BLOCKCHAIN

Πάνος Φιτσιλής

Contents

10. Εισαγωγή στην τεχνολογία blockchain

Σύνοψη
Η τεχνολογία Blockchain ή Τεχνολογία Κατανεμημένων Μητρώων - Distributed Ledger Technology είναι μια ιδιαίτερα σύγχρονη τεχνολογία η οποία χρησιμοποιείται όλο και πιο συχνά και με μεγάλη ένταση. Ο ενθουσιασμός που επικρατεί για τη νέα τεχνολογία, τα πλεονεκτήματα και τις δυνατότητες εφαρμογής της κάνουν πολλούς να μιλούν για επανάσταση αντίστοιχη με εκείνη του διαδικτύου, η οποία μέσα στα επόμενα χρόνια θα αλλάξει ριζικά τις δομές, τον τρόπο οργάνωσης και τη λειτουργία των σύγχρονων κοινωνιών. Εφαρμογές της τεχνολογίας blockchain καλύπτουν όλα σχεδόν τα πεδία της οικονομίας, ενώ ολοένα και περισσότερες εταιρείες, οργανισμοί και δημόσιες αρχές επενδύουν σημαντικούς πόρους και εφαρμόζουν τη νέα τεχνολογία. Στο κεφάλαιο αυτό παρουσιάζουμε με λεπτομερή τρόπο τις βασικές έννοιες αυτής της τεχνολογίας, τα πλεονεκτήματα, τα μειονεκτήματα καθώς επίσης και κάποιες από τις σημαντικές εφαρμογές της.

Προαπαιτούμενη γνώση
Το κεφάλαιο απαιτεί κατανόηση των βασικών αρχών λειτουργίας πληροφοριακών επιχειρήσεων, της τεχνολογίας λογισμικού, καθώς και του τρόπου που οι νέες τεχνολογίες εντάσσονται στις επιχειρήσεις ώστε να μπορούν να καινοτομήσουν παράγοντας νέα προϊόντα ή παρέχοντας νέες προηγμένες υπηρεσίες.

Στόχοι του κεφαλαίου
Αφού θα έχετε ολοκληρώσει τη μελέτη αυτού του κεφαλαίου θα μπορείτε:
1. *Να κατανοήσετε τον τρόπο λειτουργίας του blockchain*
2. *Να κατανοήσετε τον τρόπο λειτουργίας του δικτύου bitcoin*
3. *Να κατανοήσετε σε τεχνικό επίπεδο, τις πολιτικές συναίνεσης, τη συνάρτηση κατακερματισμού, τη ρίζα και το δέντρο Merkle*
4. *Να κατανοήσετε τη δομή και τον τρόπο λειτουργίας των συναλλαγών σε ένα δίκτυο blockchain*
5. *Να κατανοήσετε τη λειτουργία των έξυπνων συμβάσεων και του συστήματος Ethereum*
6. *Να γνωρίζετε τις εφαρμογές της τεχνολογίας blockchain*

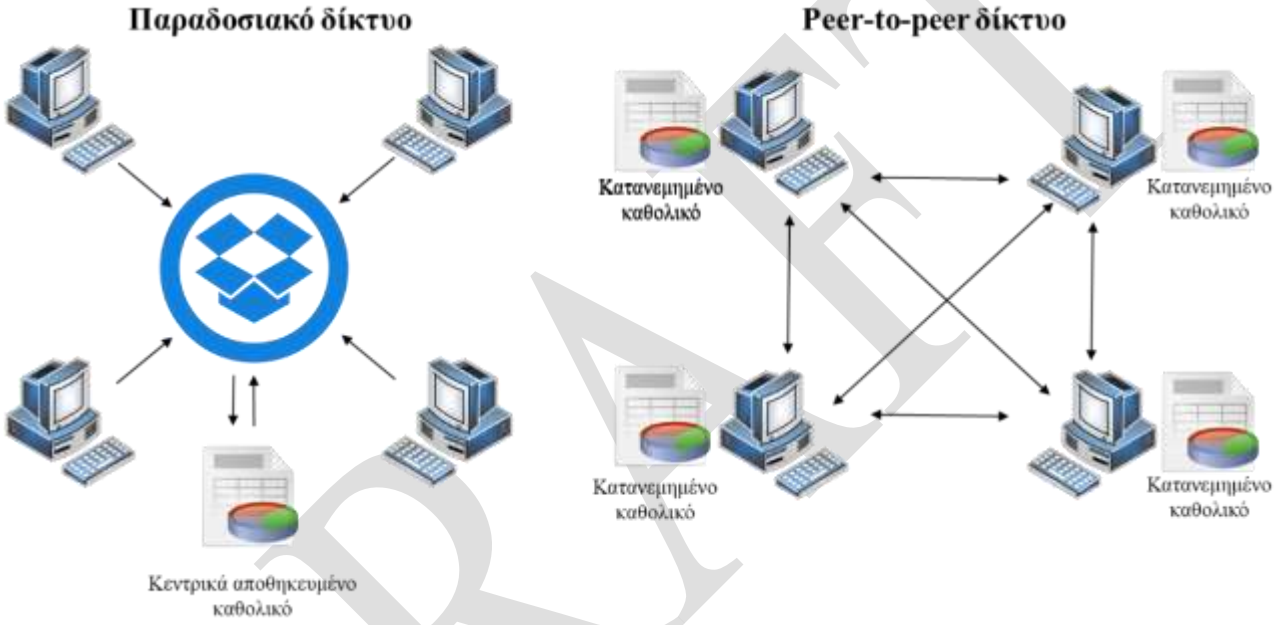
10.1 Η τεχνολογία Blockchain

Η τεχνολογία Blockchain ή Τεχνολογία Κατανεμημένων Μητρώων - Distributed Ledger Technology είναι μια ιδιαίτερα σύγχρονη τεχνολογία η οποία χρησιμοποιείται όλο και πιο συχνά και με μεγάλη ένταση. Ταυτόχρονα η τεχνολογία αυτή είναι ελάχιστα κατανοητή στο ευρύ κοινό παρότι χαρακτηρίζεται ως "τεχνολογία που μπορεί να αλλάξει ριζικά την οικονομία και το διαδίκτυο". Η τεχνολογία blockchain υπόσχεται ένα ψηφιακό περιβάλλον εμπιστοσύνης, άμεσης διενέργειας ηλεκτρονικών συναλλαγών με περισσότερη διαφάνεια. Αυτό οδηγεί στο ριζικό μετασχηματισμό του τρόπου οργάνωσης και λειτουργίας της οικονομίας καθώς δημιουργούν την τεχνολογική δυνατότητα για ύπαρξη κατανεμημένης μορφής εμπιστοσύνης. Αυτό έχει τεράστια σημασία, καθώς μπορεί να επηρεάσει τους μέχρι σήμερα παραδοσιακούς φορείς εμπιστοσύνης (π.χ. τράπεζες, κυβέρνηση, εταιρίες) και τις συναλλαγές και ηλεκτρονικές υπηρεσίες που παρέχουν αυτοί οι οργανισμοί.

Το έτος 2008, ένα άτομο ή μια ομάδα ατόμων με το όνομα Satoshi Nakamoto (Nakamoto, 2008) δημοσίευσε το άρθρο με τίτλο «Bitcoin[1]: A Peer-To-Peer Electronic Cash System». Στο άρθρο αυτό περιγράφεται η λειτουργία ενός ηλεκτρονικού κρυπτονομίσματος με το όνομα Bitcoin το οποίο θα επέτρεπε την απευθείας διενέργεια πληρωμών στο διαδίκτυο χωρίς να διαμεσολαβεί ένα χρηματοπιστωτικό ίδρυμα (π.χ. μια τράπεζα).

[1] Όταν αναφερόμαστε στο πρωτόκολλο Bitcoin το B στη λέξη είναι με κεφαλαίο γράμμα, ενώ όταν αναφερόμαστε στο κρυπτονόμισμα το γράμμα b είναι μικρό (bitcoin)

Ο συγγραφέας αυτού του πρώτου άρθρου ήθελε να παραμείνει ανώνυμος και ακόμη και σήμερα κανείς δεν γνωρίζει ποιος είναι ο Satoshi Nakamoto. Λίγους μήνες αργότερα, δημιουργήθηκε η πρώτη εφαρμογή ανοικτού κώδικα, η οποία υλοποιούσε το bitcoin, η οποία δημιούργησε και το πρώτο block, (genesis block). Το genesis block περιείχε 50 νομίσματα. Σήμερα οποιοσδήποτε μπορεί να εγκαταστήσει την εφαρμογή αυτή και να γίνει μέλος του δικτύου peer-to-peer Bitcoin. Σε αντίθεση με ένα παραδοσιακό δίκτυο όπου η αποθήκευση των δεδομένων γίνεται συνήθως κεντρικά, ένα δίκτυο υπολογιστών peer-to-peer (P2P) είναι ένα δίκτυο που επιτρέπει σε δύο ή περισσότερους υπολογιστές να μοιράζονται τους πόρους τους ισοδύναμα, αφού όλοι οι κόμβοι του δικτύου έχουν ίσα δικαιώματα. Πληροφορίες που βρίσκονται στον ένα κόμβο, ανάλογα με τα δικαιώματα που καθορίζονται, μπορούν να διαβαστούν από όλους τους άλλους και αντίστροφα. Η Εικόνα 10.1 παρουσιάζει σχηματικά τη διαφορά ενός παραδοσιακού δικτύου από ένα δίκτυο peer-to-peer.



Εικόνα 10.1 *Κεντρικό και κατανεμημένο καθολικό*

Το bitcoin είναι το πιο δημοφιλές κρυπτονόμισμα με συνολική κεφαλοποίηση 112 δισεκατομμυρίων USD (Σεπτέμβριος 2018). Ταυτόχρονα με αυτό, έχουν εμφανιστεί και άλλα κρυπτονομίσματα, όπως τα νομίσματα Ethereum, XRP, Bitcoin, Litecoin, Dogecoin, Stellar, κ.λπ. Ωστόσο η τεχνολογία blockchain μπορεί να χρησιμοποιηθεί και σε άλλες εφαρμογές όπως θα παρουσιάσουμε αναλυτικά σε επόμενη παράγραφο.

Όπως και με το υπολογιστικό νέφος που περιγράψαμε στο κεφάλαιο 8 έτσι και το blockchain μπορεί να έχει διάφορους τύπους ανάλογα με το ποιος έχει πρόσβαση στο σχετικό peer-to-peer δίκτυο.

Ένα **δημόσιο blockchain** είναι αυτό που οραματίστηκαν οι αρχικοί δημιουργοί: ένα blockchain ανοικτό σε όλους, όπου όλοι μπορούν όλοι να έχουν πρόσβαση και να συναλλάσσονται σε αυτό. Στο δημόσιο blockchain, οι συναλλαγές συμπεριλαμβάνονται στην αλυσίδα μόνο εάν είναι έγκυρες, ενώ όλοι οι χρήστες συμμετέχουν στη διαδικασία συναίνεσης[2]. Η διαδικασία της συναίνεσης είναι αυτή που καθορίζει ποια block προστίθενται στο blockchain και ποια είναι η τρέχουσα κατάσταση. Επίσης, στο δημόσιο blockchain, δεν χρησιμοποιείται κεντρικός εξυπηρετητής, αλλά το blockchain δημιουργείται, επαληθεύεται από τους χρήστες του peer-to-peer δικτύου μέσω κρυπτογραφικών μηχανισμών.

[2] Ένα θεμελιώδες πρόβλημα στα κατανεμημένα συστήματα υπολογιστών και στα συστήματα πολλαπλών πρακτόρων (multi agent systems) είναι η επίτευξη συνολικής αξιοπιστίας του συστήματος με δεδομένη την παρουσία ορισμένων ελαττωματικών διεργασιών ή κόμβων ή/και κακόβουλων χρηστών. Αυτό οδηγεί στην ανάγκη ύπαρξης διαδικασιών συναίνεσης (consensus mechanisms) ώστε να μπορεί να ληφθεί απόφαση σε περίπτωση διενέξεων.

Η διαδικασία μέσω της οποίας οι συναλλαγές επαληθεύονται και προστίθενται στο blockchain ονομάζεται εξόρυξη (mining) ενώ τα άτομα που ασχολούνται με αυτή miners (μεταφορικά από τη λέξη μεταλλωρύχος που προσπαθεί να εξορύξει το μετάλλευμα). Η διαδικασία αυτή σ'ένα δημόσιο blockchain είναι ανοικτή για όλους και ο καθένας με πρόσβαση στο διαδίκτυο και το κατάλληλο υλικό (hardware) μπορεί να συμμετέχει στην εξόρυξη. Η διαδικασία εξόρυξης περιλαμβάνει τη σύνθεση και αποθήκευση των πρόσφατων συναλλαγών σε block σε συνδυασμό με την προσπάθεια επίλυσης ενός δύσκολου υπολογιστικού παιχνιδιού (παζλ). Ο miner αφού λύσει πρώτα το δύσκολο υπολογιστικό παιχνίδι μπορεί να τοποθετήσει το επόμενο block στο blockchain και να διεκδικήσει τις σχετικές ανταμοιβές. Οι ανταμοιβές, οι οποίες ενθαρρύνουν την εξόρυξη, είναι τόσο οι αμοιβές που σχετίζονται με τις συναλλαγές όπως παραδοσιακά συμβαίνει και σε μια τράπεζα, όσο και η δημιουργία νέων κρυπτονομισμάτων, τα οποία αφού εξορυχθούν, περιέρχονται στην ιδιοκτησία των miners.

Η δεύτερη κατηγορία blockchain είναι τα **blockchain κοινοπραξιών** (consortium blockchain), όπως για παράδειγμα το R3 (www.r3cev.com). Στην κατηγορία αυτή η διαδικασία συναίνεσης ελέγχεται από ένα προεπιλεγμένο σύνολο κόμβων. Για παράδειγμα, σε μια κοινοπραξία εννέα χρηματοπιστωτικών ιδρυμάτων, στην οποία το καθένα ίδρυμα λειτουργεί έναν κόμβο, πέντε εκ των κόμβων πρέπει να υπογράψουν κάθε block, προκειμένου αυτό να είναι έγκυρο. Το δικαίωμα ανάγνωσης και χρήσης του blockchain μπορεί να είναι δημόσιο ή περιορισμένο στους συμμετέχοντες.

Η τρίτη κατηγορία blockchain είναι τα **ιδιωτικά blockchain** (private blockchain). Σε ένα ιδιωτικό blockchain τα δικαιώματα εγγραφής κρατούνται κεντρικά από έναν οργανισμό. Τα δικαιώματα ανάγνωσης ενδέχεται να είναι δημόσια ή περιορισμένα ανάλογα με τους σκοπούς και τις ανάγκες του blockchain. Πιθανές εφαρμογές περιλαμβάνουν τη διαχείριση βάσεων δεδομένων και τον εσωτερικό έλεγχο σε μια πολυεθνική εταιρεία. Στις περιπτώσεις αυτές δεν είναι απαραίτητη η αναγνωσιμότητα του blockchain από το κοινό, αν και σε πολλές περιπτώσεις ο δημόσιος έλεγχος και λογοδοσία (auditability) είναι επιθυμητά χαρακτηριστικά. Επίσης, τα ιδιωτικά blockchains μπορούν να χρησιμοποιηθούν για να παράσχουν λύσεις στα προβλήματα των χρηματοοικονομικών επιχειρήσεων, όπως το πρόβλημα της συμμόρφωσης σε κανονισμούς, την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες, την προστασία των ιδιωτικών δεδομένων κ.λπ.

Στην περίπτωση των πληροφοριακών συστημάτων επιχειρήσεων, η ενσωμάτωση της τεχνολογίας blockchain σε ένα σύστημα ERP θα δημιουργήσει μια εξαιρετικά ασφαλή πλατφόρμα συνεργασίας, μέσα στην οποία το σύστημα αρχείων αλλά και τα δεδομένα γενικότερα μπορούν να διαμοιραστούν ελεύθερα με μεγάλη αξιοπιστία.

Τα πλεονεκτήματα των συστημάτων ERP έχουν παρουσιαστεί στα κεφάλαια 1 και 3. Περιληπτικά θα μπορούσαμε να αναφέρουμε ότι: προσφέρουν ολοκλήρωση των δεδομένων, της πληροφορίας και των διεργασιών, επιτρέπουν στις επιχειρήσεις να αποκτήσουν τον πληρέστερο έλεγχο των εσωτερικών λειτουργιών και να λάβουν τεκμηριωμένες αποφάσεις για το μέλλον. Επιπλέον, όλα τα δεδομένα ενημερώνονται σε πραγματικό χρόνο, γεγονός που είναι κρίσιμο για την ομαλή λειτουργία της επιχείρησης. Η συνεχής επικοινωνία μεταξύ των τμημάτων της επιχείρησης εξαλείφει την πιθανότητα σφαλμάτων, ενώ η άμεση πρόσβαση στα δεδομένα καθιστά δυνατή την αναγνώριση πιθανών αποτυχιών. Συνεπώς, οι επιχειρήσεις έχουν τις ιδανικές συνθήκες για την ανάπτυξη των επιχειρηματικών δραστηριοτήτων τους. Είναι επίσης δυνατές διάφορες ενσωματώσεις (π.χ. λύσεις B2B), γεγονός που καθιστά περιττή την ύπαρξη άλλου λογισμικού και εργαλείων. Οι τεχνολογίες Blockchain προσθέτουν στα υπάρχοντα πλεονεκτήματα ενός συστήματος ERP, τη δυνατότητα οι επιχειρηματικές διαδικασίες μια επιχείρησης να καθίστανται προσιτές σε άλλες επιχειρήσεις με ασφαλή τρόπο, ενώ τα δεδομένα είναι σωστά με πιστοποιημένο τρόπο χωρίς την ανάγκη ύπαρξης τρίτου πιστοποιητή. Αυτή η ολοκλήρωση επιτρέπει τη βελτιστοποίηση των επιχειρηματικών λειτουργιών πολλών διαφορετικών επιχειρήσεων, καθώς και αξιόπιστων δεδομένων κοινής χρήσης και όχι μόνο των διεργασιών και των δεδομένων μιας επιχείρησης. Αυτό είναι ιδιαίτερα επωφελές στην περίπτωση των οικονομικών συναλλαγών.

Σε τεχνικό επίπεδο το blockchain είναι μία σειρά καταχωρίσεων/συναλλαγών (οικονομικών συνήθως αλλά όχι αποκλειστικά), σε ένα δημόσιο μητρώο (ledger). Κάθε καινούρια ομάδα συναλλαγών που δημιουργείται α) αποθηκεύεται σε ένα block και β) στη συνέχεια το block αυτό συνδέεται με τα προηγούμενα, δημιουργώντας έτσι μία «αλυσίδα» καταχωρίσεων, δηλαδή ένα blockchain.

Τα blocks αυτά συνδέονται μονοσήμαντα μεταξύ τους. Προκύπτουν δε μέσα από μια διαδικασία που ονομάζουμε “απόδειξη εργασίας” (proof of work), κατά την οποία επιτυγχάνεται η αλγοριθμική επίλυση ενός “δύσκολου” υπολογιστικού προβλήματος. Κατ’ αυτό τον τρόπο, το blockchain λειτουργεί ως ένα κατανεμημένο (decentralized) λογιστικό καθολικό, το οποίο είναι κοινό για όλους τους συμμετέχοντες, μιας και όλοι οι εμπλεκόμενοι αποθηκεύουν ένα αντίγραφό του· κάτι που εξασφαλίζει την ασφάλεια και τη διαφάνεια των συναλλαγών. Η βασική διαφορά -αναφορικά με την προστασία- προκύπτει από το γεγονός ότι δεν είναι πλέον απαραίτητη η ύπαρξη μιας ενδιάμεσης «έμπιστης» αρχής (π.χ. μιας τράπεζας), ενώ η εμπιστοσύνη των συναλλασσόμενων μερών βασίζεται σε αλγοριθμική επιβεβαίωση. Συνεπώς ένα blockchain είναι ένας κοινόχρηστος τόπος αποθήκευσης όλων των συναλλαγών και των ψηφιακών κινήσεων που έχουν εκτελεστεί από κοινού μεταξύ των συμμετεχόντων μερών. Κάθε συναλλαγή επαληθεύεται με τη συναίνεση της πλειοψηφίας των συμμετεχόντων στο σύστημα, ενώ μόλις μία τέτοια συναλλαγή ξεκινήσει δεν υπάρχει δυνατότητα διαγραφής.

Συνοψίζοντας, τα πλεονεκτήματα της τεχνολογίας blockchain είναι τα ακόλουθα:

- Εμπιστοσύνη χωρίς την ύπαρξη διαμεσολαβητή. Δύο μέρη είναι σε θέση να πραγματοποιήσουν συναλλαγές χωρίς τη μεσολάβηση τρίτου μέρους, μειώνοντας έτσι τον κίνδυνο.
- Ο ρόλος των χρηστών είναι αναβαθμισμένος. Οι χρήστες του συστήματος blockchain έχουν τον πλήρη έλεγχο των πληροφοριών και των συναλλαγών.
- Τα δεδομένα είναι υψηλής ποιότητας . Τα δεδομένα blockchain είναι πλήρη, έγκυρα, και άμεσα διαθέσιμα ανεξάρτητα από τη γεωγραφική θέση του χρήστη.
- Σύστημα υψηλής αξιοπιστίας και ανοχής σε σφάλματα. Το blockchain είναι ένα κατανεμημένο δίκτυο, στο οποίο δεν υπάρχει κεντρικό σημείο αποτυχίας και συνεπώς είναι σε θέση να ανεχθεί τόσο σφάλματα αλλά και κακόβουλες επιθέσεις. Όλες οι συναλλαγές που γίνονται επιτρέπονται ή αποτρέπονται από τους miners.
- Ακεραιότητα των διαδικασιών. Οι χρήστες εμπιστεύονται το δίκτυο διότι όλες οι συναλλαγές εκτελούνται σύμφωνα με το πρωτόκολλο, καταργώντας έτσι την ανάγκη για ένα αξιόπιστο τρίτο μέρος.
- Διαφάνεια και μονιμότητα των δεδομένων. Όλες οι συναλλαγές είναι ορατές σε όλους τους χρήστες, δημιουργώντας πλήρη διαφάνεια, ενώ οι συναλλαγές δεν μπορούν να τροποποιηθούν ή να διαγραφούν.
- Απλοποίηση των οικοσυστημάτων. Όλες οι συναλλαγές προστίθενται σε ένα ενιαίο κατανεμημένο μητρώο μειώνοντας έτσι την πολυπλοκότητα και το κόστος διαχείρισης πολλαπλών μητρώων.
- Ταχύτερες συναλλαγές. Οι διατραπεζικές συναλλαγές χρειάζονται ημέρες για εκκαθάριση και τελικό διακανονισμό, ιδίως εκτός των ωρών εργασίας. Οι συναλλαγές Blockchain μπορούν να μειώσουν τους χρόνους συναλλαγής σε λεπτά και να υποβληθούν για επεξεργασία 24 ώρες το 24ωρο.
- Χαμηλότερο κόστος συναλλαγής. Τα blockchains είναι λιγότερο δαπανηρά λόγω του μικρού κόστους ανά συναλλαγή, μέσω της εξάλειψης των τρίτων - μεσολαβητών και των γενικών εξόδων που απαιτούνται στα παραδοσιακά συστήματα για την αγοροπωλησία περιουσιακών στοιχείων.

10.2 Τρόπος λειτουργίας του blockchain

Στην ενότητα αυτή θα επιχειρήσουμε να παρουσιάσουμε πως λειτουργεί η τεχνολογία blockchain. Ένα blockchain είναι μια βάση δεδομένων που περιλαμβάνει μια αλυσίδα block σταθερού μήκους που περιλαμβάνουν από 1 έως N συναλλαγές. Κάθε συναλλαγή που προστίθεται σε ένα νέο block πρέπει πρώτα να επικυρωθεί και στη συνέχεια να εισαχθεί στο block. Όταν ολοκληρωθεί η κατασκευή του block, τότε το συγκεκριμένο block προστίθεται στο τέλος της υπάρχουσας αλυσίδας block. Δύο είναι μόνο οι επιτρεπτές λειτουργίες - σε αντίθεση με το κλασσικό CRUD (θυμίζουμε ότι τα αρχικά CRUD προέρχονται από τις λέξεις Create/Read/Update/Delete) - η προσθήκη νέας συναλλαγής και η προβολή υπάρχουσας συναλλαγής.

Επομένως τα βήματα που δημιουργούν ένα blockchain είναι:

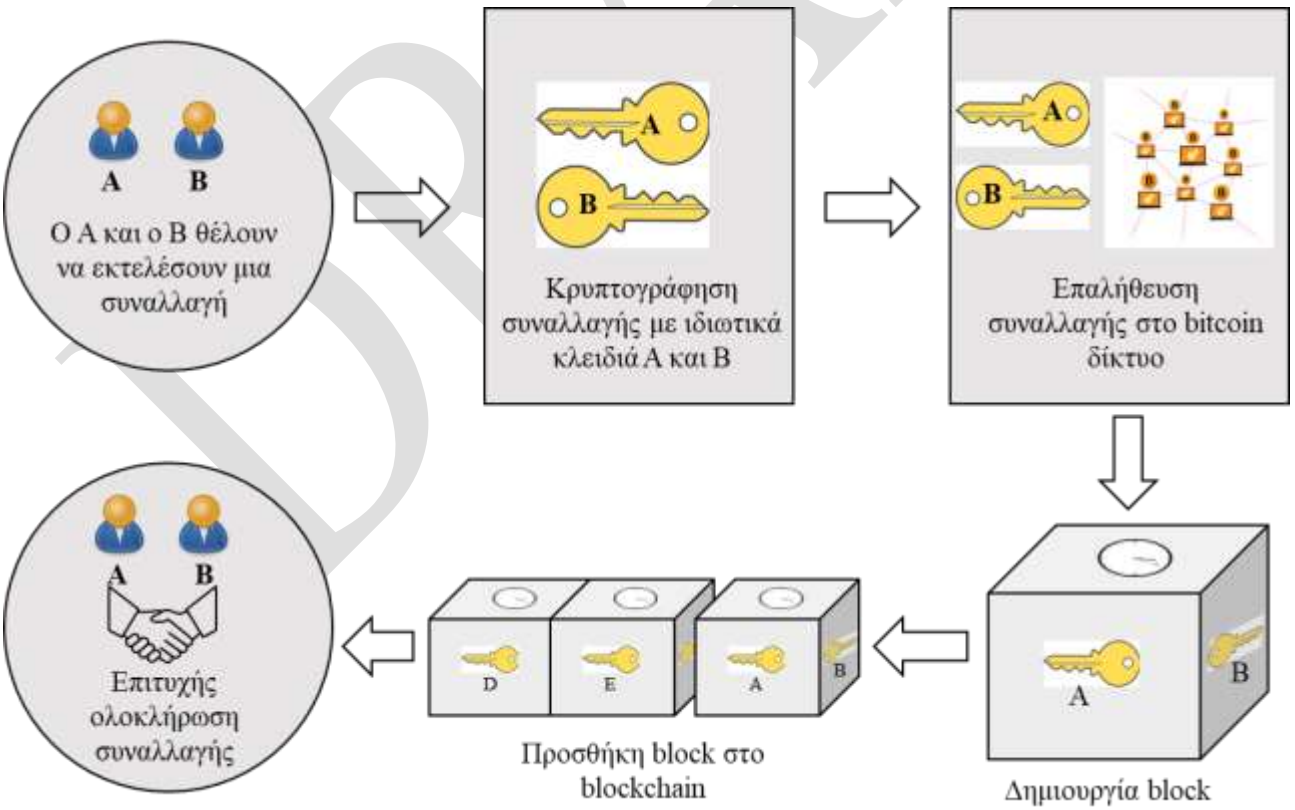
- Δημιουργία νέων αδιάβλητων συναλλαγών οργανωμένων σε block.
- Κρυπτογραφικός έλεγχος από τους miners για την εγκυρότητα της συναλλαγής που περιέχεται στο block
- Προσθήκη του νέου block στο τέλος της υπάρχουσας αναλλοίωτης αλυσίδας block.

Τα βήματα παρουσιάζονται γραφικά στην Εικόνα 10.2.

Εκτός της επαλήθευσης της συναλλαγής, η εξόρυξη (mining) επιτρέπει να δημιουργήσουμε νέα ψηφιακά νομίσματα επιβραβεύοντας τους miners για την εκτέλεση της προηγούμενης εργασίας. Για να γίνει αυτό, οι miners θα πρέπει να λύσουν ένα μαθηματικό παζλ γνωστό ως πρόβλημα απόδειξης εργασίας. Μόλις επιτευχθεί η επαλήθευση δίνεται στο miner μια ανταμοιβή.

Τα blocks έχουν σχεδιαστεί με τέτοιο τρόπο ώστε να είναι ανθεκτικά σε κάθε τροποποίηση, αφού δεν μπορούν να τροποποιηθούν αναδρομικά. Αυτό επιτυγχάνεται μέσω της χρήσης ενός peer-to-peer δικτύου, ενός κατανεμημένου εξυπηρετητή χρονοσήμανσης (timestamping)[3], και μιας κατανεμημένης δημόσιας βάσης δεδομένων blockchain διαχειρίζεται αυτόνομα. Με τον τρόπο αυτό ένα blockchain είναι ένα ανοικτό, κατανεμημένο μητρώο που μπορεί να καταγράψει τις συναλλαγές μεταξύ δύο μερών αποτελεσματικά, με μόνιμο και επαληθεύσιμο τρόπο όπως απεικονίζεται στην Εικόνα 10.3.

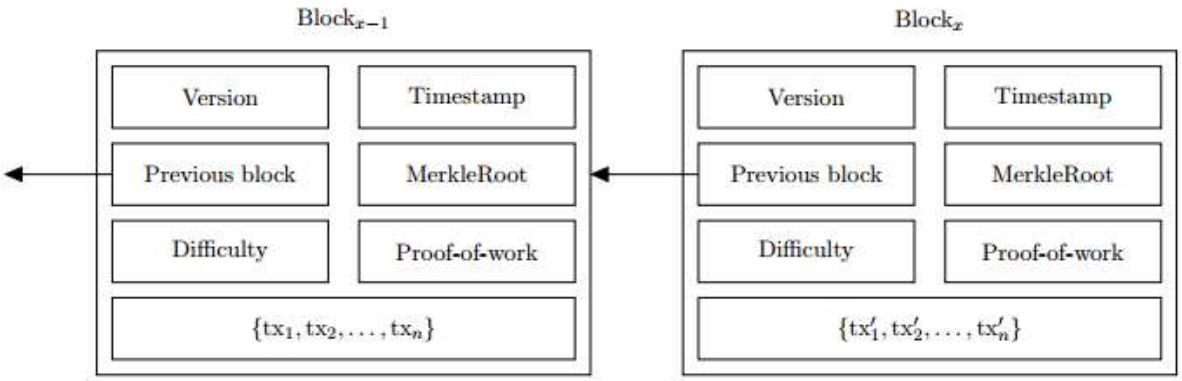
Αυτά τα χαρακτηριστικά καθιστούν το blockchain ιδανικό για την καταγραφή διάφορων ειδών γεγονότων, ιατρικών αρχείων, ταυτότητας χρηστών, την επεξεργασία συναλλαγών και μια σειρά από άλλες νέες εφαρμογές.



Εικόνα 10.2 *Η δημιουργία του blockchain*

[3] Η χρονοσήμανση είναι μια ακολουθία χαρακτήρων ή κωδικοποιημένων πληροφοριών που προσδιορίζουν πότε καταγράφηκε ένα συγκεκριμένο συμβάν από ένα εξυπηρετητή. Η πληροφορία αυτή συνήθως περιλαμβάνει ημερομηνία και ώρα της ημέρας.

Κάθε block αντιστοιχεί κατά μέσον όρο σε 1 megabyte[4] και περιέχει δεδομένα ελέγχου περίπου 200 byte, την χρονοσήμανση (timestamp), έναν σύνδεσμο που δείχνει το προηγούμενο block, κάποια άλλα πεδία (όπως απεικονίζεται στην Εικόνα 10.3), καθώς και 1 έως N συναλλαγές.



Εικόνα 10.3 *Η δομή του block*

Η έκδοση (version) περιγράφει τη δομή των δεδομένων μέσα στο block. Χρησιμοποιείται έτσι ώστε οι υπολογιστές να μπορούν να διαβάζουν σωστά τα περιεχόμενα κάθε block. Το πεδίο timestamp είναι η χρονοσήμανση του block (τύπου Unix). Μια χρονοσήμανση είναι αποδεκτή ως έγκυρη εάν είναι μεγαλύτερη από το διάμεσο (median) των χρονοσημάνσεων των προηγούμενων 11 μπλοκ και μικρότερη από το χρόνο του δικτύου + 2 ώρες. Ο "χρόνος του δικτύου" είναι ο διάμεσος των χρονοσημάνσεων που επιστρέφονται από όλους τους κόμβους (υπολογιστές) του δικτύου. Ως αποτέλεσμα, σε ένα blockchain, οι χρονοσημάνσεις των block δεν είναι διαδοχικά διατεταγμένες αλλά μπορεί να διαφέρουν ακόμη και μία ή δύο ώρες.

Τα block στα περισσότερα δίκτυα είναι διαθέσιμα δημόσια και μπορεί κάποιος να τα δει χρησιμοποιώντας έναν εξερευνητή block (block explorer). Εν συντομία, ένας εξερευνητής block χρησιμοποιείται για τις ακόλουθες λειτουργίες:

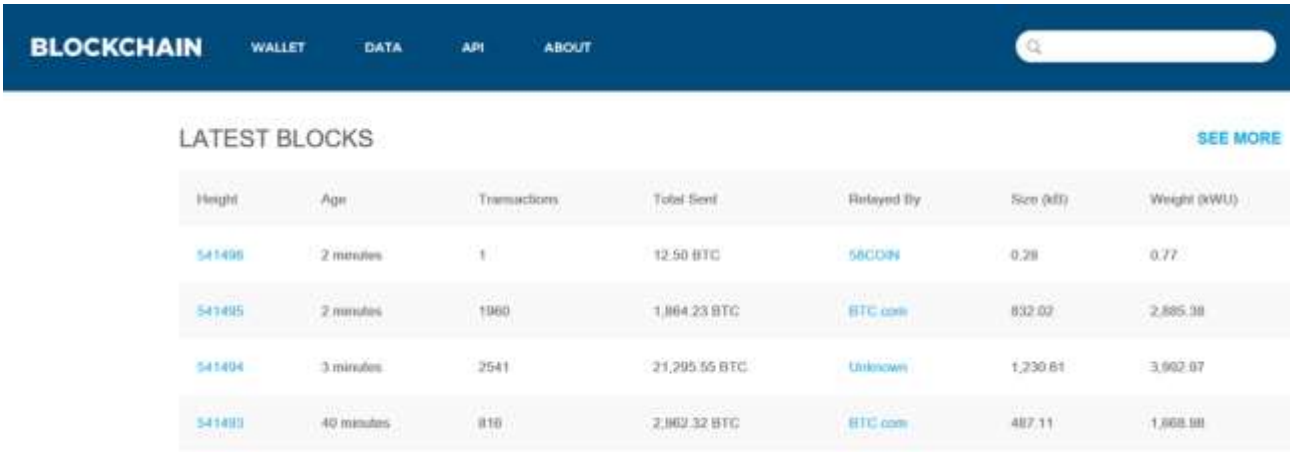
- την παρακολούθηση της ροής των block και των συναλλαγών
- την προβολή του ιστορικού των συναλλαγών μιας δεδομένης διεύθυνσης
- την προβολή των δεδομένων εισόδου και εξόδου των συναλλαγών
- τον έλεγχο της κατάστασης του mempool
- την προβολή του αρχικού block (genesis block)

Για κάθε σύστημα blockchain υπάρχει διαφορετικός εξερευνητής αφού η δομή των block διαφέρει. Για παράδειγμα μερικοί από τους πιο διαδεδομένους εξερευνητές για το Bitcoin είναι:

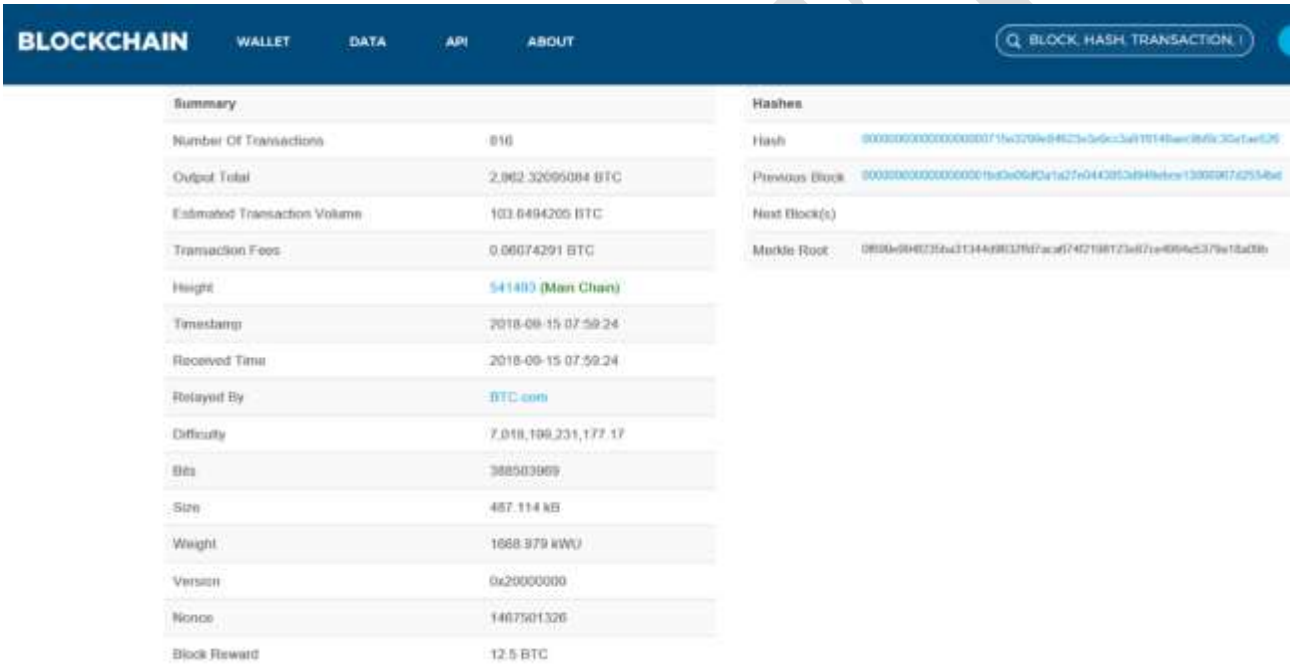
- Block Explorer (https://blockexplorer.com/)
- Blockchain.info (https://www.blockchain.com/explorer)
- BlockCypher (https://live.blockcypher.com/btc/)
- κ.λπ.

Στην Εικόνα 10.4 παρουσιάζεται η πρώτη σελίδα του εξερευνητή Blockchain.info όπου παρουσιάζονται τα τελευταία block που έχουν δημιουργηθεί, ενώ στην Εικόνα 10.5 παρουσιάζονται τα περιεχόμενα ενός block.

[4] Βλέπε https://blockchain.info/charts/avg-block-size



Εικόνα 10.4 *Ο εξερευνητής Blockchain.info (πηγή https://www.blockchain.com)*



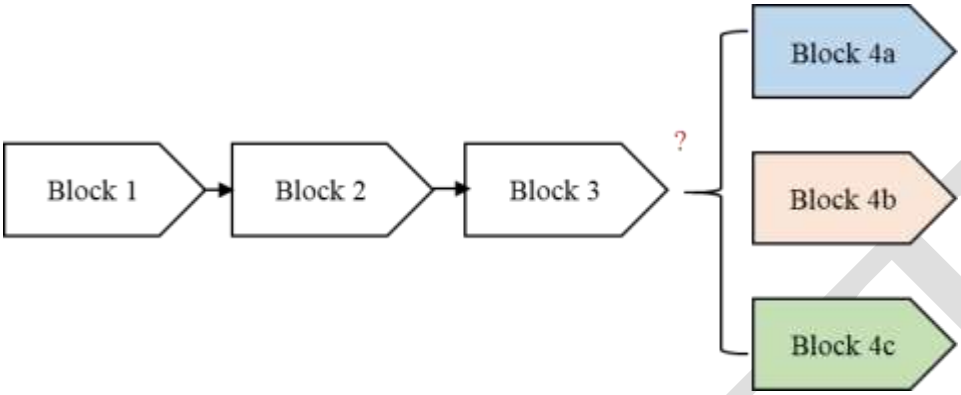
Εικόνα 10.5 *Οι λεπτομέρειες του block με τον εξερευνητή Blockchain.info (πηγή https://www.blockchain.com)*

10.2.1 Πολιτικές συναίνεσης

Το γεγονός ότι τα block δεν είναι διατεταγμένα εισάγει το πρόβλημα της διατήρησης της σειράς αυτών των συναλλαγών που μεταδίδονται σε άλλους κόμβους του peer-to-peer δικτύου. Οι συναλλαγές δεν έρχονται με τη σειρά που παράγονται και ως εκ τούτου υπάρχει ανάγκη για ένα σύστημα που να διασφαλίζει τη σωστή σειρά. Αυτό είναι ιδιαίτερα σημαντικό για τις συναλλαγές που γίνονται με τη χρήση κρυπτονομισμάτων ώστε να αποφύγουμε περιπτώσεις διπλών αγορών με το ίδιο κρυπτονόμισμα και για να υπάρχει εγγύηση ότι οι παραγγελίες στις οποίες λαμβάνονται από έναν κόμβο έχουν την ίδια σειρά με τις συναλλαγές που πραγματοποιήθηκαν.

Γενικότερα, οποιοσδήποτε κόμβος στο δίκτυο μπορεί να δημιουργήσει άκυρες συναλλαγές και με βάση αυτές ένα block, το οποίο στη συνέχεια να το μεταδίδει στο υπόλοιπο δίκτυο ως πρόταση, ώστε αυτό να είναι το επόμενο block στο blockchain. Επίσης μπορεί να δημιουργηθούν ταυτόχρονα πολλαπλά blocks από διαφορετικούς κόμβους του δικτύου. Αυτό σημαίνει ότι δεν μπορούμε να βασιστούμε στη σειρά με την οποία φτάνουν τα block, αφού τα block μπορούν να φτάνουν σε διαφορετικούς κόμβους (υπολογιστές) του δικτύου

με διαφορετική σειρά. Το πρόβλημα παρουσιάζεται γραφικά στην Εικόνα 10.6, όπου όλοι οι κόμβοι του δικτύου έχουν ένα έγκυρο blockchain το οποίο αποτελείται από τρία blocks: το block 1, το block 2 και το block 3. Τρεις χρήστες (miners) δημιουργούν ταυτόχρονα τρία νέα διαφορετικά blocks που περιέχουν διαφορετικές συναλλαγές: το 4a, το 4b και το 4c. Πώς λοιπόν αποφασίζει το δίκτυο ποιο block θα πρέπει να είναι το επόμενο στο blockchain;

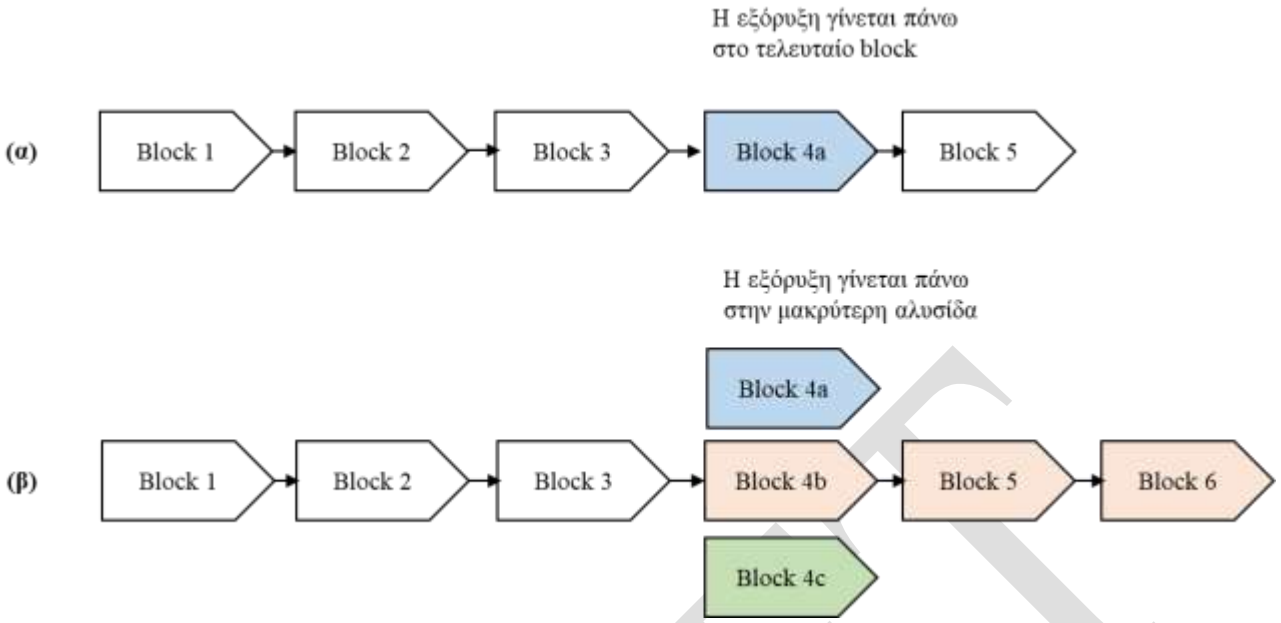


Εικόνα 10.6 *Επιλογή επόμενου block*

Στο δίκτυο Bitcoin, η σύγκρουση επιλύεται με τη χρήση του κανόνα που ονομάζεται "κανόνας μακρύτερης αλυσίδας" (longest chain rule). Οι κόμβοι το δικτύου επιλέγουν το block που περιέχει την περισσότερη "εργασία" (όπου ως εργασία ορίζεται το άθροισμα των πεδίων δυσκολία – difficulty των block του blockchain). Επιπλέον, ο μηχανισμός εξόρυξης διασφαλίζει ότι η πιθανότητα να διαφωνούν δύο κόμβοι σχετικά με τα blocks στο παρελθόν μειώνεται εκθετικά με το χρόνο. Έτσι μπορούμε να πούμε ότι δεν υπάρχει μόνο ένα σωστό blockchain αλλά υπάρχουν πολλά. Οι κόμβοι επιλέγουν το σωστό επόμενο block για τον εαυτό τους, αλλά το σύστημα έχει σχεδιαστεί ώστε να διασφαλίζεται ότι η συναίνεση προκύπτει γρήγορα.

Στην πράξη, όταν ένα νέο block φτάσει, το ενεργό blockchain επεκτείνεται, προσθέτοντας το νέο block. Αν φτάσει και ένα ακόμη νέο block, ελέγχουμε αν το νέο block έχει περισσότερη δουλειά από τον ενεργό κλάδο. Αν όχι, αποθηκεύουμε το block και σταματάμε. Αν όμως έχει περισσότερη δουλειά, κάνουμε μια αποκαλούμενη "αναδιοργάνωση" που σημαίνει απενεργοποίηση των blocks από τον παλαιό κλάδο και ενεργοποίηση των blocks στο νέο κλάδο.

Στο παραπάνω παράδειγμα, υποθέτουμε ότι το πρώτο block που φτάνει είναι το 4a (βλέπε Εικόνα 10.7.α) το οποίο είναι έγκυρο και συνεπώς προστίθεται στην αλυσίδα. Στη συνέχεια φτάνει ένα ακόμη έγκυρο block, αυτό με αριθμό 5, το οποίο προστίθεται και αυτό στο blockchain. Σε επόμενο βήμα φτάνει το block 4b το οποίο περιέχει περισσότερη εργασία. Το blockchain αναδιοργανώνεται και το block 4b αντικαθιστά το block 4a (βλέπε Εικόνα 10.7.β)



Εικόνα 10.7 *Αναδιοργάνωση του blockchain*

Έχοντας υπόψη ότι το blockchain Bitcoin, αποτελεί το πιο δημοφιλές σύστημα αυτής της κατηγορίας, θα πρέπει να αναφέρουμε ότι το σύστημα blockchain είναι στην πραγματικότητα δύο αρκετά ξεχωριστά υποσυστήματα που στην πράξη πολλές φορές συγχέονται. Το πρώτο υποσύστημα είναι το δέντρο των block ενώ το δεύτερο είναι η ενεργός αλυσίδα (active blockchain).

Το **δέντρο των block** αποτελείται από όλα τα έγκυρα μπλοκ των οποίων η καταγωγή είναι γνωστή, μέχρι το αρχικό block (genesis block). Οι κανόνες εγκυρότητας περιλαμβάνουν αποφυγή διπλών δαπανών, έγκυρες υπογραφές, μη εισαγωγή περισσότερων νομισμάτων απ' ό, τι επιτρέπεται, κ.λπ. Οι κανόνες αυτοί του δικτύου Bitcoin πρέπει να επαληθεύονται σε κάθε κόμβο Bitcoin.

Από το σύνολο των διαδρομών ως **ενεργός αλυσίδα** (active blockchain) αναφέρεται η διαδρομή αυτή που έχει την περισσότερη δουλειά, με αφετηρία το αρχικό block και τέλος κάποιο κόμβο – φύλλο - στο κάτω μέρος του δέντρου των blocks..

Απόδειξη εργασίας

Στο δίκτυο Bitcoin, στο οποίο δεν υπάρχουν κόμβοι ελέγχου, οι διαφωνίες σχετικά με τη δομή του blockchain επιλύονται με τη χρήση του "κανόνα της μακρύτερης αλυσίδας" (longest chain rule), όπως περιγράψαμε και στις προηγούμενες παραγράφους. Ο κανόνας αυτός βασίζεται στη λογική της "απόδειξης εργασίας" (**Proof of Work - PoW**), κατά την οποία όπως αναφέραμε στην προηγούμενη παράγραφο επιτυγχάνεται η αλγοριθμική επίλυση ενός "δύσκολου" υπολογιστικού προβλήματος.

Η τεχνική αυτή χρησιμοποιείται σχεδόν σε όλα τα δίκτυα κρυπτονομισμάτων και είναι ιδιαίτερα δημοφιλής. Μια απόδειξη εργασίας είναι ένα σύνολο δεδομένων που είναι δύσκολο (δαπανηρό, χρονοβόρο) να παραχθούν, αλλά είναι εύκολο να ελεγχθεί η ορθότητά τους από τρίτους. Η παραγωγή μιας απόδειξης εργασίας μπορεί να είναι μια τυχαία διεργασία με χαμηλή πιθανότητα, ώστε να απαιτούνται πολλές δοκιμές πριν καταλήξουμε στη σωστή λύση. Το σύστημα Bitcoin χρησιμοποιεί τη μέθοδο Hashcash για την απόδειξη εργασίας (Back, 2002). Η βασική αρχή ενός τέτοιου μηχανισμού είναι η αναγκαιότητα της δαπάνης πόρων κατά την επιβεβαίωση των συναλλαγών. Συνήθως, ο πόρος που καταναλώνεται είναι ένας συνδυασμός ηλεκτρικής ενέργειας και χρόνου και αντιπροσωπεύει το κόστος για την ασφάλεια του δικτύου. Οι χρήστες που κάνουν εξόρυξη κρυπτονομισμάτων - εκείνοι που κατέχουν τον υποκείμενο πόρο, και ως εκ τούτου μπορούν να τον δαπανήσουν – εργάζονται για την ασφάλεια του δικτύου και ανταμείβονται για την εργασία τους με τη μορφή συναλλαγών ή νέων κρυπτονομισμάτων.

Οι αποδείξεις εργασίας Hashcash χρησιμοποιούνται στο δίκτυο Bitcoin για την επαλήθευση νέων blocks. Για να γίνει αποδεκτό ένα block από τους συμμετέχοντες στο δίκτυο, οι miners πρέπει να δημιουργήσουν μια απόδειξη εργασίας για όλα τα δεδομένα του block. Η δυσκολία αυτής της εργασίας προσαρμόζεται έτσι ώστε να περιορίζεται ο ρυθμός με τον οποίο μπορούν να δημιουργηθούν νέα block από το δίκτυο, με ρυθμό ένα block κάθε 10 λεπτά. Αυτό σε συνδυασμό με την πολύ χαμηλή πιθανότητα επιτυχούς παραγωγής, καθιστά απρόβλεπτο ποιος κόμβος του δικτύου θα είναι αυτός που θα δημιουργήσει το επόμενο block.

Άλλα blockchain δίκτυα χρησιμοποιούν άλλες πολιτικές συναίνεσης όπως για παράδειγμα:

Απόδειξη Ενδιαφέροντος Proof of Stake (PoS)

Όπως σε κάθε επιχείρηση οι μέτοχοι έχουν ενδιαφέρον για την πρόοδο της επιχείρησης και ψήφο στη γενική συνέλευση της επιχείρησης έτσι και στα δίκτυα που υλοποιούν αυτό το μηχανισμό συναίνεσης οι χρήστες έχουν το προνόμιο να συμμετέχουν στον μηχανισμό λήψης αποφάσεων συναίνεσης.

Με κίνητρο τη μείωση του υψηλού κόστους εξόρυξης του bitcoin[5], οι σχεδιαστές των συστημάτων blockchain αναζήτησαν λιγότερο δαπανηρούς μηχανισμούς που δεν απαιτούσαν τόσο πολύπλοκους υπολογισμούς και συνεπώς λιγότερη κατανάλωση ηλεκτρικής ενέργειας Η πρώτη από αυτές τις επιλογές είναι το PoS, το οποίο επιτρέπει την επίτευξη συναινέσεων από αυτούς τους χρήστες που έχουν το περισσότερο πλούτο (αριθμό κρυπτονομισμάτων). Επομένως, όσο περισσότερα νομίσματα κατέχει ένας κόμβος, τόσο περισσότερες δυνατότητες έχει να επιλεγεί για να επαληθεύσει μια συναλλαγή (Bentov et al., 2016).

Το δίκτυο Peercoin ήταν το πρώτο δίκτυο που χρησιμοποίησε PoS. Στο Peercoin χρησιμοποιήθηκε η μετρική "ηλικία του κρυπτονομίσματος", η οποία υπολογίζεται ως το γινόμενο του αριθμού των κρυπτονομισμάτων επί τον χρόνο κατοχής αυτών από τον κάθε miner. Στη συνέχεια, ο miner θα πρέπει να επιλύσει ένα παζλ της μορφής PoW του οποίου όμως η δυσκολία έχει μειωθεί ανάλογα με το μέγεθος της "ηλικίας του κρυπτονομίσματος".

Βυζαντινή ανοχή στα σφάλματα (Byzantine Fault Tolerance - BFT)

Η βυζαντινή ανοχή σε σφάλματα είναι το χαρακτηριστικό ενός συστήματος που επιτρέπει σφάλματα που προϊδεάζουν στο πρόβλημα των βυζαντινών στρατηγών. Η βυζαντινή αποτυχία είναι η πιο δύσκολη κατηγορία σφαλμάτων, αφού δεν θέτει περιορισμούς και δεν κάνει υποθέσεις σχετικά με το είδος συμπεριφοράς που μπορεί να έχει ένας κόμβος (π.χ. ένας κόμβος μπορεί να παράγει οποιοδήποτε είδος λανθασμένων δεδομένων). Τα βυζαντινά σφάλματα είναι τα πιο σοβαρά και δύσκολα να αντιμετωπιστούν. Επίσης, η βυζαντινή ανοχή σφαλμάτων απαιτείται σε συστήματα κινητήρων αεροπλάνων, πυρηνικών σταθμών και σχεδόν όλων των συστημάτων των οποίων οι ενέργειες εξαρτώνται από τα αποτελέσματα μεγάλου αριθμού αισθητήρων.

Το πρόβλημα των βυζαντινών στρατηγών διατυπώθηκε από τους Lamport, Shostak and Pease (Lamport et al., 1982) και μελετήθηκε αρχικά σε πλήρη δίκτυα. Το πρόβλημα διατυπώνεται ως ακολούθως:

1. Τρεις ή περισσότεροι στρατηγοί θέλουν να αποφασίσουν για επίθεση ή υποχώρηση.
2. Ένας από αυτούς είναι ο αρχηγός (commander) και δίνει το αρχικό «πρόσταγμα».
3. Ο αρχηγός μπορεί να είναι προδότης ή όχι.
4. Οι υπόλοιποι στρατηγοί μπορεί να προδότες ή όχι.

Η αναλογία με το πρόβλημα της συναίνεσης, δηλαδή να αποφασίσουμε ποιες συναλλαγές είναι έγκυρες, που αντιμετωπίζουμε στα δίκτυα blockchain είναι η ακόλουθη. Οι στρατηγοί αντιστοιχούν σε κόμβους του δικτύου. Ο αρχηγός είναι αυτός που ξεκινά την αρχική διεργασία και οι εντολές που αποστέλλονται στις άλλες διεργασίες είναι μηνύματα. Οι προδότες στρατηγοί είναι οι κακόβουλοι κόμβοι του δικτύου ενώ οι πιστοί στρατηγοί είναι οι έμπιστοι κόμβοι του δικτύου.

[5] Μία συναλλαγή Bitcoin, το 2015, απαιτούσε ημερησίως την ίδια ποσότητα ηλεκτρικής ενέργειας που απαιτείται για την τροφοδοσία 1,57 αμερικανικών νοικοκυριών.

Οι βυζαντινές αποτυχίες σε ελαττωματικούς κόμβους προκαλούν συμπεριφορές που περιλαμβάνουν κακόβουλες επιθέσεις / συμπαιγνίες (π.χ. Sybil επιθέσεις (Douceur, 2002), επιθέσεις διπλής δαπάνης (Conti et al., 2017), λάθη από κόμβους (π.χ., απρόβλεπτη διακλάδωση στο blockchain λόγω ασυνέπειας στο λογισμικό (Buterin, 2013) καθώς και σφάλματα σύνδεσης.

Θεωρούμε ότι η ακολουθία των μπλοκ αντιπροσωπεύει την κατάσταση του blockchain, ενώ όταν γίνεται επαλήθευση μιας συναλλαγής πραγματοποιείται μια μετάβαση κατάστασης στο blockchain. Σύμφωνα με το πρωτόκολλο ενημέρωσης του blockchain η συναίνεση σε ένα βυζαντινό περιβάλλον ικανοποιείται αν ισχύουν οι ακόλουθες ιδιότητες (Bano et al., 2017):

- Εγκυρότητα (validity): Εάν όλοι οι έμπιστοι κόμβοι ενεργοποιηθούν και προτείνουν να επεκταθεί το blockchain με το ίδιο block. Στη συνέχεια κάθε έγκυρος κόμβος υιοθετεί το νέο επεκτεταμένο blockchain που έχει στην αρχή το νέο block και ενημερώνει το τοπικό αντίγραφο.
- Συμφωνία (agreement): Αν ένας έμπιστος κόμβος επιβεβαιώσει την επικεφαλίδα του νέου block, τότε όλοι οι έμπιστοι κόμβοι ενημερώνουν το τοπικό αντίγραφο του blockchain με αυτήν τη νέα επικεφαλίδα.
- Ζωντάνια (Liveness): Όλες οι συναλλαγές που προέρχονται από έμπιστους κόμβους τελικά θα επιβεβαιωθούν.
- Συνολική σειρά (Total order): Όλοι οι έμπιστοι κόμβοι αποδέχονται την ίδια σειρά συναλλαγών, εφόσον έχουν επιβεβαιωθεί στο τοπικό τους αντίγραφο.

Στην εργασία του Lamport et al. (1982) αποδείχθηκε ότι συναίνεση μπορεί να επιτευχθεί αν και μόνον αν $t < n/3$, όπου n είναι ο συνολικός αριθμός των κόμβων που συμμετέχουν.

10.2.2 Η συνάρτηση κατακερματισμού

Η συνάρτηση κατακερματισμού (hash function), γνωστή και ως συνάρτηση κατατεμαχισμού, είναι μια μαθηματική συνάρτηση που δέχεται ως είσοδο κάποιο δεδομένο τυχαίου μεγέθους και επιστρέφει ένα ακέραιο σταθερού μεγέθους αναπαράστασης. Οι τιμές που επιστρέφει η συνάρτηση κατατεμαχισμού ονομάζονται τιμές κατατεμαχισμού (hash values), ή κώδικες κατατεμαχισμού (hash codes), ή αθροίσματα κατατεμαχισμού (hash sums) ή απλά τιμές κατατεμαχισμού (hashes). Οι τιμές αυτές θα πρέπει να είναι διαφορετικές για διαφορετική είσοδο, καθώς η κύρια χρησιμότητα αυτών των συναρτήσεων είναι να ταυτοποιούν τα δεδομένα.

Ο κατακερματισμός γενικότερα είναι μια μέθοδος μετατροπής συμβολοσειρών σε θέσεις ενός πίνακα. Ο δείκτης του πίνακα προσδιορίζεται με "κερματισμό" (hashing) του συμβόλου κάνοντας κάποια απλή αριθμητική ή λογική πράξη με το σύμβολο και ενδεχομένως το μήκος του. Μια απλή συνάρτηση κερματισμού (hash function) θα ήταν η εσωτερική αναπαράσταση του πρώτου χαρακτήρα του συμβόλου.

Εφ' όσον δύο ονόματα δεν κάνουν κατακερματισμό στην ίδια διεύθυνση (στον ίδιο δείκτη) το κόστος της ανίχνευσης είναι μόνο το κόστος της πράξης του κατακερματισμού. Προβλήματα δημιουργούνται όταν δύο σύμβολα κερματίζουν στον ίδιο δείκτη. Τότε έχουμε σύγκρουση. Προφανώς μόνο ένα σύμβολο μπορεί να τοποθετηθεί σε κάθε θέση του πίνακα, επομένως πρέπει να βρούμε κάποια άλλη θέση για το δεύτερο σύμβολο. Μια καλή συνάρτηση κερματισμού (hash function) πρέπει να απλώνει ομοιόμορφα τις υπολογιζόμενες διευθύνσεις κατά μήκος του πίνακα ώστε οι συγκρούσεις να είναι σπάνιες. Η συνάρτηση κατακερματισμού που περιγράφηκε παραπάνω, είναι προφανώς κακή, διότι όλα τα σύμβολα που αρχίζουν με το ίδιο γράμμα κάνουν κατακερματισμό στην ίδια διεύθυνση (Πιντέλας, 2003).

Όπως αναφέραμε και αμέσως στην προηγούμενη παράγραφο, το Hashcash είναι ένας αλγόριθμος που απαιτεί μια σχετικά μικρή υπολογιστική ποσότητα εργασίας για να κωδικοποιήσει ένα αρχικό κείμενο, και πολύ λίγο χρόνο ώστε να επαληθευτεί αποτελεσματικά, ότι είναι η σωστή κωδικοποίηση. Για παράδειγμα σε ένα μήνυμα ηλεκτρονικού ταχυδρομείου, στην κεφαλίδα ενός μηνύματος ηλεκτρονικού ταχυδρομείου προστίθεται μια ψηφιακή σφραγίδα με τη χρήση του αλγορίθμου hashcash, που αποδεικνύει ότι ο αποστολέας έχει δαπανήσει ένα μέτριο ποσό χρόνου CPU για τον υπολογισμό της ψηφιακής σφραγίδας πριν από την αποστολή

του μηνύματος ηλεκτρονικού ταχυδρομείου. Με άλλα λόγια, καθώς ο αποστολέας έχει δαπανήσει αρκετό χρόνο για να δημιουργήσει τη σφραγίδα και να στείλει το μήνυμα ηλεκτρονικού ταχυδρομείου, είναι απίθανο να είναι spammer (άτομα που στέλνουν ψευδή ή διαφημιστικά ηλεκτρονικά μηνύματα). Ο αποδέκτης μπορεί, με αμελητέο υπολογιστικό κόστος, να επαληθεύσει ότι η σφραγίδα είναι έγκυρη. Ωστόσο, ο μόνος δυνατός τρόπος να βρεθεί μια κεφαλίδα με τις απαραίτητες ιδιότητες είναι με διαδοχικές προσπάθειες (brute computational force), προσπαθώντας με τυχαίες τιμές και όλους τους δυνατούς συνδυασμούς μέχρι να βρεθεί η σωστή απάντηση. Αυτό σημαίνει ότι θα απαιτηθεί ένας σημαντικός αριθμός προσπαθειών για να βρεθεί η απάντηση.

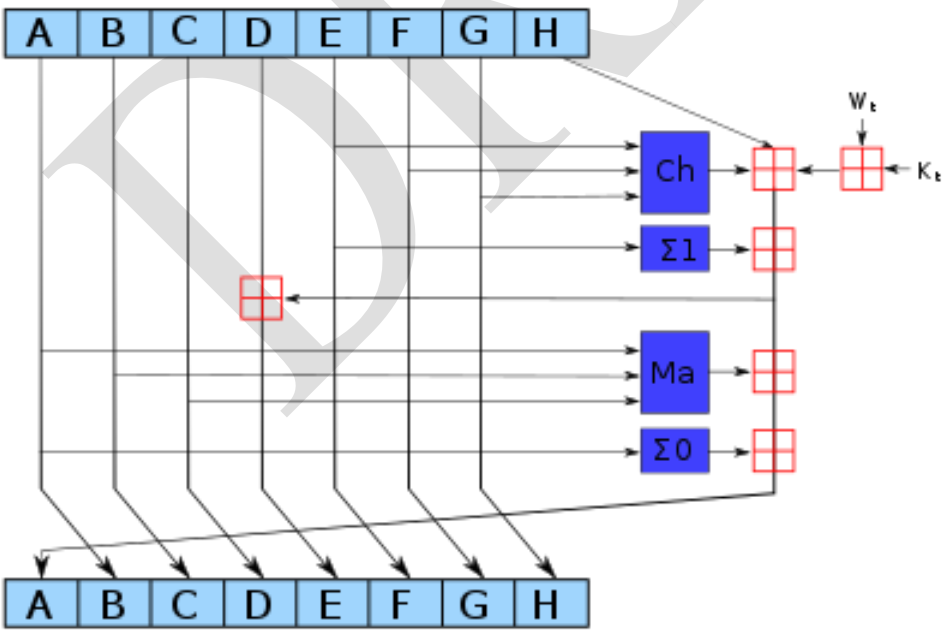
Ένα άλλο παράδειγμα είναι ο υπολογισμός του hash ενός αρχείου που έχει γίνει download και η σύγκριση του αποτελέσματος με ένα προηγουμένως δημοσιευμένο αποτέλεσμα του hash, μπορεί να δείξει αν το αρχείο έχει τροποποιηθεί ή αλλοιωθεί.

Στην περίπτωση των blockchains, η πιο διαδεδομένη συνάρτηση κατακερματισμού που χρησιμοποιείται, βασίζεται στον αλγόριθμο SHA-256 (Gilbert & Handschuh, 2003), που εισήχθη αρχικά ως μέρος του hashcash και συνεπώς ως μέρος του Bitcoin. Κάποιοι άλλοι αλγόριθμοι κατακερματισμού που χρησιμοποιούνται για την απόδειξη της εργασίας είναι οι Scrypt (King, 2013), Blake-256 (Kahri, 2013), HEFTY1, Quark, SHA-3 (Aumasson et al., 2008), καθώς και συνδυασμοί αυτών.

Ο SHA-2 (Secure Hash Algorithm 2) είναι ένα σύνολο κρυπτογραφικών συναρτήσεων κατακερματισμού που σχεδιάστηκαν από την Υπηρεσία Εθνικής Ασφάλειας των Ηνωμένων Πολιτειών (NSA) (Penard, 2008). Κατασκευάζονται χρησιμοποιώντας τη δομή Merkle-Damgård, με λειτουργία συμπίεσης μονής κατεύθυνσης, η οποία κατασκευάζεται με τη σειρά της με χρήση της δομής Davies-Meyer. Η οικογένεια SHA-2 αποτελείται από έξι συναρτήσεις κατακερματισμού που είναι οι SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 και SHA-512/224 και παράγουν τιμές κατακερματισμού μήκους 224, 256, 384 και 512 bits αντίστοιχα.

Τα SHA-256 και SHA-512 είναι νέες λειτουργίες κατακερματισμού που υπολογίζονται με λέξεις 32-bit και 64-bit αντίστοιχα. Χρησιμοποιούν διαφορετικές ποσότητες μετατόπισης και πρόσθετες σταθερές, αλλά οι δομές τους είναι κατά τα άλλα σχεδόν ίδιες, διαφέρουν μόνο στον αριθμό των επαναλήψεων.

Στην Εικόνα 10.8 παρουσιάζεται ο τρόπος εργασίας το αλγορίθμου SHA-256 για μια επανάληψη.



Εικόνα 10.8 *Η λειτουργία της hash συνάρτησης SHA-256 σε μια επανάληψη (πηγή http//en.wikipedia.org)*

Οι μπλε κόμβοι είναι οι κόμβοι υπολογισμού που κάνουν τους παρακάτω υπολογισμούς:

$$Ch(E,F,G) = (E \wedge F) \oplus (\sim E \wedge G)$$
$$Ma\,(A,B,C) = (A \wedge B) \oplus (A \wedge C) \oplus (B \wedge C)$$
$$\Sigma_o(A) = (A \ggg 2) \oplus (A \ggg 13) \oplus (A \ggg 22)$$
$$\Sigma_1(E) = (E \ggg 6) \oplus (E \ggg 11) \oplus (E \ggg 25)$$

όπου

∧ είναι το logical AND,
~ είναι το bitwise NOT,
⊕ είναι το αποκλειστικό ή (eXlusive OR), και
⋙ είναι η δεξιά μετατόπιση και το γέμισμα από αριστερά με μηδέν (zero fill right shift),

ενώ

τα κόκκινα πλέγματα αντιστοιχούν υπόλοιπο της διαίρεσης του αριθμού με το 2^{32}.

Σε πρακτικό επίπεδο η συνάρτηση κατακερματισμού είναι εξαιρετικά σημαντική για τα δίκτυα blockchain αφού συνήθως είναι άμεσα συνδεδεμένη με την απόδειξη εργασίας και συνεπώς με τους υπολογιστικούς πόρους που είναι αναγκαίοι για τη λειτουργία του συστήματος.

Για παράδειγμα στην Εικόνα 10.9 παρουσιάζεται με γραφικό τρόπο ο αριθμός των εκτιμώμενων κατακερματισμών σε tera ανά δευτερόλεπτο (τρισεκατομμύρια κατακερματισμοί ανά δευτερόλεπτο) που πραγματοποιεί το δίκτυο Bitcoin[6]. Ο αριθμός αυτός τον Σεπτέμβριο του 2018 ήταν 43,964,712.08 TH/sec, ενώ είναι τόσο μεγάλος που αποτελεί και ένα από τα βασικά προβλήματα του δικτύου Bitcoin αφού για να γίνουν αυτοί οι υπολογισμοί εκτιμάται ότι θα καταναλωθούν 73,12 TWh (Tera Watt hours)[7]. Η ενέργεια αυτή είναι αντίστοιχη με την ενέργεια που χρειάζεται για ένα χρόνο σε 6.770.506 νοικοκυριά στις Η.Π.Α. (σημειωτέων η κατανάλωση ενέργειας στα αμερικανικά νοικοκυριά είναι από τις υψηλότερες στον πλανήτη). Στην Εικόνα 10.10 παρουσιάζεται συγκριτικά με διάφορες χώρες η κατανάλωση ενέργειας του δικτύου Bitcoin.

Αυτό επεξηγεί γιατί απαιτούνται νέοι τρόποι επαλήθευσης της εργασίας με μικρότερες απαιτήσεις σε ενέργεια. Στον Πίνακα 10.1. παρουσιάζονται βασικά οικονομικά στοιχεία του δικτύου Bitcoin.

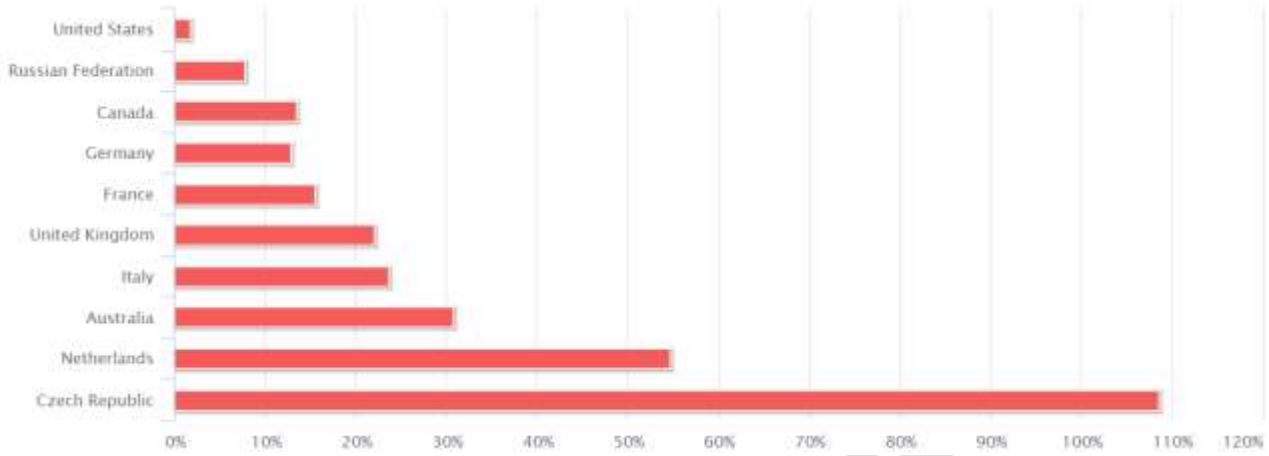
Περιγραφή	Τιμή
Η τρέχουσα εκτιμώμενη ετήσια κατανάλωση ηλεκτρικής ενέργειας του Bitcoin (TWh)	73,12
Η τρέχουσα ελάχιστη ετήσια κατανάλωση ηλεκτρικής ενέργειας του Bitcoin (TWh)	57,43
Ετήσια παγκόσμια έσοδα προερχόμενα από την εξόρυξη	$4.839.148.964
Ετήσιο εκτιμώμενο συνολικό κόστος εξόρυξης	$3.656.073.069
Το ποσοστό κόστους εξόρυξης προς τα έσοδα	75,55%
Χώρα με την μεγαλύτερη ως ποσοστό κατανάλωση ηλεκτρικής ενέργειας στο Bitcoin	Αυστρία
Εκτιμώμενη ηλεκτρική ενέργεια που χρησιμοποιήθηκε κατά την προηγούμενη ημέρα (KWh)	200.332.771

[6] Η χρησιμοποιούμενη μονάδα μέτρησης είναι TH/s (Tera Hash per second)
[7] https://digiconomist.net/bitcoin-energy-consumption

Περιγραφή	Τιμή
Εκτιμώμενα Watts ανά GH/s	0,147
Συνολικό Hashrate δικτύου σε PH / s (1.000.000 GH / s)	56,865
Ηλεκτρική ενέργεια που καταναλώνεται ανά συναλλαγή (KWh)	893
Αριθμός νοικοκυριών των ΗΠΑ που θα μπορούσαν να τροφοδοτηθούν αντί για το Bitcoin	6.770.506
Αριθμός νοικοκυριών των ΗΠΑ που μπορούσαν να τροφοδοτηθούν για 1 ημέρα από την ηλεκτρική ενέργεια που καταναλώνεται για μία μόνο συναλλαγή	30,18
Η κατανάλωση ηλεκτρικής ενέργειας του Bitcoin ως ποσοστό της παγκόσμιας κατανάλωσης ηλεκτρικής ενέργειας	0,33%
Το ετήσιο αποτύπωμα άνθρακα (kt CO2)	35.830
Αποτύπωμα άνθρακα ανά συναλλαγή (kg CO2)	437,5

Πίνακας 10.1 *Η κατανάλωση ενέργειας δικτύου Bitcoin (πηγή https://digiconomist.net/bitcoin-energy-consumption)*

Εικόνα 10.9 *Ο αριθμός των εκτιμώμενων κατακερματισμών σε TH/sec (πηγή www.blockchain.com)*

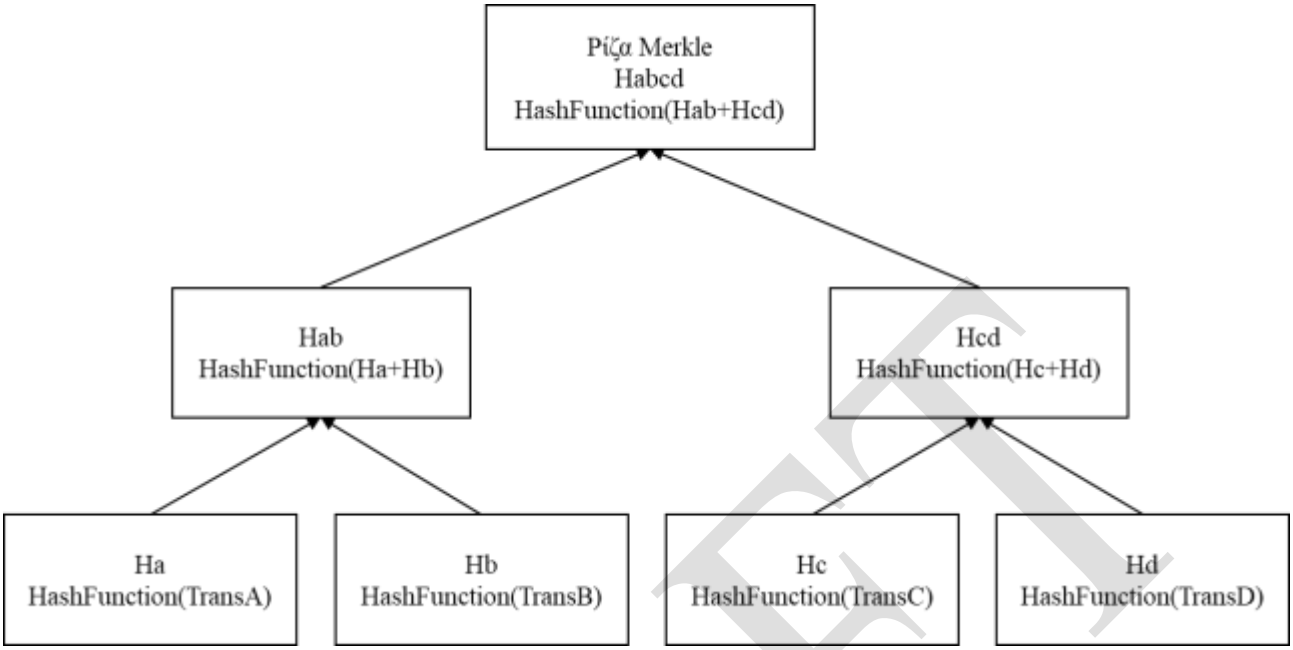


Εικόνα 10.10 *Συγκριτική κατανάλωση ενέργειας δικτύου Bitcoin με άλλες χώρες (πηγή BitcoinEnergyConsumption.com)*

10.2.3 Η ρίζα και το δέντρο Merkle

Η ρίζα Merkle είναι μια συνολική ψηφιακή υπογραφή της λίστας των συναλλαγών που περιλαμβάνονται σ'αυτό. Η ρίζα Merkle είναι μοναδική σε σχέση με τα άλλα block και συνιστά μια πολύ αποτελεσματική μέθοδο για την επαλήθευση αν όντως μία συναλλαγή περιλαμβάνεται στο block. Για το λόγο αυτό θεωρείται ως το πιο σημαντικό τμήμα της επικεφαλίδας του block.

Η ρίζα Merkle παράγεται από το δέντρο Merkle το οποίο κατασκευάζεται από τον κατακερματισμό (hash) της κάθε μεμονωμένης συναλλαγής, δημιουργώντας με αυτόν τον τρόπο για κάθε συναλλαγή ένα κόμβο - φύλλο στο δέντρο. Στη συνέχεια, οι κόμβοι αυτοί επανα-κατακερματίζονται σε ζεύγη, καταλήγοντας σε ένα νέο σύνολο κόμβων ένα επίπεδο υψηλότερα στο δέντρο Merkle. Η διαδικασία επαναλαμβάνεται έως ότου μείνει μόνο ένας κόμβος στο δένδρο, ο οποίος και αποτελεί την ρίζα Merkle. Η συμπερίληψη της ρίζας Merkle σε ένα block επιτρέπει στους χρήστες να μπορούν να πιστοποιήσουν τις εμπεριεχόμενες στο block συναλλαγές. Στην Εικόνα 10.11 παρουσιάζεται η διαδικασία παραγωγής της ρίζας Merkle για τέσσερις συναλλαγές με όνομα TransA, TransB, TransC και TransD αντίστοιχα. Σε πρώτο βήμα με τη χρήση της συνάρτησης κατακερματισμού HashFunction παράγονται οι τιμές κατακερματισμού Ha, Hb, Hc και Hd (hash values) μία για κάθε συναλλαγή. Στις συνέχεια οι τιμές κατακερματισμού Ha και Hb επανα-κατακερματίζονται με την HashFunction(Ha+Hb) ώστε να παραχθεί η νέα τιμή κατακερματισμού Hab. Με αντίστοιχο τρόπο παράγεται και η τιμή κατακερματισμού Hcd. Η ρίζα Merkle είναι η τιμή κατακερματισμού που παράγεται από τον κατακερματισμό των HashFunction(Hab+Hcd).



Εικόνα 10.11 *Η δημιουργία της λίστα Merkle*

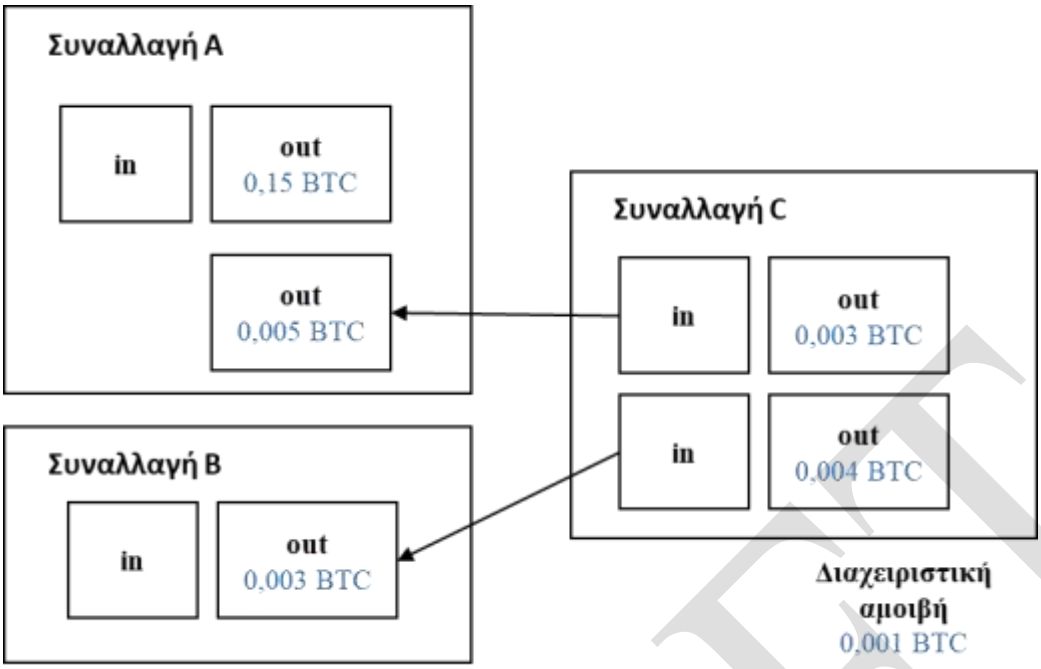
10.2.4 Η δομή και ο τρόπος λειτουργίας των συναλλαγών.

Μια συναλλαγή (transaction) σε ένα blockchain δίκτυο είναι ένα υπογεγραμμένο κομμάτι δεδομένων που μεταδίδεται στο δίκτυο και, εάν είναι έγκυρο, καταλήγει ως τμήμα ενός block του blockchain. Ο σκοπός μιας συναλλαγής είναι η μεταφορά ενός περιουσιακού στοιχείου από ένα ιδιοκτήτη σε έναν άλλο. Για την καλύτερη κατανόηση του τόπου λειτουργίας των συναλλαγών αναφερόμαστε ξανά στο δίκτυο Bitcoin. Ωστόσο ο τρόπος λειτουργίας και των άλλων συστημάτων blockchain είναι αντίστοιχος.

Όταν ένας χρήστης στέλνει ένα Bitcoinσε έναν άλλο χρήστη (τον παραλήπτη), δημιουργείται μια συναλλαγή σε Bitcoin, η οποία μεταδίδεται στο δίκτυο Bitcoin. Εάν η συναλλαγή είναι έγκυρη, οι κόμβοι του δικτύου θα την συμπεριλάβουν σε ένα block που εξορύσσεται εκείνη τη στιγμή. Συνήθως, μέσα σε 10-20 λεπτά, η συναλλαγή θα συμπεριληφθεί, μαζί με άλλες συναλλαγές, σε ένα block και θα προστεθεί στο blockchain. Σε αυτό το σημείο ο παραλήπτης των χρημάτων μπορεί να δει το ποσό της συναλλαγής στο ψηφιακό του πορτοφόλι. Ένα ψηφιακό πορτοφόλι Bitcoin είναι ένα πρόγραμμα λογισμικού όπου αποθηκεύονται τα Bitcoins. Για να είμαστε τεχνικά ακριβείς, τα Bitcoins δεν αποθηκεύονται οπουδήποτε. Όμως υπάρχει ένα ιδιωτικό κλειδί (μυστικός αριθμός) για κάθε διεύθυνση Bitcoin που αποθηκεύεται στο πορτοφόλι Bitcoin του ατόμου που κατέχει το νόμισμα αυτό. Τα ψηφιακά πορτοφόλια Bitcoin διευκολύνουν την αποστολή και τη λήψη Bitcoins και δίνουν την ιδιοκτησία ενός ποσού bitcoin σε χρήστες.

Μια συναλλαγή έχει ένα αριθμό inputs και ένα αριθμό outputs και όπως όλες οι συναλλαγές μετασχηματίζουν τα inputs σε outputs. Στην Εικόνα 10.12 παρουσιάζεται μια απλοποιημένη συναλλαγή ώστε να γίνει κατανοητός ο τρόπος λειτουργίας. Έστω οι παλαιές συναλλαγές Α και Β και η τρέχουσα συναλλαγή C. Η τρέχουσα συναλλαγή C λαμβάνει ως input 0,005 από τη συναλλαγή Α και 0,003 BTC[8] από τη συναλλαγή Β. Παρατηρήστε ότι τα βέλη στην Εικόνα 10.12 ξεκινούν από τη συναλλαγή C και κατευθύνονται προς τα πίσω υποδηλώνοντας τη ροή των bitcoins προς τα πίσω και την ιχνηλασιμότητα αυτών. Οι έξοδοι της συναλλαγής C είναι 2 και αφορούν 0,003 BTC που κατευθύνονται προς μια πρώτη διεύθυνση και 0,004 BTC που κατευθύνονται προς μια δεύτερη διεύθυνση. Το υπόλοιπο 0,001 BTC πηγαίνει στο miner του μπλοκ και παρουσιάζεται εκτός της συναλλαγής. Σημειώστε επίσης ότι το 0,015 BTC της συναλλαγής Α δεν δαπανάται σε αυτή τη συναλλαγή και παραμένει στο ψηφιακό πορτοφόλι του χρήστη.

[8] Το bitcoin υποδιαιρείται σε satoshi που είναι η μικρότερη υποδιαίρεση του νομίσματος bitcoin που καταγράφεται στην αλυσίδα των μπλοκ. Εκατό εκατομμύρια satoshi ισοδυναμούν με ένα bitcoin. Δηλαδή, η μικρότερη συναλλαγή μπορεί να είναι 0,00000001 BTC ή 1 satoshi. Η υποδιαίρεση αυτή ονομάστηκε έτσι αποτείνοντας φόρο τιμής στον αρχικό δημιουργό του Bitcoin, Satoshi Nakamoto.



Εικόνα 10.12 *Ο τρόπος εκτέλεσης των συναλλαγών στο δίκτυο Bitcoin.*

Στην Εικόνα 10.13 παρουσιάζεται μια συναλλαγή bitcoin σε μορφή κειμένου. Στην εικόνα αυτή:

- το hash προσδιορίζει την ταυτότητα της συναλλαγής (txid),
- το ver (version) προσδιορίζει ποια είναι η δομή της συναλλαγής,
- το vin_sz είναι ο αριθμός των input,
- το vout_sz είναι ο αριθμός των output,
- το lock_time πρέπει να είναι μηδέν ή χρόνος προγενέστερος του τρέχοντος ώστε η συναλλαγή να θεωρηθεί να είναι έγκυρη, και
- το size είναι το μέγεθος της συναλλαγής σε bytes.

```
{
"hash":"90b18aa54288ec610d83ff1abe90f10d8ca87fb6411a72b2e56a169fdc9b0219",
"ver":1,
"vin_sz":1,
"vout_sz":2,
"lock_time":0,
"size":226,
"in":[
 {
  "prev_out":{
   "hash":"18798f8795ded46c3086f48d5bdabe10e1755524b43912320b81ef547b2f939a",
   "n":0
  },
  "scriptSig":"3045022100c1efcad5cdcc0dcf7c2a79d9e1566523af9c7229c78ef71ee8b6300ab...[
 }
],
"out":[
 {
  "value":"5.93100000",
  "scriptPubKey":"OP_DUP OP_HASH160 4b358739fc7984b8101278988beba0cc00867adc OP_EQUALVERIFY OP_CHECKSIG"
 },
 {
  "value":"1678.06900000",
  "scriptPubKey":"OP_DUP OP_HASH160 55368b388ccfe22a3f837c9eee93d053460db339 OP_EQUALVERIFY OP_CHECKSIG"
 }
]
}
```

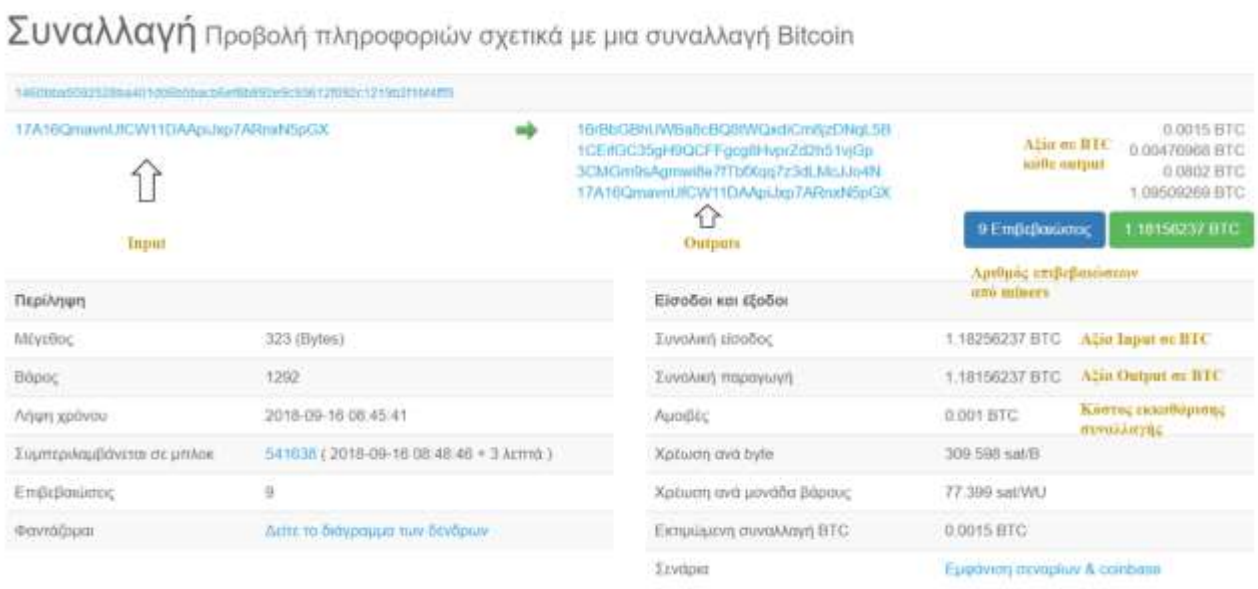

Εικόνα 10.13 *Ο τρόπος εκτέλεσης των συναλλαγών στο δίκτυο Bitcoin.*

Κάθε χρησιμοποιούμενη είσοδος πρέπει να δαπανηθεί εξ ολοκλήρου σε μια συναλλαγή. Αν μια διεύθυνση έλαβε 10 bitcoins σε μια συναλλαγή και απλά κάποιος θέλει να ξοδέψει 1 bitcoin, η συναλλαγή πρέπει να καταναλώσει και τα 10 bitcoins. Η λύση στην περίπτωση αυτή είναι να δημιουργήσουμε μια δεύτερη έξοδο, η οποία θα επιστρέφει πίσω τα 9 bitcoins που δεν καταναλώθηκαν. Το bitcoin στο σημείο αυτό λειτουργεί ακριβώς με τον ίδιο τρόπο, όπως και το χάρτινο χρήμα. Δηλαδή, δίνουμε ένα χαρτονόμισμα των 10 € για να πληρώσουμε την προμήθεια ενός αναψυκτικού που κοστίζει 1 € και παίρνουμε πίσω ως ρέστα 9 €.

Οι συναλλαγές μπορούν επίσης να περιλαμβάνουν τέλη συναλλαγής. Εάν υπάρχουν υπόλοιπα bitcoins μετά από την προσθήκη των εισροών και την αφαίρεση των εξόδων, το υπόλοιπο είναι το τέλος ή η προμήθεια που καταβάλλεται στο miner. Η προμήθεια αυτή είναι η αμοιβή των miners ώστε να επαληθεύσουν την συναλλαγή. Όταν δημιουργείται ένα μπλοκ, όλα τα τέλη από τις συναλλαγές συμπεριλαμβάνονται σε αυτό το block, και συλλέγονται από τον miner που το δημιούργησε. Τα τέλη συναλλαγής δεν είναι υποχρεωτικά αλλά υπονοούνται και είναι η διαφορά μεταξύ εισόδων και εξόδων της κάθε συναλλαγής. Βέβαια, ένα πρόσωπο που ζητά και δημιουργεί μια συναλλαγή μπορεί να μην προνοήσει ή να μην επιθυμεί να πληρώσει κάποιο ποσό ως τέλος συναλλαγής. Αντίστοιχα, οι miners δεν υποχρεούνται να συμπεριλάβουν συγκεκριμένες συναλλαγές στα block που παράγουν. Για το λόγο αυτό, προκειμένου να διασφαλιστεί ότι η συναλλαγή θα υποβληθεί σε άμεση επεξεργασία οι χρήστες συμπεριλαμβάνουν ένα τέλος συναλλαγής σε κάθε συναλλαγή ως ένα κίνητρο για τους miners. Μια τυπική χρέωση για μια συναλλαγή είναι περίπου 0.00002 bitcoins αλλά η τιμή αυτή μεταβάλλεται δυναμικά.

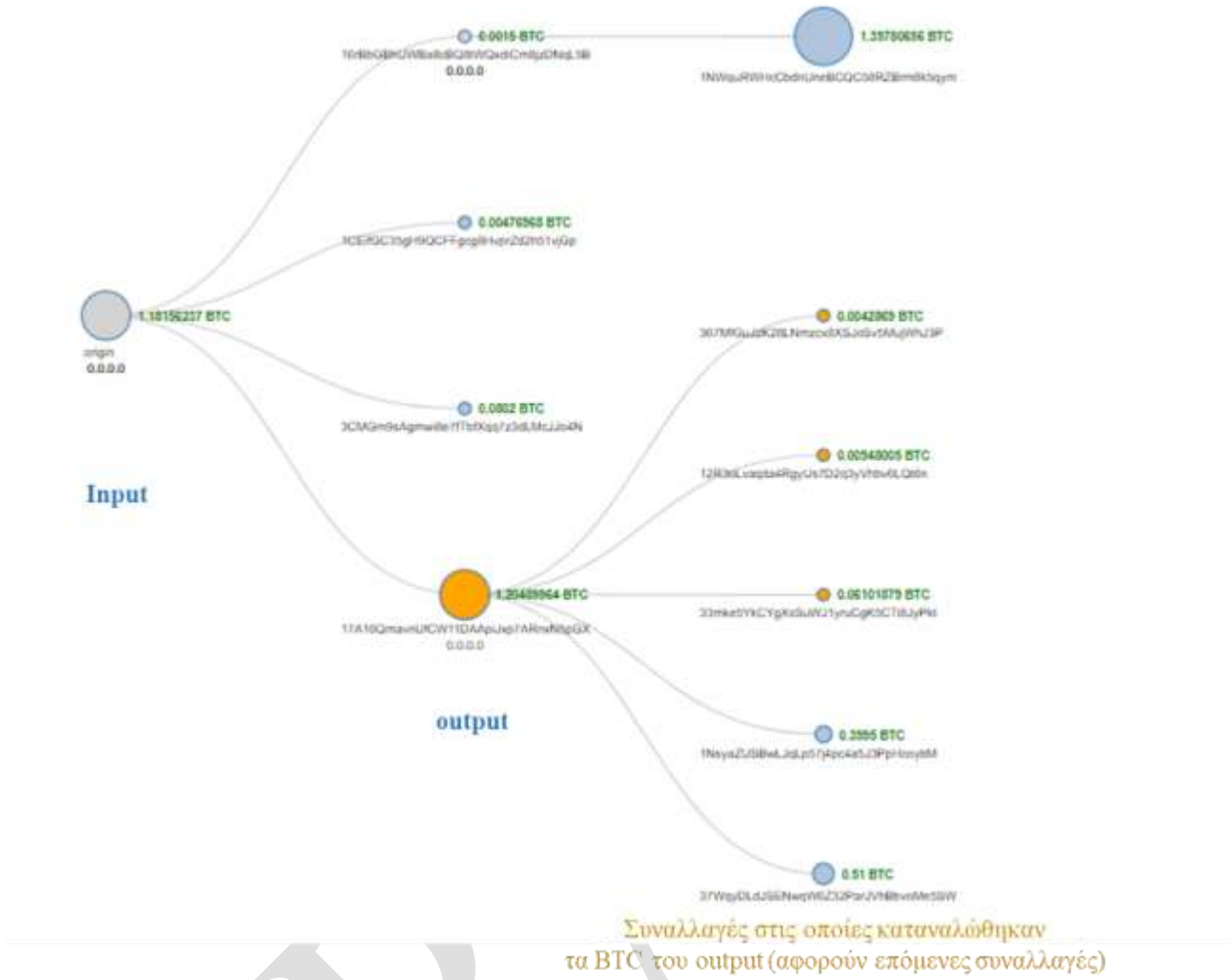
Σε πρακτικό επίπεδο με τη χρήση ενός εξερευνητή μπορούμε να δούμε όλες τις συναλλαγές που περιέχονται σε ένα block καθώς επίσης και με γραφικό τρόπο το δέντρο των συναλλαγών. Στην Εικόνα 10.14 παρουσιάζονται τα στοιχεία της συναλλαγής, δηλαδή τα inputs (TxIn), τα outputs (TxOut), η αξία του κάθε output, κ.λπ.

Ένα σημαντικό στοιχείο που δεν έχει αναφερθεί ακόμη είναι οι διευθύνσεις bitcoins. Μια διεύθυνση bitcoin είναι ένας συνδυασμός ψηφίων και χαρακτήρων και μοιράζονται όλοι όσοι θέλουν να λάβουν χρήματα (bitcoins). Στην πραγματικότητα, αυτή η διεύθυνση είναι μοναδική και καθορίζει την ιδιοκτησία bitcoin για ένα συγκεκριμένο χρήστη. Στην Εικόνα 10.14 τα inputs και outputs είναι διευθύνσεις bitcoins.



Εικόνα 10.14 *Προβολή μιας συναλλαγής με τον εξερευνητή Blockchain.info*

Στην Εικόνα 10.15 παρουσιάζεται το δέντρο των input και outputs μιας συναλλαγής. Τα ποσά των outputs που απεικονίζονται με πορτοκαλί χρώμα έχουν ήδη ξοδευτεί και για το λόγο αυτό μπορούμε να δούμε και το τρίτο επίπεδο των συναλλαγών που καταναλώθηκαν αυτά τα outputs.



Εικόνα 10.15 *Προβολή του δέντρου μια συναλλαγής με τον εξερευνητή Blockchain.info*

8.3. Έξυπνες συμβάσεις (Smart contracts) και το σύστημα Ethereum

Μια έξυπνη σύμβαση είναι ένα ειδικό πρωτόκολλο που προορίζεται στο να συμβάλει, να επαληθεύσει ή να εφαρμόσει τη διαπραγμάτευση ή την εκτέλεση μιας σύμβασης. Οι έξυπνες συμβάσεις επιτρέπουν την πραγματοποίηση αξιόπιστων συναλλαγών χωρίς τη διαμεσολάβηση τρίτων. Οι συναλλαγές αυτές είναι ιχνηλατήσιμες (traceable) και μη αναστρέψιμες (irreversible). Επιπλέον, τα έξυπνα συμβόλαια περιέχουν όλες τις πληροφορίες σχετικά με τους όρους της σύμβασης και εκτελούν αυτόματα όλες τις προβλεπόμενες ενέργειες.

Η ιδέα περιγράφηκε αρχικά από τον κρυπτογράφο Nick Szabo (1997), στο άρθρο του «Formalizing and Securing Relationships on Public Networks», ο οποίος καθόρισε τις βασικές αρχές των έξυπνων συμβάσεων, αλλά εκείνη την εποχή δεν υπήρχε κατάλληλο περιβάλλον για να τις υλοποιήσει. Σήμερα με την εμφάνιση της τεχνολογίας Blockchain και ιδιαίτερα με την εμφάνιση του Ethereum (https://www.ethereum.org/) δόθηκε η δυνατότητα εφαρμογής έξυπνων συμβάσεων σε ευρεία κλίμακα.

Η αρχή λειτουργίας των έξυπνων συμβάσεων είναι ότι η κάθε σύμβαση συνδέεται με ένα πρόγραμμα λογισμικού το οποίο εκτελείται σε προκαθορισμένα χρονικά σημεία. Το πρόγραμμα αυτό κωδικοποιεί τους συμβατικούς όρους, το οποίο στη συνέχεια κωδικοποιείται με μια συνάρτηση κατακερματισμού και

τοποθετείται στο block ενός blockchain[9]. Το πρόβλημα της προσέγγισης αυτής είναι ότι σύμφωνα με τη θεωρία υπολογισμού σε μια μηχανή Turing, δεν είναι γνωστό πότε θα τερματίσει ένα πρόγραμμα. Αυτό σημαίνει ότι μια σύμβαση με πολλούς όρους μπορεί να εκτελείται για σημαντικό χρονικό διάστημα, μπλοκάροντας όλους τους κόμβους του peer-to-peer δικτύου. Το σημαντικό αυτό πρόβλημα επιλύεται με την πληρωμή του υπολογιστικού πόρου που χρησιμοποιείται για την εκτέλεση του έξυπνου συμβολαίου. Έτσι όταν κάποιος επιθυμεί να τρέξει μια έξυπνη σύμβαση, θα πρέπει να την προικίσει με το αναγκαίο ποσό (σε κρυπτονομίσαμτα ether) που να επαρκούν για την εκτέλεση της σύμβασης τουλάχιστον για τον εκτιμώμενο χρόνο. Στην περίπτωση που το πρόγραμμα περιέχει κάποιο σφάλμα, και εκτελείται για περισσότερο από τον αναμενόμενο χρόνο, θα καταναλώσει όλα τα ether με τα οποία είναι προικισμένο και η εκτέλεσή του θα σταματήσει.

Στη συνέχεια η σύμβαση διανέμεται και αντιγράφεται πολλές φορές μεταξύ των κόμβων του δικτύου, όπως συμβαίνει σε όλα τα δίκτυα blockchain. Σε προκαθορισμένες χρονικές στιγμές, σύμφωνα με το χρονοδιάγραμμα, η σύμβαση εκτελείται, που σημαίνει ότι τρέχει το πρόγραμμα που συνδέεται με την σύμβαση και με τον τρόπο αυτό υλοποιούνται οι όροι της σύμβασης (π.χ. απαιτούμενες οικονομικές συναλλαγές).

Για να δημιουργήσουμε ένα έξυπνο συμβόλαιο χρειαζόμαστε:

- **Το αντικείμενο της σύμβασης**. Η εφαρμογή θα πρέπει να έχει πρόσβαση σε αγαθά ή υπηρεσίες με σκοπό να μπορεί να τα κλειδώνει και να τα ξεκλειδώνει αυτόματα.
- **Τις ψηφιακές υπογραφές**. Όλοι οι συμμετέχοντες ξεκινούν μια συμφωνία υπογράφοντας τη σύμβαση με τα ιδιωτικά κλειδιά τους.
- **Τους όρους της σύμβασης**. Οι όροι μιας έξυπνης σύμβασης έχουν τη μορφή μιας ακριβούς ακολουθίας λειτουργιών ώστε να μπορεί να δημιουργηθεί το πρόγραμμα λογισμικού. Όλοι οι συμμετέχοντες πρέπει να υπογράψουν αυτούς τους όρους.
- **Μια αποκεντρωμένη πλατφόρμα**. Το έξυπνο συμβόλαιο αναπτύσσεται στο blockchain αυτής της πλατφόρμας (π.χ. Ethereum) και διανέμεται μεταξύ των κόμβων του δικτύου.

Το Ethereum είναι ένα ανοικτό Blockchain σύστημα που προτάθηκε το 2013 από τον Vitalik Buterin πρώην προγραμματιστή του Bitcoin και δόθηκε στη δημοσιότητα τον Ιουλίου του 2015 (Wood, 2014; Buterin, 2013; Buterin,2014). Όπως και στην περίπτωση του Bitcoin, έτσι και το Ethereum δεν ελέγχεται από κάποια κεντρική αρχή, αλλά είναι μια πλατφόρμα ανοιχτού κώδικα. Σε αντίθεση με το Bitcoin, το Ethereum σχεδιάστηκε για να είναι προσαρμόσιμο, ευέλικτο και προγραμματιζόμενο. Αντί να δίνει στους χρήστες ένα σύνολο προκαθορισμένες υπηρεσίες (π.χ. συναλλαγές bitcoin), το Ethereum επιτρέπει στους χρήστες να δημιουργούν τις δικές τους υπηρεσίες οι οποίες ποικίλουν σε βαθμό δυσκολίας. Με τον τρόπο αυτό, χρησιμεύει ως πλατφόρμα για πολλούς διαφορετικούς τύπους αποκεντρωμένων εφαρμογών Blockchain, συμπεριλαμβανομένων, και των έξυπνων συμβάσεων.

Στην καρδιά του Ethereum βρίσκεται η εικονική μηχανή Ethereum Virtual Machine (Hirai, 2017), η οποία μπορεί να εκτελέσει κώδικα οποιασδήποτε αλγοριθμικής πολυπλοκότητας (μια μηχανή "Turing complete"). Επιπλέον, η εικονική μηχανή Ethereum ή EVM είναι εντελώς απομονωμένη, πράγμα που σημαίνει ότι ο κώδικας που τρέχει μέσα στο EVM δεν έχει πρόσβαση σε κανένα δίκτυο και συνεπώς, ο κώδικας είναι απόλυτα ασφαλής.

Το Ethereum ενσωματώνει πολλά χαρακτηριστικά και τεχνολογίες από το Bitcoin, ενώ ταυτόχρονα εισάγει πολλές καινοτομίες. Έτσι ενώ στην αλυσίδα Bitcoin το κάθε block αποτελεί έναν κατάλογο συναλλαγών, η βασική ιδέα του Ethereum είναι η ανταλλαγή «δεδομένων» μεταξύ λογαριασμών (accounts). Δηλαδή το κάθε μπλοκ στο Ethereum παρακολουθεί την κατάσταση κάθε λογαριασμού και όλες οι μεταβολές που γίνονται στο Ethereum αφορούν μεταφορά «αξίας», δηλαδή κρυπτονομισμάτων και πληροφοριών μεταξύ λογαριασμών.

Υπάρχουν δύο τύποι λογαριασμών:

- Εξωτερικά Ελεγχόμενοι Λογαριασμοί – (Externally Owned Accounts - EOA), οι οποίοι ελέγχονται από ιδιωτικά κλειδιά

- Λογαριασμοί συμβάσεων (Contract Accounts), οι οποίοι ελέγχονται από τον εσωτερικό τους κώδικα και μπορούν να «ενεργοποιηθούν» μόνο από έναν EOA

Οι λογαριασμοί EOA έχουν τα παρακάτω χαρακτηριστικά:

- έχουν ένα υπόλοιπο λογαριασμού όπως και οι τραπεζιτικοί λογαριασμοί,
- μπορούν να δημιουργούν συναλλαγές (είτε να μεταφέρουν οικονομικούς πόρους από ένα λογαριασμό σε ένα άλλο είτε να ενεργοποιούν τους όρους μια σύμβασης),
- ελέγχονται με ιδιωτικά κλειδιά χρηστών,

Αντίστοιχα οι Λογαριασμοί Συμβάσεων:

- σχετίζονται με μια σύμβαση,
- έχουν ένα υπόλοιπο λογαριασμού,
- κώδικα/λογισμικό που περιγράφει τους όρους της σύμβασης,
- η εκτέλεση του κώδικα ενεργοποιείται από συναλλαγές ή μηνύματα (κλήσεις) που λαμβάνονται από άλλες συμβάσεις.
- όταν εκτελείται - εκτελεί υπολογισμούς τυχαίας πολυπλοκότητας (πλήρης Turing) - χειρίζεται μόνο του την αποθήκευση των δεδομένων, δηλαδή μπορεί να έχει τη δική του μόνιμη κατάσταση - μπορεί να καλέσει/ενεργοποιήσει άλλες συμβάσεις, κ.λπ.

Όλες οι πράξεις στην blockchain Ethereum τίθενται σε κίνηση από συναλλαγές που ενεργοποιούνται από εξωτερικούς λογαριασμούς. Κάθε φορά που ένας συμβαλλόμενος λογαριασμός λαμβάνει μια συναλλαγή, εκτελείται ο κώδικας με τον οποίο σχετίζεται, σύμφωνα με τις παραμέτρους εισόδου που αποστέλλονται ως μέρος της συναλλαγής. Ο κώδικας εκτελείται από την εικονική μηχανή Ethereum, σε κάθε κόμβο που συμμετέχει στο δίκτυο, γεγονός που επαληθεύει και την εγκυρότητα της συναλλαγής.

Συνεπώς, η βασική διαφορά μεταξύ αυτών, είναι ότι ένας λογαριασμός EOA ελέγχεται από τους ίδιους τους χρήστες, καθώς μπορούν να ελέγχουν τα ιδιωτικά κλειδιά, τα οποία είναι απαραίτητα για την ανάληψη του ελέγχου σε ένα τέτοιο λογαριασμό, ενώ οι λογαριασμοί Contract Accounts, ελέγχονται από τον εσωτερικό κώδικα τους. Εάν ελέγχονται από έναν συγκεκριμένο χρήστη (EOA), είναι επειδή έχουν προγραμματιστεί να ελέγχονται από αυτόν με μια συγκεκριμένη διεύθυνση, η οποία με τη σειρά της ελέγχεται από όποιον κατέχει τα ιδιωτικά κλειδιά.

Όπως έχουμε ήδη αναφέρει ε προηγούμενη παράγραφο, οι χρήστες του Ethereum πρέπει να πληρώνουν μικρά τέλη σε κάθε τους συναλλαγή στο δίκτυο και αυτό γίνεται για να προστατεύεται το Blockchain Ethereum από επιθέσεις. Εάν μια συναλλαγή αφορά λογαριασμό Contract Account τότε ο αποστολέας της συναλλαγής πρέπει να πληρώσει για κάθε βήμα του "κώδικα-προγράμματος" που ενεργοποίησε. Αυτά τα τέλη συναλλαγών συλλέγονται από τους κόμβους που επικυρώνουν τα δεδομένα στο δίκτυο. Το Ethereum Blockchain χρησιμοποιεί για τις συναλλαγές μεταξύ χρηστών ένα κρυπτονόμισμα το οποίο ονομάζεται ether. Οι κόμβοι ανταμείβονται με ether για κάθε μπλοκ που επικυρώνουν.

Επομένως, κατά τη δημιουργία της κάθε συναλλαγής αυτή, προικίζεται με ένα ορισμένο ποσό ether που έχει επικρατήσει να ονομάζεται αέριο (gaz), ο σκοπός του οποίου είναι αφενός να περιορίσει το ποσό της εργασίας που απαιτείται για την εκτέλεση της συναλλαγής, αφετέρου να πληρώσει για αυτήν την εκτέλεση. Ενώ η EVM εκτελεί τη συναλλαγή, το αέριο εξαντλείται προοδευτικά σύμφωνα με συγκεκριμένους κανόνες. Η τιμή του αερίου είναι μια τιμή που καθορίζεται από το δημιουργό της συναλλαγής, ο οποίος πρέπει να πληρώσει το αέριο. Αν μετά την εκτέλεση παραμείνει κάποιο ποσό διαθέσιμο, επιστρέφεται με τον ίδιο τρόπο. Εάν το αέριο εξαντληθεί σε οποιοδήποτε σημείο της εκτέλεσης, η εκτέλεση σταματά και όλες οι τροποποιήσεις που έχουν γίνει ακυρώνονται.

Όλες οι συναλλαγές καθώς και τα υπόλοιπα λογαριασμών είναι εκφρασμένα ether και στην υποδιαίρεσή του wei. Στον Πίνακα 10.2 παρουσιάζονται οι υποδιαιρέσεις του ether σε wei.

Μονάδα	Τιμή σε Wei	Wei
Wei	1 wei	1
Kwei (babbage)	1e3 wei	1,000
Mwei (lovelace)	1e6 wei	1,000,000
Gwei (shannon)	1e9 wei	1,000,000,000
microether (szabo)	1e12 wei	1,000,000,000,000
milliether (finney)	1e15 wei	1,000,000,000,000,000
Ether	1e18 wei	1,000,000,000,000,000,000

Πίνακας 10.2 *Υποδιαιρέσεις του ether σε wei (πηγή http://ethdocs.org/en/latest/ether.html)*

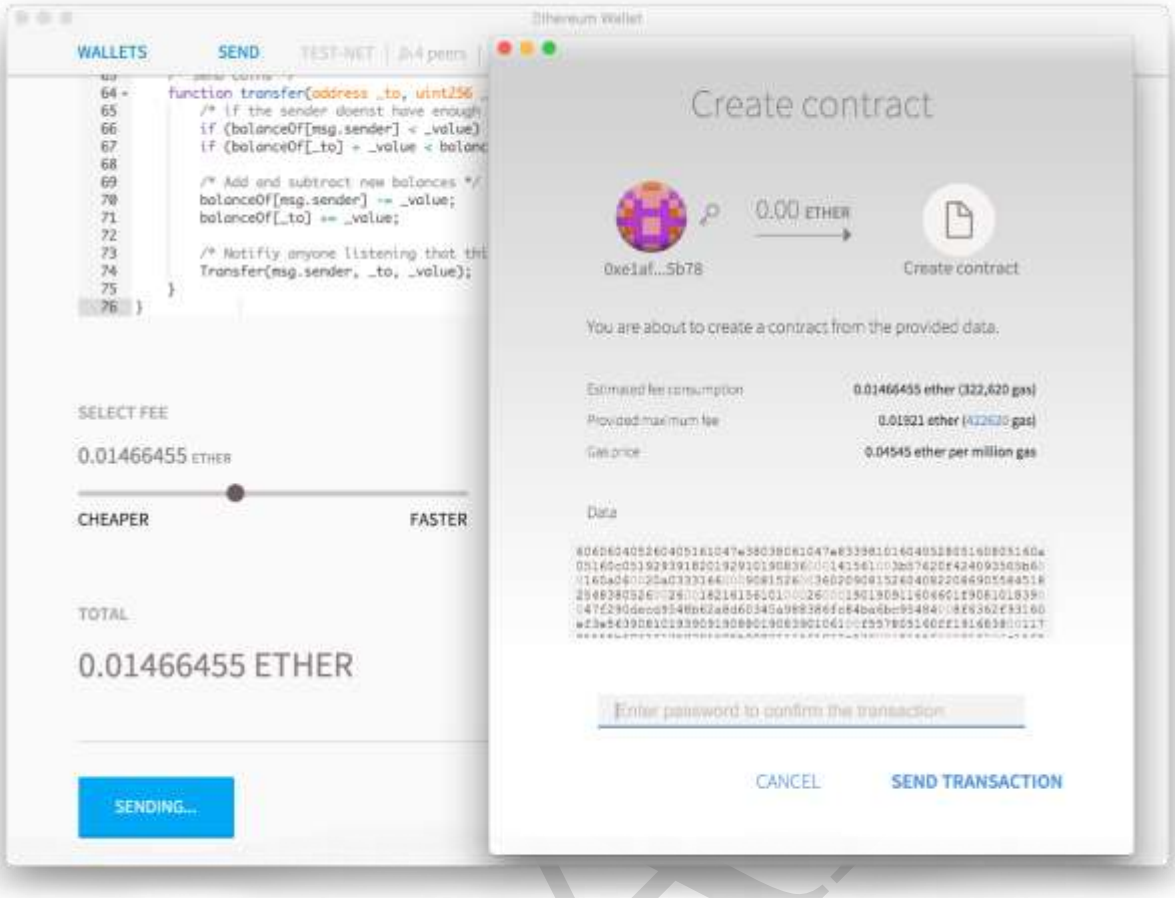
Παράδειγμα όρων έξυπνης σύμβασης

Ας υποθέσουμε ότι θέλουμε να νοικιάσουμε ένα διαμέρισμα.

a) Ο ενοικιαστής θα πρέπει να καταβάλει ένα ποσό μια προκαθορισμένη ημέρα και να λάβει μια απόδειξη και το ψηφιακό κλειδί εισόδου στο διαμέρισμα.
   - Ο ενοικιαστής θα πρέπει να πληρώσει το ενοίκιο με τη χρήση κρυπτονομίσματος.
   - Αν η πληρωμή γίνει νωρίτερα από την προκαθορισμένη ημέρα το σύστημα θα περιμένει να φτάσει η προκαθορισμένη ημερομηνία.
   - Αν το ψηφιακό κλειδί δεν έρθει την προκαθορισμένη ημερομηνία, δηλαδή δεν έρθει στην ώρα του, το blockchain δρομολογεί την επιστροφή των χρημάτων.

b) Αντίστοιχα, ο μισθωτής θα πρέπει να λάβει ένα ποσό μια προκαθορισμένη ημέρα, να εκδώσει μια απόδειξη και να παραχωρήσει το ψηφιακό κλειδί εισόδου του διαμερίσματος στον ενοικιαστή.
   - Αν το κλειδί σταλεί πριν από την προκαθορισμένη ημερομηνία έναρξης της ενοικίασης, η έξυπνη σύμβαση περιμένει τόσο την καταβολή της αμοιβής όσο και τη διάθεση του κλειδιού στον ενοικιαστή έως ότου φτάσει η προκαθορισμένη ημερομηνία.

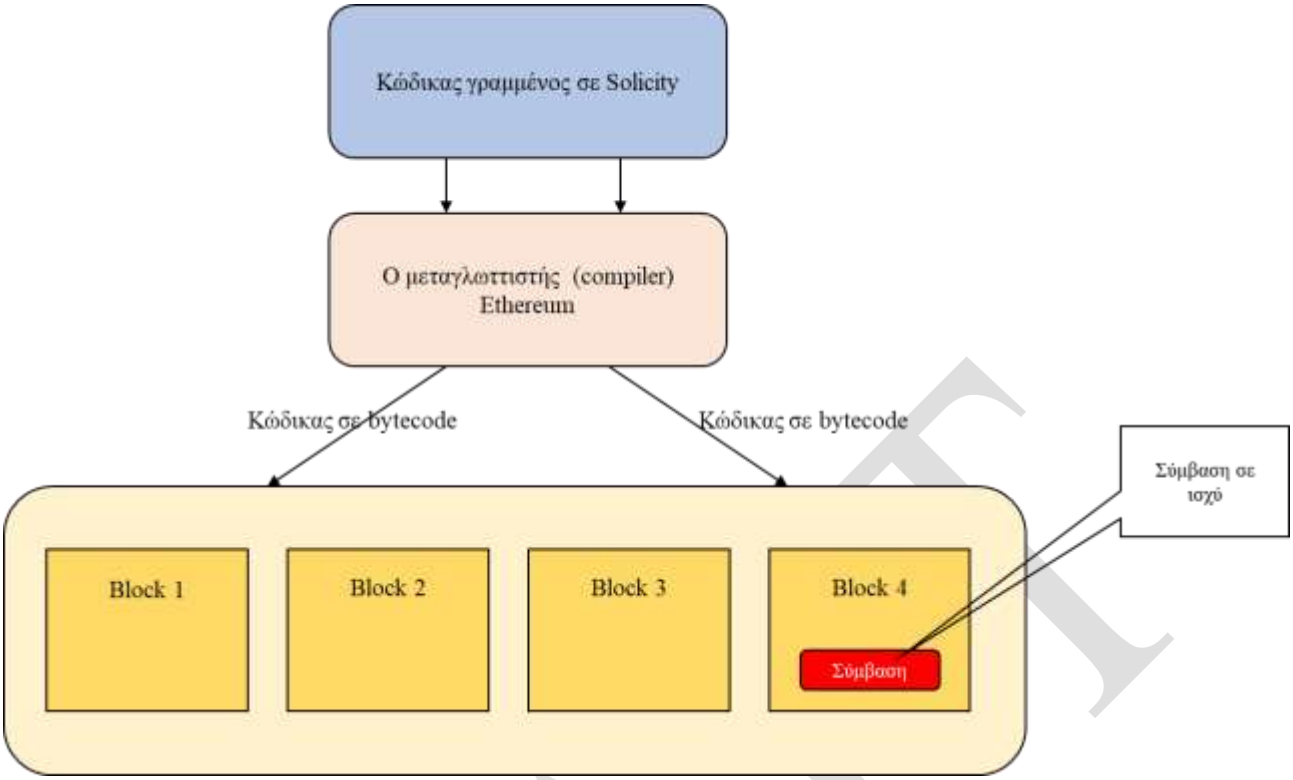
Το σύστημα blockchain εξασφαλίζει ότι εάν δοθεί το κλειδί τότε θα γίνει σίγουρα η πληρωμή. Αντίστοιχα αν σταλεί η πληρωμή bitcoins, θα ληφθεί το κλειδί. Το έγγραφο ακυρώνεται αυτόματα μετά την πάροδο του χρόνου και ο κώδικας δεν μπορεί να αλλάξει από κανένα.



Εικόνα 10.16 *Μια έξυπνη σύμβαση στο σύστημα Ethereun*

Στο δίκτυο Ethereum η γλώσσα προγραμματισμού που χρησιμοποιείται ονομάζεται Solidity. Η γλώσσα προγραμματισμού Solidity προτάθηκε αρχικά τον Αύγουστο του 2014 από τον Gavin Wood και αναπτύχθηκε αργότερα από την ομάδα Solidity του Ethereum, με επικεφαλής τον Christian Reitwiessner. Είναι μία από τις τέσσερις γλώσσες που έχουν σχεδιαστεί για να εκτελούνται με βάση την εικονική μηχανή (EVM) του Ethereum και είναι η πιο γνωστή και ευρέως χρησιμοποιούμενη γλώσσα για το συγκεκριμένο δίκτυο.

Η Solidity είναι γνωστή ως γλώσσα προγραμματισμού υψηλού επιπέδου. Είναι επίσης μια στατική γλώσσα προγραμματισμού σχεδιασμένη για την ανάπτυξη έξυπνων συμβολαίων (Smart Contracts) που εκτελούνται στο EVM. Τα αρχεία Solidity (.sol) για να μπορούν να διαβαστούν και να εκτελεστούν μέσα από την εικονική μηχανή (EVM) του Ethereum θα πρέπει να μετατραπούν σε γλώσσα μηχανής (bytecode). Η Solidity επιτρέπει στους προγραμματιστές να γράψουν κώδικα οποιασδήποτε αλγοριθμικής πολυπλοκότητας (Solidity, 2018). Στην Εικόνα 10.17, παρουσιάζεται η παραπάνω διαδικασία.



Εικόνα 10.17 *Ο τρόπος προγραμματισμούς στο σύστημα Ethereun*

Η Solidity είναι μια γλώσσα προγραμματισμού που μοιάζει με τη δημοφιλή γλώσσα Javascript. Στην Εικόνα 10.18 παρουσιάζεται ένα ψηφιακό token στη γλώσσα Solidity. Τα tokens στο οικοσύστημα του Ethereum μπορούν να αντιπροσωπεύουν οποιοδήποτε ανταλλάξιμο εμπορεύσιμο αγαθό: νομίσματα, πιστοποιητικά, αντικείμενα εντός ενός παιχνιδιού κλπ. Εφόσον όλα τα tokens υλοποιούν μερικά βασικά χαρακτηριστικά με έναν τυποποιημένο τρόπο, αυτό σημαίνει το token που κάποιος δημιουργεί θα είναι άμεσα συμβατό με κάθε άλλο πελάτη ή σύμβαση που χρησιμοποιεί τα ίδια πρότυπα.

```
pragma solidity ^0.4.20;

/* Η δημιουργία μιας σύμβασης με όνομα Mytoken */
contract MyToken {

      /* Δημιουργεί το υπόλοιπο της σύμβασης */
      mapping (address => uint256) public balanceOf;

 /* Αρχικοποιεί τη σύμβαση */
 function MyToken (uint256 initialSupply) public
      {
      // Δίνουμε στο δημιουργό την αρχική ποσότητα tokens  balanceOf[msg.sender] =
initialSupply;

      }

      // Συνάρτηση που μεταφέρει Tokens από ένα λογαριασμό σε κάποιο άλλο
      // Η συνάρτηση έχει ως παραμέτρους τον παραλήπτη και αξία προς μεταφορά
      // και κάθε φορά που κάποιος την καλεί θα αφαιρεθεί το ποσό από
      // το υπόλοιπο του αποστολέα και θα την προσθέσει στο υπόλοιπο του παραλήπτη.
      // Το πρόβλημα είναι εάν κάποιο άτομο θέλει να στείλει περισσότερα token
      // από αυτά που κατέχει. Για το λόγο αυτό πρέπει να γίνει ένας έλεγχος
      // αν το υπόλοιπο επαρκεί.
 function transfer(address _to, uint256 _value) public
            returns (bool success)
            {
```

```
            /* Ελέγχουμε αν ο αποστολέας (Sender) έχει αρκετά token
                  require(balanceOf[msg.sender] >= _value);

            require(balanceOf[_to] + _value >= balanceOf[_to]);
            /* Αφαιρούμε τα tokens από τον αποστολέα */
                  balanceOf[msg.sender] -= _value;

                  /* Προσθέτουμε τα token στον παραλήπτη */
                  balanceOf[_to] += _value;

            return true;
            }
      }
```

Εικόνα 10.18 Δημιουργία και μεταφορά tokens στο σύστημα Ethereun

10.4 Εφαρμογές με την τεχνολογία blockchain

Η τεχνολογία blockchain έχει τη δυνατότητα να μετατρέψει μακροπρόθεσμα πολλά και διαφορετικά από τα επιχειρηματικά μοντέλα. Η χρήση του blockchain θα επιτρέψει σημαντική βελτίωση της αποτελεσματικότητας στις παγκόσμιες αλυσίδες εφοδιασμού, τις χρηματοοικονομικές συναλλαγές, την αποκεντρωμένη κοινωνική δικτύωση, τη σύναψη συμφωνιών και πολλά άλλα. Κάποιες από αυτές τις εφαρμογές θα επιφέρουν δραστική αλλαγή του τρόπου του επιχειρείν.

Ο Πίνακας 10.3 παρουσιάζει ένα αριθμό κατηγοριών και περιοχών εφαρμογής στις οποίες η τεχνολογία blockchain μπορεί να επιφέρει σημαντικές αλλαγές

Κατηγορία	Παραδείγματα
Γενική	Συναλλαγές μεσεγγύησης, συμβάσεις, διαιτησίες, συναλλαγές με υπογραφή πολλαπλών συμβαλλομένων
Οικονομικές συναλλαγές	Χρηματιστήριο, ιδιωτικές τοποθετήσεις, crowdfunding, ομόλογα, αμοιβαία κεφάλαια, παράγωγα, συντάξεις
Δημόσια αρχεία	Τίτλοι γης και ιδιοκτησίας, εγγραφές οχημάτων, επιχειρηματικές άδειες, πιστοποιητικά γάμου, πιστοποιητικά θανάτου
Ταυτοποίηση	Άδειες οδήγησης, δελτία ταυτότητας, διαβατήρια, εγγραφές ψηφοφόρων
Ιδιωτικά αρχεία	Αξιόγραφα (I Own You – IOU), δάνεια, συμβόλαια, στοιχήματα, υπογραφές, διαθήκες, καταπιστεύματα, δεσμεύσεις
Επιβεβαίωση	Απόδειξη ασφάλισης, απόδειξη ιδιοκτησίας, συμβολαιογραφικά έγγραφα
Κλειδιά φυσικών στοιχείων	Οικίες, δωμάτια ξενοδοχείου, ενοικιαζόμενα αυτοκίνητα, κλειδιά αυτοκινήτων
Άυλα περιουσιακά στοιχεία	Διπλώματα ευρεσιτεχνίας, εμπορικά σήματα, δικαιώματα πνευματικής ιδιοκτησίας, κρατήσεις δωματίων ξενοδοχείων, κρατήσεις θέσεων παραστάσεων, αθλητικών γεγονότων, ονόματα τομέα διαδικτύου.

Πίνακας 10.3 *Κατανάλωση ενέργειας δικτύου Bitcoin (πηγή https://digiconomist.net/bitcoin-energy-consumption)*

Στη συνέχεια θα παρουσιάσουμε κάποιες από τις πιο ενδιαφέρουσες εφαρμογές της τεχνολογίας blockchain (Bambara & Allen, 2018).

10.4.1. Η τεχνολογία Blockchain στον χώρο των χρηματοοικονομικών υπηρεσιών

Η ραγδαία ανάπτυξη των συναλλαγών σε παγκόσμιο επίπεδο απαιτεί όλο και πιο εξελιγμένες τεχνολογικές εφαρμογές (fintech) ώστε να επιταχυνθεί και να μειωθεί το κόστος συναλλαγών για τίτλους και μετοχές. Αντίστοιχα, οι οικονομικές διαδικασίες που γίνονται με τον παραδοσιακό τρόπο διεκπεραιώνονται αργά, με χειρωνακτικό τρόπο και εμπεριέχουν σημαντικούς κίνδυνους κατά την εναρμόνιση και αντιστοίχισή τους, όταν γίνονται σε διεθνές επίπεδο – ενώ καθίστανται πιο σύνθετες με τα μη τυποποιημένα επενδυτικά προϊόντα. Σε όλο τον κύκλο ζωής αυτών των χρηματοοικονομικών προϊόντων αλλά και γενικότερα όλων των προϊόντων που εμπορευόμαστε κάθε συμμετέχων μιας συναλλαγής (π.χ. διαμεσολαβητές, διαμεσολαβητές, θεματοφύλακες, ομάδες εκκαθάρισης και διακανονισμού) διατηρεί επί του παρόντος το δικό του αντίγραφο του ίδιου αρχείου της συναλλαγής γεγονός που δημιουργεί σημαντικές ανεπάρκειες και περιθώρια για σφάλματα.

Δυστυχώς, η πραγματικότητα είναι ότι ένα ποσοστό των συναλλαγών εμπεριέχει σφάλματα, είτε από ανθρώπινα λάθη, είτε για άλλους λόγους, σφάλματα που απαιτούν χειρωνακτική εργασία για τη διόρθωσή τους καθώς και την επιμήκυνση του απαιτούμενου χρόνου για τη διευθέτηση των συναλλαγών. Η τεχνολογία blockchain δεν απαιτεί επαλήθευση, εκκαθάριση ή άλλους διακανονισμούς για τη διενέργεια ασφαλών συναλλαγών και συνεπώς αναμένεται να εξοικονομήσει ένα μεγάλο ποσό χρημάτων από τις απαιτούμενες αμοιβές και τις κεφαλαιακές επιβαρύνσεις. Έτσι αναμένεται ότι η τεχνολογία blockchain θα εξαλείψει σημαντικά τα απαιτούμενα τέλη για συναλλαγές Forex (currencies exchanges), από την εμπορία των προϊόντων (commodities) και των μετοχών ή παραγώγων που εμπορεύονται σε διεθνή χρηματιστήρια, κ.λπ.. Η τεχνολογία Blockchain μπορεί λοιπόν να απλοποιήσει και να εξορθολογίσει αυτή τη διαδικασία, παρέχοντας έναν αυτοματοποιημένο κύκλο ζωής για όλα τα υλικά ή άυλα εμπορεύσιμα αγαθά, όπου οι συμμετέχοντες σε μια συναλλαγής θα έχουν πρόσβαση στα ίδια ακριβώς δεδομένα.

10.4.2. Η τεχνολογία Blockchain και η οικονομία του διαμοιρασμού (sharing economy)

Η οικονομία του διαμοιρασμού είναι η διεργασία της ομότιμης συμμετοχής για την απόκτηση, παροχή ή κοινή χρήση αγαθών ή πρόσβασης σε αγαθά και υπηρεσίες που διευκολύνεται από μια δικτυακή πλατφόρμα και διενεργείται σε δίκτυα peer-to-peer.

Έχει παρατηρηθεί ότι οι μεγάλες επιχειρήσεις και δικτυακοί τόποι διαμοιρασμού βασίζονται σε πληροφορίες που παρέχουν οι χρήστες. Για παράδειγμα, η επιχείρηση διαμοιρασμού σπιτιών Airbnb, βασίζεται στα δεδομένα που εισάγουν οι χρήστες, με βάση τα οποία η πλατφόρμα Airbnb γίνεται δημοφιλής και αποκτά αξία.

Ένα βασικό πρόβλημα που αντιμετωπίζουμε στην οικονομία διαμοιρασμού είναι η δίκαιη κατανομή της αξίας (value) που παράγεται στα μέλη του δικτύου. Συνήθως το μεγαλύτερο ποσοστό της αξίας, των κερδών κατευθύνονται προς τους σημαντικούς μεσάζοντες του δικτύου. Στο σημείο αυτό μπορεί να παρέμβει η τεχνολογία blockchain, κάνοντας τους μεσάζοντες λιγότερο ή καθόλου αναγκαίους (στην περίπτωση αυτή η εταιρεία Airbnb δεν θα ήταν αναγκαία). Επιπλέον, ο τρόπος λειτουργίας της Airbnb έχει αλλάξει ριζικά τον τρόπο εργασίας σε ολόκληρο τον κλάδο των επιχειρήσεων φιλοξενίας, με αποτέλεσμα ορισμένες κυβερνήσεις να σπεύσουν να περιορίσουν και να φορολογήσουν τη δραστηριότητά αυτών των επιχειρήσεων, προκειμένου να προστατεύσουν τις υπάρχουσες παραδοσιακές ξενοδοχειακές επιχειρήσεις. Η ίδια ακριβώς κατάσταση υφίσταται και στο χώρο των μεταφορών με εταιρείες όπως την uber, την taxify κ.λπ.

Στην αντίπερα όχθη εφαρμογές όπως το La`Zooz (http://lazooz.org) είναι υπηρεσίες που βασίζονται σε ανοικτό κώδικα και αποτελούν ένα αποκεντρωμένο συνεργατικό σύστημα μεταφοράς. Το La`Zooz είναι μια λύση που βασίζεται στην τεχνολογία blockchain και ανταμείβει τους χρήστες της (προγραμματιστές, οδηγούς με ψηφιακά νομίσματα (tokens) τα οποία ονομάζονται zooz. Σε αντίθεση με την Uber, η La`Zooz δεν είναι κεντρικό σύστημα και συνεπώς δεν μπορεί να απαγορευτεί από κάποια κυβέρνηση. Η ιδιαιτερότητα του La`Zooz είναι ότι η ταυτότητά των χρηστών είναι προστατευμένη (στο βαθμό που κάποιος το επιθυμεί) και

συνδέεται με τις κριτικές και αξιολογήσεις που κάποιος κάνει για τις υπηρεσίες που παρέχει ή καταναλώνει. Το αποτέλεσμα είναι ότι οι χρήστες του συστήματος μπορούν να ελέγξουν ανά πάσα στιγμή την αξιοπιστία του κάθε ατόμου με βάση τον αναγνωριστικό αριθμό (id) του κάθε χρήστη. Αυτό προάγει την καλή συμπεριφορά και την υψηλή ποιότητα υπηρεσιών, διότι σε περίπτωση που κάποιος αποκτήσει κακή φήμη δεν μπορεί να διαγράψει το προφίλ του και να κάνει νέα εγγραφή με νέο όνομα, αφού όπως αναφέρθηκε, τα blocks σε ένα blockchain δεν μπορούν να αλλοιωθούν ή να αντιγραφούν.

10.4.3. Η τεχνολογία Blockchain και οι μεταφορές

Υπάρχουν διάφοροι τρόποι με τους οποίους μπορεί να εφαρμοστεί η τεχνολογία blockchain στον τομέα των μεταφορών. Ενδεικτικά αναφέρουμε:

- **Παρακολούθηση εμπορευμάτων** (Freight tracking, Load Boarding) - Η σωστή και χωρίς λάθη παρακολούθηση της παράδοσης των προϊόντων που παραδίδονται με οχήματα είναι ιδιαίτερα σημαντική σήμερα με την έκρηξη που παρατηρείται των αγορών μέσω internet. Η τεχνολογία Blockchain μπορεί να χρησιμοποιηθεί για την εξακρίβωση της ταυτότητας των δεδομένων μεταφοράς. Τα δεδομένα είναι αποθηκευμένα με χρήση της τεχνολογίας blockchain και συνεπώς είναι δύσκολο να τροποποιηθούν ή να διαγραφούν.

- **Τεχνητή νοημοσύνη και Διαδίκτυο των πραγμάτων** - Με την τεχνολογία blockchain, είναι ευκολότερο να ενσωματωθούν οι τεχνολογίες AI και IoT στον τομέα των μεταφορών. Αυτές οι τεχνολογίες χρησιμοποιούνται ουσιαστικά για να κατευθύνουν και να παρακολουθούν την κίνηση των πλοίων προς το σωστό προορισμό. Επίσης, χρησιμοποιούνται για τον υπολογισμό του διαθέσιμου χώρου στο αμπάρι των πλοίων ώστε να διασφαλιστεί η σωστή μεταφορά των προϊόντων. Επίσης, η χρήση της τεχνολογίας blockchain θα επιτρέψει την πραγματοποίηση άμεσων πληρωμών προς τις μεταφορικές εταιρείας, καθώς ο διαθέσιμος χώρος προς μεταφορά αλλά και η τιμή μεταφοράς των εμπορευμάτων είναι γνωστά μέσω του blockchain. Αυτό βοηθά στην εξοικονόμηση χρημάτων και χρόνου, καθιστώντας τις μεταφορές πιο αποτελεσματικές.
- **Παρακολούθηση στόλου** (Fleet Tracking) - Με την εφαρμογή του blockchain στον τομέα των μεταφορών, ολόκληρος ο στόλος των οχημάτων μιας επιχείρησης μπορεί εύκολα να διαχειρίζεται αφού γνωρίζουμε όχι μόνο τη γεωγραφική θέση του οχήματος, αλλά το χρόνο διέλευσης από επιλεγμένα σημεία ελέγχου, την απόσταση που διανύθηκε, τον αριθμό των διαδρομών που πραγματοποιήθηκαν από ένα συγκεκριμένο όχημα, κ.λπ.. Αυτό βοηθάει στη μείωση του κόστους μεταφοράς με ταυτόχρονη εξοικονόμηση χρόνου.
- **Carrier Onboarding** - Με τη χρήση τεχνολογίας blockchain, είναι εύκολο να επαληθευθούν όλα τα στοιχεία των επιβατών του οχήματος αλλά και της συμπεριφοράς του προσωπικού. Αυτό βοηθά στην αποφυγή των κακών οδηγών και διασφάλιση της φήμης της επιχείρησης.

10.4.4. Blockchain και η αγορά ακινήτων

Η τεχνολογία blockchain είναι βέβαιο ότι θα αλλάξει την αγορά ακινήτων (Deloitte Financial Services, 2018). Τα βασικά προβλήματα που αντιμετωπίζουν οι επαγγελματίες της αγοράς ακινήτων αλλά και οι πελάτες τους είναι οι ακόλουθες:

- Δύσκολη διαδικασία αναζήτησης ακινήτων λόγω της ύπαρξης πολλών και διαφορετικών καταλόγων με δεδομένα καταχωρήσεων.
- Χρονοβόρες και βασικά χειροκίνητες διαδικασίες επιμέλειας και συντήρησης ακινήτων
- Πολυπλοκότητα στη διαχείριση των μισθώσεων, των συμφωνιών και των αντίστοιχων ταμειακών ροών
- Έλλειψη πολυμεσικών δεδομένων που επηρεάζει την ικανότητα λήψης αποφάσεων της διοίκησης

Η εφαρμογή της τεχνολογίας blockchain είναι βέβαιο ότι θα επιλύσει τα παραπάνω προβλήματα. Για παράδειγμα, ένα σύστημα αναζήτησης ακινήτων βασισμένο σε blockchain, θα επέτρεπε τη διανομή των δεδομένων σε ένα δίκτυο peer-to-peer με τρόπο που να επιτρέπει στους μεσίτες, να έχουν περισσότερο έλεγχο

των δεδομένων τους, μαζί με αυξημένη εμπιστοσύνη, καθώς οι καταχωρήσεις των ακινήτων θα ήταν ελεύθερα προσπελάσιμες. Επιπλέον θα εξασφαλιζόταν άμεση πρόσβαση στους τίτλους ιδιοκτησίας, στο ιστορικό της ιδιοκτησίας, σε συγκρίσιμες τιμές μίσθωσης, κ.λπ.

Βιβλιογραφία/Αναφορές

Πιντέλας, Π. & Αλεφραγκής, Π. (2003). Μεταγλωττιστές. Ελληνικό Ανοικτό Πανεπιστήμιο, 2003. [Online]. από: http://www.pli.eap.gr/pdf/PLH40/PLH40-1/pintellas2.pdf

Back, A. (2002). Hashcash-a denial of service counter-measure.

Bano, S., Sonnino, A., Al-Bassam, M., Azouvi, S., McCorry, P., Meiklejohn, S., & Danezis, G. (2017). Consensus in the age of blockchains. *arXiv preprint arXiv:1711.03936*.

Bambara, J. J., & Allen, P. R. (2018). Blockchain: A practical guide to developing business, law, and technology solutions. Bentov, I., Gabizon, A., & Mizrahi, A. (2016, February). Cryptocurrencies without proof of work. In *International Conference on Financial Cryptography and Data Security* (pp. 142-157). Springer, Berlin, Heidelberg.

Buterin, V. (2013). Bitcoin network shaken by blockchain fork. The Bitcoin Magazine.

Buterin, V. (2014). A next-generation smart contract and decentralized application platform. *white paper*.

Čolaković, A., & Hadžialić, M. (2018). Internet of Things (IoT): A Review of Enabling Technologies, Challenges, and Open Research Issues. *Computer Networks*.

Conti, M., Kumar, S., Lal, C., & Ruj, S. (2018). A survey on security and privacy issues of bitcoin. *IEEE Communications Surveys & Tutorials*.

Deloite Financial Services. (2018). Blockchain in commercial real estate: The future is here. Ανακτήθηκε 17/06/2017 από https://www2.deloitte.com/us/en/pages/financial-services/articles/blockchain-in-commercial-real-estate.html

Douceur, J. R. (2002, March). The sybil attack. In *International workshop on peer-to-peer systems* (pp. 251-260). Springer, Berlin, Heidelberg.

Hirai, Y. (2017, April). Defining the ethereum virtual machine for interactive theorem provers. In *International Conference on Financial Cryptography and Data Security* (pp. 520-535). Springer, Cham.

Gilbert, H., & Handschuh, H. (2003, August). Security analysis of SHA-256 and sisters. In International workshop on selected areas in cryptography (pp. 175-193). Springer, Berlin, Heidelberg.Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, *82*, 395-411.

Kahri, F., Bouallegue, B., Machhout, M., & Tourki, R. (2013, March). An FPGA implementation of the SHA-3: The BLAKE hash function. In Systems, Signals & Devices (SSD), 2013 10th International Multi-Conference on (pp. 1-5). IEEE.

King, S. (2013). Primecoin: Cryptocurrency with prime number proof-of-work. *July 7th*.

Monar, D., Juels, A., & Wagner, D. (2005). *Security and privacy issues in e-passports*. Cryptology ePrint Archive, Report 2005/095.

Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine generals problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, *4*(3), 382-401.

Penard, W., & van Werkhoven, T. (2008). On the secure hash algorithm family. *Cryptography in Context*, 1-18.

Szabo, Nick, "Formalizing and Securing Relationships on Public Networks". Vol. 2, no. 9. 1 September 1997.

Ανακτήθηκε 20/06/2018 από στο: http://firstmonday.org/article/view/548/469.

Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, *151*, 1-32.

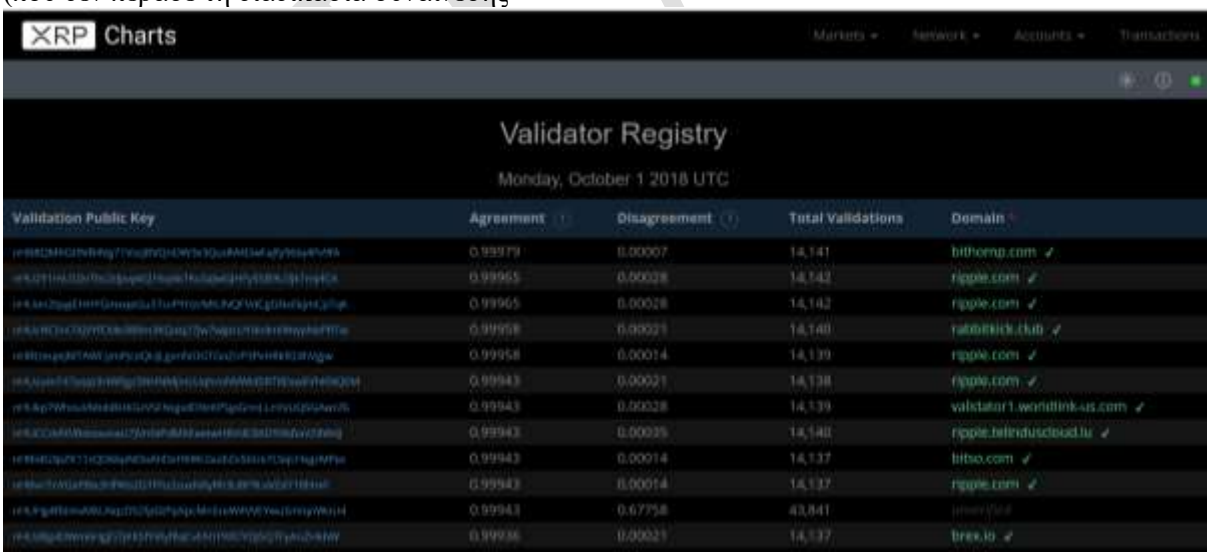
Ερωτήσεις ανακεφαλαίωσης, συζήτησης και αναζήτησης

Ερώτηση 1

Μελετήστε την πλατφόρμα blockchain https://www.r3.com και να αναφέρετε τις διαφορές που έχει ένα blockchain κοινοπραξίας από ένα δημόσιο blockchain.

Απάντηση/Λύση

Η διάκριση μεταξύ δημοσίων, κοινοπραξιών και ιδιωτικών blockchains είναι σημαντική. Ακόμη και για όσους προτιμούν ένα παραδοσιακό συγκεντρωτικό σύστημα, η προσθήκη των κρυπτογραφικών δυνατοτήτων που υπόσχεται η τεχνολογία blockchain είναι σημαντική για την ασφάλεια αλλά και τις ελεγκτικές ικανότητες (auditability) που μας δίνει. Σε σύγκριση με τα δημόσια blockchains, τόσο τα ιδιωτικά όσο και τα blockchains κοινοπραξιών έχουν πολλά πλεονεκτήματα. Ο ιδιωτικός χειριστής τέτοιων blockchains έχει τη δυνατότητα να αλλάξει τους κανόνες ενός blockchain (π.χ. version block) αλλά και να ακυρώσει τυχόν λανθασμένες συναλλαγές. Στην περίπτωση που πρόκειται για ένα blockchain μεταξύ των οικονομικών εταίρων, η δυνατότητα ακύρωσης λανθασμένων συναλλαγών είναι ιδιαίτερα σημαντική, αφού απαιτείται για την διόρθωση των ανθρώπινων σφαλμάτων τα οποία είναι αναπόφευκτα αλλά και για την προστασία από κακόβουλους χρήστες που επιβουλεύονται οικονομικούς πόρους ή άλλα περιουσιακά στοιχεία άλλων χρηστών.
Επίσης σε ένα ιδιωτικό blockchain, οι συναλλαγές είναι λιγότερο δαπανηρές, αφού χρειάζεται να επαληθευτούν μόνο από μερικούς έμπιστους κόμβους που έχουν πολύ υψηλή ισχύ επεξεργασίας και όχι από όλο το peer-to-peer δίκτυο.
Για παράδειγμα ένα δίκτυο κοινοπραξιών είναι το δίκτυο συναλλαγών Ripple (RTXP) (https://ripple.com/), το οποίο δημιουργήθηκε το 2012. Το κρυπτονόμισμα που υποστηρίζεται είναι το XRP ενώ επιτρέπονται άμεσες, ασφαλείς και σχεδόν δωρεάν οικονομικές συναλλαγές σε παγκόσμιο επίπεδο. Το Ripple είναι το τρίτο πιο δημοφιλές δίκτυο μετά το bitcoin και το Ethereum. Το δίκτυο Ripple μπορεί να θεωρηθεί δίκτυο κοινοπραξιών διότι οι συναλλαγές επικυρώνονται από ένα πεπερασμένο σύνολο κόμβων, τους επικυρωτές (validators) και όχι από όλους τους κόμβους. Στην εικόνα 10.19 παρουσιάζεται η λίστα των επικυρωτών του δικτύου, μαζί με τον αριθμό των συναλλαγών που επικύρωση ο κάθε κόσμος, το ποσοστό συμφωνίας και το ποσοστό διαφωνιών (που δεν πέρασε τη διαδικασία συναίνεσης



Εικόνα 10.19 *Η λίστα των επικυρωτών στο δίκτυο Ripple*

Έχοντας υπόψη τα παραπάνω δεδομένα φαίνεται ότι τα ιδιωτικά blockchains είναι αναμφισβήτητα μια καλύτερη επιλογή για τα οργανισμούς και επιχειρήσεις. Παρόλα αυτά τα δημόσια blockchains έχουν σημαντικά πλεονεκτήματα. Τα βασικά πλεονεκτήματα των δημόσιων blockchains είναι:

- παρέχουν έναν τρόπο προστασίας των χρηστών μιας εφαρμογής από τους προγραμματιστές, αφού ακόμη και οι προγραμματιστές αυτών των συστημάτων δεν μπορούν τα τροποποιήσουν τις συναλλαγές,

- είναι ανοικτά και επομένως χρησιμοποιούνται από πολλές διαφορετικές επιχειρήσεις, από οργανισμούς αλλά και από απλούς χρήστες γεγονός που παρέχει δυνατότητα δικτύωσης και διαφορετικούς τρόπους χρήσης, και
- είναι αξιόπιστα και ανθεκτικά σε βλάβες αφού τα δίκτυα peer-to-peer δεν έχουν κεντρικούς κόμβους ελέγχου (no single point of failure).

Ερώτηση 2

Μελετήστε τους εξερευνητές blockchain για διάφορα blockchain δίκτυα. Για παράδειγμα βρείτε εξερευνητές για το δίκτυο Ethereum, Litecoin, κ.λπ. Παρατηρείστε τη δομή του block, το ρυθμό παραγωγής νέων block, τον αριθμό των συναλλαγών που περιέχουν κ.λπ.

Απάντηση/Λύση

Το Ethereum είναι ένα ψηφιακό νόμισμα αλλά και μια ανοικτού κώδικα πλατφόρμα blockchain με προγραμματιζόμενη λειτουργία συναλλαγών και δίνει τη δυνατότητα να αναπτύξουμε διαφορετικές, ανεξάρτητες εφαρμογές. Οι υπηρεσίες αυτές μπορεί να είναι διαφόρων ειδών:

- δημιουργία ενός νέου συστήματος ψηφιακών πληρωμών,
- ανάπτυξη καινούργιων κρυπτονομισμάτων και
- ανάπτυξη δικτυακών για αγοραπωλησίες σε κρυπτονομίσματα

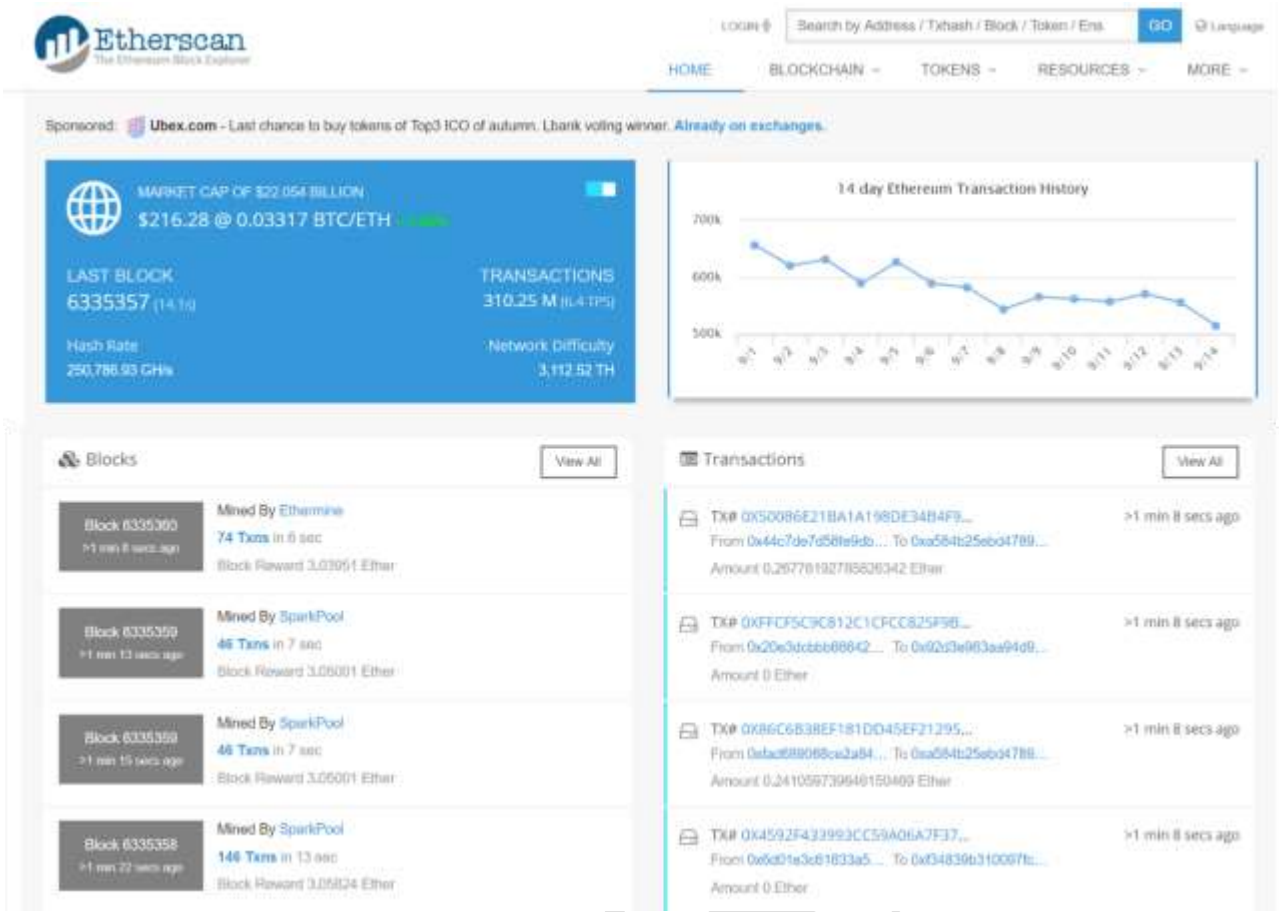
Στο δίκτυο του Ethereum, οι εφαρμογές λέγονται έξυπνα συμβόλαια (smart contracts) τα οποία προγραμματίζονται κυρίως με την γλώσσα προγραμματισμού Solidity. Για κάθε εφαρμογή, ο δημιουργός θα πρέπει να καταβάλλει ένα αντίτιμο στο νόμισμα του δικτύου, το Ether.

Ο εξερευνητής για το Ethereum βρίσκετε στη σελίδα https://etherscan.io/ (βλέπε Εικόνα 10.20). Με βάση τα στοιχεία που παρουσιάζονται στον εξερευνητή παρατηρούμε:

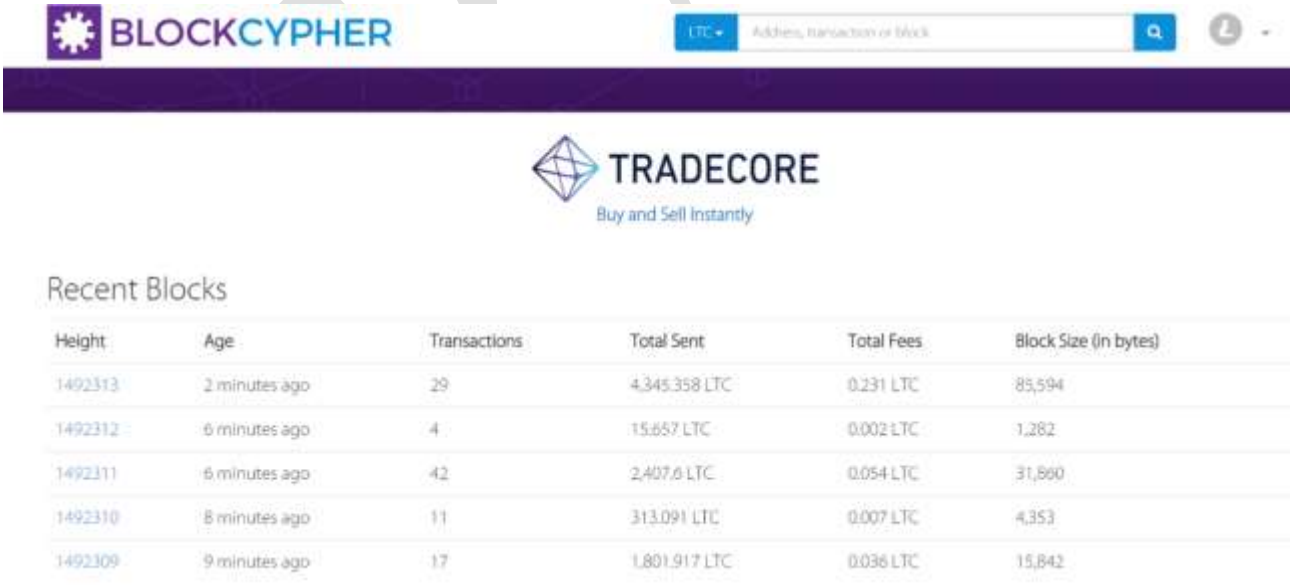
1) Τα block παράγονται πολύ γρηγορότερα από ότι τα bitcoins, σε δευτερόλεπτα. Στο δίκτυο bitcoin τα blocks παράγονται κάθε 10 λεπτά ενώ στο litecoin στο δείγμα που φαίνεται στην Εικόνα 10.21 κάθε 5 λεπτά, ενώ αν ανατρέξει κανείς στη βιβλιογραφία η τιμή στόχος είναι 2 λεπτά.
2) Τα block είναι μικρότερου μεγέθους, μερικά Kbytes.

Ο εξερευνητής για το litecoin βρίσκετε στη σελίδα https://live.blockcypher.com/ltc/.
Το Litecoin (LTC) είναι το δεύτερο πιο δημοφιλές κρυπτονόμισμα τόσο στις συναλλαγές όσο και στην εξόρυξη. Το Litecoin κάνει χρήση του αλγορίθμου κρυπτογράφησης Scrypt, σε αντίθεση με τον αλγόριθμο SHA-256 που χρησιμοποιεί το Bitcoin. Ένας από τους στόχους του Litecoin είναι να επιβεβαιώσει τις συναλλαγές με μεγαλύτερη ταχύτητα από ότι το δίκτυο Bitcoin, καθώς και να κάνει χρήση ενός αλγόριθμου που είναι ανθεκτικός σε επιταχυνόμενες τεχνολογίες εξόρυξης υλικού. Επίσης, το συνολικό ποσό των Litecoin που είναι διαθέσιμα για εξόρυξη και κυκλοφορία είναι τέσσερις φορές το ποσό του Bitcoin
Με βάση τον εξερευνητή παρατηρούμε:

3) Τα block παράγονται με μικρότερους ρυθμούς από ότι τα bitcoins. Στο δίκτυο bitcoin τα block παράγονται κάθε 10 λεπτά ενώ στο litecoin στο δείγμα που φαίνεται στην Εικόνα 10.21 κάθε 5 λεπτά.
4) Τα block είναι μικρότερου μεγέθους και με λιγότερες συναλλαγές που σημαίνει ότι χρειάζεται λιγότερος χρόνος για επαλήθευση



Εικόνα 10.20 *Ο εξερευνητής για το δίκτυο Ethereum*



Εικόνα 10.21 *Ο εξερευνητής για το δίκτυο Litecoin*

Ερώτηση 3

Επισκεφτείτε το δικτυακό τόπο https://anders.com/blockchain με σκοπό να κατανοήσετε καλύτερα τη δημιουργία των τιμών του κατακερματισμού, τη δημιουργία των block και τη δημιουργία του blockchain.

Απάντηση/Λύση

Έχουμε ήδη αναφέρει ότι στο δίκτυο Bitcoin χρησιμοποιείται η κρυπτογραφική συνάρτηση SHA-256 Hash. Ο SHA-2 (Secure Hash Algorithm 2) είναι ένα σύνολο κρυπτογραφικών συναρτήσεων κατακερματισμού που σχεδιάστηκαν από την Υπηρεσία Εθνικής Ασφάλειας των Ηνωμένων Πολιτειών (NSA) (Penard, 2008). Ο SHA-256 αλγόριθμος λαμβάνει ένα input κείμενο και παράγει ως output μια hash τιμή 256-bit (32 bytes).
Στο παρακάτω παράδειγμα για το input κείμενο "Αυτό είναι ένα παράδειγμα χρήσης της συνάρτησης SHA256" παράγεται η hash τιμή

```
f95598d174e530a9522089c5b572f03e0ac0595a9306ba918cee48294abb98bf
```

η οποία έχει μέγεθος 32 bytes (βλέπε Εικόνα 10.22) .

Εικόνα 10.22 *Παραγωγή hash με βάση τον αλγόριθμο SHA256 (πηγή https://anders.com/blockchain/hash.html)*

Η παραγωγή του hash του block γίνεται συνδυάζοντας όλα τα δεδομένα που παρουσιάζονται στην Εικόνα 10.25, δηλαδή τον αριθμό του block, το nonce και το κείμενο (data). Το **nonce** είναι ένας αυθαίρετος αριθμός που χρησιμοποιείται μόνο μία φορά σε κάθε κρυπτογραφική χρήση και είναι ένας τυχαίος ή ψευδοτυχαίος αριθμός. Ο λόγος χρήσης του nonce είναι η αποφυγή επιθέσεων επανάληψης (replay attacks). Μια επίθεση επανάληψης (γνωστή και ως επίθεση αναπαραγωγής) είναι μια μορφή επίθεσης δικτύου στην οποία μια έγκυρη διαβίβαση δεδομένων επαναλαμβάνεται ή καθυστερεί με κακόβουλο ή δόλιο τρόπο. Αυτό γίνεται είτε από τον εντολέα είτε από έναν αντίπαλο που συλλαμβάνει τα δεδομένα και τα μεταδίδει εκ νέου. Με τον τρόπο αυτό εξασφαλίζουμε ότι το hash θα είναι κάθε φορά διαφορετικό.

Στην Εικόνα 10.23 παρουσιάζεται ένα block που το hash έχει υπολογιστεί σωστά. Ένα σωστό hash ξεκινά με 4 μηδέν. Αντίστοιχα στη Εικόνα 10.24 παρουσιάζεται ένα λανθασμένο hash, διότι έχουμε χρησιμοποιήσει το ίδιο nonce με διαφορετικό κείμενο. Παρατηρήστε ότι η Εικόνα εμφανίζεται με ροζ χρώμα. Για να διορθώσουμε το hash θα πρέπει να εξορύξουμε (mine) καινούργιο nonce. Στην Εικόνα 10.25 παρουσιάζεται το νέο hash που παράγεται από το καινούργιο nonce.

Εικόνα 10.23 *Παραγωγή hash με block id, nonce και data (πηγή https://anders.com/blockchain/block.html)*

Εικόνα 10.24 *Λανθασμένη παραγωγή hash με ίδιο block id και nonce αλλά διαφορετικά data (πηγή https://anders.com/blockchain/block.html)*

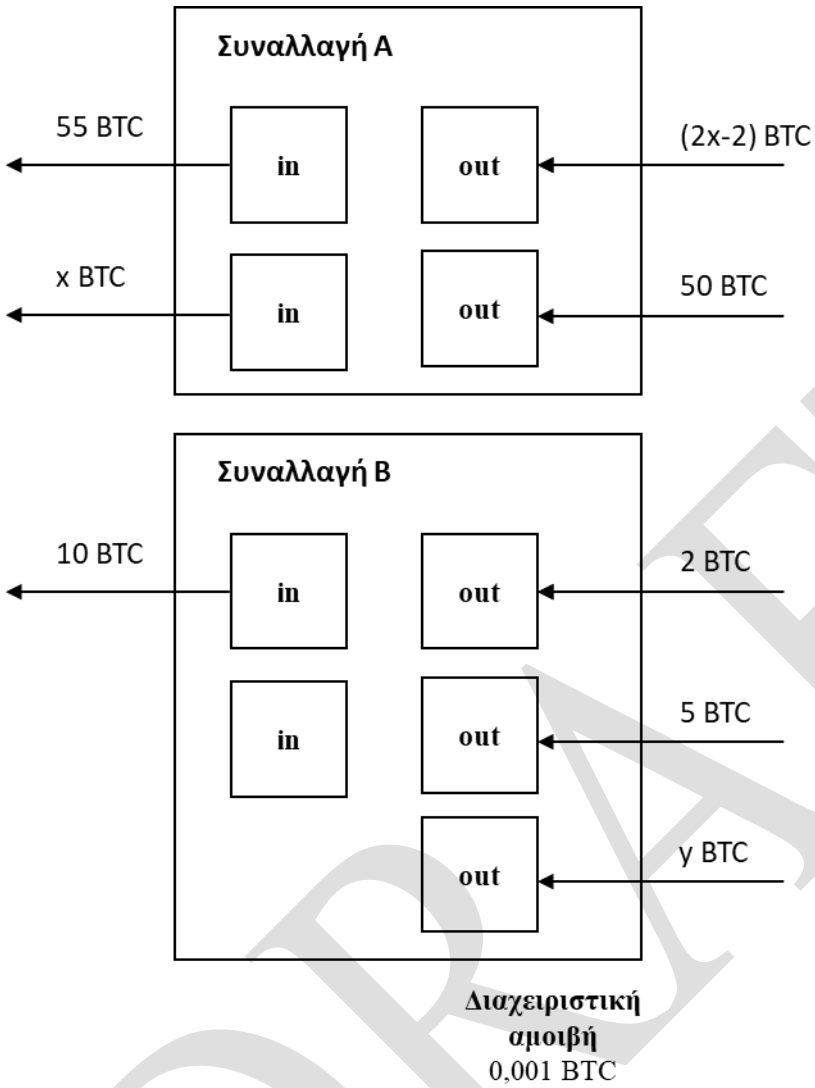
Εικόνα 10.25 *Σωστή παραγωγή hash με νέο nonce που έχουμε εξορύξει (πηγή https://anders.com/blockchain/block.html)*

Στη συνέχεια παρουσιάζουμε τη σύνδεση των block τα οποία περιέχουν συναλλαγές σε ένα blockchain (Εικόνα 10.26). Αν σε οποιαδήποτε από τα παρακάτω block αλλάξουμε την τιμή σε μια συναλλαγή, αμέσως το block γίνεται άκυρο, όπως και το hash.

Εικόνα 10.26 *Δημιουργία blockchain (πηγή https://anders.com/blockchain/tokens.html)*

Ερώτηση 4

Στην Εικόνα 10.27 υπολογίστε την τιμή των x και y.



Εικόνα 10.27 *Υπολογισμός τιμής bitecoin*

Απάντηση/Λύση

Η σωστή απάντηση του x μπορεί να προσδιοριστεί αν γνωρίζει κάποιος ότι σε μια συναλλαγή θα πρέπει τα input coins ισούνται με τα output coins.

Δηλαδή

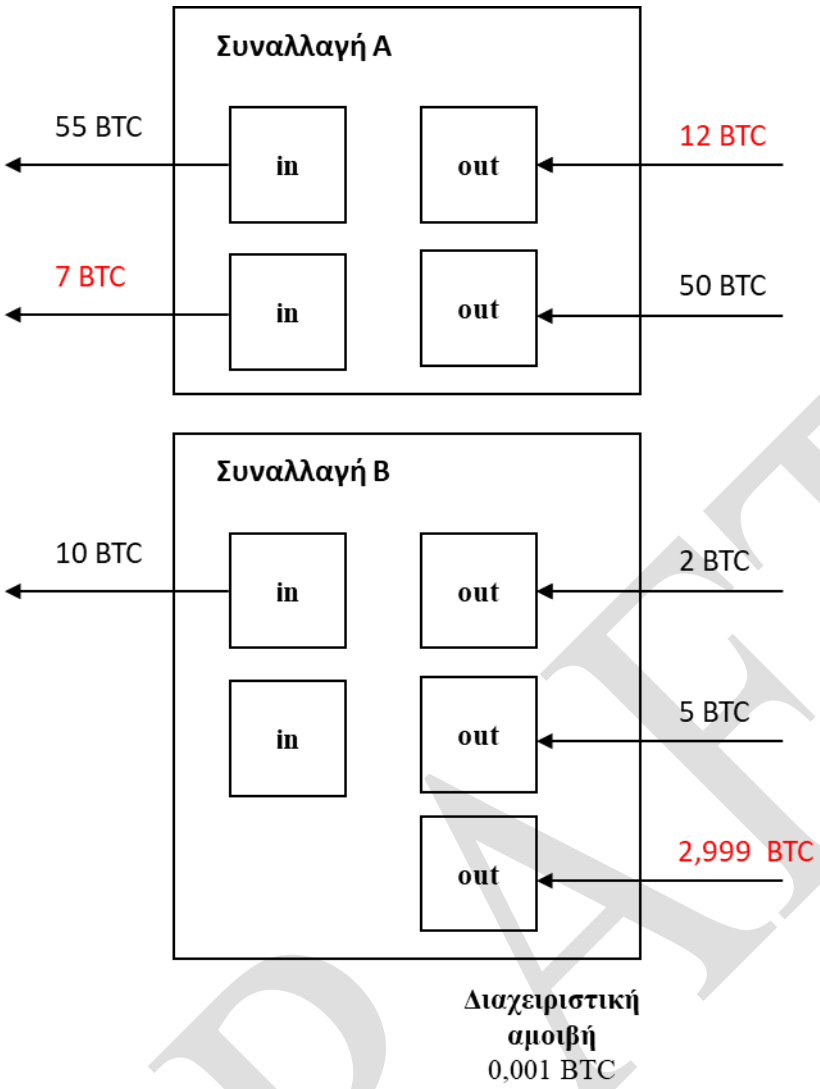
55 + x = 2x-2 +50 => 2x –x = 55+2-50 => x = 7 BTC

Αντίστοιχα και για το y. Εδώ όμως θα πρέπει να λάβουμε υπόψη και τη διαχειριστική αμοιβή.

Δηλαδή

10 = 2 + 5 + 0,001 + y => y = 2,999 BTC

Ο υπολογισμός παρουσιάζεται στην Εικόνα 10.28.



Εικόνα 10.28 *Υπολογισμός τιμής bitecoin – λύση*

Ερώτηση 5

Με τη χρήση του διαδικτύου βρείτε επιχειρήσεις στον κλάδο των μεταφορών που χρησιμοποιούν την τεχνολογία blockchain. Κάντε μια σύντομη παρουσίαση του επιχειρηματικού μοντέλου που χρησιμοποιείται.

Απάντηση/Λύση

Η IBM και η δανέζικη εταιρία μεταφορών και logistics Maersk εγκαινίασαν πρόσφατα ένα νέο δίκτυο blockchain που εστιάζεται σε διεθνείς μεταφορές εμπορευματοκιβωτίων. Το όνομα αυτής της παγκόσμιας πλατφόρμας εφοδιαστικής αλυσίδας ονομάζεται TradeLens (https://www.tradelens.com/) και έχει ως στόχο να παρακολουθεί και να καταγράφει τα δεδομένα για κάθε αποστολή αγαθών με εμπορευματοκιβώτια σε μια αλυσίδα εφοδιασμού σε πραγματικό χρόνο.

Στους συμμετέχοντες στο δίκτυο TradeLens περιλαμβάνονται σήμερα πάνω από 20 φορείς εκμετάλλευσης λιμενικών και τερματικών σταθμών σε όλο τον κόσμο, καθώς και διεθνείς τελωνειακές αρχές, μεταφορείς εμπορευμάτων, επιχειρήσεις εφοδιαστικής καθώς και ιδιοκτήτες φορτίων.

Αξίζει να αναφερθεί ότι οι συμμετέχοντες στην TradeLens, διεθνείς μεταφορείς εμπορευματοκιβωτίων Hamburg Süd και Pacific International Lines, μαζί με τη εταιρεία Maersk αντιπροσωπεύουν πάνω από το 20%

του παγκόσμιου μεριδίου αγοράς στην εφοδιαστική αλυσίδα και εξυπηρετούν 235 θαλάσσιες πύλες σε όλο τον κόσμο.

Ας δούμε ορισμένα χαρακτηριστικά του δικτύου Blockhain TradeLens

Κάθε συμμετέχων στο οικοσύστημα της εφοδιαστικής αλυσίδας μπορεί να δει τις κινήσεις των αγαθών μέσα στην αλυσίδας εφοδιασμού, γνωρίζοντας το πού βρίσκεται ένα εμπορευματοκιβώτιο. Μπορούν επίσης να δουν την κατάσταση των τελωνειακών εγγράφων ή να δουν φορτωτικές και άλλα δεδομένα.

- Η λεπτομερής προβολή της προόδου της μεταφοράς του εμπορευματοκιβωτίου ενισχύεται από την ανταλλαγή σε πραγματικό χρόνο των δεδομένων και εγγράφων της μεταφοράς.
- Κανείς δεν μπορεί να τροποποιήσει, να διαγράψει ή ακόμα και να προσθέσει οποιαδήποτε εγγραφή χωρίς τη συναίνεση των άλλων συμμετεχόντων στο δίκτυο.
- Αυτό το επίπεδο διαφάνειας συμβάλλει στη μείωση των σφαλμάτων και των περιστατικών κλοπής ή άλλης απάτης, συμβάλλει στη μείωση του χρόνου που περνούν τα προϊόντα στη διαδικασία διαμετακόμισης και αποστολής, στη βελτίωση της διαχείρισης αποθεμάτων και στην τελική μείωση των αποβλήτων και του κόστους.
- Το δίκτυο επιτρέπει την ανταλλαγή αρχικών δεδομένων και εγγράφων της αλυσίδας εφοδιασμού σε πραγματικό χρόνο μέσω μιας ψηφιακής υποδομής ή ενός αγωγού δεδομένων που συνδέει τους συμμετέχοντες σε ένα οικοσύστημα αλυσίδας εφοδιασμού.