ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

«ΜΕΛΕΤΗ , ΕΡΕΥΝΑ ΚΑΙ ΑΝΑΛΥΣΗ ΔΙΑΔΥΚΤΙΑΚΩΝ ΝΟΜΙΣΜΑΤΩΝ ΚΑΙ ΤΩΝ ΙΔΙΟΤΗΤΩΝ ΤΟΥΣ»

Επιβλέπων καθηγητής: Ιωάννης Τζήμας

Επιμέλεια: Καλλιακούδας Πέτρος αμ:1920

Πάτρα – Φεβρουάριος 2020

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή

Πάτρα, Ημερομηνία

ΕΠΙΤΡΟΠΗ ΑΞΙΟΛΟΓΗΣΗΣ

1. Ονοματεπώνυμο, Υπογραφή
2. Ονοματεπώνυμο, Υπογραφή
3. Ονοματεπώνυμο, Υπογραφή

Αφιέρωση

Ευχαριστίες

Περιεχόμενα

Contents

Λίστα Σχημάτων

Πρόλογος

…….

Περίληψη

Τα κρυπτονομισματα έχουν γίνει ένα κομμάτι της καθημερινότητας μας και γενικότερα στην κοινωνία μας. Έχουν εξελιχθεί με γοργούς ρυθμούς από την απαρχή τους το 2008-09 και μαζί με αυτά η τεχνολογία που χρησιμοποιείται ώστε να εξορυχθούν. Σε αυτήν λοιπόν την εργασία θα δούμε τι είναι , πως παράγονται , ποιες είναι οι μέθοδοι εξόρυξης , ποια υλικά χρησιμοποιούνται για αυτή (hardware) και πως μα την βοήθεια των ανανεώσιμων πηγών ενέργειας μπορούμε να μειώσουμε το κόστος και να αυξήσουμε το κέρδος.

Λέξεις κλειδιά: κρυπτονομίσματα , υλικό , εξόρυξη

Abstract

Cryptocurrencies have become a part of our daily lives and our society in general. They have evolved rapidly since their inception in 2008-09 and with them the technology used to extract them. So, in this thesis we will see what cryptocurrency is, how it is produced, what are the mining methods, what materials are used for it (hardware) and how with the help of renewable energy sources we can reduce costs and increase profit.

Keywords: cryptocurrencies , hardware , mining

Κεφάλαιο 1. Γενική αναφορά στο τι είναι τα κρυπτονομισματα.

1.1.Γενικά για τα κρυπτονομίσματα

Τα κρυπτονομίσματα δημιουργήθηκαν στο ξύπνημα της κρίσης του 2008-2009 από έναν προγραμματιστή η μια ομάδα προγραμματιστών με την ονομασία Satoshi Nakamoto. Συγκεκριμένα, ο Nakamoto (2008) δημιούργησε το κρυπτονόμισμα Bitcoin. Συγκεκριμένο, το Bitcoin ήταν το πρώτο κρυπτονόμισμα το οποίο δημιουργήθηκε και μάλιστα τα στοιχεία του σχηματίστηκαν μέσα από το άρθρο που έγραψε για αυτό το θέμα με όνομα «*Bitcoin: ένα ομότιμο σύστημα ηλεκτρονικού χρήματος*».

Τα κρυπτονομίσματα είναι ένα είδος ψηφιακού νομίσματος που προορίζεται να λειτουργήσει ως μέσο ανταλλαγής. Δηλαδή μιλάμε για εικονικά νομίσματα. Με πιο τεχνικό τρόπο, θα το λέγαμε μια αλυσίδα ψηφιακών υπογραφών. Ο τρόπος που λειτουργεί όλο αυτό ως νόμισμα είναι πολύ ενδιαφέρων: ουσιαστικά, έχουμε την ψηφιακή υπογραφή της προηγούμενης συναλλαγής αφού αυτή «περάσει» μέσα από μια συνάρτηση κατακερματισμού πρώτα, καθώς επίσης και την υπογραφή με το δημόσιο κλειδί του επόμενου κατόχου. Αυτή η διαδικασία γίνεται να επαληθευτεί από τον κάτοχο και μάλιστα να ανακτήσει όλη την αλυσίδα από τους διάφορους κατόχους.

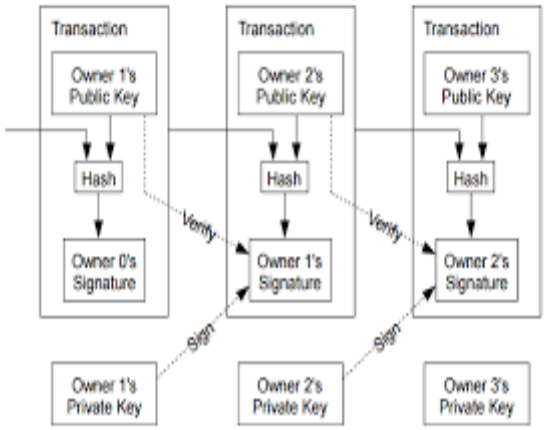


Figure 1. Το ηλεκτρονικό νόμισμα ως μια αλυσίδα από ψηφιακές υπογραφές

Όπως άρα εξηγείται και παραπάνω, αυτά όλα υφίστανται μόνο στους υπολογιστές με αυτή την ηλεκτρονική μορφή, καθώς δεν αποτελούν απτά χαρτονομίσματα ή νομίσματα εντός του συστήματος.
Κάποια βασικά στοιχεία που μπορούμ ενα πούμε πως χαρακτηρίζουν όλα τα κρυπτονομίσματα είναι τα επόμενα:

- Δίνουν τη δυνατότητα συναλλαγών 24/7, χωρίς να εξαρτώνται από κάτι άλλο εκτός από τη λειτουργία των υπολογιστών και του διαδικτύου
- Δεν υπάρχει κεντρική αρχή που εκδίδει τα νομίσματα ή ρυθμίζει την αξία τους ή κάτι σχετικό
- Οι κανόνες που ισχύουν για τις συναλλαγές με τα κρυπτονομίσματα είναι ενιαίοι για όλους όσους συμμετέχουν στις συναλλαγές, χωρίς εξαιρέσεις ή «προνομιούχους»
- Για να γίνει κανείς κάτοχος κρυπτονομισμάτων, δεν υπάρχει άλλη προϋπόθεση (γεωγραφική ή άλλη) εκτός από την πρόσβαση σε δίκτυο και κατοχή υπολογιστή

Επομένως είναι μορφή νομίσματος όπου υπάρχει μόνο ψηφιακά και συνήθως δεν έχει κεντρική αρχή έκδοσης ή ρυθμιστική αρχή, αλλά αντ' αυτού χρησιμοποιεί ένα αποκεντρωμένο σύστημα για την καταγραφή συναλλαγών και τη διαχείριση της έκδοσης νέων μονάδων και βασίζεται στην κρυπτογραφία για την αποτροπή της παραποίησης και της απάτης . Αυτή τη στιγμή υπάρχουν 5,392 διαφορετικά κρυπτονομίσματα. Μερικά από τα πιο γνωστά, που ακούμε πιο συχνά, είναι το bitcoin, το ethereum, το ripple, το litecoin και πολλά άλλα.

Τα κρυπτονομίσματα είναι ένα είδος περιουσιακού στοιχείου ψηφιακού χαρακτήρα.

Figure 2. Μητρώο κρυπτονομισμάτων (cryptocurrency ledger)

Ένα σημαντικό στοιχείο το οποίο διαθέτουν τα κρυπτονομίσματα είναι το δημόσιο βιβλίο καταγραφών (public ledger). Το συγκεκριμένο ηλεκτρονικό βιβλίο είναι μια τεχνολογία που χρησιμοποιείται από τα κρυπτονομίσματα, τα οποία γενικότερα έχουν τα εξής στοιχεία:

Α) Είναι ένας νέος τρόπος συναλλαγών με ηλεκτρονικά νομίσματα

Β) Οι συναλλαγές με κρυπτονομίσματα ούτε έχουν προϋποθέσεις από αυτούς που συναλλάσσονται (για παράδειγμα, χρεωστική ή πιστωτική κάρτα), κάτι που ωφελεί όλο το σύνολο των ανθρώπων ανά τον κόσμο που δε χρησιμοποιούν χρεωστικές-πιστωτικές κάρτες ούτε και έχουν κάποια αρχή που ρυθμίζει τις συναλλαγές (όπως για παράδειγμα, τράπεζα)[1]

Γ) Χρησιμοποιούν τεχνολογία blockchain

Δ) Συγκεκριμένα, τηρούν μητρώα με καταγραφές (τύπου ledger), όπου χρησιμοποιείται blockchain

Ε) Οι συναλλαγές μέσω κρυπτονομισμάτων γίνονται με μεγάλο βαθμό ασφάλειας

Ζ) Οι συναλλαγές με κρυπτονομίσματα είναι αποκεντρωμένες

Η) Στις συναλλαγές με κρυπτονομίσματα συμμετέχουν υπολογιστές από όλο τον κόσμο που ονομάζονται κόμβοι (nodes)

[1] Ο αριθμός των ανθρώπων, σύμφωνα με άρθρο του Liann McCarthy στο Forbes (2018), που δεν έχουν τραπεζικό λογαριασμό ήταν 1,7 εκατομμύρια το 2018

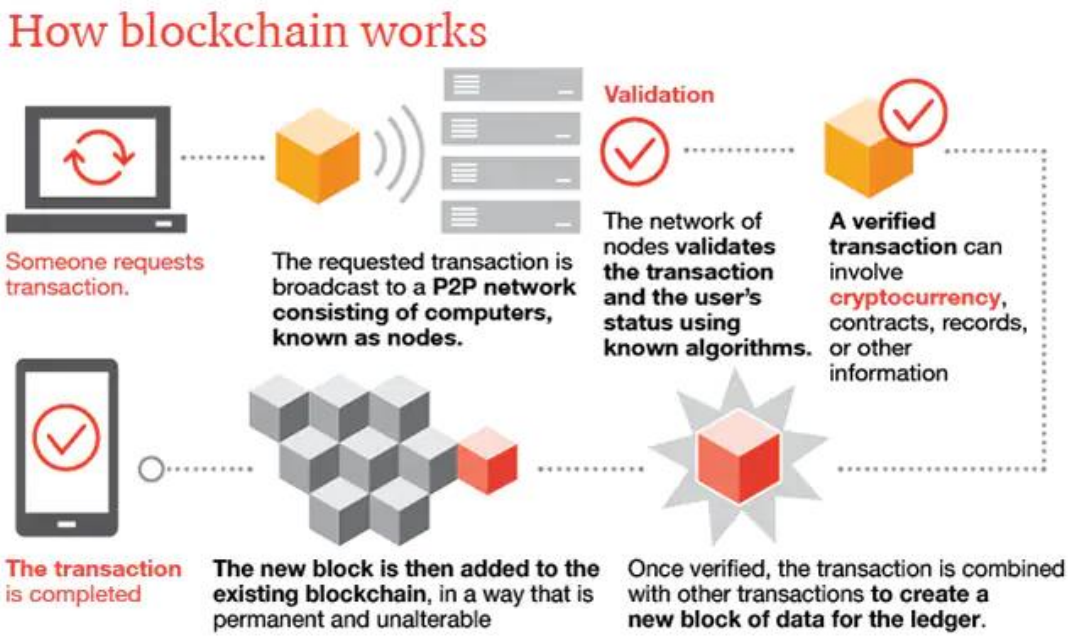


Figure 3. Τρόπος που λειτουργεί το Blockchain

Ένα άλλο στοιχείο σημαντικό, όπως αναφέρουμε παραπάνω, των κρυπτονομισμάτων είναι το blockchain. Το blockchain περιέχεται σε μια σειρά από κρυπτονομίσματα. Το blockchain είναι ουσιαστικά ένα μητρώο από πληφορορίες και δεδομένα. Μάλιστα, το blockchain περιλαμβάνει τα στοιχεία από όλες τις συναλλαγές που έχουν γίνει ως εξής:

- Ένας κόμβος ενός χρήστη κάνει αίτημα για μια νέα συναλλαγή
- Το αίτημα μεταδίδεται (εκπέμπεται) στο ομότιμο δίκτυο του κρυπτονομίσματος, σε όλους τους κόμβους
- Το δίκτυο των κόμβων επαληθεύει την κατάσταση του χρήστη που έκανε το αίτημα και τελικά, μέσα από συγκεκριμένους αλγόριθμους, την ίδια τη συναλλαγή
- Η νέα συναλλαγή προστίθεται αφού εγκριθεί στην αλυσίδα του blockchain και παραμένει εκεί και για τη συνέχεια χωρίς να μπορεί να υποστεί καμία αλλοίωση
- Η νέα συναλλαγή προστίθεται και ως νέα δεδομένα μέσα στο μητρώο-κατάλογο του ledger

Έτσι, με άλλα λόγια το blockchain προσφέρει τη δυνατότητα δημιουργίας νέων εγγραφών μέσα στο σύστημα του κρυπτονομίσματος. Αυτές οι εγγραφές επίσης, όπως περιγράφεται χαρακτηριστικά στο άρθρο με τίτλο *«Τεχνολογία BlockChain:*

Τεχνολογία πέρα από το Bitcoin» (2015), προσφέρουν βεβαιότητα για το περιεχόμενό τους, δηλαδή τα δεδομένα τους είναι ακέραια αλλά παράλληλα όλες αυτές οι εγγραφές που αναφέρονται σε συναλλαγές μπορούν να επαληθευτούν.
Έτσι, το blockchain λειτουργεί ουσιαστικά με ένα τρόπο εντελώς αποκεντρωμένο και επίσης κατανεμημένο, αφού αντί για μια κεντρική αρχή, η έγκριση δίνεται με ένα τρόπο που μπορούμε να ονομάσουμε δημοκρατικό από όλους τους κόμβους του δικτύου. Επίσης, όλο αυτό το σύστημα λειτουργεί με αυτό που λέμε επεκτασιμότητα (scalability), αφού είναι δεκτικό στο να προστίθενται συνεχώς καινούργια δεδομένα και νέες συναλλαγές στο μητρώο, εμπλουτίζοντάς το με τις νέες πληροφορίες. Με αυτό τον τρόπο, όντως φαίνεται ότι πραγματοποιείται η επανάσταση στις συναλλαγές για τις οποίες είχε μιλήσει ο Nakamoto το 2008. Αν μιλήσουμε με όρους Υπολογιστικής, το blockchain έχει θεωρήθηκε ως ένα πέμπτο μεγάλο άλμα στην Υπολογιστική, ειδικά αφού φαίνεται πως προσφέρει ασφάλεια και άρα και εμπιστοσύνη στα ψηφιακά δεδομένα και όλες τις σχετικές συναλλαγές που γίνονται με αυτά.

Μιλώντας τώρα σχετικά με τη δομή τους, η Tiana Laurence (2017) βλέπει ότι υπάρχουν τρία βασικά στοιχεία που πρέπει να τονίσουμε, για να καταλάβουμε πώς τα ορίζουμε με πιο ολοκληρωμένο τρόπο:
α)Blocks
Τα **blocks** είναι ένα σύνολο συναλλαγών τα οποία καταγράφονται ένα-ένα πάνω στο μητρώο τύπου ledger σταδιακά, όπως περιγράψαμε πριν από λίγο. Τα blocks περιέχουν το καθένα ένα σύνολο από στοιχεία όπως:

- Χρονοσφραγίδα
- Αποτέλεσμα κατακερματισμού προηγούμενης συναλλαγής
- Δεδομένα συναλλαγής

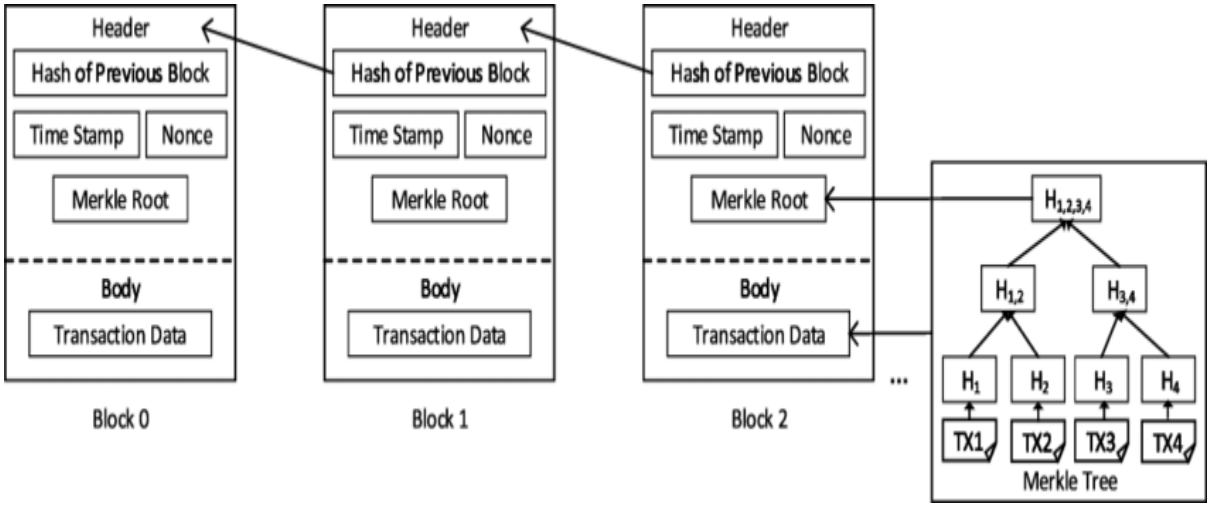


Figure 4. Μονάδες blocks του Blockchain

β) Αλυσίδα

Η **αλυσίδα** είναι το δεύτερο βασικό στοιχείο που περιέχει το blockchain. Στον ορισμό της αλυσίδας δίνουμε έμφαση στη συνάρτηση κατακερματισμού, η οποία τελικά λειτουργεί ως συνδετικός κρίκος μεταξύ των διαφόρων blocks της. Το αποτέλεσμα της συνάρτησης κατακερματισμού, που είναι μια μονόδρομη συνάρτηση, το εισάγει το blockchain σε κάθε επόμενο block. Με αυτό τον τρόπο, δημιουργείται μια σειρά και μια τάξη μέσα στα διάφορα blocks: 0,1,2 κ.ο.κ., ανάλογα με το χρόνο που είχαν αρχικά δημιουργηθεί. Η συνάρτηση κατακερματισμού (hashing) παίζει μεγάλο ρόλο εδώ, αφού, όπως είπαμε, είναι μονόδρομη και έτσι δε μπορεί να αποκρυπτογραφηθεί, με αποτέλεσμα να συμβάλει στην ασφάλεια και στη μοναδικότητα του κάθε block, πέρα από τη σύνδεση του ενός με το επόμενό του με ένα τρόπο που δε μπορεί κανείς να την απομιμηθεί. Τέτοιες συναρτήσεις υπάρχουν εδώ και δεκαετίες, και σήμερα αυτές που χρησιμοποιούνται είναι η SHA-256 και άλλες, πιο προχωρημένες.

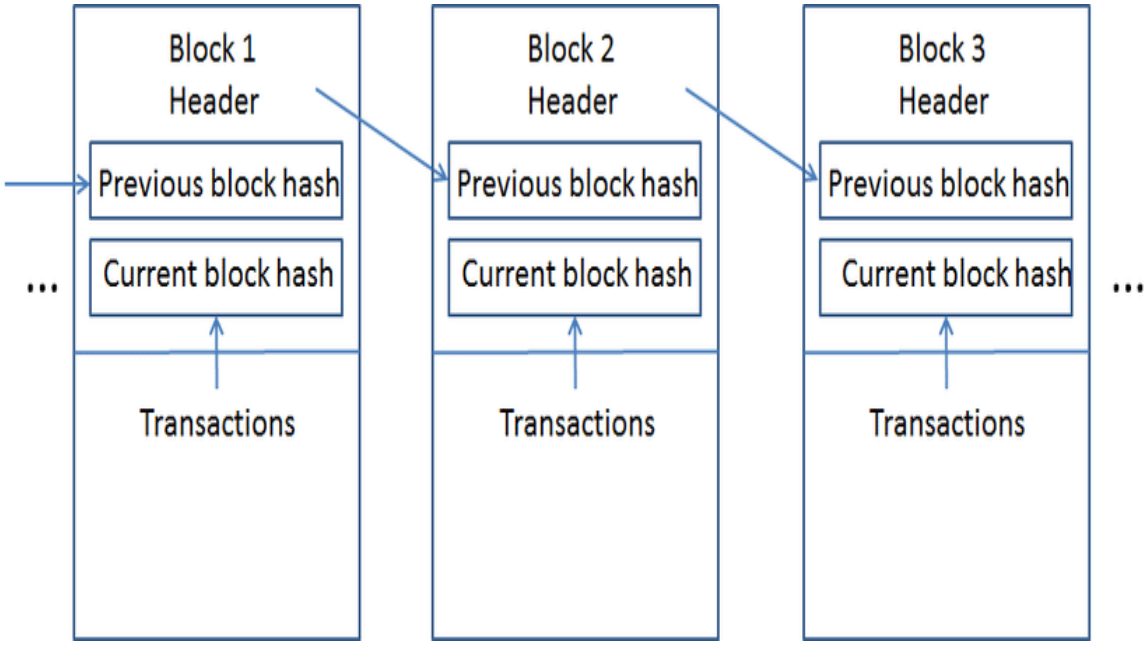


Figure 5. Αλυσίδα στο blockchain

Γ) Δίκτυο

Ένα **δίκτυο** αποτελείται από κόμβους που βρίσκονται σε διάφορες χώρες μέσα στον κόσμο. Οι κόμβοι έχουν τις καταγραφές όλων των συναλλαγών που υπάρχουν σε ένα δίκτυο blockchain. Υπάρχουν διάφορα είδη κόμβων μέσα σε ένα δίκτυο Blockchain, τα οποία είναι τα εξής:

Α) Πλήρεις κόμβοι (full nodes)

Β) Ελαφριοί κόμβοι (lightweight nodes)

Γ) Κόμβοι εξόρυξης (miners)

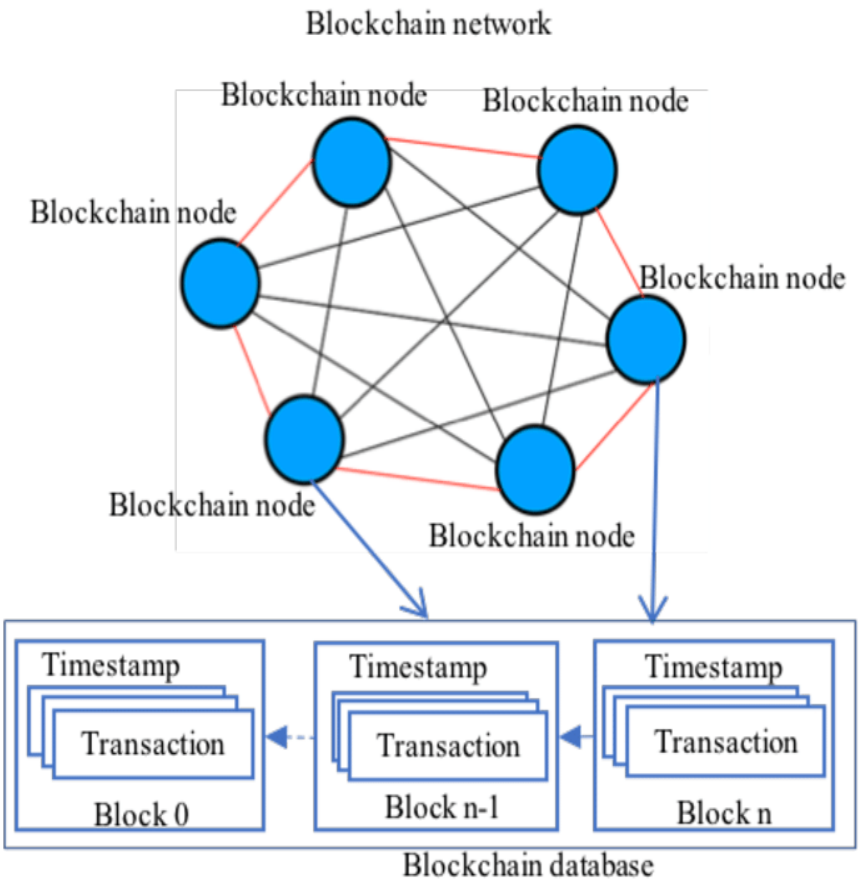


Figure 6. Δίκτυο στο Blockchain

Το δίκτυο Blockchain περιλαμβάνει σειρά από κόμβους, όπως είδαμε παραπάνω. Όμως, οι δύο σημαντικότερες κατηγορίες από κόμβους που έχει είναι οι εξής:

- Πλήρεις κόμβοι (full nodes)
  Είναι οι κόμβοι που έχουν το πλήρες σύνολο των συναλλαγών για όλο το δίκτυο Blockchain.
- Κόμβοι εξόρυξης
  Οι κόμβοι εξόρυξης είναι κόμβοι διαφορετικοί, που προσπαθούν να προσθέσουν τα επόμενα blocks στο δίκτυο Blockchain.[2] Οι κόμβοι αυτοί λύνουν κάποιο μαθηματικό πρόβλημα και, αν καταφέρουν να το λύσουν, τότε δημιουργούν ένα νέο ηλεκτρονικό νόμισμα.

[2] Τις έννοιες αυτές εξηγεί ως βασικές για το δίκτυο Blockchain ο iBen Esengulov (2020) στο βιβλίο του με τίτλο «*Bitcoin: explained in simple terms*» (2020)

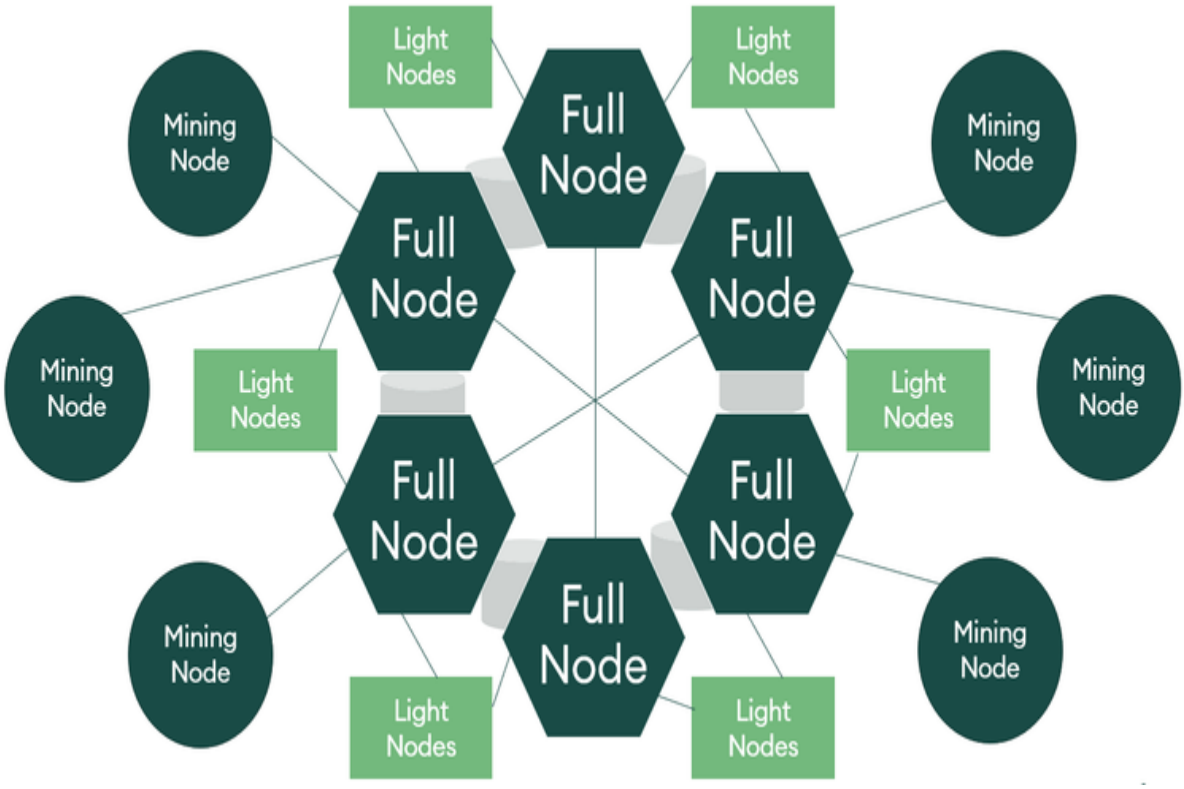


Figure 7. Δίκτυο Blockchain με διάφορα είδη κόμβων

Όπως είπαμε, το κύριο είδος κόμβου που υπάρχει σε ένα δίκτυο Blockchain είναι ο πλήρης κόμβος. Εκτός όμως από τον πλήρη κόμβο υπάρχουν και άλλα, λιγότερο σημαντικά είδη κόμβων, που φαίνονται στην εικόνα 6. Τέτοια είδη είναι ο light ή lightweight node (ελαφρύς κόμβος) και ο master node (διαχειριστής). Για παράδειγμα, ο ελαφρύς κόμβος σημαίνει ότι δεν έχει όλη την πλήρη δυνατότητα που έχει ο πλήρης κόμβος, Δηλαδή, αντί για όλη την πληροφορία που έχουν οι κόμβοι από την αλυσίδα blockchain, έχοντας έναν ελαφρύ κόμβο κατεβάζεις μόνο τις κεφαλίδες που έχουν αυτοί οι κόμβοι. Πάντως, έχοντας έναν ελαφρύ κόμβο δεν αλλάζει τίποτα όσον αφορά το ότι μπορείς να κάνεις την επαλήθευση όλων των συναλλαγών του Blockchain. Γενικά, πάντως, οι πλήρεις κόμβοι έχουν το μειονέκτημα ότι χρειάζονται πολύ μεγαλύτερη προσπάθεια για την εκτέλεσή τους αλλά και με τη συντήρηση που χρειάζονται.

Figure 8. Πορτοφόλι κρυπτονομισμάτων: λειτουργία (δημόσιο και ιδιωτικό κλειδί)

Ένα πολύ βασικό στοιχείο που έχουν τα κρυπτονομίσματα για να γίνονται οι συναλλαγές είναι τα πορτοφόλια κρυπτονομισμάτων όλων των κρυπτονομισμάτων είναι το λεγόμενο πορτοφόλι (cryptocurrency wallet). Ένα πορτοφόλι είναι μια εφαρμογή που υπάρχει σε πολλά είδη και παίζει τον ίδιο ρόλο για τα κρυπτονομίσματα με το ρόλο που παίζει ένα χρηματοκιβώτιο για μία τράπεζα[3].
Ένα πορτοφόλι κρυπτονομίσματος χρειάζεται για τη διεξαγωγή συναλλαγής με ηλεκτρονικά νομίσματα. Για να το δημιουργήσει κάποιος, εξαρτάται από το είδος του αν χρειάζεται απλώς εγκατάστσαη ή και περισσότερα βήματα. Αν κάποιος χρήστης θέλει να έχει ένα λογαριασμό με κηδεμονία, όπου έχει ένα άλλο οργανισμό (τρίτο μέρος) να φυλάει το ιδιωτικό του κλειδί για τον ίδιο (custodial crypto wallet), τότε χρειάζονται τρία βήματα:
α)Να δημιουργήσει ένα λογαριασμό κρυπτονομίσματος
β)Να γράψεις το ιδιωτικό σου κλειδί (χρειάζεται για την κρυπτογράφηση δημόσιου κλειδιού)
γ)Στη συνέχεια, να χρησιμοποιήσεις μια δημόσια διεύθυνση που θα σου δοθεί: αυτή είναι αναγκαία για να παραλάβεις κρυπτονομίσματα[4]
Η διαφορά στο χωρίς κηδεμονία πορτοφόλι είναι ότι πρέπει κάποιος να γράψει το ιδιωτικό του κλειδί σε ένα ασφαλές μέρος.

[3] Hardle, Harvey and Reule: Understanding cryptocurrencies (2019)

[4] https://coinspaid.com/what-is-a-crypto-wallet

Figure 9. Είδη από πορτοφόλια κρυπτονομισμάτων

Μπορούμε να πούμε ότι ένα ψηφιακό πορτοφόλι για κρυπτονομίσματα έχει κάποιες κύριες λειτουργίες:

i) Να αποθηκεύει δημόσια και ιδιωτικά κλειδιά και να τα χρησιμοποιεί σε συνεργασία με διάφορες αλυσίδες blocks που έχουν τα blockchains

ii) Σε συνεργασία με τα κλειδιά αυτά, να στέλνει όπως και να παραλαμβάνει κρυπτονομίσματα

iii) Να μπορεί να έχει πρόσβαση στα κρυπτονομίσματά του

Τελικά, υπάρχουν διάφορα βασικά είδη πορτοφολιών κρυπτονομισμάτων, που είναι τα εξής[5]:

Α)Πορτοφόλι χωρίς κηδεμονία (non-custodial wallet):

Το χωρίς κηδεμονία πορτοφόλι είναι μια εφαρμογή που αφήνει στο χρήστη το ελεύθερο να κάνει ό,τι θέλει με τα ηλεκτρονικά του νομίσματα, χωρίς να του βάζει κανένα περιορισμό. Γενικά θεωρείται το πορτοφόλι που προτιμούν οι χρήστες περισσότερο

Β)Πορτοφόλι με κηδεμονία (custodial wallet)

Το πορτοφόλι με κηδεμονία δίνει στο χρήστη έλεγχο στα νομίσματά του αλλά του βάζει και κάποιους περιορισμούς όσον αφορά στο να τα δαπανήσει εξολοκλήρου. Το πορτοφόλι αυτό οπότε περιέχει κάποιο έλεγχο προς το χρήστη σε περίπτωση που αυτός το θέλει, αλλά μπορεί να έχει και κάποια ζητήματα ασφάλειας, αφού δεν

[5] Την κατηγοριοποίηση αυτή κάνει ο iBek Esengulov (2020)

αποκλείεται η παραβίασή του και η απώλεια των ηλεκτρονικών νομισμάτων ενός χρήστη του.

Γ)Υβριδικό πορτοφόλι (hybrid wallet)

Το υβριδικό πορτοφόλι έχει δύο είδη ελέγχου:

από το χρήστη του πορτοφολιού και την ίδια την εφαρμογή του πορτοφολιού. Έτσι, κάποιος έλεγχος ασκείται και στο χρήστη του πορτοφολιού αλλά και ο χρήστης έχει έλεγχο αν μιλάμε για μη-εξουσιοδοτημένες πράξεις που μπορεί να προέρχονται από κακόβουλα τρίτα άτομα.

1.2 Ασφάλεια στα κρυπτονομισματα

Τα κρυπτονομίσματα χρησιμοποιούν κρυπτογραφία για τρεις βασικούς σκοπούς. για την εξασφάλιση συναλλαγών, τον έλεγχο της δημιουργίας πρόσθετων μονάδων και την επαλήθευση της μεταφοράς περιουσιακών στοιχείων. Για να επιτευχθούν όλα αυτά, τα κρυπτονομίσματα βασίζονται σε αυτό που ονομάζεται "κρυπτογράφηση δημόσιου κλειδιού.

Γενικά, κάποιος μπορεί να πει ότι η κρυπτογραφία είναι από τα πιο σημαντικά τμήματα των κρυπτονομισμάτων αφού ουσιαστικά είναι ο συνδυασμός κρυπτογραφίας και πληρωμών που δημιουργεί τα κρυπτονομίσματα.

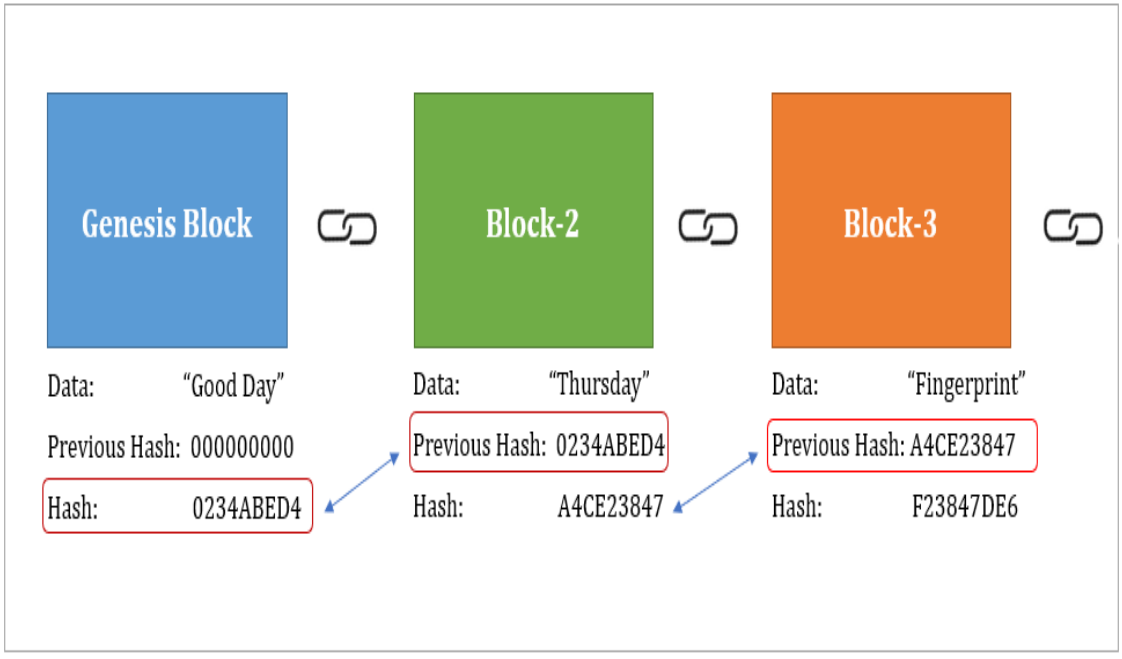


Figure 10. Οι αλυσίδες των blocks στο blockchain χρησιμοποιούν συναρτήσεις κατακερματισμού

Μπορούμε να πούμε ότι η Κρυπτογραφία ως σύνολο, με την έννοια μιας τέχνης που μας προσφέρει ασφάλεια στις επικοινωνίες, συνδυάζεται με τα κρυπτονομίσματα με κάποιους τρόπους:

Α) Η κρυπτογραφία είναι βασικά αυτή που επιτρέπει τις συναλλαγές μέσα από τα κρυπτονομίσματα

Β) Η κρυπτογραφία κάνει δυνατές τις συναλλαγές ειδικά μέσα στο χώρο του Διαδικτύου

Γ) Η κρυπτογραφία είναι πολύ σημαντική για την ίδια τη δημιουργία του κρυπτονομίσματος

Δ) Μέσω της κρυπτογραφίας, δημιουργούνται τα δίκτυα, δηλαδή οι αλυσίδες των blocks, αφού, όπως είπαμε, το κάθε block περιέχει το αποτέλεσμα της συνάρτησης κατακερματισμού από το προηγούμενο block

Ε) Τελικά, η κρυπτογραφία δίνει τη δυνατότητα να γίνονται οι συναλλαγές με ηλεκτρονικά νομίσματα χωρίς την ανάγκη καμιάς κεντρικής ρυθμιστικής αρχής

Αν μιλήσουμε τώρα πιο συγκεκριμένα, το Bitcoin Network χρησιμοποιεί ένα αλγόριθμο συνάρτησης κατακερματισμού που αναφέραμε νωρίτερα, δηλαδή τον SHA- 256 (Secure Hash Algorithm) όπου μια σημαντική του ιδιότητα είναι το ότι εάν αλλάξει ένα κομμάτι εισόδου η έξοδος τού αλλάζει σημαντικά! Επομένως και η παραμικρή αλλαγή μπορεί να εντοπιστεί ακόμη και σε μεγάλα αρχεία κειμένου. Μια ακόμη σημαντική ιδιότητα του SHA-256 είναι ότι πάντα απεικονίζει μεγάλα κείμενα σε μικρές ακολουθίες χαρακτήρων και με ένα τρόπο που δε μπορεί κανείς έχοντάς τα να αποκρυπτογραφήσει το αρχικό κείμενο, οπότε είναι εντελώς κατάλληλος για μια τέτοια περίπτωση. Τον αλγόριθμο αυτό και τη λειτουργία του βλέπουμε στην εικόνα 11.

/

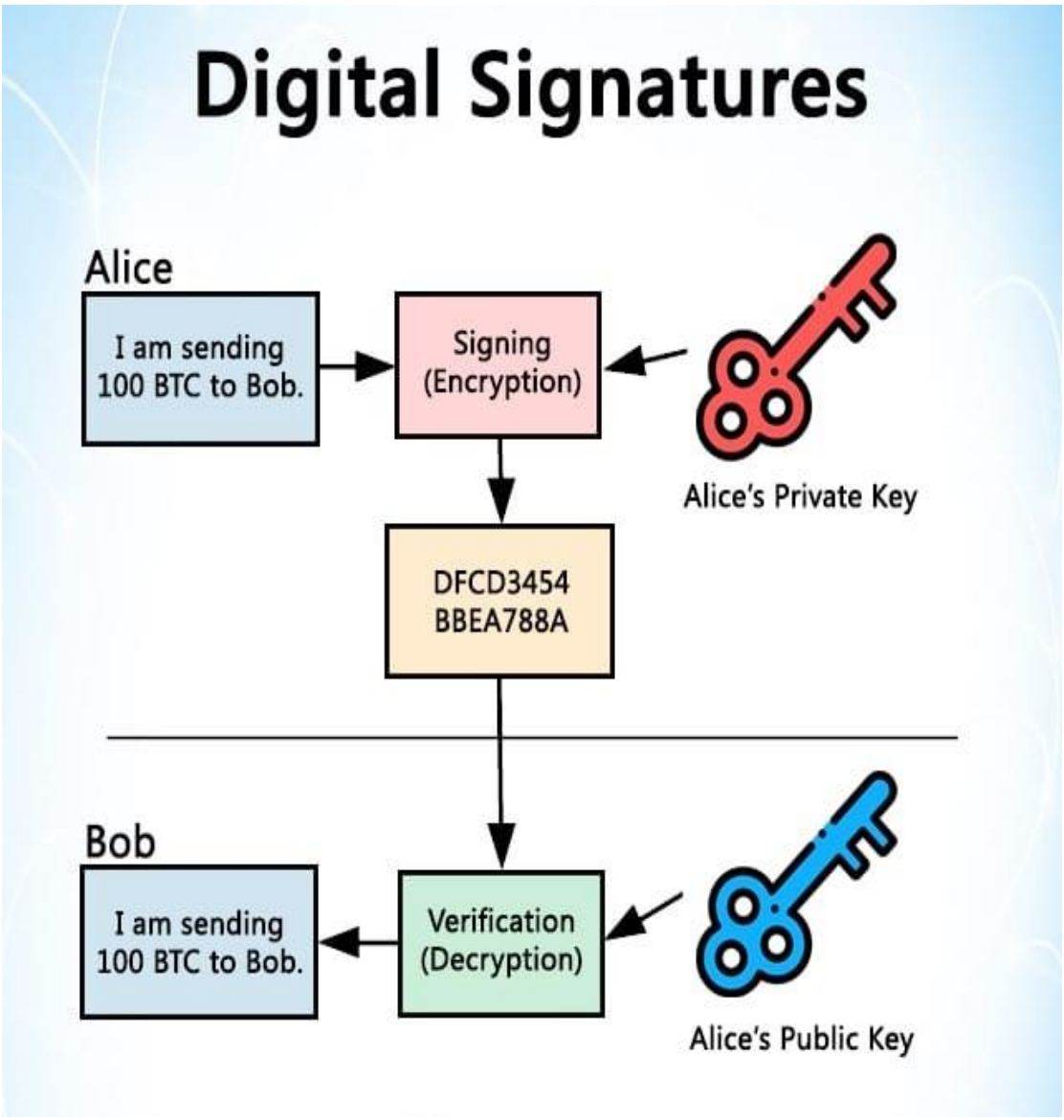


Figure 11. Secure Hash Algorithm

Κεφάλαιο 2. Γλώσσες προγραμματισμού που συναντάμε στα κρυπτονομισματα.

Κάθε γλώσσα προγραμματισμού είναι δυνατόν να χρησιμοποιηθεί για την κατασκευή ενός κρυπτονομίσματος , αυτές που συναντάμε πιο συχνά όμως είναι η C , C++ , Java , Simplicity, Solidity και Python . Γλώσσες προγραμματισμού όπως η C++ δεν χρησιμοποιούνται όμως μόνο στα κρυπτονομισματα αλλά και στην δημιουργία ενός blockchain όπου θα εξηγήσουμε παρακάτω.

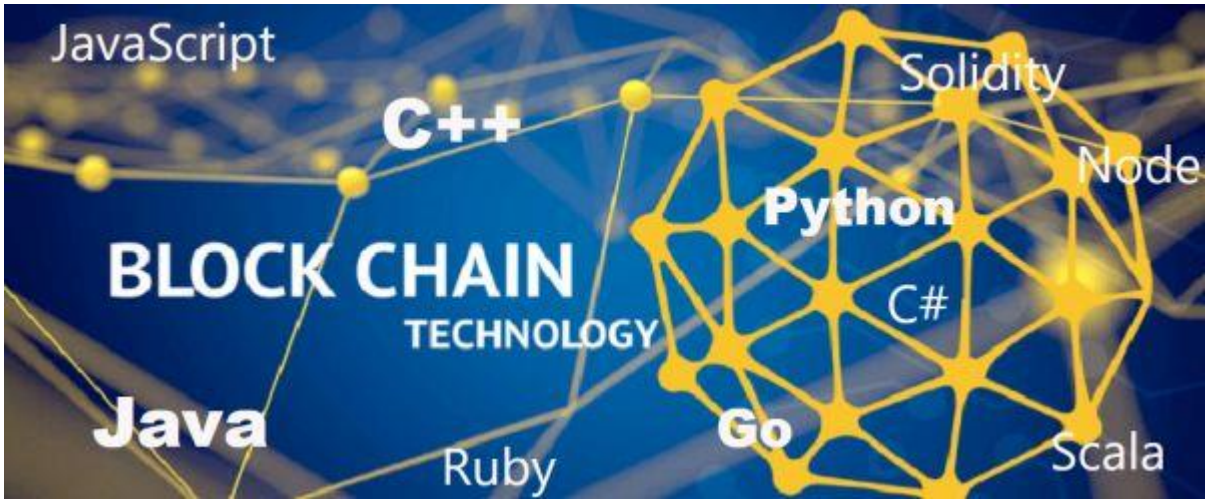


Figure 12. Γλώσσες προγραμματισμού που χρησιμοποιούνται σε κρυπτονομίσματα

Υπάρχουν πολλές γλώσσες προγραμματισμού που χρησιμοποιούνται στα κρυπτονομίσματα και τις εφαρμογές τους. Μπορούμε να δημιουργήσουμε μια λίστα με κάποιες απ' τις πιο σημαντικές από τις γλώσσες προγραμματισμού που χρησιμοποιούνται σε όλες αυτές τις εφαρμογές, καθώς επίσης και να ονομάσουμε κάποιες από τις βασικότερες περιπτώσεις που αυτές χρησιμοποιούνται.

Γλώσσες προγραμματισμού που χρησιμοποιούνται στα κρυπτονομίσματα		
Αριθμός	**Γλώσσα προγραμματισμού**	**Παράδειγμα χρησιμοποίησης**
1	C/ C++	Συμβάλλει σε καλύτερη διαχείριση πόρων και μέσω C/C++ δημιουργούνται τα κρυπτονομίσματα Ripple και Bitcoin
2	Java	Η Java ήταν η βάση στην οποία δημιουργούνται κρυπτονομίσματα αλλά και blockchains όπως Ethereum και Hyperledger.
3	Perl	Η γλώσσα PERL είναι από τις γλώσσες προγραμματισμού που βασίζονται εφαρμογές Blockchain, όπως το PERLIN
4	Python	Στην Python, επειδή είναι γλώσσα που στηρίζεται σε open-source κοινότητα, βασίζονται πολλά έργα Blockchain
5	Simplicity	Η Simplicity είναι μια εύκολη κι εύχρηστη γλώσσα που χρησιμοποιείται για να δημιουργηθούν εφαρμογές Blockchain

6	Solidity	Στη γλώσσα Solidity βασίζεται η δημιουργία από εφαρμογές Blockchain. Πιο συγκεκριμένα, με τη γλώσσα Solidity δημιουργήθηκε η το κρυπτονόμισμα Ethereum

Πίνακας 1. Λίστα με γλώσσες προγραμματισμού που χρησιμοποιούνται στα κρυπτονομίσματα

Άλλες γλώσσες προγραμματισμού που χρησιμοποιούνται στα κρυπτονομίσματα είναι και οι εξής:

- C#
- Ruby
- Go
- Phyton

Επίσης, βασισμένοι στην εργασία του Chand (2021), μπορούμε να παραθέσουμε ένα πίνακα από εφαρμογές κρυπτονομισμάτων Blockchain και τις αντίστοιχες γλώσσες που γράφτηκαν όσο και τις γλώσσες προγραμματισμού που υποστηρίζουν αυτές τις εφαρμογές.

BLOCKCHAIN	**Γλώσσα που έχει γραφτεί**	**Γλώσσες που το υποστηρίζουν**
ARK	JavaScript	JavaScript, Go, Python, C#, TypeScript, Kotlin, Ruby, Swift, PHP
CORDA	Kotlin	Java, Kotlin,
ETHEREUM	Go, C++, Rust	Solidity
EOS	C++	WebAssembly, C, C++
HYPERLEDGER FABRIC	Go, Java, JavaScript, Python	Go, Java, Kotlin

LISK	JavaScript, Node.js	JavaScript
NEO	C#	C#, Java, Kotlin, Python
QTUM	C++, Python, TypeScript	C++, Python, Rust, Go, Lua
STRATIS	C++, C#	C#
WAVES	Scala	Scala

Πίνακας 2. Πίνακας με blockchains και αντίστοιχες γλώσσες προγραμματισμού

2.2 C και C++ , blockchain και οι ιδιοτητεσ τους στα κρυπτονομισματα.

Για να δούμε αναλυτικότερα την επιρροή της γλώσσας C και C++ θα πρέπει να εστιάσουμε στο blockchain. Επομένως τι είναι το blockchain και ποια η λειτουργία του; Το blockchain είναι ένα ψηφιακό αρχείο συναλλαγών. Το όνομα προέρχεται από τη δομή του, στην οποία μεμονωμένες εγγραφές , που ονομάζονται μπλοκ, συνδέονται μεταξύ τους σε μία λίστα, που ονομάζεται αλυσίδα. Τα blockchains χρησιμοποιούνται για την καταγραφή συναλλαγών που πραγματοποιούνται με κρυπτονομίσματα, όπως το Bitcoin.

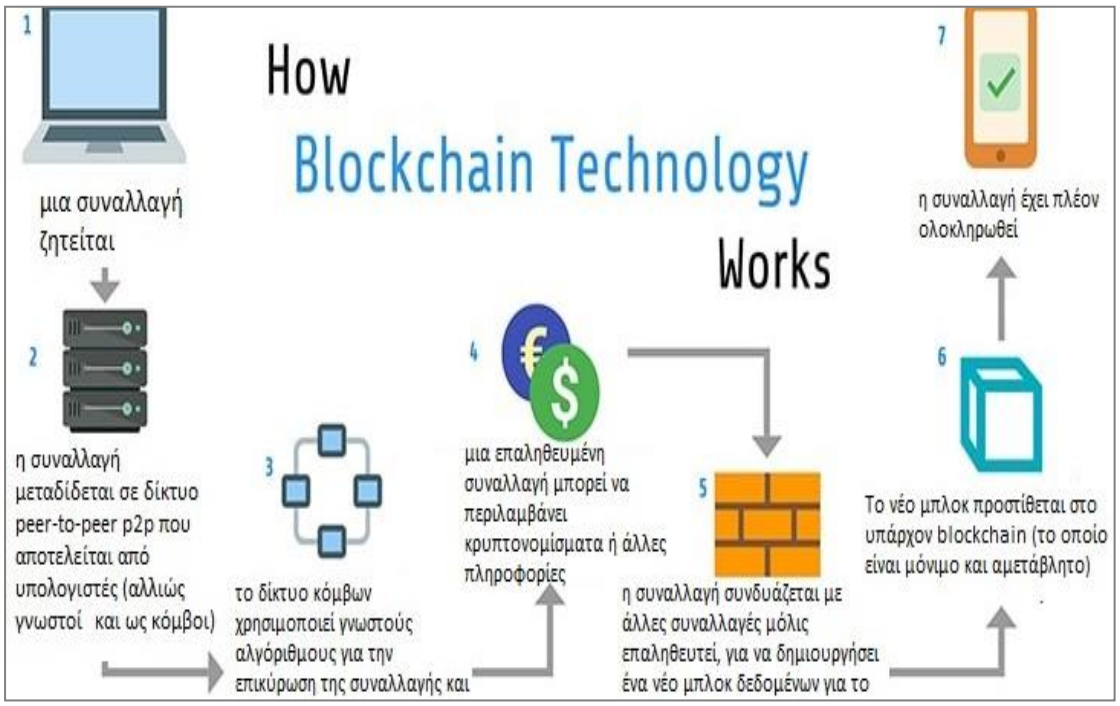


Figure 13. Blockchain Technology

Στην εισαγωγή είδαμε σε γενικές γραμμές τι είναι το blockchain όπως και το ποια είναι τα βασικά χαρακτηριστικά του. Αυτά μπορούμε να τα επαναλάβουμε κι εδώ. Είναι τα:

- Blocks
- Αλυσίδα
- Δίκτυο

Figure 14. Bitcoin logo

Κάθε block αντιστοιχεί σε μια διαφορετική συναλλαγή. Και η αλυσίδα που περιέχει τα blocks δίνει το όνομά της ουσιαστικά στο ίδιο το blockchain. Επίσης, όπως αναφέρθηκε στο πρώτο κεφάλαιο, υπάρχουν τρία είδη κόμβων:

- Πλήρης κόμβος (Full node)
- Ελαφρύς κόμβος (Lightweight node)
- Κόμβος-διαχειριστής (Master node)

Η κύρια διαφορά μεταξύ του πλήρη και του ελαφρύ κόμβου είναι ότι ο πρώτος έχει τη δυνατότητα πρόσβασης σε όλη την πληροφορία που αποθηκεύεται στο blockchain. Ο πλήρης κόμβος δηλαδή έχει πρόσβαση σε όλη την πληροφορία που έχει να κάνει με όλες τις συναλλαγές που έχουν γίνει στο συγκεκριμένο blockchain. Αντιθέτως, ένας ελαφρύς κόμβος έχει δυνατότητα επαλήθευσης όλων των συναλλαγών, αφού και πάλι μπορεί να έχει πρόσβαση στις κεφαλίδες –και μόνο στις κεφαλίδες- απ’ το σύνολο των κόμβων που συμμετέχουν στην αλυσίδα του blockchain, κάτι που είναι όμως αρκετό για αυτό το σκοπό.

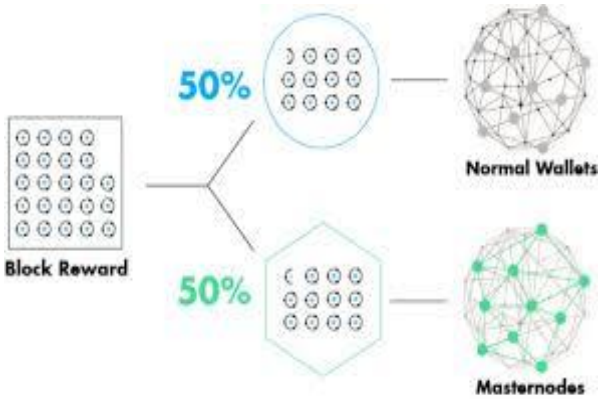


Figure 15. Απλοί κόμβοι και κόμβοι-διαχειριστές

Ο κόμβος-διαχειριστής, επιπλέον, έχει κάποιες προϋποθέσεις προκειμένου κάποιος να αποκτήσει αυτή τη μορφή, καθώς και συγκεκριμένες ιδιότητες, που θα αναφέρουμε παρακάτω:

- Ο κόμβος-διαχειριστής δεν συμβάλλει με νέες συναλλαγές στην αλυσίδα του blockchain
- Ο κόμβος-διαχειριστής είναι σε θέση να παίζει ρόλο επόπτη σε ορισμένες διαδικασίες διαχειριστικές (ψηφοφορίας για αλλαγές στο οικοσύστημα του Blockchain κ.ά.)

Εφόσον μιλάμε για δημόσιο blockchain, μια τέτοια εφαρμογή πρέπει να έχει ορισμένες ιδιότητες, κάποια βασικά χαρακτηριστικά[6]:

- Ασφάλεια
- Διαθεσιμότητα κώδικα (να είναι open source, δηλαδή ανοιχτού κώδικα)[7]
- Πόροι για διαχείριση ερωτημάτων
- Αποδοτικότητα βασικών περιπτώσεων χρήσης του συστήματος: ένα παράδειγμα είναι η επαλήθευση του χρήστη μέσω της ψηφιακής του υπογραφής

[6] Σύμφωνα με ειδικό άρθρο που δημοσιεύεται στο site Medium (2018).

[7] Εδώ δεν πρέπει να ξεχνάμε το Νόμο του Linus, δηλαδή ένα ρητό που διατύπωσε ο ιδρυτής του Λειτουργικού Συστήματος Linux και εφαρμόζεται στην ανάπτυξη λογισμικού: *«Όσα περισσότερα μάτια, τόσο λιγότερα λάθη».* Άρα, εάν ο κώδικας ενός blockchain είναι δημόσιος, αυτό προάγει την ασφάλεια.

Figure 16. Ripple logo

Κάτι που επίσης αξίζει να παρατηρήσουμε είναι ότι το μέγεθος του blockchain συνεχώς αυξάνεται. Υπάρχουν πολλά blockchains και πολλές αλυσίδες και κάθε μία από αυτές αντιστοιχεί σε διαφορετικό κρυπτονόμισμα. Υπήρχε ήδη εδώ και χρόνια η πρόβλεψη ότι ως το 2030, με την εκθετική αύξηση που φαίνεται να υπάρχει στην Εικόνα 17, το μέγεθος ορισμένων Blockchain θα έφτανε το κατώφλι του 1 Terabyte ως το 2030.

Ήδη, όμως, ως το τέλος του Σεπτέμβρη του 2021 (30-09-2021), ένα κρυπτονόμισμα ανοιχτού κώδικα με δημόσιο blockchain, είχε αγγίξει αυτό το όριο, φτάνοντας τα 991.56 GB. Παρ' όλ' αυτά, για τη συμμετοχή σε συναλλαγές με κρυπτονομίσματα, κάθε πλήρης κόμβος πρέπει να κατεβάσει το πλήρες μέγεθος αυτού του blockchain[8].

[8] (Blockchains, n.d.)

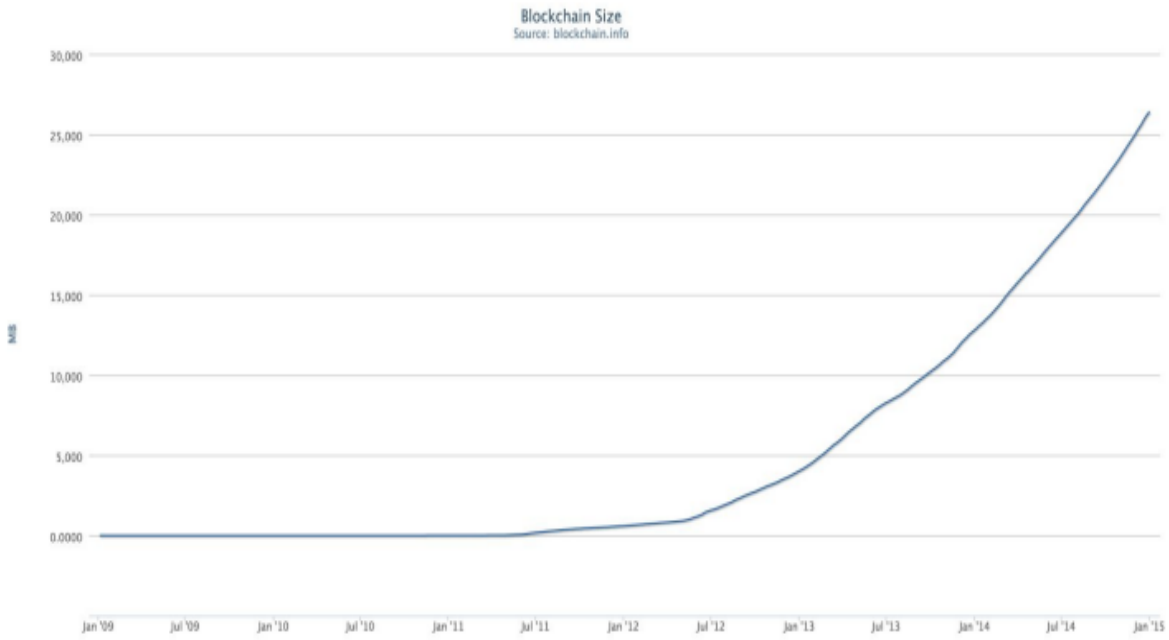


Figure 17. Κόμβοι που περιλαμβάνονται στο Blockchain του Bitcoin

Όσον αφορά τις γλώσσες προγραμματισμού C/C++, πράγματι παίζουν ένα μεγάλο ρόλο στα κρυπτονομίσματα. Παρακάτω απαριθμούμε κάποιους από τους λόγους για το μεγάλο ρόλο που παίζουν:

- Η βιβλιοθήκη bitcoind, πολύ βασική για την εκτέλεση Bitcoin από τους διάφορους χρήστες (κόμβους), είναι γραμμένη στη γλώσσα C++
- Το κρυπτονόμισμα Ripple (Εικ. 15) –έκτο στον κόσμο σε ό,τι αφορά το μέγεθός του ανάμεσα στα κρυπτονομίσματα[9]- που είναι τόσο κρυπτονόμισμα όσο και μέθοδος ψηφιακής πληρωμής που δημιουργήθηκε το 2012, είναι γραμμένο στη γλώσσα C++
- Το ίδιο το Bitcoin (Εικ. 14), που είναι το πρώτο κρυπτονόμισμα που δημιουργήθηκε από τον Satoshi Nakamoto, είναι γραμμένο σε γλώσσα C++ (υπάρχουν και εκδόσεις του γραμμένες σε Go)

Για να καταλάβουμε καλύτερα την αξία που έχει η γλώσσα αντικειμενοστραφούς προγραμματισμού C++ για τη δημιουργία των κρυπτονομισμάτων και τη λειτουργία τους μέσα στο χρόνο, πρέπει να πούμε εδώ και κάτι άλλο. Οι συναλλαγές με Bitcoin μπορούν να γίνονται με δύο τρόπους. Ο ένας από τους δύο είναι ο Bitcoin client,

[9] Εδώ μιλάμε σε όρους κεφαλαιοποίησης αγοράς (market cap): 52 δισεκατομμύρια δολάρια, όπως γράψει ο Frankenfield (2021)

δηλαδή μια εφαρμογή η οποία έχει κανονικό γραφικό περιβάλλον χρήστη (Graphical User Interface- GUI). Δεύτερη εκδοχή μέσα από την οποία κάποιος μπορεί να «τρέξει» κόμβο Bitcoin είναι μέσα από την ακέφαλη έκδοσή του, που προκύπτει μέσα από τη βιβλιοθήκη *Bitcoind*. Είναι αυτή η βιβλιοθήκη που όχι μόνο είναι δημιουργημένη με τη βοήθεια της γλώσσας C++ αλλά και που τρέχουν οι περισσότεροι χρήστες που διατηρούν κόμβους Bitcoin.

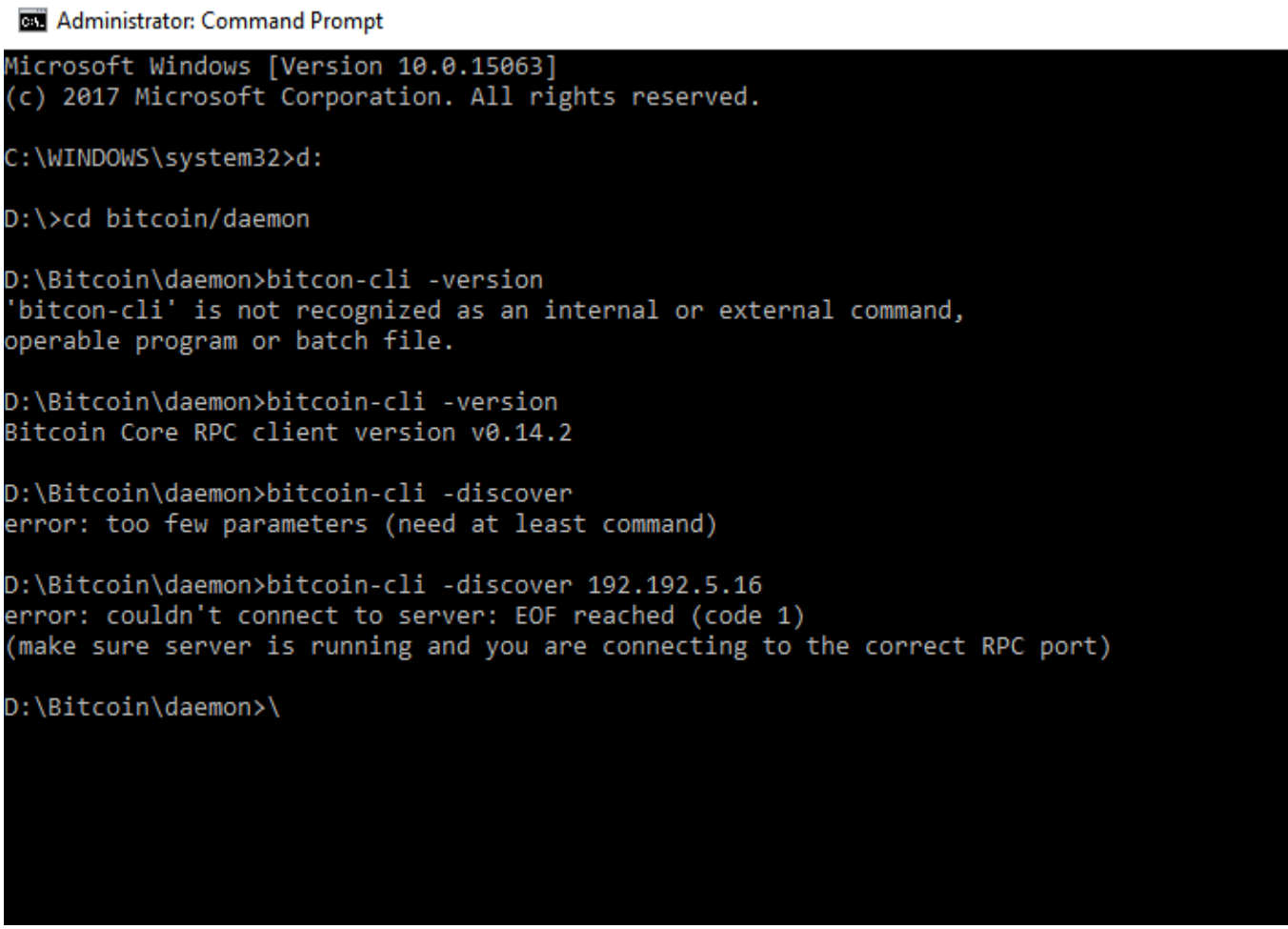


Figure 18. Περιβάλλον bitcoind

Η C++ χρησιμοποιείτια στα κρυπτονομίσματα για δύο συγκεκριμένες πλεονεκτήματα που έχει:

Α) Καλή διαχείριση πόρων

Β) Καλός έλεγχος επάνω στη μνήμη

2.3.Java στα κρυπτονομίσματα

Η Java είναι πολύ σημαντική για τον παγκόσμιο ιστό και επίσης η ανεξαρτησία της πλατφόρμας έχει αυξήσει τη δημοτικότητά της. Με την java μπορούμε σε οποιαδήποτε αλλαγή στο περιεχόμενο ενός μπλοκ, θα δημιουργηθεί ένα νέο αποφεύγοντας το νέο μπλοκ να προστεθεί στην αλυσίδα μέχρις ότου αυτό κριθεί κατάλληλο.
Επίσης, η Java, όπως και η αντίστοιχη γλώσσα scripting, που λέγεται Javascript, χρησιμοποιείται και με άλλους τρόπους στη δημιουργία κρυπτονομισμάτων. Συγκεκριμένα, συμμετέχει στη δημιουργία διαφόρων blockchains κρυπτονομισμάτων, όπως αυτά που ακολουθούν:

- Ark
- Corda
- Hyperledger Fabric
- Lisk
- Neo

Figure 19. Ethereum logo

Το πιο σημαντικό όμως κρυπτονόμισμα στου οποίου συμμετέχει τη δημιουργία η Java είναι το Ethereum (Εικ. 19). Το Ethereum δημιουργήθηκε μόλις το 2014 από τον

Vitalik Buterin .Παρ’ όλ’ αυτά, ήδη εμφανίζεται στις λίστες με τα σημαντικότερα κρυπτονομίσματα και ειδικότερα, σε επίπεδο χρηματοοικονομικό, έχει ήδη κατακτήσει τη 2^{η} θέση σε κεφαλαιοποίηση αγοράς μέσα σε όλα τα κρυπτονομίσματα. Με άλλα λόγια, είναι μόνο το Bitcoin που έχει μεγαλύτερη κεφαλαιοποίηση αγοράς (market capitalization) από το Ethereum.

Τέλος, εκτός από όλα τα παραπάνω, μπορούμε να ανακαλύψουμε μια σειρά από βιβλιοθήκες οι οποίες έχουν δημιουργηθεί με Java και προσφέρουν πολύ σπουδαίες λειτουργικότητες. Η εξειδικευμένη σελίδα Kandi, σε άρθρο της που δημοσιεύτηκε το 2021, έχει παρουσιάζει τις 48 καλύτερες βιβλιοθήκες για κρυπτονομίσματα που δημιουργήθηκαν σε Java και είναι ανοιχτού κώδικα.

Figure 20. Βιβλιοθήκη bitcoinj, δημιουργημένη σε Java (logo)

Αυτές οι βιβλιοθήκες έχουν πολύ πλούσιες λειτουργίες και δυνατότητες και στη συνέχεια παραθέτουμε κάποιες από αυτές:

- Bitcoinj (εικ. 20)
  Είναι μια υλοποίηση του πρωτοκόλλου του Bitcoin μέσα αποκλειστικά από τη γλώσσα Java
- Bisq
  Η Bisq είναι βιβλιοθήκη που επιτρέπει τη δημιουργία ενός δικτύου αποκεντρωμένου, το οποίο, χωρίς κηδεμονία, επιτρέπει τις συναλλαγές από τη

μία με Bitcoin και από την άλλη με άλλα ψηφιακά στοιχεία ενεργητικού και επίσης διάφορα εθνικά νομίσματα

- Bitcoin-wallet

  Είναι ένα πορτοφόλι για συναλλαγές με ηλεκτρονικά νομίσματα (Bitcoin), μέσα από το οποίο κανείς μπορεί να κάνει συναλλαγές με το κρυπτονομίσμα αλλά σε λειτουργικό σύστημα Android (μια εικόνα της εφαρμογής βλέπουμε στην εικ. 21)

Figure 21. Bitcoin wallet: εφαρμογή πορτοφολιού Bitcoin δημιουργημένη σε Java

2.4 Simplicity και solidity

Η **simplicity** εκτός από την ευκολότερη γλώσσα για λύσεις σε θέματα που αφορούν το blockchain, προσφέρει βελτιωμένη ασφάλεια. Επίσης, με τη χρήση στατικής ανάλυσης, μπορεί να καθορίσει το κόστος εκτέλεσης οποιουδήποτε προγράμματος **simplicity**. Κρυπτονομισματα που χρησιμοποιούν την **simplicity** δεν υπάρχουν διότι η γλώσσα χρησιμοποιείται σε προ υπάρχων κώδικες για την βελτίωση τους όπως bitcoin script και Ethereum's EVM

Η **solidity** είναι μια γλώσσα που μοιάζει με JavaScript που αναπτύχθηκε ειδικά για τη σύνταξη του Ethereum. Είναι επίσης υψηλού επιπέδου γλώσσα προγραμματισμού και είναι εύκολο για τους νέους προγραμματιστές, διότι προσφέρει πολλές εξηγήσεις σχετικά με τον τρόπο λειτουργίας του κώδικα. Κρυπτονομισματα που χρησιμοποιούν την **solidity** είναι τα εξής: ethereum , geth , metamask , remix

2.5 Python

- Η **Python** είναι γνωστή για την απλότητά της και είναι η δεύτερη ή ακόμη και η πρώτη γλώσσα προγραμματισμού που προτιμάται για ανάπτυξη λογισμικού και ιστού και πρόσφατα από ειδικούς blockchain.

  Συγκεκριμένα, υπάρχει μια σειρά από blockchain που έχουν ως βασικό σημείο αναφοράς, δηλαδή ως κύρια (ή συμπληρωματική) γλώσσα προγραμματισμού με την οποία δημιουργήθηκαν την Python. Τέτοια blockchains και κρυπτονομίσματα είναι και τα παρακάτω:
  - Ethereum (συμπληρωματικά προς τη Java)
  - Hyperledger/Fabric
  - Steem
  - Neo

Ίσως το σημαντικότερο από όλα αυτά τα έργα είναι (μετά το Ethereum, όπου όμως σημαντικότερο ρόλο παίζει η Java) το Hyperledger. Το Hyperledger δεν είναι

κρυπτονόμισμα, αλλά εφαρμογή blockchain, η οποία όμως όπως βλέπουμε στην επόμενη Εικόνα, έχει κατασκευαστεί από το The Linux Foundation, που περιέχει μια τεράστια κοινότητα από προγραμματιστές που συνεργάζονται για να δημιουργήσουν έργα ανοιχτού κώδικα με πολύ μεγάλη επιτυχία.

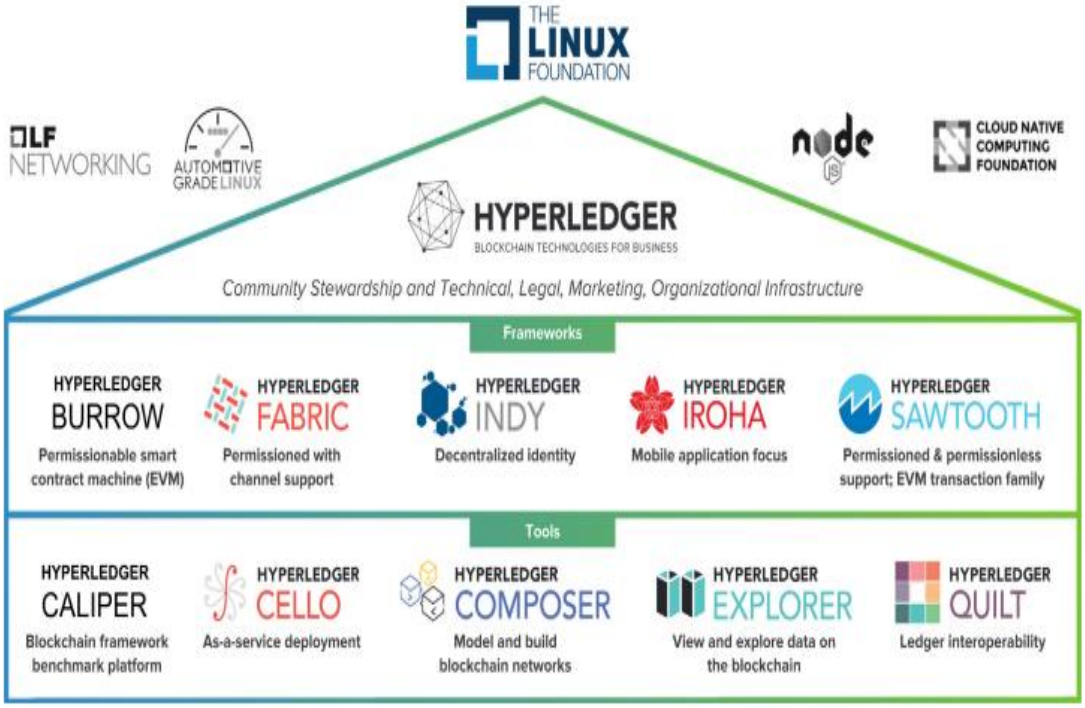


Figure 22. Το Hyperledger Fabric είναι μια σημαντική εφαρμογή κρυπτονομίσματος της Python από το Linux Foundation

- Μερικοί από τους κυρίους λόγους που προτιμάται η συγκεκριμένη γλώσσα προγραμματισμού στα κρυπτονομισματα είναι οι εξής:

1. Η **Python** μας επιτρέπει να δημιουργήσουμε ένα απλό blockchain σε λιγότερες από 50 γραμμές κώδικα.
2. Στην **Python**, το μόνο που χρειάζεται είναι να διορθώσουμε το σφάλμα και να φορτώσουμε ξανά την εφαρμογή μας - δεν θα χρειαστεί να κάνουμε recompile ξανά τον κώδικα. Και αυτό είναι ένα τεράστιο πλεονέκτημα στην κατασκευή blockchain.
3. Κάνει το έργο της οικοδόμησης blocks με τις σχετικές πληροφορίες και τη σύνδεσή τους πολύ πιο εύκολο να γίνει έχοντας και το πλεονέκτημα ότι απαρτίζεται από χρήσιμες βιβλιοθήκες.

Επίσης, η Python έχει σειρά από άλλες εφαρμογές στα κρυπτονομίσματα. Συγκεκριμένα, μπορούμε να αναπτύξουμε εφαρμογές μέσω προβλεπτικών συναρτήσεων της Python (Κινούμενου Μέσου και όχι μόνο), με σκοπό να βρούμε ποιο από τα κρυπτονομίσματα περιμένουμε να είναι η πιο επικερδής επένδυση μέσα στο επόμενο διάστημα.

Κεφάλαιο 3 Διάφοροι τύποι hardware που συναντάμε στα κρυπτονομισματα

Στα προηγούμενα κεφάλαια, είδαμε ότι υπάρχουν στα κρυπτονομίσματα γενικά διάφορα είδη κόμβων. Χαρακτηριστικά είδη είναι κυρίως ο πλήρης κόμβος, αλλά και ο ελαφρύς και άλλα, ακόμη πιο δευτερεύοντα είδη. Εκτός όμως από εκείνα τα είδη, υπάρχει κι ένα άλλο είδος κόμβου, στο οποίο αναφερθήκαμε παρενθετικά. Είναι το είδος του κόμβου εξόρυξης (miner/mining node). Οι συγκεκριμένοι κόμβοι είναι ένα είδος ειδικού κόμβου, που έχει τη δυνατότητα να κάνει εγκρίσεις πολλών συναλλαγών μεμιάς. Δηλαδή, αντί για ένα προς ένα, οι κόμβοι εξόρυξης, προχωρούν σε εγκρίσεις blocks συναλλαγών.

Στο κεφάλαιο αυτό, θα αναλύσουμε τις τεχνολογίες υλικού-υλισμικού (hardware) που βρίσκονται πίσω από τους κόμβους εξόρυξης. Υπάρχουν κάποιες βασικές τεχνολογίες οι οποίες χρησιμοποιούνται για αυτό το σκοπό:

- CPU/GPU
- ASIC (ολοκληρωμένο κύκλωμα ειδικών εφαρμογών)
- FPGA (συστοιχία επιτόπια προγραμματιζόμενων πυλών)
- Hotspot εξόρυξης Ηλίου (Helium mining hot spot)

Πίσω από την εξόρυξη στα κρυπτονομίσματα ή, όπως αλλιώς λέγεται, τους κόμβους ανθρακωρύχους, υπάρχει μια ιστορία που ανάγεται στο πρώτο κρυπτονόμισμα, το Bitcoin. Συνήθως η απόδοση ενός κρυπτονομίσματος μετριέται με βάση το ρυθμό κατακερματισμού (hash rate). Αυτός ο ρυθμός ήταν αρκετά χαμηλός αρχικά, με αποτέλεσμα να μην απαιτείται παρά ένας μέτριος ηλεκτρονικός υπολογιστής. Όμως, στη συνέχεια, τα πράγματα άλλαξαν, εφόσον για τον κατατκερματισμό που χρειάζεται ένας κόμβος-ανθρακωρύχος θα χρειάζονταν όλοι οι πόροι (ισχύς επεξεργασίας, RAM κ.λπ.) ενός υπολογιστή. Η εξέλιξη της απόδοσης αυτής για διάφορα κρυπτονομίσματα φαίνεται στην εικόνα 23 (Laurence, 2017).

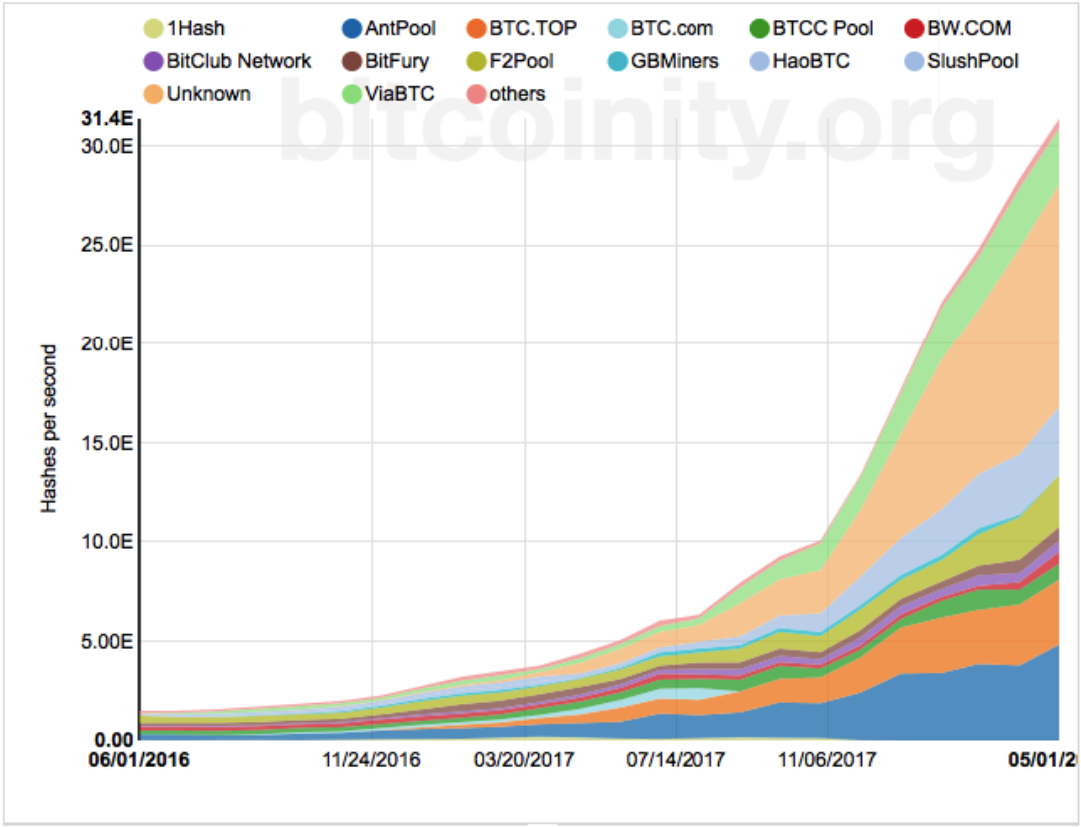


Figure 23. Ρυθμός κατακερματισμού για διάφορα κρυπτονομίσματα

Στη συνέχεια αυτής της εξέλιξης, παίζουν ρόλο τα καινούργια στοιχεία τεχνολογιών hardware που χρησιμοποιήθηκαν για την αύξηση της απόδοσης της εξόρυξης στα κρυπτονομίσματα. Ορισμένα από αυτά τα γεγονότα, όπως τα περιγράφει η Laurence (2017), ήταν τα παρακάτω:

- Πρώτον, η μονάδα επεξεργασίας γραφικών (GPU) ξεκίνησε να χρησιμοποιείται για εξόρυξη- αυτό το γεγονός έδωσε μέχρι και 50 φορές πολλαπλάσια ταχύτητα στους κόμβους ανθρακωρύχους
- Η δημιουργία ειδικών κέντρων δεδομένωνπου ονομάζονται φάρμες έδωσε ώθηση στη χρήση μιας άλλης τεχνολογίας hardware, που ονομάζεται FPGA (συστοιχία επιτόπια προγραμματιζόμενων πυλών- βλ. εικ. 24): η τεχνολογία FPGA είχε ως αποτέλεσμα την αναγκαιότητα για μικρότερη ισχύ επεξεργασίας από ό,τι πριν
- Στη συνέχεια, εμφανίστηκε στο προσκήνιο μια νέα τεχνολογία, που ονομαζόταν ολοκληρωμένο κύκλωμα ειδικών εφαρμογών (ASIC), η οποία έχει τη δυνατότητα εξαιρετικά μεγάλου ρυθμού κατακερματισμού, όπως αυτοί

που χρησιμοποιούνται τώρα- θεωρείται η καλύτερη διαθέσιμη τεχνολογία hardware με μοναδικό κύριο μειονέκτημά της τον θόρυβο

Μπορεί κανείς να πει ότι ένα σημαντικό ορόσημο στη χρήση των διαφόρων μορφών hardware ήταν και το DigiByte. Το DigiByte μπορούσε με χρήση διαφορετικών αλγόριθμων να επιταχύνει τη διαδικασία εξόρυξης. Συγκεκριμένα, το DigiByte ως λογισμικό αλυσίδας blocks (blockchain), έκανε χρήση πέντε διαφορετικών αλγορίθμων:

- SHA-256 (ASIC)
- Scrypt (ASIC/GPU)
- Qubit (GPU)
- Skein (GPU)
- Groestl (GPU)

Κάθε ένας από όλους αυτούς τους αλγορίθμους χρησιμοποιούνταν περίπου στο 20% της δημιουργίας νέων blocks στο blockchain. Με όλες αυτές τις διαφορετικές επιλογές που προσφέρονταν, το DigiByte κατόρθωσε να δώσει τη δυνατότητα και με απλούς υπολογιστές να συμμετάσχουν στη διαδικασία εξόρυξης[10].

[10] (Lauren, 2017)

Figure 24. Φάρμα εξόρυξης με τεχνολογία hardware FPGA

Στη συνέχεια, θα δούμε καθεμία από αυτές τις τεχνολογίες ξεχωριστά. Συγκεκριμένα, ξεκινάμε από τη τεχνολογία ASIC.

3.1 Εφαρμογή εξόρυξης ειδικού ολοκληρωμένου κυκλώματος (ASIC)

Η τεχνολογία hardware ASIC (Application-specific integrated circuit) ή τεχνολογία ολοκληρωμένου κυκλώματος ειδικών εφαρμογών, είναι ίσως, σύμφωνα με ορισμένες απόψεις, η πιο προηγμένη τεχνολογία που υπάρχει στις μέρες μας για κόμβους ανθρακωρύχους.

Κάποια από τα κύρια χαρακτηριστικά στοιχεία που έχει το ASIC δίνονται αμέσως παρακάτω:

- Το ASIC είναι ένα μικροτσίπ σχεδιασμένο για την εκτέλεση αλγορίθμων κατακερματισμού όπου αλγόριθμος κατακερματισμού Είναι ένας μαθηματικός αλγόριθμος που χαρτογραφεί δεδομένα αυθαίρετου μεγέθους σε κατακερματισμό σταθερού μεγέθους.
- Το ASIC είναι ένα μικροτσίπ σχεδιασμένο να εκτελεί αλγόριθμους κατακερματισμού όσο το δυνατόν γρηγορότερα. Αυτό το υλικό μπορεί να υπολογίσει κατακερματισμούς 100.000 φορές γρηγορότερα από τους καλύτερους CPU του κόσμου.

- Κατασκευάζονται με γνώμονα έναν συγκεκριμένο αλγόριθμο κατακερματισμού, οπότε θα πρέπει να αγοράσουμε έναν που έχει σχεδιαστεί για τους συγκεκριμένους τύπους νομισμάτων που θέλουμε να εξορύξουμε. Δεδομένου ότι είναι εξαιρετικά ισχυρά και χρησιμοποιούνται αποκλειστικά για εξόρυξη, αυτά τα μηχανήματα μπορούν να φτάσουν πάνω από 3.000 ευρώ.
- Δεδομένου ότι αυτό το υλικό εκτελεί τρισεκατομμύρια κατακερματισμούς ανά δευτερόλεπτο, ένα σημαντικό μειονέκτημα τους είναι η θερμότητα που εκπέμπουν. Για να τους διατηρήσουμε δροσερούς, θα χρειαστούμε πολλούς ανεμιστήρες, οι οποίοι με τη σειρά τους θα δημιουργήσουν σημαντικό θόρυβο.

Για να πάρουμε μια ιδέα για το πόσο ισχυροί (και πεινασμένοι από ρεύμα) είναι αυτοί οι miners, ας ρίξουμε μια ματιά στις προδιαγραφές ενός σύγχρονου υψηλού επιπέδου miner γνωστό και ως τον Bitmain Antminer S9. Ο Antminer S9 χαρακτηρίζεται απ' τα εξής:

- Hashrate 14 TH / s (Αυτό είναι 14 τρισεκατομμύρια κατακερματισμούς ανά δευτερόλεπτο)
- Μέσο κόστος 2100 $
- Τροφοδοσία 1600 Watt
- 189 τσιπ, σε 3 κυκλώματα

Εν κατακλείδι θα χρειαζόταν για ένα τέτοιο ASIC περίπου ένα χρόνο για να προσφέρει μια θετική απόδοση επένδυσης (ROI return of investment) και σύμφωνα με το ότι οι παράγοντες παραμένουν συνεπείς, κάτι που δεν είναι πιθανό. Αυτός είναι ο λόγος για τον οποίο το πραγματικό κέρδος επιτυγχάνεται με πολλαπλούς ASIC.

Figure 25. Ειδικό ολοκληρωμένο κύκλωμα ASIC

Εκτός όμως από αυτά, υπάρχουν και άλλα στοιχεία που σχετίζονται με αυτό που λέμε εξόρυξη ASIC. Ήδη παρατηρήσαμε πως τα κυκλώματα ASIC έχουν εξαιρετικά υψηλή ταχύτητα και χρόνο ολοκλήρωσης. Επιπλέον, ισχύουν και τα παρακάτω:
Α) Σήμερα, εκτός από πιο προχωρημένη λύση τεχνικά, ένα ολοκληρωμένο κύκλωμα ASIC προσφέρει και την περισσότερο συχνή και επικρατούσα λύση στην αγορά.
Β) Υπάρχουν διάφορα μοντέλα ASIC: άλλα είναι επαγγελματικά και απρόσιτα για τον απλό χρήστη και άλλα είναι πιο φορητά και προσιτά. Όλα αυτά τα μοντέλα επίσης παρουσιάζουν διαφορετικές αποδόσεις όσο και καταναλώσεις ενέργειας.
Γ)Μεγάλη σημασία έχει ο χρόνος ζωής ενός κυκλώματος ASIC, ο οποίος είναι μικρός. Επειδή ο ρυθμός κατακερματισμού που απαιτούνταν για τη διαδικασία της εξόρυξης ήταν γρήγορα αυξανόμενος (όπως φαίνεται καθαρά και στην εικόνα 23 άλλωστε), οι εταιρείες παραγωγής νέων ολοκληρωμένων κυκλωμάτων έπρεπε να παράγουν συνεχώς νέες, πιο προχωρημένες εκδόσεις τους σε ένα διάστημα τόσο μικρό όσο έξι μήνες.
Δ)Οι κόμβοι ανθρακωρύχοι, δηλαδή οι χειριστές τους, χρειαζόταν, ειδικά αρχικά, να αγοράζουν νέα ολοκληρωμένα κυκλώματα ASIC επίσης πολύ συχνά. Πάντως, είναι γεγονός πως μέσα σε ένα μικρό διάστημα οι αγοραστές των νέων μοντέλων ASIC ήταν σε θέση να κερδίσουν αρκετά χρήματα ώστε να μην έχουν ζημία από τις αγορές

τους αυτές. Αυτό ίσχυε για τα πρώτα χρόνια της εξόρυξης κρυπτονομισμάτων (ως το 2013).

Ε)Η σημερινή κατάσταση, όσον αφορά τη δυνατότητα απόκτησης κερδών μέσω των συναλλαγών με Bitcoin, είναι δύσκολη για τον απλό χρήστη, εφόσον τόσο το κόστος απόκτησης νέου εξοπλισμού όσο και το κόστος ψύξης και ηλεκτρισμού είναι αρκετά μεγάλο. Έτσι, είναι προτιμότερη για αυτόν που θέλει να ασχοληθεί με τα κρυπτονομίσματα για ατομικό οικονομικό όφελος, μια πιο μακροπρόθεσμη επένδυση που σε κάποια στιγμή θα μπορέσει να αποδώσει ένα κέρδος.

3.2 Εξόρυξη με την χρήση κάρτας γραφικών (GPU mining)

Η δεύτερη τεχνολογία hardware εξόρυξης που θα μελετήσουμε σε αυτό το κεφάλαιο είναι η τεχνολογία GPU. Έτσι, οι GPU, δηλαδή οι μονάδες επεξεργασίας γραφικών τις οποίες διαθέτει ένας οποιοσδήποτε υπολογιστής σήμερα, διακρίνονται από τα εξής στοιχεία:

- Οι gpu χρησιμοποιούνται πιο συχνά για το χειρισμό γραφικών σε gaming PC, αλλά η ισχύς επεξεργασίας μπορεί επίσης να χειριστεί μαθηματικά κατακερματισμού για την επίλυση blockchain.
- Τώρα, πιθανώς αναρωτιέστε γιατί θα επιλέξαμε την GPU έναντι της CPU. Είναι μια έγκυρη ερώτηση και μια που έρχεται σε αριθμούς. Ενώ οι CPU από την AMD και την Intel θα μπορούσαν κάποτε να εξορύξουν το Bitcoin σαν να ήταν εκτός στυλ, από τότε όμως έχουν μείνει πίσω.
- GPU υψηλών προδιαγραφών από κατασκευαστές όπως η NVIDIA και η AMD είναι αυτές που θα θέλαμε να χρησιμοποιήσουμε. Μια καλή GPU μπορεί πλέον να προσφέρει περίπου 800 εκατομμύρια κατακερματισμούς ανά δευτερόλεπτο εν αντιθέσει με τις CPU, θα είμαστε τυχεροί αν έχουμε 10 εκατομμύρια. Δεν είναι οι ταχύτητες που βλέπουμε με το υλικό ASIC, αλλά είναι αξιοσέβαστες.
- Οι GPU προσφέρουν επίσης αυξημένη ευελιξία έναντι του ASIC. Ένας τύπος GPU μπορεί να εξορύξει πολλά διαφορετικά νομίσματα χωρίς κανένα πρόβλημα. Το μεγαλύτερο πρόβλημα με την εξόρυξη GPU είναι η άνοδος των επιλογών ASIC, οι οποίες είναι πολύ πιο αποτελεσματικές.

- Μπορούμε να χρησιμοποιήσουμε μια μητρική πλακέτα που μπορεί να υποστηρίξει πολλαπλές gpu, ώστε να βελτιώσουμε τον ρυθμό κατακερματισμού και με αυτόν τον τρόπο για να παραμείνουμε ανταγωνιστικοί στο δίκτυο. Βέβαια όπως προ είπαμε και στους asic miners και οι κάρτες γραφικών χρειάζονται αρκετό ρεύμα για να λειτουργήσουν πολλές μαζί καθώς με μια κάρτα δεν θα έχουμε το επιθυμητό αποτέλεσμα.

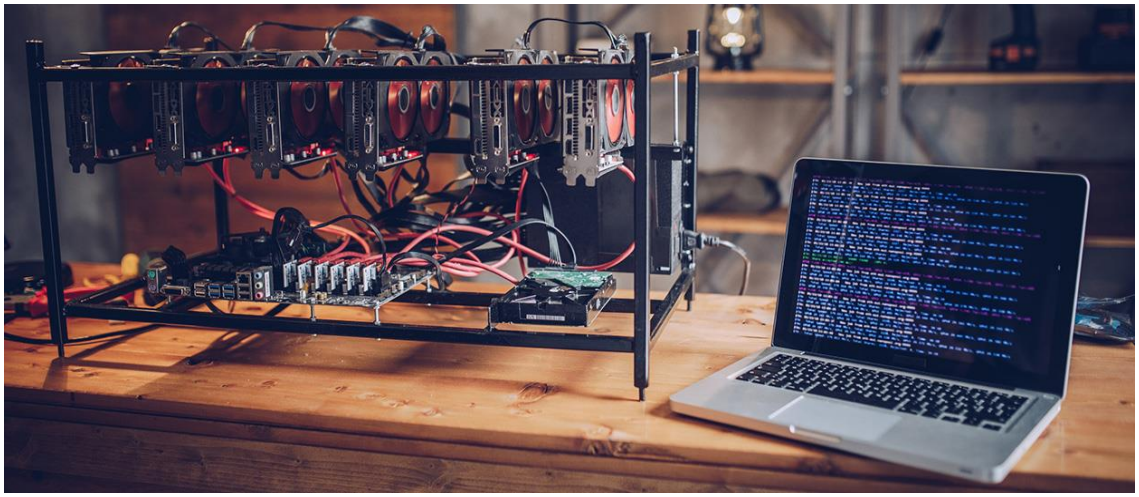


Figure 26. Παράδειγμα εξόρυξης με κάρτες γραφικών

Συνήθως, σε πηγές που έχουν να κάνουν με τα θέματα των κρυπτονομισμάτων, θα δούμε να υπάρχει ο όρος *εξόρυξη CPU/GPU*.

Σε γενικές γραμμές, μπορούμε να πούμε όμως ότι υπάρχει μια διαφοροποίηση μεταξύ αυτών των δύο μεθόδων. Με άλλα λόγια, άλλη είναι η εξόρυξη CPU και άλλη η εξόρυξη GPU (GPU mining). Η εξόρυξη CPU γενικά θεωρείται η πιο «πρωτόγονη» και πρώτης γενιάς μέθοδος, που χρησιμοποιήθηκε στις πρώτες μέρες των κρυπτονομισμάτων μόνο, αν και κάποιοι βλέπουν την εξόρυξη CPU να επανέρχεται σε μια νέα μορφή (βλ. εικόνα 27).

Figure 27. CPU mining για τα κρυπτονομίσματα Verium και Vericoin

Η εξόρυξη CPU, όπως είπαμε, δεν κράτησε για πολύ. Αυτό οφείλεται στο γεγονός ότι υπήρξαν προβλήματα με την μικρή επεξεργαστική ισχύ που μπορεί να προσφέρει μια Κεντρική Μονάδας Επεξεργασίας, σε σχέση με αυτή που απαιτείται, αν κανείς σκεφτεί την απόδοση σε ρυθμό κατακερματισμού που έχουμε ήδη δει παραπάνω ότι απαιτείται. Πάντως, η εξόρυξη GPU θεωρείται η δεύτερη γενιά στην εξόρυξη των κρυπτονομισμάτων. Μάλιστα, αυτό ισχύει πιο ειδικά και για την εξόρυξη κρυπτονομισμάτων Bitcoin. Γενικά, πρόσφερε αυξημένη ταχύτητα (50πλάσια της αρχικής) αλλά είχε και κάποια βασικά μειονεκτήματα, όπως ήταν:

- Η υπερθέρμανση της μονάδας και του υπολογιστή
- Ο υψηλός βαθμός της χρήσης του υλικού, κατά τη διάρκεια της διαδικασίας εξόρυξης

Με βάση ένα άρθρο που έχουν γράψει τρεις επιστήμονες, οι Narayanan, Bonneau and Felten (2016), η εξόρυξη GPU χαρακτηρίζεται και από τα παρακάτω:

Α) Βασίζεται σε μια εναλλακτική χρήση μιας μονάδας της πλειοψηφίας των περισσότερων σύγχρονων υπολογιστών, που δεν είναι άλλη από τη GPU, δηλαδή τη μονάδας επεξεργασίας γραφικών (Graphical Processing Unit): αυτή η μονάδα, όπως

προαναφέραμε, ήταν από τα σημαντικότερα στοιχεία που έχει ένα gaming PC, αφού εξειδικεύεται στη δημιουργία γραφικών υψηλής απόδοσης.

Β) Η GPU μπορεί και επιταχύνει τις διαδικασίες της εξόρυξης κρυπτονομισμάτων (όπως είπαμε, μέχρι και 50 φορές παραπάνω από μια απλή CPU), επειδή έχει δύο στοιχεία σημαντικά:

- Υψηλή δυνατότητα για παράλληλη επεξεργασία
- Υψηλούς ρυθμούς διεκπεραίωσης (throughput)

Γ) Επειδή η εξόρυξη μπορεί να βασίζεται σε αριθμολεξήματα, δηλαδή με απλά λόγια σε διαφορετικά νούμερα που άντιστοιχούν σε ένα ανθρακωρύχο κόμβο τα οποία όμως μπορούν να υπάρχουν στην ίδια συσκευή, η παράλληλη επεξεργασία που δίνει η GPU είναι απόλυτα κατάλληλη για τη διαδικασία της εξόρυξης

Δ)Άλλο πλεονέκτημα που έχει μια γραφική μονάδα επεξεργασίας έχει σειρά από Αριθμητικές και Λογικές Μονάδες (ALU) , που έχουν τη δυνατότητα να κάνουν με παράλληλη επεξεργασία υπολογισμούς όπως αυτοί που χρειάζονται για τις συναρτήσεις κατακερματισμού που χρησιμοποιούν οι miners (όπως ο αλγόριθμος κατακερματισμού SHA-256)

Ε)Η εξόρυξη με τη βοήθεια GPU χρησιμοποιεί και μια άλλη γλώσσα προγραμματιστική, που λέγεται OpenCL και παίζει το ρόλο του μεσολαβητή στην όλη διαδικασία της εξόρυξης

Ζ) Σε επίπεδο τεχνικό και σε επίπεδο οικονομικών, είναι ευκολότερο για τον απλό χρήστη, με την έννοια ότι είναι και προσιτό να αγοράσει κανείς μια τέτοια συσκευή και επίσης να κάνει τις διαδικασίες εγκατάστασης του εξοπλισμού

Η) Ο υπερχρονισμός επεξεργαστή (overclocking) σε ποσοστό 50% επιπλέον που μπορεί να φέρει σε πέρας μια γραφική μονάδα επεξεργασίας είναι χρήσιμος για τη διαδικασία εξόρυξης, ακόμη και αν μπορεί ως ένα ποσοστό που μπορεί να φτάνει το 30% να δίνει εσφαλμένα αποτελέσματα

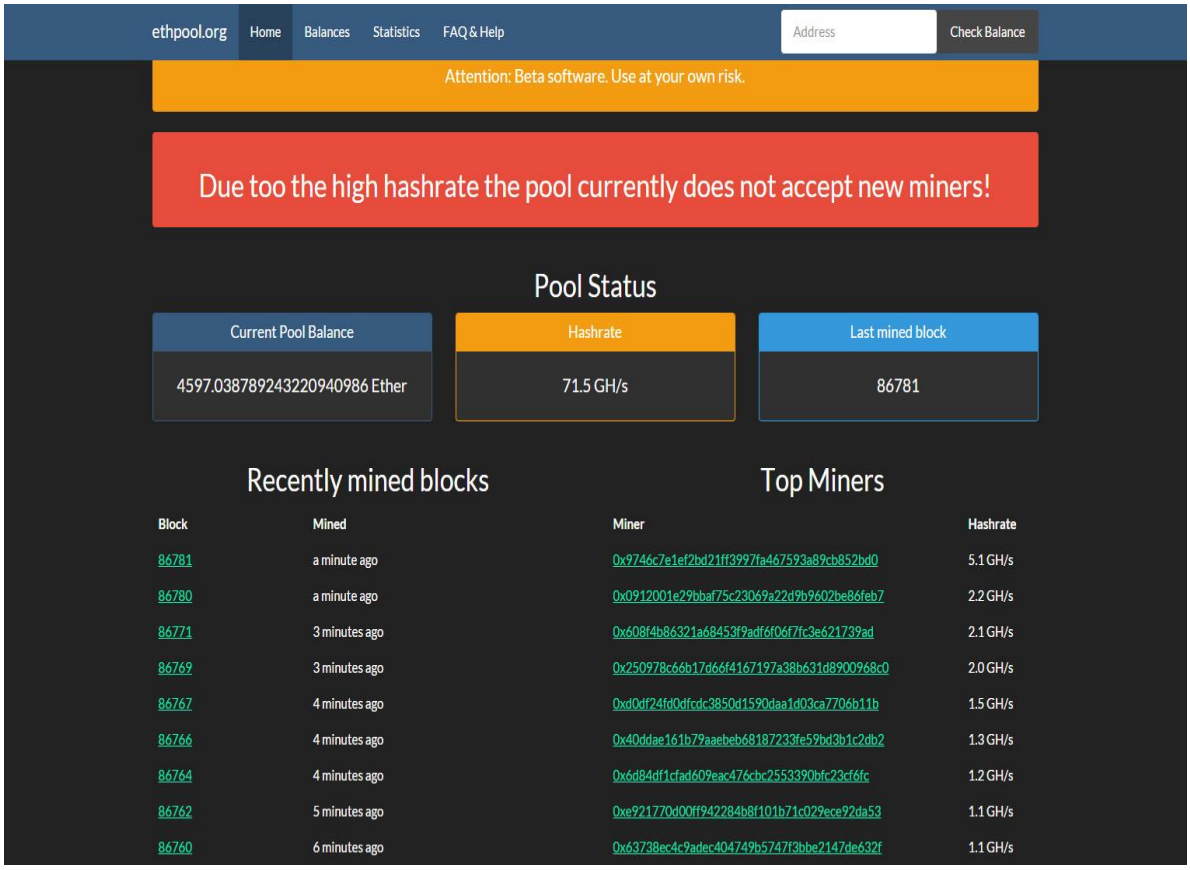


Figure 28. OpenCL για mining

Μπορούμε να πούμε γενικά ότι, ως δεύτερο στάδιο της ιστορίας του mining, το GPU mining κυρίως το λειτουργούσαν ερασιτέχνες οι οποίοι ασχολούνταν με σχετικά μικρό εξοπλισμό, ιδίως εξοπλισμό ψύξης. Όμως, τελικά, το στάδιο αυτό του GPU mining ξεπεράστηκε και υπάρχουν ορισμένοι λόγοι γι' αυτό, όπως οι παρακάτω:

- Είναι αδύνατο να χρησιμοποιηθεί όλη η εσωτερική δυναμική τους για τη διαδικασία της εξόρυξης-αυτό οφείλεται στο ότι υπάρχει σειρά από Μονάδες Κινητής Υποδιαστολής, οι οποίες δε μπορούν να χρησιμοποιηθούν καθόλου για τις ανάγκες του κατακερματισμού (ειδικά για τις συναρτήσεις κατακερματισμού SHA-256)
- Δεν έχει βολικό σύστημα ψύξης, όταν οι μονάδες τοποθετηθούν η μία πλάι στην άλλη (σειριακά)
- Η λειτουργία τους απαιτεί μεγάλη ποσότητα ισχύος, δηλαδή καταναλώνει μεγάλες ποσότητες ηλεκτρικής ενέργειας ανά μονάδα χρόνου

- Ακόμα και με δεκάδες μονάδες GPU μαζί, η μέθοδος εξόρυξης με GPU τελικά δε μπορούσε να ανταπεξέλθει στα μεγέθη των blockchains που προέκυψαν μετά το 2014

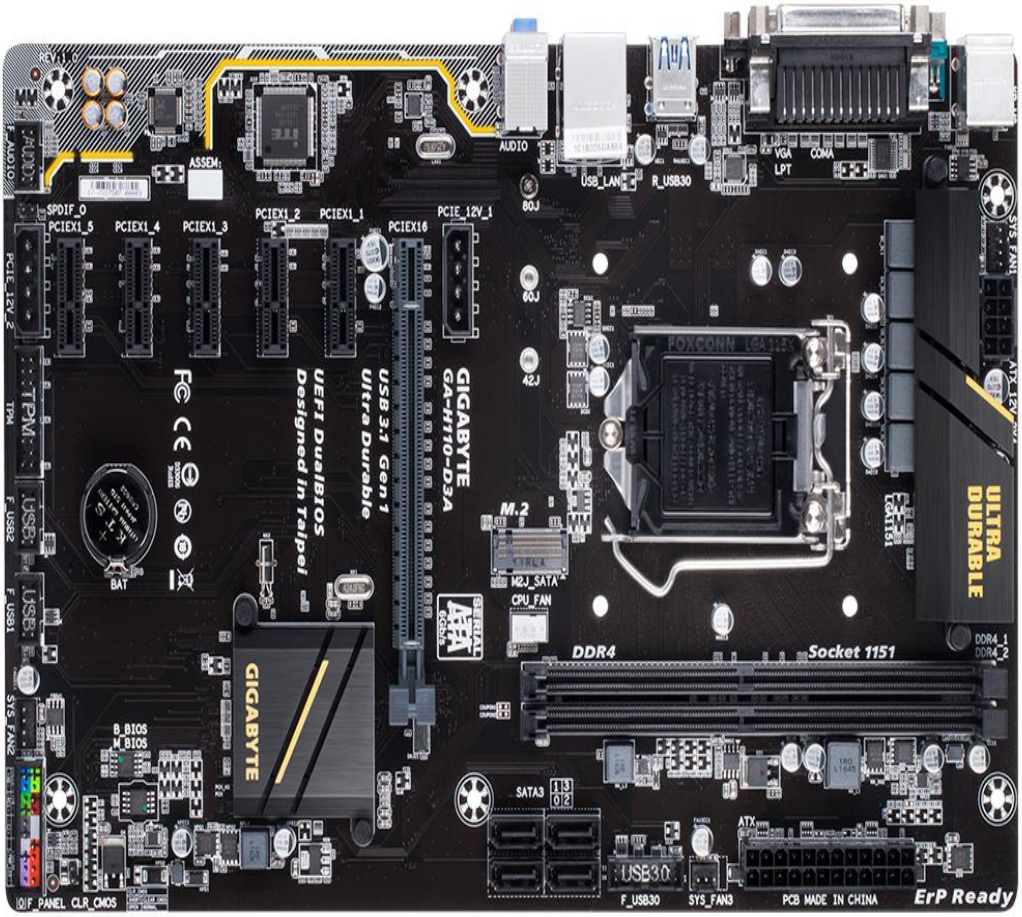


Figure 29, Εμπορικό μοντέλο μητρικής πλακέτας με 6 μονάδες GPU

Όπως εξηγήσαμε παραπάνω, είναι πλέον αδύνατο εδώ και χρόνια να χρησιμοποιηθεί μια τεχνολογία όπως η εξόρυξη GPU από ένα νόμισμα με blockchain όπως το Bitcoin. Αυτό έχει να κάνει με το γεγονός ότι ητεχνολογία κρυπτονομισμάτων γρήγορα χρειαζόταν Gigahashes/second, ενώ οι σειρές ή και οι μητρικές πλακέτες, όπως αυτές που βλέπουμε στην εικόνα 29, με μονάδες GPU μπορούσαν συνήθως να φτάσουν μόλις και μετά βίας τις μερικές εκατοντάδες MegaHashes. Η τεχνολογία αυτή, αν εξαιρέσουμε κάποια εναλλακτικά κρυπτονομίσματα που δημιουργήθηκαν στα πρώτα στάδια της ανάπτυξής τους, έχει εγκαταλειφθεί και τη θέση της πήραν

αυτές που ακολουθούν. Θα συνεχίσουμε με μία από αυτές, την τεχνολογία hardware FPGA[11]

3.3.Field-Programmable Gate Arrays (FPGA) στα κρυπτονομισματα

Τα FPGA είναι ολοκληρωμένα κυκλώματα με λογικά μπλοκ προγραμματισμένα και διαμορφωμένα χρησιμοποιώντας γλώσσα περιγραφής υλικού (HDL). Προσφέρουν ουσιαστικά μια εξειδικευμένη λύση υλικού κατασκευασμένη από την αρχή για την εξόρυξη κρυπτονομισμάτων.
Δεδομένου ότι το τσιπ έχει σχεδιαστεί για αυτό το σκοπό, μπορούσε να προσφέρει βελτίωση απόδοσης σε σχέση με CPU και GPU. Σύμφωνα όμως με τα σημερινά πρότυπα, αντιστοιχούν απλώς στα ποσοστά κατακερματισμού των GPU υψηλών προδιαγραφών, αλλά έχουν ένα πλεονέκτημα: κατανάλωση ενέργειας.
Τα FPGA είναι γνωστά για την ικανότητά τους να λειτουργούν σε περιβάλλοντα χαμηλής ισχύος, καθιστώντας τα πιο οικονομικά από άποψη ενέργειας .

Όπως εξηγήσαμε στην προηγούμενη παράγραφο, τόσο η εξόρυξη με Κεντρική Μονάδα Επεξεργασίας όσο και η εξόρυξη με Μονάδα Γραφικής Επεξεργασίας δε μπόρεσαν να πάνε μακριά όσον αφορά τη δυνατότητά τους για κατακερματισμούς στα νεότερα blockchain των κρυπτονομισμάτων που παρέμεναν ενεργά και ειδικά τα κορυφαία όπως το Bitcoin. Το 2015 ήταν εντελώς αδύνατο να χρησιμοποιήσεις GPU για εξόρυξη, αλλά μόλις το 2011 άρχισα να γίνει η αλλαγή από χειριστές κάποιων κόμβων ανθρακωρύχων σε πιο νέες τεχνολογίες hardware. Τα FPGA, όπως και οι μονάδες GPU, έχουν κάποια συγκεκριμένα πλεονεκτήματα εξόρυξης που είναι πιο προχωρημένα:

- Η απόδοσή του είναι ενός υλικού φτιαγμένου ειδικά για εξόρυξη κρυπτονομισμάτων
- Ένα υλικό FPGA επιτρέπει από το χρήστη του να το προσαρμόσει στις δικές του απαιτήσεις

[11] (Narayanan, Bonneau and Felten, 2016)

- Το hardware FPGA είναι κατάλληλο για να κάνει λειτουργίες μεταξύ δυαδικών ψηφίων
- Όλο το εύρος του hardware προσφέρεται να χρησιμοποιηθεί από το χρήστη για τη διαδικασία του mining
- Ενώ με CPU/GPU εξόρυξη, είναι δύσκολο να τοποθετηθούν σειριακά και να κερδηθεί από εκεί μεγαλύτερη απόδοση μέσω boards, στην περίπτωση του FPGA, είναι δυνατό να γίνει αυτό
- Η απόδοση που μπορεί να δώσει μια εγκατάσταση-σειρά από FPGA φτάνει από ένα GigaHash μέχρι και ένα δισεκατομμύριο hashes ανά δευτερόλεπτο, κάτι που αφήνει κατά πολύ πίσω την απόδοση του GPU

Figure 30. Συσκευή για FPGA εξόρυξη με ενσωματωμένη ψύξη

Παρ'όλ'αυτά, το FPGA έχει και κάποια μειονεκτήματα, που δεν του επέτρεψαν τελικά να εξελιχτεί στη λύση για εξόρυξη που κανείς θα περίμενε αρχικά και χρησιμοποιήθηκαν για σχετικά σύντομο χρονικό διάστημα σε μεγάλη κλίμακα:

- Είχαν και αυτά μπει σε διαδικασία υπερχρονισμού επεξεργαστή ή overclocking, με σκοπό να χρησιμοποιηθούν στα πιο προχωρημένα

κρυπτονομίσματα- η διαδικασία αυτή είχε ως αποτέλεσμα να παρατηρήσουν οι χρήστες σφάλματα εκτέλεσης και δυσλειτουργίες κατά τη διαδικασία του mining

- Το hardware FPGA δεν είναι τόσο προσιτό σε ένα απλό χρήστη, με την έννοια ότι δεν το βρίσκεις σε ένα κατάστημα πώλησης με είδη υπολογιστών, όπως βρίσκεις μια ΚΜΕ ή μια GPU
- Επιπλέον, οι μονάδες FPGA ήταν αρκετά ακριβές, με αποτέλεσμα παρά τη μεγάλη απόδοσή τους σε επίπεδο λειτουργίας να μην έχουν πολύ υψηλότερη απόδοση κόστους

Όλα τα παραπάνω είχαν ως αποτέλεσμα να μην κρατήσει πολύ καιρό η χρήση μαζικής κλίμακας των FPGA. Μάλιστα, θεωρείται πως κράτησε λιγότερο από αυτή των GPU, δηλαδή λιγότερο από ένα χρόνο. Η κρίση αυτή των FPGA οδήγησε τελικά στη λύση που είδαμε στην παράγραφο 3.1, δηλαδή στη μαζική χρήση του υλικού τύπου ASIC.

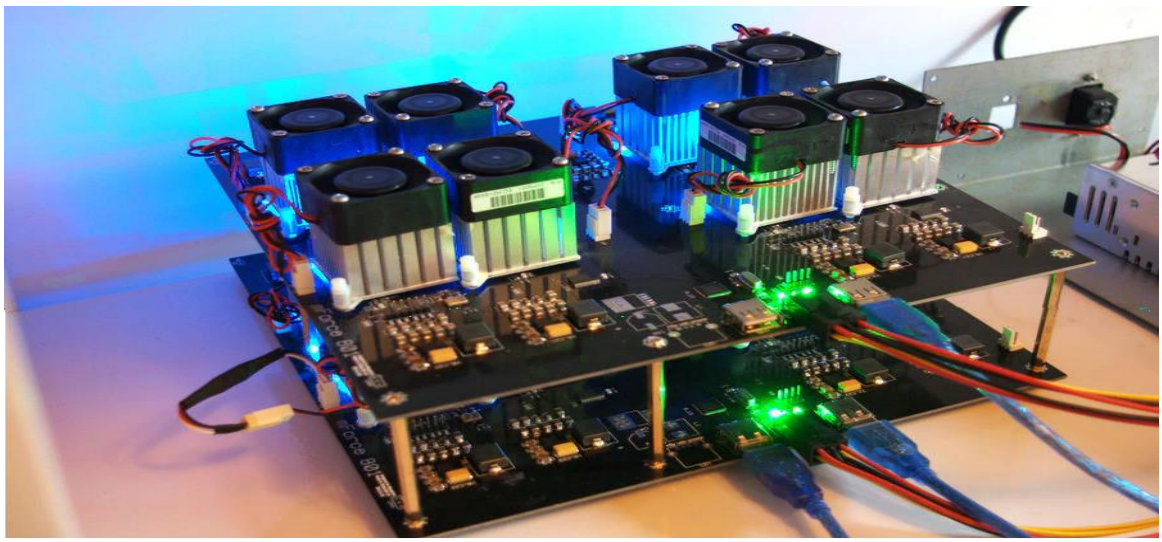


Figure 31. Εξόρυξη με FPGA

3.4 Helium mining hot spot

Η εξόρυξη για το κρυπτονόμισμα Helium πραγματοποιείται με μια πρωτοποριακή τεχνολογία η οποία χρησιμοποιεί το hotspot και βάση αυτού μπορεί κάποιος να εξορύξει ένα συγκεκριμένο νόμισμα το οποίο έχει και το ίδιο όνομα “Helium HNT”.

Η χρησιμότητα του Helium mining hot spot δεν σταματά εκεί βέβαια. Το μηχάνημα αυτό είναι παρόμοιο με το Wi-Fi router που έχουμε σπίτι μας αλλά η πραγματική του ονομασία είναι longfi router του οποίου η κεραία έχει την δυνατότητα να στείλει το σήμα του έως και 200% πιο μακριά από ένα απλό δρομολογητή το οποίο μπορεί σε συνεργασία με άλλους χρήστες που χρησιμοποιούν helium miners να δημιουργήσουν ένα δίκτυο στο οποίο μπορεί να βασιστεί οτιδήποτε υπάγεται σε internet of things. Επιπρόσθετα υπάρχουν και helium miners εξωτερικού χώρου οι οποίοι μάλιστα έχουν και την δυνατότητα να χρησιμοποιούν και 4G με την χρήση κάρτας Sim, για να καλύψουν τις ανάγκες αυτών που σε μια απομακρυσμένη περιοχή δεν διαθέτουν είτε Wi-Fi είτε μια γραμμή ethernet.

Figure 32. Indoor helium miner

Λόγω το ότι είναι βασισμένα στην αρχιτεκτονική των FPGA, η κατανάλωση σε ρεύμα είναι πολύ μικρή (10 Watts) και το bandwidth που χρειάζονται από το δίκτυο μας είναι πάρα πολύ λίγο. Έτσι λοιπόν βλέπουμε μια ενδιαφέρουσα εξέλιξη τόσο των κρυπτονομισμάτων όσο και των τεχνολογιών οι οποίες τα συνοδεύουν και μάλιστα πως μπορούν να μας είναι χρήσιμες και ακόμη και αν κάποιος δεν σχετίζεται με τα κρυπτονομισματα μπορεί με την λύση του hotspot mining να έχει και δωρεάν πρόσβαση στο internet και με αυτή την πρωτοποριακή λύση βλέπουμε πως και οι

miners κερδίζουν από την κίνηση που έχουν στο δίκτυο hotspot τους αλλά και οι καθημερινοί πολίτες! Όσο βέβαια για τους helium miners ακόμα εξελίσσονται και μένει μόνο στο μέλλον τι έχουν να παρουσιάσουν τόσο σε υλικό όσο και σε λογισμικό! Στη συνέχεια θα δούμε και κάποιες ακόμα λεπτομέρειες για τη δομή τους.

Εικόνα 1.Helium indoor miner

Figure 33. Outdoor helium miner

Εκτός από την παραπάνω γενική παρουσίαση, μπορούμε παρακάτω να δούμε ορισμενα από τα πολύ βασικά συστατικά στοιχεία που έχει ένα δίκτυο Helium. Αυτά τα στοιχεία ως σύνολο είναι έξι. Είναι αυτά που θα δούμε στη συνέχεια:

A) Proof-of-coverage

Το Helium χρησιμοποιεί ένα προχωρημένο αλγόριθμο για τους miners, που ονομάζεται proof-of-coverage ή PoF. Ο αλγόριθμος blockchain αυτός αντικαθιστά τους πιο παραδοσιακούς Proof-of-work και Proof-of-stake και επιβεβαιώνει την

παροχή κάλυψης εκ μέρους των hotspots. Με αυτό τον αλγόριθμο, οι miners μπορούν να αποδείξουν κυρίως δύο διαφορετικά πράγματα:

- Τα hospots αναπαραστούν σωστά την τοποθεσία τους
- Τα hotspots παρέχουν τη θεμιτή κάλυψη που ισχυρίζονται τα ίδια πως παρέχουν

Γενικά, ο συγκεκριμένος αλγόριθμος έχει τα εξής χαρακτηριστικά στοιχεία:

- Είναι καινοτομικός και πρωτότυπος
- Είναι ασφαλής σε επίπεδο κρυπτογραφίας

Figure 34. Αναπαράσταση του αλγορίθμου PoF

Β) Το Δίκτυο Helium

Το δίκτυο των κόμβων του Helium μπορούμε να πούμε πως έχει μια σειρά από ξεχωριστούς αλλά και συνδεδεμένους μεταξύ τους σκοπούς:

- Αναγνώριση συσκευών
- Αυθεντικοποίηση συσκευών
- Παροχή κρυπτογραφημένης μετάδοσης δεδομένων
- Παροχή της αυθεντικοποίησης δεδομένων
- Παροχή βασικών στοιχείων δοσοληψιών

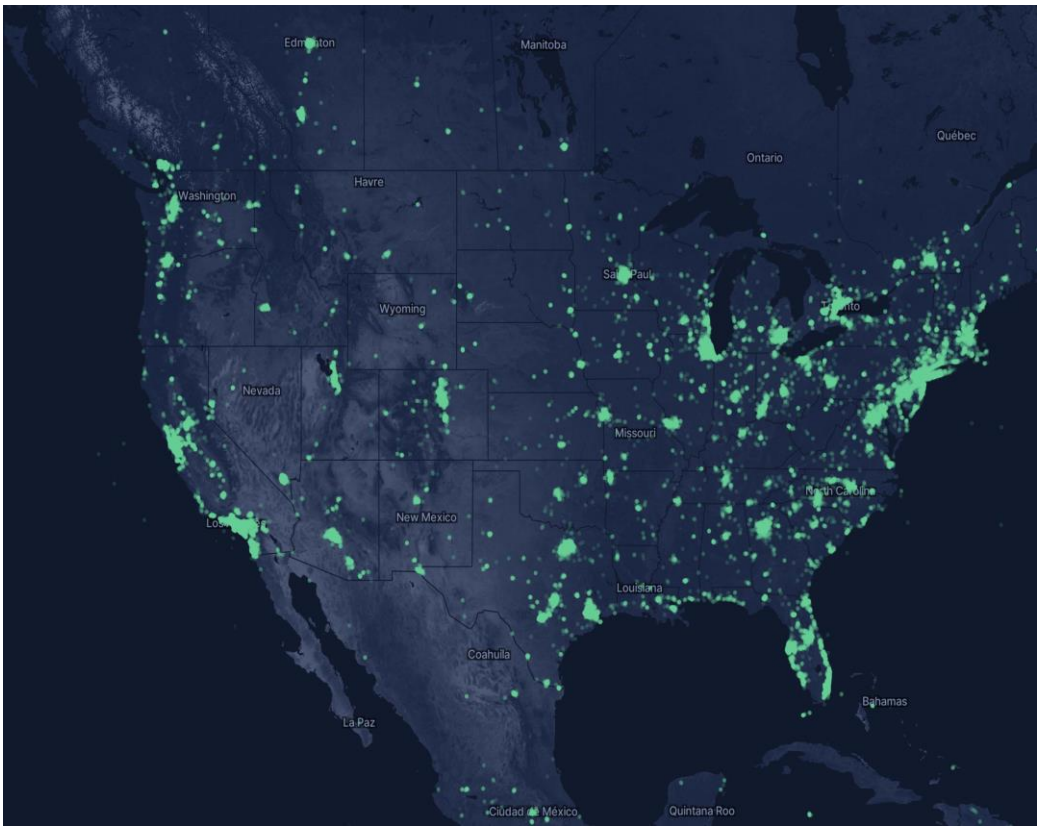


Figure 35. Απεικόνιση των κόμβων του δικτύου Helium blockchain network

Γ) Helium Consensus Protocol

Το Helium έχει το δικό του πρωτόκολλο για την ανίχνευση και διόρθωση σφαλμάτων, όπως αυτά που χρησιμοποιούνται στις αλυσίδες blockchain. Ουσιαστικά, το ζητούμενο εδώ είναι να υπάρχει ένα τρόπος συνεννόησης μεταξύ των

κόμβων miner, όταν δεν ξέρουμε εκ των προτέρων ποιος λέει αλήθεια και ποιος όχι σχετικά με μια τιμή ενός δεδομένου ή την κατάσταση του δικτύου Helium.

Το πρωτόκολλο αυτό έχει τα παρακάτω στοιχεία:

- Είναι χωρίς άδεια εισόδου (permissionless), δηλαδή το blockchain του Helium είναι ανοιχτό για ανάγνωση και γράψιμο σε οποιονδήποτε (όπως τα δημόσια blockchains)
- Δίνει υψηλό ρυθμό διεκπεραίωσης
- Είναι ανθεκτικό στην λογοκρισία (οι miners δεν έχουν πρόσβαση στις παλιότερες συναλλαγές)
- Είναι ασύγχρονο
- Έχει ανοχή λαθών βυζαντινού τύπου (byzantine fault tolerance)

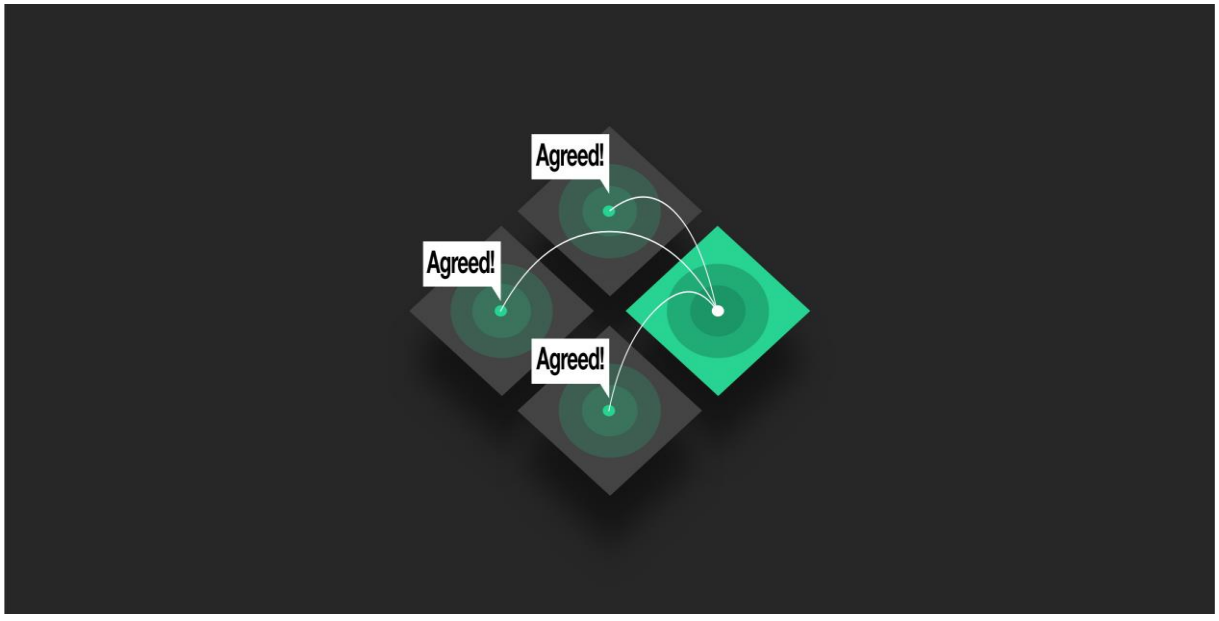


Figure 36. Πρωτόκολλο συμφωνίας Helium

Δ) WHIP

Το WHIP είναι ένα πρωτόκολλο του Helium που έχει τα παρακάτω στοιχεία:

- Έχει να κάνει μα ασύρματα δίκτυα
- Είναι ανοιχτού κώδικα
- Ακολουθεί τα δικτυακά πρωτόκολλα που ήδη υπάρχουν
- Είναι σχεδιασμένο για τεράστιες γεωγραφικά περιοχές
- Είναι σχεδιασμένο για συσκευές χαμηλής ισχύος
- Δε χρειάζεται πιο προχωρημένα ολοκληρωμένα κυκλώματα (chips) για να τρέξει
- Δε χρειάζεται άλλες τεχνολογίες ή τεχνικές διαμόρφωσης (όχι ελεύθερες-δωρεάν για να τρέξει

E) Proof-of-Location

Το Proof-of-Location είναι ένα σύστημα γεωεντοπισμού που χρησιμοποιεί το πρωτόκολλο WHIP. Έχει τα εξής στοιχεία:

- Δεν καταναλώνει μεγάλη ποσότητα πόρων
- Δίνει με ασφάλεια αποδεκτικό της τοποθεσίας του χρήστη-κόμβου που περιλαμβάνεται στην αλυσίδα blockchain

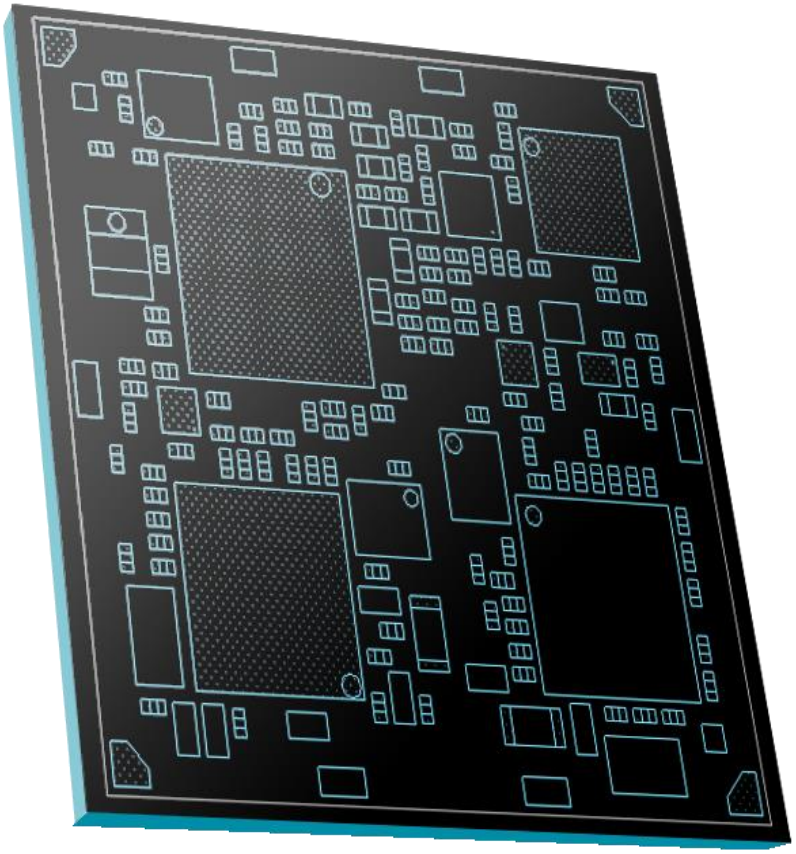
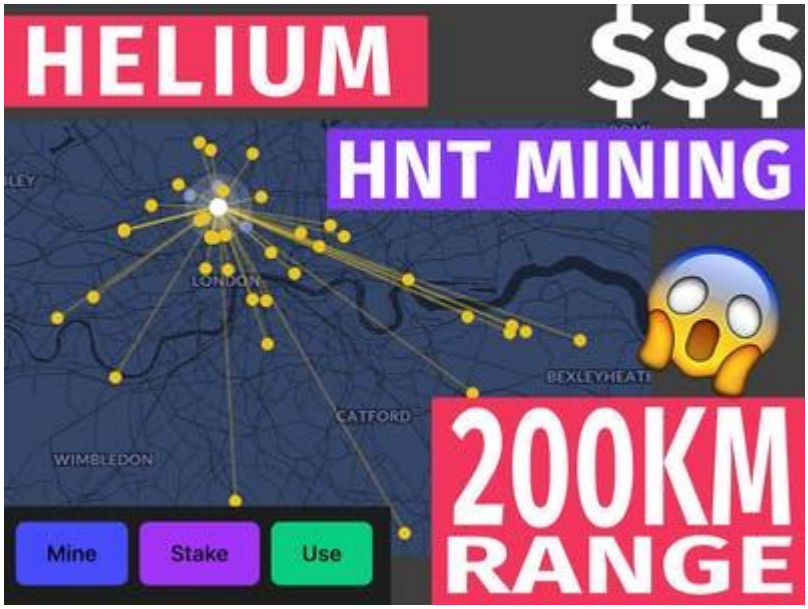


Figure 37. Γεωεντοπισμός Helium

Z) DWN

Πρόκειται για ένα ασύρματο δίκτυο με χαρακτηριστικά αποκέντρωσης, έτσι ώστε να συνδέονται πολλοί κόμβοι ανθρακωρύχοι . Οι κόμβοι αυτοί συνδέονται στη βάση του πρωτοκόλλου WHIP.


HELIUM
$$$
HNT MINING
LONDON
BEXLEYHEATH
CATFORD
WIMBLEDON
200KM
RANGE
Mine
Stake
Use

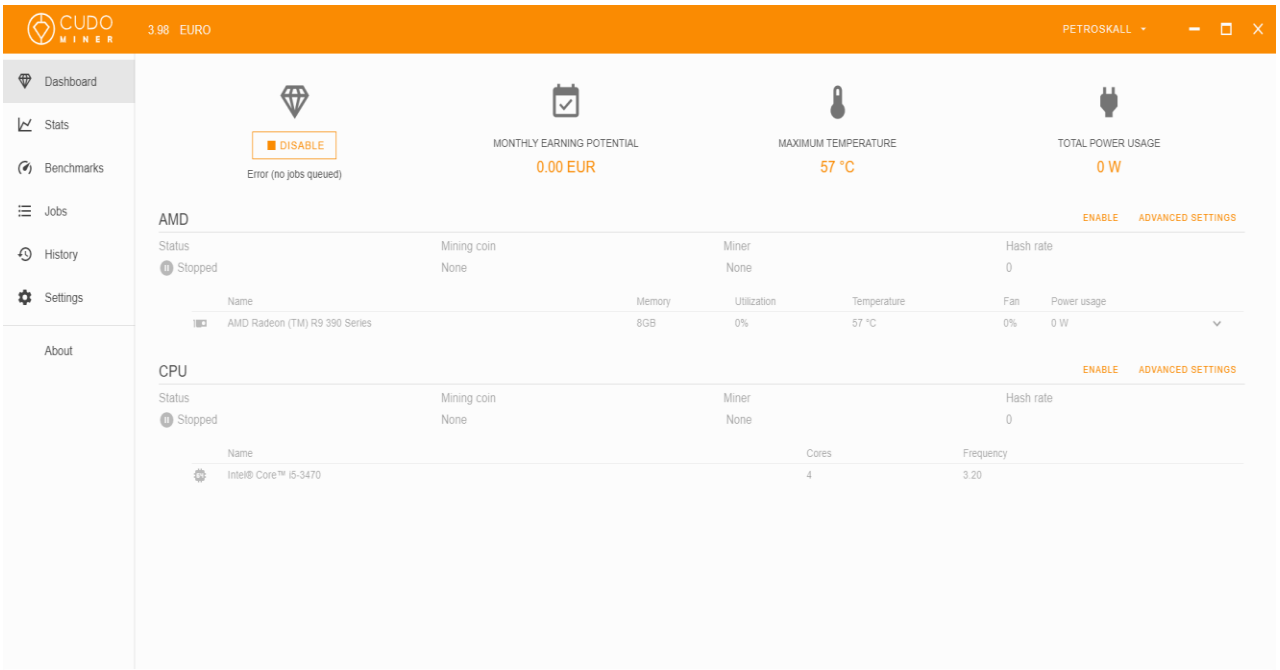
Κεφάλαιο 4. Διαφορά εξόρυξης με επεξεργαστή (cpu) , κάρτα γραφικών (gpu) και συνδυαστικά και ποιες άλλες μέθοδοι υπάρχουν.

Στο συγκεκριμένο κεφάλαιο θα χρησιμοποιήσω το πρόγραμμα εξόρυξης cudo miner για να δούμε πόση διαφορά υπάρχει μεταξύ της τεχνολογίας cpu και gpu και πόσο έχουν εξελιχθεί σε αυτό το κομμάτι οι κάρτες γραφικών με την πάροδο του χρόνου. Θα αναφερθούμε επίσης και σε άλλα λογισμικά εξόρυξης, για να δούμε τη διαδικασία που χρειάζεται να ακολουθήσει κάποιος, όταν θέλει να κάνει με ένα σχετικά απλό υπολογιστή που διαθέτει εξόρυξη CPU/GPU. Συγκεκριμένα, θα προσπαθήσουμε με χρήση ενός μέσων δυνατοτήτων υπολογιστή να χρησιμοποιήσουμε δύο διαφορετικά λογισμικά εξόρυξης. Αυτά είναι:

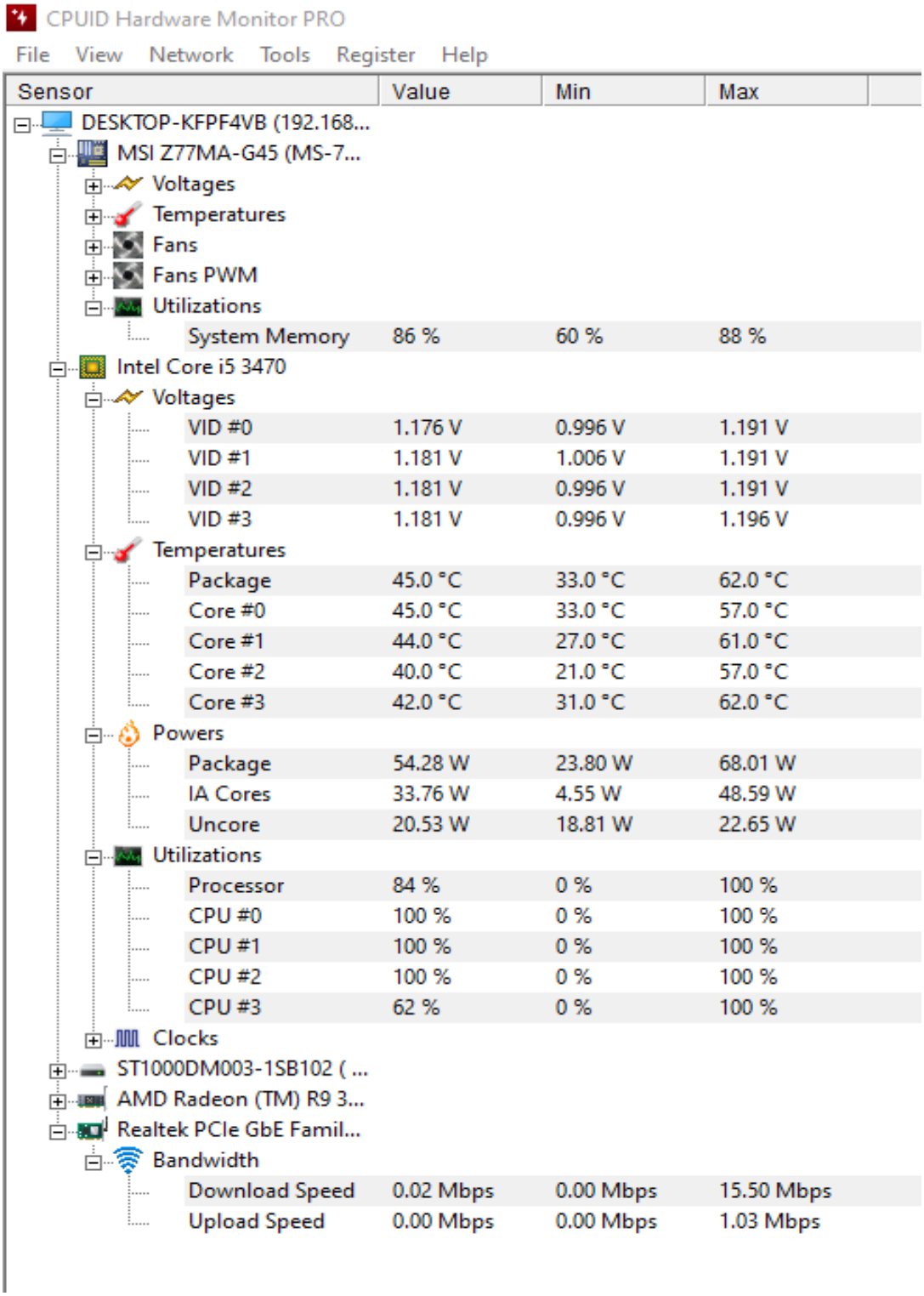
- NiceHash Miner
- BetterHash

4.1 Χρήση του προγράμματος cudo miner και παρουσίαση γραφημάτων εξόρυξης με cpu.

Παρακάτω λοιπόν βλέπουμε το πρόγραμμα στο οποίο θα λειτουργήσουμε (cudo miner) τον επεξεργαστή όπως και την κάρτα γραφικών μας. Ο επεξεργαστής ο οποίος θα χρησιμοποιήσω είναι ο i5 3470 με 4 πυρήνες και με συχνότητα στα 3.2 MHz.



Το κρυπτονόμισμα στο οποίο θα βασιστούμε και θα πάρουμε τις μετρήσεις μας είναι το **Monero** . Εφόσον λοιπόν αρχίσουμε την διαδικασία της εξόρυξης μπορούμε άμεσα να δούμε τα στοιχεία τα οποία μας ενδιαφέρουν και αυτά από τα οποία μπορούμε να διακρίνουμε εάν η συγκεκριμένη εξόρυξη μας είναι επικερδής η όχι και ποιο είναι το κέρδος/κόστος μας! Με τη χρήση του προγράμματος CPUID μπορούμε να δούμε τη κατανάλωση σε watt του επεξεργαστή μας.



Βλέπουμε λοιπόν ότι ο επεξεργαστής τρέχει σε λογική θερμοκρασία (αερόψυκτος) και η κατανάλωση σε watt είναι στα 54.28. Ξέροντας λοιπόν ότι το σημείο θερμικής σχεδίασης του συγκεκριμένου επεξεργαστή είναι στα 77watt μπορούμε να τρέξουμε το πρόγραμμα της εξόρυξης χωρίς φόβο για ζημιά στον επεξεργαστή μας.

4.2. Mining με χρήση NiceHash και BetterHash

Στο κεφάλαιο αυτό, θα παρουσιάσουμε τη διαδικασία που χρειάζεται να ακολουθήσει ένας χρήστης με ένα μέσων δυνατοτήτων υπολογιστή, αν θέλει να κάνει εξόρυξη μέσω του υπολογιστή του. Μέσα από αυτή την παρουσίαση, θα δούμε εάν είναι δυνατή η χρήση ενός τέτοιου, σχετικά απλού, υπολογιστή για CPU/GPU mining.

Πριν περάσουμε στο καθένα από τα δύο λογισμικά εξόρυξης, πρώτα παρουσιάζουμε τις προδιαγραφές του υπολογιστή που χρησιμοποιείτα.

- Επεξεργαστής: AMD A8-7410 APU με AMD Radeon R5 Graphics, ταχύτητα 2.20 GHz
- RAM: 6 GB

Α) Χρήση NiceHash

Το NiceHash είναι ένα από τα γνωστότερα και πιο δημοφιλή σήμερα λογισμικά mining. Θεωρείται το κορυφαίο λογισμικό για ανταλλαγές κρυπτονομισμάτων. Στη συνέχεια, εκτελούμε τα παρακάτω βήματα με τη βοήθεια του NiceHash, ένα προς ένα:

- Εγγραφή (sign-up) στον ιστόχωρο του Nice Hash
- Κατέβασμα και είσοδος (log-in) στον NiceHash Miner
- Αντιγραφή-επικόλληση της εσωτερικής διεύθυνσης πορτοφολιού κρυπτονομισμάτων

- Έναρξη του benchmarking των κόμβων miners (CPU/GPU)
- Τελικά: έναρξη του mining

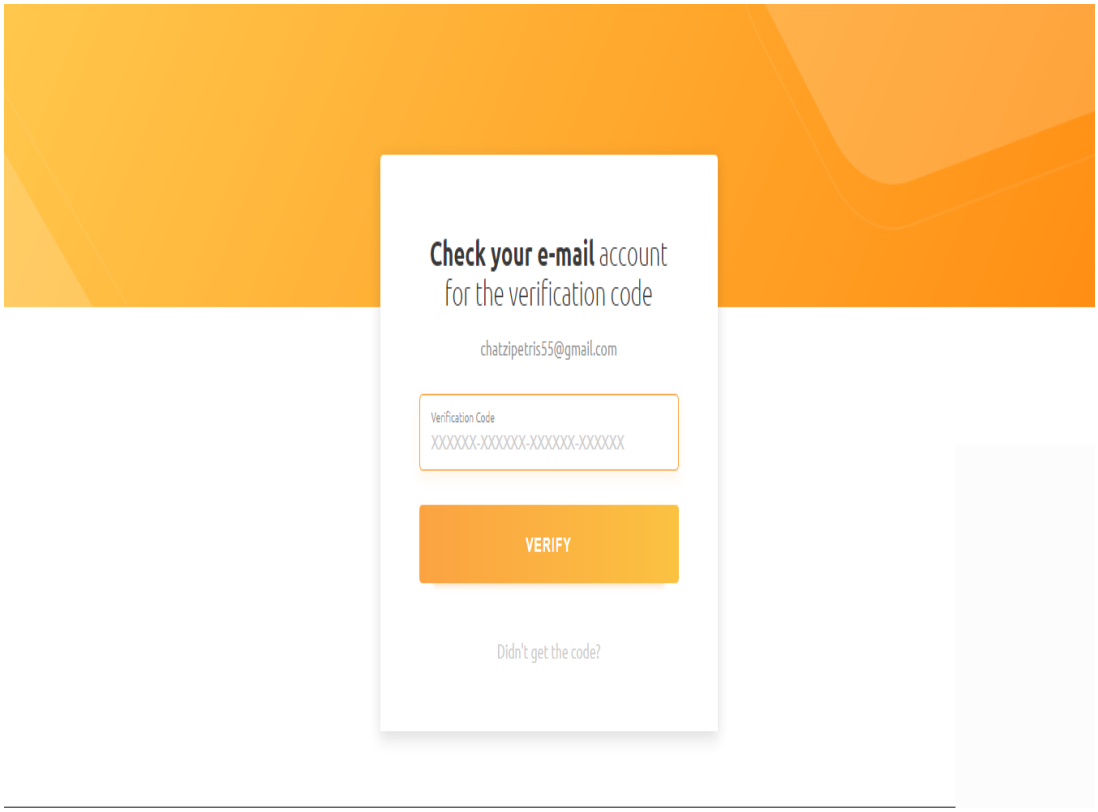


Figure 38. Επαλήθευση χρήστη του NiceHash Miner

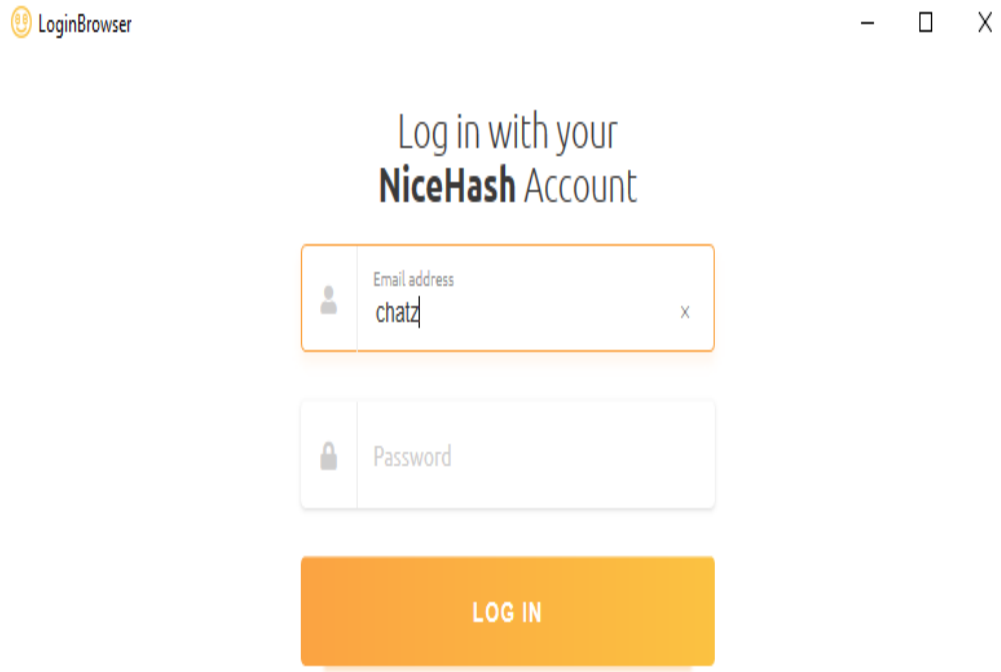


Figure 39. Είσοδος στο NiceHash Miner

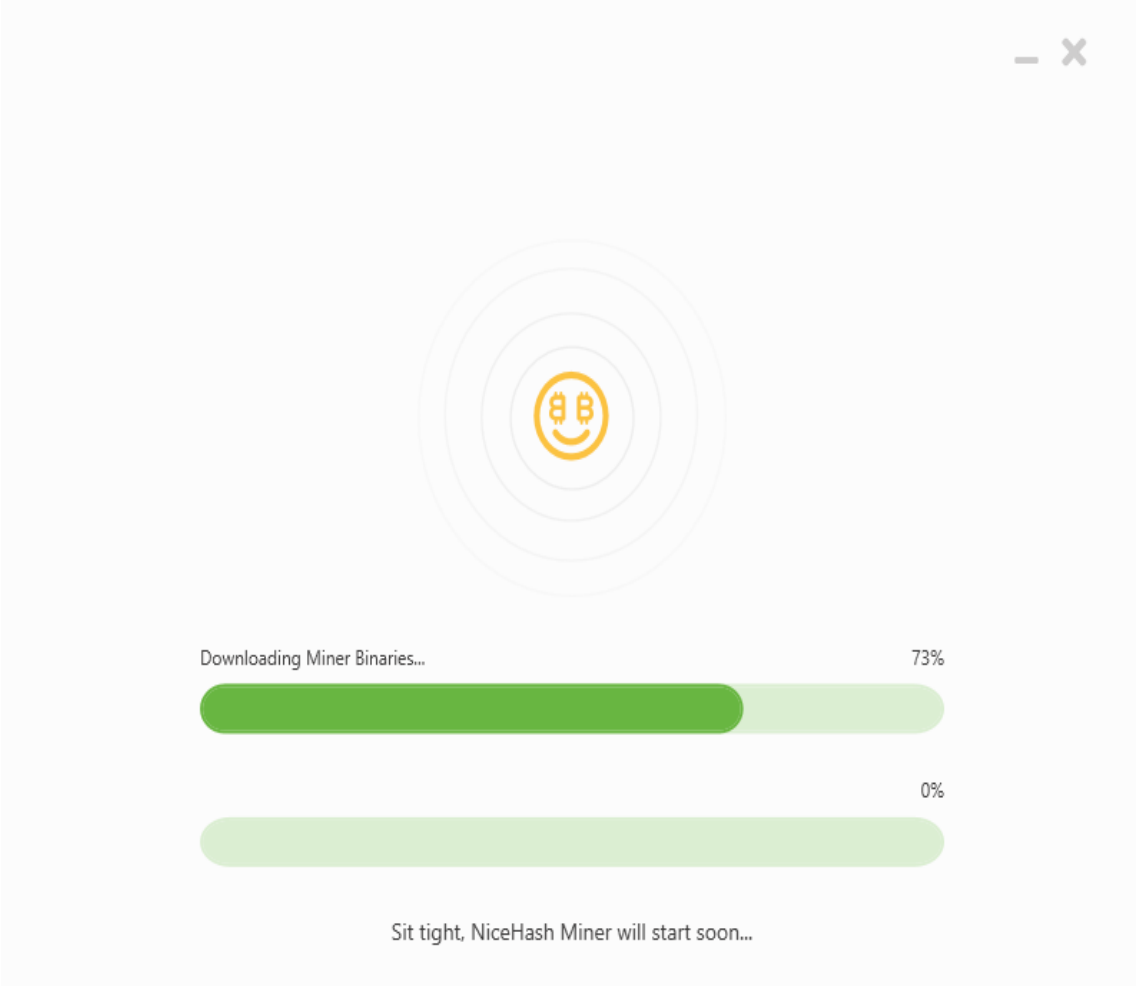


Figure 40. Έναρξη λειτουργίας NiceHash Miner

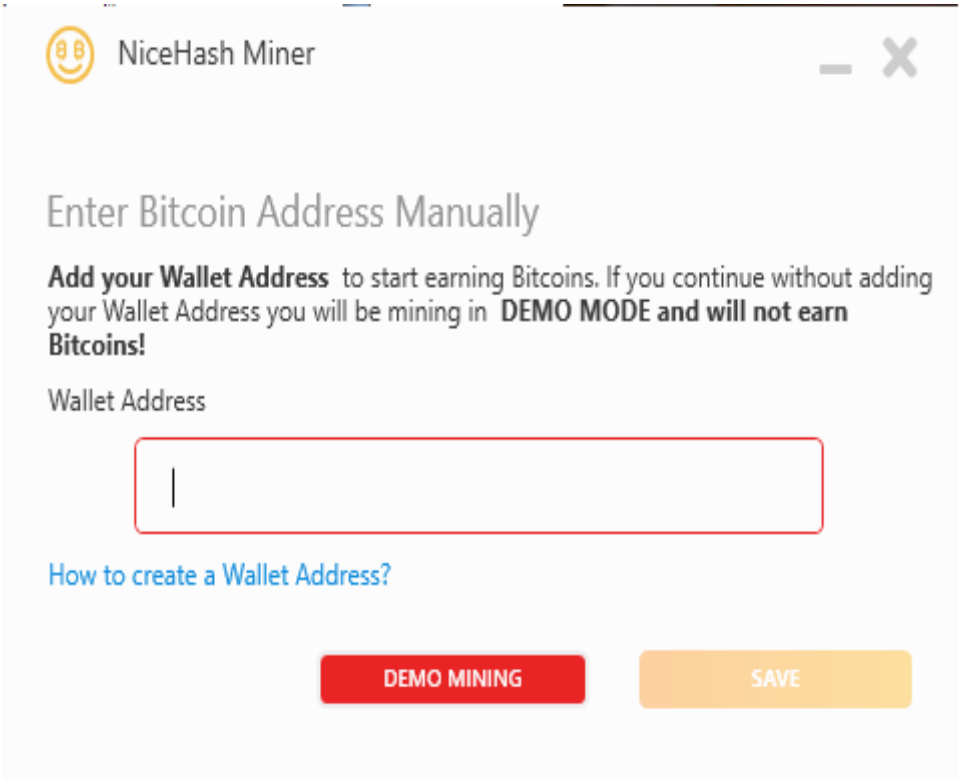


Figure 41. Εισαγωγή εσωτερικής διεύθυνσης Wallet κρυπτονομισμάτων

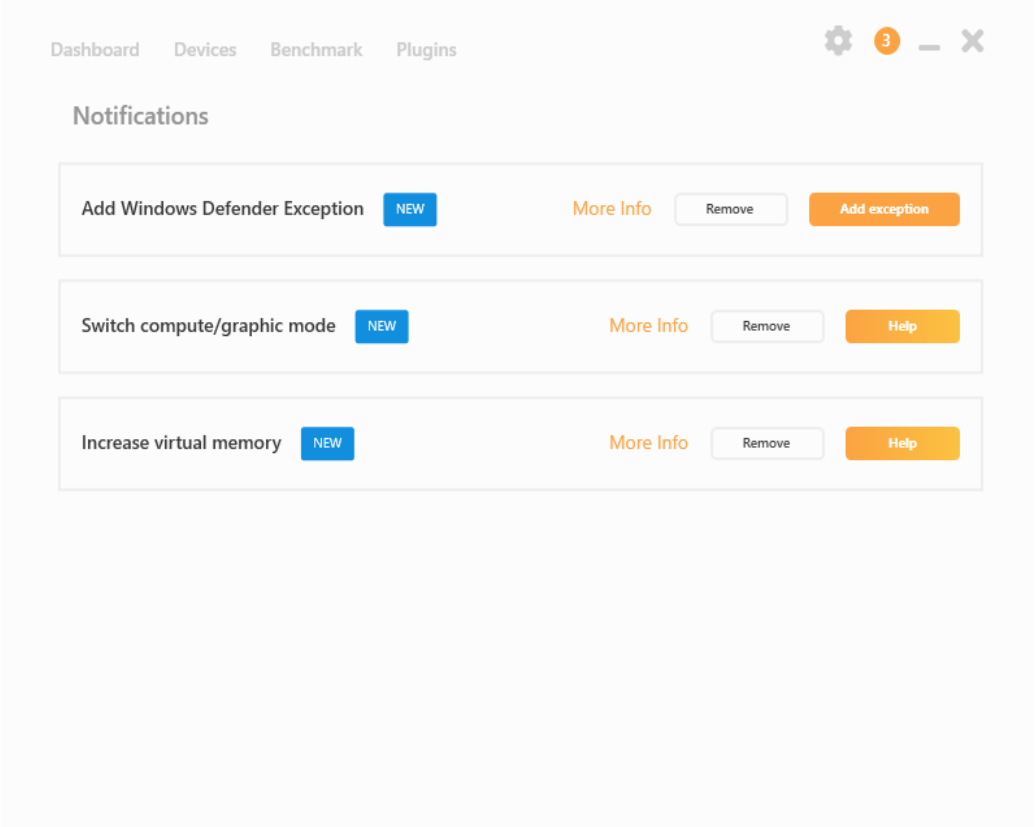


Figure 42. Tab ειδοποιήσεων NiceHash

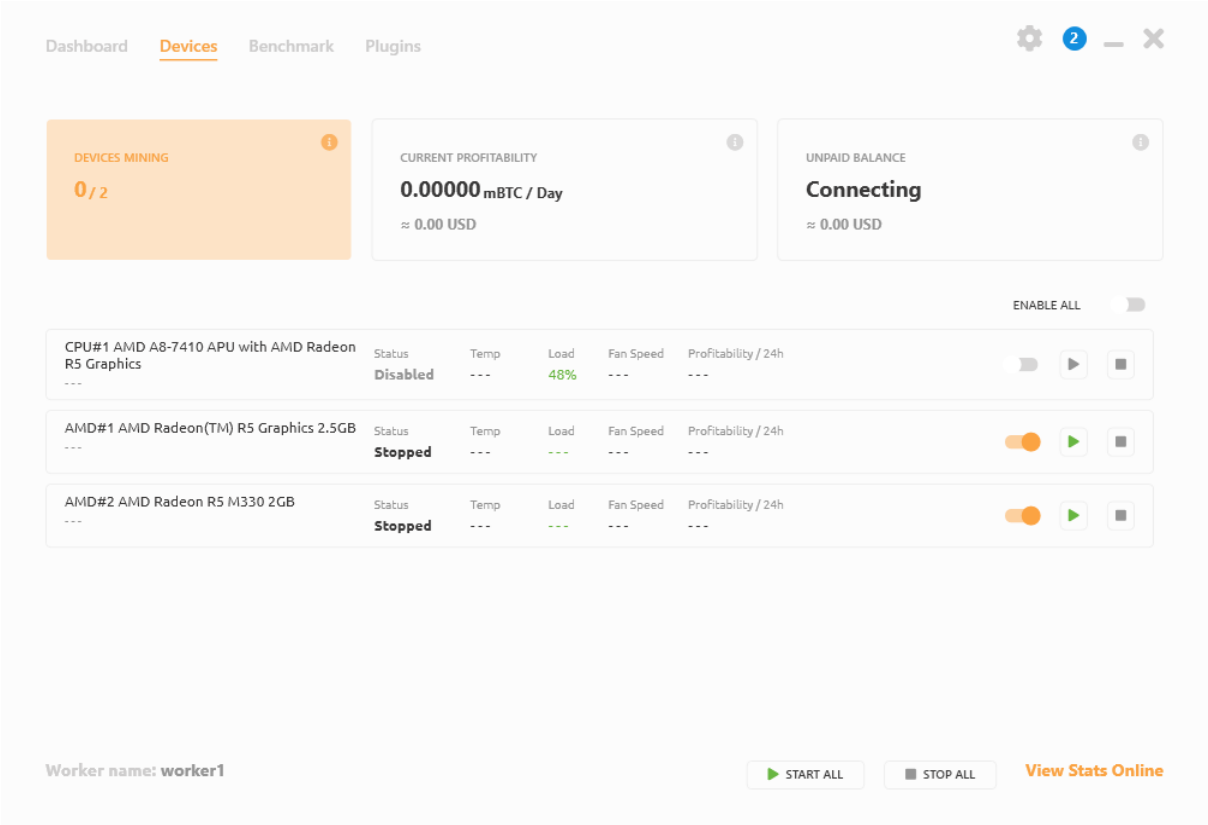


Figure 43. Συσκευές εξόρυξης CPU/GPU mining

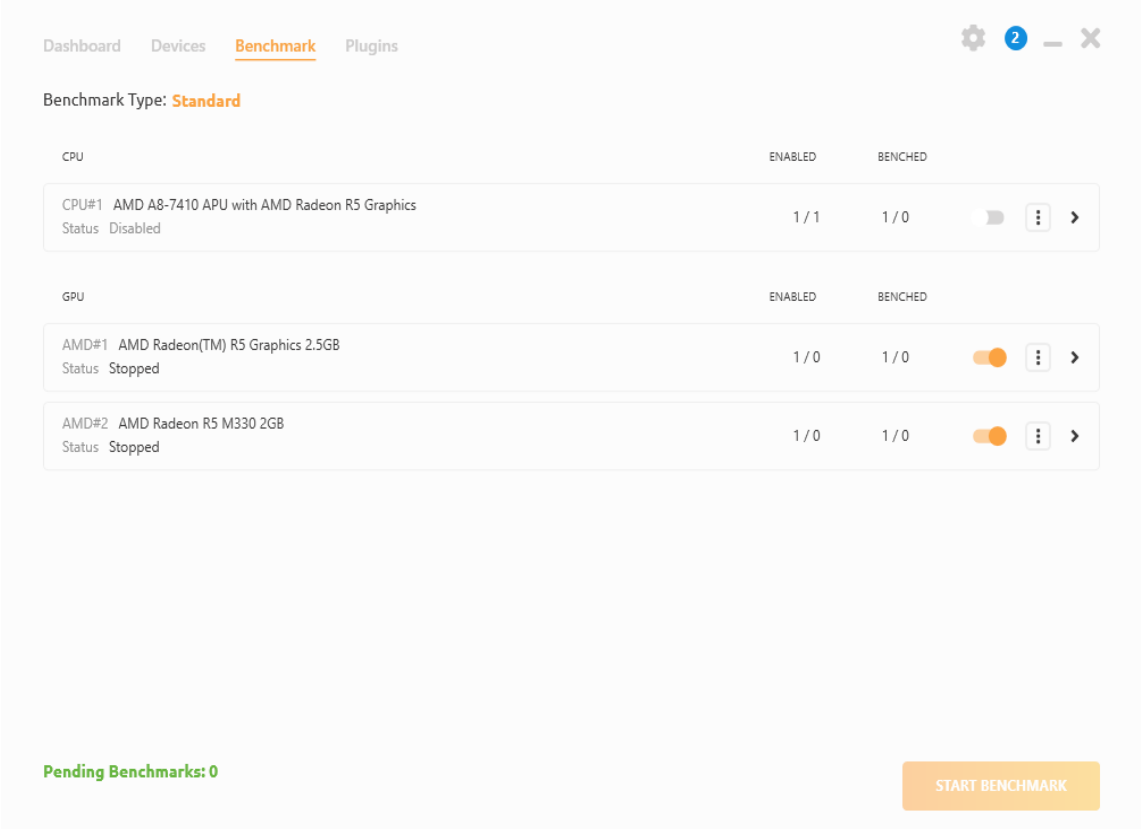


Figure 44. Benchmarking NiceHash Miner

Σε όλα τα παραπάνω στιγμιότυπα (screenshots), βλέπουμε τη διαδικασία του set-up του NiceHash Miner για την εξόρυξη. Παρ' ότι όλα τα βήματα έχουν γίνει ορθά, όπως μπορούμε να διακρίνουμε και στα τελευταία screenshots, η έναρξη του mining κολλάει στο benchmarking, δηλαδή τη σύγκριση των προδιαγραφών των 3 μονάδων CPU/GPU του υπολογιστή με κάποια πρότυπα. Συγκεκριμένα, ο NiceHash Miner απαιτεί μεγαλύτερη VRAM ώστε να τρέξει κανονικά. Διαπιστώνουμε άρα εδώ ότι ο απλός χρήστης μπορεί να αποκλείεται λόγω των μεγαλύτερων προδιαγραφών που ορίζονται ως benchmarks ή επειδή δεν υποστηρίζεται η GPU/CPU που έχει. Όμως, υπάρχουν και γνωστοί miners που υποστηρίζουν και πιο προσιτές στο μέσο χρήστη επιλογές. Μια τέτοια περίπτωση είναι ο miner **BetterHash**.

Β) Χρήση BetterHash

Ο BetterHash είναι ένα λογισμικό εξόρυξης το οποίο δεν είναι τόσο δημοφιλές όσο το NiceHash αλλά σταδιακά έχει κερδίσει έδαφος και είναι αρκετά φιλικό προς το

χρήστη που δεν είναι ειδικός στην πληροφορική και εύχρηστο. Τα βήματα που έχουμε ακολουθήσει εδώ, όπως φαίνονται στα screenshots παρακάτω, είναι τα εξής:

- Κατέβασμα/εκτέλεση BetterHash
- Benchmarking συσκευής CPU/GPU #1
- Benchmarking συσκευής CPU/GPU #2
- Benchmarking συσκευής CPU/GPU #3
- Επιλογή αλγορίθμων εξόρυξης
- Ξεκίνημα mining
- Απεικόνιση πρώτων κερδών (σε Monero)

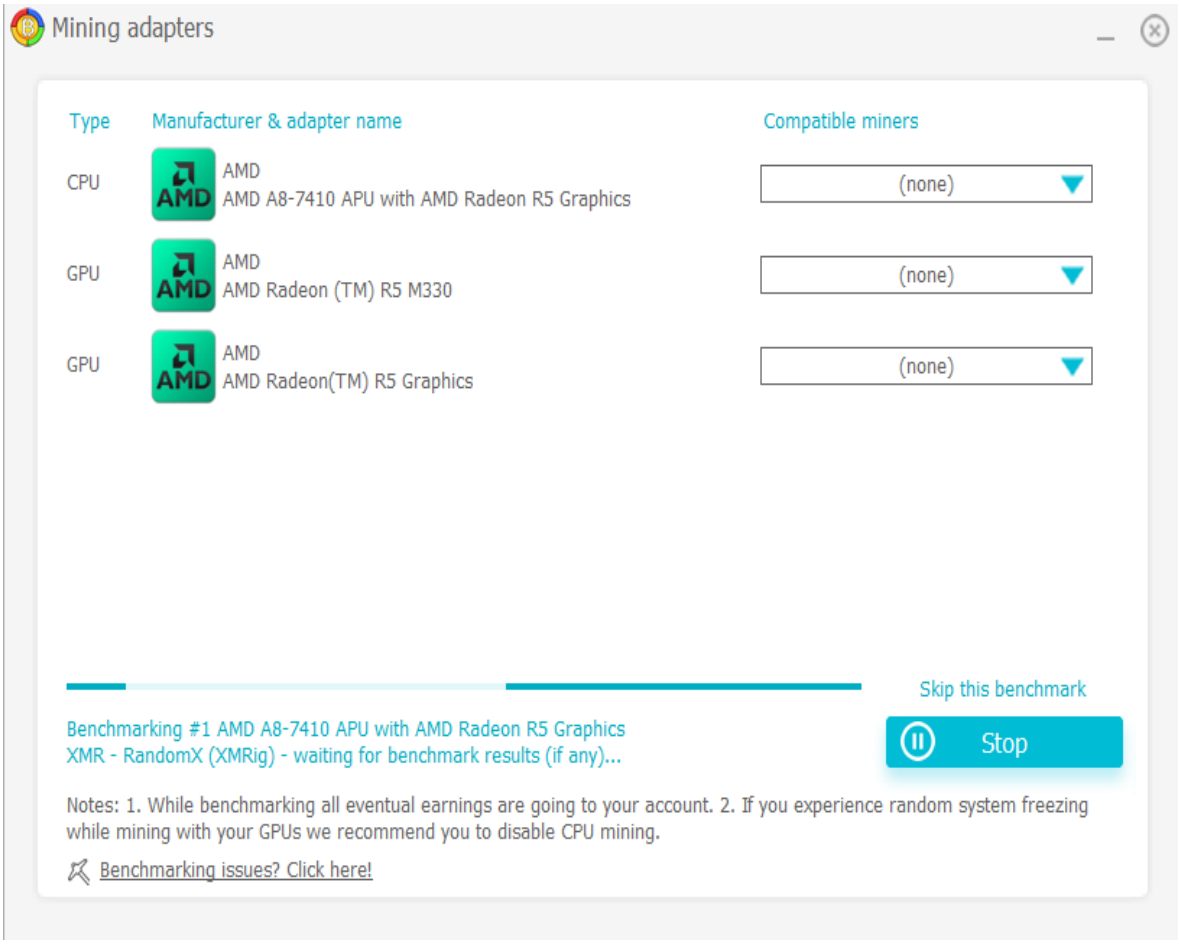


Figure 45. Better Hash: Benchmarking συσκευής 1

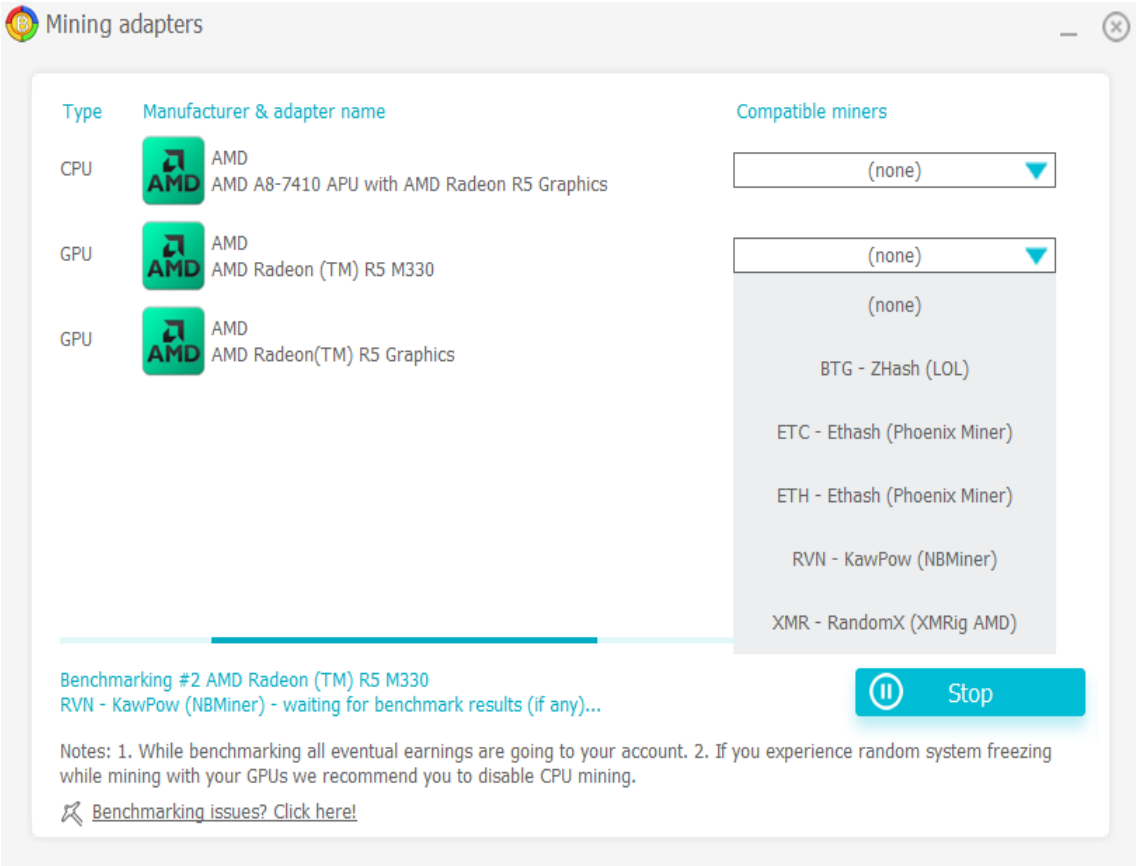


Figure 46. Benchmarking BetterHash: Συσκευή 2

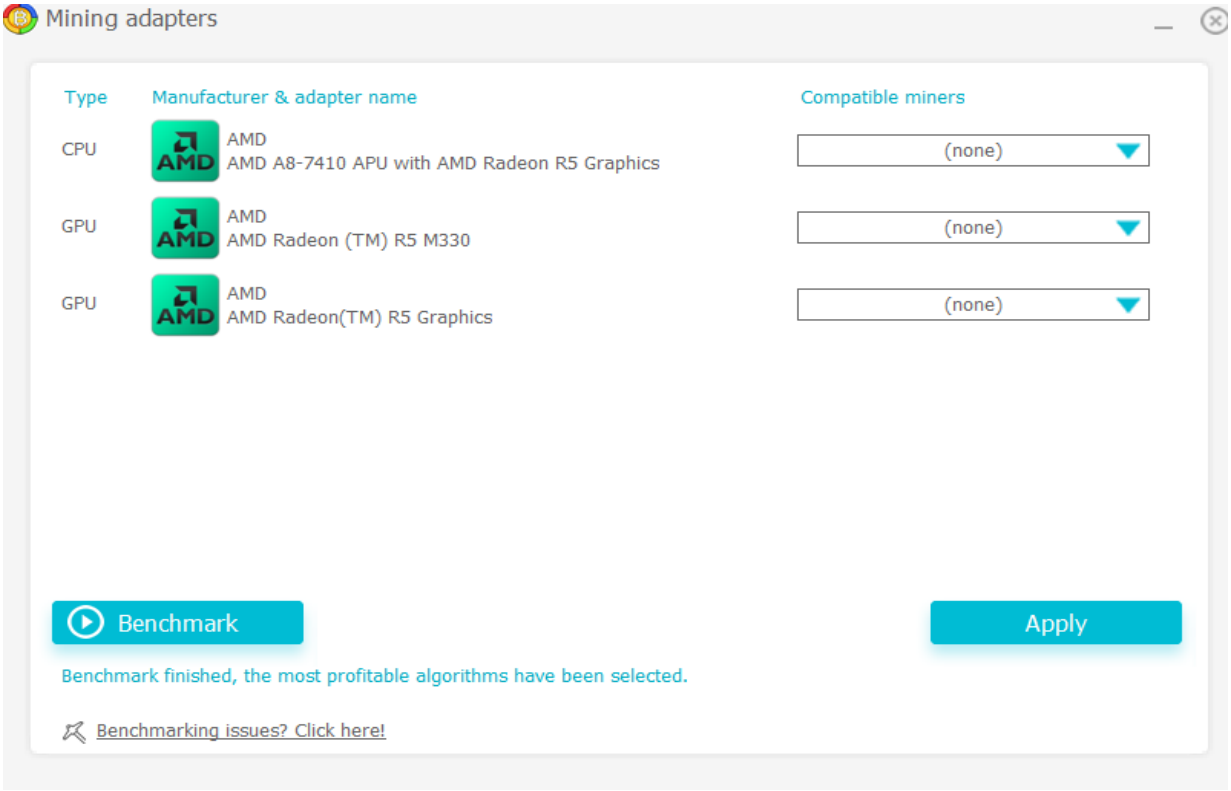


Figure 47. Benchmarking BetterHash: Συσκευή 3

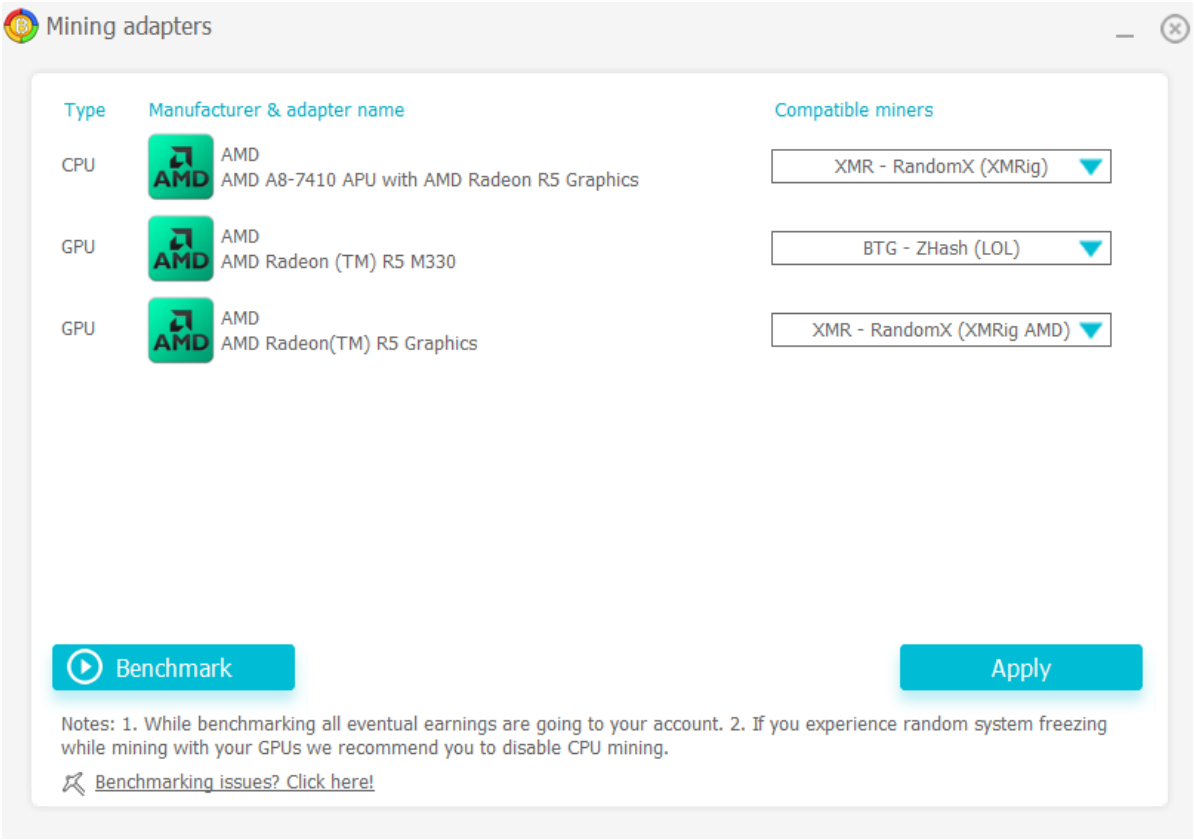


Figure 48. Επιλογή αλγορίθμων εξόρυξης

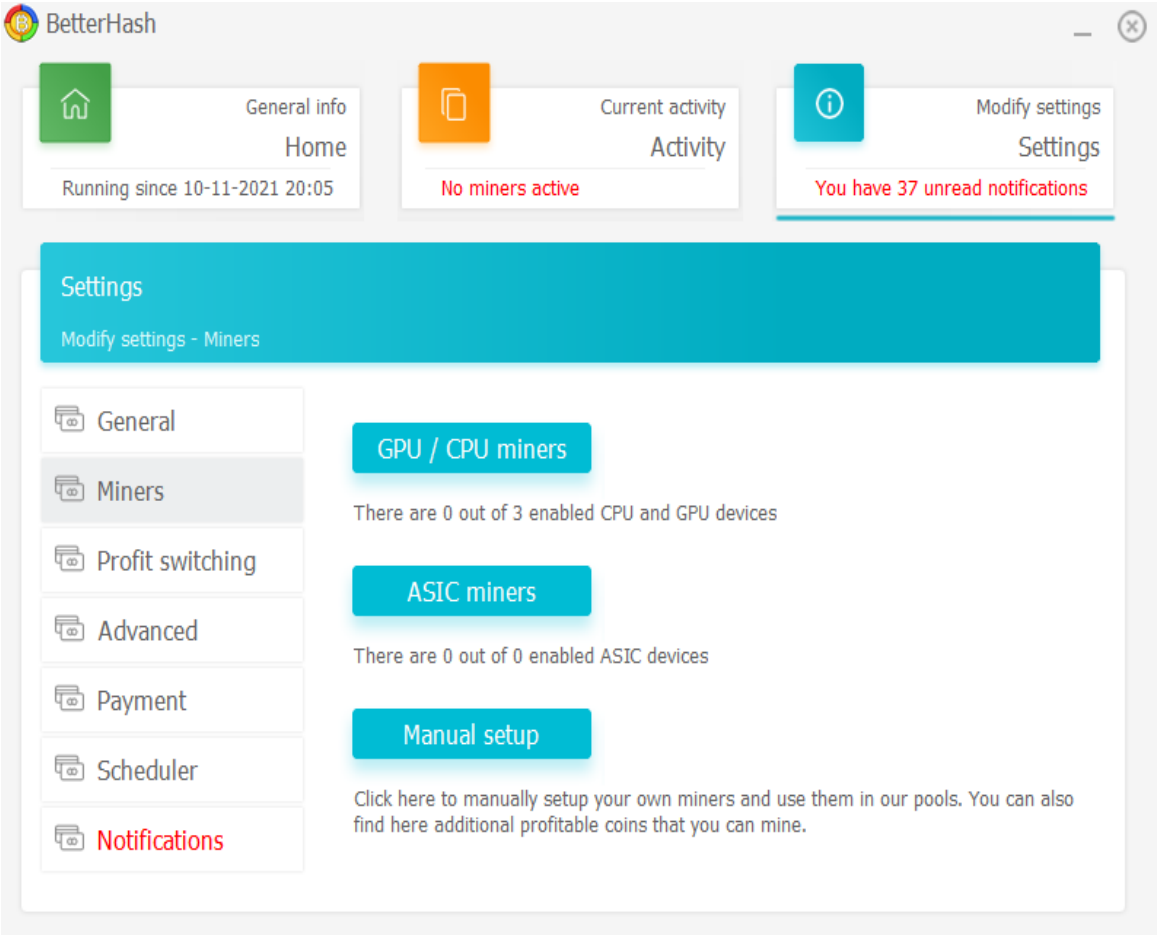


Figure 49. Miners του υπολογιστή: Επιλογή αλγορίθμου

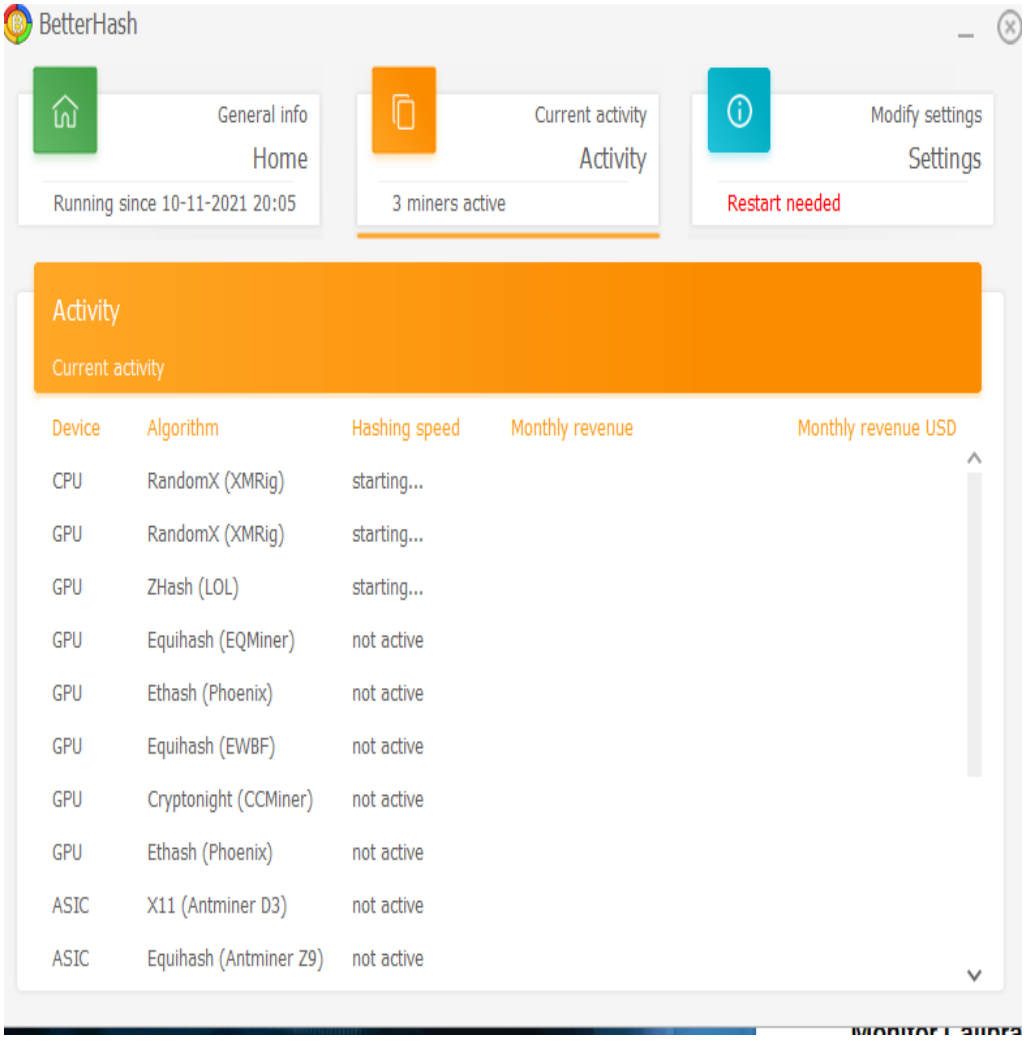


Figure 50. Δραστηριότητα αλγορίθμων εξόρυξης

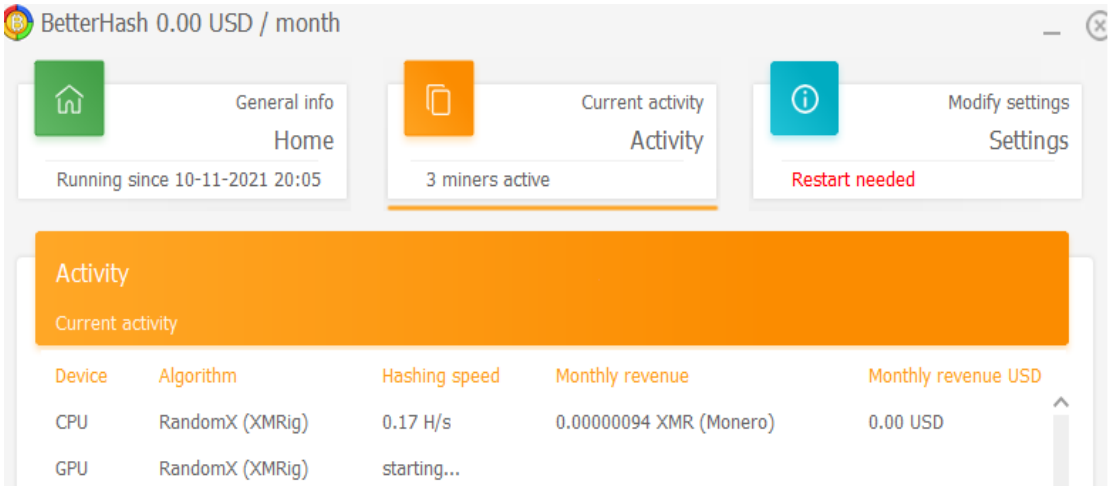


Figure 51. Έναρξη δραστηριότητας αλγόριθμου XMRig

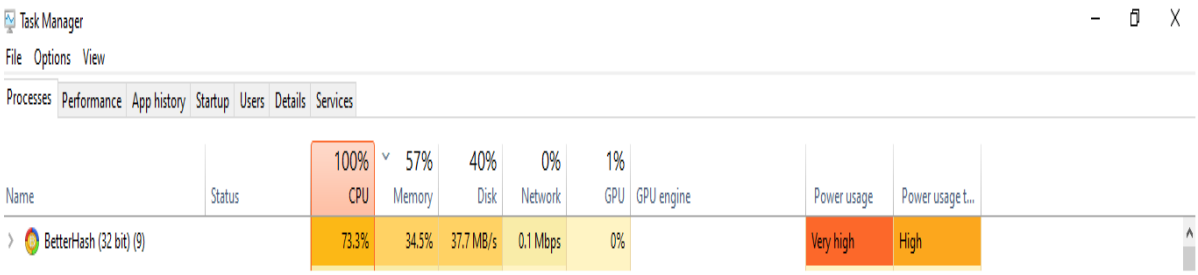


Figure 52. Κατανάλωση πόρων υπολογιστή από το mining

Αφού είδαμε όλη την παραπάνω διαδικασία μέσα από εικόνες, μπορούμε να πούμε ότι όντως μέσα από το BetterHash μπορεί και ένας χρήστης μέσα από τον υπολογιστή του να κάνει mining και να έχει και κάποιο κέρδος. Αυτό το κέρδος, ανάλογα με τον αλγόριθμο, μπορεί να είναι από .00006173 XMR ή 0.00000025 BTC μέχρι 0.00001814 BTC και αντιστοιχεί σε hash rates από 1.36 ως 10.01 H/s.

Αυτά τα ποσά, αν τα μεταφράσουμε σε μηνιαίο εισόδημα, είναι πολύ μικρά, δηλαδή 0.02 ως 1.17 δολάρια[12]. Με δεδομένο ότι και η κατανάλωση πόρων του υπολογιστή αλλά και η χρήση ηλεκτρικού είναι πολύ υψηλή (εικ. 52), είναι βέβαιο ότι σε επίπεδο οικονομικό ένας μέσος υπολογιστής δε μπορεί να αποφέρει κέρδη στο χρήστη του.

[12] https://www.betterhash.net/AMD-Radeon-(TM)-R5-M330-mining-profitability-14663230.html

5.Τελικά συμπεράσματα

Στην εργασία αυτή, ξεκινήσαμε να πραγματευόμαστε θεωρητικές έννοιες σχετικά με τα κρυπτονομίσματα που είναι βασικές για να κατανοήσει κανείς πιο σύνθετες έννοιες αλλά και τις πρακτικές εφαρμογές.

Ιδιαίτερη έμφαση δώσαμε στα θέματα που αφορούν τις γλώσσες προγραμματισμού που χρησιμοποιούνται στα κρυπτονομίσματα και στις εφαρμογές τους (Java, Python κ.ά.) αλλά και στα είδη hardware που μπορεί να συναντήσουμε στα κρυπτονομίσματα και μάλιστα την εξόρυξή τους. Εκεί δόθηκε έμφαση στα ASIC, CPU/GPU, Helium miner, FPGA.

Όλα αυτά είχαν ως σκοπό την καλύτερη κατανόηση των εννοιών που υπάρχουν πίσω από τις πρακτικές εφαρμογές των κρυπτονομισμάτων στον σύγχρονο κόσμο. Το τελευταίο κεφάλαιο ήταν μια πρακτική εφαρμογή όσων είχαν ειπωθεί προηγούμενα και ιδιαίτερα στο κεφάλαιο 3. Εκεί έγιναν δύο μελέτες περίπτωσης. Είχαμε δύο υπολογιστές, με τον πρώτο να διαθέτει ανώτερες προδιαγραφές και έγινε προσπάθεια εξόρυξης με τα λογισμικά Cudo Miner από τη μία και NiceHash και BetterHash από την άλλη. Είδαμε έτσι ότι στην περίπτωση ενός υποδεέστερου και πιο «μέσου» υπολογιστή, υπάρχουν βέβαια λογισμικά που θα υποστηρίξουν την εξόρυξη του και μπορούν οριακά να αποφέρουν και κάποια έσοδα. Όμως, τα έσοδα αυτά αναμένεται να καταναλωθούν από την αυξημένη ανάγκη πόρων που έχει το mining, ακόμα και με τους καταλληλότερους για την περίπτωση αλγόριθμους.

Στην πρώτη περίπτωση, με τον υψηλότερων προδιαγραφών υπολογιστή, βλέπουμε πως υπάρχει η δυνατότητα για κάποια έσοδα, ενώ παράλληλα η κατανάλωση πόρων είναι μειωμένη.

Τα παραπάνω σίγουρα εξηγούν το λόγο που το CPU/GPU mining εγκαταλείφθηκε σύντομα και επίσης γιατί συνήθως αυτοί που ασοχλούνται συστηματικά με το mining κάνουν πρώτα κάποια επένδυση σε σειρά από GPUs που τοποθετούν σειριακά, με σκοπό τη μεγιστοποίηση της απόδοσης.

Είναι βέβαιο πως το θέμα του mining θα απασχολήσει αρκετά την έρευνα και στο μέλλον, αφού τα κρυπτονομίσματα, μετά από κάποιο διάστημα που ήταν στην αφάνεια, έχουν βγει δυναμικά στο προσκήνιο και έχουν απασχολήσει και διάφορες κοινωνικές τάξεις, που δεν ενδιαφέρονται για τα επιστημονικά ή άλλα στοιχεία που μπορεί να έχουν ως ψηφιακά-ηλεκτρονικά νομίσματα αλλά που τα βλέπουν ως μια

ακόμη από τις επενδύσεις που μπορούν να κάνουν. Παράλληλα, τα κρυπτονομίσματα και οι διαδικασίες εξόρυξής τους έχουν και στοιχεία που απασχολούν τους ειδικούς της πληροφορικής και που εξελίσσονται ολοένα.

Πηγές

Betterhash.net. n.d. *Mining with AMD Radeon (TM) R5 M330 - BetterHash Calculator*. [online] Available at: <https://www.betterhash.net/AMD-Radeon-(TM)-R5-M330-mining-profitability-14663230.html> [Accessed 11 November 2021].

Blockchains, 1., n.d. *Blockchain Size: Everything You Need To Know*. [online] 101 Blockchains. Available at: <https://101blockchains.com/blockchain-size/#prettyPhoto> [Accessed 26 October 2021].

Coinspaid.com. n.d. *What is a crypto wallet | CoinsPaid*. [online] Available at: <https://coinspaid.com/what-is-a-crypto-wallet> [Accessed 23 October 2021].

Coinspaid.com. n.d. *What is a crypto wallet | CoinsPaid*. [online] Available at: <https://coinspaid.com/what-is-a-crypto-wallet> [Accessed 23 October 2021].

Esengulov, i., 2020. *Bitcoin Explained in Simple Terms*.

Ghimire, S., 2019. *Analysis of Bitcoin Cryptocurrency and Its Mining Techniques* (Doctoral dissertation, University of Nevada, Las Vegas).

Härdle, W., Harvey, C. and Reule, R., 2019. Understanding Cryptocurrencies. *SSRN Electronic Journal*.

Hyatt, J., 2021. *Decoding Crypto: The 10 Most Popular Cryptocurrencies*. [online] Nasdaq. Available at: <https://www.nasdaq.com/articles/decoding-crypto%3A-the-10-most-popular-cryptocurrencies-2021-08-05> [Accessed 26 October 2021].

McCarthy, N., 2018. *1.7 Billion Adults Worldwide Do Not Have Access To A Bank Account [Infographic]*. [online] Forbes. Available at: <https://www.forbes.com/sites/niallmccarthy/2018/06/08/1-7-billion-adults-worldwide-do-not-have-access-to-a-bank-account-infographic/> [Accessed 21 October 2021].

Medium. 2018. *Best Programming Languages for Cryptocurrency*. [online] Available at: <https://medium.com/@4kcode/best-programming-languages-for-cryptocurrency-8be71327987c> [Accessed 25 October 2021].

Premier, E., 2018. *Understanding what cryptocurrency wallet is and how it works | Hacker Noon*. [online] Hackernoon.com. Available at:

<https://hackernoon.com/understanding-what-cryptocurrency-wallet-is-and-how-it-works-d68499480b48> [Accessed 23 October 2021].
Sutardja Center for Entrepreneurship & Technology Technical Report, 2015. BlockChain Technology: Beyond Bitcoin.