμήσει τη κατανάλωση ενέργειας που υπάρχει στο δίκτυο του Bitcoin και καταλήγει στο συμπέρασμα ότι κατά μέσο όρο χρειάζονται 300 kWh για μία συναλλαγή μέσα στο δίκτυο του Bitcoin. Ο συγγραφέας καταλήγει σε αυτό το συμπέρασμα υπολογίζοντας τους μέσους όρους και αντλώντας δεδομένα, από το δίκτυο του blockchain.info για τις μεταβλητές των hashrates, Mega Joule και Kwh. Οι Kufeoglou και Ozkuran το 2019 εξετάζοντας δεδομένα κατανάλωσης ενέργειας από διαφορετικά hardware ειδικά για την εξόρυξη κρυπτονομισμάτων (όπως ASIC, GPU και CPU) καταλήγουν να ορίσουν δύο μέτρα ως προς την επιλογή του πιο αποτελεσματικού hardware. Το πρώτο μέτρο επιλέγει το πιο αποτελεσματικό ως προς την εξόρυξη και το δεύτερο μέτρο επιλέγει το πιο αποτελεσματικό hardware από τη μεριά του κόστους της ηλεκτρικής ενέργειας. Λαμβάνοντας και τα δύο μέτρα υπόψιν το πιο αποτελεσματικό hardware κατά τους συγγραφείς είναι τα νέα γενιάς ASIC.

Οι Έλληνες Πολέμης και Τσιονάς το 2020 μέσω ενός CQVAR μοντέλου και μίας μπασσιανής ανάλυσης καταλήγουν στο συμπέρασμα ότι υπάρχει σημαντική σχέση ανάμεσα στη μεταβλητή των εκπομπών του διοξειδίου του άνθρακα και της μεταβλητής της κατανάλωσης ενέργειας που χρησιμοποιείται στην εξόρυξη του bitcoin.

Οι Ma, Gans και Tourky το 2018 προσπαθούν να συνδέσουν τη κατανάλωση της ενέργειας στην εξόρυξη των Bitcoin με τις συνθήκες που διαμορφώνονται στην αγορά του Bitcoin. Οι ερευνητές εδώ καταλήγουν στο συμπέρασμα ότι εάν δεν προκύπτουν σημαντικά οφέλη μέσω του ανταγωνισμού στην αγορά του bitcoin, οι πόροι που θα πρέπει να δαπανήσουν οι miner για την εξόρυξη των bitcoin και της ηλεκτρικής ενέργειας που είναι αναγκαία στη διαδικασία αυτή, δεν θα αποφέρουν τα αναμενόμενα

κέρδη για τους ίδιους τους miner.

Οι Stoll και Gellersdofer το 2020 μετρώντας τα hashrate από το δίκτυο του bitcoin συμπεραίνουν ότι η αλυσίδα του Bitcoin είναι υπεύθυνη για τα δύο τρίτα της παγκόσμιας κατανάλωσης ενέργειας ενώ όλα τα υπόλοιπα κρυπτονομίσματα ευθύνονται για το υπόλοιπο ένα τρίτο. Εδώ στην έρευνα των ερευνητών σχετικά με τις καταναλώσεις της ενέργειας των κρυπτονομισμάτων εγείρονται σημαντικά περιβαλλοντικά ζητήματα που έχουν να κάνουν με τη σχέση του δικτύου εξόρυξης του bitcoin και την αύξηση της παγκόσμιας θερμοκρασίας. Είναι ένα θέμα που δεν αφορά τη παρούσα διπλωματική εργασία αλλά είναι ένα σημαντικό θέμα το οποίο το συναντάμε συχνά στη διεθνή βιβλιογραφία.

Οι Sedlmeir, Buhl, Fridgen και Keller το 2020 αντλώντας στοιχεία από τη βάση δεδομένων Coinmarketcap και Coinswitch υπολογίζουν και αυτοί τα hashrate και καταλήγουν στο συμπέρασμα ότι το δίκτυο με τη μεγαλύτερη κατανάλωση ενέργειας είναι το δίκτυο των Bitcoin.

Ο Stachovski σε μία πρόσφατη έρευνά του το 2021 μετράει τη κατανάλωση ενέργειας στα τρία γνωστά κρυπτονομίσματα, το Monero, το Zcash και το Ethereum. Μέσω της NVML βιβλιοθήκης μετρά τα δεδομένα της κατανάλωσης της ενέργειας και καταλήγει ότι το Ethereum έχει τη μεγαλύτερη κατανάλωση ενέργειας από τα τρία αυτά κρυπτονομίσματα.

Οι Fadeyi, Krejcar, Maresova, Kuca, Brida και Selamat το 2019 αντλούν και αυτοί δεδομένα από το Blockchain.info και προσπαθούν να εκτιμήσουν συνολικά τη κατανάλωση ενέργειας του δικτύου του bitcoin. Τα αποτελέσματά τους είναι παρόμοια με αυτά του Vries το 2018.

Οι Pinto, Castor και Liu το 2014 σε μία έρευνα που έκαναν κατέληξαν στο συμπέρασμα ότι στο δίκτυο χρηστών του StackOverflow οι πιο συχνές ερωτήσεις που έκαναν οι χρήστες σχετικά με τη κατανάλωση ενέργειας στα κρυπτονομίσματα είχαν να κάνουν με τη μέτρηση της κατανάλωσης της ενέργειας και με την τροποποίηση του κώδικα. Τα αποτελέσματα βασίστηκαν στη μέθοδο της απλής γραμμικής παλινδρόμησης (OLS). Οι Das και Dutta το 2019 χρησιμοποιώντας τη μέθοδο της παλινδρόμησης QR και αντλώντας στοιχεία από το δίκτυο του digieconomist συμπέραναν ότι τα έσοδα των miner και οι μεταβλητές της κατανάλωσης της ενέργειας διατηρούν μία αρνητική σχέση. Με λίγα λόγια η δημιουργία των bitcoin δεν είναι συμφέρουσα εάν δεν υπάρχει φτηνή πηγή ενέργειας αλλά και η δυνατότητα απόκτησης αποτελεσματικού hardware εξειδικευμένα για την εξόρυξη κρυπτονομισμάτων.

4.0.2 Εκτίμηση κατανάλωσης ενέργειας μέσω του προγραμματιστικού περιβάλλοντος της Python

Μέσα από τον κώδικα στο προγραμματιστικό περιβάλλον της Python προσπαθήσαμε να αναδείξουμε μία προσπάθεια για να εκτιμήσουμε την καθημερινή κατανάλωση ενέργειας του κρυπτονομίσματος του Ethereum καθώς και τις ημερήσιες εκπομπές διοξειδίου του άνθρακα. Τα hashrate τα οποία έχουμε μετρηθεί χρονολογούνται από τα τέλη Ιουλίου του 2015 έως και τις 15 μαρτίου του 2021. Τα GPU που έχουν μελετηθεί έχουν χρησιμοποιηθεί στην αγορά από τις 8 Αυγούστου του 2013 με το πιο παλιό να είναι το Radeon R5240 και το πιο πρόσφατο που έχει χρησιμοποιηθεί για την εξόρυξη του Ethereum να είναι το GeForce RTX3060. Στην ουσία έχουν συλλεχθεί πληροφορίες σχετικά με τις κάρτες γραφικών GPU που τρέχουν τον αλγόριθμο Ethash για το Ethereum σε μία διάρκεια 6 χρόνων και εκτιμώνται κατά μέσο όρο η ποσότητα ενέργειας που καταναλώνεται από αυτές τις μηχανές εξόρυξης, σύμφωνα με τα hashrate που είναι σε θέση να εκτελέσει η κάθε μηχανή. Τα στοιχεία των hashrate που χρησιμοποιήθηκαν για την εκτίμηση της κατανάλωσης της ενέργειας αντλήθηκαν από τις παρακάτω πηγές :

1. tomshardware.com
2. whattomine.com
3. minerstat.com
4. 2cryptocalc.com
5. profitmine.com
6. asicminervable.com
7. hashrates.com
8. minermonitoring.com

Οι ακόλουθοι πίνακες (Πίνακες 2,3,4)δείχουν συνοπτικά στατιστικά στοιχεία που αφορούν τα hashrates, την ενέργεια σε Watt που καταναλώνει η κάθε μηχανή εξόρυξης αλλά και τις πηγές με τη χρονολογία που έχει αντληθεί η κάθε πληροφορία (δεν έχουν τοποθετηθεί όλα γιατί ήταν πάρα πολλά και θα ήταν κουραστικό και για τον αναγνώστη, παραθέτω την πηγή κάτω από τους πίνακες για να μπορεί κάποιος να μπει και να τα δει).

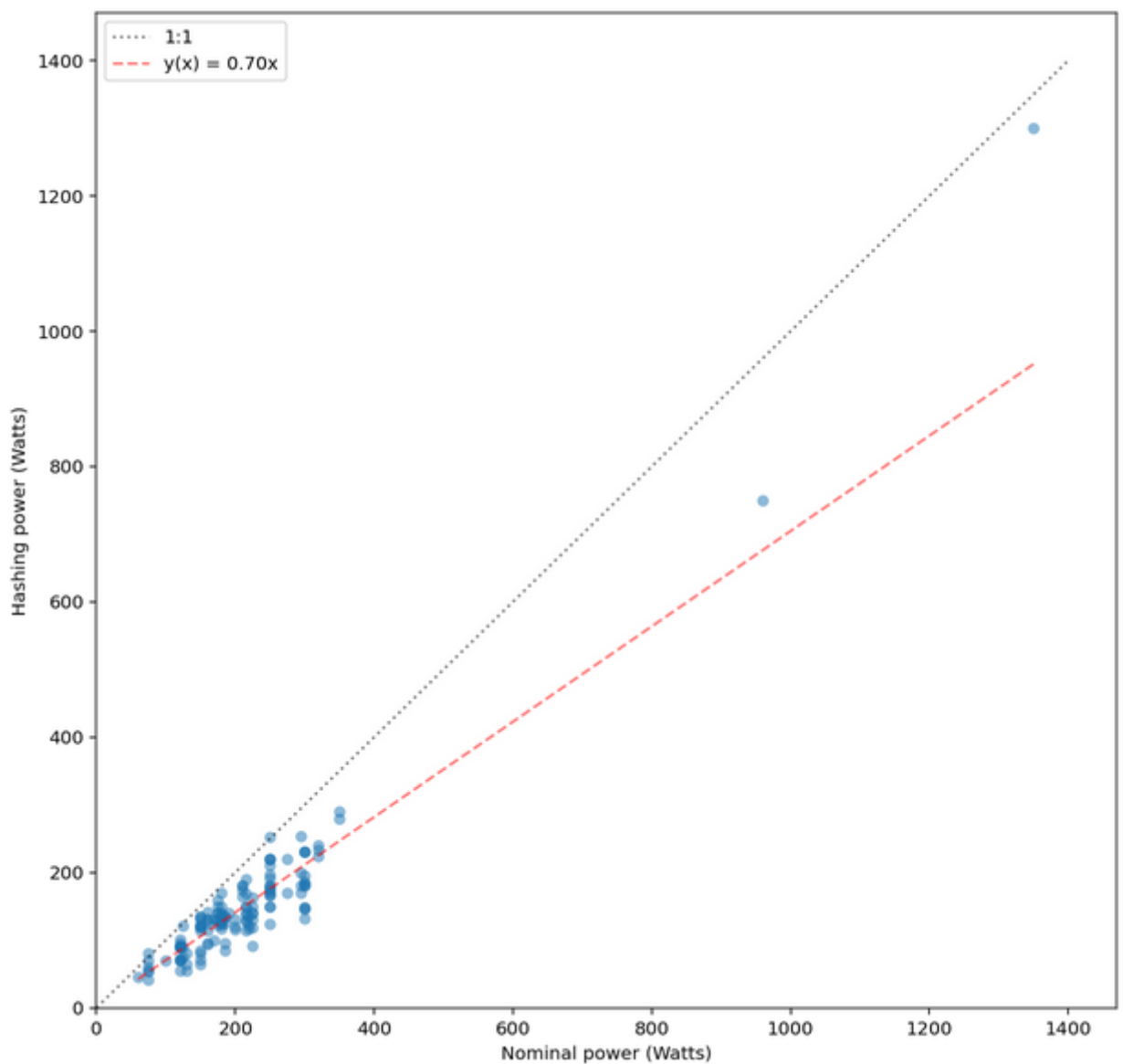
ΠΙΝΑΚΑΣ 2 : Ενδεικτικά τα μοντέλα GPU που χρησιμοποιήθηκαν για την ανάλυση της κατανάλωσης της ενέργειας στο Ethereum.			
ΜΟΝΤΕΛΟ	Hashrate (Mh)	ΕΝΕΡΓΕΙΑ (Watts)	ΠΗΓΗ
GeForce GTX 1070	29.32	122	minermonitoring.com
GeForce GTX 1060 6GB	23.14	95	minermonitoring.com
GeForce GTX 1070 Ti	31.42	123	minermonitoring.com
GeForce RTX 2080	43.5	169	minermonitoring.com
AMD RX 460	11.66	41	minerstat.com
Innosilicon A10 PRO ETHMaster	500	960	asicminervalue.com
Innosilicon A10 PRO+ ETHMiner	750	1350	asicminervalue.com
687F:C1 / 8 GB	25.2		hashrates.com
AMD 15D8:C9 / 8 GB	0.79		hashrates.com
AMD Radeon (TM) R7 M360 / 4 GB	1.28		hashrates.com
AMD Radeon RX 5700 XT /	4.02		hashrates.com
GeForce GTX 1050 Ti / 4 GB	15.6		hashrates.com
AMD Radeon R9 Fury	30	170	profit-mine.com
AMD Radeon RX 5700 XT	55	140	profit-mine.com
GeForce RTX 2060 Super	43.7	129	tomshardware.com
GeForce RTX 2080 Ti	60.1	180	tomshardware.com
Radeon RX Vega 64	40	200	whattomine.com
AMD Radeon RX 480	29		2cryptocalc.com
Antminer E3Ethash	190	760	minerstat.com
Πηγή : www.github.com			

Πίνακας 3 : Ενδεικτικός πίνακας με τις τιμές των Hashrate που χρησιμοποιήθηκαν για την μέτρηση της κατανάλωσης της ενέργειας.		
ΗΜΕΡΟΜΗΝΙΑ	ΚΩΔΙΚΟΣ ΧΡΟΝΙΚΗΣ ΑΝΑΦΟΡΑΣ	ΑΞΙΑ
7/30/2015	1438214400	11.5297
8/1/2015	1438387200	57.7845
8/16/2015	1439683200	231.8948
11/15/2015	1447545600	550.2513
3/7/2016	1457308800	1047.5369
3/15/2016	1458000000	1295.5505
3/20/2016	1458432000	1450.4615
12/5/2016	1480896000	5409.3217
1/26/2017	1485388800	8367.5758
2/6/2017	1486339200	8877.6557
5/23/2017	1495497600	30236.4543
9/3/2018	1535932800	274967.4979
9/11/2018	1536624000	255565.1744
12/5/2018	1543968000	185236.3756
12/13/2018	1544659200	171179.1852
9/9/2019	1567987200	177112.0631
11/15/2019	1573776000	184339.1196
3/10/2020	1583798400	182248.8650
3/15/2021	1615766400	439958.3667
Πηγή : Github.com		

Πίνακας 4 : Ενδεικτικός πίνακας των GPU με τις ημερομηνίες που εμφανίστηκαν στην αγορά και χρησιμοποιήθηκαν για την μέτρηση της κατανάλωσης της ενέργειας του Ethereum.

MONTEΛΟ	ΗΜΕΡΟΜΗΝΙΑ ΕΜΦΑΝΙΣΗΣ ΣΤΗΝ ΑΓΟΡΑ	ΕΝΕΡΓΕΙΑ (WATTS)
GeForce RTX 3060	25/2/2021	170
GeForce RTX 3070	29/10/2020	220
GeForce RTX 2060 TU104	10/1/2020	160
GeForce RTX 2070	17/10/2018	175
GeForce RTX 2080	20/10/2018	215
GeForce RTX 2080 Super	23/7/2019	250
GeForce GT 1010	January 2021	30
GeForce GT 1030	17/5/2017	30
GeForce GTX 1060 3GB	18/8/2016	120
GeForce GTX 1060 6GB (GDDR5X)	10/2018	120
GeForce GTX 1650 (GDDR6)	3/4/2020	75
GeForce GTX 1650 Super	22/11/2019	100
Radeon R7 M445	14/5/2016	20
Radeon R7 M465X	5/2016	
Radeon R5 220	21/12/2013	18
Radeon R9 370X	8/2015	185
Radeon RX 5700 XT 50th Anniversary Edition	7/7/2019	235
Innosilicon A10 PRO+ ETHMiner	12/2020	1350
Innosilicon A10 ETHMaster	9/2018	850
Πηγή : Github.com		

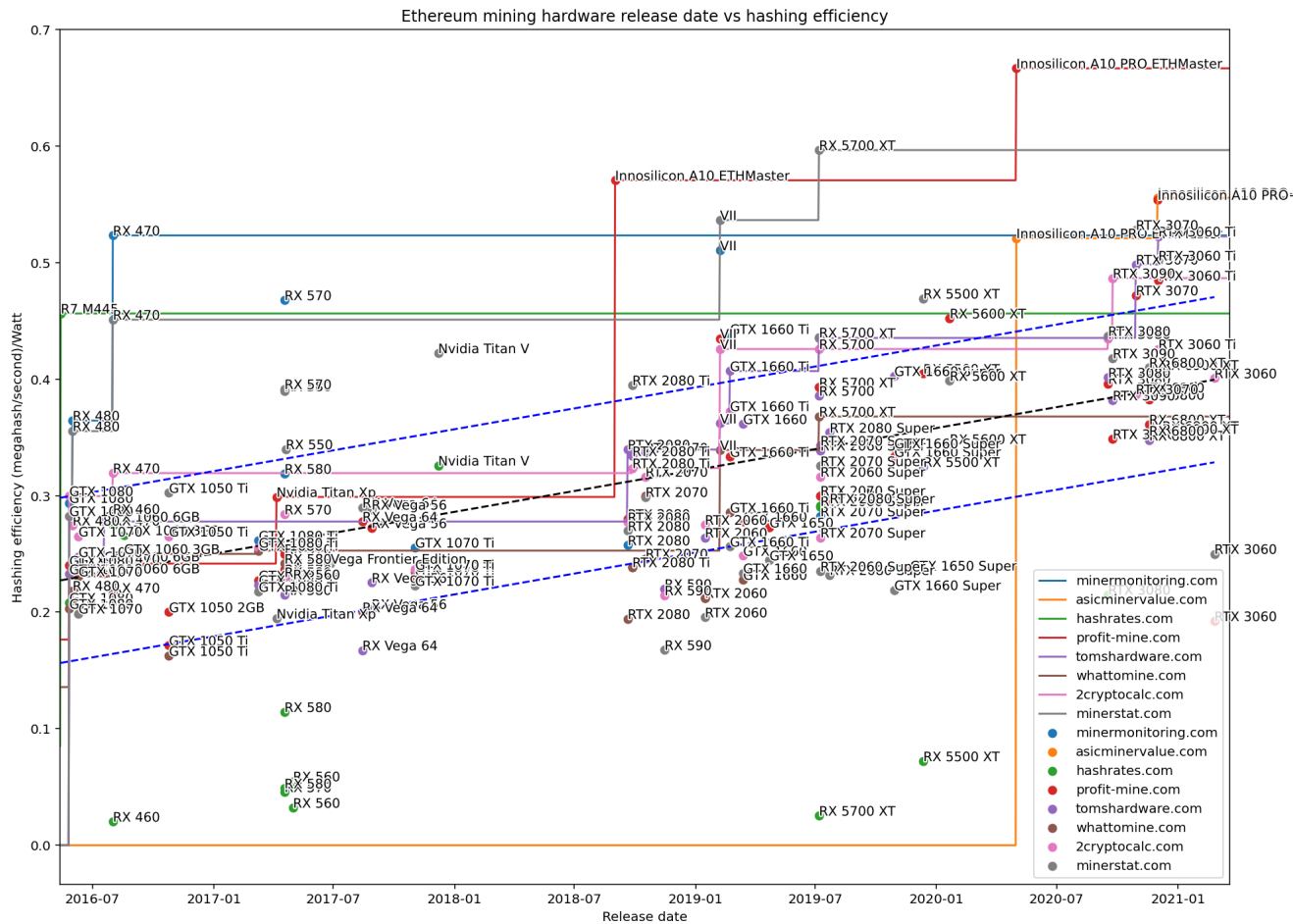
Για τον υπολογισμό της δύναμης (στην υπολογιστική δύναμη αναφερόμαστε) της κάθε GPU μονάδας ελήφθησαν στοιχεία από τον λογαριασμό της Wikipedia που έδειξαν ποια ήταν η μέγιστη δύναμη της. Αυτό έγινε γιατί κατά την διαδικασία της εξόρυξης κατά μέσο όρο έχει υπολογιστεί ότι μόνο το 70 τοις εκατό της δύναμης της GPU χρησιμοποιείται σε σχέση με την πραγματική δύναμη της. Δηλαδή έχουμε απώλεια περίπου 30 τοις εκατό της υπολογιστικής δύναμης της κάρτας γραφικών λόγω της διαδικασίας της εξόρυξης. Ακολουθεί το διάγραμμα (Διάγραμμα 1) που ακριβώς δείχνει αυτή τη διαφορά που υπάρχει κατά μέσο όρο μεταξύ της πραγματικής υπολογιστικής δύναμης και της υπολογιστικής δύναμης που χρησιμοποιείται κατά το hashing.



(Διάγραμμα 1, σχέση μεταξύ πραγματικής και δύναμης της GPU κατά τη διαδικασία του hashing, πηγή : Github.com)

Όσον αφορά το κατά πόσο είναι αποτελεσματική μία μονάδα GPU, έχει παρατηρηθεί ότι τα νεότερα μοντέλα από τις κάρτες γραφικών μπορούν να τρέξουν πολύ πιο γρήγορα τη διαδικασία του hashing και κατ'επέκταση τη διαδικασία της εξόρυξης. Με την δύναμη της κάθε μονάδας να είναι σχετική με το λογισμικό. Βέβαια έχει παρατηρηθεί το φαινόμενο λογισμικά να μπορούν να τρέξουν τον ίδιο ή και περισσότεροι αριθμό hashrate με τα επίπεδα της ενέργειας να είναι τα ίδια. Από την άλλη μεριά αξίζει να αναφέρουμε ότι πολλοί miner προγραμματίζουν με τέτοιο τρόπο τις κάρτες γραφικών τους έτσι ώστε να αυξάνουν τα επίπεδα των hashrate που να είναι σε θέση να υπολογίζουν αλλά να αυξάνουν και τα επίπεδα της ενέργειας που καταναλώνουν.

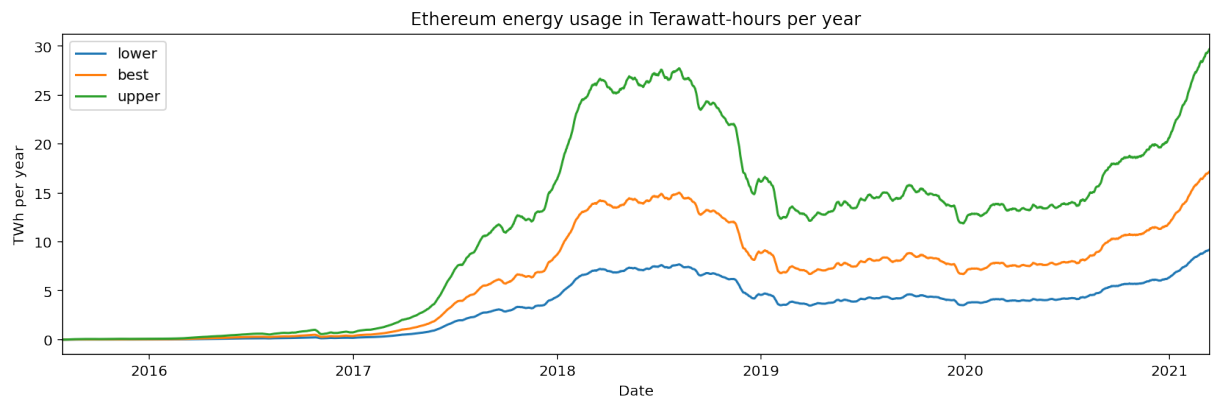
Εδώ η έρευνα που έχει γίνει έχει συλλέξει αρκετές εκτιμήσεις από διάφορες πηγές που παρουσιάζονται συγκεντρωτικά στο παρακάτω διάγραμμα (Διάγραμμα 2). Το διάγραμμα δείχνει και συγκρίνει μέσω μίας benchmark ανάλυσης την ημέρα που μία μηχανή εξόρυξης πρωτοπαρουσιάστηκε στην αγορά σε σχέση με όλες τις υπόλοιπες αλλά και πως έχει βελτιωθεί η αποτελεσματικότητα εξόρυξης αυτών των μηχανών με το πέρασμα του χρόνου.



(Διάγραμμα 2, Η βελτίωση της αποτελεσματικότητας του hashing με την πάροδο του χρόνου. Πηγή : github.com)

Όπως παρατηρούμε και από το διάγραμμα, όσο πηγαίνουμε προς τα δεξιά και οι μηχανές εξόρυξης είναι και πιο σύγχρονες τόσο περισσότερο βελτιώνεται και η αποτελεσματικότητα της διαδικασίας του hashing. Δηλαδή στον ίδιο χρόνο μπορούν να "τρέξουν" πολλά περισσότερα hashrate.

Στο τελευταίο διάγραμμα (Διάγραμμα 3) παρουσιάζονται τρία σενάρια. Τα σενάρια αυτά δεν έχουν την ίδια αυστηρότητα όσον αφορά τα κέρδη. Έτσι έχουμε μία εκτίμηση που δείχνει μία υψηλή κατανάλωση ενέργειας, μίας χαμηλή και μία εκτίμηση που θα ήταν και ηγκαλύτερη με βάση τα στοιχεία και του κώδικα που τρέξαμε. Με βάση λοιπόν του καλύτερου σεναρίου από άποψη κατανάλωσης ενέργειας και κερδοφορίας, η καλύτερη εκτίμηση τοποθετείται στις 15 μαρτίου του 2021 με την κατανάλωση της ενέργειας για το Ethereum να είναι στα 17.2 Terawatt ανά χρόνο.



(Πηγή : Github.com)

5 Συμπεράσματα

Από το 2008 και μετά την εμφάνιση του bitcoin από τον Satoshi Nakamoto, τα κρυπτονομίσματα έχουν αποκτήσει μία τεράστια δυναμική. Η τεχνολογία του blockchain, αλλά και οι αλγόριθμοι κρυπτογράφησης που χρησιμοποιούν (όπως είναι ο SHA-256) εξασφαλίζουν αφενός την ανωνυμία και αφετέρου τον αποκεντρωμένο έλεγχο. Οι ειδικοί σε όλο τον κόσμο από το κομμάτι της πληροφορικής, που ασχολούνται με την βελτίωση των μεθόδων κρυπτογράφησης μέχρι και το τομέα της νομικής, που θέλουν να δούν το πλαίσιο με βάση το οποίο τα κρυπτονομίσματα μπορούν να θεωρηθούν νόμιμο μέσο συναλλαγών, προσφέρουν μία πληθώρα άρθρων που κάποιος μπορεί να ασχοληθεί και να αντλήσει πληροφορίες. Πολλά ερωτήματα εγείρονται σχετικά με τις υψηλές καταναλώσεις ενέργειας που οφείλονται στη διαδικασία εξόρυξης των κρυπτονομισμάτων, γεγονός που έχει θορυβήσει κάποιους επιστήμονες και έχουν προειδοποιήσει ότι μόνο το δίκτυο του Bitcoin καταναλώνει ενέργεια όσο ολόκληρες χώρες και είναι πιθανό να οδηγήσει σε αύξηση της παγκόσμιας θερμοκρασίας κατά δύο βαθμών Κελσίου. Το κομμάτι αυτό των εκπομπών διοξειδίου του άνθρακα που ευθύνεται για την ατμοσφαιρική ρύπανση έχει οδηγήσει τους ερευνητές και τους miner να ψάχνουν φιλικότερες προς το περιβάλλον ενέργειες για την εξόρυξη των κρυπτονομισμάτων, αλλά από την άλλη μεριά επιστήμονες επισημαίνουν ότι η τεχνολογία του blockchain είναι τόσο απαιτητική που μόνο η εξόρυξη των bitcoin απαιτεί γιγαντιαίες ποσότητες ενέργειας. Μελετήθηκαν πάνω από είκοσι τρόποι ερευνητών που ο σκοπός τους ήταν να εκτιμήσουν την κατανάλωση ενέργειας στα πλαίσια των κρυπτονομισμάτων. Η μέθοδος που παρατηρήσαμε τις πιο πολλές φορές βασίζονταν στη μέτρηση των hashrates. Στο τέλος της εργασίας ερευνήσαμε έναν κώδικα στο προγραμματιστικό περιβάλλον της Python που αφορούσε την κατανάλωση ενέργειας στο κρυπτονόμισμα του Ethereum και βρήκαμε ότι με βάση το καλύτερο σενάριο κερδοφορίας και κατανάλωσης, η καλύτερη και πιο συμφέρουσα κατανάλωση ήταν στα 17,2 Terawatt ανά χρόνο στις 15 Μαρτίου του 2021.

Βιβλιογραφία

1. Narayanan, Bonneau, Felten, Miller, Goldfeder (2016), Bitcoin and Cryptocurrency technologies, Princeton University Press, Princeton and Oxford.
2. Hileman, Rauchs (2017), Global Cryptocurrency Benchmarking Study, Cambridge Centre for Alternative Finance.
3. Kent, Bain (2020), Cryptocurrency Mining for Dummies, Library of Congress Control Number, ISBN: 978-1-119-57929-8
4. Ji, Bouri, Roubaud, Kristoufek (2019), Information Interdependence Among Energy, Cryptocurrency and Major Commodity Markets, Elsevier Journal, Energy Economics 81 (2019) 1042-1055.
5. Symitsi, Chalvatzis (2018), Return, volatility and shock spillovers of Bitcoin with energy and technology companies, Elsevier Journal, Economics Letters 170 (2018) 127–130.
6. Bouri, Jalkh, Molnár, Roubaud (2017), Bitcoin for energy commodities before and after the December 2013 crash: diversifier, hedge or safe haven? Applied Economics, 49:50, 5063-5073.
7. Feng, Wang, Zhang (2018), Can cryptocurrencies be a safe haven: a tail risk perspective analysis, Applied Economics, 50:44, 4745-4762.
8. Cong, He, Li (2019), Decentralized Mining in Centralized Pools, NBER Working Paper No. 25592.
9. Naeem, Farid , Balli, Jawad, Shahzad (2021), Hedging the downside risk of commodities through cryptocurrencies, Applied Economics Letters, 28:2, 153-160.
10. Hayes (2015), A Cost of Production Model for Bitcoin, Working Paper 05/2015 Department of Economics The New School for Social Research.

11. Chiu, Koepl (2018), The Economics of Cryptocurrencies Bitcoin and Beyond, SSHRC Insight Grant 435 - 2014-1416.
12. Schilling, Uhlig (2019), Some Simple bitcoin Economics, National Bureau of Economic Research, Working Paper 24483.
13. Budish (2018), The Economic Limits of Bitcoin and the Blockchain, National Bureau of Economic Research, Working Paper 24717.
14. Cason, morris, Habig, Sun (2018), Charge me: A comparison of electrical efficiency in cryptocurrency mining algorithms, Issues in Information Systems Volume 19, Issue 1, pp. 139-149.
15. Delgado-Mohatar, Felis-Rota, Fernández-Herraiz (2019), The Bitcoin mining breakdown: Is mining still profitable? Elsevier Journal, Economics Letters 184 (2019) 108492.
16. Corbet, Lucey, Yarovaya (2021), Bitcoin-energy markets interrelationship, Elsevier Journal, Resources Policy 70 101916.
17. Sobhanifard, Sadatfarizani (2019), Consumer-based modeling and ranking of the consumption factors of cryptocurrencies, Elsevier journal, Physica A 528 121263.
18. Hayes (2017), Cryptocurrency Value formation : An empirical study leading to a cost of production model for valuing bitcoin, Elsevier Journal, Telematics and informatics 34 1308-1321.
19. Vranken (2017), Sustainability of bitcoin and blockchains, Elsevier Journal, Science Direct.
20. Greenberg, Bugden (2019), Energy consumption boomtowns in the United States: Community responses to a cryptocurrency boom, Energy Research and Social Science 50 162-167.

21. Biryukov, Khovratovichy (2017), Equihash: Asymmetric Proof-of-Work Based on the Generalized Birthday Problem, *Ledger Journal*, ISSN 2379-5980.
22. Denisova, Mikhaylov, Lopatin (2019), Blockchain Infrastructure and Growth of Global Power Consumption, *International Journal of Energy Economics and Policy*, 9(4), 22-29..
23. Schinckus, Nguyen, Ling (2019), Crypto-currencies Trading and Energy Consumption, *International Journal of Energy Economics and Policy*, 10(3), 355-364.
24. Bondarev (2020), Energy Consumption of Bitcoin Mining, *International Journal of Energy Economics and Policy*, 10(4), 525-529.
25. Rana, Giungato, Tarabella, Tricase (2019), Blockchain sustainability and blockchain issues, *Amfiteatru Economic*, 21(Special Issue No. 13), pp. 861-870.
26. Vries (2018), Bitcoin's Growing Energy Problem, <https://www.researchgate.net/publication/32>
27. Küfeoğlu, Özkuran (2019), Energy consumption of bitcoin mining, *Cambridge Working Papers in Economics*: 1948.
28. Li, Li, Peng, Cui, Wu (2019), Energy consumption of cryptocurrency mining : A study of electricity consumption in cryptocurrency mining, *Elsevier Journal, Energy* 168 160-168.
29. Polemis, Tsionas (2020), The environmental consequences of blockchain technology: A Bayesian quantile cointegration analysis for Bitcoin, *Wiley Int J Fin Econ.* 2021;1–20.
30. Ma, Gans, Tourky (2018), Market structure in bitcoin mining, *National Bureau of economic research, Working Paper* 24242.

31. Gallersdorfer, klaaben, Stoll (2020), Energy consumption of cryptocurrencies beyond bitcoin, Elsevier journal Joule 4, 1839–1851.
32. Sedlmeir, Buhl, Fridgen, Keller (2020), The Energy Consumption of Blockchain Technology: Beyond Myth, Bus Inf Syst Eng 62(6):599–608.
33. Chohan (2021), The Double Spending Problem and Cryptocurrencies, SSRN, Critical blockchain research initiative (2021).
34. Stachowski, Fiebig, Rauber (2020), Autotuning based on frequency scaling toward energy efficiency of blockchain algorithms on graphics processing units, The Journal of Supercomputing 77:263–291.
35. Fadeyi, Krejcar, Maresova, Kuca, Brida, Selamat (2019), Opinions on Sustainability of Smart Cities in the Context of Energy Challenges Posed by Cryptocurrency Mining, Sustainability 2020, 12, 169; doi:10.3390/su12010169.
36. Tahir, Huzaifa, Das, Ahmad, Gunter, Zaffar, Caesar, Borisov (2017), Mining on Someone Else’s Dime: Mitigating Covert Mining Operations in Clouds and Enterprises, Springer International Publishing RAID 2017, LNCS 10453, pp. 287–310.
37. Pinto, Castor, Liu (2014), Mining Questions about Software Energy Consumption, MSR’14, May 31 – June 1, 2014.
38. Nakamoto (2008), Bitcoin: A Peer-to-Peer Electronic Cash System, www.bitcoin.org.
39. Das, Dutta (2020), Bitcoin’s energy consumption: Is it the Achilles heel to miner’s revenue? Elsevier Journal, Economics Letters 186 (2020) 108530.
40. Yi, Cho, Sohn, Ahn (2020), After the Splits: Information Flow between Bitcoin and Bitcoin Family, Elsevier Journal, Chaos, Solitons and Fractals 142 (2021) 110464.

41. Corbetta, Lucey, Yarovaya (2018), Datestamping the Bitcoin and Ethereum bubbles, Elsevier Journal, Finance Research Letters 26 (2018) 81-88.
42. STEGĂROIU (2018), The advantages and disadvantages of bitcoin payments in the new economy, Economy Series, Issue 1/2018, ISSN 2248-0889, ISSN-L 2248-0889.
43. Bunjaku, Gjorgieva-Trajkovska, Miteva-Kacarski (2020), Cryptocurrencies - Advantages and Disadvantages, ISSN 1857-9973 336.743:004.031.4.
44. Javarone, Wright (2018), From Bitcoin to Bitcoin Cash: a network analysis, ACM ISBN 978-1-4503-5838-5/18/06.
45. Barysevich, Solad (2018), Litecoin Emerges as the Next Dominant Dark Web Currency, Recorded Future, CTA-2018-0208.
46. Meshcheryakov, Ivanov (2020), Ethereum as a Hedge: The intraday analysis, Economics Bulletin, Volume 40, Issue 1, pages 101-108.
47. Mărgulescu, Moagăr-Poladian (2017), Global Economic Reserver, No. 2, vol. 5/2017, ISSN 2343 - 9742 ISSN-L 2343 - 9742.
48. Sabalionis, Wang, Park (2020), What affects the price movements in Bitcoin and Ethereum? Library of Wiley, The Manchester School. 2021;89:102–127.
49. Bhosale, Mavale (2018), Volatility of select Crypto-currencies: A comparison of Bitcoin, Ethereum and Litecoin, Pune Annual Research Journal of Symbiosis Centre for Management Studies, Pune Vol. 6, March 2018.
50. Wood (2017), Ethereum : A secure decentralised generalised transaction ledger, EIP-150 REVISION (a04ea02 - 2017-09-30).

51. Chohan (2021), A History of Dogecoin, Critical Blockchain Research Initiative, SSRN-id3091219.
52. Young (2018), Dogecoin Survey, SSRN-SSRN-id3306060.
53. Miller, Moser, Lee, Narayanan (2017), An Empirical Analysis of Linkability in the Monero Blockchain, Princeton Univeristy 2017.
54. Ramos, Zanko (2019), A Review of Zcash as a Cryptocurrency Platform Aimed Towards Maintaining Privacy Between All Parties, University of Colombia.
55. Noether (2015), Ring Confidential Transactions, Monero Research Labs.