Πανεπιστήμιο Κρήτης
Τμήμα Επιστήμης Υπολογιστών

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

«Διατύπωση επερωτήσεων σε ανοικτά σύνολα δεδομένων κρυπτονομισμάτων»

Χαρίδημος Μαυροτσουπάκης

ΑΜ: 3289

Επιβλέπων: καθ. Δημήτρης Πλεξουσάκης

Συνεπιβλέπων: Νίκος Τσατσάκης

Εισαγωγή

Στη σύγχρονη εποχή, οι ηλεκτρονικές αγορές έχουν γίνει ρουτίνα. Για την πραγματοποίησή τους θα πρέπει τα χρήματα να βρίσκονται σε ψηφιακή μορφή, η οποία υποστηριζόταν αποκλειστικά από κατάλληλες τραπεζικές υπηρεσίες μέχρι το 2009, οπότε και εμφανίστηκαν και άρχισαν να χρησιμοποιούνται και κρυπτονομίσματα. Τα κρυπτονομίσματα έχουν ψηφιακή υπόσταση και συγκεντρώνουν ένα πλήθος από πλεονεκτήματα, όπως η αμεσότητα των συναλλαγών, η ασφάλεια, η ταχύτητα, το μειωμένο κόστος (καθώς παρακάμπτονται οι ενδιάμεσοι φορείς -τράπεζες, κυβερνήσεις- που εμπλέκονται διαφορετικά) και η δυσκολία στην παραποίησή τους, αφού βασίζονται σε μια αποκεντρωμένη δομή αντίθετα από τη λειτουργία των τραπεζών. Είναι ένα νέο ψηφιακό προϊόν, του οποίου οι δυνατότητες και οι περιορισμοί δεν έχουν ερευνηθεί πλήρως.

Με τον καιρό έχουμε αύξηση της διαφάνειας στα δεδομένα των κρυπτονομισμάτων, γεγονός που επιτρέπει σε ολοένα και μεγαλύτερο πλήθος καταναλωτών να τα χρησιμοποιεί.

Στο πλαίσιο αυτό, δεδομένα του Bitcoin, όπως και άλλων κρυπτονομισμάτων, είναι διαθέσιμα για εξερεύνηση και ανάλυση στην πλατφόρμα BigQuery. Όλα τα ιστορικά δεδομένα βρίσκονται στο σύνολο δεδομένων bigquery-public-data, το οποίο ενημερώνεται κάθε 10 λεπτά. Το BigQuery με τη σειρά του έχει συλλέξει δεδομένα από 65 αποθετήρια https://github.com/blockchain-etl (BlockchainETL, 2020) στα οποία μπορούμε επιπλέον να έχουμε πρόσβαση και να εφαρμόσουμε τεχνικές μηχανικής μάθησης για την ανάλυσή τους μέσα από την πλατφόρμα Kaggle (Will, 2018).

Σκοπό της εργασίας αποτελεί η μελέτη και παρουσίαση ποιοτικών και ποσοτικών χαρακτηριστικών σχετικών με τα κρυπτονομίσματα εν γένει και το Bitcoin ειδικότερα. Αναφορικά με το Bitcoin θα περιηγηθούμε και θα αναλύσουμε δεδομένα που διατηρούνται στο BigQuery. Από τα πολλά public datasets που περιέχει, θα ασχοληθούμε με αυτό του crypto_bitcoin και τα γνωρίσματά του. Τέλος, αφού αναλυθούν και διατυπωθούν ενδιαφέροντα ερωτήματα (queries) πάνω στο crypto_bitcoin dataset, ορισμένα αποτελέσματα θα οπτικοποιηθούν και από αυτήν τη διαδικασία θα εξαχθούν χρήσιμα στατιστικά στοιχεία για το Bitcoin.

Περιεχόμενα

1 Κρυπτονόμισμα: ορισμοί, τεχνολογίες, χρήση, είδη και ιστορία

1. Βασικοί ορισμοί

1.1.1 Εικονικό νόμισμα

Τα εικονικά νομίσματα ή αλλιώς κρυπτονομίσματα έχουν ψηφιακή υπόσταση και χρησιμοποιούν την κρυπτογραφία για την ασφάλεια της διακίνησής τους. Χρησιμοποιούνται κυρίως για την αγορά και πώληση αγαθών και υπηρεσιών. Δεν έχουν καμία εγγενή αξία**,** καθώς δεν μπορούν να έχουν ισοτιμία με ένα άλλο νομισματικό προϊόν, όπως ο χρυσός και, σε αντίθεση με το παραδοσιακό νόμισμα, δεν εκδίδονται από μια κεντρική αρχή.

Ακολουθούν τα τρία κυριότερα πλεονεκτήματά τους:

Ψευδωνυμία (δυνατότητα ανωνυμίας)

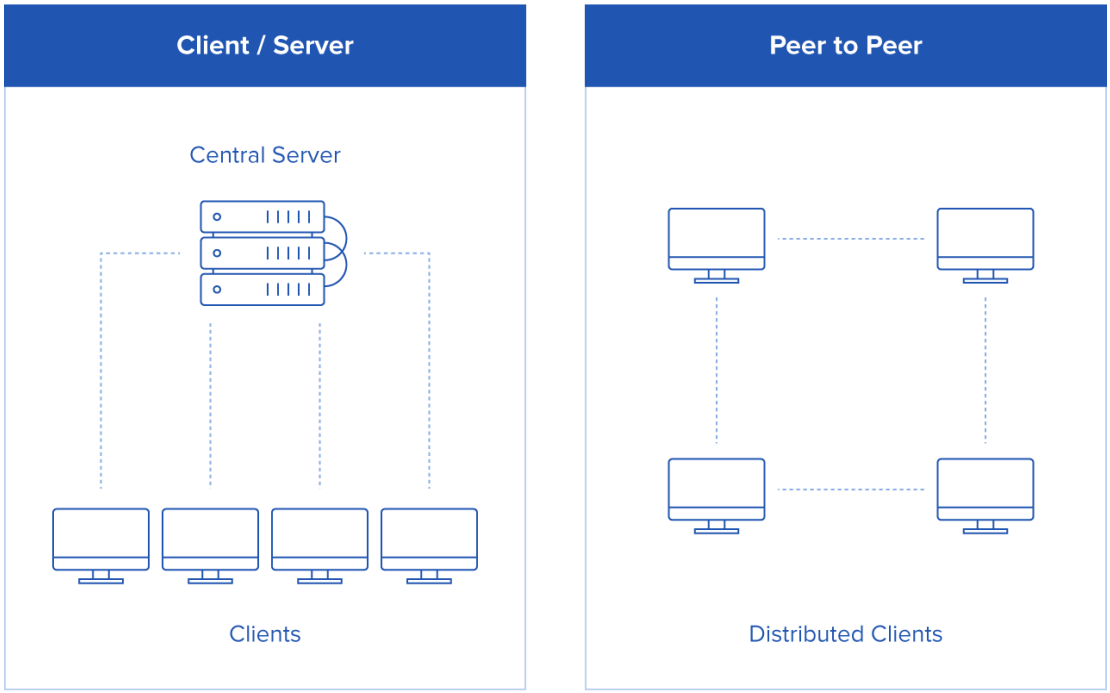
Η αγορά αγαθών και υπηρεσιών με κρυπτονομίσματα πραγματοποιείται με σύνδεση στο διαδίκτυο και δεν απαιτεί γνωστοποίηση ταυτότητας. Παρόλα αυτά, για την επίτευξη μιας συναλλαγής, θα πρέπει να υπάρχει κάποιο αναγνωριστικό-ψευδώνυμο και από τις δύο πλευρές (παραλήπτης-αποστολέας). Επομένως, οι συναλλαγές, οι οποίες είναι σχεδόν ανώνυμες, χαρακτηρίζονται από ψευδωνυμία. Επιτρέπουν έτσι στους καταναλωτές να ολοκληρώνουν τις αγορές, χωρίς να αποκαλύπτουν προσωπικές πληροφορίες στους εμπόρους ή σε τράπεζες.

Ομότιμη (Peer-To-Peer) αγορά (Wikipedia, 2020)

Ένα από τα μεγαλύτερα πλεονεκτήματα των κρυπτονομισμάτων είναι ότι δεν υπάρχουν μεσάζοντες. Για τους προμηθευτές, η έλλειψη μεσάζοντα μειώνει το κόστος συναλλαγής, ενώ για τους καταναλωτές υπάρχει ένα τεράστιο πλεονέκτημα σε περίπτωση που το χρηματοπιστωτικό σύστημα υποστεί κυβερνοεπίθεση (hack) ή αν ο χρήστης δεν εμπιστεύεται το παραδοσιακό σύστημα.

Για παράδειγμα, εάν η βάση δεδομένων μιας τράπεζας ήταν «πειραγμένη» ή κατεστραμμένη, η τράπεζα θα ήταν εντελώς εξαρτημένη από τα αντίγραφα ασφαλείας της για να αποκαταστήσει τυχόν ελλείπουσες πληροφορίες. Με τα κρυπτονομίσματα, ακόμη και αν ένα τμήμα βρίσκεται σε κίνδυνο από κακόβουλες παρεμβολές, τα υπόλοιπα τμήματα θα συνεχίσουν να είναι σε θέση να επιβεβαιώσουν τις συναλλαγές.

Figure 1: Cryptocurrencies Eliminate Financial Intermediaries



Source: Bitsonblocks.net

toptal

Ταχύτητα στις συναλλαγές

Η διαδικασία μεταφοράς χρημάτων, σε αντίθεση με τις συμβατικές μεθόδους μεταφορών, που απαιτούν κάποιο χρονικό διάστημα για να ολοκληρωθούν, γίνεται με μεγάλη ταχύτητα σε μερικά δευτερόλεπτα.

Τα εικονικά χρήματα μπορούν να είναι ή συγκεντρωμένα, εκεί όπου υπάρχει ένα κεντρικό σημείο ελέγχου που αφορά την προσφορά χρήματος (τραπεζικό σύστημα), ή αποκεντρωμένα, εκεί όπου ο έλεγχος στην προσφορά χρήματος μπορεί να προέλθει από διάφορες πηγές. Κάθε κρυπτονόμισμα ανήκει στη δεύτερη κατηγορία.

1.1.2 Κρυπτογραφία

Η λέξη κρυπτογραφία (αγγλ.: cryptography) προέρχεται από τα συνθετικά «κρυπτός» + «γράφω» και είναι ένα διεπιστημονικό γνωστικό πεδίο που ασχολείται με τη μελέτη, την ανάπτυξη και τη χρήση τεχνικών κρυπτογράφησης και αποκρυπτογράφησης με σκοπό την

απόκρυψη του περιεχομένου των μηνυμάτων. Η κρυπτογραφία είναι ο ένας από τους δύο κλάδους της κρυπτολογίας (ο άλλος είναι η κρυπτανάλυση (Βικιπαιδεία, 2019), η οποία ασχολείται με τη μελέτη της ασφαλούς επικοινωνίας. Σήμερα η κρυπτολογία θεωρείται ένα διεπιστημονικό γνωστικό πεδίο, το οποίο μπορεί να μελετηθεί ως όψη των εφαρμοσμένων μαθηματικών, της θεωρητικής πληροφορικής ή της επιστήμης ηλεκτρονικού μηχανικού.

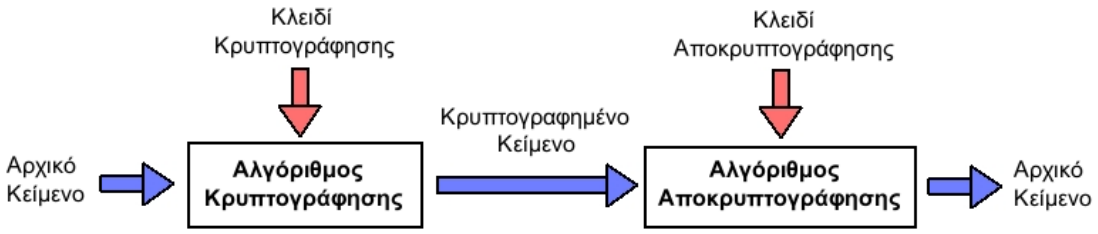
Η σημασία της κρυπτολογίας είναι τεράστια στους τομείς της ασφάλειας υπολογιστικών συστημάτων και των τηλεπικοινωνιών. Ο κύριος στόχος της είναι να δημιουργεί μηχανισμούς, ώστε δυο ή περισσότερα άκρα επικοινωνίας (π.χ. άνθρωποι, προγράμματα υπολογιστών κλπ.), να ανταλλάσσουν μηνύματα χωρίς κανένας τρίτος να μπορεί να διαβάζει την περιεχόμενη πληροφορία, εκτός από τα δύο κύρια άκρα.

Κρυπτογραφία γενικότερα είναι η ανταλλαγή μηνυμάτων μεταξύ δύο ατόμων με τέτοιο τρόπο, ώστε η κατανόηση του περιεχομένου των μηνυμάτων να είναι δυνατή μόνο από τον αποστολέα και τον παραλήπτη.

Η κρυπτογραφία χαρακτηρίζεται από τέσσερις βασικές λειτουργίες:

- *Εμπιστευτικότητα:* Η πληροφορία προς μετάδοση είναι προσβάσιμη μόνο στα εξουσιοδοτημένα μέλη. Η πληροφορία είναι ακατανόητη σε κάποιον τρίτο.
- *Ακεραιότητα:* Η πληροφορία μπορεί να τροποποιηθεί μόνο από τα εξουσιοδοτημένα μέλη.
- *Αποδοχή:* Ο αποστολέας ή ο παραλήπτης της πληροφορίας δεν μπορεί να αρνηθεί την αυθεντικότητα της μετάδοσης ή της δημιουργίας της.
- *Πιστοποίηση:* Οι αποστολέας και παραλήπτης μπορούν να εξακριβώνουν τις ταυτότητές τους, καθώς και την πηγή και τον προορισμό της πληροφορίας, με τη βεβαιότητα ότι οι ταυτότητές τους δεν είναι πλαστές.

Η κρυπτογράφηση και αποκρυπτογράφηση ενός μηνύματος γίνεται με τη βοήθεια ενός αλγόριθμου κρυπτογράφησης (cipher) και ενός κλειδιού κρυπτογράφησης (key). Συνήθως ο αλγόριθμος κρυπτογράφησης είναι γνωστός, οπότε η εμπιστευτικότητα του κρυπτογραφημένου μηνύματος που μεταδίδεται βασίζεται ως επί το πλείστον στη μυστικότητα του κλειδιού κρυπτογράφησης. Το μέγεθος του κλειδιού κρυπτογράφησης μετριέται σε αριθμό bits. Γενικά ισχύει ο εξής κανόνας: όσο μεγαλύτερο είναι το κλειδί κρυπτογράφησης, τόσο δυσκολότερα μπορεί να αποκρυπτογραφηθεί το κρυπτογραφημένο μήνυμα από επίδοξους εισβολείς. Διαφορετικοί αλγόριθμοι κρυπτογράφησης απαιτούν διαφορετικά μήκη κλειδιών, για να πετύχουν το ίδιο επίπεδο ανθεκτικότητας της κρυπτογράφησης.



Ένα τυπικό σύστημα κρυπτογράφησης - αποκρυπτογράφησης.

Αρχικό κείμενο (plaintext) είναι το μήνυμα το οποίο αποτελεί την είσοδο σε μία διεργασία κρυπτογράφησης.

Κλειδί (key) είναι ένας αριθμός αρκετών bit που χρησιμοποιείται ως είσοδος στη συνάρτηση κρυπτογράφησης.

Αλγόριθμος κρυπτογράφησης (cipher) είναι η μέθοδος μετασχηματισμού δεδομένων σε μία μορφή που να μην επιτρέπει την αποκάλυψη των περιεχομένων τους από μη εξουσιοδοτημένα μέρη. Κατά κανόνα ο κρυπτογραφικός αλγόριθμος είναι μία πολύπλοκη μαθηματική συνάρτηση.

Κρυπτογραφημένο κείμενο (ciphertext) είναι το αποτέλεσμα της εφαρμογής ενός κρυπτογραφικού αλγόριθμου πάνω στο αρχικό κείμενο.

Η αντίστροφη διαδικασία, όπου από το κρυπτογραφημένο κείμενο παράγεται το αρχικό μήνυμα, ονομάζεται **αποκρυπτογράφηση (decryption)**.

Υπάρχουν διάφοροι τύποι αλγορίθμων για κρυπτογράφηση. Μερικοί συνηθισμένοι αλγόριθμοι περιλαμβάνουν:

Κρυπτογράφηση μυστικού κλειδιού (SKC): Εδώ χρησιμοποιείται ένα κλειδί, τόσο για την κρυπτογράφηση, όσο και για την αποκρυπτογράφηση. Αυτός ο τύπος κρυπτογράφησης αναφέρεται επίσης ως συμμετρική κρυπτογράφηση

Κρυπτογραφία δημόσιου κλειδιού (PKC): Εδώ χρησιμοποιούνται δύο κλειδιά. Αυτός ο τύπος κρυπτογράφησης ονομάζεται επίσης και ασύμμετρη κρυπτογράφηση. Ένα κλειδί είναι το δημόσιο κλειδί, με το οποίο μπορεί κανείς να έχει πρόσβαση. Το άλλο κλειδί είναι το ιδιωτικό κλειδί, στο οποίο μόνο ο ιδιοκτήτης έχει πρόσβαση. Ο αποστολέας κρυπτογραφεί τις πληροφορίες χρησιμοποιώντας το δημόσιο κλειδί του δέκτη. Ο δέκτης αποκρυπτογραφεί το μήνυμα χρησιμοποιώντας το ιδιωτικό του κλειδί. Για τη μη αναδημοσίευσή του, ο αποστολέας το κρυπτογραφεί σε απλό κείμενο χρησιμοποιώντας ένα ιδιωτικό κλειδί, ενώ ο δέκτης χρησιμοποιεί το δημόσιο κλειδί του αποστολέα, για να το αποκρυπτογραφήσει. Έτσι, ο παραλήπτης γνωρίζει ποιος το έστειλε.

Λειτουργίες Hash: Αυτές είναι διαφορετικές από SKC και PKC. Δε χρησιμοποιούν κανένα κλειδί και ονομάζονται επίσης και «μονόδρομη κρυπτογράφηση». Οι λειτουργίες Hash χρησιμοποιούνται κυρίως για να διασφαλιστεί ότι ένα αρχείο παρέμεινε αμετάβλητο.

1.1.3 Αποκέντρωση

Τα κρυπτονομίσματα είναι αποκεντρωμένα, διότι τα συστήματα λειτουργούν χωρίς να υπάρχει μια κεντρική τράπεζα ή ένας μεμονωμένος διαχειριστής. Η αξία και η προσφορά του ψηφιακού νομίσματος ρυθμίζεται από τους ίδιους τους χρήστες. Κατά μία έννοια, αποτελεί ένα νόμισμα το οποίο ανήκει πραγματικά στους ανθρώπους.

Προκειμένου να κατανοήσουμε πώς λειτουργεί το Bitcoin, είναι αναγκαίο να καταλάβουμε τι είναι ένα αποκεντρωμένο δίκτυο. Η έννοια της αποκέντρωσης έχει ήδη περιγραφεί παραπάνω, αλλά μπορούμε να την εξετάσουμε από μία άλλη οπτική γωνία. Όταν επισκέπτεστε το πρόγραμμα περιήγησής σας και εισέρχεστε στο «www.google.com», ο υπολογιστής σας «ξεκινάει μια συνομιλία» με τους διακομιστές της Google. Έπειτα, το πρόγραμμα περιήγησης σάς εμφανίζει διάφορα αποτελέσματα αναζήτησης. Εάν οι διακομιστές της Google δεν ήταν διαθέσιμοι για οποιονδήποτε λόγο, δε θα μπορούσατε να δείτε αυτά τα αποτελέσματα. Αυτό συμβαίνει λόγω του ότι τα δεδομένα αποθηκεύονται σε ένα κεντρικό δίκτυο.

Σε ένα αποκεντρωμένο δίκτυο, μπορούμε να αποφύγουμε τέτοιου είδους προβλήματα.

Το βασικό χαρακτηριστικό των κρυπτονομισμάτων είναι ότι δεν εκδίδονται από οποιαδήποτε κεντρική αρχή, γεγονός που τα καθιστά θεωρητικά άτρωτα σε παρεμβάσεις κάθε είδους ή απόπειρες χειραγώγησης από την εκάστοτε κυβέρνηση.

1.2 Χρησιμοποιούμενες τεχνολογίες

1.2.1 Blockchain

Η αλυσίδα των blocks (blockchain) είναι μια μορφή τεχνολογίας «κατανεμημένου λογιστικού βιβλίου», συνεχώς ενημερωμένου, που χαρακτηρίζεται από διαφάνεια και σταθερότητα, το οποίο βασίζεται στο Bitcoin και σε πολλά άλλα κρυπτονομίσματα. Πρόκειται για ένα ημερολόγιο όπου καταγράφονται δημόσια όλα τα δεδομένα συναλλαγών. Προκειμένου να καταγραφεί μια συναλλαγή, πρέπει να επιτευχθεί συναίνεση από την πλειονότητα των

χρηστών του δικτύου (Βικιπαιδεία, 2020). Κατ' αυτόν τον τρόπο το δίκτυο συμφωνεί για την εγκυρότητα μιας συναλλαγής.

Το Blockchain είναι πρωτοποριακό, επειδή επιτρέπει τη διεκπεραίωση των συναλλαγών χωρίς μια κεντρική αρχή - όπως μια τράπεζα, κυβέρνηση ή μια εταιρεία πληρωμών. Ο αγοραστής και ο πωλητής αλληλεπιδρούν άμεσα μεταξύ τους, καταργώντας την ανάγκη επαλήθευσης από αξιόπιστο τρίτο μεσάζοντα. Έτσι, αποκλείει τους δαπανηρούς μεσάζοντες και επιτρέπει στις επιχειρήσεις και τις υπηρεσίες να είναι αποκεντρωμένες.

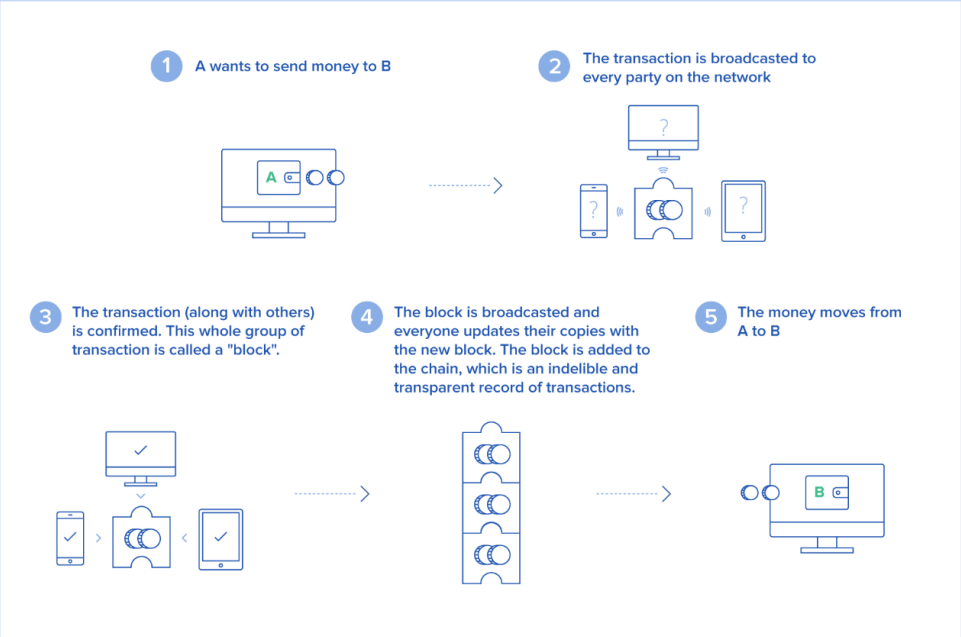
Από τεχνική άποψη, το blockchain χρησιμοποιεί αλγόριθμους συναίνεσης και οι συναλλαγές καταγράφονται σε πολλαπλούς κόμβους αντί σε έναν διακομιστή.

Ένας κόμβος είναι ένας υπολογιστής συνδεδεμένος σε δίκτυο μπλοκ αλυσίδων, ένα σύστημα βασισμένο στο πρωτόκολλο του bitcoin, ο οποίος μεταφορτώνει αυτόματα ένα αντίγραφο του blockchain κατά την ένταξή του στο δίκτυο. Για να είναι έγκυρη μια συναλλαγή, όλοι οι κόμβοι πρέπει να συμφωνούν.

Το blockchain (μια αλυσίδα από blocks/αρχεία) είναι μια βάση συναλλαγών διαμοιρασμένη σε όλους τους κόμβους. Ένα πλήρες αντίγραφο αλυσίδας μπλοκ που περιλαμβάνει ένα σύνολο συναλλαγών, περιέχει κάθε συναλλαγή που έχει γίνει διαχρονικά. Έτσι μπορεί να ανακαλύπτεται πόση αξία είχε κάθε διεύθυνση συναλλαγής από την στιγμή της δημιουργίας της. Κάθε block περιέχει ένα hash από το προηγούμενο block. Αυτό δίνει τη δυνατότητα να δημιουργείται μια αλυσίδα από blocks (chain of blocks) από το αρχικό (genesis block) μέχρι το τρέχον. Επίσης δεν μπορεί να τροποποιηθεί ένα block πάνω στην αλυσίδα μετά από ένα χρονικό διάστημα, γιατί αυτό θα σήμαινε ότι όλα τα υπόλοιπα θα έπρεπε με τη σειρά τους να αλλάξουν αντιστοίχως. Το μήκος της αλυσίδας υπολογίζεται σα συνολική «πολυπλοκότητα» και όχι με τον αριθμό των blocks και θεωρείται έγκυρο, όταν όλες οι συναλλαγές που έχουν καταγραφεί είναι αντιστοίχως έγκυρες. Τα blocks σε μικρότερες αλυσίδες (ή αλλιώς μη έγκυρες αλυσίδες) δε χρησιμοποιούνται. Όταν ο bitcoin client αλλάζει σε μια μεγαλύτερη αλυσίδα, όλες οι έγκυρες συναλλαγές προστίθενται ξανά στην ουρά των συναλλαγών (pool)

και συμπεριλαμβάνονται σε ένα άλλο block. Επιπροσθέτως, υπάρχουν και τα orphan blocks, τα οποία είναι blocks σε μικρότερες αλυσίδες και ονομάζονται έτσι, διότι οι δημιουργημένες συναλλαγές δεν έχουν κάποιο γονικό block στη «μακριά» αλυσίδα. Έτσι αυτές οι συναλλαγές εμφανίζονται σαν «ορφανές» στη λίστα συναλλαγών.

Figure 2: How a Blockchain Works



Source: World Economic Forum

toptal

1.2.2 Εξόρυξη κρυπτονομίσματος

Η διαδικασία δημιουργίας νέων κρυπτονομισμάτων ονομάζεται εξόρυξη, καθώς παρουσιάζει πολλές ομοιότητες με την εξόρυξη του χρυσού. Και στις δύο περιπτώσεις προϋποθέτει την επένδυση μεγάλου φόρτου εργασίας και ενέργειας για την παραγωγή ενός πολύτιμου προϊόντος.

Οι «ανθρακωρύχοι του Bitcoin» στην πραγματικότητα ελέγχουν την εγκυρότητα παλαιότερων συναλλαγών επενδύοντας μεγάλη υπολογιστική ισχύ, προκειμένου να συντηρηθεί και να προστατευθεί το δίκτυο. Στην εν λόγω διαδικασία, δεν εμπλέκεται καμία κεντρική κυβέρνηση. Έτσι, προστατεύεται η ουδετερότητα του δικτύου Bitcoin.

Όταν κάποιος χρήστης θέλει να πραγματοποιήσει μια συναλλαγή, ο καθένας στο αποκεντρωμένο δίκτυο λαμβάνει ένα αντίγραφο της συγκεκριμένης συναλλαγής. Όλα τα μέλη του δικτύου πρέπει να επιβεβαιώσουν αυτή τη συναλλαγή και συνεπώς μειώνεται ή εξαλείφεται η πιθανότητα απάτης.

Όταν πρόκειται για επαλήθευση, ένας μεμονωμένος υπολογιστής δεν είναι αρκετά ισχυρός ώστε να αποκομίσει οικονομικό όφελος. Για να αντιμετωπιστεί αυτό, οι ανθρακωρύχοι συγκεντρώνονται συχνά στα λεγόμενα mining pools για να αυξήσουν τη συλλογική υπολογιστική ισχύ, κατανέμοντας κέρδη από την εξόρυξη στους συμμετέχοντες. Ομάδες από ανθρακωρύχους ανταγωνίζονται για να επαληθεύσουν τις εκκρεμείς συναλλαγές και να αποκομίσουν τα κέρδη, αξιοποιώντας εξειδικευμένο υλικό και φθηνή ηλεκτρική ενέργεια. Αυτός ο «διαγωνισμός» συμβάλλει στη διασφάλιση της ακεραιότητας των συναλλαγών.

Τα πιο συχνά χρησιμοποιούμενα mining pools είναι τα ακόλουθα:

- *Antpool*: Είναι μια από τις μεγαλύτερες εταιρίες bitcoin στην Κίνα που ελέγχει το 30% των hash rates(μονάδα μέτρησης ισχύος) όλου του δικτύου.
- *BTCC*: Έχει στην επιρροή της το 15% των hash rates του δικτύου.
- *Slushpool*: Διευθύνεται από τα satoshi labs(εταιρία που ασχολείται με κρυπτονομίσματα και κρυπτογραφία για το Bitcoin) και έχει έδρα την Τσεχία. Ο έλεγχος της ανέρχεται στα 7% των hash rates του δικτύου.
- *ELIGIUS*: Ήταν το πρώτο mining pool που είχε δημιουργηθεί και σήμερα ελέγχει κάτι λιγότερο από το 1% των hash rates.
- *Bitminer*: Όπως και η eligius πλέον η bitminer ελέγχει κάτι λιγότερο από 1% των hash rates.
- *KanockPOOL*: Δημιουργήθηκε το 2014 και σήμερα ελέγχει το 3% των hash rates.
- *F2POOL*: Είναι η δεύτερη μεγαλύτερη mining pool που υπάρχει, ελέγχοντας το 25% των hash rates του δικτύου, όμως το γραφικό του περιβάλλον υποστηρίζει μόνο την κινέζικη γλώσσα
- *BW POOL*: Ελέγχει το 7% των hash rates του δικτύου και όπως το f2pool υποστηρίζει την κινέζικη γλώσσα.

1.3 Ανταλλαγές κρυπτονομισμάτων

Οι ανταλλαγές κρυπτονομισμάτων γίνονται σε ιστότοπους, όπου οι επισκέπτες μπορούν να αγοράσουν, να πουλήσουν ή να ανταλλάξουν κρυπτονομίσματα με άλλα ψηφιακά ή παραδοσιακά νομίσματα. Οι ανταλλαγές μπορούν να μετατρέψουν τα κρυπτονομίσματα σε μεγάλα εθνικά νομίσματα ή άλλα κρυπτονομίσματα. Μερικές από τις μεγαλύτερες υπηρεσίες ανταλλαγής κρυπτονομισμάτων, περιλαμβάνουν τις Poloniex, Bitfinex, Kraken και GDAX, οι οποίες μπορούν διακινήσουν περισσότερα από 100 εκατομμύρια δολάρια την ημέρα. Σχεδόν κάθε ανταλλαγή υπόκειται σε κυβερνητικούς νομοθετικούς κανονισμούς για την προστασία από παράνομες δραστηριότητες και οι πελάτες οφείλουν να προσκομίζουν αποδεικτικά στοιχεία ταυτότητας, όταν ανοίγουν λογαριασμό.

Αντί για ανταλλαγές, οι χρήστες χρησιμοποιούν μερικές φορές peer-to-peer συναλλαγές μέσω ιστότοπων, όπως οι Local Bitcoins, οι οποίες επιτρέπουν στους εμπόρους να αποφύγουν την αποκάλυψη προσωπικών πληροφοριών. Σε μια συναλλαγή μεταξύ χρηστών, οι συμμετέχοντες διακινούν κρυπτονομίσματα στις συναλλαγές μέσω λογισμικού, χωρίς τη συμμετοχή οποιουδήποτε άλλου διαμεσολαβητή.

1.3.1 Πορτοφόλια κρυπτονομισμάτων

Τα πορτοφόλια κρυπτονομισμάτων είναι απαραίτητα στους χρήστες για να στέλνουν και να λαμβάνουν ψηφιακά νομίσματα και να παρακολουθούν την ισοτιμία τους. Τα πορτοφόλια μπορούν να είναι είτε τύπου hardware είτε τύπου software, αν και τα πορτοφόλια hardware θεωρούνται πιο ασφαλή. Για παράδειγμα, το πορτοφόλι Ledger (Worldwide, 20 Δεκεμβρίου, 2019)(hardware) μοιάζει με μονάδα USB thumb drive και συνδέεται στη θύρα USB του υπολογιστή. Ενώ οι συναλλαγές και τα υπόλοιπα για ένα λογαριασμό bitcoin καταγράφονται στο ίδιο το blockchain, το ιδιωτικό κλειδί που χρησιμοποιείται για την υπογραφή νέων συναλλαγών αποθηκεύεται στο πορτοφόλι Ledger. Όταν γίνεται προσπάθεια να δημιουργηθεί μια νέα συναλλαγή, ο υπολογιστής ζητά την υπογραφή του ιδιωτικού κλειδιού και στη συνέχεια θα τη μεταδώσει στο blockchain. Δεδομένου ότι το ιδιωτικό κλειδί είναι κρυπτογραφημένο στο πορτοφόλι hardware, τα bitcoins είναι ασφαλή, ακόμα και αν ο υπολογιστής έχει υποστεί hack. Παρόλα αυτά, αν δεν δημιουργηθεί αντίγραφο ασφαλείας, η απώλεια του πορτοφολιού θα έχει ως αποτέλεσμα την απώλεια των περιουσιακών στοιχείων του κατόχου.

Αντίθετα, ένα πορτοφόλι software, όπως το πορτοφόλι Coinbase (Team, 19.11.2018),είναι εικονικό. Αυτός ο τύπος λογισμικού μπορεί να τοποθετήσει ηλεκτρονικά τα κεφάλαια του κατόχου στο πορτοφόλι του.

Τα κρυπτονομίσματα, όπως είπαμε, υφίστανται μόνο σε ψηφιακή μορφή οπότε ενδεχομένως να υπάρχει η σκέψη ότι η πληρωμή με αυτά γίνεται με παρόμοιο τρόπο όπως στην περίπτωση των πιστωτικών ή χρεωστικών καρτών. Εκ πρώτης όψεως, μπορεί να φαίνεται έτσι, αλλά τα πράγματα λειτουργούν εντελώς διαφορετικά στο παρασκήνιο.

Τα κρυπτονομίσματα υφίστανται μόνο στη blockchain και οι χρήστες έχουν πρόσβαση μόνο στα δικά τους νομίσματα με τα επονομαζόμενα δημόσια και ιδιωτικά κλειδιά.

Φανταστείτε ότι τα κρυπτονομίσματα λειτουργούν παρόμοια με το email. Για τη λήψη ενός email από κάποιον πρέπει πρώτα να κοινοποιηθεί η διεύθυνση email σας σε αυτόν. Το ίδιο ισχύει και για τα κρυπτονομίσματα, με τη διαφορά ότι πρέπει να κοινοποιηθεί το δημόσιο κλειδί (διεύθυνση πορτοφολιού).

Εάν θέλουμε να έχουμε πρόσβαση στα μηνύματα email μας, πρέπει να γνωρίζουμε τον κωδικό πρόσβασής μας. Το ίδιο ισχύει και για τα κρυπτονομίσματα, αλλά εδώ χρειαζόμαστε το ιδιωτικό κλειδί μας.

Το κρυπτο-πορτοφόλι αποτελείται πάντοτε από δύο μέρη. Το πρώτο είναι η δημόσια διεύθυνση του πορτοφολιού, την οποία μπορούμε να κοινοποιήσουμε σε άλλους, χωρίς να συντρέχει λόγος ανησυχίας. Το δεύτερο είναι ένα ιδιωτικό κλειδί που δεν πρέπει ποτέ να αποκαλύψουμε σε κανέναν.

Το ιδιωτικό κλειδί χρησιμοποιείται για την κρυπτογράφηση της συναλλαγής, ενώ το δημόσιο κλειδί για την αποκρυπτογράφηση της. Ως εκ τούτου, είναι πάρα πολύ σημαντικό το ιδιωτικό κλειδί να παραμένει σε κάθε περίπτωση ασφαλές και αυτός είναι ο λόγος που λέμε ότι όποιος έχει πρόσβαση στο ιδιωτικό κλειδί, είναι επίσης και ο ιδιοκτήτης του πορτοφολιού. Το δημόσιο κλειδί προορίζεται να κοινοποιηθεί σε τρίτους και υποδηλώνει ότι είστε ο ιδιοκτήτης της διεύθυνσης.

Συνεπώς, μπορούμε να κοινοποιήσουμε τα δημόσια κλειδιά σε άλλους, ενώ τα ιδιωτικά κλειδιά πρέπει να παραμένουν ασφαλή στην κατοχή μας.

1.4 Τα είδη των κρυπτονομισμάτων

1.4.1 Bitcoin

Κυκλοφόρησε το 2009 από κάποιον με το ψευδώνυμο Satoshi Nakamoto. Το Bitcoin είναι το πιο γνωστό κρυπτονόμισμα. Παρά την περίπλοκη τεχνολογία πίσω από αυτό, η πληρωμή μέσω του Bitcoin είναι απλή. Σε μια συναλλαγή ο αγοραστής και ο πωλητής χρησιμοποιούν κινητά πορτοφόλια για την αποστολή και λήψη πληρωμών.

Παρόλο που το Bitcoin αναγνωρίζεται ευρέως ως πρωτοπόρος, έχει και κάποιους περιορισμούς. Για παράδειγμα, μπορεί να επεξεργαστεί μόνο επτά συναλλαγές ανά δευτερόλεπτο. Αντίθετα, η Visa χειρίζεται χιλιάδες συναλλαγές ανά δευτερόλεπτο. Ο χρόνος που απαιτείται για την επιβεβαίωση των συναλλαγών έχει επίσης αυξηθεί. Το Bitcoin δεν είναι μόνο πιο αργή τεχνολογία από κάποιες από τις εναλλακτικές της λύσεις, αλλά η λειτουργικότητά του είναι επίσης περιορισμένη. Αυτό αντανακλάται στο μερίδιο αγοράς που μειώθηκε από 81% τον Ιούνιο του 2016 σε 40% περίπου δύο χρόνια αργότερα. Ενώ η τιμή του Bitcoin ακολούθησε γενικά ανοδική πορεία, στις αρχές του 2018 η τιμή του Bitcoin υποχώρησε αισθητά, μειούμενη κάτω από τα 8.000 δολάρια, καθώς προέκυψαν νέα κρυπτονομίσματα με σχετικά αυστηρότερους κανονισμούς από την Κίνα και τη Νότια Κορέα. Άλλα νομίσματα όπως το Bitcoin είναι τα Litecoin, Zcash και Dash, τα οποία ισχυρίζονται ότι παρέχουν μεγαλύτερη ανωνυμία.

1.4.2 Ether και Ethereum

Το Ethereum είναι δημόσια πλατφόρμα blockchain ανοιχτού κώδικα που βασίζεται σε κατανεμημένα (Wikipedia, 2018) και λειτουργικά σύστημα (Wikipedia, 2019) διαθέτοντας τη λειτουργικότητα έξυπνης σύμβασης (scripting). Υποστηρίζει μια τροποποιημένη έκδοση της συναίνεσης Νακαμότο μέσω συναλλαγής με βάση μεταβάσεων.

Το Ether είναι κρυπτονόμισμα του οποίου το blockchain δημιουργείται από τη πλατφόρμα Ethereum. Το Ether μπορεί να μεταφέρεται μεταξύ λογαριασμών και να χρησιμοποιηθεί για την αντιστάθμιση συμμετεχόντων κόμβων εξόρυξης για τους εκτελούμενους υπολογισμούς. Το Ethereum παρέχει μια αποκεντρωμένη εικονική μηχανή, την Εικονική Μηχανή του Ethereum, η οποία μπορεί να εκτελέσει σενάρια χρησιμοποιώντας διεθνές δίκτυο δημόσιων κόμβων. Ο "Gas", ένας μηχανισμός τιμολόγησης εσωτερικών συναλλαγών, χρησιμοποιείται για να μετριάσει το σπαμ(μαζική αποστολή μηνυμάτων) και να κατανείμει τους πόρους του δικτύου.

Το Ethereum προτάθηκε στα τέλη του 2013 από τον Βιτάλικ Μπουτέριν, ερευνητή και προγραμματιστή κρυπτονομισμάτων. Η ανάπτυξη χρηματοδοτήθηκε από μια διαδικτυακή χρηματοδότηση (crowdsale) που έλαβε χώρα μεταξύ του Ιουλίου και του Αυγούστου του 2014. Το σύστημα δημιουργήθηκε στις 30 Ιουλίου 2015, με 11.9 εκατομμύρια "προεξορυγμένα" κέρματα για το crowdsale. Αυτό αντιπροσωπεύει περίπου το 13 τοις εκατό της συνολικής κυκλοφορίας προμηθειών.

Το 2016, ως αποτέλεσμα της κατάρρευσης του εγχειρήματος The DAO, το Ethereum χωρίστηκε σε δύο ξεχωριστά blockchains. Η νέα ξεχωριστή έκδοση είναι το Ethereum (ETH) και η αρχική συνεχιζόμενη έκδοση έγινε γνωστή ως Ethereum Classic (ETC). Η αξία του νομίσματος Ethereum αυξήθηκε πάνω από 13.000% το 2017 με την κεφαλαιοποίηση της αγοράς του να φτάνει τα 28 δισεκατομμύρια δολάρια. Σε ένα σημείο, οι οικονομικοί αναλυτές είχαν προβλέψει ότι η κεφαλαιοποίηση του Ether θα ξεπεράσει εκείνη του Bitcoin ("flippening" (Ma, 2017)). Ωστόσο, τα προβλήματα με την τεχνολογία Ether προκάλεσαν την πτώση της αξίας του. Το Ether χαρακτηρίζεται από αστάθεια. Όπως και με το Bitcoin, στα μέσα Ιανουαρίου του 2018, η τιμή του παρουσίασε απότομη πτώση, από περίπου 1.400$ σε κάτω από 1.000$ μέσα σε λίγες μέρες.

1.4.3 Άλλα δημοφιλή κρυπτονομίσματα

- *Litecoin*: Ξεκίνησε το 2011. Το Litecoin λειτουργεί παρόμοια με το Bitcoin, καθώς είναι επίσης ανοιχτό, αποκεντρωμένο και υποστηριζόμενο από την κρυπτογραφία. Ωστόσο,

προοριζόταν να υπηρετήσει συμπληρωματικό ρόλο στο Bitcoin, «το ασήμι στον χρυσό του Bitcoin». Το Litecoin έχει ταχύτερο ρυθμό δημιουργίας μπλοκ και ταχύτερη επιβεβαίωση συναλλαγής.

- *Dash*: Το Dash κυκλοφόρησε το 2014 ως «Darkcoin». Το Dash έχει ανακατασκευαστεί και προσφέρει περισσότερη ανωνυμία στους χρήστες του λόγω του αποκεντρωμένου δικτύου mastercode του. Χρησιμοποιεί κάτι που ονομάζεται δίκτυο "Masternode" (DashTeam, n.d.) το οποίο έχει πιο ισχυρή βάση από το Bitcoin.
- *Zcash*: Κυκλοφόρησε τον Οκτώβριο του 2016. Το Zcash είναι σχετικά νεοφερμένο στο χώρο. Ωστόσο, υπάρχουν ισχυρισμοί ότι είναι το πρώτο αληθινά ανώνυμο κρυπτονόμισμα που υπάρχει, λόγω της χρήσης μηδενικών γνώσεων SNARKS, (COMPANY, n.d.) τεχνολογία η οποία δεν περιλαμβάνει κανένα αρχείο συναλλαγών. Η τεχνολογία εξασφαλίζει ότι παρά τις κρυπτογραφημένες πληροφορίες, εξακολουθεί να είναι σωστή και ότι οι διπλές δαπάνες είναι αδύνατες.
- *Monero*: Το Monero διαθέτει μοναδικές ιδιότητες προστασίας προσωπικών δεδομένων. Για παράδειγμα, το Monero επιτρέπει πλήρη προστασία της ιδιωτικότητας χρησιμοποιώντας μια τεχνική που ονομάζεται «υπογραφές δακτυλίου». Είναι δημοφιλές στη μαύρη αγορά σκοτεινού ιστού, όπου οι χρήστες αγοράζουν τα πάντα, από ναρκωτικά μέχρι πυροβόλα όπλα.
- *Ripple*: Κυκλοφόρησε το 2012 .Το Ripple προσφέρει άμεσες και χαμηλού κόστους διεθνείς πληρωμές. Το Ripple χρησιμοποιεί ένα «βιβλίο ομοφωνίας» ως μέθοδο επαλήθευσής του και δεν απαιτεί εξόρυξη - κάτι που το διακρίνει από το Bitcoin και άλλα κρυπτονομίσματα. Απαιτεί συνεπώς λιγότερη υπολογιστική ισχύ.

1.5 Σύντομη ιστορική αναδρομή

(-2008) Εποχή προ Bitcoin

Στα χρόνια πριν τη δημιουργία του Bitcoin, υπήρξαν μερικά πρωτότυπα παραδείγματα online ψηφιακών νομισμάτων, αλλά κανένα εξ αυτών δεν κατάφερε να εδραιωθεί πιο σοβαρά. Δύο παραδείγματα τέτοιων νομισμάτων είναι τα B-Money και BitGold, τα οποία σχεδιάστηκαν, αλλά δεν κατάφεραν ποτέ να προχωρήσουν πέραν του αρχικού σταδίου.

(***2008) Satoshi Nakamoto και Bitcoin***

Τον Αύγουστο του 2008, καταχωρίστηκε ο Διαδικτυακός χώρος bitcoin.org, ο οποίος παραμένει η κεντρική σελίδα του πιο διάσημου κρυπτονομίσματος. Στις 31 Οκτωβρίου του ίδιου έτους, ένα άτομο ή οργανισμός με το ψευδώνυμο Satoshi Nakamoto δημοσίευσε μια επιστημονική εργασία με τίτλο «Bitcoin: A Peer-to-PeerElectronic Cash System» (Nakamoto, 2008). Η εργασία παρουσίαζε την έννοια της τεχνολογίας blockchain και το Bitcoin περιγράφτηκε ως ψηφιακός πόρος και σύστημα ανοικτού κώδικα (open source system). Αυτό

πρακτικά σημαίνει ότι κανείς δεν είναι ιδιοκτήτης του και ότι καθένας μπορεί να συμμετέχει στη χρήση και την εξέλιξή του.

Μέχρι σήμερα, κανείς δεν γνωρίζει ποιος είναι στην πραγματικότητα ο Satoshi Nakamoto, οπότε η ταυτότητά του έχει δημιουργήσει πολλούς μύθους και διάφορες θεωρίες. Το πιο πιθανό είναι ότι η ταυτότητα του θα παραμείνει για πάντα άγνωστη.

(2009) Η εμφάνιση της κρυπτο-εξόρυξης

Στις αρχές του 2009, το λογισμικό του Bitcoin έγινε διαθέσιμο για πρώτη φορά στο ευρύ κοινό και ο Satoshi Nakamoto εξόρυξε τα πρώτα 50 Bitcoins, ξεκινώντας κατά συνέπεια την ιστορία της κρυπτο-εξόρυξης. Την εποχή αυτή, υπήρχε μόνο μία μικρή ομάδα προγραμματιστών και φανατικών χρηστών που συμμετείχαν στην εξέλιξη μιας ιδέας που ορισμένοι εξ αυτών περίμεναν ότι θα οδηγούσε σε μια άκρως πρωτοποριακή τεχνολογία.

(2010) Πρώτες επιτυχημένες συναλλαγές

Στα πρώτα χρόνια ύπαρξής του, ήταν κάπως δύσκολο να αποδοθεί οποιαδήποτε πραγματική αξία στο Bitcoin, δεδομένου ότι δεν πραγματοποιούνταν συναλλαγές σε μεγάλη κλίμακα. Για παράδειγμα, ο προγραμματιστής Gavin Andresen αγόρασε 10.000 Bitcoins για 50$ και δημιούργησε μια ιστοσελίδα ονόματι Bitcoin Faucet, όπου κυριολεκτικά έκανε δωρεά Bitcoin για πλάκα.

Στην πιο διάσημη υπόθεση αυτής της εποχής, πρωταγωνιστής είναι ο Laszlo Hanyecz, ένας προγραμματιστής που αγόρασε δύο πίτσες με αντίτιμο 10.000 Bitcoins. Αυτή θεωρείται και η πρώτη ουσιαστική συναλλαγή με κρυπτονόμισμα. Στην ανώτατη τιμή που έχει αγγίξει το Bitcoin, αυτές οι δύο πίτσες θα κόστιζαν πάνω από 100 εκατομμύρια δολάρια. Ωστόσο, ο Laszlo δεν μετάνιωσε ποτέ για αυτή του την απόφαση, καθώς πιστεύει ότι ήταν ένα καίριο βήμα που βοήθησε στην ανάπτυξη του κρυπτο-οικοσυστήματος.

Το Δεκέμβριο του 2010, ο Satoshi Nakamoto δημοσίευσε το τελευταίο δημόσιο μήνυμά του στο δημοφιλές online forum ονόματι «bitcoin talk» ((Nakamoto, Novemner 2009-Today)). Έγραψε μερικές μικρολεπτομέρειες σχετικά με την τελευταία έκδοση του λογισμικού. Έπειτα, διατήρησε επαφή με κάποιους προγραμματιστές μέσω email, αλλά τα ίχνη του έχουν χαθεί εντελώς από τον Απρίλιο του 2011. Είναι πάρα πολύ πιθανό ότι η ταυτότητα του θα παραμείνει για πάντα ένα μυστήριο.

(2011) Εμφάνιση καινούργιων κρυπτονομισμάτων

Βάσει της επαναστατικής τεχνολογίας του Bitcoin και δεδομένης της σχετικής επιτυχίας της, η ιδέα των αποκεντρωμένων νομισμάτων άρχισε σταδιακά να κερδίζει έδαφος. Ως εκ τούτου, έκαναν την εμφάνιση τους τα πρώτα εναλλακτικά κρυπτονομίσματα. Εμείς τα αποκαλούμε altcoins.

Τα περισσότερα εξ αυτών προσπαθούν να βελτιώσουν το πρωτόκολλο του Bitcoin με επιπρόσθετα χαρακτηριστικά, όπως υψηλότερη ταχύτητα, ανωνυμία κτλ. Το Litecoin συγκαταλέγεται στα πρώτα εναλλακτικά νομίσματα (altcoins) και αυτός είναι ο λόγος για τον οποίο επονομάστηκε «ασήμι», ενώ το Bitcoin «χρυσός». Αυτή τη στιγμή, κυκλοφορούν στην αγορά χιλιάδες κρυπτονομίσματα.

(2013) Η πρώτη μεγάλη «φούσκα»

Τον Ιανουάριο του 2013, η τιμή του Bitcoin ξεπέρασε για πρώτη φορά τα 1.000$. Αυτό αποτέλεσε ένα σημαντικό ορόσημο στην ιστορία του, παρόλο που η τιμή έπεσε γρήγορα και στη συνέχεια παρέμεινε στάσιμη για δύο χρόνια, προτού καταφέρει να εκτιναχθεί και πάλι στο ψηλότερο σημείο όλων των εποχών.

Κατά τη διάρκεια της συγκεκριμένης χρονικής περιόδου, ορισμένοι άνθρωποι έχασαν πολλά χρήματα και αυτό είχε αρνητικό αντίκτυπο για το Bitcoin. Ακόμα κι έτσι, κάθε μορφής δημοσιότητα είναι καλή και τα κρυπτονομίσματα ήρθαν για τα καλά στο προσκήνιο, αφού εμφανίστηκαν σε δελτία τύπου των ΜΜΕ και έγιναν γνωστά στο ευρύ κοινό.

Τα κρυπτονομίσματα άφησαν πίσω «την παιδική τους ηλικία», ωστόσο δεν ήταν ακόμα ξεκάθαρο εάν τελικά θα επιβίωναν. Πολλά εξ αυτών, δεν τα κατάφεραν.

(2014) Mt. Gox και έντονη αναταραχή

Τον Ιανουάριο του 2014, το μεγαλύτερο ανταλλακτήριο Bitcoin, ονόματι Mt. Gox, δέχτηκε κυβερνοεπίθεση. Το μέγεθος της κλοπής ανήλθε σε περίπου 850.000 Bitcoins! Δεν έχει ξεκαθαριστεί ακόμα ποιος ευθύνεται και παραμένει η μεγαλύτερη κλοπή Bitcoin που έχει σημειωθεί στην ιστορία.

Τα κρυπτονομίσματα βασίζονται στην ανωνυμία και την αποκέντρωση, οπότε δεν αποτελεί έκπληξη το γεγονός ότι είναι πολύ ελκυστικά για τους εγκληματίες. Όσοι είναι τεχνικά καταρτισμένοι, μπορούν εύκολα να καλύψουν τα ίχνη τους.

Το Νοέμβριο του 2014, ο κόσμος των κρυπτονομισμάτων δέχτηκε ακόμα ένα πλήγμα, καθώς ο ιδρυτής της ιστοσελίδας Silk Road ονόματι Ross Ulbricht καταδικάστηκε σε ισόβια κάθειρξη. Το 70% των προϊόντων προς πώληση στην εν λόγω ιστοσελίδα αφορούσε ναρκωτικές ουσίες και οι συναλλαγές μπορούσαν να πραγματοποιηθούν με Bitcoin. Πολλά άτομα πιστεύουν ότι ο κος Ulbricht κατηγορήθηκε άδικα, διότι πολλά από τα αποδεικτικά στοιχεία εναντίον του ήταν άκρως αμφιλεγόμενα. Ωστόσο υπάρχει μικρή έως μηδενική πιθανότητα να αποφυλακιστεί κάποια στιγμή στο μέλλον.

(2015) Ethereum και η έκρηξη των altcoins

Το Ethereum project λανσαρίστηκε το 2015 και συχνά παρατίθεται ως η πρώτη πραγματικά χρήσιμη εφαρμογή του συστήματος, πάνω στο οποίο οικοδομήθηκε η ιδέα blockchain του Bitcoin. Το Ethereum παρουσίασε τα έξυπνα συμβόλαια, μια ενδιαφέρουσα έννοια που

καθιστά εφικτή τη διενέργεια δημόσιων συμβολαίων με διαφάνεια, όπου οι συναλλαγές πραγματοποιούνται κάτω από επακριβώς καθορισμένες συνθήκες. Η φιλοσοφία των έξυπνων συμβολαίων στάθηκε αφορμή για αμέτρητα νέα νομίσματα τα οποία κατασκευάστηκαν σύμφωνα με το πρότυπο ERC20 και ανήκουν στην blockchain του Ethereum.

(2016) Επιτυχημένα projects ICO

Η δημοτικότητα του Ethereum συνοδεύτηκε από την εμφάνιση projects για start-ups με κεφάλαια που προέρχονταν από συμμετοχική χρηματοδότηση (crowd funding). Αυτός ο τύπος χρηματοδότησης στην κρυπτο-σφαίρα ονομάζεται Initial Coin Offering (ICO), δηλαδή Αρχική Προσφορά Νομισμάτων.

Άτομα αγόραζαν τα συγκεκριμένα νομίσματα και κέρματα βασιζόμενοι στην πίστη που είχαν για την επιτυχία του project και την πεποίθηση ότι τα εικονικά νομίσματα θα αποκτήσουν κάποια στιγμή αξία, όταν τελικά θα υλοποιηθεί το project υπό σχεδιασμό.

Ορισμένες χώρες (όπως η Κίνα και οι ΗΠΑ) απαγόρευσαν τέτοιου είδους projects, ή τουλάχιστον προειδοποίησαν τους χρήστες ότι ενδεχομένως να πρόκειται για απάτες, όπως τα Σχήματα Πόντσι (Ponzi schemes) τα οποία παρουσιάζονται αναληθώς ως νόμιμες επενδύσεις.

(2017) Το Bitcoin αγγίζει τα 20.000 USD

Ο αριθμός με τις διαθέσιμες προς το κοινό πλατφόρμες συναλλαγών και τα ανταλλακτήρια διαρκώς αυξανόταν, καθιστώντας πιο εύκολη την αγορά και πώληση κρυπτονομισμάτων. Επιπλέον, ήταν η χρυσή εποχή των ICO projects.

Όλα αυτά συνέβαλαν στη ραγδαία αύξηση του κρυπτο-οικοσυστήματος. Αυτή η νέα τεχνολογία υποσχόταν τεράστια κέρδη και η συνολική κεφαλαιοποίηση της αγοράς κρυπτονομισμάτων ξεπέρασε τα 800 δις δολάρια ΗΠΑ στις αρχές του 2018. Πρακτικά, όλα τα κρυπτονομίσματα πουλούσαν σαν ζεστό ψωμί …

(2018) Επιστροφή στην πραγματικότητα

Η συγκεκριμένη αύξηση ήταν μη βιώσιμη, οπότε δεν αποτέλεσε έκπληξη, όταν η φούσκα έσκασε και οι τιμές άρχισαν να φθίνουν. Πολλά projects κατέρρευσαν καθώς ήταν υπερβολικά φιλόδοξα για μια τόσο εκκολαπτόμενη τεχνολογία. Ωστόσο, η ευμετάβλητη φύση αυτής της νέας αγοράς θεωρείται κάτι το φυσιολογικό.

(2019) Αναζωπύρωση

Το Bitcoin βλέπει μια νέα ανάκαμψη στην τιμή (και τον όγκο), που αυξάνεται σε περίπου 10.000$. Από το τέλος του 2019, η τιμή ενός Bitcoin είναι περίπου 7.250$.

2 Εισαγωγή στο BigQuery-Χαρακτηριστικά και Κοστολόγηση

2.1 Χαρακτηριστικά

Η αποθήκευση και η αναζήτηση τεράστιων συνόλων δεδομένων μπορεί να είναι χρονοβόρα και δαπανηρή χωρίς την κατάλληλη υποδομή.

Το BigQuery είναι μια πλήρως διαχειριζόμενη αποθήκη δεδομένων, χωρίς διακομιστή, που επιτρέπει κλιμακούμενη ανάλυση δεδομένων, τάξης μεγέθους peta bytes, που κυκλοφόρησε στις 19 Μαΐου του 2010 . Λειτουργεί ως SaaS (υπηρεσία προσβάσιμη από χρήστες διαδικτυακά και απομακρυσμένα), χωρίς να απαιτείται δηλαδή η τοπική εγκατάσταση και συντήρηση λογισμικού, εξυπηρετητών ή άλλων συστημάτων και υποδομών και υποστηρίζει την αναζήτηση μέσω ANSI SQL γλώσσας επερωτήσεων.

Τα κύρια χαρακτηριστικά του συνοψίζονται στα:

Χωρίς διακομιστή: Στα περισσότερα περιβάλλοντα αποθήκευσης δεδομένων με διακομιστή οι διαχειριστές θα πρέπει να ελέγχουν για την απόδοση, την ασφάλεια, την ελαστικότητα και την αξιοπιστία τους. Σε ένα μοντέλο όμως χωρίς διακομιστή η επεξεργασία των δεδομένων διανέμεται αυτόματα σε μεγάλο αριθμό μηχανημάτων που λειτουργούν παράλληλα. Χρησιμοποιώντας το μοντέλο χωρίς διακομιστές του BigQuery, οι μηχανικοί δεδομένων και οι διαχειριστές βάσεων δεδομένων εστιάζουν λιγότερο στην υποδομή και περισσότερο στη λήψη πληροφοριών από τα δεδομένα.

BigQuery Omni: Το κόστος μεταφοράς δεδομένων μεταξύ παρόχων cloud (Βικιπαιδεία, 2020) δεν είναι βιώσιμο για πολλές επιχειρήσεις. Το BigQuery Omni αντιπροσωπεύει έναν νέο τρόπο ανάλυσης δεδομένων που είναι αποθηκευμένα σε πολλά δημόσια clouds και επιτρέπει την υποβολή ερωτημάτων χωρίς την κίνηση μεταξύ σε αυτά ή της δημιουργίας αντιγράφων.

Για παράδειγμα, μπορεί να χρησιμοποιηθεί το BigQuery Omni για να υποβληθούν ερώτημα σε δεδομένα του Google Analytics 360 Ads που είναι αποθηκευμένα στο Google Cloud, καθώς και δεδομένα καταγραφής ερωτημάτων από την πλατφόρμα ηλεκτρονικού εμπορίου και εφαρμογές που είναι αποθηκευμένες στο AWS S3.

BigQuery ML: Η μηχανική εκμάθηση είναι ένα πεδίο της τεχνητής νοημοσύνης (Artificial Intelligence) που χρησιμοποιεί εφαρμογές λογισμικού που μπορούν να μάθουν να αυξάνουν την ακρίβειά τους για τα αναμενόμενα αποτελέσματα. Είναι ο τρόπος εκπαίδευσης των υπολογιστών σχετικά με τον τρόπο εκτέλεσης σύνθετων εργασιών που οι άνθρωποι δεν ξέρουν πώς να πραγματοποιήσουν. Είναι δημοφιλές αυτές τις μέρες που υπάρχουν πολλές δραστηριότητες μηχανικής μάθησης που συμβαίνουν στην καθημερινή μας ζωή και σύντομα θα γίνει αναπόσπαστο μέρος της καθημερινότητας(πχ προτάσεις που δεχόμαστε από Netflix).

Το BigQuery ML αυξάνει την ταχύτητα ανάπτυξης εξαλείφοντας την ανάγκη μεταφοράς δεδομένων και επιτρέπει τη δημιουργία και εκτέλεση μοντέλων μηχανικής μάθησης στο BigQuery χρησιμοποιώντας ερωτήματα standard SQL. Το BigQuery ML εκδημοκρατίζει τη μηχανική μάθηση επιτρέποντας στους επαγγελματίες της SQL να κατασκευάσουν μοντέλα χρησιμοποιώντας υπάρχοντα εργαλεία και δεξιότητες SQL. Οι αναλυτές μπορούν να το χρησιμοποιήσουν για να δημιουργήσουν και να αξιολογήσουν μοντέλα ML στο BigQuery.

BigQuery BI: Είναι μια γρήγορη υπηρεσία ανάλυσης της μνήμης για το BigQuery που επιτρέπει στους χρήστες να αναλύουν μεγάλα και πολύπλοκα σύνολα δεδομένων παράλληλα με το χρόνο απόκρισης των ερωτημάτων. Το BigQuery BI Engine ενσωματώνεται απρόσκοπτα με γνωστά εργαλεία όπως το Data Studio και βοηθάει στην επιτάχυνση της εξερεύνησης και ανάλυσης δεδομένων για το Looker (GoogleCloud, n.d.), Sheets και για τους συνεργάτες BI του BigQuery.

Συνδεδεμένα φύλλα (**Connected Sheets):** επιτρέπει στους χρήστες να αναλύουν, να οπτικοποιούν και να μοιράζονται δισεκατομμύρια σειρών δεδομένων του BigQuery στα υπολογιστικά φύλλα της Google χωρίς να απαιτούν γνώσεις SQL. Οι χρήστες μπορούν να εφαρμόσουν οικεία εργαλεία - όπως συγκεντρωτικούς πίνακες, γραφήματα και τύπους - για να αντλήσουν εύκολα πληροφορίες από μεγάλα δεδομένα.

2.2 Κοστολόγηση

Το BigQuery προσφέρει ποικίλες και ευέλικτες επιλογές τιμολόγησης για την κάλυψη των τεχνικών αναγκών και του προϋπολογισμού του κάθε χρήστη.

Λειτουργία	**Τιμή**
Αποθήκευση	$0.02 ανά GB, ανά μήνα $0.01 ανά GB, ανά μήνα για αποθήκευση long-term (CloudGoogle, n.d.)
Streaming Inserts	$0.01 ανά 200 MB
Φόρτωση, αντιγραφή και εξαγωγή δεδομένων.	Δωρεάν

Τύπος συνδρομής	**Τιμή**
Pay-as-you-go	$5 ανά TB

	Το πρώτο terabyte (1 TB) ανά μήνα είναι δωρεάν
Flat-rate pricing	Ξεκινά στα $1,700/μήνα για αποκλειστική κράτηση 100 slot (GoogleCloud, n.d.) $4 ανά ώρα για 100 Flex slot.

3 Bitcoin Cash Cryptocurrency: δομή και πεδία

3.1 Εισαγωγή στο Bitcoin Cash Cryptocurrency

Το Bitcoin Cash είναι ένα κρυπτονόμισμα με το δικό του blockchain. Δημιουργήθηκε στα τέλη του 2016, επομένως είναι πολύ νεότερο από το Bitcoin.

Το Bitcoin Cash προήλθε από το Bitcoin. Οι κόμβοι του ήταν κάποτε μέρος του Bitcoin blockchain και αποτελούν πλέον ένα «fork». Forking είναι η διαδικασία κατά την οποία προγραμματιστές παίρνουν ένα αντίγραφο του πηγαίου κώδικα ενός open source προγράμματος (πρόγραμμα στο οποίο υπάρχει δικαίωμα επεξεργασίας του) και ξεκινούν ανεξάρτητη ανάπτυξη σε αυτό με σκοπό τη δημιουργία ενός νέου

Υπάρχουν αρκετά τέτοια forks, αλλά κανένα δεν είναι τόσο γνωστό ούτε έχει χρησιμοποιηθεί όσο το Bitcoin Cash.

Το Bitcoin διαμορφώθηκε για να δημιουργήσει το Bitcoin Cash, επειδή οι προγραμματιστές του ήθελαν να κάνουν κάποιες σημαντικές αλλαγές σε αυτό.

Οι αλλαγές που διαφοροποιούν τα Bitcoin Cash και Bitcoin είναι οι ακόλουθες:

- Το Bitcoin Cash έχει φθηνότερα τέλη μεταφοράς (περίπου 0,20$ ανά συναλλαγή), οπότε η πραγματοποίηση συναλλαγών στο BCH θα εξοικονομήσει περισσότερα χρήματα από τη χρήση του BTC. Μια συναλλαγή BTC μπορεί να κοστίσει περίπου 1$ ανά συναλλαγή, αν και στο παρελθόν αυξήθηκε σε περίπου 25$ ανά συναλλαγή.
- Το BCH έχει ταχύτερους χρόνους μεταφοράς. Επομένως, δε χρειάζεται αναμονή για τα 10 λεπτά που απαιτούνται για την επαλήθευση μιας συναλλαγής Bitcoin.
- Το BCH μπορεί να χειριστεί περισσότερες συναλλαγές ανά δευτερόλεπτο. Αυτό σημαίνει ότι περισσότερα άτομα μπορούν να χρησιμοποιούν το BCH ταυτόχρονα, από όσα μπορούν το BTC.

Όλες αυτές οι αλλαγές οφείλονται στο γεγονός ότι ένα block Bitcoin Cash (στο blockchain) είναι οκτώ φορές μεγαλύτερο από ένα block Bitcoin. Αυτό κάνει το BCH γρηγορότερο, φθηνότερο και πιο επεκτάσιμο. Τα μετρητά Bitcoin Cash υιοθετούνται όλο και περισσότερο λόγω των παραπάνω.

3.2 Δομή του block και επαύξηση του blockchain

Εδώ θα αναλύσουμε τα πεδία για το bitcoin cash τα οποία βρίσκονται στο BigQuery. Όπως έχουμε ήδη δει, η κύρια τεχνολογία που χρησιμοποιείται για τη διατήρηση όλων των δεδομένων και για τη διασφάλιση έγκυρων συναλλαγών είναι το blockchain. Αυτό ως γνωστόν αποτελείται από blocks.

Ένα block καταγράφει μερικές ή όλες τις πιο πρόσφατες συναλλαγές που δεν έχουν ακόμα εισαχθεί από προηγούμενα blocks. Όταν γίνεται κάποια bitcoin συναλλαγή αυτή δεν προστίθεται κατευθείαν στο blockchain αλλά καταχωρείται σε μια αποθήκη (transaction pool). Οι miners έχουν ευθύνη να συγκεντρώσουν όλες τις συναλλαγές σε ένα «υποψήφιο» block. Κάθε τέτοιο block αποτελείται από τα εξής πεδία:

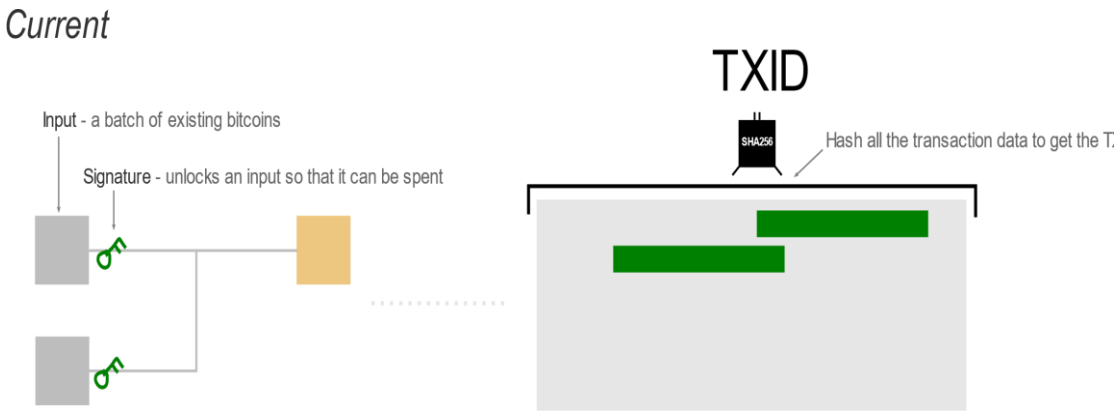
- Block size: το μέγεθος του block
- Block header: σημαντικές πληροφορίες (metadata) για το block
    - Version: Χαρακτηρίζει τη δομή των δεδομένων μέσα στο block και χρησιμοποιείται για να εντοπίζει αλλαγές στο λογισμικό
    - Previous block hash: η τιμή hash στο προηγούμενο block
    - Merkle root hash: Η ρίζα του Merkle tree. Είναι η δομή που περιέχει όλες τις συναλλαγές. Αν συμβεί κάποια αλλαγή στις συναλλαγές, τότε και η ρίζα αλλάζει τιμή
    - Timestamp: ο χρόνος δημιουργίας του block
    - Difficulty target: Οι miners προκειμένου να κάνουν έγκυρο ένα block θα πρέπει να κατακερματίσουν το header του block, ούτως ώστε αυτό να είναι μικρότερο η ίσο από τον target αριθμό. Αυτός ο αριθμός υπολογίζεται από το difficulty, μια τιμή η οποία καθορίζει πόσος χρόνος θα χρειαστεί προκειμένου οι miners να προσθέσουν ένα νέο block στο blockchain
- Transactions counter: ο αριθμός των συναλλαγών που βρίσκονται στο block
- Transactions: δομή που περιέχει όλες τις συναλλαγές στο block.

Μια bitcoin συναλλαγή συγκεντρώνει δεδομένα που περιγράφουν την κίνηση των bitcoins. Δέχεται εισόδους (inputs-bitcoins που χρησιμοποιούνται σε μια συναλλαγή) και δημιουργεί-επιστρέφει εξόδους (outputs-bitcoins που δημιουργούνται σε μια συναλλαγή). Πιο συγκεκριμένα αποτελείται από τα εξής πεδία:

- Version: Χαρακτηρίζει τη δομή των δεδομένων των συναλλαγών και χρησιμοποιείται για να εντοπίζει αλλαγές στο λογισμικό
- Input Count: Πλήθος των εισόδων
- Inputs:
    - TXDIS (Transaction ID): αναγνωριστικό της συναλλαγής
    - VOUT: αναγνωριστικό μιας εξόδου σε μια συναλλαγή
    - ScriptSigSize: δηλώνει το μέγεθος του unlocking κώδικα (χρησιμοποιείται για να ξεκλειδώσει την είσοδο)

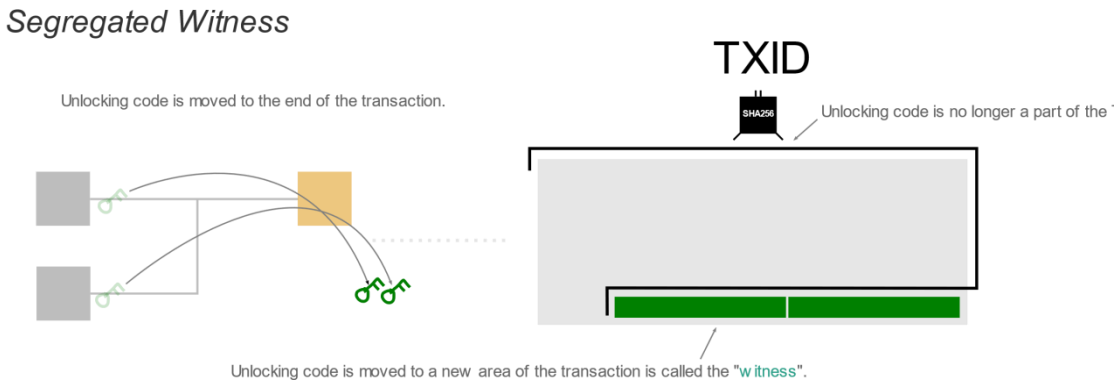
    - ScriptSig: ο unlocking κώδικας
    - Sequence: ένας αριθμός ο οποίος σηματοδοτεί τη σειρά με την οποία μια συναλλαγή θα τύχει επεξεργασίας
- Output Count: Ποσότητα των εξόδων
- Outputs:
    - Value: η τιμή της εξόδου σε satoshi (μονάδα μέτρησης των bitcoins - η μικρότερη τιμή τους)
    - ScriptPubKeySize: δηλώνει το μέγεθος του locking κώδικα (χρησιμοποιείται για να κλειδώσει την είσοδο)
    - ScriptPubKey: ο locking κώδικας
- Locktime: δηλώνει την ώρα (σε Unix χρόνο) στην οποία μια συναλλαγή μπορεί να συμπεριληφθεί στο block.

Στην κύρια δομή των συναλλαγών, ο unlocking κώδικας βρίσκεται αμέσως μετά από μια είσοδο, που αυτό σημαίνει ότι μεταδίδεται σε όλα τα δεδομένα της συναλλαγής. Αυτό έχει ως αποτέλεσμα το TXID να δημιουργείται βάσει όλων αυτών. Συνεπώς έτσι προκαλείται το λεγόμενο πρόβλημα για το Bitcoin, «Transaction Malleability». Αναφέρεται στο γεγονός ότι τα TXID μιας συναλλαγής μπορούν να αλλάξουν τροποποιώντας τον unlocking κώδικα και έτσι όταν θέλουμε να στείλουμε μια συναλλαγή στο δίκτυο Bitcoin, κάθε κόμβος μπορεί να αλλάξει το TXID πριν να περάσει σε αυτό.



Το Segregated Witness είναι η διαδικασία που άλλαξε τη δομή των bitcoin συναλλαγών. Ο κύριος λόγος της πρότασης αυτής είναι να ρυθμιστεί το πρόβλημα αυτό. Παρόλα αυτά, αυτή η αλλαγή επιφέρει και άλλο πλεονέκτημα, αυτό της επαύξησης των συναλλαγών που ένα block μπορεί να χωρέσει.

Στο Segregated Witness ή SegWit η πρόταση είναι να μεταφερθεί ο unlocking κώδικας στο τέλος των δεδομένων της συναλλαγής. Το TXID έτσι δημιουργείται από όλα τα δεδομένα, εκτός από αυτά που αφορούν τον unlocking κώδικα.



Το γεγονός ότι ο κώδικας έχει μεταφερθεί σε ένα νέο «witness» πεδίο στα δεδομένα των συναλλαγών, σημαίνει ότι και ο τρόπος με τον οποίο μετράμε ένα block μπορεί επίσης να αλλάξει. Πριν το μέγιστο μέγεθος ενός block έφτανε τα 1.000.000 bytes (1 MB). Τώρα το μέγεθος δεν υπολογίζεται σε bytes αλλά σε «weight». Μέγιστο μέγεθος πλέον είναι 4.000.000 weight. Ένα byte σε μια συναλλαγή έχει weight 4 και ένα witness byte έχει weight 1.

Οπότε, το όριο μεγέθους ενός block πολλαπλασιάζεται επί 4 για δώσει το νέο όριο block weight. Κάθε byte σε μια συναλλαγή πολλαπλασιάζεται επίσης επί 4 για να δώσει το weight της συναλλαγής. Ωστόσο, πολλαπλασιάζονται μόνο τα witness bytes με 1, πράγμα που δίνει ουσιαστικά 75% αύξηση για τον χώρο που καταλαμβάνει ένα block.

3.3 Δοσολοηψίες BCH

Η αποστολή BCH προϋποθέτει την πρόσβαση στα δημόσια και ιδιωτικά κλειδιά που σχετίζονται με την ποσότητα των bitcoin που διαθέτει κάθε χρήστης. Τα δημόσια κλειδιά, που ονομάζονται και ως διεύθυνση της συναλλαγής είναι μια τυχαία αλληλουχία από γράμματα και αριθμούς όπως πχ μια διεύθυνση ηλεκτρονικού ταχυδρομείου. Είναι δημόσια ούτως ώστε να διαμοιράζονται με ασφάλεια σε τρίτους. Τα ιδιωτικά κλειδιά από την άλλη είναι μια επίσης μια τυχαία αλληλουχία αριθμών και γραμμάτων που πρέπει να φυλάσσονται μυστικά.

Για παράδειγμα, έστω ότι έχουμε δύο άτομα, τον Γιάννη ο οποίος θέλει να στείλει BCH και τη Μαρία η οποία θα τα παραλάβει. Για να συμβεί αυτό ο Γιάννης χρησιμοποιεί το ιδιωτικό κλειδί του για να κλειδώσει ένα μήνυμα με πληροφορίες για τη συναλλαγή. Τα βασικά μέρη που αποτελείται μια συναλλαγή είναι:

- Header:
    - Hash: χρησιμοποιείται για τον έλεγχο της ακεραιότητας της συναλλαγής.
    - Version: η έκδοση πρωτοκόλλου που πρέπει να χρησιμοποιηθεί για να γίνει έγκυρο το block
    - Input-output count: ο αριθμός των εισόδων-εξόδων της συναλλαγής
    - Lock time: Ο ελάχιστος χρόνος που χρειάζεται μια συναλλαγή για να εξορυχθεί.
- Input:
    - Hash της προηγούμενης εξόδου: ένας δείκτης στην προηγούμενη έξοδο της συναλλαγής η οποία έχει ακόμα bitcoins (unspent transaction output UTXO)
    - Inputs.index: αναγνωριστικό στη λίστα των εξόδων της προηγούμενης συναλλαγής.
    - Inputs.scirpt: κωδικοποιημένο μήνυμα που χρησιμοποιείται για να κλειδώσει τη συναλλαγή.
- Output:
    - Output.value: τα συνολικά bitcoins που θα ξοδευτούν.
    - Output.script: κωδικοποιημένο μήνυμα που χρησιμοποιείται για να ξεκλειδώσει τη συναλλαγή.

Η συναλλαγή τότε διαδίδεται στο δίκτυο Bitcoin Cash στο οποίο οι miners θα επαληθεύσουν αν τα στοιχεία του Γιάννη είναι έγκυρα χρησιμοποιώντας τον συμβολικό κώδικα των εισόδων και εξόδων (input.script , output.script).

Για να συμπεριληφθεί η συναλλαγή σε ένα block όπως έχουμε πει προηγουμένως αποθηκεύεται στο memory pool. Οι miners από εκεί διαλέγουν αυτές αρχικά που έχουν μεγαλύτερο transaction fee τα οποία συγκαταλέγονται στην πρώτη συναλλαγή του block που ονομάζεται coinbase transaction και είναι η πρώτη συναλλαγή του block. Εν τέλη οι miners τη χρησιμοποιούν για να αποκτήσουν τα fees και την ανταμοιβή του block και η συναλλαγή ολοκληρώνεται.

3.4 Περιγραφή των πεδίων του dataset crypto_bitcoin και επεξήγηση αυτών σε μορφή πίνακα

BLOCKS

Field name	Type	Mode	Description
hash	STRING	REQUIRED	Αναγνωριστικό του block. Προέρχεται από τον κατακερματισμό του block header από την συνάρτηση SHA256.
size	INTEGER	NULLABLE	Το μέγεθος του block σε bytes
stripped_size	INTEGER	NULLABLE	Το μέγεθος του block που δεν περιλαμβάνει witness data
weight	INTEGER	NULLABLE	Είναι το τριπλάσιο του βασικού μεγέθους, συν το συνολικό μέγεθος
number	INTEGER	REQUIRED	Ο αριθμός των blocks που προηγούνται ενός συγκεκριμένου σε μια αλυσίδα blocks (blockchain)
version	INTEGER	NULLABLE	Στοιχείο του block header που χρησιμεύει στην παρακολούθηση των αλλαγών και ενημερώσεων του πρωτοκόλλου
merkle_root	STRING	NULLABLE	Είναι η ρίζα του Merkle tree που περιλαμβάνει πληροφορία για όλες τις συναλλαγές που βρίσκονται στο block. Τα φύλλα του δέντρου Merkle δημιουργούνται με εφαρμογές της συνάρτησης κατακερματισμού σε TXIDS, ενώ οι υπόλοιποι κόμβοι του είναι αποτέλεσμα της εφαρμογής της Hash-256 σε ζεύγη κόμβων του προηγούμενου στην ιεραρχία επιπέδου
timestamp	TIMESTAMP	REQUIRED	Χρονοσήμανση του block βασισμένη στον Unix time που περιλαμβάνεται στο block header
timestamp_month	DATE	REQUIRED	Ο μήνας δημιουργίας του block όπως ορίζεται στη χρονοσήμανση

Field name	Type	Mode	Description
nonce	STRING	NULLABLE	Προκύπτει από τη φράση “not only used once” και είναι αριθμός που προστίθεται σε κατακερματισμένο block ενός blockchain και, όταν κατακερματιστεί ξανά, ικανοποιεί τους περιορισμούς σε επίπεδο δυσκολίας. Είναι ο αριθμός που όταν υπολογίσουν οι Miners, κερδίζουν σε κρυπτονόμισμα.
bits	STRING	NULLABLE	Το κατώφλι δυσκολίας που ορίζεται στην επικεφαλίδα του block Μικρότερη έκδοση του target αριθμού
coinbase_param	STRING	NULLABLE	Περιεχόμενο (πληροφορία) σχετικό με τη δοσοληψία που δημιούργησε το «νόμισμα»
transaction_count	INTEGER	NULLABLE	Ο αριθμός των συναλλαγών που περιέχει το block

TRANSACTIONS

Fieldname	Type	Mode	Description
hash	STRING	REQUIRED	Αναγνωριστικό που χρησιμοποιείται για τον μοναδικό προσδιορισμό μιας συγκεκριμένης συναλλαγής (TXID)
size	INTEGER	NULLABLE	Το μέγεθος της συναλλαγής σε bytes
virtual_size	INTEGER	NULLABLE	Το εικονικό μέγεθος μιας συναλλαγής. Ένα άλλο είδος

Fieldname	Type	Mode	Description
			μέτρησης vbytes, το οποίο ισοδυναμεί με 4 weight.
version	INTEGER	NULLABLE	Το πρωτόκολλο που χαρακτηρίζει ένα block που περιέχει αυτή τη συναλλαγή
lock_time	INTEGER	NULLABLE	Ο ελάχιστος χρόνος που χρειάζεται μια συναλλαγή για να εξορυχθεί σε ένα block.Εάν locktime<500.000.000 τότε χρειάζονται τόσα block όσο το locktime για να εξορυχθεί το block. Αλλιώς το locktime καθορίζει το χρόνο που θα χρειαστεί για να γίνει η εξόρυξη(σε Unix time) Οι περισσότερες συναλλαγές δεν κάνουν χρήση Lock_time και για αυτό έχουν 0
block_hash	STRING	REQUIRED	Το hash του block που περιέχει αυτή τη συναλλαγή
block_number	INTEGER	REQUIRED	Ο αριθμός του block που περιέχει αυτή τη συναλλαγή
block_timestamp	TIMESTAMP	REQUIRED	Η ημερομηνία δημιουργίας του block που περιέχει αυτή τη συναλλαγή σε Unix time
block_timestamp_month	DATE	REQUIRED	Ο μήνας δημιουργίας του block που περιέχει αυτή τη συναλλαγή

Fieldname	Type	Mode	Description
input_count	INTEGER	NULLABLE	Ο αριθμός των εισόδων
output_count	INTEGER	NULLABLE	Ο αριθμός των εξόδων
input_value	NUMERIC	NULLABLE	Η συνολική τιμή των εισόδων
output_value	NUMERIC	NULLABLE	Η συνολική τιμή των εξόδων
is_coinbase	BOOLEAN	NULLABLE	Έλεγχος αν η συναλλαγή είναι coinbase ή όχι (Αν είναι η πρώτη συναλλαγή στο block)
fee	NUMERIC	NULLABLE	Το χρηματικό «έπαθλο» για τους miners από τη συναλλαγή
inputs	RECORD	REPEATED	Περιεχόμενα των εισόδων
inputs. index	INTEGER	REQUIRED	Αναγνωριστικό της εισόδου
inputs. spent_transaction_hash	STRING	NULLABLE	Το Hash της συναλλαγής που περιέχει την έξοδο που αυτή η είσοδος ξοδεύει
inputs. spent_output_index	INTEGER	NULLABLE	Ο Index αριθμός που η είσοδος αυτή ξοδεύει (VOUT)
inputs. script_asm	STRING	NULLABLE	Συμβολική αναπαράσταση της script γλώσσας που χρησιμοποιείται για το κλείδωμα των εξόδων

Fieldname	Type	Mode	Description
inputs. script_hex	STRING	NULLABLE	Δεκαεξαδική αναπαράσταση της script γλώσσας που χρησιμοποιείται για το κλείδωμα των εξόδων
inputs. sequence	INTEGER	NULLABLE	Αριθμός που υποδηλώνει τη σειρά στην οποία θα γίνει η συναλλαγή
inputs. required_signatures	INTEGER	NULLABLE	Ο αριθμός των υπογραφών που χρειάζονται για γίνει έγκυρη μια πληρωμή
inputs. type	STRING	NULLABLE	Το είδος της διεύθυνσης
inputs. addresses	STRING	REPEATED	Η διεύθυνση που περιέχει αυτή την έξοδο
inputs. value	NUMERIC	NULLABLE	Η τιμή της εξόδου σε satoshi
outputs	RECORD	REPEATED	Περιεχόμενα των εξόδων
outputs. index	INTEGER	REQUIRED	Αναγνωριστικό της εξόδου
outputs. script_asm	STRING	NULLABLE	Συμβολική αναπαράσταση της bitcoin script γλώσσας opcode
outputs. script_hex	STRING	NULLABLE	Δεκαεξαδική αναπαράσταση της bitcoin script γλώσσας opcode
outputs. required_signatures	INTEGER	NULLABLE	Ο αριθμός των υπογραφών που χρειάζονται για να εγκριθεί η

Fieldname	Type	Mode	Description
			πληρωμή της συγκεκριμένης εξόδου
outputs. type	STRING	NULLABLE	Τύπος της διεύθυνσης
outputs. addresses	STRING	REPEATED	Η διεύθυνση που στέλνονται τα χρήματα
outputs. value	NUMERIC	NULLABLE	Η τιμή του output σε satoshi

4 Ενδιαφέρουσες ερωτήσεις και αναλύσεις

ΕΡΩΤΗΜΑΤΑ

1. Ποια περίοδο έχουμε περισσότερα blocks και πόσα είναι αυτά;

```
1. SELECT timestamp,size
2. FROM  `bigquery-public-data.crypto_bitcoin.blocks`
3. WHERE size IN(
4. SELECT max(size) FROM `bigquery-public-data.crypto_bitcoin.blocks`
5. )
```

Row	timestamp	size
1	2020-04-14 01:32:39 UTC	2422858

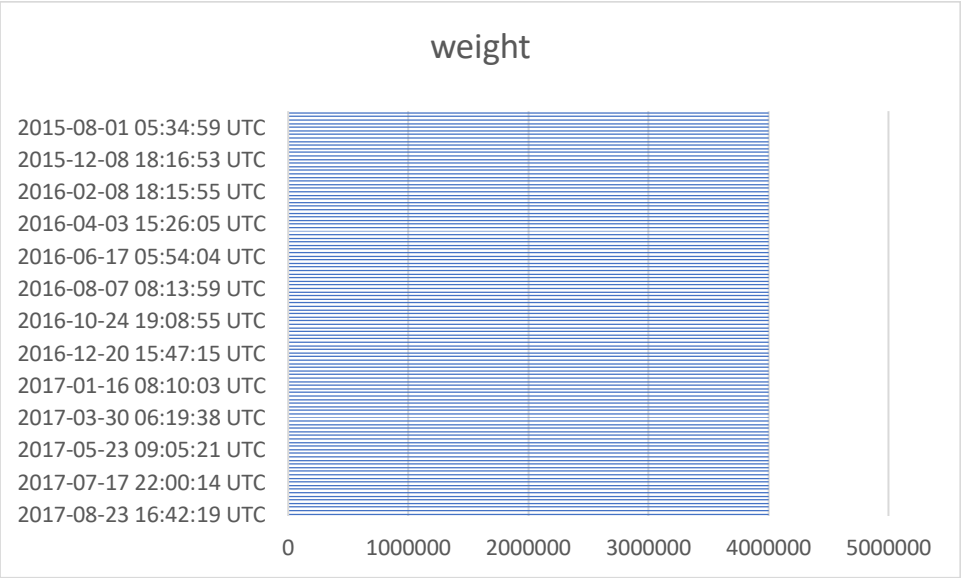
Η περίοδος που παρατηρούμε μεγαλύτερη εμφάνιση block είναι στις 14/4/2020 και ώρα 01:32:39 UTC.
Το μέγεθος των block αυτών είναι 2422858

2. *Υπάρχουν blocks που φτάνουν στο ανώτατο χωρικό όριο; Και αν ναι ποια περίοδο;*

```
1.  SELECT  timestamp,weight FROM `bigquery-public-data.crypto_bitcoin.blocks`
2.  WHERE weight in(
3.  SELECT MAX(weight) FROM `bigquery-public-data.crypto_bitcoin.blocks`
4.  )
5.  ORDER BY timestamp DESC
```

Ένα υποσύνολο των αποτελεσμάτων φαίνεται στην παρακάτω εικόνα:

Row	timestamp	weight
1	2017-08-23 16:42:19 UTC	4000000
2	2017-08-23 12:55:36 UTC	4000000
3	2017-08-17 16:14:29 UTC	4000000
4	2017-08-16 18:09:04 UTC	4000000
5	2017-08-09 11:19:48 UTC	4000000
6	2017-08-08 18:40:39 UTC	4000000
7	2017-08-04 14:24:47 UTC	4000000
8	2017-08-03 03:39:15 UTC	4000000
9	2017-07-22 12:26:42 UTC	4000000



Στο διάγραμμα παρουσιάζονται οι ημερομηνίες και οι χρόνοι που συμβαίνει το γεγονός στις γραμμές, ενώ στις στήλες το μέγεθος αυτών.

Παρατηρούμε ότι ανάμεσα στα έτη 2015-2017 είχαμε μέγιστο μέγεθος 4000000 weight

3. Ποια version των blocks είναι η πιο συχνή;

```
1.  SELECT version,count(version) AS total
2.  FROM `bigquery-public-data.crypto_bitcoin.blocks`
3.  GROUP BY version
4.  ORDER BY total DESC
```

Row	version	total
1	1	215047
2	536870912	162332
3	2	140752
4	3	29304
5	4	27212
6	536870914	15833
7	541065216	10682
8	549453824	9227
9	545259520	8872
10	1073733632	6614

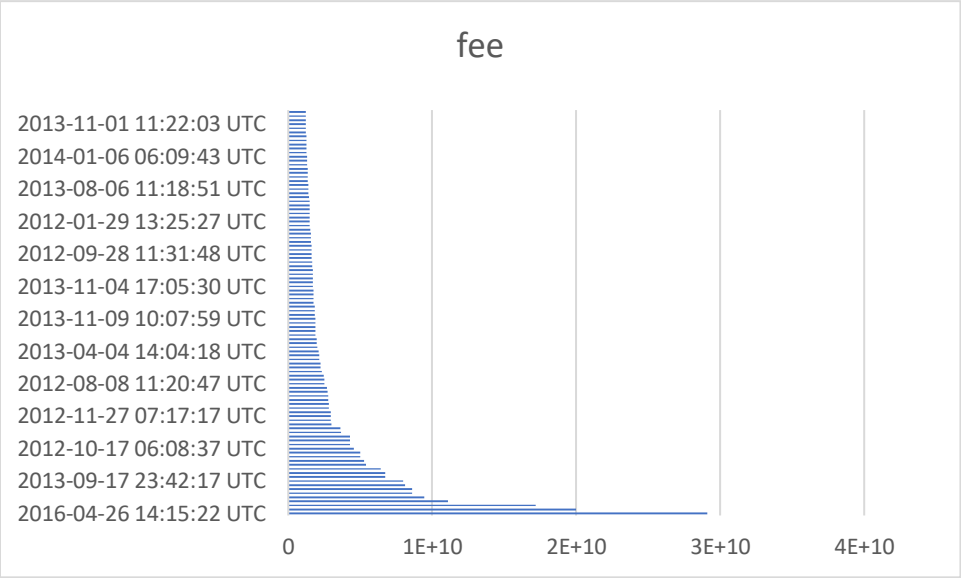
Παρουσιάζονται τα 10 πρώτα versions

4. Χρονολογία 100 blocks με τα περισσότερα fees

```
1.  SELECT fee, block_timestamp
2.  FROM `bigquery-public-data.crypto_bitcoin.transactions`
3.  ORDER BY fee DESC
4.  LIMIT 100
```

Ένα υποσύνολο των αποτελεσμάτων φαίνεται στην παρακάτω εικόνα:

Row	fee	block_timestamp
1	29124090000	2016-04-26 14:15:22 UTC
2	20000000000	2013-08-28 10:45:17 UTC
3	17179869184	2011-12-12 16:57:45 UTC
4	11100000000	2013-01-10 03:51:25 UTC
5	9435425882	2013-03-06 23:15:04 UTC
6	8589984592	2015-04-25 17:36:05 UTC
7	8589934592	2011-12-11 23:39:20 UTC
8	8098000000	2013-09-17 21:23:26 UTC
9	8000000000	2013-09-17 23:42:17 UTC
10	6750450000	2012-01-29 13:16:59 UTC
11	6750450000	2012-01-29 13:26:08 UTC
12	6402609211	2012-10-04 01:29:46 UTC



Στον οριζόντιο άξονα παρουσιάζονται οι χρονολογίες και στον κάθετο άξονα τα fees υπολογισμένα σε Satoshi(1 Satoshi= 0.00000001 ฿)

Παρατηρούμε ότι το 2016 είχαμε μεγάλη αύξηση των fees συγκριτικά με τις χρονιές 2012-2014 που οι τιμές κυμαίνονται στα ίδια περίπου επίπεδα.

5. Ποιο block έχει τις περισσότερες συναλλαγές;

```
1. SELECT `bigquery-public-
   data.crypto_bitcoin.blocks`.hash ,timestamp, transaction_count
2. FROM `bigquery-public-data.crypto_bitcoin.blocks`
3. WHERE transaction_count IN(
4. SELECT MAX(transaction_count)
5. FROM `bigquery-public-data.crypto_bitcoin.blocks`)
```

Row	hash	timestamp	transaction_count
1	00000000000000001080e6de32add416cd6cda29f35ec9bce694fea4b964c7be	2015-08-01 01:06:41 UTC	12239

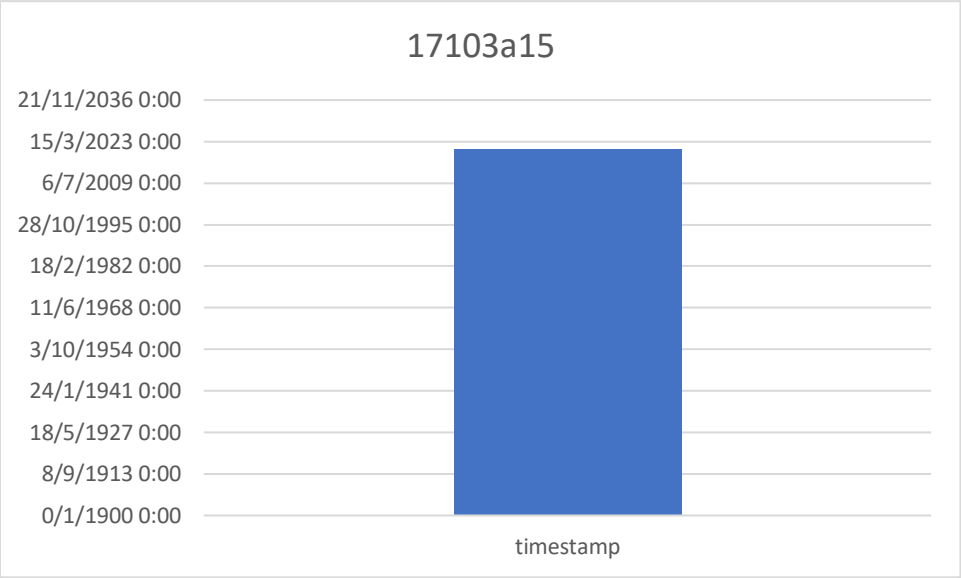
Το block με το παραπάνω hash που δημιουργήθηκε στις 1/8/2015 περιέχει 12239 συναλλαγές

6. *Ποιες περιόδους είχαμε το μικρότερο target-bit αριθμό;*

```
1.  SELECT  timestamp, bits
2.  FROM `bigquery-public-data.crypto_bitcoin.blocks`
3.  WHERE bits IN(
4.  SELECT MIN(bits)
5.  FROM `bigquery-public-data.crypto_bitcoin.blocks`)
6.  ORDER BY timestamp DESC
```

Ένα υποσύνολο των αποτελεσμάτων φαίνεται στην παρακάτω εικόνα:

Row	timestamp	bits
1	2020-11-03 08:17:57 UTC	170e134e
2	2020-11-03 08:17:17 UTC	170e134e
3	2020-11-03 08:17:02 UTC	170e134e
4	2020-11-03 08:16:44 UTC	170e134e
5	2020-11-03 08:14:34 UTC	170e134e
6	2020-11-03 07:35:29 UTC	170e134e
7	2020-11-03 07:22:41 UTC	170e134e
8	2020-11-03 07:22:38 UTC	170e134e
9	2020-11-03 07:15:14 UTC	170e134e
10	2020-11-03 07:00:04 UTC	170e134e
11	2020-11-03 06:59:37 UTC	170e134e
12	2020-11-03 06:50:14 UTC	170e134e



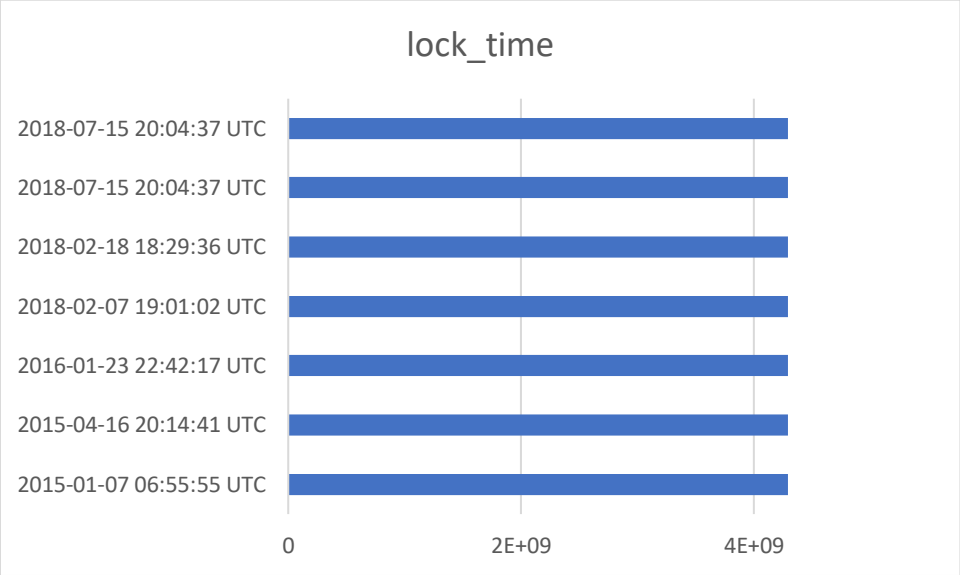
Στον οριζόντιο άξονα παρουσιάζονται οι χρονολογίες με το μικρότερο target-bit αριθμό, ο οποίος ισούται με 17103α15

Παρατηρούμε η μικρότερη τιμή bit είναι αυτή που αναγράφεται στην κορυφή του διαγράμματος και συμβαίνει κατά το διάστημα 13/7/2020 -27/7/2020.

7. Πότε είχαμε μεγαλύτερο locktime;

```
1. SELECT block_timestamp,lock_time
2. FROM `bigquery-public-data.crypto_bitcoin.transactions`
3. WHERE lock_time IN(
4. SELECT MAX(lock_time) FROM `bigquery-public-
   data.crypto_bitcoin.transactions`)
5. ORDER BY block_timestamp ASC
```

Row	block_timestamp	lock_time
1	2015-01-07 06:55:55 UTC	4294967295
2	2015-04-16 20:14:41 UTC	4294967295
3	2016-01-23 22:42:17 UTC	4294967295
4	2018-02-07 19:01:02 UTC	4294967295
5	2018-02-18 18:29:36 UTC	4294967295
6	2018-07-15 20:04:37 UTC	4294967295
7	2018-07-15 20:04:37 UTC	4294967295



Παρατηρούμε ότι η μέγιστη τιμή του Lock_time είναι 4.264.967.295 και λαμβάνει χώρα σε 7 διαφορετικές περιόδους. Η τιμή αυτή είναι μικρότερη από 500.000.000 και άρα συμβολίζεται ο χρόνος σε Unix time που χρειάστηκαν τα blocks για να εξορυχθούν.

8. Ποιο block είχε τις περισσότερες εισόδους και πότε;

```
1.  SELECT input_value,block_timestamp,block_hash
2.  FROM `bigquery-public-data.crypto_bitcoin.transactions`
3.  WHERE input_value in(
```

```
4.  SELECT MAX(input_value) FROM `bigquery-public-
    data.crypto_bitcoin.transactions`)
```

Row	input_value	block_timestamp	block_hash
1	55000000000000	2011-11-16 05:59:08 UTC	00000000000000fb62bbadc0a9dcda556925b2d0c1ad8634253ac2e83ab8382f

Το block με το παραπάνω hash στις 16/11/2011 έχει 55*10^12 εισόδους

9. Ποιο block είχε τις περισσότερες εξόδους;

```
1.  SELECT output_value,block_timestamp,block_hash
2.  FROM `bigquery-public-data.crypto_bitcoin.transactions`
3.  WHERE output_value IN(
4.  SELECT MAX(output_value) FROM `bigquery-public-
    data.crypto_bitcoin.transactions`)
```

Row	output_value	block_timestamp	block_hash
1	55000000000000	2011-11-16 05:59:08 UTC	00000000000000fb62bbadc0a9dcda556925b2d0c1ad8634253ac2e83ab8382f

Το block με το παραπάνω hash στις 16/11/2011 έχει 55*10^12 εξόδους

10. Πότε και ποια συναλλαγή έγινε πρώτη;

```
1.  SELECT block_timestamp,block_hash
2.  FROM `bigquery-public-data.crypto_bitcoin.transactions`
3.  WHERE block_timestamp IN(
4.  SELECT MIN(block_timestamp) FROM `bigquery-public-
    data.crypto_bitcoin.transactions`)
```

Row	block_timestamp	block_hash
1	2009-01-03 18:15:05 UTC	000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

Η πρώτη συναλλαγή έγινε στις 3/1/2009 με το παραπάνω block_hash

11. Για ποιες τιμές target έχουμε μεγαλύτερο Nonce; Πότε συνέβη αυτό;

```
1. SELECT nonce AS max_nonce, bits,timestamp
2. FROM `bigquery-public-data.crypto_bitcoin.blocks`
3. WHERE nonce IN(
4. SELECT MAX(nonce) FROM `bigquery-public-data.crypto_bitcoin.blocks` )
```

Row	max_nonce	bits	timestamp
1	ffffd71	172e6f88	2019-02-22 10:01:28 UTC

Ο αριθμός ffffd71 στο 16αδικό είναι ο μέγιστος που χρησιμοποιήθηκε ποτέ για την ικανοποίηση της δυσκολίας για τον target αριθμό 172e6f88 προκειμένου να εξορυχθεί ένα block

12. Κατά μέσο όρο, τι ποσοστό του μεγέθους των block είναι witness data και τι κανονικά data;

```
1. SELECT SUM(pososto_witness)/COUNT(size)AS m_o_witness,SUM(pososto_normal)/COUN
   T(size) AS m_o_normal
2. FROM(
3. SELECT ((size-
   stripped_size)/size)*100 AS pososto_witness,((stripped_size)/size)*100 AS poso
   sto_normal,size
4. FROM `bigquery-public-data.crypto_bitcoin.blocks`
5. GROUP BY size,stripped_size)
```

Row	m_o_witness	m_o_normal
1	10.808756241623655	89.19124375837626

Τα witness data που περιέχουν δεδομένα για τις υπογραφές των συναλλαγών αποτελούν περίπου το 10% των δεδομένων ενός block.

13. Πόσα blocks έχουν μεγαλύτερο ποσοστό από το μέσο όρο των witness data και πότε συμβαίνει αυτό;

```
SELECT timestamp FROM(
SELECT stripped_size,size,timestamp from `bigquery-public-data.crypto_bitcoin.blocks`)a
FULL OUTER JOIN
(SELECT SUM(pososto_witness)/COUNT(size) AS m_o_witness,size
FROM(
SELECT ((size-stripped_size)/size)*100 AS pososto_witness,((stripped_size)/size)*100 AS pososto_normal,size
FROM `bigquery-public-data.crypto_bitcoin.blocks`
GROUP BY size,stripped_size
)
GROUP BY size)b
ON a.size=b.size
WHERE a.size-stripped_size>m_o_witness
GROUP BY timestamp
ORDER BY timestamp DESC
```

Ένα υποσύνολο με τα 10 πιο πρόσφατα και τα 10 παλαιότερα των αποτελεσμάτων φαίνεται στην παρακάτω εικόνα:

Row	timestamp
1	2020-12-03 17:27:10 UTC
2	2020-12-03 17:16:47 UTC
3	2020-12-03 17:00:17 UTC
4	2020-12-03 16:57:23 UTC
5	2020-12-03 16:47:06 UTC
6	2020-12-03 16:44:29 UTC
7	2020-12-03 16:19:28 UTC
8	2020-12-03 15:41:00 UTC
9	2020-12-03 15:33:40 UTC
10	2020-12-03 15:33:25 UTC

177006	2017-08-24 04:21:53 UTC
177007	2017-08-24 04:07:25 UTC
177008	2017-08-24 03:49:31 UTC
177009	2017-08-24 03:34:51 UTC
177010	2017-08-24 03:30:37 UTC
177011	2017-08-24 02:54:58 UTC
177012	2017-08-24 02:51:10 UTC
177013	2017-08-24 02:44:20 UTC
177014	2017-08-24 02:26:36 UTC
177015	2017-08-24 01:57:37 UTC

Τα αποτελέσματα δείχνουν ότι τέτοια δεδομένα έχουμε από τις 24/8/2017 έως και τις 3/12/2020

14. Για ποια block θέλουμε τις περισσότερες υπογραφές;

```
1. SELECT block_timestamp,block_hash, required_signatures FROM `bigquery-public-
   data.crypto_bitcoin.transactions`,UNNEST(inputs)
2. WHERE required_signatures IN(
3. SELECT MAX(required_signatures) FROM `bigquery-public-
   data.crypto_bitcoin.transactions` ,UNNEST(inputs))
4. ORDER BY block_timestamp DESC
```

Row	block_timestamp	block_hash	required_signatures
1	2014-09-11 18:08:39 UTC	0000000000000000246ab27f014e452487e23faa2cf26cdf40122df4eb16ac2c	16
2	2014-04-26 08:17:02 UTC	0000000000000008205dfa0bef686a2cefe24a1fe138a350215123bc5b20136	16

Για τα παραπάνω blocks χρειάστηκαν οι περισσότερες υπογραφές(16) προκειμένου να εγκριθεί η συναλλαγή

15. Ποιες διευθύνσεις έχουν τα μεγαλύτερα input.values και output.values; Πότε και ποιες ήταν οι τιμές τους

```
1. SELECT addresses,block_timestamp
2. FROM `bigquery-public-data.crypto_bitcoin.transactions`,UNNEST(inputs)
3. WHERE value IN(
```

```
4.  SELECT MAX(value) FROM `bigquery-public-
    data.crypto_bitcoin.transactions` ,UNNEST(inputs))
```

Row	addresses	block_timestamp
1	1M8s2S5bgAzSSzVTeL7zruvMPLvzSkEAuv	2011-11-16 09:17:36 UTC

Στην παραπάνω διεύθυνση είχαμε τα μεγαλύτερα input και output τιμές

5 Συμπεράσματα από τις απαντήσεις των queries

Όλα τα queries εκτελέστηκαν στην πλατφόρμα BigQuery της Google.

Από τις απαντήσεις αυτών παρατηρούμε ότι αν και το κρυπτονόμισμα Bitcoin έχει κάνει την εμφάνισή του το 2009 και από τότε έχουν εμφανιστεί πολλά άλλα, αυτό παραμένει στο προσκήνιο με τη μεγαλύτερη ποσότητα blocks να ανταλλάσσεται το έτος 2020.

Παρόλα αυτά η δημοτικότητά του μειώνεται με το πέρασμα του χρόνου, καθώς μετά το διάστημα 2015-2017 που είχαμε μέγιστο όριο χωρητικότητας σε blocks, η κινητικότητα των συναλλαγών του έχει περιοριστεί, με τον μέγιστο αριθμό να εμφανίζεται το 2011. Το ίδιο συνέβη και με το mining, στο οποίο κατά το διάστημα 2012-2014 υπήρχε μεγάλη αποδοτικότητα στις αμοιβές, με το μεγαλύτερο όμως κέρδος-αμοιβή από τη διαδικασία αυτή να επιτυγχάνεται την περίοδο του 2016. Μετά από αυτό το διάστημα παρατηρείται ότι η δυσκολία εξόρυξης (target) ενός block έχει μικρότερες τιμές το έτος 2020, κάτι που αιτιολογεί επίσης και τη μείωση του ανταγωνισμού στο mining.

Αξίζει να επισημανθεί το γεγονός ότι, στην ακμή του η ασφάλεια του δικτύου bitcoin ήταν πολύ μεγάλη, εφόσον χρειάζονταν 16 υπογραφές για να επικυρωθεί μια συναλλαγή και ότι επίσης υπήρχε μεγάλη εγγύηση προστασίας στα δεδομένα των blocks αφού η πληροφορία που αφορούσε αποκλειστικά τις υπογραφές των συναλλαγών αποτελούσε κατά μέσο όρο το 10% του συνολικού μεγέθους.

6 Βιβλιογραφία

1. Jeffrey Mazer, 2010, *Demystifying Cryptocurrencies, Blockchain, and ICOs*, Available at: <https://www.toptal.com/finance/financial-consultants/cryptocurrency-market>, [Accessed 14 August 2020]

2. Blockchain ETL,2020[online] Available at: <https://github.com/blockchain-etl>, [Accessed 14 August 2020]

3. Will, 2018, Available at: < https://www.kaggle.com/slickwilly/bigquery-bitcoin-blockchain-data/data>, [Accessed 15 August 2020]

4. Wikipedia, last edited on 27 July 2020, *Peer-to-peer*, Available at: <https://en.wikipedia.org/wiki/Peer-to-peer>

5. Satoshi Nakamoto, *Bitcoin: A Peer-to-PeerElectronic Cash System,*2008.

6. Harsh Agrawal, 6 September 2019, Available at: <https://coinsutra.com/bitcoin-hash/>

7. Bitcoin community, Established April 14, 2010, *Bitcoin Wiki*, , Available at: <https://en.bitcoin.it/wiki/Main_Page>, [Accessed 16 August 2020]

8. Bitcoin Team, 2009, *Bitcoin Developer Guide*, Available at: <https://btcinformation.org/en/developer-guide#transactions>, [Accessed 16 August 2020]

9. Techopedia, February 6, 2018, *Cryptography*, Available at: <https://www.techopedia.com/definition/1770/cryptography>

10. John Ma, 2017, Available at: < https://academy.binance.com/glossary/flippening>, [Accessed 16 August 2020]

11. Google cloud, Last updated 2020-06-29 UTC, *Introduction to BigQuery,* Video(Online), Available at: <https://cloud.google.com/bigquery/what-is-bigquery>

12. Βικιπαιδεία, Τελευταία τροποποίηση 17 Δεκεμβρίου 2019, *Κρυπτανάλυση*, Διαθέσιμο στον διαδικτυακό τόπο: <https://el.wikipedia.org/wiki/%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%B1%CE%BD%CE%AC%CE%BB%CF%85%CF%83%CE%B7>

13. Βικιπαιδεία, Τελευταία τροποποίηση 1 Ιουλίου 2020 , *Δίκτυο Bitcoin*, Διαθέσιμο στον διαδικτυακό τόπο: <https://el.wikipedia.org/wiki/%CE%94%CE%AF%CE%BA%CF%84%CF%85%CE%BF_Bitcoin>

14. Βικιπαιδεία, Τελευταία τροποποίηση 3 Ιουνίου 2020, *Υπολογιστικό νέφος,* Διαθέσιμο στον διαδικτυακό τόπο: <https://el.wikipedia.org/wiki/%CE%A5%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CE%B9%CE%BA%CF%8C_%CE%BD%CE%AD%CF%86%CE%BF%CF%82>

15. Βικιπαιδεία, Τελευταία τροποποίηση 12 Οκτωβρίου 2019, *Λειτουργικό σύστημα,* Διαθέσιμο στον διαδικτυακό τόπο: <https://el.wikipedia.org/wiki/%CE%9B%CE%B5%CE%B9%CF%84%CE%BF%CF%85%CF%81%CE%B3%CE%B9%CE%BA%CF%8C_%CF%83%CF%8D%CF%83%CF%84%CE%B7%CE%BC%CE%B1>

16. Βικιπαιδεία, Τελευταία τροποποίηση 26 Αυγούστου 2018, *Παράλληλα και κατανεμημένα συστήματα,* Διαθέσιμο στον διαδικτυακό τόπο: <https://el.wikipedia.org/wiki/%CE%A0%CE%B1%CF%81%CE%AC%CE%BB%CE%BB%CE%B7%CE%BB%CE%B1_%CE%BA%CE%B1%CE%B9_%CE%BA%CE%B1%CF%84%CE%B1%CE%BD%CE%B5%CE%BC%CE%B7%CE%BC%CE%AD%CE%BD%CE%B1_%CF%83%CF%85%CF%83%CF%84%CE%AE%CE%BC%CE%B1%CF%84%CE%B1>

17. Αναστασία Ξαρχάκου, Οκτώβριος 2017, *ΤΟ ΨΗΦΙΑΚΟ ΝΟΜΙΣΜΑ:Η ΘΕΩΡΗΤΙΚΗ,ΟΙΚΟΝΟΜΙΚΗ ΚΑΙ ΤΕΧΝΟΛΟΓΙΚΗ ΠΡΟΣΕΓΓΙΣΗ ΤΟΥ,* Διπλωματική Εργασία[Online], Πανεπιστήμιο Μακεδονίας, Διαθέσιμο στον διαδικτυακό τόπο: <https://dspace.lib.uom.gr/bitstream/2159/21023/4/XarchakouAnastasiaMsc2017.pdf>, [Πρόσβαση στις 16 Αυγούστου 2020].

18. Kriptomat, Σεπτέμβριος 2019, *Τι είναι τα Κρυπτονομίσματα; Πράγματα που Πρέπει να Γνωρίζετε,* Διαθέσιμο στον διαδικτυακό τόπο: <https://kriptomat.io/gr/kryptonomismata/ti-einai-kryptonomisma/> [Πρόσβαση στις 16 Αυγούστου 2020]

19. Βικιπαιδεία, Τελευταία τροποποίηση 4 Απριλίου 2020, *Κρυπτογραφία*, Διαθέσιμο στον διαδικτυακό τόπο: <https://el.wikipedia.org/wiki/%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%B1%CF%86%CE%AF%CE%B1>

20. Δημήτριος Ταχμετζίδης, Δεκέμβριος 2017, *ΧΡΗΣΗ ΚΑΙ ΕΦΑΡΜΟΓΗ ΤΟΥ BITCOIN ΣΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΑΓΟΡΕΣ*, Διπλωματική Εργασία[Online], ΤΕΙ Ηπείρου, Διαθέσιμο στον διαδικτυακό τόπο: <http://apothetirio.teiep.gr/xmlui/bitstream/handle/123456789/8511/%CF%80%CF%84%CF%85%CF%87%CE%B9%CE%B1%CE%BA%CE%AE%20bitcoin%20%CE%A4%CE%95%CE%9B%CE%99%CE%9A%CE%97.pdf?sequence=1>