ΧΑΡΟΚΟΠΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

ΣΧΟΛΗ ΨΗΦΙΑΚΗΣ ΤΕΧΝΟΛΟΓΙΑΣ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΜΑΤΙΚΗΣ

Το blockchain ως μια σύγχρονη βάση δεδομένων και η σημασία του στα κρυπτονομίσματα.

Πτυχιακή εργασία

Δαγκλής Γεώργιος

Αθήνα, 2021

ΧΑΡΟΚΟΠΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

ΣΧΟΛΗ ΨΗΦΙΑΚΗΣ ΤΕΧΝΟΛΟΓΙΑΣ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΜΑΤΙΚΗΣ

Τριμελής Εξεταστική Επιτροπή

ΒΑΡΛΑΜΗΣ ΗΡΑΚΛΗΣ
Αναπληρωτής Καθηγητής, Πληροφορικής και Τηλεματικής,
Χαροκόπειο Πανεπιστήμιο

ΔΗΜΗΤΡΑΚΟΠΟΥΛΟΣ ΓΕΩΡΓΙΟΣ
Αναπληρωτής Καθηγητής, Πληροφορικής και Τηλεματικής,
Χαροκόπειο Πανεπιστήμιο

ΤΣΕΡΠΕΣ ΚΩΝΣΤΑΝΤΙΝΟΣ
Αναπληρωτής Καθηγητής, Πληροφορικής και Τηλεματικής,
Χαροκόπειο Πανεπιστήμιο

Ο Δαγκλής Γεώργιος

δηλώνω υπεύθυνα ότι:

1) Είμαι ο κάτοχος των πνευματικών δικαιωμάτων της πρωτότυπης αυτής εργασίας και από όσο γνωρίζω η εργασία μου δε συκοφαντεί πρόσωπα, ούτε προσβάλει τα πνευματικά δικαιώματα τρίτων.

2) Αποδέχομαι ότι η ΒΚΠ μπορεί, χωρίς να αλλάξει το περιεχόμενο της εργασίας μου, να τη διαθέσει σε ηλεκτρονική μορφή μέσα από τη ψηφιακή Βιβλιοθήκη της, να την αντιγράψει σε οποιοδήποτε μέσο ή/και σε οποιοδήποτε μορφότυπο καθώς και να κρατά περισσότερα από ένα αντίγραφα για λόγους συντήρησης και ασφάλειας.

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να εκμεταλλευτώ αυτή σελίδα για να εκφράσω την βαθύτατη του ευγνωμοσύνη και σεβασμό στον επιβλέπων καθηγητή της μελέτης και πτυχιακής εργασίας μου, τον κ. Ηρακλή Βαρλάμη για την πολύτιμη βοήθεια και υπομονή που έδειξε στο πρόσωπό μου. Τον ευχαριστώ επίσης και για τη στήριξη και τις συμβουλές που έλαβα όλο αυτό το διάστημα.

Επίσης θα ήθελα να ευχαριστήσω την οικογένεια μου και τους φίλους μου για την οικονομική και ψυχολογική υποστήριξη καθώς και για τις συμβουλές που δεν με άφησαν να πέσω αλλά με παρότρυναν σε όλη αυτή την περίοδο.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Περίληψη στα Ελληνικά

Η πληροφορική αναπτύσσεται συνέχεια. Μαζί της αναπτύσσονται και όλες οι τεχνολογίες και παροχές που μας ξεκλειδώσει. Από τις τηλεπικοινωνίες, την τηλεργασία μέχρι και την αποθήκευση δεδομένων. Πάντα ήταν ανάγκη να αποθηκεύουμε πληροφορία για να ανατρέξουμε σε αυτή όταν την χρειαζόμασταν. Αυτό στην αρχή γινόταν με τετράδια, δηλαδή με μία φυσική μορφή. Ωστόσο όσο η τεχνολογία προχωρούσε, το επόμενο μέσο αποθήκευσης πληροφορίας έγιναν οι βάσεις δεδομένων. Αποτελούμενες από πίνακες με σειρές και στήλες, οι βάσεις δεδομένων περιείχαν πληροφορία εύκολα προσβάσιμη για το χρήστη. Ωστόσο οι βάσεις είχαν ένα θέμα. Έπρεπε να στεγάζονται σε έναν και μόνο υπολογιστή (σήμερα μπορεί ναι είναι πολλοί διάσπαρτοι υπολογιστές που διαμοιράζονται τα δεδομένα) και έπρεπε ο χρήστης να έχει πρόσβαση σε αυτόν. Εδώ έρχεται πάλι η ανάπτυξη να διορθώσει τα πράγματα. Δημιουργούνται τα blockchains που αποτελούν πλέον ένα σύστημα στο οποίο διατηρείται η πληροφορία σε διάφορους υπολογιστές που είναι συνδεδεμένοι σε δίκτυο ομότιμων. Έτσι πολλοί υπολογιστές συμμετέχουν σε αυτό. Αυτή την τεχνολογία την εκμεταλλεύτηκαν τα κρυπτονομίσματα. Τα κρυπτονομίσματα είναι ένα ψηφιακό νόμισμα στο οποίο οι συναλλαγές επαληθεύονται και τα αρχεία διατηρούνται από ένα αποκεντρωμένο σύστημα που χρησιμοποιεί κρυπτογραφία και όχι από μια κεντρική αρχή. Σε αυτή την πτυχιακή θα επιχειρήσουμε να κατανοήσουμε την τεχνολογία του blockchain, τι το διαχωρίζει και τι το συνδέει με τις βάσεις δεδομένων. Επίσης θα αναλύσουμε την έννοια του κρυπτονομίσματος, μέσα από το πιο γνωστό κρυπτονόμισμα που είναι το bitcoin. Τέλος θα αναφερθούμε στα τεχνικά χαρακτηριστικά που ενώνουν τα blockchain με τα κρυπτονομίσματα και σε τι βοηθάει αυτό.

Λέξεις κλειδιά: blockchain, βάσεις δεδομένων, bitcoin, κρυπτονόμισμα

Abstract ή Περίληψη στα Αγγλικά

Computer science is constantly evolving. With it, all the technologies and benefits that unlock us are developed. From telecommunications, teleworking to data storage. We always needed to store information to refer to when we needed it. This was initially done with notebooks, ie in a physical form. However, as technology advanced, the next means of storing information became databases. Consisting of rows and columns, the databases contained information that was easily accessible to the user. However, the bases had an issue. They had to be housed on a single computer (today there may be many scattered computers sharing data) and the user had to have access to it. Here comes development again to fix things. Blockchains are created which are now a system in which information is stored on various computers that are connected to a peer network. So many computers are involved in this. This technology was exploited by cryptocurrencies. Cryptocurrencies are a digital currency in which transactions are verified and records are maintained by a decentralized system that uses cryptography rather than a central authority. In this dissertation we will try to understand blockchain technology, what separates it and what connects it to databases. We will also analyze the meaning of cryptocurrency, through the most famous cryptocurrency which is bitcoin. Finally, we will talk about the technical features that blockchains associate with cryptocurrencies and what it helps.

Keywords: blockchain, database, bitcoin, cryptcurency

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

Crypto	Κρυπτονόμισμα
DB	Βάση δεδομένων
SHA-256	Secure Hash Algorithm 256 bits
SVP	Simple verification payment
ETH	Ethereum
BTC	Bitcoin
UTXO	Unspent transaction output

ΕΙΣΑΓΩΓΗ

Η περίοδος που ζούμε είναι παράξενη από πολλές μεριές. Ένα μεγάλο μέρος αυτής της παραξενιάς οφείλεται στους υπολογιστές και την πληροφορική. Αυτή η επιστήμη έχει ανοίξει διάπλατα τους ορίζοντες των δυνατοτήτων που μπορούμε να φτάσουμε. Δημιουργεί ωστόσο και συγχύσεις μεταξύ εννοιών που προϋπήρχαν πολύ καιρό τώρα. Εκτός από αυτό, κάθε χρόνος που περνάει αναπτύσσονται οι ήδη υπάρχουσες τεχνολογίες που η πληροφορική μας σύστησε. Μια από αυτές είναι και οι βάσεις δεδομένων. Πλέον δεν μας αρκούν, και ψάχνουμε καινούριους τρόπους να αναπαράγουμε βάσεις δεδομένων. Ένας από αυτούς τους τρόπους είναι το blockchain. Το blockchain είναι ένας μηχανισμός αποκεντρωμένης αποθήκευσης δεδομένων. Αποτελείται από blocks, που είναι tables πληροφοριών με συγκεκριμένο μέγεθος. Ένα σύνολο από blocks ενώνεται μεταξύ τους σε ένα μια αλυσίδα. Αυτή ήταν και η ιδέα αυτής της νέας τεχνολογίας. Μεταξύ άλλων αυτή η τεχνολογία βοήθησε στην ανάπτυξη των κρυπτονομισάτων. Τα κρυπτονομίσματα

είναι ψηφιακά νομίσματα με συνεχώς μεταβαλλόμενη αξία που χρησιμοποιούνται για διαδικτυακές αγορές.

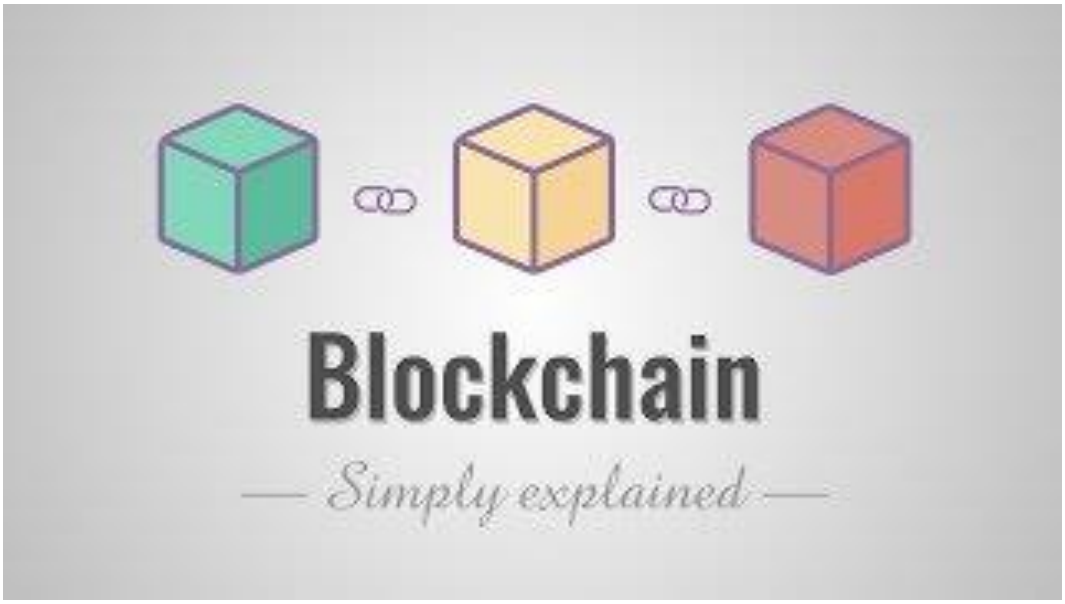
Η εργασία έχει ως σκοπό να αναλύσει τη σχέση της τεχνολογίας του blockchain με τις βάσεις δεδομένων και να αναλύσει τη χρήση του στα σύγχρονα και συνεχώς ανερχόμενα κρυπτονομίσματα.

Η εργασία έχει τρία κεντρικά κεφάλαια. Στο πρώτο θα αναλύσουμε την τεχνολογία του blockchain σε σχέση με τις βάσεις δεδομένων.

Στο δεύτερο, θα αναλύσουμε την έννοια του των κρυπτονομισμάτων μέσω του πιο διαδεδομένου από αυτά, του bitcoin.

Στο τρίτο θα ενώσουμε αυτές τις δύο έννοιες και θα εξηγήσουμε κάποια τεχνικά χαρακτηριστικά μεταξύ blockchain και bitcoin.

Στο τέταρτο θα προβούμε σε συμπεράσματα σχετικά με τη χρήση του blockchain στο bitcoin και γενικά στα κρυπτονομίσματα.



Εικόνα 1 Απλή γραφική αναπαράσταση blockchain (https://www.youtube.com/watch?v=SSo_EIwHSd4)

ΚΕΦ.1:Blockchain και Βάσεις δεδομένων

Ορισμός blockchain και βάσης δεδομένων

Τα blockchain μπορεί να είναι φαινομενικά ένας παράξενος όρος για τον απλό άνθρωπο αλλά και για κάποιον πιο εξοικειωμένο με την πληροφορική. Γι' αυτό μπορεί να υπάρχουν πολλές απορίες σχετικα με την τεχνολογία αυτή. Ωστόσο είναι μία σχετικά απλή τεχνολογία στον πυρήνα του. Το blockchain είναι ένα σύστημα καταγραφής πληροφοριών με τρόπο που καθιστά δύσκολη ή αδύνατη την αλλαγή, το χακάρισμα ή την εξαπάτηση του συστήματος. Το blockchain είναι ουσιαστικά ένα ψηφιακό λογιστικό βιβλίο συναλλαγών που αντιγράφεται και διανέμεται σε ολόκληρο το δίκτυο υπολογιστών που ανήκουν στο blockchain. Σε πολύ γενικό πλαίσιο το blockchain ανήκει σε μια κατηγορία των σύγχρονων βάσεων δεδομένων. Άρα για να καταλάβουμε εξ ολοκλήρου την τεχνολογία του blockchain, θα πρέπει να κατανοήσουμε αυτή των σύγχρονων βάσεων δεδομένων.

Γενικά μια βάση δεδομένων είναι ένα σύνολο πληροφοριών και δεδομένων το οποίο είναι ηλεκτρονικά αποθηκευμένο σε έναν υπολογιστή. Αυτή η πληροφορία και η πληθώρα των δεδομένων είναι γενικά αποθηκευμένη και δομημένη με τη μορφή των tables. Αυτό συμβαίνει διότι με αυτόν τον τρόπο επιτυγχάνεται πιο εύκολα το φλιτάρισμα αλλά και η αναζήτηση συγκεκριμένης πληροφορίας. Άρα εδώ έρχεται το λογικό ερώτημα του ποια είναι η διαφορά μεταξύ της αποθήκευσης πληροφορίας σε ένα spreadsheet ας πούμε με το να αποθηκεύουμε τις ίδιες πληροφορίες σε μια βάση δεδομένων; Η απάντηση έρχεται στη χρηστικότητα του "spreadsheet" και της βάσης. Οι βάσεις δεδομένων έχουν δημιουργηθεί όχι μόνο με σκοπό να φιλοξενούν τεράστιες ποσότητες δεδομένων και πληροφορίας αλλά και να μπορούν να τις χειρίζονται πολλά άτομα ταυτόχρονα να επιτρέπουν επερωτήσεις κλπ. Αντίθετα, τα "spreadsheets" έχουν δημιουργηθεί για να τα χειρίζεται ένα άτομο ή μια μικρή ομάδα ανθρώπων και να φιλοξενούν μικρές σχετικά ποσότητες πληροφορίας.

ID	NAME	CLASS
1	John Deo	Four
2	Max Ruin	Three
3	Arnold	Three
4	Krish Star	Four
5	John Mike	Four

Εικόνα 2 Απλή αναπαράσταση πίνακα βάσης δεδομένων (https://examplanning.com/what-is-database-its-types-and-examples/)

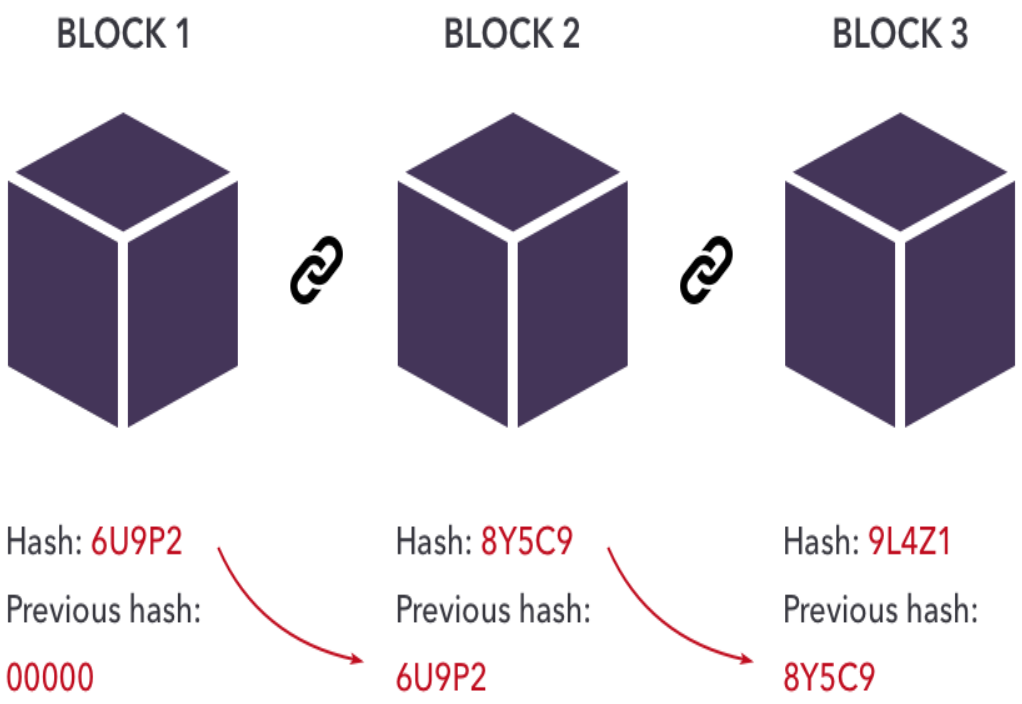
Οι μεγάλες βάσεις δεδομένων το καταφέρνουν αυτό διότι στεγάζουν τα δεδομένα τους σε servers που είναι φτιαγμένοι σε πολύ ισχυρούς υπολογιστές. Κάποιοι από αυτούς τους "servers" είναι φτιαγμένοι από πολλαπλούς ισχυρούς υπολογιστές (εκατοντάδες, ακόμα και χιλιάδες υπολογιστές) για να έχουν την απαραίτητη ισχύ αλλά αποθηκευτικό χώρο για να μπορούν να χειρίζονται πολλαπλούς χρήστες ταυτόχρονα. Αν και δεν υπάρχει όριο στο πόσοι άνθρωποι έχουν δικαίωμα να χειρίζονται αυτές τις βάσεις ή τα "spreadsheets", ανήκουν κυρίως σε εταιρίες και τις προσέχουν συγκεκριμένοι προγραμματιστές που έχει ορίσει η εκάστοτε εταιρία, έχουν τον απόλυτο έλεγχο πάνω τους και πάνω στα δεδομένα που έχουν. Άρα το ερώτημα παραμένει, σε τι διαφέρει μια βάση δεδομένων από ένα blockchain;

1.1:Διαφορές blockchain και βάσεων δεδομένων

1.1.1:Δομή αποθηκευτικού χώρου

Μία βασική διαφορά μεταξύ μίας τυπικής βάσης δεδομένων και ενός blockchain είναι ο τρόπος που έχει δομηθεί ο αποθηκευτικός χώρος καθεμίας από τις δύο τεχνολογίες. Ένα blockchain συλλέγει πληροφορίες και τις κατατάσσει σε ομάδες, που είναι γνωστές και σαν blocks, που κρατάνε σετ πληροφοριών. Το κάθε block έχει συγκεκριμένη χωρητικότητα και όταν γεμίσει συνδέεται με το προηγούμενο block δημιουργώντας μια αλυσίδα (chain) από πολλά blocks. Από εκεί δημιουργήθηκε και το όνομα της τεχνολογίας blockchain (chain that consists of blocks). Κάθε νέα πληροφορία δημιουργεί ένα καινούριο block που περιμένει να γεμίσει και να προστεθεί στην αλυσίδα.

Μία βάση δεδομένων, δομεί τις πληροφορίες της σε πίνακες αντί για blocks ενωμένα σε μία αλυσίδα. Αυτό το σύστημα υποδηλώνει πως αν και όλα τα blockchains μπορούν να θεωρηθούν βάσεις δεδομένων, δεν μπορούν να θεωρηθούν όλες οι βάσεις δεδομένων ως blockchains. Αυτό το σύστημα καθιστά επίσης εγγενώς ένα μη αναστρέψιμο χρονοδιάγραμμα δεδομένων όταν εφαρμόζεται σε αποκεντρωμένο χαρακτήρα. Όταν ένα block γεμίσει γίνεται αναπόσπαστο μέρος του χρονοδιαγράμματος της αλυσίδας και δεν μπορεί να σπάσει. Κάθε block αποκτά συγκεκριμένη χρονική σήμανση (timestamp) όταν γίνεται μέρος της αλυσίδας.



Εικόνα 3 Blocks και αλυσίδες (https://www.ig.com/en/trading-strategies/what-is-blockchain-technology--200710)

1.1.2: Αποκέντρωση

Στο blockchain η αποκέντρωση (decentralization) είναι ουσιαστικά η μεταφορά της λήψης των αποφάσεων και του ελέγχου του blockchain από συγκεκριμένη οντότητα (ένας άνθρωπος, μία εταιρία) σε ένα κατανεμημένο δίκτυο. Τα αποκεντρωμένα δίκτυα καταφέρνουν να μη εξαρτώνται από το την εμπιστοσύνη μεταξύ των συμμετεχόντων αποτρέπουν την ικανότητά τους να ασκούν εξουσία ή έλεγχο ο ένας πάνω στον άλλο με τρόπους που υποβαθμίζουν τη λειτουργικότητα του δικτύου. Με την αποκέντρωση της διαχείρισης και της πρόσβασης σε πόρους σε μια εφαρμογή, μπορεί να επιτευχθεί μεγαλύτερη και πιο δίκαιη εξυπηρέτηση. Η αποκέντρωση τυπικά έχει κάποιες αντισταθμίσεις, όπως χαμηλότερη απόδοση συναλλαγών, αλλά ιδανικά, οι αντισταθμίσεις αξίζουν τη βελτιωμένη σταθερότητα και τα επίπεδα υπηρεσιών που παράγουν.

1.1.2.1:Οφέλη από την αποκέντρωση

Βελτίωση της εναρμόνισης δεδομένων

Οι εταιρείες συχνά ανταλλάσσουν δεδομένα με τους συνεργάτες τους. Αυτά τα δεδομένα, με τη σειρά τους, τυπικά μετατρέπονται και αποθηκεύονται στα σιλό δεδομένων κάθε μέρους, μόνο για να εμφανιστούν ξανά όταν πρέπει να περάσουν προς τα κάτω. Κάθε φορά που τα δεδομένα μετασχηματίζονται, ανοίγουν ευκαιρίες για απώλεια δεδομένων ή λανθασμένα δεδομένα για είσοδο στη ροή εργασίας. Έχοντας μια αποκεντρωμένη αποθήκευση δεδομένων, κάθε οντότητα έχει πρόσβαση σε μια κοινή προβολή των δεδομένων σε πραγματικό χρόνο.

Μειώνει τα σημεία αδυναμίας

Η αποκέντρωση μπορεί να μειώσει τα σημεία αδυναμίας σε συστήματα όπου μπορεί να υπάρχει μεγάλη εξάρτηση από συγκεκριμένους παράγοντες. Αυτά τα αδύνατα σημεία θα μπορούσαν να οδηγήσουν σε συστημικές αποτυχίες, συμπεριλαμβανομένης της μη παροχής υποσχόμενων υπηρεσιών ή αναποτελεσματικών υπηρεσιών λόγω εξάντλησης πόρων, περιοδικών διακοπών, συμφόρησης, έλλειψης επαρκών κινήτρων για καλή εξυπηρέτηση ή διαφθοράς.

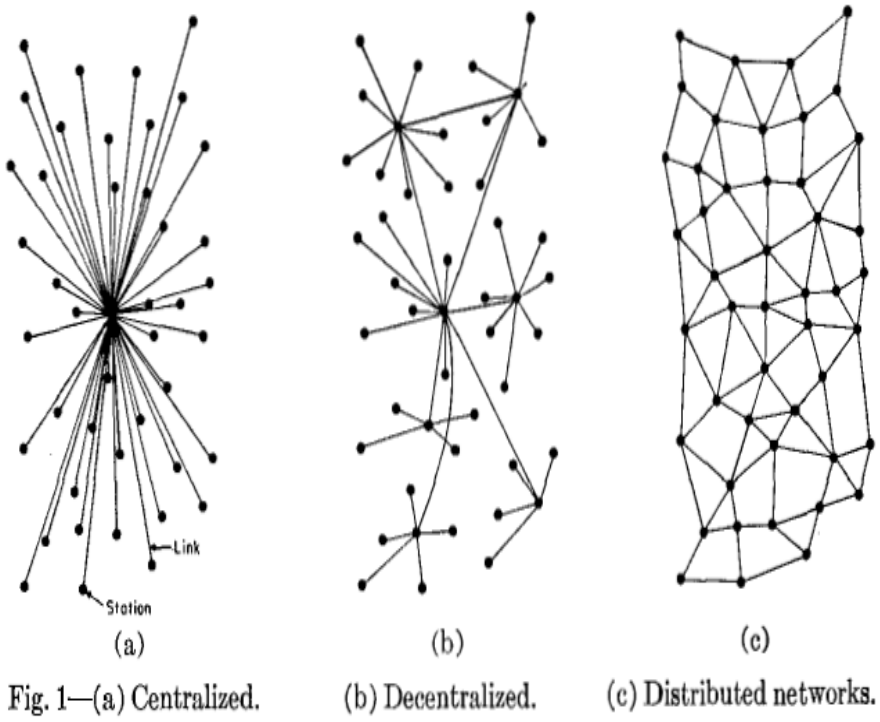
Βελτιστοποιεί τη διανομή πόρων

Η αποκέντρωση μπορεί επίσης να συμβάλει στη βελτιστοποίηση της κατανομής των πόρων, έτσι ώστε οι υποσχόμενες υπηρεσίες να παρέχονται με καλύτερη απόδοση και συνέπεια, καθώς και μειωμένη πιθανότητα καταστροφικής αποτυχίας.

Περιβάλλον χωρίς την απαίτηση εμπιστοσύνης μεταξύ των συμμετεχόντων.

Σε ένα αποκεντρωμένο δίκτυο blockchain, κανείς δεν πρέπει να γνωρίζει ή να εμπιστεύεται κανέναν άλλο. Κάθε μέλος στο δίκτυο έχει ένα αντίγραφο των ίδιων ακριβώς δεδομένων με τη μορφή κατανεμημένου βιβλίου (distributed ledger). Εάν

το βιβλίο του μέλους τροποποιηθεί ή αλλοιωθεί με οποιονδήποτε τρόπο, θα απορριφθεί από την πλειοψηφία των μελών στο δίκτυο.



Εικόνα 4 Κεντρικά, αποκεντρωμένα, κατανεμημένα δίκτυα (https://medium.com/delta-exchange/centralized-vs-decentralized-vs-distributed-41d92d463868)

1.1.3: Διαφάνεια

Λόγω της αποκεντρωμένης φύσης του blockchain του Bitcoin, όλες οι συναλλαγές μπορούν να προβληθούν με διαφάνεια είτε με έναν προσωπικό κόμβο είτε χρησιμοποιώντας εξερευνητές blockchain που επιτρέπουν σε οποιονδήποτε να βλέπει τις συναλλαγές να γίνονται ζωντανά. Κάθε κόμβος έχει το δικό του αντίγραφο της αλυσίδας που ενημερώνεται καθώς επιβεβαιώνονται και προστίθενται νέα μπλοκ. Αυτό σημαίνει ότι αν το θέλατε, μπορείτε να παρακολουθείτε το Bitcoin. Για παράδειγμα, το χρηματιστήριο είχε παραβιαστεί στο παρελθόν. Αυτό είχε σαν αποτέλεσμα εκείνοι που κατείχαν Bitcoin στο χρηματιστήριο, τα έχασαν όλα για

πάντα. Ο εκάστοτε χάκερ που πραγματοποίησε αυτή την επίθεση παρέμεινε εντελώς ανώνυμος χωρίς να μπορέσει να βρεθεί. Ωστόσο, τα bitcoins που κλάπηκαν και εξήχθησαν είναι εύκολα ανιχνεύσιμα αν μετακινηθούν ή αν ξοδευτούν κάπου αλλού. Εκ του αποτελέσματος καταλαβαίνουμε πως στις συναλλαγές, το blockchain δεν κρατάει το άτομο που έκανε την συναλλαγή αλλά κρατάει πληροφορίες για την συναλλαγή αυτή κάθε αυτή.

1.2: Είναι το Blockchain ασφαλές;

Η τεχνολογία Blockchain καλύπτει τα θέματα ασφάλειας και εμπιστοσύνης με διάφορους τρόπους. Πρώτον, τα νέα μπλοκ αποθηκεύονται πάντα γραμμικά και χρονολογικά. Δηλαδή, προστίθενται πάντα στο «τέλος» του blockchain. Αν ρίξετε μια ματιά στο blockchain του Bitcoin, θα δείτε ότι κάθε μπλοκ έχει μια θέση στην αλυσίδα, που ονομάζεται "ύψος". Από τον Νοέμβριο του 2020, το ύψος του μπλοκ είχε φτάσει τα 656.197 μπλοκ μέχρι τώρα.

Μετά την προσθήκη ενός μπλοκ στο τέλος του blockchain, είναι πολύ δύσκολο να επιστρέψετε και να αλλάξετε το περιεχόμενο του μπλοκ, εκτός εάν η πλειοψηφία κατέληξε σε συναίνεση για να το κάνει. Αυτό συμβαίνει επειδή κάθε μπλοκ περιέχει το δικό του hash, μαζί με το hash του μπλοκ πριν από αυτό, καθώς και την προαναφερθείσα χρονική σφραγίδα. Οι κώδικες Hash δημιουργούνται από μια μαθηματική συνάρτηση που μετατρέπει τις ψηφιακές πληροφορίες σε μια σειρά αριθμών και γραμμάτων. Εάν αυτές οι πληροφορίες τροποποιηθούν με οποιονδήποτε τρόπο, αλλάζει και ο κώδικας κατακερματισμού.

Παρακάτω υπάρχει ένα παράδειγμα που αναλύει τη σημαντικότητα της ασφάλειας του blockchain. Ας υποθέσουμε ότι ένας χάκερ θέλει να αλλάξει το blockchain και να κλέψει Bitcoin από όλους τους άλλους. Εάν οι χάκερ μετά επρόκειτο να τροποποιήσουν το δικό τους αντίγραφο, δεν θα ήταν πλέον ευθυγραμμισμένο με το αντίγραφο όλων των άλλων. Όταν όλοι οι άλλοι

διασταυρώνουν τα αντίγραφά τους μεταξύ τους, θα έβλεπαν αυτό το αντίγραφο να ξεχωρίζει από τα άλλα και ότι αυτή είναι η εκδοχή της αλυσίδας που έχει ο χάκερ. Έτσι αυτή η εκδοχή της αλυσίδας θα απορριφθεί ως παράνομη.

Η επιτυχία ενός τέτοιου hack θα απαιτούσε από τον χάκερ να ελέγχει και να τροποποιεί ταυτόχρονα το 51% των αντιγράφων του blockchain έτσι ώστε το νέο του αντίγραφο να γίνει το αντίγραφο της πλειοψηφίας και έτσι, η συμφωνημένη αλυσίδα. Μια τέτοια επίθεση θα απαιτούσε επίσης ένα τεράστιο ποσό χρημάτων και πόρων καθώς θα χρειαζόταν να ξανακάνει όλα τα μπλοκ επειδή θα είχαν τώρα διαφορετικές χρονικές σημάνσεις και κωδικούς κατακερματισμού (hash codes).

Λόγω του μεγέθους του δικτύου του Bitcoin και του πόσο γρήγορα αυξάνεται, το κόστος για να επιτευχθεί ένα τέτοιο κατόρθωμα θα ήταν πιθανώς αξεπέραστο. Αυτό όχι μόνο θα ήταν εξαιρετικά ακριβό, αλλά πιθανότατα θα ήταν και άκαρπο. Κάνοντας κάτι τέτοιο δεν θα περνούσε απαρατήρητο, καθώς τα μέλη του δικτύου θα έβλεπαν τέτοιες δραστικές αλλαγές στο blockchain. Στη συνέχεια, τα μέλη του δικτύου θα προχωρήσουν σε μια νέα έκδοση της αλυσίδας που δεν έχει επηρεαστεί.

Αυτό θα μπορούσε να οδηγήσει σε πτώση της αξίας της επιτιθέμενης μορφής του Bitcoin, καθιστώντας την επίθεση τελικά άσκοπη. Το ίδιο θα συνέβαινε αν ο hacker επιτίθετο στη νέα version του Bitcoin. Είναι κατασκευασμένο με αυτόν τον τρόπο, έτσι ώστε η συμμετοχή στο δίκτυο αυτό να έχει οικονομικό κόστος πολύ περισσότερο από το όφελος που θα αποκομίσει κάποιος του επιτεθεί.

1.3: Πώς χρησιμοποιείται το Blockchain;

Όπως γνωρίζουμε τώρα, μπλοκ στα δεδομένα blockchain του Bitcoin που αποθηκεύουν σχετικά με νομισματικές συναλλαγές. Αλλά αποδεικνύεται ότι το blockchain είναι στην πραγματικότητα ένας αξιόπιστος τρόπος αποθήκευσης δεδομένων και για άλλους τύπους συναλλαγών.

Ορισμένες εταιρείες που έχουν ήδη ενσωματώσει blockchain στις πληρωμές τους είναι η Walmart, η Pfizer, η AIG, η Siemens, η Unilever και μια σειρά από άλλες. Για παράδειγμα, η IBM δημιούργησε το blockchain της Food Trust για να εντοπίσει το ταξίδι που κάνουν τα τρόφιμα για να φτάσουν στις τοποθεσίες προορισμού τους. Η IBM Food Trust χρησιμοποιεί το blockchain για να συνδέει τους συμμετέχοντές του μέσω μιας διαφανούς, μόνιμης και κοινής καταγραφής κάποιων πληροφοριών των τροφίμων όπως, των λεπτομερειών της προέλευσης τροφίμων, την επεξεργασία δεδομένων, των λεπτομερειών αποστολής και πολλών άλλων.

Γιατί να το συμβεί αυτό; Η βιομηχανία τροφίμων έχει δει αμέτρητες εστίες e-Coli, σαλμονέλας, καθώς και επικίνδυνα υλικά που εισήχθησαν κατά λάθος στα τρόφιμα. Στο παρελθόν, χρειάστηκαν εβδομάδες για να βρεθεί η πηγή αυτών των επιδημιών ή η αιτία της ασθένειας από αυτό που τρώνε οι άνθρωποι.

Η χρήση blockchain δίνει στις μάρκες τη δυνατότητα να παρακολουθούν τη διαδρομή ενός προϊόντος τροφίμων από την προέλευσή του, μέσω κάθε στάσης που κάνει και, τέλος, την παράδοσή του. Εάν διαπιστωθεί ότι ένα τρόφιμο είναι μολυσμένο, τότε μπορεί να εντοπιστεί το μονοπάτι διάδοσης προς τα πίσω, μέχρι την προέλευσή του, σε κάθε στάση. Όχι μόνο αυτό, αλλά αυτές οι εταιρείες μπορούν επίσης τώρα να δουν οτιδήποτε άλλο μπορεί να έχει έρθει σε επαφή, επιτρέποντας στον εντοπισμό του προβλήματος να συμβεί πολύ νωρίτερα, σώζοντας δυνητικά ζωές. Αυτό είναι ένα παράδειγμα blockchains στην πράξη, αλλά υπάρχουν πολλές άλλες μορφές εφαρμογής blockchain.

1.3.1: Νόμισμα

Το Blockchain αποτελεί τη βάση για κρυπτονομίσματα όπως το Bitcoin. Το δολάριο ΗΠΑ ελέγχεται από την Federal Reserve. Σύμφωνα με αυτό το κεντρικό σύστημα αρχών, τα δεδομένα και το νόμισμα ενός χρήστη είναι τεχνικά κατά την επιθυμία της τράπεζας ή της κυβέρνησής τους. Εάν παραβιαστεί η τράπεζα ενός

χρήστη, οι ιδιωτικές πληροφορίες του πελάτη κινδυνεύουν. Εάν η τράπεζα του πελάτη καταρρεύσει ή ζουν σε μια χώρα με ασταθή κυβέρνηση, η αξία του νομίσματός τους ενδέχεται να κινδυνεύει. Το 2008, ορισμένες από τις τράπεζες που έμειναν χωρίς χρήματα διασώθηκαν εν μέρει χρησιμοποιώντας χρήματα φορολογουμένων. Αυτές είναι οι ανησυχίες από τις οποίες δημιουργήθηκε και αναπτύχθηκε για πρώτη φορά το Bitcoin. Με την εξάπλωση των λειτουργιών του σε ένα δίκτυο υπολογιστών, το blockchain επιτρέπει στο Bitcoin και σε άλλα κρυπτονομίσματα να λειτουργούν χωρίς την ανάγκη κεντρικής αρχής. Αυτό όχι μόνο μειώνει τον κίνδυνο αλλά εξαλείφει πολλά από τα τέλη επεξεργασίας και συναλλαγών. Μπορεί επίσης να δώσει σε εκείνες τις χώρες με ασταθή νομίσματα ή χρηματοπιστωτικές υποδομές ένα πιο σταθερό νόμισμα με περισσότερες εφαρμογές και ένα ευρύτερο δίκτυο ατόμων και ιδρυμάτων με τα οποία μπορούν να συνεργαστούν, τόσο στο εσωτερικό όσο και στο εξωτερικό.

Η χρήση πορτοφολιών κρυπτονομισμάτων για λογαριασμούς ταμιευτηρίου ή ως μέσο πληρωμής είναι ιδιαίτερα δύσκολη για εκείνους που δεν έχουν κρατική ταυτότητα. Ορισμένες χώρες μπορεί να έχουν πληγεί από τον πόλεμο ή να έχουν κυβερνήσεις που στερούνται πραγματικής υποδομής για την παροχή ταυτότητας. Οι πολίτες τέτοιων χωρών ενδέχεται να μην έχουν πρόσβαση σε λογαριασμούς αποταμίευσης ή μεσιτείας και ως εκ τούτου, κανέναν τρόπο για την ασφαλή αποθήκευση του πλούτου.

Εικόνα 5 Bitcoin και Etherium (https://markets.businessinsider.com/news/currencies/bitcoin-vs-ethereum-experts-which-asset-rather-hold-btc-eth-2021-5)

1.3.2: Φροντίδα υγείας

Οι πάροχοι υγειονομικής περίθαλψης μπορούν να αξιοποιήσουν το blockchain για την ασφαλή αποθήκευση των ιατρικών αρχείων των ασθενών τους. Όταν δημιουργείται και υπογράφεται ένα ιατρικό αρχείο, μπορεί να εγγραφεί στο blockchain, το οποίο παρέχει στους ασθενείς την απόδειξη και την εμπιστοσύνη ότι το αρχείο δεν μπορεί να αλλάξει. Αυτά τα προσωπικά αρχεία υγείας θα μπορούσαν να κωδικοποιηθούν και να αποθηκευτούν στο blockchain με ιδιωτικό κλειδί, ώστε να είναι προσβάσιμα μόνο από συγκεκριμένα άτομα, διασφαλίζοντας έτσι την ιδιωτικότητα.

1.3.3: Αρχεία Ιδιοκτησίας

Εάν έχετε περάσει ποτέ χρόνο στο τοπικό σας γραφείο καταγραφής, θα γνωρίζετε ότι η διαδικασία καταγραφής των δικαιωμάτων ιδιοκτησίας είναι τόσο επαχθής όσο και αναποτελεσματική. Σήμερα, μια φυσική πράξη πρέπει να παραδοθεί σε κυβερνητικό υπάλληλο στο τοπικό γραφείο καταγραφής, όπου

καταχωρείται χειροκίνητα στην κεντρική βάση δεδομένων του νομού και στο δημόσιο ευρετήριο. Σε περίπτωση διαφοράς ιδιοκτησίας, οι απαιτήσεις για το ακίνητο πρέπει να συμβιβάζονται με το δημόσιο ευρετήριο.

Αυτή η διαδικασία δεν είναι μόνο δαπανηρή και χρονοβόρα-είναι επίσης γεμάτη με ανθρώπινα λάθη, όπου κάθε ανακρίβεια καθιστά την παρακολούθηση της ιδιοκτησίας ακινήτου λιγότερο αποδοτική. Το Blockchain έχει τη δυνατότητα να εξαλείψει την ανάγκη σάρωσης εγγράφων και εντοπισμού φυσικών αρχείων σε τοπικό γραφείο εγγραφής. Εάν η ιδιοκτησία ακινήτου αποθηκεύεται και επαληθεύεται στο blockchain, οι ιδιοκτήτες μπορούν να εμπιστευτούν ότι η πράξη τους είναι ακριβής και καταγράφεται μόνιμα.

Σε χώρες που έχουν πληγεί από τον πόλεμο ή περιοχές που έχουν ελάχιστη έως καθόλου κυβερνητική ή οικονομική υποδομή και σίγουρα κανένα «Γραφείο Καταγραφής», μπορεί να είναι σχεδόν αδύνατο να αποδειχθεί η ιδιοκτησία ενός ακινήτου. Εάν μια ομάδα ανθρώπων που ζουν σε μια τέτοια περιοχή είναι σε θέση να αξιοποιήσει το blockchain, θα μπορούσε να καθοριστεί διαφανές και σαφές χρονοδιάγραμμα ιδιοκτησίας.

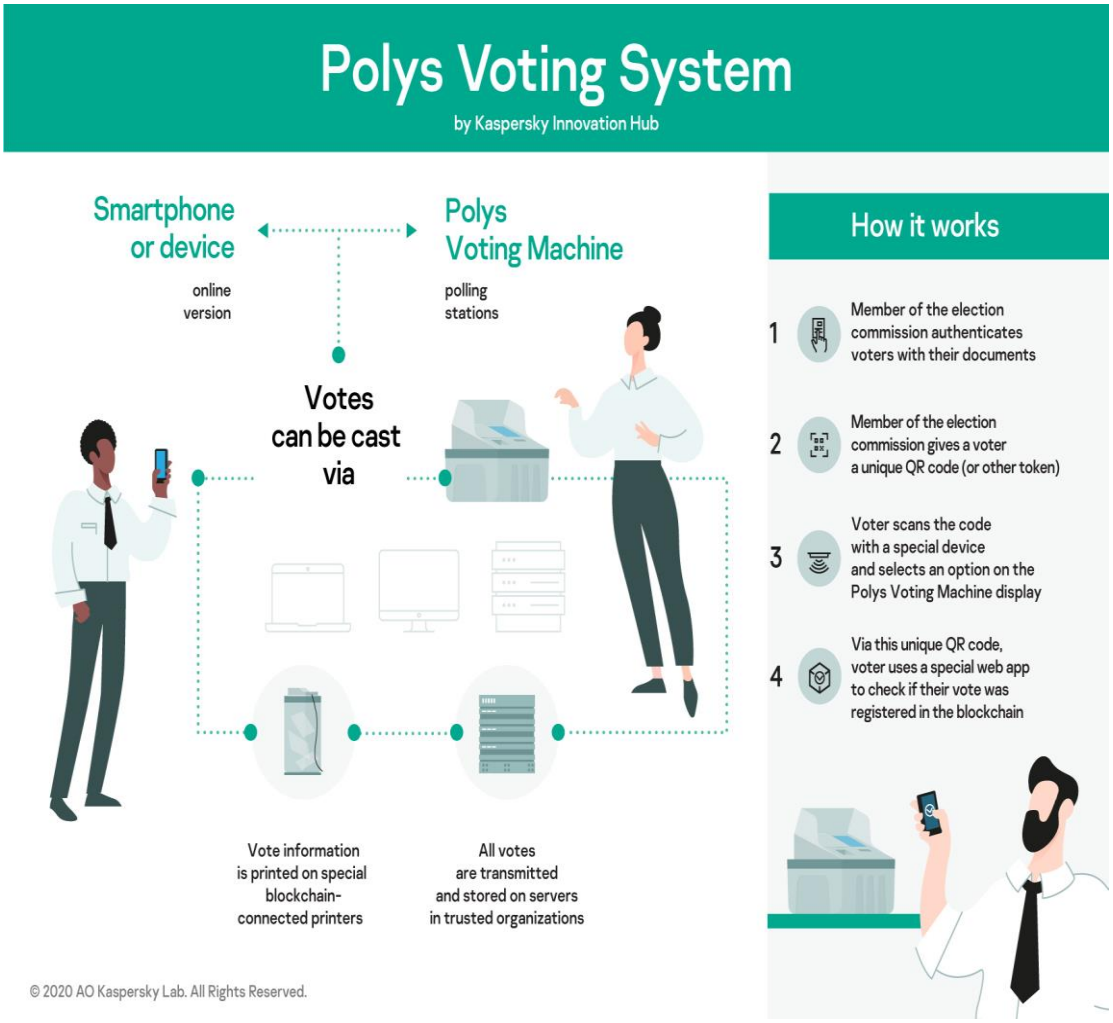
1.3.4: Έξυπνα Συμβόλαια – Smart contracts

Ένα έξυπνο συμβόλαιο είναι ένας κωδικός υπολογιστή που μπορεί να ενσωματωθεί στο blockchain για να διευκολύνει, να επαληθεύσει ή να διαπραγματευτεί μια συμφωνία σύμβασης. Τα έξυπνα συμβόλαια λειτουργούν υπό μια σειρά από προϋποθέσεις στις οποίες συμφωνούν οι χρήστες. Όταν πληρούνται αυτές οι προϋποθέσεις, οι όροι της συμφωνίας εκτελούνται αυτόματα. Ας πούμε, για παράδειγμα, ένας δυνητικός ενοικιαστής θα ήθελε να μισθώσει ένα διαμέρισμα χρησιμοποιώντας ένα έξυπνο συμβόλαιο. Ο ιδιοκτήτης συμφωνεί να δώσει στον ενοικιαστή τον κωδικό της πόρτας στο διαμέρισμα μόλις ο ενοικιαστής πληρώσει την εγγύηση ασφαλείας. Τόσο ο ενοικιαστής όσο και ο ιδιοκτήτης θα έστελναν τα αντίστοιχα τμήματα της συμφωνίας στο έξυπνο συμβόλαιο, το οποίο θα

κρατούσε και θα ανταλλάσσει αυτόματα τον κωδικό της πόρτας για την εγγύηση κατά την ημερομηνία έναρξης της μίσθωσης. Εάν ο ιδιοκτήτης δεν παρέχει τον κωδικό της πόρτας μέχρι την ημερομηνία μίσθωσης, το έξυπνο συμβόλαιο επιστρέφει την εγγύηση ασφαλείας. Αυτό θα εξαλείψει τα τέλη και τις διαδικασίες που συνήθως σχετίζονται με τη χρήση συμβολαιογράφου, διαμεσολαβητή τρίτων ή πληρεξούσιων.

1.3.5: Ψηφοφορία

Όπως αναφέρθηκε, το blockchain θα μπορούσε να χρησιμοποιηθεί για τη διευκόλυνση ενός σύγχρονου συστήματος ψηφοφορίας. Η ψηφοφορία με blockchain έχει τη δυνατότητα να εξαλείψει την εκλογική απάτη και να αυξήσει τη συμμετοχή των ψηφοφόρων, όπως δοκιμάστηκε στις ενδιάμεσες εκλογές του Νοεμβρίου 2018 στη Δυτική Βιρτζίνια. Η χρήση blockchain με αυτόν τον τρόπο θα καθιστούσε σχεδόν αδύνατη την παραποίηση των ψήφων. Το πρωτόκολλο blockchain θα διατηρήσει επίσης τη διαφάνεια στην εκλογική διαδικασία, μειώνοντας το προσωπικό που απαιτείται για τη διεξαγωγή εκλογών και παρέχοντας στους υπαλλήλους σχεδόν άμεσα αποτελέσματα. Αυτό θα εξαλείψει την ανάγκη για επαναμέτρηση ή οποιαδήποτε πραγματική ανησυχία ότι η απάτη μπορεί να απειλήσει τις εκλογές.



Εικόνα 6 Το Blockchain στις ψηφοφορίες (https://www.kaspersky.com/about/press-releases/2020_polys-from-kaspersky-innovation-hub-presents-first-blockchain-based-voting-machine)

1.4: Πλεονεκτήματα και μειονεκτήματα του Blockchain

Για όλη την πολυπλοκότητά του και τη δυναμική του, το ταβάνι των δυνατοτήτων του blockchain ως μια αποκεντρωμένη μορφή αποθήκευσης πληροφορίας είναι σχεδόν χωρίς όριο. Από το μεγαλύτερο απόρρητο του χρήστη και την αυξημένη ασφάλεια έως τις χαμηλότερες χρεώσεις επεξεργασίας και λιγότερα σφάλματα, η τεχνολογία blockchain μπορεί κάλλιστα να βλέπει εφαρμογές πέρα από αυτές που περιγράφονται παραπάνω. Υπάρχουν όμως και κάποια

μειονεκτήματα. Όπως και στο παράδειγμα της IBM Food Trust, οι προμηθευτές μπορούν να χρησιμοποιήσουν το blockchain για να καταγράψουν την προέλευση των υλικών που έχουν αγοράσει. Αυτό θα επέτρεπε στις εταιρείες να επαληθεύουν την αυθεντικότητα των προϊόντων τους, μαζί με κοινές ετικέτες όπως "Βιολογικά", "Τοπικά" και "Δίκαιο Εμπόριο".

1.4.1: Πλεονεκτήματα του Blockchain

Ακρίβεια της Αλυσίδας

Οι συναλλαγές στο δίκτυο blockchain εγκρίνονται από ένα δίκτυο χιλιάδων υπολογιστών. Αυτό αφαιρεί σχεδόν όλη την ανθρώπινη συμμετοχή στη διαδικασία επαλήθευσης, με αποτέλεσμα λιγότερο ανθρώπινο λάθος και ακριβή καταγραφή πληροφοριών. Ακόμα κι αν ένας υπολογιστής στο δίκτυο έκανε ένα υπολογιστικό λάθος, το σφάλμα θα γινόταν μόνο σε ένα αντίγραφο του blockchain. Για να εξαπλωθεί αυτό το σφάλμα στο υπόλοιπο blockchain, θα πρέπει να γίνει τουλάχιστον από το 51% των υπολογιστών του δικτύου - σχεδόν αδύνατο για ένα μεγάλο και αναπτυσσόμενο δίκτυο μεγέθους Bitcoin.

Αποκέντρωση

Το Blockchain δεν αποθηκεύει καμία από τις πληροφορίες του σε κεντρική τοποθεσία. Αντ 'αυτού, το blockchain αντιγράφεται και εξαπλώνεται σε ένα δίκτυο υπολογιστών. Κάθε φορά που προστίθεται ένα νέο μπλοκ στο blockchain, κάθε υπολογιστής στο δίκτυο ενημερώνει το blockchain του για να αντικατοπτρίζει την αλλαγή. Διαδίδοντας αυτές τις πληροφορίες σε ένα δίκτυο, αντί να τις αποθηκεύσετε σε μια κεντρική βάση δεδομένων, το blockchain γίνεται πιο δύσκολο να παραβιαστεί. Εάν ένα αντίγραφο του blockchain έπεσε στα χέρια ενός χάκερ, μόνο αυτό το αντίγραφο των πληροφοριών, και όχι ολόκληρο το δίκτυο, θα ήταν σε κίνδυνο.

Μειώσεις κόστους

Συνήθως, οι καταναλωτές πληρώνουν μια τράπεζα για να επαληθεύσουν μια συναλλαγή, έναν συμβολαιογράφο για να υπογράψει ένα έγγραφο ή έναν υπουργό για να πραγματοποιήσουν έναν γάμο. Το Blockchain εξαλείφει την ανάγκη επαλήθευσης τρίτου μέρους και, μαζί με αυτό, το σχετικό κόστος τους. Για παράδειγμα οι ιδιοκτήτες επιχειρήσεων επιβαρύνονται με ένα μικρό τέλος κάθε φορά που δέχονται πληρωμές χρησιμοποιώντας πιστωτικές κάρτες, επειδή οι τράπεζες και οι εταιρείες επεξεργασίας πληρωμών πρέπει να επεξεργάζονται αυτές τις συναλλαγές. Το Bitcoin, από την άλλη πλευρά, δεν έχει κεντρική αρχή και έχει περιορισμένες χρεώσεις συναλλαγών.

Προσωπικές συναλλαγές

Πολλά δίκτυα blockchain λειτουργούν ως δημόσιες βάσεις δεδομένων, πράγμα που σημαίνει ότι οποιοσδήποτε με σύνδεση στο Διαδίκτυο μπορεί να δει μια λίστα με το ιστορικό συναλλαγών του δικτύου. Παρόλο που οι χρήστες μπορούν να έχουν πρόσβαση σε λεπτομέρειες σχετικά με τις συναλλαγές, δεν μπορούν να έχουν πρόσβαση σε πληροφορίες ταυτοποίησης για τους χρήστες που πραγματοποιούν αυτές τις συναλλαγές. Είναι μια κοινή εσφαλμένη αντίληψη ότι τα δίκτυα blockchain όπως το bitcoin είναι ανώνυμα, ενώ στην πραγματικότητα είναι μόνο εμπιστευτικά.

Δηλαδή, όταν ένας χρήστης πραγματοποιεί δημόσιες συναλλαγές, ο μοναδικός κωδικός του, που ονομάζεται δημόσιο κλειδί, καταγράφεται στο blockchain αλλά όχι και τα προσωπικά του στοιχεία. Εάν ένα άτομο έχει κάνει μια αγορά Bitcoin σε ανταλλαγή που απαιτεί ταυτοποίηση, η ταυτότητα του ατόμου εξακολουθεί να συνδέεται με τη διεύθυνση blockchain, αλλά μια συναλλαγή, ακόμη και όταν συνδέεται με το όνομα ενός ατόμου, δεν αποκαλύπτει προσωπικές πληροφορίες.

Αποτελεσματικές Συναλλαγές

Οι συναλλαγές που πραγματοποιούνται μέσω κεντρικής αρχής μπορεί να χρειαστούν έως και μερικές ημέρες για να διευθετηθούν. Εάν επιχειρήσετε να καταθέσετε μια επιταγή το βράδυ της Παρασκευής, για παράδειγμα, ενδέχεται να μην δείτε πραγματικά χρήματα στο λογαριασμό σας μέχρι τη Δευτέρα το πρωί. Ενώ τα χρηματοπιστωτικά ιδρύματα λειτουργούν κατά τις εργάσιμες ώρες, πέντε ημέρες την εβδομάδα, το blockchain λειτουργεί 24 ώρες την ημέρα, επτά ημέρες την εβδομάδα και 365 ημέρες το χρόνο. Οι συναλλαγές μπορούν να ολοκληρωθούν σε μόλις δέκα λεπτά και μπορούν να θεωρηθούν ασφαλείς μετά από λίγες μόνο ώρες. Αυτό είναι ιδιαίτερα χρήσιμο για διασυνοριακές συναλλαγές, οι οποίες συνήθως διαρκούν πολύ περισσότερο λόγω ζητημάτων ζώνης ώρας και του γεγονότος ότι όλα τα μέρη πρέπει να επιβεβαιώσουν την επεξεργασία πληρωμών.

Ασφαλείς Συναλλαγές

Μόλις καταγραφεί μια συναλλαγή, η γνησιότητά της πρέπει να επαληθευτεί από το δίκτυο blockchain. Χιλιάδες υπολογιστές στο blockchain σπεύδουν να επιβεβαιώσουν ότι οι λεπτομέρειες της αγοράς είναι σωστές. Αφού ένας υπολογιστής επικυρώσει τη συναλλαγή, προστίθεται στο μπλοκ blockchain. Κάθε μπλοκ στο blockchain περιέχει το δικό του μοναδικό hash, μαζί με το μοναδικό hash του block πριν από αυτό. Όταν οι πληροφορίες σε ένα μπλοκ επεξεργάζονται με οποιονδήποτε τρόπο, ο κώδικας κατακερματισμού αυτού του μπλοκ αλλάζει - ωστόσο, ο κωδικός κατακερματισμού στο μπλοκ αφού δεν θα το έκανε. Αυτή η ασυμφωνία καθιστά εξαιρετικά δύσκολη την αλλαγή των πληροφοριών σχετικά με το blockchain χωρίς προειδοποίηση.

Διαφάνεια

Τα περισσότερα blockchains είναι εντελώς λογισμικό ανοιχτού κώδικα. Αυτό σημαίνει ότι ο καθένας και ο καθένας μπορεί να δει τον κωδικό του. Αυτό δίνει στους ελεγκτές τη δυνατότητα να αναθεωρούν κρυπτονομίσματα όπως το Bitcoin για ασφάλεια. Αυτό σημαίνει επίσης ότι δεν υπάρχει πραγματική εξουσία για το ποιος ελέγχει τον κώδικα του Bitcoin ή πώς επεξεργάζεται. Εξαιτίας αυτού, ο

καθένας μπορεί να προτείνει αλλαγές ή αναβαθμίσεις στο σύστημα. Εάν η πλειοψηφία των χρηστών του δικτύου συμφωνεί ότι η νέα έκδοση του κώδικα με την αναβάθμιση είναι καλή και αξίζει τον κόπο, τότε το Bitcoin μπορεί να ενημερωθεί.

Τραπεζικές εργασίες χωρίς τράπεζες

Ίσως η πιο βαθιά όψη του blockchain και του Bitcoin είναι η δυνατότητα για οποιονδήποτε, ανεξάρτητα από την εθνικότητα, το φύλο ή το πολιτιστικό υπόβαθρο, να το χρησιμοποιήσει. Σύμφωνα με την παγκόσμια τράπεζα, υπάρχουν σχεδόν 2 δισεκατομμύρια ενήλικες που δεν διαθέτουν τραπεζικούς λογαριασμούς ή κανένα μέσο αποθήκευσης των χρημάτων ή του πλούτου τους. 5 Σχεδόν όλα αυτά τα άτομα ζουν σε αναπτυσσόμενες χώρες όπου η οικονομία βρίσκεται στα σπάργανα και εξαρτάται πλήρως από μετρητά.

Αυτοί οι άνθρωποι συχνά κερδίζουν λίγα χρήματα που πληρώνονται σε φυσικά μετρητά. Στη συνέχεια, θα πρέπει να αποθηκεύσουν αυτά τα φυσικά μετρητά σε κρυφές τοποθεσίες στα σπίτια τους ή στους χώρους διαβίωσής τους αφήνοντάς τους ληστείες ή περιττή βία. Τα κλειδιά για ένα πορτοφόλι bitcoin μπορούν να αποθηκευτούν σε ένα κομμάτι χαρτί, σε ένα φτηνό κινητό τηλέφωνο ή ακόμη και να απομνημονευτούν εάν είναι απαραίτητο. Για τους περισσότερους ανθρώπους, είναι πιθανό ότι αυτές οι επιλογές κρύβονται πιο εύκολα από ένα μικρό σωρό μετρητών κάτω από ένα στρώμα. Τα blockchains του μέλλοντος αναζητούν επίσης λύσεις για να μην είναι μόνο μια μονάδα λογαριασμού για την αποθήκευση πλούτου, αλλά και για την αποθήκευση ιατρικών αρχείων, δικαιωμάτων ιδιοκτησίας και μια ποικιλία άλλων νομικών συμβάσεων.

1.4.2: Μειονεκτήματα του Blockchain

Ενώ υπάρχουν σημαντικά πλεονεκτήματα στο blockchain, υπάρχουν επίσης σημαντικές προκλήσεις για την υιοθέτησή του. Τα εμπόδια στην εφαρμογή της τεχνολογίας blockchain σήμερα δεν είναι μόνο τεχνικά. Οι πραγματικές προκλήσεις

είναι πολιτικές και κανονιστικές, ως επί το πλείστον, για να μην πούμε τίποτα για τις χιλιάδες ώρες (διαβάστε: χρήματα) του προσαρμοσμένου σχεδιασμού λογισμικού και του προγραμματισμού back-end που απαιτούνται για την ενσωμάτωση του blockchain στα τρέχοντα επιχειρηματικά δίκτυα. Ακολουθούν μερικές από τις προκλήσεις που εμποδίζουν την ευρεία υιοθέτηση blockchain.

Κόστος τεχνολογίας

Παρόλο που το blockchain μπορεί να εξοικονομήσει χρήματα χρημάτων για τέλη συναλλαγών, η τεχνολογία δεν είναι καθόλου δωρεάν. Το σύστημα «απόδειξη της εργασίας» που χρησιμοποιεί το bitcoin για την επικύρωση συναλλαγών, για παράδειγμα, καταναλώνει τεράστια ποσά υπολογιστικής ισχύος. Στον πραγματικό κόσμο, η ενέργεια από εκατομμύρια υπολογιστές στο δίκτυο bitcoin είναι κοντά σε αυτήν που καταναλώνει η Δανία ετησίως. Υποθέτοντας κόστος ηλεκτρικής ενέργειας 0,03 $ 0.0 0,05 $ ανά κιλοβατώρα, το κόστος εξόρυξης χωρίς τα έξοδα υλικού είναι περίπου $ 5,000 7 7,000 $ ανά νόμισμα.

Παρά το κόστος εξόρυξης bitcoin, οι χρήστες συνεχίζουν να αυξάνουν τους λογαριασμούς ηλεκτρικού ρεύματος, προκειμένου να επικυρώσουν συναλλαγές στο blockchain. Αυτό συμβαίνει επειδή όταν οι ανθρακωρύχοι προσθέτουν ένα μπλοκ στο blockchain του bitcoin, ανταμείβονται με αρκετό bitcoin για να αξίζει τον χρόνο και την ενέργειά τους. Όσον αφορά τα blockchains που δεν χρησιμοποιούν κρυπτονομίσματα, ωστόσο, οι ανθρακωρύχοι θα πρέπει να αμείβονται ή να έχουν κίνητρο για να επικυρώσουν συναλλαγές.Κάποιες λύσεις σε αυτά τα θέματα έχουν αρχίσει να εμφανίζονται. Για παράδειγμα, έχουν δημιουργηθεί αγροκτήματα εξόρυξης bitcoin για να χρησιμοποιούν ηλιακή ενέργεια, υπερβολικό φυσικό αέριο από χώρους fracking ή ενέργεια από αιολικά πάρκα.

Ανεπάρκεια ταχύτητας

Το Bitcoin είναι μια τέλεια μελέτη περίπτωσης για τις πιθανές αναποτελεσματικότητες του blockchain. Το σύστημα "απόδειξη εργασίας" του

Bitcoin χρειάζεται περίπου δέκα λεπτά για να προσθέσει ένα νέο μπλοκ στο blockchain. Με αυτόν τον ρυθμό, εκτιμάται ότι το δίκτυο blockchain μπορεί να διαχειριστεί μόνο περίπου επτά συναλλαγές ανά δευτερόλεπτο (TPS). Αν και άλλα κρυπτονομίσματα όπως το Ethereum έχουν καλύτερη απόδοση από το bitcoin, εξακολουθούν να περιορίζονται από το blockchain. Η παλαιά μάρκα Visa, για περιβάλλον, μπορεί να επεξεργαστεί 24.000 TPS. Λύσεις σε αυτό το ζήτημα έχουν αναπτυχθεί εδώ και χρόνια. Αυτήν τη στιγμή υπάρχουν blockchains που διαθέτουν πάνω από 30.000 συναλλαγές ανά δευτερόλεπτο.

Παράνομη Δραστηριότητα

Ενώ το απόρρητο στο δίκτυο blockchain προστατεύει τους χρήστες από παραβιάσεις και διατηρεί το απόρρητο, επιτρέπει επίσης παράνομες συναλλαγές και δραστηριότητες στο δίκτυο blockchain. Το πιο αναφερόμενο παράδειγμα του blockchain που χρησιμοποιείται για παράνομες συναλλαγές είναι πιθανώς το Silk Road, μια διαδικτυακή αγορά ναρκωτικών «σκοτεινού ιστού» που λειτουργεί από τον Φεβρουάριο του 2011 έως τον Οκτώβριο του 2013, όταν έκλεισε από το FBI.

Ο ιστότοπος επέτρεψε στους χρήστες να περιηγηθούν στον ιστότοπο χωρίς να παρακολουθούνται χρησιμοποιώντας το πρόγραμμα περιήγησης Tor και να κάνουν παράνομες αγορές σε Bitcoin ή άλλα κρυπτονομίσματα. Οι ισχύοντες κανονισμοί των ΗΠΑ απαιτούν από τους παρόχους χρηματοπιστωτικών υπηρεσιών να λαμβάνουν πληροφορίες σχετικά με τους πελάτες τους όταν ανοίγουν λογαριασμό, επαληθεύουν την ταυτότητα κάθε πελάτη και επιβεβαιώνουν ότι οι πελάτες δεν εμφανίζονται σε καμία λίστα γνωστών ή υπόπτων τρομοκρατικών οργανώσεων. Αυτό το σύστημα μπορεί να θεωρηθεί τόσο υπέρ όσο και κατά. Δίνει σε οποιονδήποτε πρόσβαση σε οικονομικούς λογαριασμούς, αλλά επιτρέπει επίσης στους εγκληματίες να συναλλάσσονται πιο εύκολα. Πολλοί έχουν υποστηρίξει ότι οι καλές χρήσεις κρυπτογράφησης, όπως η τραπεζική στον τραπεζικό κόσμο, υπερτερούν των κακών χρήσεων κρυπτονομισμάτων, ειδικά όταν οι περισσότερες παράνομες δραστηριότητες επιτυγχάνονται ακόμη μέσω μη ανιχνεύσιμων μετρητών.

Κανονισμ*οί* λειτουργίας

Πολλοί στον χώρο των κρυπτονομισμάτων έχουν εκφράσει ανησυχίες σχετικά με την κυβερνητική ρύθμιση για τα κρυπτονομίσματα. Ενώ γίνεται ολοένα και πιο δύσκολο και σχεδόν αδύνατο να τερματιστεί κάτι σαν το Bitcoin καθώς το αποκεντρωμένο δίκτυό του μεγαλώνει, οι κυβερνήσεις θεωρητικά θα μπορούσαν θεωρητικά να καταστήσουν παράνομο να κατέχουν κρυπτονομίσματα ή να συμμετέχουν στα δίκτυά τους. Με την πάροδο του χρόνου, αυτή η ανησυχία έγινε μικρότερη καθώς μεγάλες εταιρείες όπως το PayPal αρχίζουν να επιτρέπουν την ιδιοκτησία και τη χρήση κρυπτονομισμάτων στην πλατφόρμα του.

ΥΠΕΡ		ΚΑΤΑ
• Βελτίωση ακρίβειας διότι δεν απαιτείται ανθρώπινη επαλήθευση		• Η αύξηση του κόστους της τεχνολογίας σχετίζεται με το mining των bitcoin
• Μείωση του κόστους επειδή δεν απαιτείται επαλήθευση από τρίτο		• Λίγες συναλλαγές το δευτερόλεπτο
• Η αποκέντρωση βοηθά στο να μη παραβιάζεται εύκολα		• Ιστορικό χρησιμοποίησης για αθέμητους και παράνομους λόγους
• Οι συναλλαγές είναι ασφαλείς, ιδιωτικές και αποτελεσματικές		
• Διαυγείς τεχνολογία		
• Δίνει εναλλακτική δυνατότητα τραπεζικών θεμάτων και παρέχει ένα τρόπο να διατηρούνται τα προσωπικά δεδομένα των		

πολιτών ασφαλή σε χώρες με ασταθή κυβερνήσεις		

1.5: Οι τύποι του Blockchain

Το Blockchain αποτελείται από 3 διαφορετικούς τύπους. Η επιλογή του Blockchain τύπου που θα χρησιμοποιηθεί εξαρτάται από τους εξής παράγοντες:

- Αν το λογιστικό βιβλίο θα είναι κατανεμημένο ή όχι.
- Ποιοι χρήστες θα έχουν πρόσβαση σε αυτό.
- Ποιοι χρήστες θα επαληθεύουν και θα καταχωρούν τις συναλλαγές δεδομένων στο βιβλιάριο.

Public /Permissionless

Τα δημόσια Blockchains όπως είναι για παράδειγμα το Bitcoin και το Ethereum είναι από τα μεγαλύτερα σε αριθμό συμμετεχόντων κατανεμημένα δίκτυα. Ο κώδικας εκδίδεται ανοιχτά προς όλους και οποιοσδήποτε μπορεί να τον επιθεωρήσει. Ο κάθε χρήστης λοιπόν έχει πρόσβαση στο δίκτυο και χρησιμοποιώντας το εκάστοτε κρυπτονόμισμα δύναται να συμμετάσχει στο επίπεδο λειτουργιών που επιθυμεί. Για παράδειγμα μπορεί να συμμετέχει στο σύστημα σαν απλός χρήστης ή να λάβει μέρος σε πιο σύνθετες λειτουργίες όπως είναι η συμμετοχή στην επαλήθευση και επικύρωση των συναλλαγών. Επιπλέον το δίκτυο έχει συνήθως έναν μηχανισμό παροχής κινήτρων κατά τον οποίο οι χρήστες κερδίζουν κρυπτονομίσματα κατά την επαλήθευση και επικύρωση των συναλλαγών τους, προκειμένου να ενθαρρύνει περισσότερους συμμετέχοντες να ενταχθούν σε αυτό και να χρησιμοποιήσουν το κρυπτονόμισμα.

Αξιοσημείωτο κρίνεται και το γεγονός ότι τα δημόσια Blockchains τείνουν να είναι πιο ασφαλή από τους υπόλοιπους τύπους Blockchain λόγω του ότι κανένας

οργανισμός ή κυβέρνηση δεν ελέγχει το δίκτυο και η συμμετοχή γίνεται ανώνυμα. Ο κώδικας με τη σειρά του ανανεώνεται αποκλειστικά από την κοινότητα του κάθε Blockchain δικτύου στην οποία συμμετέχουν εθελοντικά προγραμματιστές.

Εξετάζοντας τα μειονεκτήματα των δημόσιων Blockchains καθίσταται φανερό ότι απαιτείται σημαντικό ποσό υπολογιστικής ισχύος για να επιτευχθεί ο συγχρονισμός και η διατήρηση του κατανεμημένου βιβλιαρίου. Επίσης το δημόσιο Blockchain είναι συχνά πιο αργό από τους υπόλοιπους τύπους Blockchain και με τη συνεχόμενη αύξηση των συναλλαγών αντιμετωπίζει προβλήματα αποθηκευτικού χώρου.

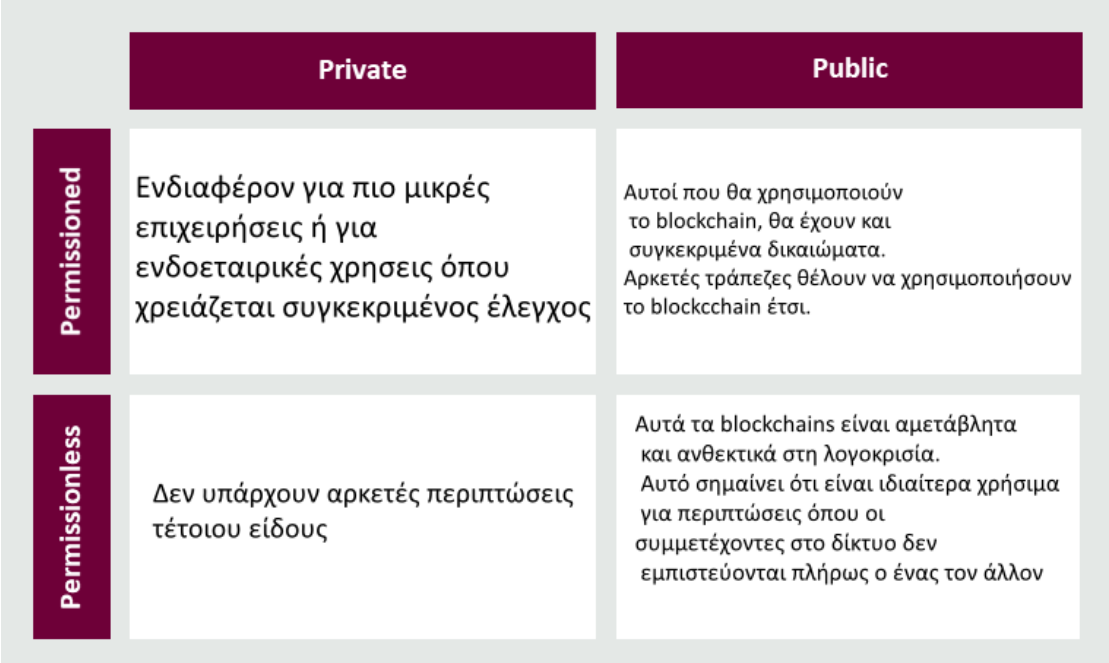
Permissioned

Το εξουσιοδοτημένο Blockchain διατηρεί και αυτό ένα κατανεμημένο βιβλιάριο δεδομένων, όμως η συμμετοχή σε αυτό ελέγχεται από μια κεντρική αρχή. Η κεντρική αυτή αρχή γνωρίζει τους συμμετέχοντες και δίνει το δικαίωμα επικύρωσης των συναλλαγών σε έμπιστα προς αυτούς άτομα. Αυτό το χαρακτηριστικό διευκολύνει την αύξηση του όγκου των συναλλαγών που πραγματοποιούνται ημερησίως και ταυτόχρονα τα εξουσιοδοτημένα δίκτυα μπορούν να είναι πολύ γρήγορα με μεγαλύτερη αποθηκευτική χωρητικότητα. Επίσης ο βασικός κώδικας του κάθε εξουσιοδοτημένου Blockchain μπορεί να εκδίδεται ανοιχτά προς όλους για να τον επιθεωρήσουν ή και όχι.

Private

Τα ιδιωτικά Blockchains τείνουν να είναι πολύ πιο μικρά σε αριθμό συμμετεχόντων σε σχέση με τους υπόλοιπους τύπους Blockchain. Ενδέχεται μάλιστα ο κόσμος να μην γνωρίζει καν την ύπαρξή τους επειδή τις περισσότερες φορές δεν είναι ορατά στο κοινό . Η συμμετοχή κάθε χρήστη είναι ελεγχόμενη από μια κεντρική αρχή. Ως προς τα χαρακτηριστικά τους θα πρέπει να αναφερθεί ότι είναι πολύ πιο γρήγορα από τους υπόλοιπους τύπους και ενδέχεται να μην παρουσιάζουν

καμία καθυστέρηση στο χρόνο επικύρωσης των δεδομένων. Έχουν επίσης χαμηλό κόστος λειτουργείας, απεριόριστη χωρητικότητα και μπορούν να κατασκευαστούν σε πολύ γρήγορο χρονικό διάστημα. Εντούτοις τα περισσότερα ιδιωτικά Blockchain δεν χρησιμοποιούν κρυπτονόμισμα και δεν έχουν την ίδια ασφάλεια που παρέχει ένα αποκεντρωμένο Blockchain δίκτυο.



Εικόνα 7 Private, Public, Permissioned, Permissionless blockchains

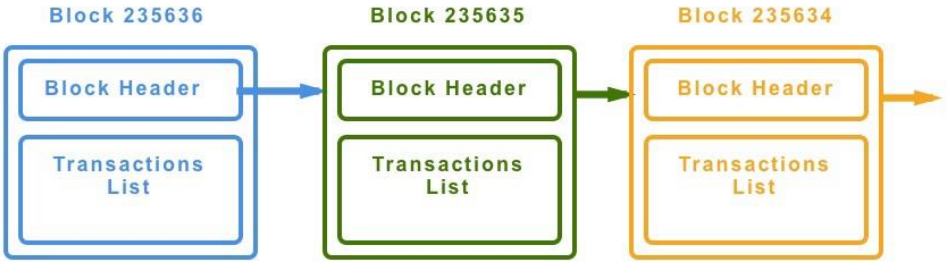
1.6: Αρχιτεκτονική του Blockchain

Η αρχιτεκτονική του Blockchain βασίζεται κυρίως σε 5 στοιχεία: το μπλοκ (Block), την αλυσίδα (Chain), τις ψηφιακές υπογραφές (Digital Signatures), το Peer-to-peer δίκτυο και τον έμπιστο μηχανισμό (Consensus Protocol).

1.6.1: Block

Σε ένα μπλοκ καταγράφονται οι πιο πρόσφατες συναλλαγές που έχουν γίνει σε ένα Blockchain δίκτυο. Συνεπώς, ένα μπλοκ είναι μια μόνιμη «αποθήκη δεδομένων», τα οποία, μόλις γραφτούν, δεν μπορούν να τροποποιηθούν ή να αφαιρεθούν. Τα μπλοκ όμως διαφέρουνε από Blockchain σε Blockchain και εκτός

από τις συναλλαγές περιέχουνε κι, άλλα δεδομένα όπως αυτά που εξετάζονται στο μπλοκ του Bitcoin δικτύου.



Εικόνα 8 Bitcoin blocks (https://medium.com/coinmonks/the-bitcoin-blockchain-a3eb996f7140)

Χρήσιμες ένοιες:

-Block Size: Είναι το μέγεθος του παρόν μπλοκ σε bytes (μονάδα μέτρησης ποσότητας πληροφορίας)

-Block Header: Είναι η κεφαλίδα του μπλοκ

-Version: Είναι η έκδοσης του παρόν μπλοκ

-Previous Block Hash: Είναι το Hash του προηγούμενου μπλοκ

-Merkle root: Είναι ένα Hash το οποίο δημιουργείται από όλες τις συναλλαγές που περιλαμβάνονται σε αυτό το μπλοκ

-Timestamp: Είναι ο χρόνος που δημιουργήθηκε αυτό το μπλοκ

-Difficulty target: Είναι η δυσκολία που χρειάζεται για να επικυρωθεί αυτό το μπλοκ

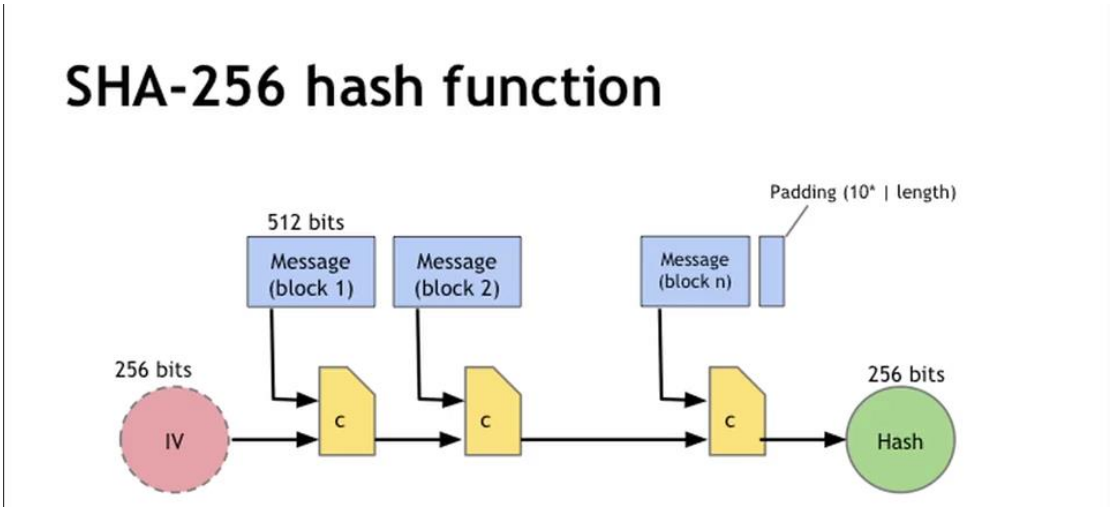
-Nonce: Είναι ένας τυχαίος αριθμός ο οποίος χρησιμοποιείται από το τον αλγόριθμο Proof-of-Work.

-Transaction Counter: Είναι ο συνολικός αριθμός των συναλλαγών στο μπλοκ

-Transactions: Είναι όλες οι συναλλαγές που έχουν καταχωρηθεί στο μπλοκ, οι οποίες είναι περίπου 500 .

1.6.2: Chain

Ο όρος αλυσίδα (Chain) σχετίζεται με τον τρόπο που είναι ταξινομημένα τα μπλοκ σε ένα δίκτυο Blockchain. Η δομή των δεδομένων στο Blockchain είναι μια ταξινομημένη λίστα από μπλοκ συνδεδεμένη προς τα πίσω. Αυτή η ταξινόμηση των μπλοκ σχηματίζει τελικά την αλυσίδα. Το Block Header αποτελείται από 6 δεδομένα και μέσα σε αυτά τα δεδομένα υπάρχει το Previous Block Hash το οποίο είναι αυτό που συνδέει αυτό το μπλοκ με το προηγούμενο μπλοκ στο Blockchain. Το Hash λοιπόν δημιουργείται πάντα από τα δεδομένα του προηγούμενου μπλοκ. Το Hash είναι η “μαγική κόλλα” που ενώνει τα μπλοκ μεταξύ τους και επιτρέπει εμπιστοσύνη με μαθηματική ακρίβεια. Για τη δημιουργία του Hash χρησιμοποιείται ο αλγόριθμος κρυπτογράφησης SHA-256, ο οποίος όταν κρυπτογραφεί τα δεδομένα επιστρέφει σχεδόν πάντα ένα μοναδικό αλφαριθμητικό 64 χαρακτήρων Hash. Η λειτουργία του αλγορίθμου χαρακτηρίζεται ως μη αντιστρέψιμη και λειτουργεί σαν ψηφιακό αποτύπωμα το οποίο είναι μοναδικό και δεν μπορεί να αποκρυπτογραφηθεί. Στην παρακάτω εικόνα παρουσιάζεται το αποτέλεσμα Hash που προκύπτει όταν εφαρμόσουμε τον αλγόριθμο SHA-256 σε 2 διαφορετικές προτάσεις.



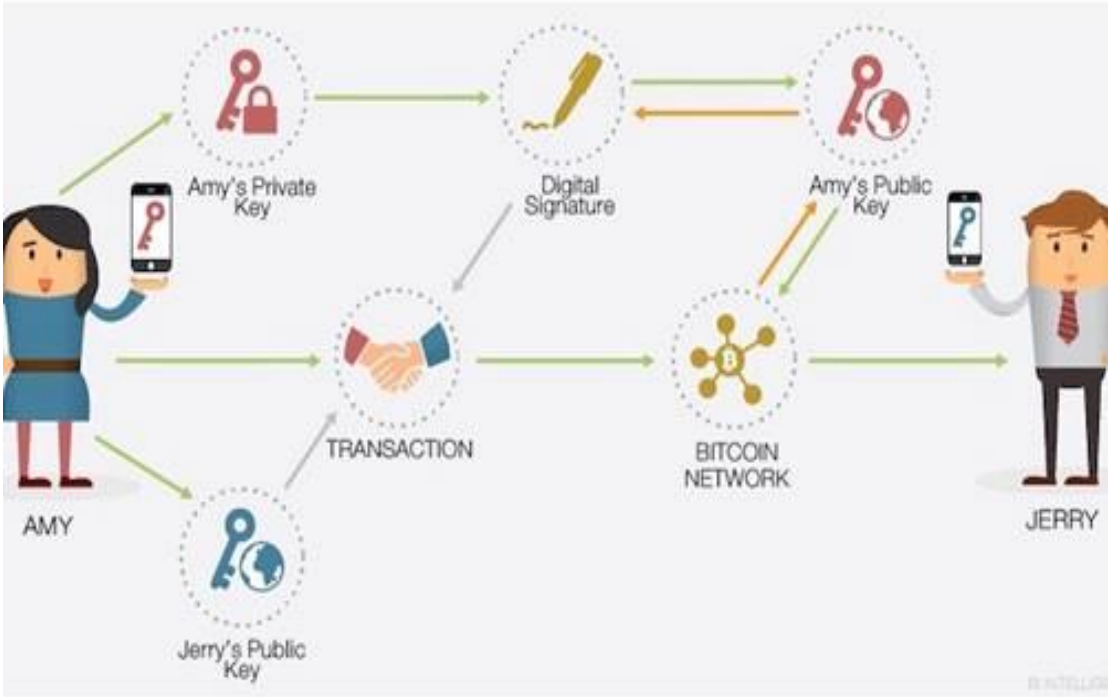
Εικόνα 9 Αλγόριθμος Κατακερματισμού SHA-256 (https://medium.com/@pkmar437/blockchain-for-layman-part-2-a8984fda0acc)

1.6.3: Ψηφιακές υπογραφές

Η δημιουργία μιας συναλλαγής στο Blockchain απαιτεί ψηφιακή υπογραφή για τον έλεγχο και την εγκυρότητας της. Πιο αναλυτικά, για τη δημιουργία μιας ψηφιακής υπογραφής κάθε χρήστης χρησιμοποιεί ένα ζευγάρι κλειδιών, ένα ιδιωτικό και ένα δημόσιο.

Το ιδιωτικό κλειδί, το οποίο γνωρίζει μόνο ο χρήστης χρησιμοποιείται για τη δημιουργία της ψηφιακής υπογραφής.

Το δημόσιο κλειδί λειτουργεί σαν τις διευθύνσεις email, είναι δηλαδή ορατό προς όλους και χρησιμοποιείται για την επαλήθευση των δεδομένων. Μια ψηφιακή υπογραφή περιλαμβάνει δύο φάσεις: a) τη φάση υπογραφής και b) τη φάση της επαλήθευσης.



Εικόνα 10 Συναλλαγη και ψηφιακες υπογραφές (https://medium.com/blockchain-editorial/anatomy-of-bitcoin-transactions-e5ad47f01e31)

Στην παραπάνω εικόνα παρουσιάζεται ένα παράδειγμα ψηφιακής υπογραφής. Παρατηρούμε λοιπόν ότι για να υπογράψει ο χρήστης, Amy, μια συναλλαγή πρέπει να ακολουθήσει τα εξής βήματα:

i. Αρχικά δημιουργεί ένα Hash από τα δεδομένα της συναλλαγής χρησιμοποιώντας ένα αλγόριθμο κρυπτογράφησης.
ii. Έπειτα δημιουργεί μια ψηφιακή υπογραφή αφού κρυπτογραφήσει την τιμή Hash χρησιμοποιώντας το ιδιωτικό κλειδί.
iii. Τέλος αποστέλλει στον χρήστη "Jerry" την ψηφιακή υπογραφή μαζί με τα αρχικά δεδομένα της συναλλαγής.

Ο Jerry έχει τώρα στην κατοχή του τα δεδομένα της συναλλαγής και την ψηφιακή υπογραφή του χρήστη “Amy”. Για να ελέγξει την εγκυρότητα της συναλλαγής ο Jerry χρειάζεται να κάνει 2 ενέργειες:

i. να αποκρυπτογραφήσει την ψηφιακή υπογραφή με το δημόσιο κλειδί της Amy για να αποκτήσει το Hash
ii. να δημιουργήσει ένα 2ο Hash από τα δεδομένα που του έχουνε σταλεί.

Αν αυτά τα 2 Hash είναι ίδια τότε η συναλλαγή είναι έγκυρη.

1.6.4: Peer-to-Peer Δίκτυο

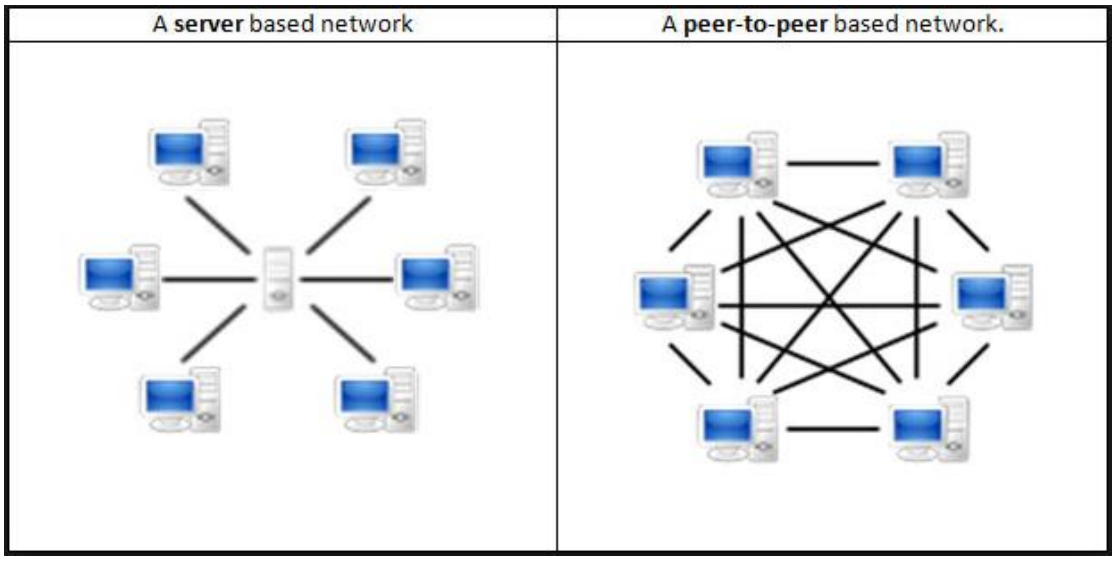
Οι χρήστες για να αλληλοεπιδράσουν με το Blockchain χρησιμοποιούν κατά κύριο λόγο ένα αποκεντρωμένο δίκτυο Peer-to-Peer (P2P) στο οποίο κάθε χρήστης αντιπροσωπεύει και έναν κόμβο. Για να θεωρείται όμως ο χρήστης κόμβος του δικτύου θα πρέπει να έχει ένα ηλεκτρονικό υπολογιστή με σχετικά μεγάλο αποθηκευτικό χώρο και συνδεδεμένο πάντα με το ίντερνετ. Επιπλέον οι χρήστες-κόμβοι του δικτύου προσφέρουν και λαμβάνουν υπηρεσίες μεταξύ τους αφού δεν υπάρχει κεντρικός εξυπηρετητής.

Όταν ένας χρήστης πραγματοποιεί συναλλαγή με ένα άλλο χρήστη ή όταν ένας κόμβος λαμβάνει δεδομένα από άλλο κόμβο, ελέγχετε η αυθεντικότητα των δεδομένων. Στη συνέχεια μεταδίδονται τα επικυρωμένα δεδομένα σε κάθε άλλο κόμβο που είναι συνδεδεμένος και σε πολύ μικρό χρονικό διάστημα τα δεδομένα

διαδίδονται σε όλο το δίκτυο. Το πλεονέκτημα της χρήσης ενός Peer-2-Peer δικτύου είναι ότι για την αποθήκευση και επιβεβαίωση της ορθότητας της κάθε συναλλαγής δεν χρειάζεται κάποιος ενδιάμεσος ή κάποια κεντρική αρχή, κάτι το οποίο κάνει το δίκτυο πιο ασφαλές από κακόβουλες επιθέσεις.

Ο Server ή αλλιώς εξυπηρετητής, στην πιο απλή του μορφή είναι ένας ηλεκτρονικός υπολογιστής που έχει κατάλληλο λογισμικό ώστε να εξυπηρετεί τα αιτήματα των χρηστών που συνδέονται με αυτόν. Επίσης τα δεδομένα των χρηστών είναι αποθηκευμένα σ, αυτόν τον κεντρικό εξυπηρετητή και αν για κάποιο λόγο χάσει την συνδεσιμότητα του στο δίκτυο τότε και όλοι οι υπόλοιποι χρήστες θα χάσουν την πρόσβαση στα δεδομένα τους.

Αντίθετα, στο δίκτυο Peer-to-Peer όλοι οι χρήστες έχουν όλα τους τα δεδομένων σε όλους τους συνδεδεμένους υπολογιστές, μπορούν να συνεχίσουν να λειτουργούν και να ανταλλάζουν δεδομένα ακόμη και αν κάποιοι από τους κόμβους χάσουν τη συνδεσιμότητα τους με το υπόλοιπο δίκτυο. Επίσης, τα Peer-to-Peer δίκτυα είναι πιο ισχυρά, καθώς δεν υπάρχει κεντρικός διακομιστής, οπότε το να πάψει να λειτουργεί ένα τέτοιο δίκτυο είναι εξαιρετικά δύσκολο. Στην παρακάτω εικόνα παρουσιάζεται στα αριστερά ένα δίκτυο με κεντρικό εξυπηρετητή και στα δεξιά ένα δίκτυο Peer-to-Peer:



Εικόνα 11 Peer to peer and server based network

(https://en.bitcoinwiki.org/wiki/Peer-to-peer)

1.6.5: Consensus Protocol

Κάθε Peer-2-Peer δίκτυο βασισμένο σε Blockchain μπορεί να λειτουργήσει σωστά μόνο με την πλήρη συναίνεση όλων των χρηστών, αφού δεν υπάρχει κεντρική αρχή για να παρέχει εμπιστοσύνη και ακεραιότητα στις πληροφορίες που ανταλλάζονται.

Για να υπάρξει λοιπόν συναίνεση, χρειάζεται ένας τρόπος για να αποφασιστεί ποια δεδομένα είναι έγκυρα και ποια όχι. Η διαδικασία της επικύρωσης των δεδομένων σε ένα δίκτυο Peer-to-Peer ονομάζεται εξόρυξη (mining) και απαιτεί τη χρήση σύνθετων αλγορίθμων όπως Proof-of-work, Proof of Stake και Practical Byzantine Fault Tolerance. Μέσω αυτής της διαδικασίας επιτυγχάνεται επίσης, η προσθήκη των επικυρωμένων μπλοκ από συναλλαγές στην αλυσίδα του Blockchain.

1.6.6: Proof of Work Δίκτυο

Ο αλγόριθμος Proof-of-Work (PoW) έχει ως κύριο στόχο να διασφαλίσει την διαδικασία επικύρωσης των δεδομένων και την αποτροπή επιθέσεων στο δίκτυο. Η ιδέα του αλγορίθμου αυτού υπήρχε και πριν από το Bitcoin, αλλά ο Satoshi Nakamoto εφάρμοσε για πρώτη φορά αυτήν την τεχνική στο ψηφιακό νόμισμά bitcoin. Στην πραγματικότητα, η ιδέα του αλγορίθμου PoW δημοσιεύθηκε αρχικά από τους Cynthia Dwork και Moni Naor το 1992 με τίτλο "Pricing via Processing or Combatting Junk Mail". Αργότερα μια παρόμοια πρόταση που ονομάζεται Hashcash προτάθηκε το 1997 από τον Adam Back αλλά ο όρος "Proof-of-Work" δημιουργήθηκε από τους Markus Jakobsson και Ari Juels σε έγγραφο με ονομασία «Proofs of Work and Bread Pudding Protocols (Extended Abstract)» που

δημοσιεύθηκε το 1999. Ο αλγόριθμος αυτός είναι ο πιο ευρέως χρησιμοποιούμενος αλγόριθμος στην τεχνολογία Blockchain.

Για να κατανοήσουμε τη λειτουργία του αλγορίθμου proof of work θα πρέπει να έχουμε υπόψη μας ότι κάθε φορά που πραγματοποιείται μια συναλλαγή στο δίκτυο Bitcoin, η συναλλαγή αυτή καταγράφεται και αποθηκεύεται σε ένα προσωρινό μπλοκ. Στη συνέχεια, μόλις το μπλοκ γεμίσει με συναλλαγές, μεταδίδεται σε όλους τους κόμβους που συμμετέχουν στο δίκτυο. Στην προκειμένη φάση όλοι οι κόμβοι θα πρέπει να ελέγξουν την εγκυρότητα ολόκληρου του μπλοκ. Σε αυτό το σημείο χρησιμοποιείται ο αλγόριθμος Proof-of-Work. Στη συνέχεια κάθε κόμβος προσθέτει ένα κομμάτι δεδομένου στο μπλοκ το οποίο ονομάζεται «nonce» και σχηματίζεται τελικά το «Block + nonce». Αυτό το «Block + nonce» τοποθετείται σε έναν αλγόριθμο κρυπτογράφησης με ονομασία SHA-256 (Secure Hash Algorithm). Με τη σειρά του αυτός ο αλγόριθμος παράγει ένα αλφαριθμητικό 64 χαρακτήρων το οποίο ονομάζεται Hash.

Το πρωτόκολλο του Bitcoin θέτει αυτόματα ένα στόχο (Difficulty target). Ο στόχος είναι το επίπεδο δυσκολίας που χρειάζεται ένας κόμβος για να επικυρώσει το μπλοκ. Όλοι οι κόμβοι στο δίκτυο συναγωνίζονται για το ποιος θα βρει πρώτος ένα αλφαριθμητικό Hash μικρότερο του στόχου. Το μόνο που μπορούν να κάνουν είναι κάθε φορά να αλλάζουν την τιμή του «nonce» και να τοποθετούνε το «Block + (καινούργιο)nonce» στον αλγόριθμο κρυπτογράφησης SHA256. Η διαδικασία της αλλαγής του «nonce» γίνεται αυτόματα και ο πρώτος κόμβος που θα βρει το σωστό αποτέλεσμα έχει επίσημα επικυρώσει τις συναλλαγές στο μπλοκ και κερδίζει ένα ποσό bitcoins. Τότε αποστέλλεται σε όλους τους υπόλοιπους κόμβους το «Block+ nonce + Hash» και αφού πιστοποιήσουν οι υπόλοιποι κόμβοι ότι είναι σωστή η λύση, τότε προσκολλάτε στην αλυσίδα του Blockchain. Μόλις ολοκληρωθεί η διαδικασία αυτή η οποία διαρκεί περίπου 10 λεπτά, οι κόμβοι αμέσως μαζεύουνε τις καινούργιες συναλλαγές και συναγωνίζονται πάλι για να βρούνε το σωστό «nonce» .

Εικόνα 12 Proof of work (https://wolfcone.com/proof-of-work-and-proof-of-stake-explained/)

1.6.7: Proof of Stake

Ο Proof-of-Stake (PoS) είναι ένας ακόμα αλγόριθμος, ο σκοπός του οποίου είναι ίδιος με τον αλγόριθμο Proof-of-Work. Εντούτοις η διαδικασία για την επικύρωση των συναλλαγών είναι αρκετά διαφορετική. Η πρώτη ιδέα του Proof-of-Stake προτάθηκε στο διαδικτυακό φόρουμ bitcointalk.org το 2011, αλλά το πρώτο κρυπτονόμισμα που έκανε χρήση αυτής της μεθόδου ήταν το Peercoin το 2012, μαζί με το ShadowCash, το Nxt, το BlackCoin, το NuShares/NuBits, το Qora και το NavCoin.

Σε αντίθεση με το Proof-of-Work όπου επικυρώνει τις συναλλαγές ο γρηγορότερος κόμβος, στο Proof-of-Stake, ο κόμβος που θα επικυρώσει τις συναλλαγές επιλέγεται με ντετερμινιστικό τρόπο. Οι κόμβοι δηλαδή, καταθέτουν στο δίκτυο ένα ποσό από τα κρυπτονομίσματα τους ως εγγύησή ότι θα επικυρώσουν τις συναλλαγές σε ένα μπλοκ. Το ποιος κόμβος τελικά θα επιλεγεί,

καθορίζεται από το ποσό που έχει καταθέσει. Για παράδειγμα, εάν η Μαρία καταθέσει 60 κρυπτονομίσματα, η Άννα 30 και η Κατερίνα 10, η Μαρία έχει 60% πιθανότητα να επικυρώσει το μπλοκ, η Άννα έχει 30% και η Κατερίνα 10%. Έτσι στο PoS εμπιστευόμαστε την αλυσίδα με την υψηλότερη εγγύηση. Επίσης δεν υπάρχει ανταμοιβή για την επικύρωση του κάθε μπλοκ, όμως ο κόμβος που θα επικυρώσει το μπλοκ λαμβάνει ένα ποσό από την κάθε συναλλαγή.

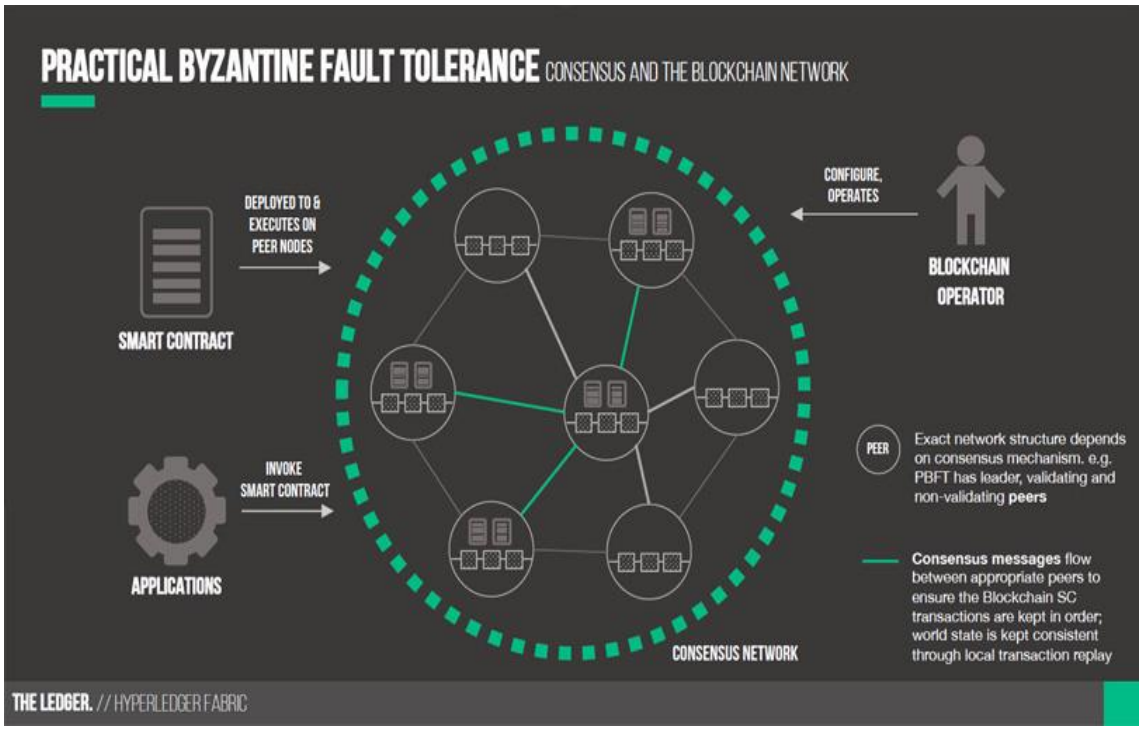
Εικόνα 13 Proof of stake (https://wolfcone.com/proof-of-work-and-proof-of-stake-explained/)

1.6.8: Practical Byzantine Fault Tolerance

Το 1999, οι Miguel Castro και Barbara Liskov εισήγαγαν τον αλγόριθμο "Practical Byzantine Fault Tolerance" (PBFT), που αποτέλεσε την πρώτη πρακτική λύση απέναντι στο πρόβλημα των Βυζαντινών Στρατηγών, η οποία έγινε αποδεκτή από όλους. Θα πρέπει να διευκρινιστεί στο σημείο αυτό ότι το πρόβλημα των Βυζαντινών Στρατηγών παρουσιάζεται όταν διαφορετικοί κόμβοι σε ένα αναξιόπιστο δίκτυο πρέπει να καταλήξουν σε μια τελική απόφαση, ελέγχοντας τα δεδομένα που

ανταλλάζονται. Παράλληλα ο αλγόριθμος «PBFT» θεωρήθηκε ως ο πρώτος πρακτικός αλγόριθμος που είναι κατάλληλος για χρήση σε ασύγχρονα δίκτυα.

Ο συγκεκριμένος αλγόριθμος χρησιμοποιείται από εξουσιοδοτημένα Blockchain δίκτυα όπως το Hyperledger Fabric, Ripple, Stellar και απαιτεί ο κάθε κόμβος να είναι γνωστός στο δίκτυο. Κάθε φορά που πραγματοποιείται μια συναλλαγή, επικυρώνεται μέσω μιας συγκεκριμένης διαδικασίας. Πιο αναλυτικά, σε κάθε φάση της διαδικασίας, επιλέγεται με βάση ορισμένους κανόνες ένας κύριος εισηγητής κόμβος, ο οποίος είναι υπεύθυνος να εξετάσει αν τα δεδομένα είναι σωστά. Αφού εξετάσει τα δεδομένα στέλνει τα αποτελέσματα σε όλους τους υπόλοιπους κόμβους του δικτύου. Ο εισηγητής θα περάσει στην επόμενη φάση εξέτασης των δεδομένων, αν τα 2/3 όλων των κόμβων έχουν ψηφίσει ότι συμφωνούν μαζί του. Αν οι ψήφοι είναι λιγότεροι, τότε εκλέγεται ένας καινούργιος εισηγητής. Η διαδικασία ολοκληρώνεται σε 3 φάσεις, όπου κάθε φάση ακολουθείται η ίδια διαδικασία.



Εικόνα 14 Practical Byzantine Fault Tolerance

(https://blockonomi.com/practical-byzantine-fault-tolerance/)

ΚΕΦ.2: Cryptocurency

Αντικείμενο αυτής της πτυχιακής εργασίας είναι να αναγνωρίσουμε και να αναλύσουμε τη σχέση μεταξύ blockchain και των υπάρχων κρυπτονομισμάτων. Ωστόσο για να γίνει αυτό, αν και πρώτα κατανοήσαμε το τι είναι το blockchain, θα πρέπει να κατανοήσουμε και τι είναι το κρυπτονόμισμα. Αρκετοί επενδύουν σε κρυπτονομίσματα ή ακόμα κανούν και αγορές με αυτό χωρίς όμως να γνωρίζουν ακριβώς τι είναι αυτό και τί σημαίνει ο όρος “επενδύω σε ένα κρυπτονόμισμα”. Τα περισσότερα κρυπτονομίσματα χρησιμοποιούν τεχνολογία blockchain για την καταγραφή συναλλαγών. Για παράδειγμα, το bitcoin και το Ethereum που είναι από τα πιο διαδεδομένα κρυπτονομίσματα βασίζονται και τα δύο σε blockchain.

Εικόνα 15 Αναπαράσταση κρυπτονομισμάτων (https://www.euronews.com/next/2021/06/08/what-are-cryptocurrencies-and-how-do-you-use-them-a-beginner-s-guide-to-cryptocurrencies)

2.1: Τι είναι το κρυπτονόμισμα;

Το κρυπτονόμισμα είναι ένα είδος νομίσματος που είναι ψηφιακό και αποκεντρωμένο. Τα κρυπτονομίσματα μπορούν να χρησιμοποιηθούν για την αγορά και πώληση αντικειμένων και η δυνατότητά τους να αποθηκεύουν και να αυξάνουν την αξία έχουν τραβήξει επίσης τα βλέμματα πολλών επενδυτών.

Υπάρχουν χιλιάδες διαφορετικά κρυπτονομίσματα διαθέσιμα σήμερα. Το πιο δημοφιλές - και το πρωτότυπο - είναι το Bitcoin, το οποίο δημιουργήθηκε το 2009. Άλλα κοινά κρυπτονομίσματα περιλαμβάνουν Ethereum, XRP και Bitcoin Cash. Κάθε ένα από αυτά τα νομίσματα εξυπηρετεί διαφορετικό σκοπό, με άλλα να είναι

σχεδιασμένα για χρήση αντί μετρητών και άλλα σχεδιασμένα για ιδιωτικές, άμεσες συναλλαγές.

Τα κρυπτονομίσματα είναι εντελώς ψηφιακά, επομένως δεν υπάρχει φυσικό νόμισμα ή λογαριασμός συνδεδεμένος με το κρυπτογράφημα που έχετε στην κατοχή σας. Αντ 'αυτού, οι ιδιοκτήτες κρατούν κρυπτονομίσματα σε ένα ψηφιακό πορτοφόλι και αγοράζουν ή πωλούν μέσω μιας διαδικτυακής ανταλλαγής. Το πορτοφόλι σας μπορεί να είναι online (ορισμένες δημοφιλείς ανταλλαγές όπως το Coinbase προσφέρουν ένα πορτοφόλι εντός εφαρμογής) ή να είναι αποθηκευμένο εκτός σύνδεσης σε μια συσκευή υλικού παρόμοια με μια μονάδα USB.

Η αποκέντρωση είναι το βασικό δόγμα του κρυπτονομίσματος. Ενώ τα περισσότερα νομίσματα υποστηρίζονται από μια κεντρική τράπεζα - το δολάριο ΗΠΑ, για παράδειγμα, υποστηρίζεται από την "πλήρη πίστη και πίστωση" της κυβέρνησης των ΗΠΑ - τα κρυπτονομίσματα διατηρούνται και αποτιμώνται από τους χρήστες τους.

Οι συναλλαγές κρυπτονομισμάτων καταγράφονται σε ένα αποκεντρωμένο βιβλίο. Εδώ παρεμβαίνει σε αρκετές περιπτώσεις το blockchain. Κάθε φορά που αγοράζουμε ή πουλάμε μέσω κρυπτονομίσματος, η συναλλαγή αυτη προστίθεται στο blockchain το οποίο όπως είπαμε αποτελεί μια δημόσια βάση δεδομένων των συναλλαγών, η οποία είναι διαθέσιμη σε άλλους κατόχους κρυπτογράφησης. Ο καθένας μπορεί να συμμετάσχει και να συμμετάσχει στο blockchain, αλλά τα δεδομένα για μεμονωμένες συναλλαγές και τα άτομα που εμπλέκονται σε αυτά διασφαλίζονται με χρήση κρυπτογραφίας η οποία αποτελεί τη βάση για τον ορισμό του κρυπτονομίσματος. Για κάθε συναλλαγή που προστίθεται στο blockchain, υπάρχει μια διαδικασία ψηφιακής επικύρωσης για την επαλήθευση και την πρόληψη της απάτης.

2.2: Ποια ανάγκη ήταν η αιτία της «γέννησης» του πρώτου κρυπτονομίσματος (bitcoin);

Υπήρχε πάντοτε σε κάποιους μια έμμονη ιδέα. Πως δεν θα ήταν καθόλου κακό οι άνθρωποι να μπορούν να κάνουν τις δοσοληψίες τους, όσο μακριά και αν είναι, χωρίς τη διαμεσολάβηση μιας τράπεζας ή και περισσοτέρων που θα εισπράξουν ένα καλό μερτικό με βάση το διακινούμενο ποσό. Το ποσό το εισπράττει η τράπεζα ως εγγυητής τού ότι θα γίνει σωστά η δοσοληψία χωρίς ο ένας να… ρίξει τον άλλον. Γιατί λοιπόν να μην τα βρούμε μεταξύ μας οι δύο πλευρές και να υπάρχει δίπλα μας ένας μηχανισμός που σχεδόν ανέξοδα θα εγγυάται και ότι ο πωλητής πήρε τα χρήματά του και ότι ο αγοραστής δεν θα κοροϊδέψει στέλνοντας σε έναν

πωλητή το ποσό που πρέπει και μετά αστραπιαία, μόλις επικυρωθεί η συναλλαγή, να το αποσύρει και να το στείλει και σε κάποιον άλλον; Επιπλέον κανείς εκτός από τους δύο δεν θα γνωρίζει λεπτομέρειες για τη συναλλαγή πέρα από το ότι αυτή έγινε.

2.3: Η ιστορία του bitcoin

Πώς δημιουργήθηκαν όμως τα κρυπτονομίσματα, και πιο συγκεκριμένα το bitcoin ως το πρώτο από αυτά; Η σχετική ιδέα αναπτύχθηκε για πρώτη φορά από ένα άγνωστο πρόσωπο ή ομάδα με το ψευδώνυμο Satoshi Nakamoto. Συγκεκριμένα, τον Οκτώβριο του 2008 ο Satoshi Nakamoto δημοσίευσε ένα άρθρο όπου περιέγραφε ένα σύστημα συναλλαγών σε πλήρως αποκεντρωμένο περιβάλλον, ανεξάρτητο από τρίτα μέρη και υποστηριζόμενο από την υποκείμενη τεχνολογία του blockchain. Η αληθινή ταυτότητα του Satoshi είναι ακόμη άγνωστη, εντούτοις υπάρχουν ενδείξεις ότι ο Satoshi δεν είναι ένα άτομο αλλά ομάδα, πιθανώς δυτικής καταγωγής. Μάλιστα, ο Satoshi προτάθηκε το 2015 για το βραβείο Νόμπελ στις οικονομικές επιστήμες για τη συμβολή του στη σύγχρονη οικονομία μέσω της εισαγωγής των κρυπτονομισμάτων στο σύστημα οικονομικών συναλλαγών.

Λίγους μήνες μετά, και συγκεκριμένα τον Ιανουάριο του 2009, η ιδέα του Satoshi ενσαρκώθηκε μέσω της γέννησης του bitcoin ως πρώτου κρυπτονομίσματος. Το bitcoin είναι μοναδικό στον σχεδιασμό του δεδομένου ότι η προσφορά του είναι πεπερασμένη- θα διατεθούν μόνο 21 εκατομμύρια bitcoin συνολικά παγκοσμίως σε καθορισμένες χρονικές περιόδους και επί του παρόντος 16,3 εκατομμύρια έχουν ήδη εξ ορυχθεί και διακινούνται στο διεθνές οικονομικό σύστημα. Το τελευταίο bitcoin προγραμματίζεται να εξ ορυχθεί το 2140, σημείο μετά το οποίο δεν θα μπορούν πλέον να εξορυχθούν νέα bitcoin. Τον Ιανουάριο του 2018, ο Satoshi κατείχε bitcoin συνολικής αξίας 16,5 δισεκατομμυρίων δολαρίων, ενώ περίπου 1.000 άτομα κατέχουν το 40% του συνολικού αριθμού bitcoin.

Στην αρχή της διακίνησής του, το bitcoin άξιζε μόνο λίγα λεπτά του Ευρώ. Κανένας χρήστης δεν χρησιμοποιούσε νόμιμο χρήμα για ν' αγοράσει bitcoin. Ο βασικός τρόπος απόκτησης bitcoin ήταν ν' αφιερώσει ο χρήστης την υπολογιστική ισχύ του υπολογιστή του για την επικύρωση συναλλαγών μέσα από το blockchain. Όταν ο υπολογιστής είχε επικυρώσει αρκετές συναλλαγές, επιβραβευόταν με την «εξόρυξη» ενός bitcoin, το οποίο ήταν η αμοιβή για τον χρόνο, την η λεκτρική ενέργεια και την υπολογιστική ισχύ που διέθεσε. Μέσα σε λίγα χρόνια ωστόσο

η αξία του Bitcoin εκτινάχθηκε, ξεπερνώντας την αξία μιας ουγκιάς χρυσού, και φτάνοντας μέχρι και τα $17.550 (περίπου 15.500 Ευρώ) για ένα bitcoin. Το bitcoin διακρίνεται από μεγάλες αυξομειώσεις στην αξία του, καθώς απώλεια ή κέρδος 10% της συνολικής αξίας του θεωρείται αναμενόμενη σε μια τυπική ημέρα συναλλαγών. Αυτή η μεγάλη διακύμανση καθιστά το bitcoin, και κάθε κρυπτονόμισμα, μια ιδιαίτερα κινδυνώδη επένδυση που μπορεί να αποφέρει ένα εξαιρετικά υψηλό κέρδος, αλλά μπορεί εξίσου να εξανεμίσει το κεφάλαιο του επενδυτή. Κατά τη συγγραφή του παρόντος άρθρου,η αξία ενός bitcoin ξεπερνούσε λίγο τα $4.100 (περίπου 3.625 Ευρώ).

Έτσι, το bitcoin πέρασε από το περιθώριο στην αναγνώρισή του απ' το ευρύ κοινό το 2017, καθώς μέχρι τότε η έννοια της ιδιοκτησίας και εμπορίας bitcoin με νόμιμο χρήμα θεωρείτο μάλλον ανορθόδοξη. Στα πρώτα χρόνια της δημιουργίας του bitcoin, κανένα κατάστημα δεν ήταν πρόθυμο να το δεχθεί ως μέσο πληρωμών. Η πρώτη αγορά προϊόντος με bitcoin έγινε στις 22 Μαΐου 2010, όταν ένας χρήστης πλήρωσε 10.000 bitcoin για μια πίτσα. Σήμερα, το bitcoin μπορεί να χρησιμοποιηθεί για την αγορά ποικίλων αγαθών και υπηρεσιών, από έναν καφέ μέχρι ένα αυτοκίνητο ή τα δίδακτρα φοίτησης σ' ένα εκπαιδευτικό ίδρυμα.

Παρά την καινοτομία του, το bitcoin έχει συχνά γίνει στόχος αρνητικών σχολίων. Για παράδειγμα, το 2017 ο Διευθύνων Σύμβουλος της μεγαλύτερης τράπεζας των ΗΠΑ, JP Morgan, δήλωσε ότι το bitcoin είναι μια απάτη που "απευθύνεται μόνο σε δολοφόνους και εμπόρους ναρκωτικών", ενώ τόνισε ότι θ' απολύσει κάθε εργαζόμενό του που συναλλάσσεται με το κρυπτονόμισμα ως "ανόητο". Ωστόσο, μετά την πτώση των τιμών του bitcoin, η JP Morgan άρχισε να συναλλάσσεται με το κρυπτονόμισμα, κάτι που ακούγεται αρχικά ως ειρωνία, αλλ' εν τέλει είναι καθόλα φυσιολογικό, δεδομένου ότι οι τράπεζες είναι επιχειρήσεις παροχής υπηρεσιών που λειτουργούν με τους νόμους της αγοράς.

Ποιοι είναι όμως οι κίνδυνοι που κρύβονται πίσω από την χρήση αμφίδρομων νομισμάτων, όπως το bitcoin; Πρώτον, τα κρυπτονομίσματα μπορούν να χρησιμοποιηθούν για τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες και χρηματοδότησης της τρομοκρατίας, λόγω της σχετικής ανωνυμίας και της ταχύτητας που προσφέρουν. Δεύτερον, η Ευρωπαϊκή Κεντρική Τράπεζα (ΕΚΤ) έχει προειδοποιήσει ότι τα εικονικά νομίσματα έχουν πολύ μεγάλη αστάθεια, και ότι η ευμετάβλητη τιμή τους μπορεί ν' αποσταθεροποιήσει την συστημική οικονομία. Τρίτον, τα κρυπτονομίσματα μπορεί να δημιουργήσουν κίνδυνο για την σταθερότητα των συστημάτων πληρωμής ευρύτερα καθώς δεν υπόκεινται σε κάποια ρυθμιστική εποπτεία. Επίσης, τα bitcoin είναι προσπελάσιμα μέσω ενός

ιδιωτικού κλειδιού το οποίο ο χρήστης πρέπει να γνωρίζει πάντοτε, αλλιώς χάνονται και κανείς άλλος δεν μπορεί να τα χρησιμοποιήσει ή να τ' ανακτήσει, κάτι που αποσταθεροποιεί την οικονομία λόγω και της πεπερασμένης φύσης των κρυπτονομισμάτων. Τέλος, η ευρύτερη χρήση των εικονικών νομισμάτων μπορεί να επηρεάσει την φήμη των κεντρικών τραπεζών και να δημιουργήσει μια πεπλανημένη αίσθηση κανονικότητας και ασφάλειας στη χρήση τους, αν η δημοφιλία τους αυξηθεί έτι περαιτέρω.

Το τελευταίο διάστημα το bitcoin έχει «απολαύσει» μια αρνητική φήμη ως εργαλείο έκνομης δραστηριότητας, και ως το κρυπτονόμισμα που προτιμούν οι εγκληματίες. Οι σχεδόν ανώνυμες ψηφιακές συναλλαγές το καθιστούν τόσο εύκολο στη διακίνησή του όσο το νόμιμο χρήμα. Είναι ενδεικτικό μάλιστα ότι η πλειοψηφία των λύτρων που ζητούνται από εγκληματικές δραστηριότητες καταβάλλεται συνήθως σε bitcoin λόγω της σχεδόν ανώνυμης φύσης του.

Εικόνα 16 Αναπαράσταση του bitcoin σαν νόμισμα (https://www.bbc.com/news/business-58309024)

2.4: Τι μπορείτε να κάνετε με το κρυπτονόμισμα;

Ενώ μοιράζεται τα χαρακτηριστικά τόσο του νομίσματος όσο και των επενδύσεων, εξακολουθεί να υπάρχει συζήτηση μεταξύ των ειδικών σχετικά με το

αν το κρυπτονόμισμα είναι ένα νόμισμα, μία μορφή σθναλλαγής ή αν είναι μία επένδυση που μπορεί να προσδώσει πολλά κέρδη στο μέλλον.

Όπως υποδηλώνει το όνομά του, μπορείτε να χρησιμοποιήσετε κρυπτονόμισμα για να κάνετε αγορές. Αλλά η αγοραστική σας δύναμη είναι περιορισμένη. Το crypto δεν είναι ακόμη ευρέως αποδεκτό μεταξύ των λιανοπωλητών και άλλων επιχειρήσεων.

Αυτή η έλλειψη ευρείας υιοθέτησης, καθώς και η μεταβλητότητα των κρυπτονομισμάτων, περιορίζει τη χρήση του ως νομίσματος, λέει ο Roger Aliaga-Díaz, κύριος και ανώτερος οικονομολόγος της Vanguard Investment Strategy Group.

Για πολλούς ανθρώπους, η κρυπτογράφηση είναι ένας τύπος εναλλακτικής επένδυσης. Όπως μπορείτε να αγοράσετε και να ανταλλάξετε μετοχές σε δημόσιες εταιρείες, μπορείτε να αγοράσετε κρυπτονομίσματα με την ελπίδα ότι θα αυξηθεί σε αξία με την πάροδο του χρόνου, επιτρέποντάς σας να εξαργυρώσετε κέρδη σε μεταγενέστερη ημερομηνία. Μερικοί επενδύουν σε κρυπτογράφηση λιγότερο για την πεποίθηση ότι θα γίνει δημοφιλές νόμισμα και περισσότερο ως στοίχημα στην τεχνολογία blockchain που βρίσκεται πίσω από αυτό.

Αλλά η ταξινόμηση των κρυπτονομισμάτων ως επένδυσης είναι επίσης περίπλοκη. Δεν ταιριάζει απόλυτα στο καλούπι μιας παραδοσιακής μετοχής ή ομολόγου, και ενώ τα κρυπτονομίσματα μοιράζονται χαρακτηριστικά αγαθών όπως ο χρυσός - μπορούν να αγοραστούν και να πωληθούν με μετρητά και ως παράγωγα με βάση την αναμενόμενη μελλοντική αξία - δεν έχουν εγγενή φυσική αξία ή χρήση.

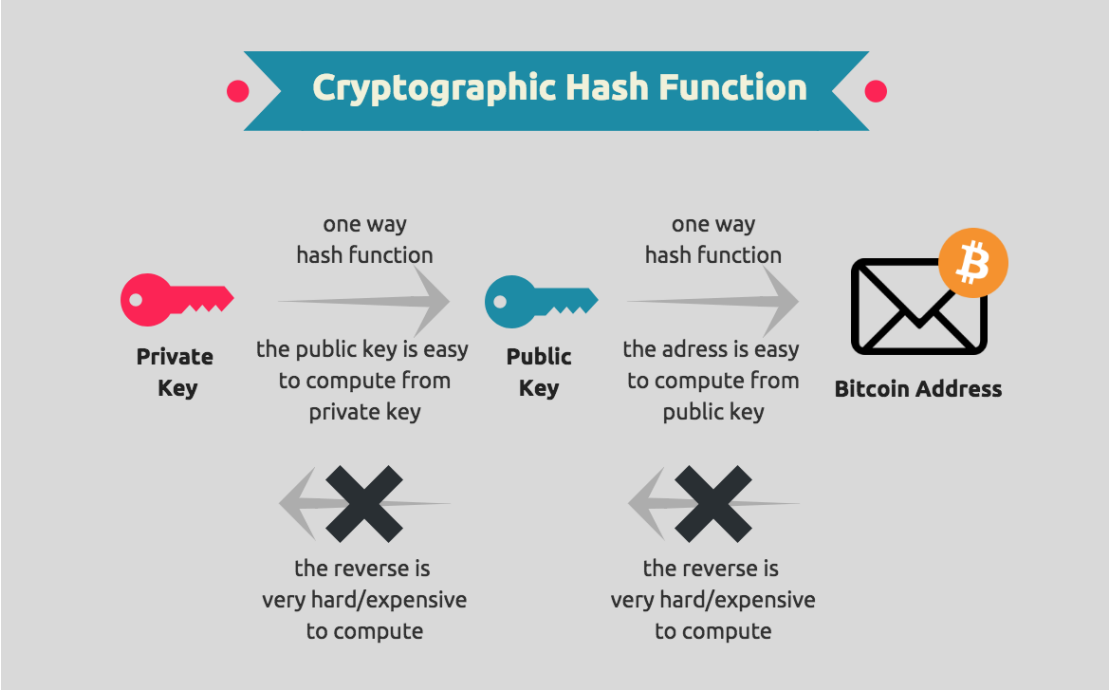
Χωρίς σαφές ιστορικό για την εκτίμηση της μακροπρόθεσμης αξίας, τα κρυπτονομίσματα αυξάνονται και πέφτουν σε έναν απρόβλεπτο κύκλο ζήτησης. Και για μεμονωμένους επενδυτές, η πρόκληση είναι ότι πραγματικά δεν ξέρετε πού μπορεί να καταλήξει η προσφορά και η ζήτηση άρα δεν ξέρετε που θα καταλήξει η αξία του νομίσματος σας.

Παρόμοια με τις συναλλαγές τέτοιου συναλλάγματος, μπορεί να υπάρχουν σημαντικοί κίνδυνοι για μια σε μεγάλο βαθμό μη ρυθμιζόμενη αγορά και το καλύτερο στοίχημά σας είναι να ενημερωθείτε εκ των προτέρων και να μην επενδύσετε χρήματα που δεν μπορείτε να χάσετε. Οι ρυθμιστικές αρχές εξακολουθούν να προσπαθούν να καταλάβουν πώς να ταξινομήσουν τα κρυπτονομίσματα, για σκοπούς συναλλαγών, πληρωμών, καταπολέμησης της απάτης, φορολογίας και άλλα. Η σαφής ρύθμιση μπορεί να μας βοηθήσει να καταλάβουμε πώς να χρησιμοποιούμε το κρυπτονόμισμα και πώς μπορεί να μοιάζει το μέλλον του, αλλά δεν είμαστε ακόμα εκεί.

2.5: Τι είναι αυτό που κρυπτογραφείται στη συναλλαγή με κρυπτονόμισμα;

Από την πρώτη φορά που κάποιος θέλει να πραγματοποιήσει μια δοσοληψία με bitcoin «γεννιούνται» για λογαριασμό του δύο (κρυπτογραφικά) κλειδιά. Το ιδιωτικό και το δημόσιο. Το καθένα είναι ένα μείγμα από αριθμούς και γράμματα. Το ιδιωτικό το ξέρει μόνο ο ιδιοκτήτης, είναι η προσωπική του ταυτότητα και το φυλάει όσο μπορεί καλύτερα .

Με βάση το ιδιωτικό δημιουργείται και το δημόσιο κλειδί, που κοινοποιείται σε αυτούς που συναλλάσσεται μαζί τους κάποιος. Υπάρχουν δε και ειδικοί εξυπηρετητές δημόσιων κλειδιών (public key servers), στους οποίους μπορεί κανείς να απευθυνθεί για να βρει το δημόσιο κλειδί του χρήστη που τον ενδιαφέρει ή να ανεβάσει το δικό του δημόσιο κλειδί για να είναι διαθέσιμο στο κοινό. Διότι η γνώση του δημόσιου κλειδιού κρυπτογράφησης δεν επιτρέπει με κανέναν τρόπο τον υπολογισμό του ιδιωτικού κλειδιού κρυπτογράφησης. Ομως τα δύο αυτά κλειδιά (ιδιωτικό και δημόσιο) έχουν μαθηματική σχέση μεταξύ τους. Εάν το ένα χρησιμοποιηθεί για την κρυπτογράφηση κάποιου μηνύματος, τότε το άλλο χρησιμοποιείται για την αποκρυπτογράφησή του.



Εικόνα 17 Κρυπτογραφία στις συναλλαγές bitcoin (https://blockchainhub.net/blog/blog/cryptography-blockchain-bitcoin/)

2.5.1: Πώς δουλεύουν τα δύο αυτά κλειδιά;

Για παράδειγμα, η διάθεση ένας ποσού για αγορά κρυπτογραφείται και κατά κάποιον τρόπο «σφραγίζεται» από το ιδιωτικό κλειδί με τα χαρακτηριστικά του αποστολέα. Από το δημόσιο κλειδί του, που είναι ένας ολόκληρος «συρμός» από ψηφία, ύστερα από συμπίεση και συντόμευση προκύπτει η λεγόμενη «δημόσια διεύθυνση» του καθενός. Εχουμε δηλαδή: Ιδιωτικό κλειδί > Δημόσιο κλειδί >δημόσια διεύθυνση. Οι δύο συναλλασσόμενοι έχουν γνωστοποιήσει ο ένας στον άλλον στην ουσία μόνο ένας δημόσιες διευθύνσεις ένας και τίποτε άλλο. Αυτές παίζουν τον ρόλο του αριθμού λογαριασμού που χρησιμοποιείται ένας τραπεζικές συναλλαγές (ενώ, κατά κάποιον τρόπο, το ιδιωτικό κλειδί θυμίζει λίγο το PIN). Συνδυάζοντας τα δύο παραπάνω είναι εφικτό να επιτύχουμε εμπιστευτικότητα του μηνύματος και πιστοποίηση του αποστολέα. Δηλαδή αφενός το μήνυμα παραμένει γνωστό μονάχα στον αποστολέα και στον παραλήπτη και αφετέρου ο παραλήπτης γνωρίζει με ασφάλεια ποιος του έστειλε το μήνυμα. Για να επιτευχθεί αυτό, ο αποστολέας μπορεί να κρυπτογραφήσει το μήνυμα πρώτα με το δικό του ιδιωτικό κλειδί και στη συνέχεια με το δημόσιο κλειδί του παραλήπτη. Ένας ο παραλήπτης λάβει το μήνυμα, θα πρέπει να χρησιμοποιήσει το ιδιωτικό του κλειδί για να το αποκρυπτογραφήσει (εμπιστευτικότητα) και στη συνέχεια, χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα, να βεβαιωθεί πως ήταν εκείνος που έστειλε το μήνυμα ή το ποσό.

Η δοσοληψία, για να είναι πλέον γεγονός, πρέπει να εμφανιστεί κάπου δημόσια, να ελεγχθεί για την εγκυρότητά ένας και να μείνει καταγεγραμμένη για πάντα. Χωρίς υπερβολή υπάρχουν καταχωρισμένες και προσβάσιμες (χωρίς τα προσωπικά στοιχεία αυτών που ένας πραγματοποίησαν, αλλά μόνο με ένας δημόσιες διευθύνσεις ένας) ένας οι δοσοληψίες από την πρώτη που έγινε το 2009!
Η κάθε συναλλαγή, ένας είναι η μεταφορά χρημάτων από τον έναν στον άλλον, κρυπτογραφείται με μια μέθοδο κατακερματισμού (hashing), ένας λέγεται. Με αυτή παράγεται ένας πολυψήφιος αριθμός (hash) που ενσωματώνει τα δεδομένα ένας συναλλαγής. Μαζί είναι το ιδιωτικό και το δημόσιο κλειδί κάθε χρήστη. Το ίδιο συμβαίνει και με ένας ένας συναλλαγές, έως ότου συμπληρωθεί ένας αριθμός συναλλαγών, που εντάσσονται σε ένα μπλοκ του 1 Mbyte. Τα κρυπτογραφικά στοιχεία κάθε συναλλαγής που δημιουργούνται (δηλαδή οι αριθμοί που παράγονται μέσω ένας διαδικασίας hashing) κρυπτογραφούνται και άλλο. Ανά δύο ή περισσότερες συναλλαγές, ένας με την ίδια μέθοδο, έως ότου δημιουργηθεί ένας τελικός «αριθμός hash», αντίστοιχος τελικά στο συγκεκριμένο μπλοκ.

2.5.2: Ποιος ελέγχει αν όλα έγιναν σωστά;

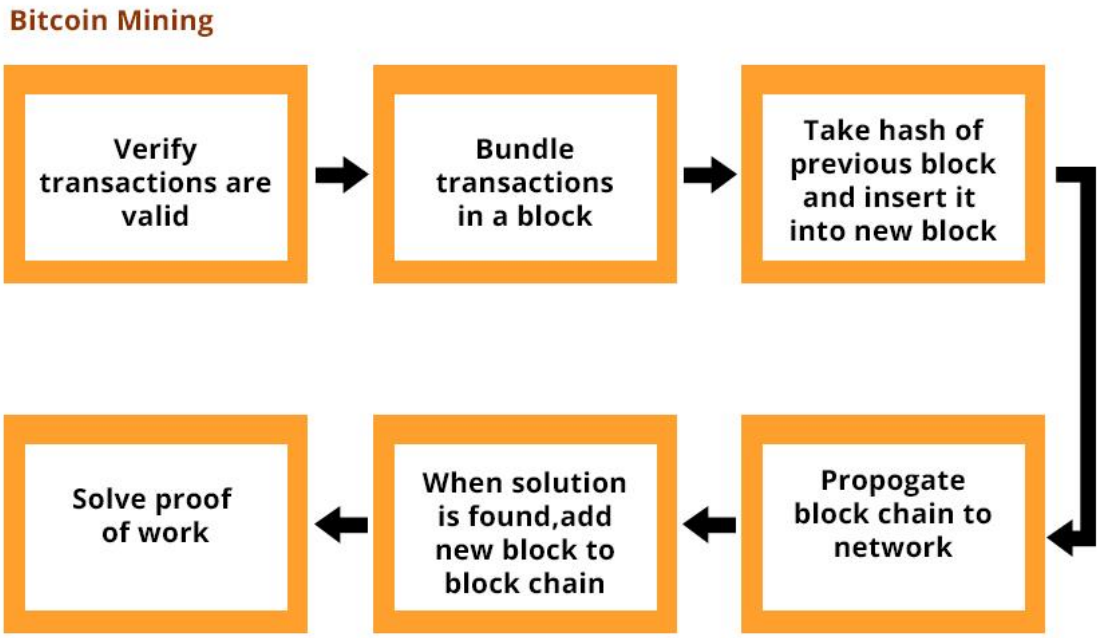
Υπάρχουν πλέον κάπου 12.000 σταθμοί ελέγχου, κόμβοι σε ένα παγκόσμιο δίκτυο και όλοι λαμβάνουν γνώση της (κάθε) δοσοληψίας σε bitcoin. Εκτελούν ο

καθένας χωριστά έλεγχο για το αν από αυτή τη διεύθυνση που στάλθηκε η εντολή πληρωμής υπήρχε πραγματικά το συγκεκριμένο ποσό και στέλνεται ένα σήμα έγκρισης ή μη. Είναι σαν να παίζουν κάποιοι μπριτζ (ή και πρέφα) μέσω υπολογιστή. Ο καθένας χωριστά καταγράφει τους πόντους όλων ύστερα από κάθε παρτίδα και πριν ξεκινήσουν την επόμενη συγκρίνουν το τι έγραψαν για να είναι βέβαιοι πως όλοι έχουν καταχωρίσει τα ίδια.

Μπορεί σε ένα μπλοκ να υπάρχει μόνο μια δοσοληψία, αλλά μπορεί να είναι και χιλιάδες. Αυτοί που βρίσκονται πίσω από τα μηχανήματα πιστοποίησης είναι οι miners, οι άνθρωποι των εξορύξεων δηλαδή, που πρέπει πρώτα να πιστοποιήσουν τις συναλλαγές και να τις εντάξουν σε μπλοκ.
Όταν θα είναι έτοιμο το μπλοκ με τις εγκεκριμένες δοσοληψίες, πρέπει να καταχωριστεί σε ένα μεγάλο ηλεκτρονικό λογιστικό βιβλίο (ledger). Εκεί θα ενταχθεί (=συνδεθεί) ως άλλος ένας κρίκος στην αλυσίδα των προηγούμενων μπλοκ (blockchain). Έχει σημασία όμως το ποιος από όλους θα έχει το προνόμιο να το εντάξει στην αλυσίδα κερδίζοντας και την ανταμοιβή (6,25 bitcoin σήμερα). Το κυνήγι αρχίζει. Πρέπει λοιπόν να λυθεί ένας μαθηματικός «γρίφος», στην ουσία να μαντέψει το μηχάνημα κάποιου από τους εξορύκτες έναν αριθμό με 64 ψηφία που προκύπτει μέσω μιας εξαιρετικά περίπλοκης μαθηματικής εργασίας.

2.5.3: Χρήση των υπολογιστών

Οι υπολογιστές κάποιου από τους εξορύκτες πρέπει να πέσουν κοντά σε έναν αριθμό, χωρίς να τον ξεπεράσουν, που αποτελείται κάθε φορά από 64 ψηφία στο δεκαεξαδικό σύστημα (δηλαδή αυτό που χρησιμοποιεί τους αριθμούς από το 1 έως το 10 και τα γράμματα A, B, C, D, E, F). Ο βαθμός δυσκολίας ρυθμίζεται ξανά μετά τη διεκπεραίωση μιας ομάδας από 2.016 μπλοκ, προς τα επάνω ή προς τα κάτω, ανάλογα με το πλήθος των υπολογιστών που συμμετέχουν, για να τηρείται ο χρόνος της διεκπεραίωσης ενός μπλοκ ανά 10 λεπτά περίπου. Και αυτό χρονικά αντιστοιχεί σε διάστημα δύο εβδομάδων περίπου. Τον Απρίλιο του 2021 ο βαθμός δυσκολίας να πετύχεις τον αριθμό των 64 ψηφίων με τη μία αναλογούσε σε μια πιθανότητα 1 στα 23 τρισεκατομμύρια. Αλλά αν λάβουμε υπ’ όψιν πως οι κυνηγοί διαθέτουν εξαιρετικά γρήγορους υπολογιστές, ειδικά ρυθμισμένους για τη δουλειά αυτή, ώστε να κάνουν δισεκατομμύρια ή και χιλιάδες δισεκατομμύρια μαντεψιές ανά δευτερόλεπτο, κάποιος πέφτει όσο χρειάζεται κοντά περίπου κάθε 10 λεπτά. Ένας είναι πάντα ο νικητής.



Εικόνα 18 Bitcoin mining (https://www.supportsages.com/bitcoin-mining/)

2.5.4: Γιατί είναι γνωστοί ως εξορύκτες (miners) ή και χρυσωρύχοι;

Για όλη αυτή τη δουλειά που κάνουν, τον έλεγχο των δοσοληψιών και τον διαγ(κ)ωνισμό για τον 64ψήφιο αριθμό, όποιος έχει τακτοποιήσει ένα μπλοκ θα πάρει ως αμοιβή ένα ποσό σε (τι άλλο από) bitcoin. Είναι δηλαδή σαν να βρίσκει κοσκινίζοντας τους αριθμούς έναν μικρό βόλο από χρυσάφι.

2.5.6: Πόσο αξίζει αυτός ο βόλος χρυσού;

Κάθε τέσσερα χρόνια είναι προσυμφωνημένο η τιμή για την οικειοποίηση ενός μπλοκ να πέφτει στο μισό. Ξεκίνησε από τα 50 bitcoin, το 2012 έγινε 25, από τον Μάιο του 2020 είναι στα 6,25. Βέβαια αυτή την εβδομάδα (στις 19/4) η ισοτιμία ήταν 1 bitcoin = 46.223 ευρώ, ενώ στις 11/4/2021 είχε σκαρφαλώσει στα 53.193 ευρώ. Μέχρι σήμερα έχουν εξορυχθεί περίπου 18,5 εκατομμύρια bitcoin και τελικά έχει οριστεί να μην ξεπεράσουν τα 21 εκατομμύρια, που υπολογίζουν πως θα τα φτάσουν περίπου το 2.140, αν «ζήσει» μέχρι τότε.

Μετά οι εξορύκτες, όσοι θα έχουν μείνει, θα παίρνουν μόνο ένα ποσό επί των συναλλαγών που υπολογίζεται να είναι μερικές χιλιάδες δολάρια για κάθε

μπλοκ, ενώ σήμερα αυτό είναι μερικές εκατοντάδες δολάρια. Κάπως μικρό σε σχέση με τα 6,25 bitcoin και την τωρινή ισοτιμία.
Επειδή πάντως κοστίζει πλέον πολύ αυτή η ενασχόληση (πριν από 10 χρόνια αρκούσε ένας δυνατός υπολογιστής στο σπίτι, σήμερα χρειάζονται υπολογιστικά τερατάκια ειδικά φτιαγμένα για να βγαίνουν κάποια bitcoin), πολλοί συνασπίζονται δημιουργώντας «αγέλες υπολογιστών» με σκοπό να μοιράζονται τα κέρδη, ενώ φτάνουν και στα βάθη της Ασίας, ακόμα και στη Μογγολία, για να βρουν φθηνή ηλεκτρική ενέργεια για τα αδηφάγα μηχανήματά τους!Δημιουργείτε όμως ένα ερώτημα: **Και με το τακτοποιημένο πλέον μπλοκ τι γίνεται;**

Προσαρτάται στην αρχή του ο χαρακτηριστικός αριθμός από την κωδικοποίηση μέσω κατακερματισμού του προηγούμενου μπλοκ, επίσης ακριβής ώρα, λεπτό, δευτερόλεπτο και ημερομηνία δημιουργίας. Οποιος προσπαθήσει να αλλάξει κάτι σε προηγούμενα μπλοκ πρέπει μετά να αλλάξει όλους τους κωδικούς στους κρίκους της αλυσίδας και αυτό κάθε άλλο από εύκολο θα ήταν.

2.5.7: Πώς καθορίζεται η ισοτιμία του με τα άλλα νομίσματα;

Από την προσφορά, τη ζήτηση, τους συγκυρίες και αναταράξεις στην παγκόσμια οικονομία, τη συμπεριφορά διαφόρων κρατών. Η απόφαση τους Τουρκίας πριν από λίγες ημέρες να απαγορεύσει τους συναλλαγές με κρυπτονομίσματα επέφερε πτώση στην τιμή. Λέγεται πως και τους Ηνωμένες Πολιτείες σκέπτονται να κάνουν πολύ πιο ασφυκτικούς τους ελέγχους. Το 2017, μέσα σε έναν χρόνο, η τιμή του από τα 19.000 δολάρια έπεσε στα 4.000 δολάρια.

2.5.8: Πώς αποκτάται

Υπάρχουν ανταλλακτήρια και στο Διαδίκτυο αλλά και κάποια σε πόλεις της Ελλάδας, αλλά θέλει μεγάλη προσοχή με ποιον συναλλάσσεται κάποιος. Αυτή την εβδομάδα η τιμή του κυμαινόταν γύρω στα 46.105 ευρώ.

2.6: Είναι ασφαλές το Crypto;

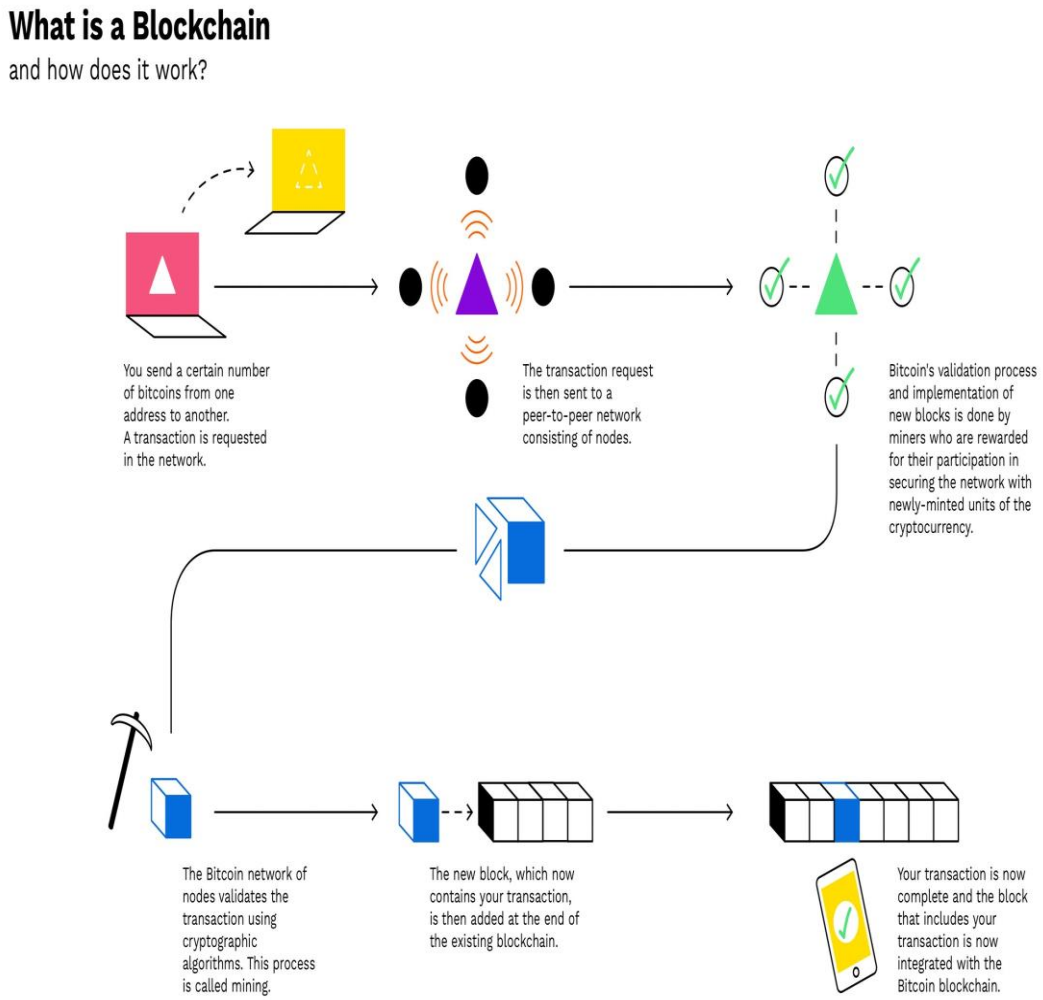
Η τεχνολογία blockchain που υποστηρίζει το κρυπτονόμισμα είναι εγγενώς ασφαλής, χάρη στην αποκεντρωμένη - και δημόσια - φύση της τεχνολογίας κατανεμημένων καθολικών και τη διαδικασία κρυπτογράφησης που υφίσταται κάθε συναλλαγή.

Αλλά αυτό δεν σημαίνει ότι είναι απολύτως ασφαλές με τον ίδιο τρόπο που οι περισσότεροι άνθρωποι θεωρούν το δολάριο ΗΠΑ ή άλλα καθιερωμένα νομίσματα ασφαλή. Δεδομένου ότι το κρυπτονόμισμα δεν υποστηρίζεται από καμία κυβερνητική αρχή, δεν έχει την ίδια προστασία με πολλά τυποποιημένα νομίσματα σε όλο τον κόσμο.

Σε αντίθεση με τα χρήματα που εξοικονομείτε σε μια τράπεζα που ασφαλίζεται από την Federal Deposit Insurance Corporation (FDIC), "Εάν μια εταιρεία εικονικών νομισμάτων αποτύχει - και πολλοί έχουν - η κυβέρνηση δεν θα καλύψει τη ζημία", προειδοποίησε το Γραφείο Οικονομικής Προστασίας Καταναλωτών σε ανακοίνωση του 2014 σχετικά με το κρυπτονόμισμα (η πιο πρόσφατη καθοδήγησή του).

Το CFPB αναφέρει πιο συγκεκριμένους κινδύνους για τους οποίους πρέπει να είναι προετοιμασμένοι οι καταναλωτές, συμπεριλαμβανομένων των ασταθών συναλλαγματικών ισοτιμιών, των πιθανών υψηλών τελών στις πλατφόρμες συναλλάγματος και του κινδύνου απάτης. Εάν τα κεφάλαιά σας χαθούν ή κλαπούν, μπορεί να είναι ιδιαίτερα δύσκολο να ανακτηθούν, χάρη στην αποκεντρωμένη φύση του blockchain και την έλλειψη κυβερνητικής εποπτείας.

Και, το σημαντικότερο, μόνο και μόνο επειδή το κρυπτονόμισμα είναι ασφαλές δεν το καθιστά τελείως ασφαλές. Όσο η πρόσφατη δημοτικότητα του κρυπτονομίσματος οφείλεται στην πεποίθηση των επενδυτών στην αξία του, αυτή η αξία εξακολουθεί να βασίζεται στην κερδοσκοπία. Για όσους επενδύουν σε κρυπτογράφηση, θα είναι από τις πιο επικίνδυνες επενδύσεις που κάνουν.



Εικόνα 19 Συναλλαγή bitcoin (https://www.bitpanda.com/academy/en/lessons/how-does-a-blockcha)

2.7: Bitcoin και Ethereum

Ο Αιθέρας (ETH), το κρυπτονόμισμα του δικτύου Ethereum, είναι αναμφισβήτητα το δεύτερο πιο δημοφιλές ψηφιακό διακριτικό μετά το bitcoin (BTC). Πράγματι, ως το δεύτερο μεγαλύτερο κρυπτονόμισμα κατά όριο αγοράς, οι συγκρίσεις μεταξύ Αιθέρα και BTC είναι φυσιολογικές.

Ο αιθέρας και το bitcoin μοιάζουν με πολλούς τρόπους: το καθένα είναι ένα ψηφιακό νόμισμα που διαπραγματεύεται μέσω διαδικτυακών ανταλλαγών και αποθηκεύεται σε διάφορους τύπους πορτοφολιών κρυπτονομισμάτων. Και οι δύο αυτές μάρκες είναι αποκεντρωμένες, πράγμα που σημαίνει ότι δεν εκδίδονται ή ρυθμίζονται από κεντρική τράπεζα ή άλλη αρχή. Και οι δύο κάνουν χρήση της τεχνολογίας

blockchain. Ωστόσο, υπάρχουν επίσης πολλές κρίσιμες διαφορές μεταξύ των δύο πιο δημοφιλών κρυπτονομισμάτων ανά όριο αγοράς. Παρακάτω, θα ρίξουμε μια πιο προσεκτική ματιά στις ομοιότητες και τις διαφορές μεταξύ bitcoin και αιθέρα.

2.7.1: Ομοιότητες

Τόσο το Bitcoin όσο και το Ethereum είναι αποκεντρωμένα προϊόντα και επομένως δεν ελέγχονται από κυβέρνηση ή άλλη κεντρική αρχή. Και τα δύο είναι χτισμένα σε κατανεμημένες δομές, γνωστές ως blockchain, το οποίο είναι ιδανικά ανθεκτικό σε παραβιάσεις (τεχνολογικοί ειδικοί με εξωφρενικά ακριβά εργαλεία μπορούν να λειτουργήσουν γύρω από την προστασία της πλατφόρμας).

Τα Blockchain ελέγχονται από ένα αποκεντρωμένο δίκτυο ατόμων που έχουν κίνητρα να φροντίζουν σωστά το δίκτυο. Οι ανθρακωρύχοι Bitcoin και Ethereum πληρώνονται για την επικύρωση δεδομένων που είναι αποθηκευμένα σε κάθε blockchain. Οποιαδήποτε μεμονωμένη προσπάθεια απάτης θα εντοπιστεί αμέσως από την πλειοψηφία και δεν θα κερδίσει χρήματα για την υποβολή ψευδών δεδομένων. Τα blockchains είναι αμετάβλητα εφόσον η πλειοψηφία του δικτύου δεν είναι κακόβουλη.

2.7.2: Διαφορές

Ενώ και τα δύο δίκτυα Bitcoin και Ethereum τροφοδοτούνται από την αρχή των κατανεμημένων καθολικών και της κρυπτογραφίας, τα δύο διαφέρουν τεχνικά με πολλούς τρόπους. Για παράδειγμα, οι συναλλαγές στο δίκτυο Ethereum ενδέχεται να περιέχουν εκτελέσιμο κώδικα, ενώ τα δεδομένα που τοποθετούνται σε συναλλαγές δικτύου Bitcoin είναι γενικά μόνο για την τήρηση σημειώσεων. Άλλες διαφορές περιλαμβάνουν το χρόνο μπλοκ (μια συναλλαγή αιθέρα επιβεβαιώνεται σε δευτερόλεπτα σε σύγκριση με τα λεπτά για bitcoin) και τους αλγόριθμους στους οποίους εκτελούνται (το Ethereum χρησιμοποιεί ethash ενώ το Bitcoin χρησιμοποιεί SHA-256).

Το πιο σημαντικό, όμως, είναι ότι τα δίκτυα Bitcoin και Ethereum διαφέρουν ως προς τους γενικούς στόχους τους. Ενώ το bitcoin δημιουργήθηκε ως εναλλακτική λύση στα εθνικά νομίσματα και έτσι φιλοδοξεί να είναι μέσο ανταλλαγής και αποθήκη αξίας, το Ethereum προοριζόταν ως πλατφόρμα για τη διευκόλυνση αμετάβλητων συμβάσεων μέσω προγραμματισμού και εφαρμογών μέσω του δικού του νομίσματος.

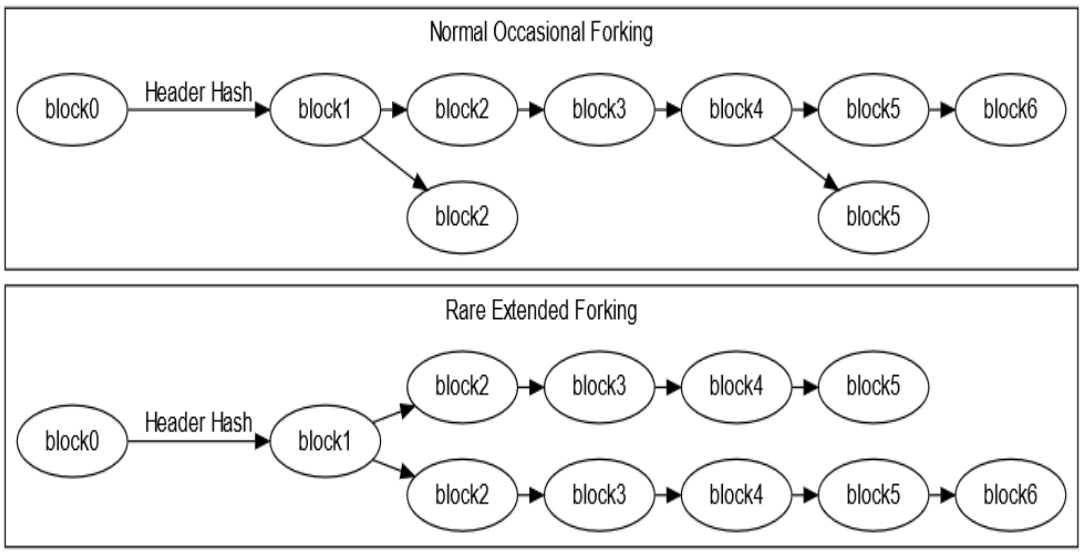
Το BTC και το ETH είναι και τα δύο ψηφιακά νομίσματα, αλλά ο πρωταρχικός σκοπός του αιθέρα δεν είναι να καθιερωθεί ως εναλλακτικό νομισματικό σύστημα, αλλά μάλλον να διευκολύνει και να δημιουργήσει έσοδα από τη λειτουργία της έξυπνης σύμβασης Ethereum και της αποκεντρωμένης πλατφόρμας εφαρμογής (dapp).

Το Ethereum είναι μια άλλη περίπτωση χρήσης για ένα blockchain που υποστηρίζει το δίκτυο Bitcoin και θεωρητικά δεν πρέπει να ανταγωνίζεται πραγματικά το Bitcoin. Ωστόσο, η δημοτικότητα του αιθέρα τον ώθησε σε ανταγωνισμό με όλα τα κρυπτονομίσματα, ειδικά από την πλευρά των εμπόρων. Για το μεγαλύτερο μέρος της ιστορίας του από τα μέσα του 2015, ο αιθέρας βρίσκεται πολύ πίσω από το bitcoin στην κατάταξη των κορυφαίων κρυπτονομισμάτων ανά όριο αγοράς. Τούτου λεχθέντος, είναι σημαντικό να έχουμε κατά νου ότι το οικοσύστημα του αιθέρα είναι πολύ μικρότερο από αυτό του bitcoin: από τον Ιανουάριο του 2020, το όριο αγοράς του αιθέρα ήταν μόλις κάτω από 16 δισεκατομμύρια δολάρια, ενώ το bitcoin είναι σχεδόν 10 φορές μεγαλύτερο από 147 δισεκατομμύρια δολάρια.

ΚΕΦ.3: Τεχνικα χαρακτηριστικά μεταξύ blockchain και bitcoins

3.1:Ύψος block και Fork

Οποιοσδήποτε ανθρακωρύχος Bitcoin που κατακερματίζει με επιτυχία μια κεφαλίδα μπλοκ σε μια τιμή κάτω από το όριο στόχου μπορεί να προσθέσει ολόκληρο το μπλοκ στην αλυσίδα μπλοκ (υποθέτοντας ότι το μπλοκ είναι διαφορετικά έγκυρο). Αυτά τα μπλοκ αντιμετωπίζονται συνήθως από το ύψος του μπλοκ τους - τον αριθμό των μπλοκ μεταξύ τους και το πρώτο μπλοκ Bitcoin (μπλοκ 0, πιο γνωστό ως μπλοκ γένεσης).



Εικόνα 20 Συνηθισμένα και ασυνήθιστα forks (https://developer.bitcoin.org/devguide/block_chain.html)

Όλα τα πολλαπλά μπλοκ μπορούν να έχουν το ίδιο ύψος μπλοκ, όπως συμβαίνει συνήθως όταν δύο ή περισσότεροι ανθρακωρύχοι παράγουν ο καθένας ένα μπλοκ περίπου την ίδια στιγμή. Αυτό δημιουργεί ένα εμφανές fork στην αλυσίδα μπλοκ, όπως φαίνεται στην παραπάνω εικόνα.

Όταν οι ανθρακωρύχοι παράγουν ταυτόχρονα μπλοκ στο τέλος της αλυσίδας μπλοκ, κάθε κόμβος επιλέγει ξεχωριστά ποιο μπλοκ θα δεχτεί. Ελλείψει άλλων προβληματισμών, που συζητούνται παρακάτω, οι κόμβοι συνήθως χρησιμοποιούν το πρώτο μπλοκ που βλέπουν.

Τελικά ένας ανθρακωρύχος παράγει ένα άλλο μπλοκ το οποίο προσαρτάται μόνο σε ένα από τα ανταγωνιστικά μπλοκ που εξορύσσονται ταυτόχρονα. Αυτό καθιστά εκείνη την πλευρά του fork ισχυρότερη από την άλλη πλευρά. Αν υποθέσουμε ότι ένα fork περιέχει μόνο έγκυρα μπλοκ, ακολουθείτε πάντα τη πιο δύσκολη αλυσίδα για να αναδημιουργήσουν και να πετάξουν τα μπαγιάτικα μπλοκ που ανήκουν σε κοντύτερα forks. (Τα παλιά μπλοκ ονομάζονται επίσης μερικές φορές ορφανά ή ορφανά μπλοκ, αλλά αυτοί οι όροι χρησιμοποιούνται επίσης για αληθινά ορφανά μπλοκ χωρίς γνωστό γονικό μπλοκ.)

Τα μακροπρόθεσμα forks είναι δυνατά εάν διαφορετικοί ανθρακωρύχοι εργάζονται για πολλαπλούς σκοπούς, όπως ορισμένοι ανθρακωρύχοι που εργάζονται επιμελώς για να επεκτείνουν την αλυσίδα μπλοκ την ίδια στιγμή που άλλοι ανθρακωρύχοι επιχειρούν μια επίθεση 51 τοις εκατό για να αναθεωρήσουν το ιστορικό συναλλαγών.

Δεδομένου ότι πολλά μπλοκ μπορούν να έχουν το ίδιο ύψος κατά τη διάρκεια μιας Fork αλυσίδας μπλοκ, το ύψος του μπλοκ δεν πρέπει να χρησιμοποιείται ως παγκόσμιο μοναδικό αναγνωριστικό. Αντ 'αυτού, τα μπλοκ αναφέρονται συνήθως με το hash της κεφαλίδας τους (συχνά με την αντίστροφη σειρά των byte, και δεκαεξαδική).

3.2: Δεδομένα συναλλαγής

Κάθε μπλοκ πρέπει να περιλαμβάνει μία ή περισσότερες συναλλαγές. Η πρώτη από αυτές τις συναλλαγές πρέπει να είναι συναλλαγή coinbase, που ονομάζεται επίσης συναλλαγή γενιάς, η οποία πρέπει να συλλέγει και να δαπανά την ανταμοιβή μπλοκ (αποτελείται από επιδότηση μπλοκ και τυχόν τέλη συναλλαγής που πληρώνονται από συναλλαγές που περιλαμβάνονται σε αυτό το μπλοκ).

Το UTXO μιας συναλλαγής coinbase έχει την ειδική προϋπόθεση ότι δεν μπορεί να δαπανηθεί (να χρησιμοποιηθεί ως είσοδος) για τουλάχιστον 100 μπλοκ. Ο όρος UTXO αναφέρεται στο ποσό του ψηφιακού νομίσματος που έχει απομείνει από κάποιον μετά την εκτέλεση μιας συναλλαγής κρυπτονομισμάτων όπως το bitcoin. Τα γράμματα αντιπροσωπεύουν το αχρησιμοποίητο αποτέλεσμα συναλλαγών. Αυτό εμποδίζει προσωρινά έναν ανθρακωρύχο να ξοδέψει τα τέλη συναλλαγής και να αποκλείσει την ανταμοιβή από ένα μπλοκ που μπορεί αργότερα να προσδιοριστεί ως παρωχημένο (και συνεπώς η συναλλαγή coinbase καταστράφηκε) μετά από ένα δίκρανο αλυσίδας μπλοκ.

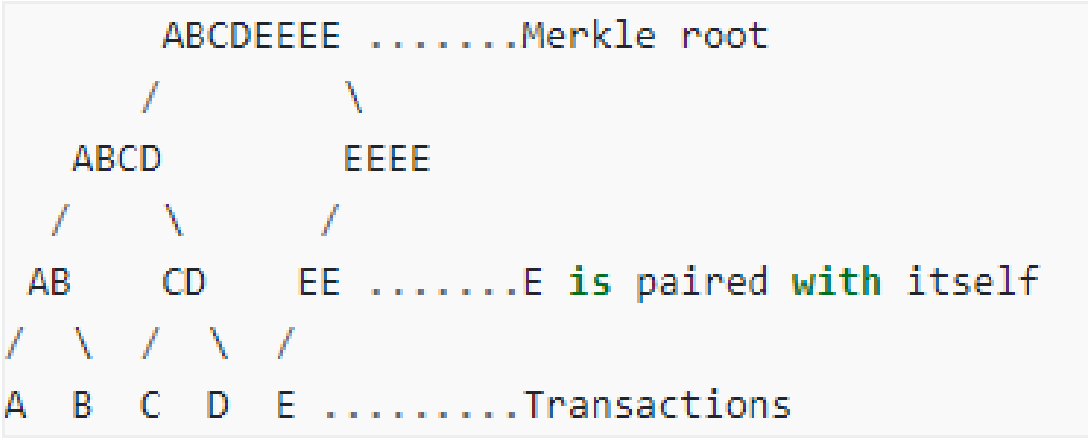
Τα μπλοκ δεν απαιτείται να περιλαμβάνουν οποιεσδήποτε συναλλαγές χωρίς coinbase, αλλά οι ανθρακωρύχοι σχεδόν πάντα περιλαμβάνουν επιπλέον συναλλαγές προκειμένου να εισπράξουν τα τέλη συναλλαγής τους. Όλες οι συναλλαγές, συμπεριλαμβανομένης της συναλλαγής coinbase, κωδικοποιούνται σε μπλοκ σε μορφή δυαδικής ακατέργαστης συναλλαγής.

Η ακατέργαστη μορφή συναλλαγής κατακερματίζεται για να δημιουργήσει το αναγνωριστικό συναλλαγής (txid). Από αυτά τα txids, το δέντρο merkle κατασκευάζεται συνδυάζοντας κάθε txid με ένα άλλο txid και στη συνέχεια τα συνδέει μαζί. Εάν υπάρχει περιττός αριθμός txids, το txid χωρίς συνεργάτη κατακερματίζεται με ένα αντίγραφο του εαυτού του.

Οι ίδιοι οι κατακερματισμοί που προκύπτουν συνδυάζονται ο καθένας με έναν άλλο κατακερματισμό και κατακερματίζονται μαζί. Οποιοσδήποτε κατακερματισμός χωρίς συνεργάτη κατακερματίζεται με τον εαυτό του. Η διαδικασία επαναλαμβάνεται μέχρι να παραμείνει μόνο ένας κατακερματισμός, η ρίζα merkle.

Το δέντρο Merkle είναι μια δομή δεδομένων που χρησιμοποιείται σε εφαρμογές επιστήμης υπολογιστών. Σε bitcoin και άλλα κρυπτονομίσματα, τα δέντρα Merkle χρησιμεύουν για την κωδικοποίηση των δεδομένων blockchain πιο αποτελεσματικά και με ασφάλεια. Αναφέρονται επίσης ως "δυαδικά δέντρα κατακερματισμού" (binary hash trees).

Για παράδειγμα, εάν οι συναλλαγές ήταν απλώς συνδεδεμένες (όχι κατακερματισμένες), ένα δέντρο merkle πέντε συναλλαγών θα μοιάζει με την ακόλουθη εικόνα:



Εικόνα 21Merkle (https://developer.bitcoin.org/devguide/block_chain.html)

Όπως συζητήθηκε στην υποενότητα Απλοποιημένη Επαλήθευση Πληρωμής (SPV), το δέντρο merkle επιτρέπει στους πελάτες να επαληθεύσουν μόνοι τους ότι μια συναλλαγή συμπεριλήφθηκε σε ένα μπλοκ, αποκτώντας τη ρίζα merkle από μια κεφαλίδα μπλοκ και μια λίστα των ενδιάμεσων κατακερματισμών από έναν πλήρη ομότιμο. Δεν χρειάζεται εμπιστοσύνη στον πλήρη ομότιμο χρήστη: είναι ακριβό να ψεύδονται κεφαλίδες μπλοκ και οι ενδιάμεσοι κατακερματισμοί δεν μπορούν να παραποιηθούν ή η επαλήθευση θα αποτύχει.

Για παράδειγμα, για να επαληθεύσει ότι η συναλλαγή D προστέθηκε στο μπλοκ, ένας πελάτης SPV χρειάζεται μόνο ένα αντίγραφο των κατακερματισμών C, AB και EEEE εκτός από τη ρίζα merkle. ο πελάτης δεν χρειάζεται να γνωρίζει τίποτα για οποιαδήποτε άλλη συναλλαγή. Εάν οι πέντε συναλλαγές σε αυτό το μπλοκ ήταν όλες στο μέγιστο μέγεθος, η λήψη ολόκληρου του μπλοκ θα απαιτούσε πάνω από 500.000 bytes - αλλά η λήψη τριών κατακερματισμών συν την κεφαλίδα μπλοκ απαιτεί μόνο 140 byte.

Εάν εντοπιστούν πανομοιότυπα txids στο ίδιο μπλοκ, υπάρχει πιθανότητα το δέντρο merkle να συγκρουστεί με ένα μπλοκ με μερικά ή όλα τα διπλότυπα να αφαιρεθούν λόγω του τρόπου με τον οποίο εφαρμόζονται τα μη ισορροπημένα δέντρα merkle (αντιγράφοντας το μοναδικό κατακερματισμό). Δεδομένου ότι είναι

ανέφικτο να υπάρχουν ξεχωριστές συναλλαγές με πανομοιότυπα txids, αυτό δεν επιβαρύνει το τίμιο λογισμικό, αλλά πρέπει να ελέγχεται εάν πρόκειται να αποθηκευτεί η μη έγκυρη κατάσταση ενός μπλοκ. Διαφορετικά, ένα έγκυρο μπλοκ με τα διπλότυπα που έχουν εξαλειφθεί θα μπορούσε να έχει την ίδια ρίζα merkle και μπλοκ μπλοκ, αλλά να απορριφθεί από το προσωρινά αποθηκευμένο μη έγκυρο αποτέλεσμα, με αποτέλεσμα σφάλματα ασφαλείας

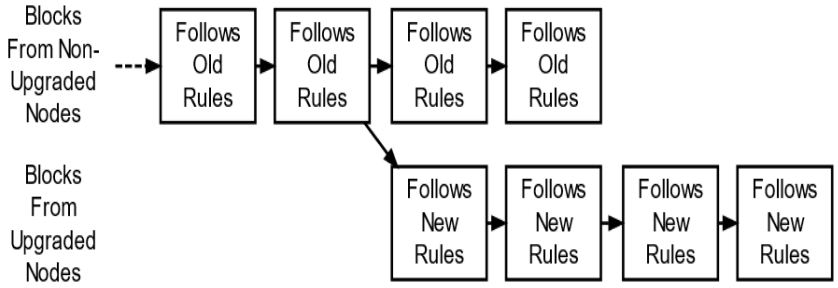
3.3:Αλλαγές κανόνα συναίνεσης

Για να διατηρηθεί η συναίνεση, όλοι οι πλήρεις κόμβοι επικυρώνουν μπλοκ χρησιμοποιώντας τους ίδιους κανόνες συναίνεσης. Ωστόσο, μερικές φορές οι κανόνες συναίνεσης αλλάζουν για να εισαχθούν νέες δυνατότητες ή να αποφευχθεί η κατάχρηση δικτύου. Όταν εφαρμοστούν οι νέοι κανόνες, πιθανότατα θα υπάρξει μια χρονική περίοδος που οι μη αναβαθμισμένοι κόμβοι θα ακολουθούν τους παλιούς κανόνες και οι αναβαθμισμένοι κόμβοι θα ακολουθούν τους νέους κανόνες, δημιουργώντας δύο πιθανούς τρόπους για να σπάσει η συναίνεση.

Ένα μπλοκ που ακολουθεί τους νέους κανόνες συναίνεσης γίνεται αποδεκτό από αναβαθμισμένους κόμβους αλλά απορρίπτεται από μη αναβαθμισμένους κόμβους. Για παράδειγμα, μια νέα λειτουργία συναλλαγής χρησιμοποιείται μέσα σε ένα μπλοκ: οι αναβαθμισμένοι κόμβοι κατανοούν τη λειτουργία και την αποδέχονται, αλλά οι μη αναβαθμισμένοι κόμβοι την απορρίπτουν επειδή παραβαίνει τους παλιούς κανόνες.

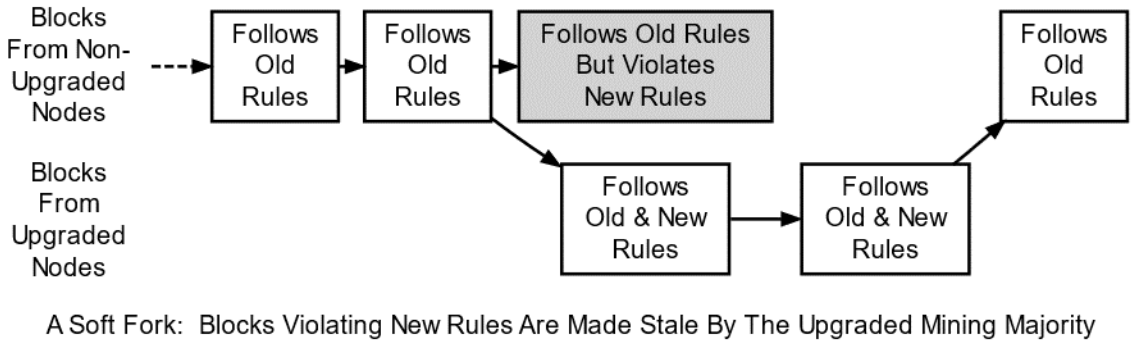
Ένα μπλοκ που παραβιάζει τους νέους κανόνες συναίνεσης απορρίπτεται από αναβαθμισμένους κόμβους αλλά γίνεται αποδεκτό από μη αναβαθμισμένους κόμβους. Για παράδειγμα, μια καταχρηστική λειτουργία συναλλαγής χρησιμοποιείται μέσα σε ένα μπλοκ: οι αναβαθμισμένοι κόμβοι την απορρίπτουν επειδή παραβαίνει τους νέους κανόνες, αλλά οι μη αναβαθμισμένοι κόμβοι την αποδέχονται επειδή ακολουθεί τους παλιούς κανόνες.

Στην πρώτη περίπτωση, η απόρριψη από μη αναβαθμισμένους κόμβους, το λογισμικό εξόρυξης που λαμβάνει δεδομένα αλυσίδας μπλοκ από αυτούς τους μη αναβαθμισμένους κόμβους αρνείται να βασιστεί στην ίδια αλυσίδα με το λογισμικό εξόρυξης που λαμβάνει δεδομένα από αναβαθμισμένους κόμβους. Αυτό δημιουργεί μόνιμα αποκλίνουσες αλυσίδες-μία για μη αναβαθμισμένους κόμβους και μία για αναβαθμισμένους κόμβους-που ονομάζονται hard Fork.



Εικόνα 22 Hard Fork (https://developer.bitcoin.org/devguide/block_chain.html)

Στη δεύτερη περίπτωση, απόρριψη από αναβαθμισμένους κόμβους, είναι δυνατό να αποφύγετε τη μόνιμη απόκλιση της αλυσίδας μπλοκ εάν οι αναβαθμισμένοι κόμβοι ελέγχουν το μεγαλύτερο μέρος του ρυθμού κατακερματισμού. Αυτό συμβαίνει γιατί, σε αυτήν την περίπτωση, οι μη αναβαθμισμένοι κόμβοι θα δεχτούν ως έγκυρα όλα τα ίδια μπλοκ με τους αναβαθμισμένους κόμβους, οπότε οι αναβαθμισμένοι κόμβοι μπορούν να δημιουργήσουν μια ισχυρότερη αλυσίδα που οι μη αναβαθμισμένοι κόμβοι θα δεχτούν ως την καλύτερη έγκυρη αλυσίδα μπλοκ. Αυτό ονομάζεται soft fork.



Εικόνα 23 Soft fork (https://developer.bitcoin.org/devguide/block_chain.html)

Παρόλο που το fork είναι μια πραγματική απόκλιση στις αλυσίδες μπλοκ, οι αλλαγές στους κανόνες συναίνεσης περιγράφονται συχνά από τη δυνατότητά τους να δημιουργήσουν είτε σκληρό είτε soft fork.Για παράδειγμα, "η αύξηση του μεγέθους μπλοκ πάνω από 1 MB απαιτεί hard fork." Σε αυτό το παράδειγμα, δεν απαιτείται πραγματικά fork αλυσίδας μπλοκ - αλλά είναι πιθανό αποτέλεσμα.

Οι αλλαγές κανόνα συναίνεσης μπορεί να ενεργοποιηθούν με διάφορους τρόπους. Κατά τη διάρκεια των δύο πρώτων ετών του Bitcoin, ο Satoshi Nakamoto πραγματοποίησε αρκετά soft forks μόλις απελευθερώσει την αλλαγή που είναι συμβατή προς τα πίσω σε έναν πελάτη που άρχισε να εφαρμόζει αμέσως τον νέο κανόνα. Πολλά soft forks όπως το BIP30 έχουν ενεργοποιηθεί μέσω μιας ημέρας σημαίας όπου ο νέος κανόνας άρχισε να εφαρμόζεται σε μια προκαθορισμένη ώρα ή σε ύψος μπλοκ. Τέτοια forks που ενεργοποιούνται μέσω ημέρας σημαίας είναι γνωστά ως User Activated Soft Forks (UASF) καθώς εξαρτώνται από την ύπαρξη επαρκών χρηστών (κόμβων) για την επιβολή των νέων κανόνων μετά την ημέρα της σημαίας.

Αργότερα soft forksπερίμεναν την πλειοψηφία του ποσοστού κατακερματισμού (τυπικά 75% ή 95%) για να σηματοδοτήσουν την ετοιμότητά τους να επιβάλουν τους νέους κανόνες συναίνεσης. Μόλις περάσει το όριο σηματοδότησης, όλοι οι κόμβοι θα αρχίσουν να εφαρμόζουν τους νέους κανόνες.

Αυτά τα forks είναι γνωστά ως Miner Activated Soft Forks (MASF) καθώς εξαρτώνται από τους ανθρακωρύχους για ενεργοποίηση.

3.4: Ανίχνευση forks

Οι μη αναβαθμισμένοι κόμβοι ενδέχεται να χρησιμοποιούν και να διανέμουν λανθασμένες πληροφορίες και στους δύο τύπους forks δημιουργώντας διάφορες καταστάσεις που θα μπορούσαν να οδηγήσουν σε οικονομική απώλεια. Συγκεκριμένα, οι μη αναβαθμισμένοι κόμβοι μπορούν να αναμεταδίδουν και να δέχονται συναλλαγές που θεωρούνται άκυρες από αναβαθμισμένους κόμβους και έτσι δεν θα γίνουν ποτέ μέρος της παγκοσμίως αναγνωρισμένης καλύτερης αλυσίδας μπλοκ. Οι μη αναβαθμισμένοι κόμβοι μπορούν επίσης να αρνηθούν τη μετάδοση μπλοκ ή συναλλαγών που έχουν ήδη προστεθεί στην καλύτερη αλυσίδα μπλοκ ή σύντομα θα γίνουν, και έτσι να παρέχουν ελλιπείς πληροφορίες.

Το Bitcoin Core περιλαμβάνει κώδικα που ανιχνεύει ένα hard fork εξετάζοντας την απόδειξη της αλυσίδας μπλοκ της εργασίας. Εάν ένας μη αναβαθμισμένος κόμβος λάβει κεφαλίδες αλυσίδας μπλοκ που δείχνουν τουλάχιστον έξι μπλοκ περισσότερη απόδειξη εργασίας από την καλύτερη αλυσίδα που θεωρεί έγκυρη, ο κόμβος αναφέρει μια προειδοποίηση στα αποτελέσματα RPC "getnetworkinfo" και εκτελεί την εντολή -alertnotify εάν οριστεί. Αυτό προειδοποιεί τον χειριστή ότι ο μη αναβαθμισμένος κόμβος δεν μπορεί να μεταβεί στην πιο πιθανή αλυσίδα μπλοκ.

Οι πλήρεις κόμβοι μπορούν επίσης να ελέγξουν τους αριθμούς έκδοσης μπλοκ και συναλλαγών. Εάν οι αριθμοί έκδοσης μπλοκ ή συναλλαγής που εμφανίζονται σε πολλά πρόσφατα μπλοκ είναι υψηλότεροι από τους αριθμούς έκδοσης που χρησιμοποιεί ο κόμβος, μπορεί να υποθέσει ότι δεν χρησιμοποιεί τους τρέχοντες κανόνες συναίνεσης. Το Bitcoin Core αναφέρει αυτήν την κατάσταση μέσω της εντολής "getnetworkinfo" RPC και -alertnotify εάν έχει οριστεί.

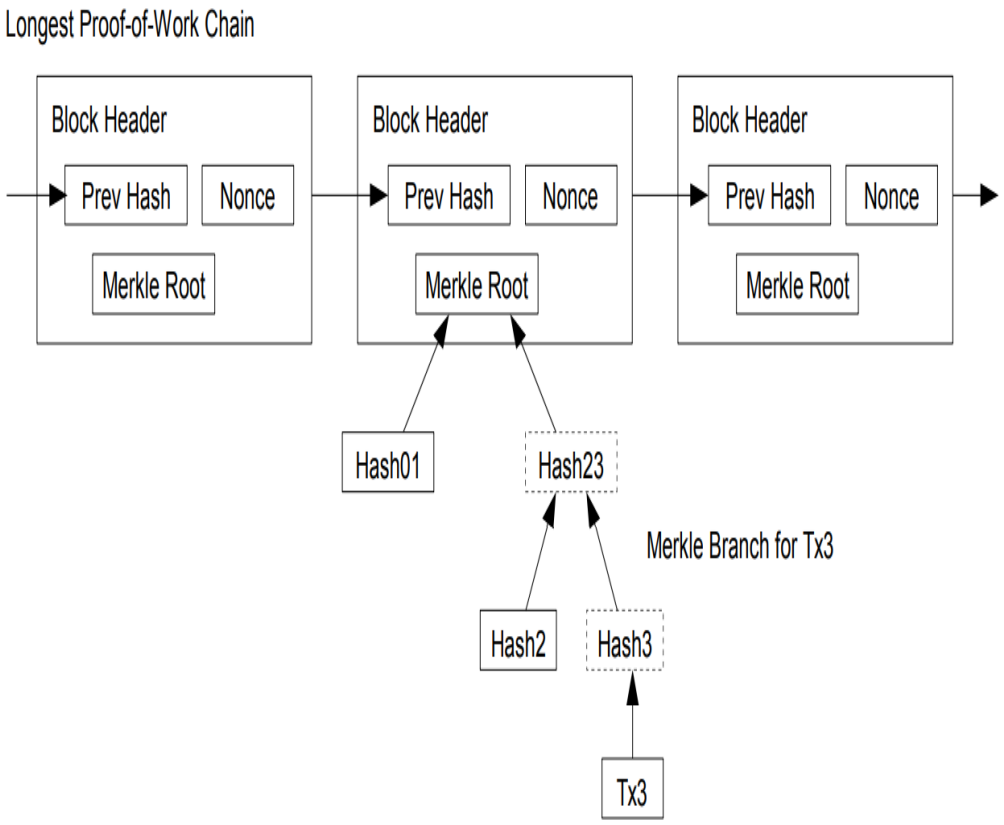
Σε κάθε περίπτωση, τα δεδομένα αποκλεισμού και συναλλαγών δεν πρέπει να βασίζονται εάν προέρχονται από έναν κόμβο που προφανώς δεν χρησιμοποιεί τους τρέχοντες κανόνες συναίνεσης.

Οι πελάτες SPV που συνδέονται με πλήρεις κόμβους μπορούν να ανιχνεύσουν ένα πιθανό hard fork συνδέοντας σε πολλούς πλήρεις κόμβους και διασφαλίζοντας ότι όλοι βρίσκονται στην ίδια αλυσίδα με το ίδιο ύψος μπλοκ, συν ή πλην πολλών μπλοκ για να εξηγήσουν τις καθυστερήσεις μετάδοσης και τα παλιά μπλοκ. Εάν υπάρχει απόκλιση, ο πελάτης μπορεί να αποσυνδεθεί από κόμβους με ασθενέστερες αλυσίδες.

3.5: Simple Verification Payment (SPV)

Η απλή επαλήθευση πληρωμής (SPV) είναι μια τεχνική που περιγράφεται στο έγγραφο του Satoshi Nakamoto. Το SPV επιτρέπει σε έναν πελάτη να επαληθεύσει ότι μια συναλλαγή περιλαμβάνεται στο blockchain Bitcoin, χωρίς να γίνει λήψη ολόκληρου του blockchain. Ο πελάτης SPV χρειάζεται μόνο λήψη των κεφαλίδων μπλοκ, οι οποίες είναι πολύ μικρότερες από τις πλήρεις ομάδες. Για να επαληθεύσει ότι μια συναλλαγή βρίσκεται σε μπλοκ, ένας πελάτης SPV ζητά απόδειξη συμπερίληψης, με τη μορφή Merkle.

Οι πελάτες SPV προσφέρουν μεγαλύτερη ασφάλεια από τα πορτοφόλια ιστού, επειδή δεν χρειάζεται να εμπιστεύονται τους διακομιστές με τις πληροφορίες που στέλνουν. Οι πελάτες SPV θα πρέπει επίσης να παρακολουθούν τις αυξήσεις αριθμού έκδοσης μπλοκ και συναλλαγών για να διασφαλίσουν ότι επεξεργάζονται τις ληφθείσες συναλλαγές και δημιουργούν νέες συναλλαγές χρησιμοποιώντας τους τρέχοντες κανόνες συναίνεσης.



Εικόνα 24 SPV (https://medium.com/coinmonks/spv-proofs-explained-f38f8bb8f580)

ΚΕΦ 4: ΣΥΜΠΕΡΑΣΜΑΤΑ

Εν κατακλείδι, το blockchain ως ένα μέσο αποθήκευσης πληροφορίας είναι μια τεχνολογία που έχει ανοίξει πολλές πόρτες σε πολλούς τομείς. Λόγω όμως της δομής του κάποιοι προσπάθησαν να το εκμεταλλευτούν και να το χρησιμοποιήσουν για αθέμιτους λόγους. Όμως τα θετικά του και οι θετικές χρήσεις του είναι περισσότερες από τις αρνητικές. Γι' αυτό και χρησιμοποιήθηκε σε μεγάλο βαθμό από τα ανερχόμενα και πλέον πολύ διάσημα κρυπτονομίσματα. Η χρήση του για τις συναλλαγές και το mining των κρυπτονομισμάτων και ειδικά του bitcoin είναι κομβικής σημασίας για την ανάπτυξη του κρυπτονομίσματος. Από τη μεριά τους τα κρυπτονομίσματα όπως το bitcoin επωφελήθηκαν αρκετά από αυτή τα blockchains και δεν φαίνεται να την αποχωρίζονται για πολλά χρόνια ακόμα. Ωστόσο όσο περνάει ο καιρός θα βλέπουμε όλο και πιο πολλές χρήσεις του blockchain στην υγεία, στις ψηφοφορίες και σε άλλους τομείς. Παράδειγμα αυτού αποτελεί η IBM με το Food Trust. Σιγά σιγά και όσο μειώνονται αρνητικά του blockchain θα το συναντάμε όλο και πιο συχνά.

ΒΙΒΛΙΟΓΡΑΦΙΑ ΚΑΙ ΠΗΓΕΣ

- A. (2018, December 9). *Η Χρήση Κρυπτονομισμάτων για Παράνομες Δραστηριότητες και Σχετικές Νομοθετικές Πρωτοβουλίες*. The Art of Crime. https://theartofcrime.gr/%CE%B7-%CF%87%CF%81%CE%AE%CF%83%CE%B7-%CE%BA%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%BD%CE%BF%CE%BC%CE%B9%CF%83%CE%BC%CE%AC%CF%84%CF%89%CE%BD-%CE%B3%CE%B9%CE%B1-%CF%80%CE%B1%CF%81%CE%AC%CE%BD%CE%BF%CE%BC/#_ftn
- *Bitcoin: A Peer-to-Peer Electronic Cash System*. (n.d.). Bitcoin. https://bitcoin.org/en/bitcoin-paper
- *Bitcoin vs. Ethereum: What's the Difference?* (n.d.). Investopedia. https://www.investopedia.com/articles/investing/031416/bitcoin-vs-ethereum-driven-different-purposes.asp
- *Block Chain — Bitcoin*. (n.d.). Https://Developer.Bitcoin.Org/. https://developer.bitcoin.org/devguide/block_chain.html
- *Blockchain Explained*. (2021, May 31). Investopedia. https://www.investopedia.com/terms/b/blockchain.asp#what-is-blockchain
- Curran, B. (2020, April 18). *What is Practical Byzantine Fault Tolerance? Complete Beginner's Guide*. Blockonomi. https://blockonomi.com/practical-byzantine-fault-

tolerance/?fbclid=IwAR0MXLjzQWyssq8R6NuK-keKLDvL2vsoi8Xy8t9T3zQy0MoCPN4MCgbPT9I

- Ethereum. (n.d.). *What is Ethereum?* Ethereum.Org. https://ethereum.org/en/what-is-ethereum/
- Kaspersky. (2021, May 26). *Polys from Kaspersky Innovation Hub presents first blockchain-based voting machine*. Www.Kaspersky.Com. https://www.kaspersky.com/about/press-releases/2020_polys-from-kaspersky-innovation-hub-presents-first-blockchain-based-voting-machine?fbclid=IwAR2unBDE9lQdp0Zl1aVQ4LpzRtCT2Xy36xzkjweSqTlutO_hJnyamP5XzYM
- NextAdvisor. (2021, August 30). *What is Cryptocurrency?* NextAdvisor with TIME. https://time.com/nextadvisor/investing/cryptocurrency/what-is-cryptocurrency/?fbclid=IwAR3FIEPx2EnyMFDPDMsqM-ymjtdyoMxYuDVddSvjGrU0X00yP58tfWo12Hc
- PricewaterhouseCoopers. (n.d.). *Making sense of bitcoin, cryptocurrency and blockchain*. PwC. https://www.pwc.com/us/en/industries/financial-services/fintech/bitcoin-blockchain-cryptocurrency.html?fbclid=IwAR2Yf4ZeAE6_-XvxE9zZtZI9tMoo7IApmZ_Z1ptIeKrK33DQJ4k5wcGpcE4
- *Public and private blockchains: The security-efficiency trade-off*. (2020, May 14). Capgemini Deutschland. https://www.capgemini.com/de-de/2018/06/private-and-

public-blockchains/?fbclid=IwAR0MXLjzQWyssq8R6NuK-keKLDvL2vsoi8Xy8t9T3zQy0MoCPN4MCgbPT9I

- Ross, L. (2021, August 16). *Bitcoin vs Ethereum.What's the Difference?*. Benzinga. https://www.benzinga.com/money/bitcoin-vs-ethereum/
- *Simple Payment Verification — Electrum 3.3 documentation*. (n.d.). Electrum Documentation. https://electrum.readthedocs.io/en/latest/spv.html
- *Wallets — Bitcoin*. (n.d.). BitcoinDeveloper. https://developer.bitcoin.org/devguide/wallets.html
- *What Is Cryptocurrency?* (2020, October 5). Dummies. https://www.dummies.com/personal-finance/what-is-cryptocurrency/?fbclid=IwAR3NYencjfXGEBr3ep1wtiuCym-c6iY3FLGxTWA-ejQUuTSQpxddQF0dxVk
- *What is Decentralization?* (n.d.). Amazon Web Services, Inc. https://aws.amazon.com/blockchain/decentralization-in-blockchain/
- Wolfson, R. (2018, July 11). *Understanding How IBM And Others Use Blockchain Technology To Track Global Food Supply Chain*. Forbes. https://www.forbes.com/sites/rachelwolfson/2018/07/11/understanding-how-ibm-and-others-use-blockchain-technology-to-track-global-food-supply-chain/?sh=3b1b086b2d1e
- Γαλδαδάς, Γ. Α. (2021, May 1). *Οδηγός: Τι είναι και πώς λειτουργεί το Bitcoin – Πώς η τεχνολογία blockchain αλλάζει τα δεδομένα στις συναλλαγές*. ΤΟ ΒΗΜΑ.

https://www.tovima.gr/2021/05/01/science/odigos-ti-einai-kai-pos-leitourgei-to-bitcoin-pos-i-texnologia-blockchain-allazei-ta-dedomena-stis-synallages/

- ToBHMA team. (2021, May 2). *Τι είναι και πώς λειτουργεί το Bitcoin – Πώς η τεχνολογία blockchain αλλάζει τα δεδομένα στις συναλλαγές*. Www.Tovima.Gr. https://www.tovima.gr/2021/05/02/finance/ti-einai-kai-pos-leitourgei-to-bitcoin-pos-i-texnologia-blockchain-allazei-ta-dedomena-stis-synallages/