ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΤΜΗΜΑΤΟΣ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΜΕΛΕΤΗ ΤΕΧΝΟΛΟΓΙΩΝ ΓΙΑ ΣΥΝΑΛΛΑΓΕΣ ΜΕ ΨΗΦΙΑΚΑ ΝΟΜΙΣΜΑΤΑ

Διπλωματική Εργασία

του

Αναστάσιου Λαμπριανίδη

Θεσσαλονίκη, Νοέμβριος 2020

ΜΕΛΕΤΗ ΤΕΧΝΟΛΟΓΙΩΝ ΓΙΑ ΣΥΝΑΛΛΑΓΕΣ ΜΕ ΨΗΦΙΑΚΑ ΝΟΜΙΣΜΑΤΑ

Αναστάσιος Λαμπριανίδης

Πτυχίο Οικονομικών Επιστημών, ΑΠΘ, 2018

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΗΝ ΕΦΑΡΜΟΣΜΕΝΗ ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέπων Καθηγητής
Παναγιώτης Παπαδημητρίου

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 04/11/2020

Παπαδημητρίου Παναγιώτης	Μαυρίδης Ιωάννης	Κολωνιάρη Γεωργία
.....	.....	.....

Αναστάσιος Λαμπριανίδης

....

Περίληψη

Η τεχνολογία blockchain ξεκίνησε ως η καινοτομία που τροφοδότησε το bitcoin. Ωστόσο, τα τελευταία χρόνια, η τεχνολογία αυτή άρχισε να εντάσσεται και σε άλλους τομείς, όπως στον τομέας της υγείας, στα χρηματοοικονομικά, στην εφοδιαστική αλυσίδα. Αναζητούν συνεχώς νέες τεχνολογίες ώστε να αντικαταστήσουν το σύστημα τους που συχνά είναι αναποτελεσματικό και δαπανηρό για να λειτουργήσει. Το δημόσιο blockchain, όπου ο καθένας μπορεί να συμμετέχει μπορεί να επεξεργαστεί μερικές συναλλαγές το δευτερόλεπτο. Το blockchain το οποίο χρειάζεται άδεια για να συμμετέχει κάποιος αποτελεί τον δεύτερο τύπο blockchain, όπου μόνο ένα περιορισμένο σύνολο χρηστών μπορεί να αποφασίζει για το τι θα μπαίνει στην αλυσίδα.

Σε αυτή την εργασία, αναλύουμε την τεχνολογία blockchain, για το πως λειτουργεί, τον τρόπο λειτουργίας των μηχανισμών του, για το πως γίνεται η διαδικασία τη εξόρυξης (mining), τα οφέλη και τα μειονεκτήματα του blockchain. Γίνεται αναφορά στην υποδομή του Hyperledger Fabric που επιτρέπει την δημιουργία ενός δικτύου blockchain. Ακόμη γίνεται αναφορά στην εγκατάσταση του Hyperledger Caliper που αποτελεί το εργαλείο για την μέτρηση της αποδοτικότητας του δικτύου.

Λέξεις Κλειδιά: Ψηφιακά νομίσματα, Blockchain, Bitcoin, Εξόρυξη, Hyperledger

Abstract

Blockchain technology started as the innovation that fueled bitcoin. In recent years, however, this technology has begun to integrate into other sectors, such as health, finance, and the supply chain. They are constantly looking for new technologies to replace their system which is often inefficient and costly to operate. The public blockchain, where anyone can participate can process a few transactions per second. The blockchain that requires a license to participate is the second type of blockchain, where only a limited set of users can decide who want to join the chain.

In this thesis, we analyze blockchain technology, how it works, how its mechanisms work, how the mining process is done, the advantages and disadvantages of blockchain. Reference is made to the Hyperledger Fabric infrastructure that allows the creation of a blockchain network. Reference is also made to the installation of the Hyperledger Caliper which is the tool for measuring the efficiency of the network.

Keywords: Digital currencies, Blockchain, Bitcoin, Mining, Hyperledger

Περιεχόμενα

Κατάλογος Εικόνων

1 Εισαγωγή

1.1 Πρόβλημα – Σημαντικότητα του θέματος

Η τεχνολογία Blockchain δεν ήταν τόσο διαδεδομένη έως το 2008, από τη στιγμή που ο Satoshi Nakamoto δημιούργησε το Bitcoin, από τότε και μετά οι άνθρωποι άρχισαν να ασχολούνται με το Bitcoin αλλά και να ψάχνουν την τεχνολογία στην οποία βασίστηκε αυτό το κρυπτονόμισμα. Στην παρούσα εργασία γίνεται αναφορά σχετικά με τον τρόπο λειτουργίας αυτής της τεχνολογίας αλλά και τους μηχανισμούς που χρησιμοποιεί που την κάνουν να ξεχωρίζει, αλλά και στα μειονεκτήματα. Γίνεται αναφορά, της χρήσης της τεχνολογίας και άλλους κλάδους. Ακόμη, γίνεται αναφορά του Hyperledger Fabric που αποτελεί μια υποδομή blockchain που θα χρησιμοποιηθεί και παρακάτω. Τέλος, γίνεται αναφορά και σε μερικά άλλα κρυπτονομίσματα αλλά και τον τρόπο με τον οποίο γίνεται η εξόρυξη Bitcoin.

Η τεχνολογία blockchain μπορεί να είναι κάτι καινούργιο σε εφαρμογή, αλλά η αναφορά της έχει γίνει από πιο πριν. Πιο συγκεκριμένα, το 1982 ο κρυπτογράφος David Chaum, πρότεινε για πρώτη φορά ένα πρωτόκολλο που μοιάζει με το blockchain, στη διατριβή του «Συστήματα υπολογιστών που καθιερώθηκαν, διατηρήθηκαν από αμοιβαία ύποπτες ομάδες». [1] Περαιτέρω εργασία για μια πιο κρυπτογραφικά ασφαλισμένη αλυσίδα μπλοκ αναλύθηκε το 1991 από τους Stuart Haber και W. Scott Stornetta, όπου ήθελαν να εφαρμόσουν ένα σύστημα στο οποίο δεν μπορούσαν να παραβιαστούν οι χρονικές εγγραφές. [2]

Αυτό που την κάνει να ξεχωρίζει, είναι κυρίως η ακεραιότητα των δεδομένων που διασφαλίζει αυτή η τεχνολογία αλλά και το ότι δεν ελέγχεται από καμία κυβέρνηση (αποκεντροποίηση), αφού ζούμε σε μια περίοδο όπου ο κυβερνητικός έλεγχος βρίσκεται σχεδόν παντού. Ακόμη, η ανωνυμότητα, που προσφέρει το Bitcoin στο διαδίκτυο μπορεί να θεωρηθεί σαν μία επανάσταση.

Όπως είναι γνωστό, η τεχνολογία blockchain έγινε γνωστή στο κόσμο με την εισαγωγή του bitcoin στην αγορά. Η εφαρμογή της δεν σταματάει μόνο στο bitcoin. Η τεχνολογία της μπορεί να εφαρμοστεί και σε άλλους κλάδους. Εκτός από ένα σύστημα πληρωμών, χωρίς την παρουσία διαμεσολαβητών, η τεχνολογία αυτή μπορεί να εφαρμοστεί και σε άλλους τομείς του χρηματοπιστωτικού τομέα. Για παράδειγμα, ο παραδοσιακός τρόπος επεξεργασίας και εκκαθάρισης συναλλαγών, εκτός από δαπανηρός, είναι και περίπλοκος, συνεπώς είναι αργός, ταυτόχρονα συμμετέχουν και περισσότερα μέλη, όπου ο κάθε ένας συντηρεί το δικό του αρχείο, με αποτέλεσμα να δημιουργούνται ζητήματα πρακτικότητας αλλά και να αυξάνει τις πιθανότητες σφαλμάτων. Η τεχνολογία blockchain απλοποιεί σημαντικά την διαδικασία και καθιστά περιττή την ανάγκη ύπαρξης ενδιάμεσων προσώπων. Ο χρόνος επιβεβαίωσης και εκκαθάρισης συναλλαγών μειώνεται δραματικά, ανεξάρτητα μάλιστα από την γεωγραφική θέση των συναλλασσόμενων. Πλέον, διεθνή χρηματοπιστωτικά ιδρύματα δοκιμάζουν την τεχνολογία αυτή προκειμένου να εκμεταλλευτούν τις δυνατότητες της σε όλο το φάσμα των υπηρεσιών που παρέχουν.

Στη σημερινή εποχή, όπου κάθε σπίτι διαθέτει τουλάχιστον 5 συσκευές που συνδέονται το διαδίκτυο (IoT), από το πλυντήριο του νοικοκυριού έως και την τηλεόραση, δημιουργείται το θέμα της ασφάλειας των δεδομένων, λόγο του ότι αυτές οι συσκευές επικοινωνούν μεταξύ τους αλλά και με τον κάτοχο τους, αποστέλλοντας και λαμβάνοντας δεδομένα. Η κρυπτογράφηση των δεδομένων των εν λόγω συσκευών σε βάση δεδομένων blockchain παρέχει υψηλότερο επίπεδο προστασίας και μετάδοσης των πληροφοριών. Ο αμετάβλητος χαρακτήρας της τεχνολογίας blockchain την καθιστά κατάλληλη για σκοπούς όπως η παρακολούθηση των προϊόντων όπως αλλάζουν κατοχή στην εφοδιαστική αλυσίδα. Καταχωρήσεις στην βάση του blockchain μπορούν να χρησιμοποιηθούν για τη δρομολόγηση γεγονότων στην αλυσίδα προμήθειας (όπως π.χ. η κατανομή των προϊόντων όπως φτάνουν σε ένα λιμάνι στα διαφορετικά containers). Η τεχνολογία blockchain προσφέρει ένα νέο δυναμικό τρόπο για την οργάνωση και παρακολούθηση δεδομένων και προϊόντων. Επιπλέον, αισθητήρες που τίθενται επί των προϊόντων παρέχουν πλήρη διαφάνεια και ακριβή γνώση της διαδικασίας προμήθειας προϊόντων καθώς παρέχουν δεδομένα σε πραγματικό χρόνο για την τοποθεσία και την κατάστασή τους, καθώς μεταφέρονται στην παγκόσμια αγορά. Η τεχνολογία blockchain θα αποθηκεύει, διαχειρίζεται, προστατεύει και μεταφέρει τις έξυπνες αυτές πληροφορίες με τον βέλτιστο τρόπο, παρέχοντας διαφάνεια σε πραγματικό χρόνο καθώς όλοι οι συμμετέχοντες (υπολογιστές) θα τηρούν και από ένα πλήρως ενημερωμένο αρχείο αυτών των δεδομένων.

1.2 Στόχοι – Συνεισφορά

Σκοπός της παρούσας εργασίας είναι, να δώσει την έννοια του blockchain, για το πως λειτουργεί, ποια είναι τα βασικά συστατικά αυτής της τεχνολογίας αλλά και για το πως δουλεύει το κάθε ένα. Ακόμη, αναφέρονται τα πλεονεκτήματα και τα μειονεκτήματα του blockchain, ώστε να δούμε τα οφέλη αυτής της τεχνολογίας αλλά και τους κινδύνους που έχει. Γίνεται μια ιστορική αναδρομή του χρήματος, μέχρι το ψηφιακό χρήμα, και δίνονται παραδείγματα μεγάλων και εναλλακτικών νομισμάτων. Με την εργασία, θέλουμε να γίνει η κατανόηση για τις βασικές έννοιες του Bitcoin, για την ασφάλεια του ηλεκτρονικού πορτοφολιού (e-Wallet), δηλαδή για το μέσο που χρησιμοποιείται για την αποθήκευση των μονάδων Bitcoin, για την ασφάλεια αυτού του πορτοφολιού αλλά και τρόπους διαχείρισης του κλειδιού, που αποτελεί την κύρια πρόσβαση του περιεχομένου. Ακόμη, δίνεται εξήγηση για το πως δημιουργείται το Bitcoin Address από το ιδιωτικό κλειδί. Ένας ακόμη στόχος είναι, να γίνουν κατανοητά τα μέσα που χρησιμοποιούνται για την εξόρυξη από την αρχή μέχρι το τέλος, δηλαδή στην αρχή που γινόταν η εξόρυξη τα μαθηματικά προβλήματα ήταν πιο εύκολα, και στη συνέχεια με την πάροδο του χρόνου και τη δημιουργία νέων μπλοκ, τα προβλήματα γίνονταν πιο δύσκολα, και οι απαιτήσεις των εργαλείων (hardware) γινόταν πιο αποδοτική, αλλά και οι εναλλακτικοί τρόποι που χρησιμοποιούνται για την εξόρυξη (cloud & pool mining).Τέλος, με την παρούσα εργασία, θέλουμε να γίνει κατανοητό ο τρόπος με τον οποίο δουλεύει το Hyperledger Fabric, που αποτελεί το εργαλείο για τη δημιουργία blockchain δηλαδή τα βασικά χαρακτηριστικά σχεδίασης του Fabric αλλά και της βάσης, η διαδικασία με την οποία εκτελείται μια συναλλαγή μεταξύ δύο μελών, τα βήματα που απαιτούνται για την ανάπτυξη ενός δικτύου, και μια εξήγηση και ένα παράδειγμα του εργαλείου αξιολόγησης του Hyperledger, το Caliper.

1.3 Διάρθρωση της διπλωματικής

Στο Κεφάλαιο 2 γίνεται αναφορά για το τι είναι το blockchain, αλλά και ο τρόπος με τον οποίο λειτουργεί. Αναφέρεται, επίσης και ο τρόπος με τον οποίο λειτουργούν το PoW (Proof of Work) και το SHA-256, αλλά και το τι είναι. Ακόμη, αναφέρονται τα οφέλη του blockchain που το κάνουν δελεαστικό στη χρήση για μια ασφαλή βάση δεδομένων, αλλά και τα μειονεκτήματα που δείχνουν τα ελαττώματα του. Γίνεται εξήγηση για το τι είναι το λογισμικό ανοικτού κώδικα, αλλά και μια μικρή ιστορική αναδρομή και περιγραφή για το hyperledger fabric.

Στο Κεφάλαιο 3, γίνεται αναφορά για το τι είναι το ψηφιακό νόμισμα, αλλά και μια ιστορική αναδρομή του χρήματος από την αρχή μέχρι τώρα, ακόμη γίνεται αναφορά για το ποια είναι τα μεγαλύτερα κρυπτονομίσματα σύμφωνα με την κεφαλαιαγορά (διαθέσιμες μονάδες * παρούσα τιμή). Τέλος, αναφέρονται τα εναλλακτικά κρυπτονομίσματα που αποτελούν αποτέλεσμα από τον αρχικό κώδικα του Bitcoin, αφού το bitcoin είναι λογισμικό ανοικτού κώδικά.

Στο Κεφάλαιο 4, γίνεται αναφορά στις βασικές έννοιες του Bitcoin, δηλαδή, τι είναι το ηλεκτρονικό πορτοφόλι, που χρησιμοποιείται για την αποθήκευση των μονάδων bitcoin, όπως γίνεται και η χρήση του πορτοφολιού που χρησιμοποιούμαι στην καθημερινότητά μας. Κάθε ψηφιακό πορτοφόλι διατρέχει κινδύνους από κακόβουλους χρήστες. Κάθε ηλεκτρονικό πορτοφόλι χρησιμοποιεί ένα κλειδί, το οποίο μας δίνει την πρόσβαση σε αυτό, στο κεφάλαιο 4, αναφέρονται τρόποι για την ασφαλή αποθήκευση του κλειδιού. Ακόμη, δίνεται η περιγραφή για το πως δημιουργείται το bitcoin address. Τέλος, γίνεται αναφορά στους τρόπους με τους οποίους γίνεται η εξόρυξη (mining), αλλά και τα μέσα που χρησιμοποιούνται για την καλύτερη δυνατή αποδοτικότητα αλλά και παραγωγικότητα.

Στο κεφάλαιο 5, γίνεται μια εισαγωγή για το πως λειτουργεί το blockchain, αναφέρονται μερικά από τα βασικά χαρακτηριστικά του, γίνεται αναφορά για τις προϋποθέσεις που απαιτούνται για την για την επικύρωση μιας συναλλαγής αλλά και μια σύντομη περιγραφή για την λειτουργία κατακερματισμού (Hash Function). Τέλος, αναφέρονται τα βασικά εργαλεία που απαιτούνται για την δημιουργία ενός λειτουργικού δικτύου συναλλαγών με το εργαλείο του Hyperledger το Fabric, αλλά και μια σύντομη περιγραφή αυτών των εργαλείων και ένα δείγμα του κώδικα μερικών από αυτών που βρίσκεται στην Ενότητα Παράρτημα.

Στο κεφάλαιο 6, γίνεται αναφορά για τη λειτουργία του Hyperledger, πιο συγκεκριμένα, εξηγούνται οι έννοιες σχετικά με την Βυζαντινή Ανοχή Σφαλμάτων αλλά και για το Βυζαντινό Πρόβλημα των Στρατηγών. Ακόμη, γίνεται αναφορά για το μοντέλο του Hyperledger Fabric, που περιγράφει τα βασικά χαρακτηριστικά σχεδίασης του Fabric που το κάνουν ένα ολοκληρωμένο και προσαρμόσιμο blockchain. Περιγράφεται η διαδικασία με την οποία εκτελείται η ροή μιας συναλλαγής, από τον πελάτη που εκκινεί μια συναλλαγή μέχρι την εκτέλεση της συναλλαγής και την ενημέρωση της βάσης του blockchain, αλλά οι υπηρεσίες μου μεσολαβούν για την εκτέλεση της συναλλαγής, αλλά και τα βήματα που απαιτούνται για την ανάπτυξη ενός ολοκληρωμένου δικτύου. Τέλος, γίνεται μια αναφορά για το Caliper, που αποτελεί, ένα εργαλείο αξιολόγησης για ένα δίκτυο blockchain, και ένα παράδειγμα ενός μικρού δικτύου, που δείχνει μερικούς δείκτες αξιολόγησης αλλά και τους πόρους που καταναλώνουν οι peers.

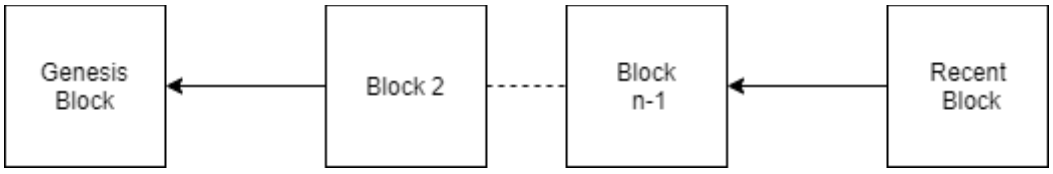
Στο κεφάλαιο 7, αναφέρονται τα συμπεράσματα της εργασίας, γίνεται αναφορά για τις μελλοντικές επεκτάσεις που μπορούν να πραγματοποιηθούν στο μέλλον ώστε να δούμε τις διαφορές που υπάρχουν στα αποτελέσματα όταν γίνεται η χρήση της τεχνολογίας με διαφορετικό υλικό (Κάρτα γραφικών, ολοκληρωμένα συστήματα εξόρυξης). Ακόμη, γίνεται αναφορά για τους τομείς στις οποίες έχει γίνει εισαγωγής της τεχνολογίας blockchain (κυβέρνηση, εφοδιαστικής αλυσίδα κλπ).

2 ΤΕΧΝΟΛΟΓΙΑ ΚΑΙ ΛΟΓΙΣΜΙΚΟ BLOCKCHAIN

2.1 Τι είναι το Blockchain

Το Blockchain είναι μια ακολουθία από μπλοκ, όπου το κάθε ένα περιέχει ένα πλήρες αρχείο συναλλαγών όπως ένα δημόσιο βιβλίο. Αυτό υποδεικνύει την σειρά με την οποία πραγματοποιήθηκαν οι συναλλαγές. Η Εικόνα 1 αντιπροσωπεύει ένα Blockchain, όπου το πιο πρόσφατο μπλοκ περιέχει πληροφορίες που υποδεικνύουν το προηγούμενο. Κάθε μπλοκ στην αλυσίδα επιβεβαιώνει την ακεραιότητα του προηγούμενου, μέχρι το πρώτο μπλοκ, που ονομάζεται Genesis Block. [3]

Κανένας δεν μπορεί να αλλοιώσει τις πληροφορίες που περιλαμβάνονται σε ένα μπλοκ. Για να γίνει αυτό, χρειάζεται μεγάλη υπολογιστική ισχύ, που το καθιστά αδύνατο.



Εικόνα 1 Blockchain

Το Blockchain είναι ένα αποκεντρωποιημένο δίκτυο P2P (Peer-to-Peer). Με την έννοια, ότι δεν υπάρχει καμία αρχή που να ελέγχει το δίκτυο, εκτός εάν το δίκτυο είναι ιδιωτικό τότε σε αυτή την περίπτωση υπάρχει έλεγχος από τον οργανισμό. Η έννοια P2P, αναφέρεται στο ότι κάθε μέλος έχει ένα αντίγραφο της αλυσίδας, γιατί η αρχή που ελέγχει την αλυσίδα είναι όλα τα μέλη που συμμετέχουν σε αυτή. Τα μέλη που συμμετέχουν είναι αυτοί που θα αποφασίζουν αν ένα μπλοκ είναι ορθό, και αν συμφωνούν οι περισσότεροι, τότε το συγκεκριμένο μπλοκ διανέμεται στους συμμετέχοντες, και το κάθε μέλος προσθέτει το συγκεκριμένο μπλοκ στην αλυσίδα.

Υπάρχουν δύο είδη Blockchain:
Και τα δύο, δημόσιο και ιδιωτικό Blockchain, είναι P2P δίκτυα, όπου ο κάθε συμμετέχοντας διατηρεί ένα αντίγραφο της αλυσίδας το οποίο αποθηκεύει τις ψηφιακές συναλλαγές. Αυτή η αλυσίδα μπορεί μόνο να ενημερωθεί. Οι συμμετέχοντες διατηρούν την αλυσίδα συγχρονισμένη μέσα από ένα πρωτόκολλο συναίνεσης. Με αυτό τον τρόπο εξασφαλίζεται η ακεραιότητα της αλυσίδας, ακόμη και αν υπάρχουν κακόβουλη συμμετέχοντες.

i) Δημόσιο Blockchain

Τα δημόσια Blockchain είναι ανοιχτά δίκτυα που επιτρέπουν σε οποιονδήποτε να συμμετέχει στο δίκτυο αρκεί να έχει πρόσβαση στο διαδίκτυο. Ένα τέτοιο δίκτυο εξαρτάται από τον αριθμό των συμμετεχόντων για την επιτυχία και την ασφάλεια του, ως εκ τούτου ενθαρρύνει τους υποψήφιους συμμετέχοντες μέσω ενός μηχανισμού παροχής κινήτρων. Το καλύτερο παράδειγμα δημόσιου Blockchain, είναι το Bitcoin, όπου αυτοί που συμμετέχουν στο δίκτυο ανταμείβονται με Bitcoin (BTC), αυτοί είναι οι λεγόμενοι miners.

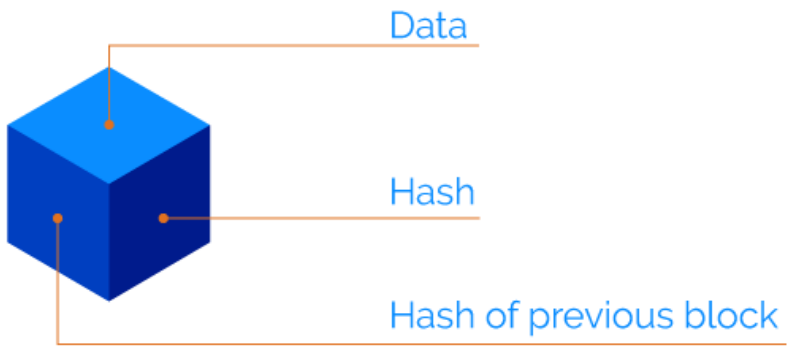
ii) Ιδιωτικά Blockchain

Τα ιδιωτικά Blockchain, είναι πιο μικρά σε μέγεθος και δεν έχουν πρόσβαση όλοι, αλλά χρειάζεται άδεια. Οι εταιρείες δημιουργούν ιδιωτικά Blockchain για την εξασφάλιση της ιδιωτικότητας αλλά και για την προστασία των δεδομένων. Πρόσβαση έχουν κυρίως οι χρήστες που τους παρέχεται άδεια από τον διαχειριστή του δικτύου ή από ένα σύνολο κανόνων που μπορούν να τεθούν σε εφαρμογή. Ένα τέτοιο δίκτυο μπορεί να χαρακτηριστεί και ως ένα επιτρεπόμενο δίκτυο. Τα ιδιωτικά Blockchain μπορούν να περιορίσουν την δραστηριότητα ορισμένων συμμετεχόντων, έτσι ώστε ορισμένες συναλλαγές να μπορούν να πραγματοποιηθούν ανάμεσα σε συγκεκριμένους συμμετέχοντες και όχι από όλους που συμμετέχουν στο δίκτυο. Αυτό, προσθέτει ακόμη ένα επίπεδο στην προστασία των προσωπικών δεδομένων.

2.2 Πως λειτουργεί

Όπως αναφέρθηκε και πάνω, το Blockchain είναι ένα αποκεντρωποιημένο δίκτυο, όπου οι συμμετέχοντες είναι απλοί χρήστες, που έχουν πρόσβαση στο διαδίκτυο. Εκτός, του ότι καμία τρίτη-εταιρεία δεν μπορεί να ελέγξει την λειτουργία του, η αλλοίωση των δεδομένων του είναι σχεδόν αδύνατη, γιατί χρειάζεται μεγάλη επεξεργαστική ισχύ για να πραγματοποιηθεί.

Κάθε Block, αποτελείται από 3 στοιχεία, **1) τα δεδομένα** που περιέχει το block, **2) ένα στοιχείο αναγνώρισης (Hash)** και **3) το στοιχείο αναγνώρισης του προηγούμενου block (Hash of previous block)**



Εικόνα 2 Μπλοκ **πηγή:** https://rubygarage.org/blog/how-blockchain-works

Τα δεδομένα που αποθηκεύονται σε ένα Block, εξαρτώνται από τον τύπο του Block. Για παράδειγμα, στο Blockchain του Bitcoin, το κάθε block, περιέχει τις λεπτομέρειες μιας συναλλαγής, όπου είναι ο αποστολέας, ο παραλήπτης και τις μονάδες Bitcoin. Ακόμη, περιέχει ένα στοιχείο αναγνώρισης, μοναδικό για κάθε block.

Το Blockchain χρησιμοποιεί ένα πρωτόκολλο Hashcash, το SHA-256 (PoW), για να αποφύγει κακόβουλες επιθέσεις, παράγοντας ένα στοιχείο αναγνώρισης για κάθε block, όπου είναι και

μοναδικό. Το SHA-256 αυτό που κάνει είναι, να μετατρέπει οποιοδήποτε εισροή σε ένα μήνυμα 256-bit. [3]

Για παράδειγμα το αλφαριθμητικό ¨UOM¨ = B89436BAC1ED915DA74ADB08B82D838F87A3EE67CD587DAB1C0353AC5D087B65.
Οποιαδήποτε μικρή αλλαγή πραγματοποιηθεί πάνω στο αλφαριθμητικό αυτό θα έχει ως συνέπεια να αλλάξει εντελώς το hash του συγκεκριμένου αλφαριθμητικού, ¨UOM1¨ = 3E1CBB5B3077C7F82C7871B00ADB16DF1D06F29D9E6564560992AECFDB704C96

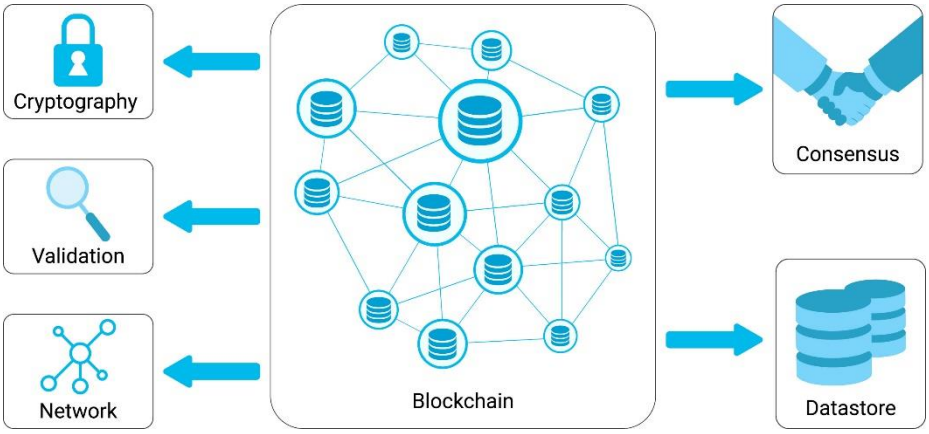
Για την παραγωγή, αυτού του hash, χρειάζεται μεγάλη επεξεργαστική ισχύ σε χρόνο που ισοδυναμεί περίπου με 10 λεπτά. Οποιαδήποτε αλλαγή, μέσα στο block θα αλλάξει και το hash του ίδιου του block, δηλαδή θα έχουμε ένα τελείως διαφορετικό block από αυτό που είχαμε στη αρχή. Και αφού κάθε block, περιέχει το hash του προηγούμενου block θα χρειαστεί να αλλάξει και το hash του προηγούμενου. Για να πραγματοποιηθεί η αλλαγή όλων των hash χρειάζεται μεγάλη επεξεργαστική ισχύ, που είναι σχεδόν αδύνατη να πραγματοποιηθεί.

Αν και υπάρχουν διάφορα είδη Blockchain, όλα χρησιμοποιούν μια κοινή λειτουργία που περιγράφεται στη συνέχεια. Για παράδειγμα, ο χρήστης Α θα πρέπει να μεταφέρει κάποιες μονάδες στον χρήστη Β για την απόκτηση ενός αντικειμένου. [4]

1. Ο Α μεταφέρει την συναλλαγή στο Blockchain, η οποία καταλήγει στο mempool, το οποίο είναι το «μέρος» όπου όλες οι συναλλαγές που πραγματοποιούνται στον κόσμο περιμένουν να συμπεριληφθούν σε ένα block.
2. Ένας κόμβος (ο Μ), που είναι υπεύθυνος για την παραγωγή blocks, συλλέγει την συναλλαγή της Α, μαζί με άλλες συναλλαγές ώστε να δημιουργήσει ένα καινούργιο block.
3. Αλλά προτού ο Μ καταφέρει να συμπεριλάβει το καινούργιο block στην αλυσίδα, θα πρέπει πρώτα να εκπληρώσει τις απαιτήσεις του αλγορίθμου συναίνεσης. Στη περίπτωση, του Bitcoin, θα πρέπει να εκτελέσει διάφορους υπολογισμούς.
4. Όταν οι απαιτήσεις εκπληρωθούν, μερικοί κόμβοι επαληθεύουν το αποτέλεσμα που έχει δοθεί από τον Μ. Αν η πλειοψηφία των κόμβων, δεχθούν το αποτέλεσμα, το καινούργιο block που έχει δημιουργηθεί από τον Μ, προστίθεται στην αλυσίδα, και ο Μ ανταμείβεται για την δουλειά που έκανε.
5. Από την στιγμή που το καινούργιο block, που περιέχει την συναλλαγή της Α προς τον Β, έχει γίνει αποδεκτό και περιλαμβάνεται στην αλυσίδα, η πληρωμή θεωρείται έγκυρη.
6. Ο Β πληρώθηκε για το αντικείμενο.

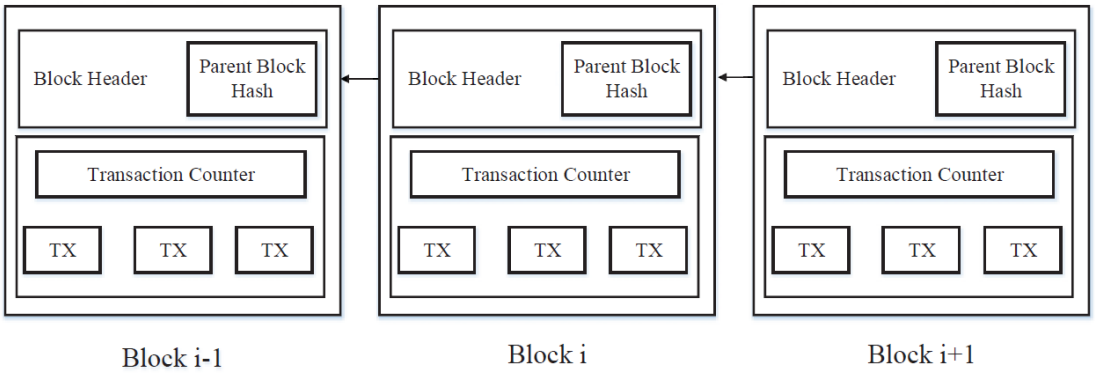
Στην παραπάνω περίπτωση, ο Μ είναι ο λεγόμενος miner. Και οι κόμβοι, είναι απλοί χρήστες που ελέγχουν αν το αποτέλεσμα του Μ είναι έγκυρο ώστε να διατηρηθεί η ακεραιότητα της αλυσίδας.

Στην περίπτωση του Bitcoin, ο Μ θα ανταμειβόταν με μονάδες Bitcoin αλλά και με μια μικρή προμήθεια που θα έχει βάλει η Α, ώστε να επικυρωθεί πιο γρήγορα η συναλλαγή της. Μεγαλύτερη προμήθεια σημαίνει, ότι περισσότεροι miners, θα δουλέψουν πιο γρήγορα σε αυτήν.

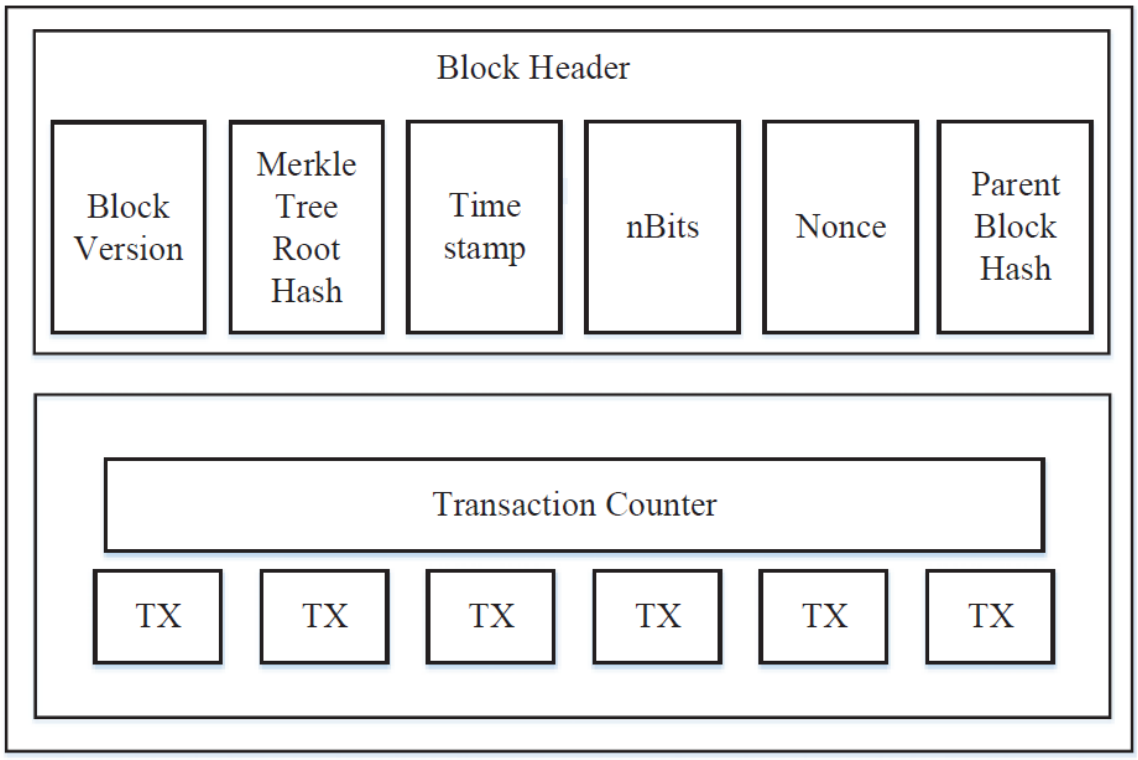


Εικόνα 3 Τα χαρακτηριστικά ενός τυπικού συστήματος Blockchain, πηγή: **[5]**

Στην Εικόνα 3, βλέπουμε την αρχιτεκτονικής ενός Blockchain, το οποίο αποτελείται από το **Datastore,** που είναι η δομή δεδομένων του blockchain, όπου περιέχει όλα της αλυσίδας. Το μηχανισμό συναίνεσης (**Consensus**), δηλαδή η συμφωνία που εξασφαλίζει την ακεραιότητα των δεδομένων. Η επικύρωση των συναλλαγών (**Validation**). Είναι ένα κατανεμημένο δίκτυο (**Peer-to-Peer**). Και η κρυπτογραφία (**Cryptography**) που διασφαλίζει την ασφάλεια και την ιδιωτικότητα των δεδομένων που περιλαμβάνονται στην αλυσίδα. [5]



Εικόνα 4 Παράδειγμα Blockchain με μια ακολουθία από Block, **πηγή: [6]**



Εικόνα 5 Δομή ενός Block, **πηγή: [6]**

Ένα μπλοκ αποτελείται από την επικεφαλίδα και το σώμα, όπως φαίνεται και στην Εικόνα 5. Η επικεφαλίδα του μπλοκ περιλαμβάνει:

Block Version: δηλώνει ποιο σύνολο κανόνων επικύρωσης πρέπει να ακολουθήσει.

Merkle tree root hash: η τιμή κατακερματισμού όλων των συναλλαγών στο μπλοκ.

Timestamp: την τρέχουσα ώρα σε δευτερόλεπτα.

nBits: όριο στόχου για την έγκυρη τιμή κατακερματισμού ενός μπλοκ.

Nonce: ένα πεδίο 4-byte, συνήθως ξεκινά από το 0 και αυξάνεται για κάθε υπολογισμό μια τιμής κατακερματισμού.

Parent block hash: Μια τιμή κατακερματισμού 256-bit που δείχνει το προηγούμενο μπλοκ.

Το σώμα του μπλοκ αποτελείται από τον αριθμό τον μετρητή των συναλλαγών και τις συναλλαγές. Ο μέγιστος αριθμός των συναλλαγών που μπορεί να περιέχει ένα μπλοκ, εξαρτάται από το μέγεθος του μπλοκ και από το μέγεθος της κάθε συναλλαγής. [6]

2.2.1 Η λειτουργεία του Proof of Work (PoW)

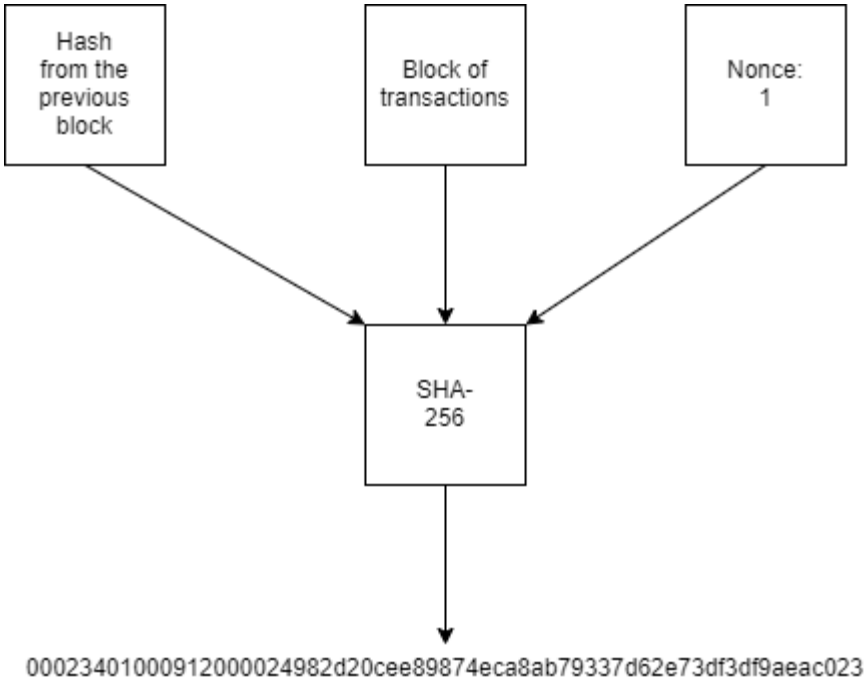
Το PoW είναι ο πιο κλασικός μηχανισμός συναίνεσης που χρησιμοποιείται από το Bitcoin. Η βασική ιδέα αυτού του μηχανισμού είναι, ότι τα μέλη του συστήματος (miners) χρησιμοποιούν την υπολογιστική ισχύ του συστήματος τους, στη διαδικασία της λειτουργίας του κατακερματισμού (hashing operation), το οποίο αποτελεί μια ανταγωνιστική διαδικασία αφού, ο πρώτος που θα βρει την τιμή του κατακερματισμού η οποία είναι χαμηλότερη από τον

αναγγελθέντα στόχο έχει το δικαίωμα να εισάγει ένα καινούργιο μπλοκ στην αλυσίδα, και να κερδίσει ένα ορισμένο ποσό σαν ανταμοιβή. [7]

Οι miners θα πρέπει θα πρέπει να βρουν ένα τυχαίο αριθμό που να τους δίνει το σωστό στοιχείο (hash) για το μπλοκ που περιέχει τις συναλλαγές. Για αυτή την διαδικασία θα χρειαστούν δύο στοιχεία.
Nonce (32-bit) – Είναι ένας τυχαίος αριθμός που χρησιμοποιείται μόνο μια φορά. Στη περίπτωση του Bitcoin, μπορεί να είναι ένας αριθμός μεταξύ του 0 και του 4,294,967,26.
Hash – Είναι ένας αλγόριθμος ο οποίος μετατρέπει οποιαδήποτε αλληλουχία χαρακτήρων σε ένα αλφαριθμητικό 64 χαρακτήρων.

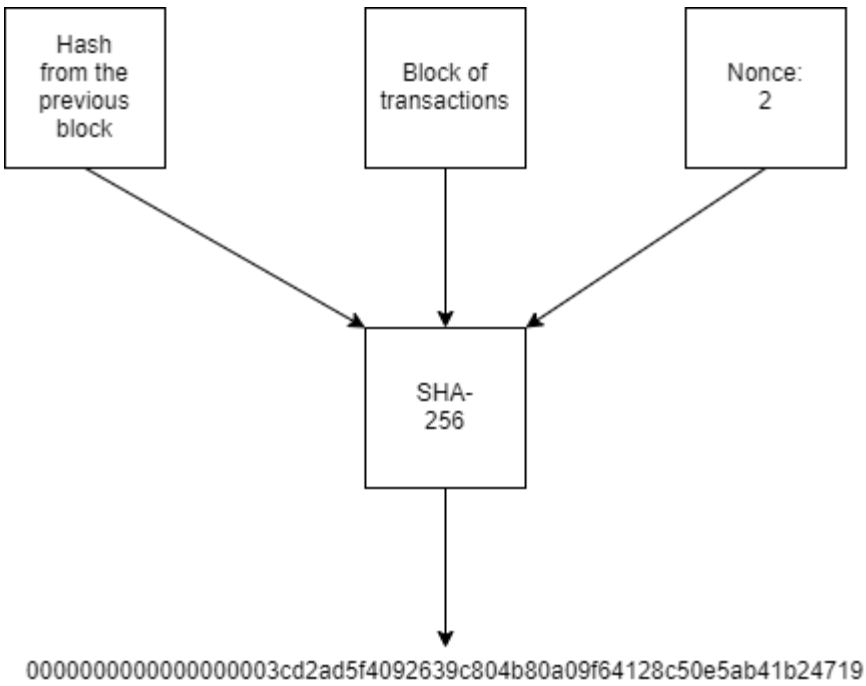
Όπως έχει ήδη, αναφερθεί κάθε μπλοκ έχει το δικό του hash, είναι δηλαδή ένα αλφαριθμητικό το οποίο το βρήκε κάποιος, όταν επαλήθευσε ένα μπλοκ. Τώρα, όταν κάποιος θελήσει να επαληθεύσει το επόμενο μπλοκ, θα χρειαστεί το hash του προηγούμενου μπλοκ και θα προσθέσει τις συναλλαγές του καινούργιου μπλοκ. Το επόμενο βήμα είναι να πάρει ένα τυχαίο αριθμό (nonce) και να το προσθέσει στο τέλος του κειμένου. Τώρα ο miner θα έχει ένα μπλοκ κειμένου που θα αποτελείται από το hash του προηγούμενου μπλοκ, τις νέες συναλλαγές και τον τυχαίο αριθμό (nonce). Για τους υπολογισμούς χρησιμοποιείται η λειτουργία κατακερματισμού, αλλάζοντας τον τυχαίο αριθμό μέχρι να βρεθεί ένα αλφαριθμητικό το οποίο θα έχει ένα συγκεκριμένο αριθμό μηδενικών στην αρχή.

Φαίνεται απλό, αλλά ο υπολογιστής θα χρειαστεί να εφαρμόσει πολλούς υπολογισμούς, μια διαδικασία που θα χρειαστεί περίπου 10 λεπτά για την εύρεση του σωστού αριθμού που θα έχει σαν αποτέλεσμα το σωστό αλφαριθμητικό.



Εικόνα 6 Λειτουργία κατακερματισμού με σωστό αποτέλεσμα

Παραπάνω, βλέπουμε την διαδικασία που έχει το λάθος αποτέλεσμα. Το αλφαριθμητικό έχει μόνο 3 μηδενικά στην αρχή, ενώ εμείς ψάχνουμε ένα αλφαριθμητικό που να ξεκινάει με 18 μηδενικά. Άρα, γίνεται η επιλογή ενός άλλους τυχαίου αριθμού και γίνεται η επανάληψη της διαδικασίας. Αυτή τη φορά με το 2 (nonce).



Εικόνα 7 Λειτουργία κατακερματισμού με λάθος αποτέλεσμα

Τώρα το αποτέλεσμα, ξεκινάει με 18 μηδενικά. Επικυρώνεις το μπλοκ, και άμα είσαι ο πρώτος παίρνεις και την ανταμοιβή.

Ο υπολογιστής, θα αυξάνει τον τυχαίο αριθμό, μέχρι να βρει τον σωστό αριθμό. Θα πρέπει να εκτελεί εκατομμύρια υπολογισμούς για να βρει τον σωστό αριθμό που θα έχει σαν αποτέλεσμα, το αλφαριθμητικό με τον ίδιο αριθμό μηδενικών που έχει καθοριστεί. Αυτή η διαδικασία (PoW) είναι χρονοβόρα και έχει μεγάλο κόστος, αλλά είναι εύκολο για κάποιον να πιστοποιήσει αν ένα μπλοκ είναι σωστό.

Ας υποθέσουμε ότι κάποιος θέλει να ελέγξει εάν ο κόμβος Α έκανε την απαιτούμενη εργασία. Θα χρησιμοποιήσει το αλφαριθμητικό του μπλοκ που ο κόμβος Α πήρε μετά την επικύρωση και θα πάρει τον αριθμό (nonce) που χρησιμοποίησε. Σε αυτά θα εφαρμόσει την λειτουργία του κατακερματισμού και αν το αποτέλεσμα έχει στην αρχή τον σωστό αριθμό μηδενικών, τότε είναι σωστό.

Το Proof of Work εξασφαλίζει ότι τα μπλοκ δεν μπορούν να προστεθούν στην αλυσίδα χωρίς να εκτελούνται οι απαραίτητες εργασίες. Με αυτόν τον τρόπο, ένας κακόβουλος κόμβος δεν μπορεί να επικυρώσει εύκολα ένα μπλοκ και να το προσθέσει στην αλυσίδα. Εάν το προσπαθήσει, οι άλλοι συμμετέχοντες του δικτύου θα απορρίψουν αυτό το μπλοκ γνωρίζοντας ότι δεν είναι έγκυρο.

2.2.2 Proof of Stake

Η έννοια Proof of Stake (PoS), αναφέρθηκε για πρώτη φορά στο PeerCoin (PpCoin) [8], χρησιμοποιήθηκε κυρίως για την επίλυση της άσκοπης σπατάλης ενέργειας που γίνεται από το Proof of Work (PoW).

Το PoW βοήθησε στη γέννηση της σημαντικής ανακάλυψης του Nakamoto, ωστόσο, η φύση του PoW σημαίνει ότι το κρυπτονόμισμα εξαρτάται από την κατανάλωση ενέργειας, εισάγοντας έτσι σημαντικό κόστος στη λειτουργία τέτοιων δικτύων, το οποίο το επωμίζονται οι χρήστες μέσω τέλη συναλλαγών. Καθώς ο ρυθμός επιβραδύνεται στο δίκτυο Bitcoin, τελικά θα μπορούσε να ασκήσει πίεση στην αύξηση των τελών συναλλαγών για να διατηρήσει ένα προτιμώμενο επίπεδο ασφάλειας.

Είναι εύκολο να κατανοήσουμε τον αλγόριθμο του PoS. Ο τύπος είναι:
Hash(block_header) < target * coinage (1)
Coinage = number of coins * remaining usage of coin (2)

Η έννοια του coinage ήταν γνωστή από τον Nakamoto τουλάχιστον από το 2010 και χρησιμοποιήθηκε στο Bitcoin για να βοηθήσει στην ιεράρχηση των συναλλαγών, αν και δεν έπαιξε ρόλο στο μοντέλο ασφάλειας του Bitcoin [8], ο υπολογισμός του coinage επιτυγχάνεται με τον αριθμό κερμάτων επί τον υπόλοιπο χρόνο χρήσης των νομισμάτων, πράγμα που σημαίνει ότι όσα περισσότερα νομίσματα έχει κάποιος, τόσο πιο εύκολα μπορεί να βρεθεί λύση στο

πρόβλημα. Επομένως, το PoS λύνει το πρόβλημα της σπατάλης πόρων του PoW. Ταυτόχρονα, το PoS αποφεύγει τον αποπληθωρισμό. Η κρυπτογράφηση με βάση το PoW μπορεί να οδηγήσει σε αποπληθωρισμό λόγω διαφόρων λόγων όπως η απώλεια χρηστών. Η κρυπτογράφηση με βάση το PoS αυξάνει το νόμισμα με ένα ορισμένο ετήσιο επιτόκιο, το οποίο μπορεί αποτελεσματικά να αποφύγει την εμφάνιση αποπληθωρισμού και να διατηρήσει τη σταθερότητα. [9]

Σε νομίσματα που χρησιμοποιούν PoS, μόνο λίγοι θα μπορούν να παίρνουν κρυπτονομίσματα με χαμηλό κόστος. Ενόψει των συμφερόντων, δεν υπάρχει εγγύηση ότι δεν θα πουλήσουν σε μεγάλες ποσότητες. Η κρυπτογράφηση του PoS δεν είναι αρκετά ασφαλής. Για την επίλυση αυτού του προβλήματος, πολλές πλατφόρμες blockchain υιοθετούν ένα συνδυασμό και των δύο (PoS + PoW), χρησιμοποιούν το PoW για την εξόρυξη και το PoS για τη διατήρηση της σταθερότητας του δικτύου.

Ο Άγγελος Κιάγιας πρότεινε μια συναίνεση που βασίζεται στο PoS, το ¨Ouroboros¨. [10] Το Ouroboros είναι μια αλυσίδα που βασίζεται στο PoS, που διαλέγει τυχαία ένα κόμβο για την παραγωγή του μπλοκ. Η πιθανότητα επιλογής σχετίζεται με το μερίδιο που έχει. Το κλειδί είναι πώς να εγγυηθεί την «τυχαιότητα». Η παραδοσιακή λύση του PoS ξεκινά με τα υπάρχοντα δεδομένα στην αλυσίδα, όπως η χρήση της τιμής κατακερματισμού (hash value) του προηγούμενου μπλοκ και η χρονική σήμανση (timestamp) του προηγούμενου μπλοκ ως πηγή του τυχαίου αριθμού, αλλά αυτά συνεπάγονται πρόσθετους κινδύνους ασφαλείας. Δεδομένου ότι οι πληροφορίες του ίδιου του μπλοκ γράφονται από τον κόμβο, και στη συνέχεια οι επόμενοι κόμβοι επιλέγονται σύμφωνα με τις πληροφορίες του μπλοκ, υπάρχει κίνδυνος κυκλικής επιχειρηματολογίας. Το Ouroboros είναι η πρώτη συναίνεση PoS της οποίας η ασφάλεια επαληθεύτηκε μαθηματικά. [9]

2.2.3 Πρακτική Βυζαντινή Ανεκτικότητας Σφαλμάτων

Η Βυζαντινή Ανεκτικότητα Σφαλμάτων (BFT) αποτελεί το χαρακτηριστικό ενός δικτύου που έχει ως στόχο την επίτευξη της συναίνεσης για την ίδια τιμή, ακόμη και όταν οι κόμβοι του δικτύου αποτυγχάνουν να ανταποκριθούν ή ανταποκρίνονται με εσφαλμένες πληροφορίες. Το BFT έχει ως στόχο την προστασία από τις αποτυχίες του συστήματος, χρησιμοποιώντας συλλογική λήψη αποφάσεων και από τους σωστούς κόμβους αλλά και από τους ελλαττωματικούς κόμβους που στοχεύει στη μείωση της επιρροής των ελαττωματικών κόμβων. Το BFT προέρχεται από το πρόβλημα των βυζαντινών στρατηγών.

Έχει δοθεί εξήγηση από τους Leslie Lamport, Robert Shostak και Marshall Pease για το πρόβλημα των δύο στρατηγών, πιο συγκριμένα, για παράδειγμα πολλά τμήματα του βυζαντινού στρατού στρατοπεδεύουν έξω από μια εχθρική πόλη, κάθε τμήμα διοικείται από τον δικό του στρατηγό. Οι στρατηγοί μπορούν να επικοινωνούν μεταξύ τους μόνο μέσω ενός αγγελιοφόρου. Αφού παρατηρήσουν τις κινήσεις του εχθρού, θα πρέπει να πάρουν μια απόφαση, αυτή η απόφαση αφορά το κοινό σχέδιο δράσης. Ωστόσο, ένας αριθμός των στρατηγών μπορεί να είναι προδότες που έχουν ως σκοπό να εμποδίσουν τους πιστούς στρατηγούς στο να φτάσουν σε μια συμφωνία. Αυτή η συμφωνία αφορά για πότε πρέπει να προβούν σε επίθεση στη πόλη, αλλά το πιο σημαντικό είναι ότι πρέπει αυτή η επίθεση να γίνει από ένα μεγάλο αριθμό του στρατού την ίδια

στιγμή. Γι’ αυτό οι στρατηγοί πρέπει να ΄έχουν έναν αλγόριθμο το οποίο να εγγυάται ότι (i) όλοι οι πιστοί στρατηγοί θα προβούν σε μια απόφαση ενός κοινού σχεδίου δράσης και (ιι) ότι ένας μικρός αριθμός προδοτών δεν μπορεί να κάνει τους πιστούς στρατηγούς να υιοθετήσουν ένα κακό σχέδιο δράσης. Οι πιστοί στρατηγοί θα κάνουν ότι λέει ο αλγόριθμός, αλλά οι προδότες θα κάνουν ότι θέλουν. Ο αλγόριθμος πρέπει να εγγυάται την κατάσταση ανεξάρτητα από το τι θα κάνουν οι προδότες. Οι πιστοί στρατηγοί δεν θα πρέπει να προβούν στη συμφωνία ενός κοινού σχέδιο δράσης, αλλά να πρέπει να συμφωνήσουν και σε ένα λογικό σχέδιο.

Το PBFT (Practical Byzantine Fault Tolerance) είναι μια συντομογραφία πρακτικής βυζαντινής ανεκτικότητας σφαλμάτων. Ο αλγόριθμος προτάθηκε από τους Miguel Castro και Barbara Liskov το 1999. [11] Οι συγγραφείς πιστεύουν ότι ο βυζαντινός αλγόριθμος ανοχής σφαλμάτων θα γίνει πιο σημαντικός καθώς όλο και περισσότερες κακόβουλες επιθέσεις και σφάλματα λογισμικού εμφανίζονται και οι αποτυχημένοι κόμβοι θα συμπεριφέρονται αυθαίρετα. Ο πρώιμος βυζαντινός αλγόριθμος ανεκτικός σε σφάλματα προϋποθέτει ότι το σύστημα έχει χαμηλή απόδοση. Ο αλγόριθμος που περιγράφεται στο [11] είναι πρακτικός επειδή λειτουργεί σε ασύγχρονο περιβάλλον και βελτιώνει την απόδοση απόκρισης κατά περισσότερο από μια τάξη μεγέθους. Η συναίνεση PBFT έχει υψηλή απόδοση, αλλά το ποσοστό ανοχής σφαλμάτων είναι χαμηλό. Και λόγω του προβλήματος της επεκτασιμότητας κόμβων, είναι πιο κατάλληλο για ένα κλειστό σύστημα κόμβων. Καθώς κάθε κόμβος πρέπει να συγχρονιστεί με τη συναίνεση άλλων κόμβων στο P2P, η απόδοση του αλγορίθμου PBFT θα μειωθεί γρήγορα με την αύξηση των κόμβων, αλλά μπορεί να έχει καλή απόδοση στην περίπτωση λιγότερων κόμβων. [9]

Το Algorand είναι μια λύση κρυπτογράφησης που παρουσίασε η Silvio Micali. [12] Αυτό το σχήμα χρησιμοποιεί αλγόριθμο κρυπτογράφησης με τυχαίες επιλογές για την επίτευξη της μεγάλης κλίμακας επέκτασης του βυζαντινού αλγορίθμου συναίνεσης και μπορεί να εφαρμοστεί στο σύστημα κρυπτογράφησης της δημόσιας αλυσίδας. Σε σύγκριση με τους παραδοσιακούς αλγόριθμους συναίνεσης κρυπτογράφησης όπως τα PoW και PoS, το Algorand είναι πιο ασφαλές, είναι σχεδόν αδύνατο να υποστεί διαχωρισμό (forking) και πιο αποτελεσματικό (κάθε γύρος συναίνεσης επιτυγχάνεται εντός 1 λεπτού). Το Algorand περιέχει δύο κύριους αλγόριθμους: (i) τον αλγόριθμο κρυπτογράφησης κληρώσεων κλήρωσης, ο οποίος χρησιμοποιείται για να διασφαλίσει ότι τα μέλη της επιτροπής συναίνεσης που συμμετέχουν στη συναίνεση κάθε φορά είναι σχεδόν εντελώς τυχαία. (ii) τον αλγόριθμος BA *, ο οποίος λειτουργεί από τα μέλη της επιτροπής συναίνεσης για την παραγωγή των μπλοκ που θα έπρεπε να είναι ¨συσκευασμένα¨ εκείνη τη στιγμή. Ο αλγόριθμος BA * χωρίζεται σε τρία στάδια: δημιουργία μπλοκ, GC και BBA *. Ο χρόνος διακοπής του αλγορίθμου είναι αβέβαιος, αλλά είναι εγγυημένο ότι θα λήξει σε πεπερασμένα βήματα με μεγάλη πιθανότητα. [9]

2.2.4 SHA-256

Οι λειτουργίες κατακερματισμού (hash functions) μονής κατεύθυνσης (one-way) είναι επαναληπτική αλγόριθμοι που λειτουργούν σε ένα μήνυμα αυθαίρετου μήκους και επιστρέφουν μια έξοδο σταθερού μήκους (h), που ονομάζεται digest ή hash value. Δεν είναι υπολογιστικά εφικτό να βρεθούν δύο διαφορετικά μηνύματα με την ίδια τιμή. Οι αλγόριθμοι hash για να

υπολογίσουν την τιμή, εκτελούν μια σειρά ταυτόσημων ή ελαφρώς διαφορετικών λειτουργιών που ονομάζονται κύκλοι μετασχηματισμού (transformation rounds) ή λειτουργίες (operations).

Με τη λειτουργία κατακερματισμού το εισαγόμενο μήνυμα M, μήκους l προ επεξεργάζεται μέσω μιας λειτουργίας padding. Ο σκοπός του padding εξασφαλίζει ότι το μήνυμα εισόδου είναι πολλαπλάσιο του 512 ή του 1024 – bits (ανάλογα με τον αλγόριθμο). Για το SHA-1 και το SHA-256 χωρίζεται σε μπλοκ των 512-bit και στο τέλος του τελευταίου μπλοκ προσαρτάται το bit “1” ακολουθούμενο από k μηδενικά bits, όπου k είναι η μικρότερη μη-αρνητική λύση της εξίσωσης l + 1 +κ = 448mod512. Στη συνέχεια προσαρτάται ένα μπλοκ 64-bit που ισούται με το l σε δυαδική μορφή. Συγκεκριμένα, ένα ¨1¨ ακολουθούμενο από k μηδενικά επισυνάπτονται στο τέλους του M και να δημιουργηθεί ένα padded μήνυμα μήκους 512 * n. Για παράδειγμα, το μήνυμα ¨abc¨, έχει μήκος l = 8 * 3 = 24, επομένως το μήνυμα είναι γεμισμένο με 1 bit, άρα l +1 + k = 448 $\Rightarrow$ k = 448 – (24 + 1) $\Rightarrow$ k = 423 μηδενικά. [13]

Στη συνέχεια, εκτελείται ένα πρόγραμμα μηνυμάτων στα μπλοκ του M παράγουν τις τιμές W_t, όπου η κάθε μία τροφοδοτείται από την αντίστοιχη t-th επανάληψη του γύρου μετασχηματισμού. Ο γύρος μετασχηματισμού παίρνει ως είσοδο την τιμή W_t, μια σταθερή τιμή K_t που ορίζεται από το πρότυπο και οι αρχικές τιμές, $H^{(0)}$ (στη πρώτη επανάληψη) ή οι τιμές που παράχθηκαν στην προηγούμενη επανάληψη, και εκτελείται η επεξεργασία μετασχηματισμού, όπου μέσα από μια σειρά επαναλήψεων παράγει μια σειρά από τιμές hash. Η τελευταία παραγόμενη τιμή θεωρείται ως το μήνυμα digest, h. [13]

Ένα hash δεν αποτελεί αποτέλεσμα μια κρυπτογράφησης και έτσι δεν μπορεί να αποκρυπτογραφηθεί ξανά στο αρχικό κείμενο (είναι μια κρυπτογραφική λειτουργία «μονής κατεύθυνσης» και έχει σταθερό μέγεθος για οποιοδήποτε μέγεθος κειμένου που εισάγεται). Αυτό το καθιστά κατάλληλο όταν χρειάζεται να συγκρίνουμε τις εκδοχές των κειμένων που μετατρέπονται σε μια «μοναδική ταυτότητα» (hash), σε αντίθεση με την αποκρυπτογράφηση του κειμένου για να αποκτήσουμε την αρχική πηγή.

Τέτοιες εφαρμογές περιλαμβάνουν hash πίνακες, επαλήθευση ακεραιότητας, πρόκληση επαλήθευσης χειραψίας, ψηφιακές υπογραφές κλπ.

Πρόκληση επαλήθευσης χειραψίας, αποφεύγει την αποστολή του κωδικού, μπορεί ένας πελάτης να στείλει το hash ενός κωδικού μέσω διαδικτύου για επικύρωση από τον διακομιστή χωρίς να γίνει γνωστός ο κωδικός.

Anti-tamper, σύνδεση ενός hash ενός μηνύματος με το αρχικό μήνυμα και ο παραλήπτης θα το συγκρίνει με το παρεχόμενο hash, άμα ταιριάζουν τότε το μήνυμα ήρθε αναλλοίωτο, αυτό μπορεί να χρησιμοποιηθεί για την επιβεβαίωση ότι δεν υπάρχει απώλεια δεδομένων στη μετάδοση.

Με τις **ψηφιακές υπογραφές** μπορούμε να υπογράψουμε το hash ενός εγγράφου, με την βοήθεια του ιδιωτικού κλειδιού, δημιουργώντας μια ψηφιακή υπογραφή. Ο καθένας μπορεί να

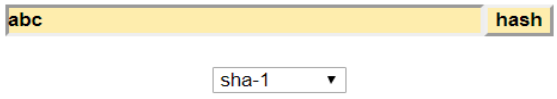
δει ότι το έγγραφο έχει την ψηφιακή υπογραφή μας, και μπορεί να την αποκρυπτογραφήσει με το δημόσιο κλειδί που εμείς παρείχαμε και να συγκρίνει το δικό μας hash με το δικό του.

Οι λειτουργίες του κατακερματισμού (hash function) δεν είναι κατάλληλες για την αποθήκευση κωδικών, αφού έχουν σχεδιαστεί για να είναι γρήγοροι στον υπολογισμό και επομένως θα αποτελούν στόχο για επίθεση από κακόβουλους χρήστες. Υπάρχουν άλλες λειτουργίες για την εξαγωγή και αποθήκευση κωδικών, όπως είναι το bcrypt (Niels Provos & David Mazieres, 1999) και το scrypt (Colin Percival), που είναι σχεδιασμένα για αργούς υπολογισμούς.

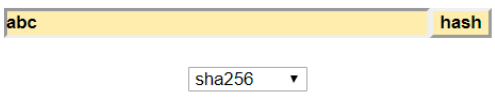
2.2.4.1 SHA-1 and SHA-2

Το SHA αντιπροσωπεύει το Secure Hashing Algorithm. Το SHA-1 και SHA-2 είναι δύο διαφορετικές εκδόσεις του αλγορίθμου. Και τα δύο διαφέρουν στην κατασκευή (δηλαδή, το πως δημιουργείται hash από τα αρχικά δεδομένα) και στο μήκος (bit) υπογραφής. Το SHA-2 αποτελεί γενική βελτίωση του SHA-1.

Κατά κύριο λόγο, οι άνθρωποι εστιάζουν στο μήκος bit ως σημαντική διάκριση. Το SHA-1 είναι ένα hash με μήκος 160-bit, ενώ το SHA-2 που είναι μια «οικογένεια» από hashes που έχουν διαφορετικά μήκη, όπου το δημοφιλέστερο είναι το hash με μήκος 256-bit. Στο SHA-2 εντάσσονται τα SHA-224, SHA-384 και SHA-512.
Στην Εικόνα 8 & στην Εικόνα 9 φαίνεται το μήκος του abc με SHA-1 και SHA-256 που ανήκει στην «οικογένεια» SHA-2.



Εικόνα 8 SHA-1 του abc, πηγή: http://www.sha1-online.com/



Εικόνα 9 SHA-2 (256-bit) του abc, **πηγή:** http://www.sha1-online.com/

2.3 Λογισμικού ανοιχτού κώδικα (Open Source Platform)

Το λογισμικό ανοιχτού κώδικα (OSS) είναι ένας τύπος λογισμικού υπολογιστή στον οποίο ο πηγαίος κώδικας είναι ελεύθερος, όπου ο κάτοχος των πνευματικών δικαιωμάτων παρέχει στους χρήστες τα δικαιώματα να μελετούν, να αλλάζουν και να διανέμουν το λογισμικό σε οποιονδήποτε και για οποιονδήποτε σκοπό. Το λογισμικό ανοικτού κώδικα μπορεί να αναπτυχθεί με συνεργατικό τρόπο και αποτελεί ένα παράδειγμα ανοικτής συνεργασίας. Ο στόχος τους ανοιχτού κώδικα είναι να κάνει την ανάπτυξη λογισμικού παρόμοια με την ακαδημαϊκή έρευνα. Με την δημοσίευση του πηγαίου κώδικα σε οποιονδήποτε, είτε για να τον διαβάσει είτε για να τον ελέγξει, το οποίο στοχεύει στην αύξηση της ποιότητας του λογισμικού.

Η διαφορά μεταξύ λογισμικού ανοιχτού κώδικα και ιδιόκτητου κώδικα έγκειται στις άδειες χρήσης τους. Μια άδεια χρήσης αποκλειστικού λογισμικού παρέχει το δικαίωμα χρήσης ενός αντίγραφου του προγράμματος στον τελικό χρήστη, αλλά η ιδιοκτησία του λογισμικού παραμένει στον τελικό χρήστη. Στην περίπτωση, της άδειας ανοιχτού κώδικα, παρέχει στον χρήστη το δικαίωμα χρήσης, αντιγραφής, τροποποίησης και αναδιανομής του λογισμικού. Τα πνευματικά δικαιώματα του λογισμικού παραμένουν στον δημιουργό, αλλά ο δημιουργός μεταφέρει τα δικαιώματα στον χρήστη, εφόσον τηρούνται οι υποχρεώσεις της άδειας. [14]

Μία ακόμη διαφορά είναι, ότι τα ιδιόκτητα προγράμματα διανέμονται μεταγλωτισμένα σε δυαδικά αρχεία. Δηλαδή, διανέμεται συνήθως σε γλώσσα μηχανής. Αυτοί που επιθυμούν να αποκτήσουν γνώση για το τι κάνει το λογισμικό θα πρέπει η γλώσσα μηχανής να περάσει από μια χρονοβόρα διαδικασία που ονομάζεται αντίστροφη μηχανική (reverse engineering). Οι περισσότερες άδειες ιδιοκτησίας απαγορεύουν την χρήση αυτών των τεχνικών, έτσι ο χρήστης δεν χρειάζεται συνήθως να κατανοεί για το τι κάνει το λογισμικό. Αντίθετα, το λογισμικό ανοιχτού κώδικα διανέμεται πάντα με ένα αντίγραφο του πηγαίου κώδικα. Έτσι, ένας χρήστης που θέλει να καταλάβει για το τι κάνει το λογισμικό, χρειάζεται απλώς να διαβάσει τον πηγαίο κώδικα. Το κρυπτογραφικό λογισμικό ανοιχτού κώδικα έχει το πλεονέκτημα να δίνει την δυνατότητα στους χρήστες να ελέγχουν για το αν ο κώδικας έχεις αδυναμίες στην ασφάλεια ή πίσω πόρτες (backdoor). [14]

Το OSS είναι λογισμικό που δημιουργείται και συντηρείτε μέσω πρακτικών ανάπτυξης ανοικτού κώδικα και διανέμεται με άδεια ανοικτού κώδικα. Το OSS προσφέρει πολλά οφέλη που ευνοούν την υιοθεσία, όπως το χαμηλό κόστος, να τροποποιεί και να προσαρμόζει τον πηγαίο κώδικα ανάλογα με τις ανάγκες, έχει μεγαλύτερο έλεγχο και δεν υπάρχει ο κίνδυνος κλειδώματος ή η δημιουργία περιοριστικών όρων από τον προμηθευτή. Το χαμηλό κόστος καθιστά χρήσιμες εφαρμογές να είναι προσβάσιμες για τις μικρές και μεσαίες επιχειρήσεις που δεν μπορούν να ανταποκριθούν οικονομικά σε πιο ακριβές λύσεις λογισμικού. [15]

Παραδείγματα δημοφιλών λογισμικών ανοικτού κώδικα είναι, τα Linux (λειτουργικό σύστημα διακομιστή), MySQL (διακομιστής βάσης δεδομένων), Mozilla Firefox (φυλλομετρητής), Apache (διακομιστής ιστού), Sendmail (διακομιστής e-mail), Python (γλώσσα προγραμματισμού), Android (λειτουργικό σύστημα), Ethereum (πλατφόρμα blockchain) και άλλα πολλά.

2.3.1 *Hyperledger Fabric*

Τον Δεκέμβριο του 2015, το Ίδρυμα Linux και 30 εταιρείες δημιούργησαν το σχέδιο Hyperledger, για να προωθήσουν την διεπαγγελματική τεχνολογία blockchain και παρέχει λογισμικό ανοιχτού κώδικα. Το hyperledger fabric έχει προωθήσει την ανάπτυξη των σχετικών πρωτοκόλλων, προδιαγραφών, και προτύπων blockchain και της βάσης δεδομένων των συναλλαγών. Το fabric είναι ένα από τα πρώτα προγράμματα που προστέθηκαν στον hyperledger, και παρουσιάστηκαν από την IBM, DAH, και από άλλες εταιρίες έως τα τέλη του 2015. Ο σχεδιασμός του hyperledger fabric υποστηρίζει την συνδεσιμότητα και την επεκτασιμότητα. Είναι το πρώτο πρόγραμμα λογισμικού ανοιχτού κώδικα για την αλυσίδα. Μέχρι τον Αύγουστο του 2018, το hyperledger, έχει περισσότερα από 250 μέλη (π.χ. Intel, Huawei κ.α.). [16]

Το Hyperledger Fabric είναι μια υποδομή blockchain άδειας, παρέχοντας μια αρθρωτή αρχιτεκτονική με οριοθέτηση των ρόλων μεταξύ των κόμβων, την εκτέλεση των έξυπνων συμβολαίων (smart contracts ή chaincode) και διαμορφωμένες υπηρεσίες συναίνεσης και συνδρομής. Ένα δίκτυο Fabric περιλαμβάνει ¨Peer nodes¨, οι οποίοι εκτελούν αλυσιδωτό κώδικα (chaincode), έχει πρόσβαση σε βιβλιοθήκες δεδομένων, υποστηρίζουν συναλλαγές. Αποτελεί, επίσης μια πλατφόρμα που δημιουργεί λύσεις για την κατασκευή διανεμημένων βάσεων, με μια αρθρωτή αρχιτεκτονική που προσφέρει εμπιστευτικότητα, ευελιξία, ανθεκτικότητα και επεκτασιμότητα σε μεγάλο βαθμό. Αυτό επιτρέπει στις λύσεις που αναπτύχθηκαν με το Fabric να προσαρμόζονται σε κάθε κλάδο.

Επίσης, το Fabric αξιοποιεί την τεχνολογία container το οποίο φιλοξενεί τα έξυπνα συμβόλαια, τα οποία ονομάζονται αλυσιδωτός κώδικας τα οποία περιέχουν τους επιχειρηματικούς κανόνες του συστήματος.

Το Fabric διαθέτει μια εξαιρετικά αρθρωτή και διαμορφωμένη αρχιτεκτονική που επιτρέπει την καινοτομία, την ευελιξία και τη βελτιστοποίηση για ένα ευρύ φάσμα περιπτώσεων βιομηχανικής χρήσης, όπως τραπεζική, χρηματοοικονομική, ασφαλιστική, ανθρωπίνου δυναμικού, υγειονομική περίθαλψη, αλυσίδα εφοδιασμού και ακόμη και ψηφιακή μουσική.

Το Fabric είναι η πρώτη κατανεμημένη πλατφόρμα λογισμικού που υποστηρίζει smart contracts που συντάσσονται σε γλώσσες προγραμματισμού γενικού σκοπού, όπως Java, Go και Node.js αντί για περιορισμένες γλώσσες γενικού σκοπού (Domain – Specific Language ή DSL). Αυτό σημαίνει ότι οι περισσότερες επιχειρήσεις διαθέτουν ήδη το απαιτούμενο σύνολο δεξιοτήτων για την ανάπτυξη έξυπνων συμβάσεων και δεν απαιτείται πρόσθετη κατάρτιση για την εκμάθηση μιας νέας γλώσσας ή DSL.

Για την πλατφόρμα Fabric χρειάζεται άδεια, αντίθετα δηλαδή με ένα δημόσιο δίκτυο που δεν χρειάζεται άδεια (Bitcoin network), οι συμμετέχοντες γνωρίζονται μεταξύ τους και δεν είναι ανώνυμοι και επομένως αξιόπιστοι. Αυτό δεν σημαίνει ότι στο δίκτυο που απαιτείται άδεια, υπάρχει εμπιστοσύνη μεταξύ των συμμετεχόντων, μπορεί να είναι, για παράδειγμα, ανταγωνιστές στην ίδια την εταιρία. Ένα δίκτυο μπορεί να λειτουργήσει σύμφωνα με ένα

μοντέλο διακυβέρνησης που βασίζεται στην εμπιστοσύνη μεταξύ των συμμετεχόντων, όπως είναι μια νομική συμφωνία ή ένα πλαίσιο για την διεκπεραίωση των διαφορών.

Chaincode

Το Chaincode είναι ένα πρόγραμμα, γραμμένο σε Go, node.js ή Java που υλοποιεί μια καθορισμένη διεπαφή. Ο κώδικα τρέχει σε ένα ασφαλές Docker που είναι απομονωμένο από την επικυρωτική διαδικασία. Ο κώδικας (chaincode) διαχειρίζεται την κατάσταση του ημερολογίου συναλλαγών που υποβάλλονται από εφαρμογές.

Ένας αλυσιδωτός κώδικας συνήθως χειρίζεται την επιχειρηματική λογική που έχει συμφωνηθεί από τα μέλη του δικτύου, έτσι ώστε να είναι παρόμοια με το ¨smart contract¨. Ένας αλυσιδωτός κώδικας μπορεί να χρησιμοποιηθεί για την ενημέρωση ή για την ερώτηση (query) στο βιβλίο σε μια προτεινόμενη συναλλαγή. Με την κατάλληλη άδεια, ο αλυσιδωτός κώδικας μπορεί να επικαλεσθεί έναν άλλον αλυσιδωτό κώδικα, είτε αυτός βρίσκεται στο ίδιο κανάλι είτε βρίσκεται σε άλλο.

Αυτή η ενότητα παρέχει μια περίληψη της τεκμηρίωσης του Hyperledger Fabric. Το hyperledger fabric είναι μια πλατφόρμα ανοιχτού κώδικα που έχει σχεδιαστεί για χρήση σε επιχειρηματικά περιβάλλοντα, που προσφέρει ορισμένες βασικές δυνατότητες διαφοροποίησης σε σχέση με άλλες πλατφόρμες distributed ledger (DL) ή blockchain.

Το Hyperledger Fabric παρέχει τις ακόλουθες λειτουργίες δικτύου blockchain:

Διαχείριση ταυτότητας

Η διαφορά από ένα σύστημα blockchain είναι ότι το hyperledger είναι ιδιωτικό και χρειάζεται άδεια για να συμμετάσχει κάποιος. Η διαφορά από ένα ανοικτό δίκτυο, όπου ο καθένας μπορεί να συμμετάσχει (που απαιτεί πρωτόκολλα, όπως το Proof of work, για την εγκυρότητα των συναλλαγών και την ασφάλεια του δικτύου), το hyperledger fabric εισάγει νέους χρήστες μέσω μιας αξιόπιστης υπηρεσία συνδρομής (Membership Service Provider).

Αποτελεσματική επεξεργασία

Στο hyperledger fabric κάθε κόμβος έχει έναν ή περισσότερους ρόλους. Για την ενίσχυση του συγχρονισμού και του παραλληλισμού του δικτύου, η δέσμευση των συναλλαγών και η εκτέλεση των συναλλαγών διατηρούνται χωριστά.

Λειτουργία κώδικα αλυσίδας

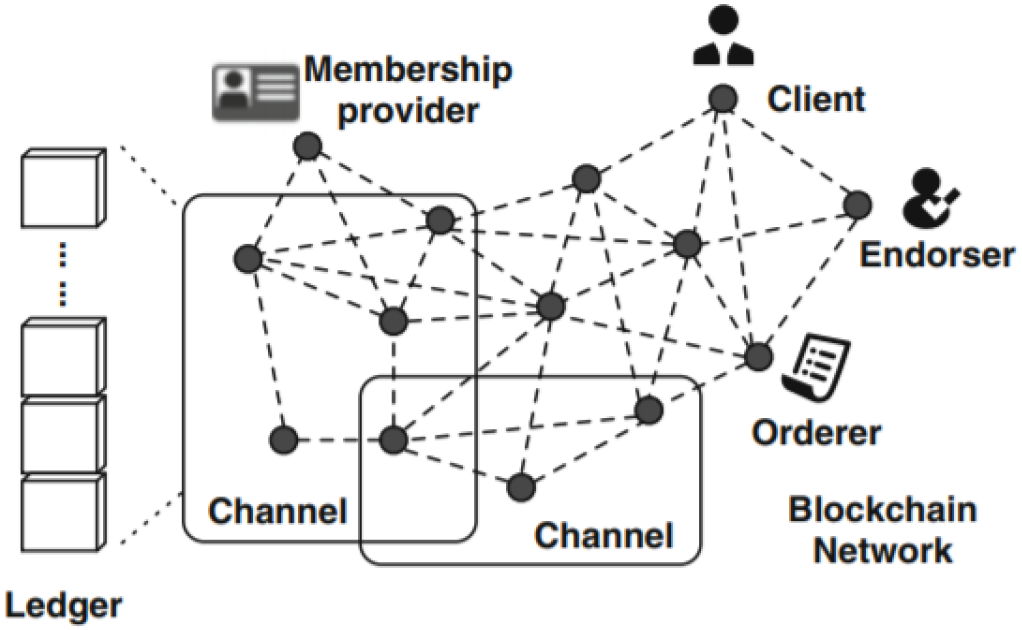
Μια εξωτερική εφαρμογή που χρειάζεται να αλληλεπιδράσει με το βιβλίο (ledger) μπορεί να επικαλεστεί το hyperledger fabric smart contracts. Τα smart contracts μπορούν να γραφούν σε πολλές γλώσσες προγραμματισμού.

Απόρρητο και εμπιστευτικότητα

Το hyperledger fabric παρέχει την ευκαιρία δημιουργίας καναλιών. Το βιβλίο (ledger) υπάρχει στο πλαίσιο ενός καναλιού, έτσι με αυτόν τον τρόπο αυτοί που συμμετέχουν μπορούν να δημιουργήσουν ένα ξεχωριστό βιβλίο συναλλαγών.

Αρθρωτή σχεδίαση

Το hyperledger fabric προσφέρει πολλές επιλογές σύνδεσης όσον αφορά τα πρωτόκολλα συναίνεσης και τις μορφές (formats).



Εικόνα 10 Επισκόπηση του συστήματος Hyperledger Fabric, **πηγή: [17]**

Υπάρχουν τρεις τύποι κόμβων μέσα σε ένα σύστημα Hyperledger Fabric: **client, peer και orderer.**

Client (Πελάτης): Ενεργεί για λογαριασμό ενός τελικού χρήστη. Συνδέετε με άλλους (peers) για να επικοινωνεί με την αλυσίδα (blockchain). Ένας πελάτης-κόμβος δημιουργεί συναλλαγές και να μεταδίδει μηνύματα στους παραλήπτες μέσω καναλιών επικοινωνίας.

Peer: Ένας κόμβος λαμβάνει εντοπισμένες καταστάσεις αναβάθμισης από τους παραλήπτες, δεσμεύει συναλλαγές και διατηρεί την κατάσταση του ημερολογίου. Κάθε σύστημα (peer) μπορεί να αναλάβει ένα ρόλο που δεσμεύει. Κάθε συναλλαγή που περιλαμβάνει ένα αλυσιδωτό κώδικα (chaincode) πρέπει να εγκριθεί. Κάθε αλυσιδωτός κώδικάς μπορεί να καθορίσει μια πολιτική επικύρωσης που καθορίζει τους απαραίτητους και επαρκείς όρους για την έγκυρη επικύρωση συναλλαγών. [17]

Orderer: Ένας κόμβος εντολέων επικυρώνει τις συναλλαγές με βάση την πολιτική επικύρωσης. Οι εντολείς παρέχουν κοινόχρηστα κανάλια στους clients και στα συστήματα (peers). Οι clients

που είναι συνδεδεμένοι με ένα κανάλι μπορούν εκπέμπουν συναλλαγές στο κανάλι, οι οποίοι παραδίδονται και στους υπόλοιπους του καναλιού.

2.4 Τα οφέλη του Blockchain

Διαφάνεια: Κάθε χρήστης στο δίκτυο έχει ένα αντίγραφο της αλυσίδας, όπου περιέχει το ιστορικό των συναλλαγών, που δίνει την δυνατότητα εντόπισης της πηγής κάθε περιουσιακού στοιχείου.

Αποκεντρωποιημένο σύστημα: Αποτελεί ένα από τα πιο διάσημα χαρακτηριστικά του Blockchain, και αυτό που το κάνει ιδιαίτερο και πιο ελκυστικό. Το Blockchain είναι ένα δίκτυο P2P, όπου όλοι οι χρήστες που συμμετέχουν στο δίκτυο έχουν τα ίδια δικαιώματα. Οι κεντρικές αρχές δεν συμμετέχουν σε αυτό το σύστημα, , όπου οι κανόνες και οι συμπεριφορές έχουν προκαθοριστεί από το ίδιο το λογισμικό. Αυτό έχει ως αποτέλεσμα οι συναλλαγές να έχουν χαμηλότερο κόστος, αφού η προμήθεια που βάζει ένα τρίτο-μέρος, (π.χ τράπεζα) δεν υπάρχει πλέον. [18]

Ομοφωνία (Consensus): Είναι ο κύριος μηχανισμός ενός δικτύου ενός αποκεντρωποιημένου συστήματος που επιτρέπει την συναλλαγή μεταξύ χρηστών χωρίς την παρέμβαση ενός μεσάζοντα, επιτρέποντας σε ολόκληρο το δίκτυο να φτάσει σε μια συμφωνία για το ποια block είναι έγκυρα και ποια όχι, με τη βοήθεια του PoW.

Δυσκολία αλλοίωσης: Όπως είδαμε και παραπάνω, το Bitcoin χρησιμοποιεί την λειτουργεία hash, SHA-256, όπου μετατρέπει κάθε εισερχόμενο μήνυμα σε 256-bit. Αυτή η λειτουργία έχει ως αποτέλεσμα, με οποιαδήποτε παραλλαγή στο εισερχόμενο μήνυμα να δημιουργεί μια εντελώς διαφορετική εκροή. Έτσι, ένας κακόβουλος χρήστης που επιθυμεί να αλλάξει οποιοδήποτε στοιχείο ενός block, θα έχει ως αποτέλεσμα να ξανά υπολογίσει το στοιχείο αναγνώρισης (hash) του block. Και επειδή κάθε block, περιέχει το hash του προηγούμενου block, θα πρέπει να αλλάξει όλα τα στοιχεία των block που υπάρχουν στην αλυσίδα.

Μη παραποιήσιμο (Tamper-Proof): Είναι ένα κατανεμημένο σύστημα που στηρίζεται κυρίως σε ένα σύστημα κρυπτογράφησης για τη διατήρηση ολόκληρου του δικτύου. Ουσιαστικά, κάθε συμμετέχων στο δίκτυο έχει ένα ιδιωτικό/δημόσιο κλειδί. Το δημόσιο κλειδί διανέμεται σε όλους που συμμετέχουν στο δίκτυο, ενώ το ιδιωτικό κλειδί διατηρείται από τον χρήστη. Κάθε συναλλαγή υπογράφεται ψηφιακά χρησιμοποιώντας το ιδιωτικό κλειδί του χρήστη, επικυρωμένο από το δημόσιο κλειδί, για την διασφάλιση ότι η συναλλαγή πραγματοποιήθηκε από τον κάτοχο με το συγκεκριμένο ιδιωτικό κλειδί. Μετά χρησιμοποιείται η λειτουργία κατακερματισμού (hash function), για την δημιουργία, ψηφιακού αποτυπώματος που είναι μοναδικό για την συναλλαγή, το οποίο μετά εντάσσεται σε ένα μπλοκ. Και μετά την εισαγωγή του μπλοκ στην αλυσίδα, το μπλοκ αυτό διανέμεται σε όλους τους χρήστες που συμμετέχουν στο δίκτυο. [18]

Smart Contracts: Είναι ένα χαρακτηριστικό που ενσωματώθηκε στο Blockchain δεύτερης γενιάς. Είναι ένας κώδικας που βασίζεται στη συνθήκη ¨If - then¨, όπου τα γεγονότα είναι άμεσα

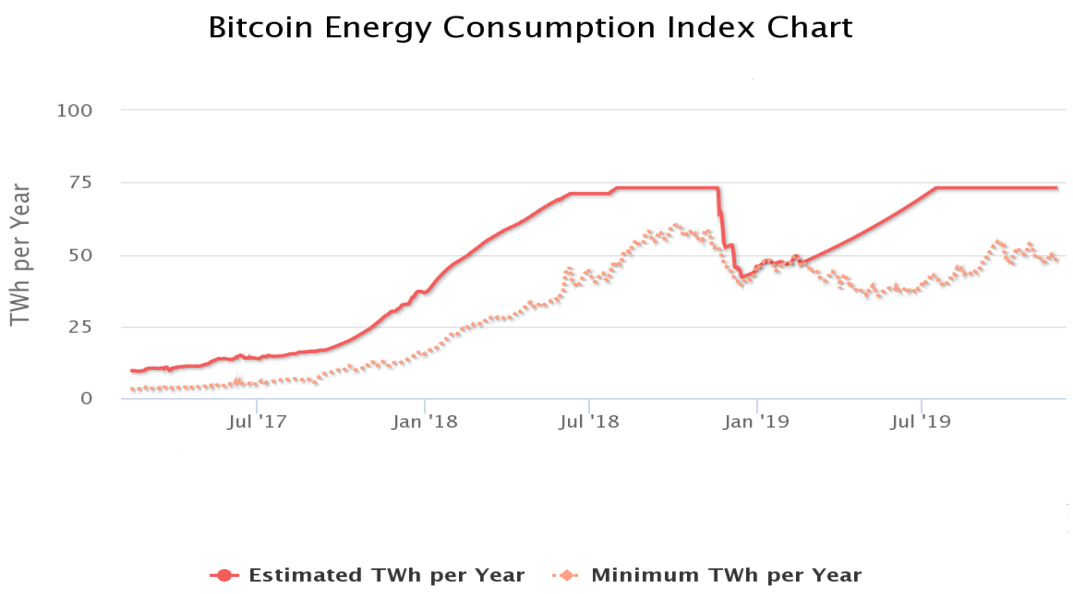
συνδεδεμένα με το συμβόλαιο και τα οποία εκτελούνται αυτόματα αν πληρωθούν οι προϋποθέσεις που έχουν τεθεί. Τα συμβόλαια αυτά υπάρχουν εδώ και πολλά χρόνια στην πιο απλή μορφή τους, όπως για παράδειγμα στη περίπτωση ενός αυτόματου πωλητή, η ενσωμάτωση της λειτουργίας τους μέσα από την τεχνολογία blockchain τους δίνει νέες δυνατότητες. Χαρακτηριστική περίπτωση, αποτελεί ο διακόπτης εκκίνησης (**starter interrupter**), μια συσκευή, που έχει ενσωματωμένο ένα τέτοιο συμβόλαιο, το οποίο εκτελείται αυτόματα σε περίπτωση που παραβιαστούν οι όροι χρηματοδότησης για την απόκτηση του αυτοκινήτου και δεν επιτρέπει την εκκίνηση του κινητήρα. Τα συμβαλλόμενα μέρη σε ένα έξυπνο συμβόλαιο διαπραγματεύονται τους βασικούς όρους, όπως προδιαγραφές των προϊόντων, ποσότητα , τιμή και τόπος εκπλήρωσης. Αν εκατομμύρια υπολογιστές βεβαιώσουν ότι η Αλίκη καταβάλει στον Κώστα το ποσό των 100 ευρώ στην ημερομηνία που έχει συμφωνηθεί, και οι υπολογιστές αυτοί είναι ουδέτεροι και δεν κάνουν υπολογιστικά λάθη, τότε μπορεί κάποιος να υποθέσει με μεγάλο βαθμό βεβαιότητας ότι η πληρωμή πραγματοποιήθηκε. Το Ethereum είναι ένα από τις εφαρμογές που βασίζεται κυρίως στα «έξυπνα συμβόλαια». Η ενσωμάτωση των Smart Contracts με το Blockchain εξαλείφει την ανάγκη για ένα διαμεσολαβητή, ελαχιστοποιώντας τα έξοδα συναλλαγής (προμήθεια)

2.5 Τα μειονεκτήματα του Blockchain

Το Blockchain, θεωρείται μία καινοτομία στον τρόπο με τον οποίο γίνονται οι συναλλαγές, αλλά δεν γίνεται από μία καινοτομία να λείπουν και τα μειονεκτήματα της.
Αυτή η αλυσίδα, εκτός από τα πλεονεκτήματα που έχει, όπως είναι η ανωνυμία, η ασφάλεια κλπ, διαθέτει και κάποια μειονεκτήματα, που συνδέονται με τα πλεονεκτήματα της.

Κόστος ενέργειας

Η χρήση του Blockchain στην εξόρυξη, είναι μία από τις διαδικασίες που χρειάζεται ενέργεια για να πραγματοποιηθεί, και αυτό σε συνδυασμό με την δυσκολία (που ολοένα και αυξάνεται ανά 2016 μπλοκ) της λύσης των προβλημάτων για την δημιουργία καινούργιων μπλοκ.



Εικόνα 11 Κατανάλωση ενέργειας του Bitcoin, **πηγή:** www.digiconomist.net

51% Attack

Ένα από τα μεγαλύτερα προβλήματα, που φοβούνται όσοι συμμετέχουν στο δίκτυο είναι η περίπτωση του **51% Attack,** δηλαδή, ένα άτομο ή μια ομάδα ατόμων (mining pool) να έχει το 51% της επεξεργαστικής ισχύς του δικτύου. Σε μια τέτοια περίπτωση, ο χρήστης θα μπορεί να πραγματοποιεί συναλλαγές με τις ίδιες μονάδες Bitcoin.

Η στρατηγική ενός κακόβουλου χρήστη είναι αρκετά απλή:

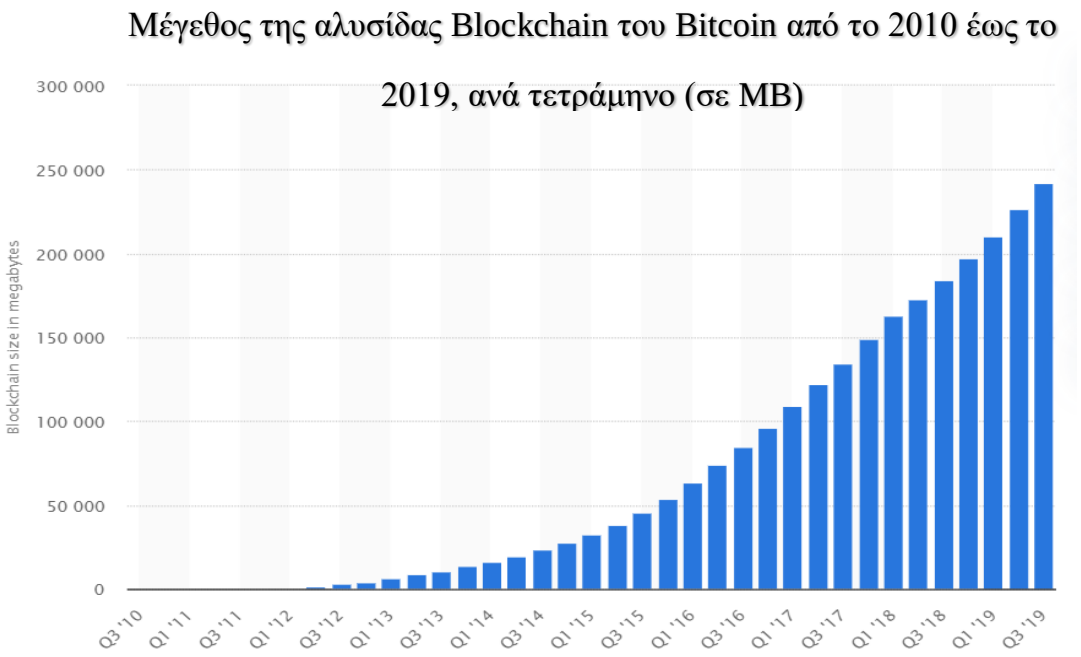
1. Πραγματοποιεί μια αποστολή 100 μονάδων BTC, σε έναν έμπορα σε αντάλλαγμα για ένα προϊόν (κατά προτίμηση, ψηφιακό προϊόν, που η αποστολή του γίνεται άμεσα).
2. Αναμονή για την παραλαβή του προϊόντος.
3. Πραγματοποιεί ακόμη μία συναλλαγή που στέλνει τις ίδιες μονάδες BTC στον εαυτό του.
4. Ο χρήστης προσπαθεί να πείσει το δίκτυο ότι η συναλλαγή προς τον ίδιο, πραγματοποιήθηκε πρώτη.

Όταν πραγματοποιηθεί το πρώτο βήμα, ένας miner θα συμπεριλάβει τη συναλλαγή σε ένα μπλοκ, πχ το μπλοκ με αριθμό 5. Μετά, από περίπου μία ώρα, ακόμη 5 μπλοκ, θα προστεθούν στην αλυσίδα, όπου κάθε καινούργιο μπλοκ θα δείχνει στο 5ο μπλοκ. Σε αυτό το σημείο, ο έμπορος θα αποδεχτεί τη πληρωμή και θα παραδώσει το προϊόν (ψηφιακό). Τώρα ο κακόβουλος χρήστης πραγματοποιεί τη συναλλαγή όπου στέλνει τις ίδιες 100 μονάδες BTC στον εαυτό του. Τώρα, ο χρήστης αρχίζει να δουλεύει σε μία παραλλαγή του 5ο μπλοκ, όπου δείχνει στο 4ο αλλά με μία νέα συναλλαγή αντί της αρχικής. Αλλά, επειδή τα δεδομένα άλλαξαν, θα πρέπει να ξανά υπολογιστεί, η ταυτότητα (hash) του μπλοκ, δηλαδή να ξανά επαναληφθεί η διαδικασία του PoW (Proof of Work). Τα επόμενα μπλοκ που είχαν δημιουργηθεί, δεν δείχνουν στο νέο 5ο μπλοκ, αλλά δείχνουν στον αρχικό 5ο. Άρα, η αρχική αλυσίδα, με την καινούργια αλυσίδα που δημιούργησε ο χρήστης είναι ξεχωριστές. Ο κανόνας της αλυσίδας είναι, ότι η μεγαλύτερη αλυσίδα (δηλαδή αυτή που έχει υποστεί μεγαλύτερη επεξεργαστική ισχύ) είναι η αληθής και, άρα οι miners, θα συνεχίζουν να εργάζονται στο 10ο μπλοκ, όπου ο χρήστης θα δουλεύει στο

καινούργιο 5ο μπλοκ. Για να κάνει ο χρήστης την αλυσίδα του μεγαλύτερη, θα πρέπει να έχει μεγαλύτερη επεξεργαστική ισχύ από τους υπόλοιπους που συμμετέχουν μαζί, ώστε να το πετύχει. [19]

Τώρα η διαδικασία της εξόρυξης (mining) δεν είναι δουλεία ενός ατόμου, αλλά πολλών (mining pool), αφού η δυσκολία αυξάνεται ανά 2016 μπλοκ, και οι απαιτήσεις της επεξεργαστικής ισχύς είναι μεγάλες (32,798 PH/s), όσο αφορά το Bitcoin, σε άλλα νομίσματα η επεξεργαστική ισχύ που χρειάζεται είναι μικρότερη από αυτή του Bitcoin. Για παράδειγμα, στη περίπτωση του Ethereum, χρειάζεται περίπου 213 TH/s.
Μία ομάδα χρηστών (Gash.io) κατάφερε να φτάσει σχεδόν το 51% του δικτύου Bitcoin τον Ιανουάριο του 2014, και αυτό έφερε μια αναστάτωση στην κοινότητα, αλλά διορθώθηκε σύντομα όταν μερικά άτομα αποχώρησαν ώστε να επέλθει μια ισορροπία.

Χώρος αποθήκευσης
Η αλυσίδα με τον καιρό, μεγαλώνει αρκετά. Είναι ένα φαινόμενο, που θα αποτελέσει πρόβλημα για τους miners στο μέλλον. Στην Εικόνα 12, φαίνεται το διάγραμμα του μεγέθους της αλυσίδας από το 3ο τετράμηνο του 2010 μέχρι το 3ο τετράμηνο του 2019.



Εικόνα 12 Μέγεθος του Blockchain, **πηγή:** www.statista.com

Στην παραπάνω εικόνα βλέπουμε, ότι μετά το 3ο τετράμηνο του 2012 αρχίζει να αυξάνεται με γρήγορους ρυθμούς το μέγεθος της αλυσίδας, και αυτό εξάλλου φαίνεται αφού το 3ο τετράμηνο το μέγεθος ισούταν με 1 MB ενώ το 3ο τετράμηνο του 2019 έφτασε 242,3 GB. Με τον συγκεκριμένο ρυθμό εξόρυξης του Bitcoin και σε συνδυασμό ότι ανά 210,000 μπλοκ, η αμοιβή κάθε νέου μπλοκ μειώνεται στο μισό, εκτιμάται ότι και τα 21 εκατομμύρια Bitcoin που είναι και

το όριο που όρισε ο δημιουργός του, θα έχουν παραχθεί μέχρι το 2140, άρα το μέγεθος της αλυσίδας θα αποτελέσει πρόβλημα για τους miners στο μέλλον.

Μη αποδοτικό

Τα Blockchain, ειδικά αυτά που χρησιμοποιούν PoW (Proof of Work), είναι εξαιρετικά μη αποδοτικά. Και αυτό, γιατί η διαδικασία της εξόρυξης είναι ανταγωνιστική, και αφού ανά 10 λεπτά μόνο ένας καταφέρνει, να προσθέσει ένα νέο μπλοκ, άρα να πάρει και τις μονάδες BTC, αυτό σημαίνει ότι η δουλειά των υπολοίπων θεωρείται αποτυχημένη. Καθώς τα άτομα που συμμετέχουν στην διαδικασία της εξόρυξης, προσπαθούν να αυξήσουν την επεξεργαστική ισχύ, ώστε να έχουν περισσότερες πιθανότητες να λάβουν την ανταμοιβή ενός νέου μπλοκ, έχει ως αποτέλεσμα οι πόροι που χρησιμοποιούνται από το Bitcoin να αυξάνονται συνεχώς, και να αυξάνεται η κατανάλωση ενέργειας, όπως έχει αναφερθεί και παραπάνω.

Τροποποίηση δεδομένων

Η τροποποίηση δεδομένων αν και είναι ένα από τα πλεονεκτήματα του Blockchain, δεν είναι πάντα καλή. Τροποποιώντας τα δεδομένα ή των κώδικα της αλυσίδας είναι συνήθως αναγκαίο και συνήθως είναι απαραίτητη μια διαδικασία που ονομάζεται hard fork.

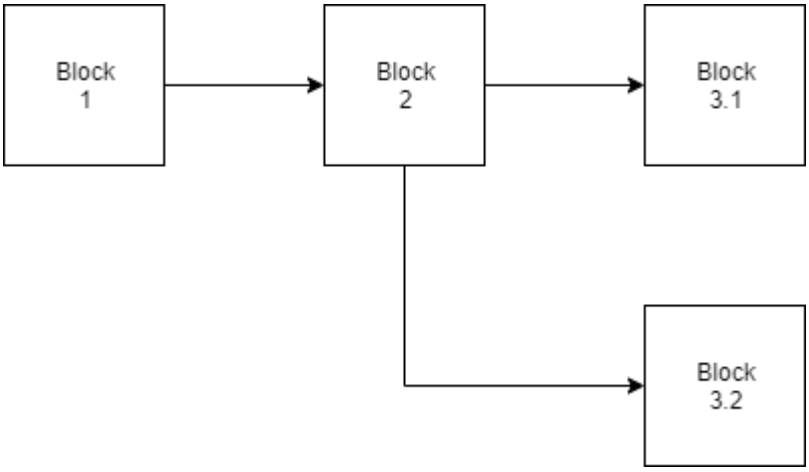
Αυτή η διαδικασία αναφέρεται στο ότι όταν ένα σύστημα έχει μια καινούργια έκδοση και δεν είναι συμβατή με την παλαιά έκδοση, οι κόμβοι με την παλιά έκδοση δεν συμφωνούν με τους νέους κανόνες και άρα, αντί για μία υπάρχουν δύο αλυσίδες. Παρόλο, που η επεξεργαστική ισχύ των κόμβων με τη καινούργια έκδοση είναι μεγαλύτερη από αυτών με την παλιά έκδοση, θα συνεχίσουν να διατηρούν την παλιά αλυσίδα. Όταν, συμβαίνει η διαδικασία του hard fork, πρέπει να σταλεί ένα αίτημα, σε όλους του κόμβους του δικτύου, να κάνουν την αναβάθμιση, οι κόμβοι που δεν θα προβούν στην αναβάθμιση δεν θα μπορούν να συνεχίσουν να δουλεύουν όπως συνήθως. Αν υπήρχαν περισσότεροι, που ακολουθήσαν την παλιά έκδοση, θα συνέχιζαν να δουλεύουν σε μια διαφορετική αλυσίδα. [20]

2.5.1 *Fork*

Το blockchain διατηρείται από ένα αποκεντρωμένο δίκτυο υπολογιστών, είναι δυνατόν να υπάρχουν περισσότεροι κόμβοι στο δίκτυο που λύνουν ανεξάρτητα το μαθηματικό πρόβλημα ώστε να κερδίσουν την δυνατότητα να προσθέσουν το επόμενο μπλοκ στην αλυσίδα. Όταν συμβεί αυτό, περισσότεροι κόμβοι θα μεταδώσουν το νέο μπλοκ στο δίκτυο, ταυτόχρονα.

Ενώ η επικοινωνία μεταξύ των κόμβων είναι γρήγορη, δεν είναι στιγμιαία, επειδή η γεωγραφική θέση, η δρομολόγηση των πληροφοριών στο διαδίκτυο και η ποιότητα υποδομής μεταφοράς έχουν αντίκτυπο στην ταχύτητα μετάδοσης. Έτσι, η εξάπλωση νέων μπλοκ σε όλο το δίκτυο θα προχωρήσει ανομοιογενώς.

Αυτή, η ανομοιόμορφη εξάπλωση μπορεί να οδηγήσει σε μια κατάσταση όπου πολλαπλοί κόμβοι του δικτύου να έχουν αποδεχθεί ένα νέο μπλοκ, ενώ άλλοι να έχουν λάβει ένα εναλλακτικό νέο μπλοκ από ένα διαφορετικό κόμβο, όπου θα το έχουν αποδεχθεί και στη συνέχεια αυτό το μπλοκ θα προστεθεί στην αλυσίδα.



Εικόνα 13 Αλυσίδα μπλοκ που έχει υποστεί διαχωρισμό

Το λογισμικό του Bitcoin, διαχειρίζεται τον «διαχωρισμό» (forking) του blockchain χρησιμοποιώντας τον ακόλουθο κανόνα, όλοι οι κόμβοι κρατούν ταυτόχρονα όλες τις διακλαδώσεις του blockchain, αλλά εργάζονται μόνο για την επέκταση του κλάδου που περιέχει το νέο μπλοκ, που δέχτηκαν πρώτο. [21]

2.6 Άλλες χρήσεις του Blockchain

Πρώτη αναφορά του Blockchain, έγινε το 1991 από τον Stuart Haber και τον W. Scott Stometta, και έγινε διάσημη αυτή η τεχνολογία, το 2008 από τον Satoshi Nakamoto, που παρουσίασε το Bitcoin, που βασίζεται σε αυτή την τεχνολογία. Αλλά, υπάρχουν και άλλοι τομείς όπου το Blockchain, μπορεί να χρησιμοποιηθεί, όπως για παράδειγμα στα χρηματοοικονομικά, στον τομέα της υγείας, στην κυβέρνηση, και στο εμπόριο και στην παραγωγή. [22]

Διαχείριση Αλυσίδας Εφοδιασμού (SCM)

Η διαχείρισης αλυσίδας εφοδιασμού αποτελεί μια έννοια διαχείρισης των συνολικών ροών ενός καναλιού διανομής. Η αλυσίδα εφοδιασμού είναι σύνθετη επειδή περιλαμβάνει κατανεμημένες δραστηριότητες, που ασχολούνται με ανθρώπους, φυσικούς πόρους και παραγωγικές διαδικασίες, που καλύπτει ολόκληρη την διαδικασία πώλησης, δηλαδή συμβάσεις, πωλήσεις, σε πελάτες, διανομή και διάθεση.

Για τα περιουσιακά στοιχεία (δηλαδή, τα φυσικά περιουσιακά στοιχεία) και για τα άυλα (δηλαδή, τα έγγραφα), είναι σημαντικό να έχουμε ακριβή και αξιόπιστα αρχεία για τον προσδιορισμό της ιδιοκτησίας και για την εξασφάλιση της ορθότητας και την πληρότητα των πολύτιμων πληροφοριών που σχετίζονται με την ιδιοκτησία. Ο περεταίρω έλεγχος των φυσικών περιουσιακών στοιχείων μπορεί να επιτευχθεί με την καταχώρηση και διαπραγμάτευση των ιδιοτήτων μέσω blockchain ως έξυπνη ιδιοκτησία ή διαχείρισης ψηφιακών περιουσιακών στοιχείων. Είναι δυνατόν να επιτευχθεί η ανιχνευσιμότητα μέσω της χρήσης των IoT (Internet of Things). [23]

Ακόμη, ένα από τα κύρια χαρακτηριστικά του blockchain, το οποίο είναι αποκεντρωποιημένο και οι συναλλαγές διανέμονται σε όλους τους συμμετέχοντες, χρησιμεύει στην διαχείριση της εφοδιαστικής αλυσίδας, αφού όλες οι συναλλαγές που σχετίζονται με το κομμάτι αυτό μπορούν να καταχωρηθούν και να επιβεβαιωθούν, συμπεριλαμβανομένης της παραγγελίας, της απογραφής και των προϊόντων.

Σύστημα Υγείας

Η διαρροή δεδομένων στα ηλεκτρονικά αρχεία υγείας, θα μπορούσε να οδηγήσει στην παραβίαση της ιδιωτικής ζωής του ασθενούς. Γενικά, τα περισσότερα ιατρικά αρχεία παραμένουν αμετάβλητα μόλις μεταφορτωθούν στο σύστημα. Έτσι, το blockchain μπορεί να χρησιμοποιηθεί για να διευκολύνει την ανταλλαγή τέτοιων δεδομένων. Διάφορες συμμετέχουσες ιατρικές οργανώσεις και άτομα (π.χ. ιατροί, νοσοκομεία, ιατρικά εργαστήρια και ασφαλιστικές εταιρείες), θα μπορούσαν να έχουν πρόσβαση στα ιατρικά αρχεία των ασθενών που είναι αποθηκευμένα στο blockchain, με μεγαλύτερη εμπιστευτικότητα. [24]

Κυβέρνηση

Ένα χαρακτηριστικό της κυβέρνησης είναι το σύστημα ψηφοφορίας, αφού αποτελεί ένα από τους βασικούς πυλώνες της μοντέρνας δημοκρατίας. Οι δυνατότητες που προσφέρει το blockchain, μπορούν να αξιοποιηθούν από το σύστημα ηλεκτρονικής ψηφοφορίας, αφού η τεχνολογία αυτή προσφέρει, την ακεραιότητα των δεδομένων και ανωνυμία. [25] Δύο χαρακτηριστικά , σημαντικά για την ψηφοφορία, είναι η ακεραιότητα, αφού κάθε δεδομένο που βρίσκεται στην αλυσίδα είναι δύσκολο να αλλάξει και η ανωνυμία του ψηφοφόρου.

Χρηματοοικονομικά

Η τεχνολογία blockchain μπορεί να μειώσει το κόστος συναλλαγών, να δημιουργήσει κατανεμημένη εμπιστοσύνη, και να ενισχύσει τις αποκεντρωμένες πλατφόρμες, και μπορεί να γίνει μια νέα βάση για το αποκεντρωμένο επιχειρηματικό μοντέλο. Στον χρηματοπιστωτικό κλάδο, η τεχνολογία blockchain επιτρέπει την ανάπτυξη αποκεντρωμένων χρηματοπιστωτικών υπηρεσιών, οι οποίες τείνουν να είναι περισσότερο αποκεντρωμένες και χωρίς σύνορα. Με την τεχνολογία αυτήν, οι αποκεντρωμένες χρηματοπιστωτικές υπηρεσίες έχουν την δυνατότητα να διευρύνουν την οικονομική ένταξη, την ανοικτή πρόσβαση και να ενθαρρύνουν τους επιχειρηματίες να δημιουργήσουν νέες ευκαιρίες. [26]

3 Ψηφιακά νομίσματα

3.1 Τι είναι το ψηφιακό νόμισμα

Καθ' όλη τη διάρκεια της ιστορίας υπήρξαν διαφορετικές εκδοχές του χρήματος, και φυσικές και ηλεκτρονικές. Οι οικονομολόγοι προσδιορίζουν τα χρήματα μέσω των ρόλων που εξυπηρετούν στην κοινωνία. Συγκεκριμένα, από την οπτική της οικονομικής θεωρίας, χρήμα μπορεί να θεωρηθεί, οτιδήποτε μπορεί να χρησιμεύει ως μέσο ανταλλαγής για την πραγματοποίηση πληρωμών. Μια αξία που έχει τη δυνατότητα για την αγορά προϊόντων και υπηρεσιών από σήμερα μέχρι μια μελλοντική ημερομηνία, και μια μονάδα με την οποία θα μετράμε την αξία οποιοδήποτε αντικειμένου προς πώληση. [27]

Τα κρυπτονομίσματα έχουν παρόμοιες ιδιότητες με τα παραδοσιακά νομίσματα και είναι πιο κοντά με το ηλεκτρονικό χρήμα το οποίο θεωρείται ως εναλλακτικό νόμισμα. Η διαφορά τους έγκειται στο γεγονός ότι τα κρυπτονομίσματα κάνουν χρήση της κρυπτογραφίας ώστε να αποκρύπτουν τις πληροφορίες που σχετίζονται με τις συναλλαγές και την ασφάλεια αυτών. Για την κρυπτογράφηση των δεδομένων χρησιμοποιείται η επιστήμη των μαθηματικών. [28]

Τον Αύγουστο του 2015 πάνω από 600 κρυπτονομίσματα είχαν καταγραφεί ότι υπάρχουν. Το πιο γνωστό είναι το Bitcoin το οποίο κατέχει την υψηλότερη κεφαλαιοποίηση (σύνολο των μονάδων που κυκλοφορούν στην αγορά επί την παρούσα αξία), στη δεύτερη θέση βρίσκεται το Ethereum και στη τρίτη θέση ακολουθεί το Ripple. [28]

Το ψηφιακό νόμισμα περιλαμβάνει, ένα νέο αποκεντρωποιημένο σύστημα πληρωμών και ένα νέο νόμισμα. Όλα τα σχήματα, περιλαμβάνουν ένα δημόσιο «βιβλίο συναλλαγών» (ledger) το οποίο κοινοποιείται σε όσους συμμετέχουν στο δίκτυο. Ένα χαρακτηριστικό που καθορίζει κάθε σχήμα ψηφιακού νομίσματος είναι η διαδικασία, με την οποία οι χρήστες έρχονται σε μια συμφωνία στο βιβλίο συναλλαγών (δηλαδή, ποιες συναλλαγές να αποδεχτούν σαν έγκυρες).

3.2 Τα μεγαλύτερα κρυπτονομίσματα

Πίνακας 1 Τα 7 μεγαλύτερα κρυπτονομίσματα **πηγή: www.coinmarketcap.com**

Έτος κυκλοφορίας	Όνομα	Market Cap 12/02/19 (δις)	Hash Algorithm	Supply	Δημιουργός
2009	Bitcoin	131,356	SHA-256	21 εκατ.	
2013	Ethereum	16,151	Ethash	108 εκατ.	Vitalik Buterin
2012	XRP	9,531	SHA-512	100 δις	Brad Garlinhouse & Chris Larsen
2014	Tether	4,116	SHA-256	4,2 δις	J.R Willet
2017	Bitcoin Cash	3,868	SHA-256	21 εκατ.	Split from Bitcoin
2011	Litecoin	2,919	SHA-256	84 εκατ.	Charlie Lee
2018	EOS	2,550	SHA-256	1 δις.	Daniel Larimer

Στον παραπάνω πίνακα, είναι τα 7 μεγαλύτερα κρυπτονομίσματα που κυκλοφορούν στην αγορά. Η κατάταξη έγινε με το κριτήριο της κεφαλαιαγοράς, που προκύπτει από τις μονάδες που κυκλοφορούν στην αγορά επί την παρούσα αξία (12/02/2019). Τα στοιχεία για την δημιουργία του πίνακα είναι από την σελίδα www.coinmarketcap.com.

Το Bitcoin Cash είναι το αποτέλεσμα της διαδικασίας fork, που αναφέρθηκε πιο πάνω. Το Bitcoin Cash είναι ένα κρυπτονόμισμα που δημιουργήθηκε τον Αύγουστο του 2017, από το αποτέλεσμα της διαδικασίας fork, αυξάνοντας το μέγεθος των block, επιτρέποντας περισσότερες συναλλαγές.

3.3 Εναλλακτικά κρυπτονομίσματα

Τα εναλλακτικά κρυπτονομίσματα αποτελούν αποτελέσματα της αντιγραφής ενός μέρους του κώδικα του Bitcoin, με κάποιες αλλαγές. Αφού, ο πηγαίος κώδικας του Bitcoin, εκδίδεται υπό μια άδεια ανοιχτού κώδικα, όπου προγραμματιστές εφαρμόζουν αλλαγές στον κώδικα και εκδίδουν νέα κρυπτονομίσματα. Παρακάτω αναφέρονται μερικά εναλλακτικά κρυπτονομίσματα:

Ethereum (ETH): Το Ethereum είναι ένα έργο που επιχειρεί να χτίσει την γενικευμένη τεχνολογία, στην οποία μπορούν να στηρίζονται όλες οι έννοιες μηχανών βάσει συναλλαγών. Επιπλέον, στοχεύει να παρέχει στον τελικό προγραμματιστή ένα σφιχτά ολοκληρωμένο σύστημα από άκρο σε άκρο για τη δημιουργία λογισμικού σε ένα έως τώρα ανεξερεύνητο πρότυπο υπολογιστών, δηλαδή ένα αξιόπιστο πλαίσιο υπολογιστή ανταλλαγής μνημάτων αντικειμένων. [29] Μια μεγάλη διαφορά του ethereum από το bitcoin είναι ο χρόνος που απαιτείται για την δημιουργία ενός μπλοκ. Στη περίπτωση του bitcoin, όπως αναφέραμε και πιο πάνω, είναι 10 λεπτά ανά μπλοκ, ενώ στη περίπτωση του ethereum, κάθε μπλοκ παράγεται ανά 14 δευτερόλεπτα. [30]
Το Ethereum βασίζεται στην καινοτομία του Bitcoin, με κάποιες μεγάλες διαφορές. Και οι δύο, επιτρέπουν την χρήση των ψηφιακών νομισμάτων χωρίς διαμεσολαβητές, αλλά το ethereum είναι προγραμματιζόμενο, οπότε μπορεί να χρησιμοποιηθεί για πολλά διαφορετικά ψηφιακά στοιχεία – ακόμη και Bitcoin. Αυτό σημαίνει, ότι το ETH είναι κάτι παραπάνω από πληρωμές. Είναι μια αγορά χρηματοοικονομικών υπηρεσιών, παιχνιδιών και εφαρμογών, όπου δεν μπορούν να κλέψουν τα δεδομένα σας. [31]

Litecoin (LTC): Επί του παρόντος, υπάρχουν χιλιάδες κρυπτονομίσματα στην αγορά, είτε ως υποκατάστατα είτε αντίγραφα του Bitcoin, ή ως κάποιο άλλο τύπο παραγώγων. Το LItecoin ή το LTC, ήταν το πρώτο υποκατάστατο του Bitcoin, με μια τροποποιημένη έκδοση του αλγορίθμου (ο λεγόμενος «αλγόριθμος εξόρυξης»). Ως υποκατάστατο νόμισμα, το Litecoin αποτελεί μια εναλλακτική πλατφόρμα που πρέπει να αποκτήσει τη δική του βάση χρηστών. [32]

PeerCoin (PPC): νόμισμα που εισήχθη το 2012. Η κύρια καινοτομία σε αυτό είναι ότι χρησιμοποιεί ένα συνδυασμό του Proof of Stake/Proof of Work. Το Proof of Stake δεν συνεπάγεται στην επίλυση ενός μερικού κατακερματισμού και γι' αυτό δεν απαιτεί μεγάλη κατανάλωση ενέργειας. Και γι' αυτό το λόγο το peercoin αποτελεί το πράσινο εναλλακτικό κρυπτονόμισμα του bitcoin. [14]
Το πρωτόκολλο του Peercoin συνδυάζει κάποιο ποσό τυχαιοποίησης με την ηλικία των νομισμάτων για να επιλέξει αυτόματα το επόμενο άτομο που κόβει ένα μπλοκ. Ένας minter με υψηλή ηλικία νομισμάτων έχει μεγαλύτερη πιθανότητα να κόβει το επόμενο μπλοκ από ένα minter με χαμηλή ηλικία νομισμάτων. Δεν υπάρχουν δύσκολα υπολογιστικά προβλήματα όπως είναι στο Bitcoin. Οι πιθανότητες ενός minter να επιλεγεί ως ο επόμενος που θα προσθέσει ένα νέο μπλοκ εξαρτάται συγκεκριμένα από τον αριθμό των κερμάτων που κρατούνται και τον χρόνο με τη μορφή της ηλικίας και κάποια ποσότητα τύχης. [33]

Namecoin (NMC): αποτελεί και κρυπτονόμισμα και αποκεντροποιημένη αποθήκη κλειδιού/αξίας. Αυτή η αποθήκη χρησιμοποιείται για την υλοποίηση ενός εναλλακτικού Domain Name System (DNS). Το DNS είναι κομμάτι της υποδομής του διαδικτύου που επιτρέπει τη διευθέτηση των διευθύνσεων που διαβάζονται από ανθρώπους σε διευθύνσεις IP. [14]
Το Namecoin μπορεί να θεωρηθεί ως το πρώτο μεγάλος σκέλος των Altcoins, το οποίο δημιουργήθηκε το 2010 και μπορεί να περιγραφεί ως αποκεντρωμένη βάση δεδομένων εγγραφής ονόματος στο blockchain. Με άλλα λόγια, το Namecoin, αντιπροσωπεύει μια διέυθυνση τομέα ανώτατου επιπέδου (LTD) που τελειώνει με το ¨.bit¨, το οποίο μπορεί να αγοραστεί και να πωληθεί, και ως εκ τούτου μπορεί να θεωρηθεί ως είδος κρυπτογράφησης που υποστηρίζεται και ως μη εύχρηστο αλλά εμπορεύσιμο περουσιακό στοχείο. [34]

Freicoin (FRC): εκδόθηκε το 2012. Πρόκειται για ένα εναλλακτικό νόμισμα το οποίο βασίζεται στο Bitcoin με την κύρια διαφοροποίηση ότι έχει τόκο υπερημερίας. Η υπερημερία εφαρμόζεται σαν φόρος στις συναλλαγές που παρακρατεί ένα κλάσμα από τα freicoin. Όπου αυτό το κλάσμα αυξάνεται σύμφωνα με το χρόνο που μεσολάβησε από την τελευταία συναλλαγή που πραγματοποιήθηκε. Δηλαδή, δρα σαν ένα αρνητικό επιτόκιο στους κατόχους νομισμάτων. [14]
Το Freicon εφάρμοσε την έννοια demurrage (ποινή για την κατοχή / αποθήκευση των μονάδων αντί να τα δαπανήσει). Αυτό έγινε για να αντιμετωπιστεί ο ισχυρισμός ορισμένων παραδοσιακών οικονομολόγων ότι ένα αποπληθωριστικό σύστημα (όπως το Bitcoin) θα οδηγούσε σε «αποπληθωριστική σπείρα», καθώς οι άνθρωποι δεν θα ήταν πρόθυμοι να ξοδέψουν τα νομίσματά τους με την ελπίδα ότι η αξία αυτών των νομισμάτων θα αυξηθεί στο μέλλον (στην πραγματικότητα, ωστόσο, οι αυξήσεις τιμών στο Bitcoin συσχετίζονται με τον αυξημένο, και όχι μειωμένο αριθμό συναλλαγών). Στο Freicoin, το τέλος αποζημίωσης είναι περίπου 5% ετησίως, δηλαδή εάν ένας χρήστης διαθέτει 100 Freicoins και δεν τις μετακινεί για ένα χρόνο, αφού περάσει το έτος, θα είχαν απομείνει 95 Freicoins. [35]

Primecoin (XMP): εκδόθηκε το 2013. Η κύρια καινοτομία που παρουσιάστηκε από το primecoin είναι, ότι η λειτουργία Proof of Work παράγει χρήσιμα επιστημονικά αποτελέσματα. Αυτό έρχεται σε αντίθεση με τις περισσότερες λειτουργίες του Proof of Work, όπως είναι το SHA256, όπου τα αποτελέσματα δεν έχουν καμία αξία εκτός από την εξασφάλιση της ασφάλειας του blockchain. [14]
Η βελτίωση του Primecoin είναι ένας αλγόριθμος για τη μετατροπή χωρίς νόημα κατακερματισμού σε μια ουσιαστική αναζήτηση μεγάλων αριθμών πρώτου αριθμού κατά την αναζήτηση Nonce. Αναμένεται να φέρει κάποιες επιστημονικές συνεισφορές στους μαθηματικούς ακαδημαϊκούς. Εστιάζοντας στον αυξανόμενο συγκεντρωτισμό της υπολογιστικής ισχύος που προκαλείται από τις εξορύξεις ASIC (Application Specific Integrated Circuit). [36]

Auroracoin (AUR): εκδόθηκε το Φεβρουάριο του 2014. Πρόκειται για μια διακλάδωση του Litecoin. Η βασική του καινοτομία δεν είναι στο τεχνικό κομμάτι, αλλά στην κατανομή του νομίσματος. Το 50% των μονάδων του Auroracoin, είχε προ-εξορυχθεί, δηλαδή το 50% του συνόλου της προσφοράς είχε ήδη δημιουργηθεί. Το υπόλοιπο 50% θα διανεμόταν ως ανταμοιβή στους miners. [14]
Το Auroracoin προοριζόταν να χρησιμεύσει ως μηχανισμός διασυνοριακών μεταφορών στην τοπική οικονομία. Η αξία του κρυπτονομίσματος έπεσε αμέσως μετά την έναρξη του Μαρτίου

2014 και θεωρήθηκε «αποτυχημένο πείραμα». Όμως, η Auroracoin αναβίωσε το 2016 από μια ομάδα προγραμματιστών που διεύρυνε το πεδίο των λειτουργιών της ώστε να συμπεριλαμβάνει καθημερινές συναλλαγές. Διοικείται από το ίδρυμα Auroracoin, το οποίο ιδρύθηκε το 2015. [37]

4 Βασικές έννοιες του Bitcoin

4.1 Πορτοφόλι Bitcoin (e-Wallet)

Το λογισμικό που βοηθά έναν χρήστη να διαχειριστεί τις μονάδες Bitcoin ονομάζεται πορτοφόλι. Οι λειτουργίες του λογισμικού (πορτοφόλι) είναι να κρατάει ασφαλή τα ιδιωτικά κλειδιά του χρήστη, να δημιουργεί συναλλαγές, οι οποίες στέλνονται στο δίκτυο, και να συλλέγουν εισερχόμενες και εξερχόμενες συναλλαγές για να εμφανίζουν το υπόλοιπο των διαθέσιμων μονάδων στον χρήστη. Ένας χρήστης μπορεί να κατέχει πολλές διευθύνσεις, τα περισσότερα πορτοφόλια μπορούν να διαχειριστούν πολλαπλές διευθύνσεις συγκεντρώνοντας τα κεφάλαια σε αυτά.

Για να αποθηκεύσει κάποιος μονάδες Bitcoin σε μια συσκευή, θα πρέπει να κάνει εγκατάσταση του λογισμικού Bitcoin αλλά και ενός πορτοφολιού (e-wallet), σε μια συσκευή, είτε αυτή είναι μια κινητή συσκευή (Android or iOS) ή ένας ηλεκτρονικός υπολογιστής. Υπάρχουν διάφορα πορτοφόλια για κάθε είδος με την έννοια, ότι μερικά είναι πιο αποτελεσματικά για την ασφάλεια, που είναι ένα σημαντικό χαρακτηριστικό, αφού μιλάμε για ένα κρυπτονόμισμα, άλλα είναι καλύτερα για κινητές συσκευές κ.ο.κ.

Ένα πορτοφόλι Bitcoin, είναι σαν ένα φυσικό πορτοφόλι, που κουβαλάει κάθε άνθρωπος μαζί του καθημερινά, όπου μπορεί ο χρήστης να δει, να κοινοποιήσει, αλλά και να κάνει χρήση των διαθέσιμων μονάδων που υπάρχουν στο πορτοφόλι. Ο χρήστης έχει πρόσβαση στο πορτοφόλι, και μπορεί να πληρώσει ή να κάνει μια συναλλαγή με κάποιον άλλον χρήστη, όπως με ένα φυσικό πορτοφόλι. Ο χρήστης ακόμη, θα χρειαστεί και μια διεύθυνση Bitcoin, η οποία είναι παρόμοια με ένα όνομα ή μια ταυτότητα, που πιστοποιεί την ταυτότητα του χρήστη.

Το λογισμικό Bitcoin, δημιουργεί ένα ζεύγος κλειδιών, ένα ιδιωτικό κλειδί, που το γνωρίζει μόνο ο χρήστης, και το δημόσιο κλειδί, που χρησιμοποιείται για μια συναλλαγή που θέλει να πραγματοποιήσει. Το δημόσιο κλειδί είναι παρόμοιο με τον λογαριασμό της τράπεζας. Κάθε δημόσιο κλειδί είναι μοναδικό και το δημοσιεύει σε κάποιον, ώστε να γνωρίζει που να στείλει τις μονάδες.

Κάθε δημόσιο κλειδί δημιουργείται με την δημιουργία του πορτοφολιού αλλά και μετά από κάθε νέα συναλλαγή. Αυτό γίνεται, γιατί η συχνή δημιουργία δημόσιου κλειδιού διατηρεί την ανωνυμία στο δίκτυο. Αλλά, μπορεί ακόμη να χρησιμοποιηθεί το ίδιο δημόσιο κλειδί όσες φορές το επιθυμεί ο χρήστης.

4.1.1 *Ασφάλεια του ηλεκτρονικού πορτοφολιού*

Μία από τις κύριες απειλές για το Bitcoin, είναι η δυνατότητα διατήρησης της αξίας για τους κατόχους. Στο παρελθόν, πολλοί κάτοχοι Bitcoin υπήρξαν θύματα διαδικτυακής απάτης, που είχε σαν αποτέλεσμα να χάσουν τις μονάδες Bitcoin. Τα κλασικά νομίσματα μπορούν να τα προστατέψουν οι κάτοχοι τους εναντίον των ληστών κρύβοντάς τα (π.χ κάτω από το πάπλωμα, σε ένα χρηματοκιβώτιο) ή σε μια τράπεζα. Το Bitcoin είναι ένα ψηφιακό νόμισμα και έτσι δεν μπορεί να προστατευθεί με τους κλασικούς τρόπους, αντιθέτως αποθηκεύονται σε ψηφιακά πορτοφόλια. [38]

Με την δημιουργία ηλεκτρονικού πορτοφολιού, είναι σημαντικό και η δημιουργία ενός αντίγραφου ασφάλειας, ώστε ο χρήστης να έχει πρόσβαση στο πορτοφόλι και κατ' επέκταση στο περιεχόμενο του. Το πορτοφόλι δημιουργεί μια σειρά από 12 τυχαίες λέξεις (seed phrase ή recovery seed), όπου η κάθε λέξη αντιστοιχεί σε έναν αριθμό. Τα περισσότερα ηλεκτρονικά πορτοφόλια προτείνουν για λόγους ασφάλειας, αυτή η φράση να αποθηκευτεί χειρόγραφα και όχι σε ένα ψηφιακό έγγραφο.

Όπως κάθε λογαριασμό που διατηρεί κάθε χρήστης σε διαφορετικές ιστοσελίδες στο διαδίκτυο με ευαίσθητο περιεχόμενο (πχ. E-banking), το ίδιο αποτελεί και το ηλεκτρονικό πορτοφόλι, που περιέχει τις μονάδες Bitcoin, η ασφάλεια θα πρέπει να είναι όσο το δυνατόν μεγαλύτερη, ώστε να αποφευχθεί οποιαδήποτε προσπάθεια εισόδου ενός κακόβολου χρήστη. Κάθε χρήστης για να έχει πρόσβαση στο λογαριασμό του, συνήθως εισάγει κάποια δεδομένα, που μόνο ο ίδιος γνωρίζει, τις περισσότερες φορές αυτά είναι, το «όνομα χρήστη ή την ηλεκτρονική του διεύθυνση (e-mail)» και τον «κωδικό», που είναι γνωστά μόνο από τον ίδιο τον χρήστη.

Όπως θα διατηρούσε ο καθένας το φυσικό του πορτοφόλι ασφαλής, έτσι γίνεται το ίδιο με το ηλεκτρονικό πορτοφόλι. Υπάρχουν, διάφοροι τρόποι να διατηρήσει κάποιος την ασφάλεια του ηλεκτρονικού του πορτοφολιού.

Αποφυγή της αποθήκευσης των εφεδρικών στοιχείων ψηφιακά
Ο καλύτερος τρόπος για την αποθήκευση τέτοιου είδους δεδομένα, είναι σε ένα χαρτί. Πρέπει ακόμη, να αποφεύγεται η λήψη φωτογραφίας μέσω κινητής συσκευής, γιατί κάθε κινητή συσκευή είναι μόνιμα συνδεδεμένη στο διαδίκτυο.

Όταν είναι δυνατόν, να επιλέγεται τον έλεγχο ταυτότητας δύο παραγόντων (2 – FA)
Συνήθως, η είσοδος στον λογαριασμό, δεν γίνεται μόνο από μία συσκευή αλλά από περισσότερες. Με τον έλεγχο ταυτότητας δύο παραγόντων, ο κακόβουλος χρήστης δεν μπορεί να έχει πρόσβαση στον λογαριασμό, μόνο με την χρήση του κωδικού. Για την πρόσβαση στο πορτοφόλι, χρειάζεται ακόμη ένας κωδικός που αποστέλλεται μέσω ενός SMS στη κινητή συσκευή στον αριθμό που έχει εισάγει ο χρήστης για την ενεργοποίηση του διπλού ελέγχου.

4.1.2 *Διαχείριση κλειδιού για το πορτοφόλι Bitcoin*
Όπως έχει αναφερθεί, το ηλεκτρονικό πορτοφόλι είναι παρόμοιο με το φυσικό πορτοφόλι που έχει μαζί του κάθε άνθρωπος στη καθημερινή ζωή του.

Η ασφάλεια κάθε πορτοφολιού εξαρτάται από το πως ο καθένα προστατεύει το ιδιωτικό κλειδί, το οποίο η κλοπή του με οποιονδήποτε τρόπο θα έχει σαν αποτέλεσμα ο κακόβουλος χρήστης να αφαιρέσει όλες τις μονάδες Bitcoin από το πορτοφόλι του νόμιμου ιδιοκτήτη. Υπάρχουν διάφοροι τρόποι διαχείρισης κλειδιού για την ασφάλεια του πορτοφολιού.

Αποθήκευση κλειδιού στον τοπικό δίσκο

Με αυτό τον τρόπο τα κλειδιά αποθηκεύεται στον τοπικό δίσκο, τα οποία είναι προσβάσιμα από το λογισμικό bitcoin. Τα πλεονεκτήματα είναι η εύκολη και γρήγορη πρόσβαση για οποιαδήποτε συναλλαγή, αλλά δεν είναι ασφαλές από έναν κακόβουλο χρήστη ή λογισμικό.

Πορτοφόλι που προστατεύεται με κωδικό

Με αυτό τον τρόπο τα κλειδιά προστατεύονται με έναν κωδικό. Μπορούν να χρησιμοποιηθούν από το λογισμικού του Bitcoin μόνο και αν, εισαχθεί ο σωστός κωδικός. Και σε αυτήν την περίπτωση ένας κακόβουλος χρήστης με την χρήση κατάλληλου λογισμικού να αποκτήσει τον κωδικό προστασίας ή ο ιδιοκτήτης να ξεχάσει τον κωδικό. Και τα δύο οδηγούν στο ίδιο αποτέλεσμα, στην μη χρήση των μονάδων bitcoin.

Αποθήκευση κλειδιών εκτός σύνδεσης

Ένας κακόβουλος χρήστης σε αυτή την περίπτωση, δεν μπορεί να κλέψει το κλειδί. Αφού αποθηκεύονται σε συσκευές που δεν είναι συνδεδεμένες με το διαδίκτυο, όπως είναι ένα USB ή σε μια μορφή χαρτοφυλακίου. Το μειονέκτημα είναι, ότι το πορτοφόλι δεν είναι άμεσα προσβάσιμο.

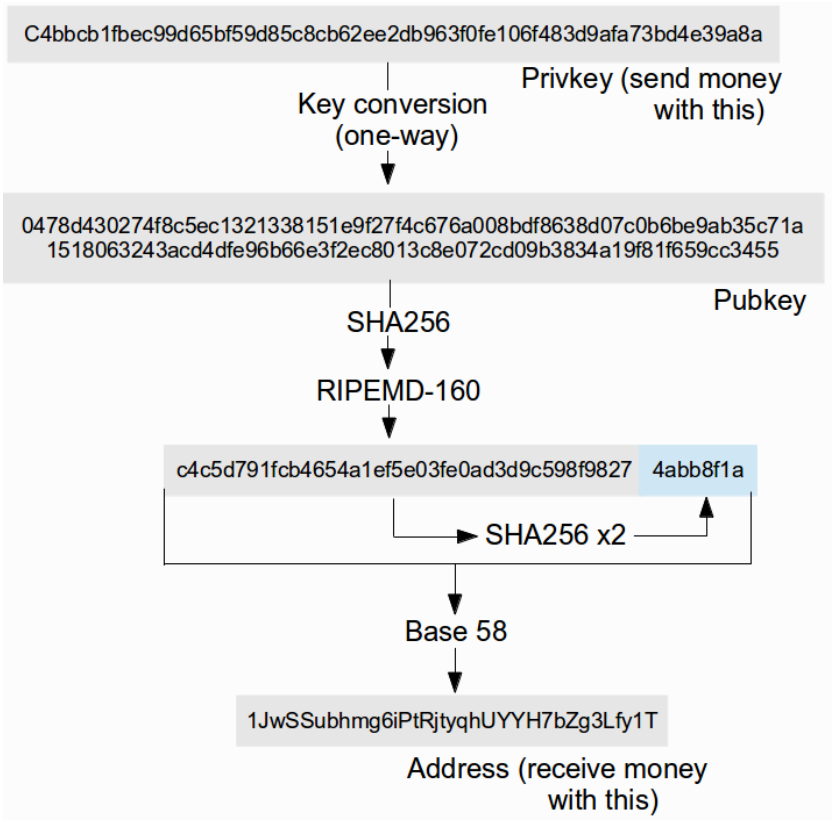
Φιλοξενούμενο πορτοφόλι

Στη περίπτωση αυτή, τα στοιχεία λογαριασμού του χρήστη, φιλοξενούνται από τον διακομιστή τρίτου. Γίνεται χρήση διαδικτυακού μηχανισμού ταυτοποίησης, ώστε ο χρήστης να έχει πρόσβαση στο ηλεκτρονικό πορτοφόλι του. Είναι σκόπιμο να διατηρείται ένα μικρό ποσό σε αυτά τα πορτοφόλια, επειδή η ασφάλεια του πορτοφολιού γίνεται από τρίτο. [39]

4.2 Bitcoin Address

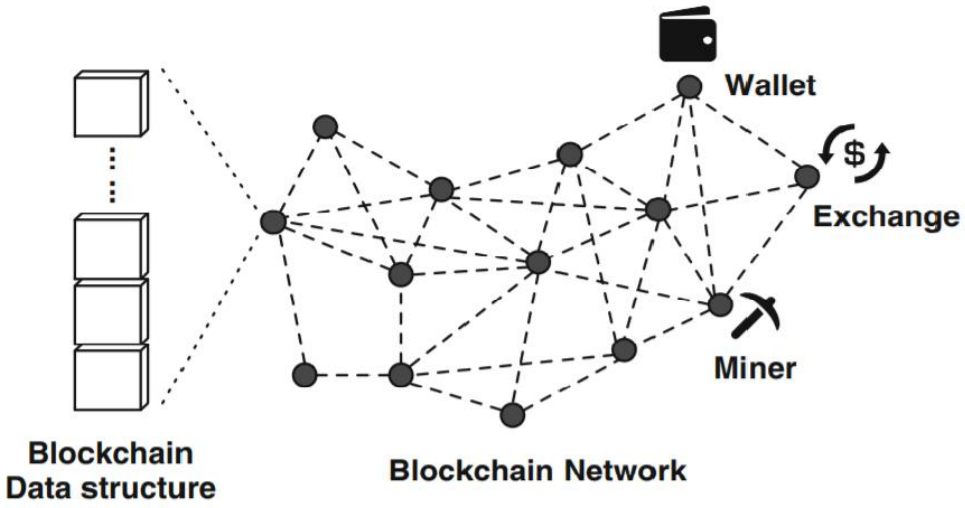
Για την πραγματοποίηση μιας συναλλαγής, ο χρήστης παράγει το δημόσιο και ιδιωτικό κλειδί χρησιμοποιώντας το πρόγραμμα πορτοφολιού που είναι εγκατεστημένο στον υπολογιστή. Το αρχείο δεδομένων του πορτοφολιού κρατάει την διεύθυνση bitcoin (Bitcoin Address), η οποία είναι μια hash τιμή 160-bit του δημόσιου κλειδιού (public key).

Όπως είναι γνωστό, το δημόσιο κλειδί, παράγεται από το ιδιωτικό κλειδί. Τότε το δημόσιο κλειδί (ΔΚ), κατακερματίζεται (hashed) χρησιμοποιώντας την λειτουργία sha-256 και το αποτέλεσμα ξαναπερνάει την ίδια διαδικασία αλλά με την λειτουργία RIPEMD-160, που είναι μια κρυπτογραφική λειτουργία κατακερματισμού που παράγει μια τιμή 160-bit, τότε ξανά περνάει από την λειτουργία SHA-256, η τιμή αυτή (RIPEMD-160).



Εικόνα 14 Διεύθυνση Bitcoin, πηγή: www.bitcoinnotbombs.com

Checksum είναι τα 4 byte που βρίσκονται στο τέλος αριστερά, του αποτελέσματος της διπλής λειτουργίας SHA-256, τα οποία μπαίνουν στο τέλος του αποτελέσματος της λειτουργίας RIPEMD-160, το οποίο μετά μετατρέπεται σε ένα αλφαριθμητικό base58, το οποίο είναι μια ομάδα σχημάτων κωδικοποίησης δυαδικών προς κείμενο που χρησιμοποιούνται για να αντιπροσωπεύουν μεγάλους ακέραιους αριθμούς ως αλφαριθμητικό κείμενο, που εισήγαγε ο Satoshi Nakamoto, για τη χρήση του Bitcoin, χρησιμοποιώντας την κωδικοποίηση Base58Check. Αυτή η μορφή της διεύθυνσης Bitcoin αναφέρεται ως Base58Check διεύθυνση. Το πορτοφόλια Bitcoin ελέγχουν την εγκυρότητα της διεύθυνσης πριν από κάθε συναλλαγή. Οι διευθύνσεις περιέχουν ενσωματωμένο κώδικα ελέγχου, γεγονός που την καθιστά ανθεκτική στα τυπολογικά λάθη. [3]



Εικόνα 15 Επισκόπηση ενός συστήματος Bitcoin, πηγή**: [17]**

Στην Εικόνα 15 παρουσιάζεται μια επισκόπηση του συστήματος Bitcoin. Στο σύστημα Bitcoin υπάρχει ένας κατανεμημένος ρόλος (ledger) που αποθηκεύει όλες τις συναλλαγές Bitcoin. Το περιεχόμενο του ημερολογίου (ledger) αντιγράφεται σε πολλούς γεωγραφικά κατανεμημένους κόμβους εντός του δικτύου Bitcoin.

4.3 Εξόρυξη (Mining)

Υπάρχουν διάφοροι τρόποι για να αποκτήσει κάποιος μονάδες BTC, υπάρχουν διαθέσιμα ανταλλακτήρια, όπου ο καθένας μπορεί να μετατρέψει χρήματα σε Bitcoin, ένας ακόμη τρόπος είναι να σου μεταφέρουν Bitcoin, αλλά ο πιο γνωστός τρόπος για την απόκτηση αυτού του κρυπτονομίσματος είναι η διαδικασία της εξόρυξης (mining).

Οι miners είναι αυτοί που εκτελούν την διαδικασία της εξόρυξης, οι οποίοι λύνουν υπολογιστικά προβλήματα, όπου η δυσκολία των προβλημάτων αυξάνεται ανά 2016 μπλοκ. Η ανταμοιβή κάθε νέου μπλοκ γίνεται με μονάδες Bitcoin.

Για να μπορέσουν να ανταπεξέλθουν στις απαιτήσεις της εξόρυξης, οι miners, πρέπει να έχουν και τον κατάλληλο εξοπλισμό (hardware). Στην αρχή οι απαιτήσεις δεν ήταν μεγάλες, αλλά με τον καιρό όπου η δυσκολία αυξανόταν, χρειαζόταν να βρεθούν νέοι τρόποι.

CPU

Στην αρχή χρησιμοποιούσαν τον κεντρικό επεξεργαστή του υπολογιστή. Αυτός ο τρόπος ήταν ο λιγότερος ισχυρός και πιο αργός για την εξόρυξη με τα σημερινά πρότυπα, και καθώς η δυσκολία της εξόρυξης αυξανόταν το λειτουργικό κόστος του επεξεργαστή υπερέβαινε τα κέρδη από την εξόρυξη.

GPU

Οι κάρτες γραφικών μπορούσαν να ανταπεξέλθουν στις απαιτήσεις της εξόρυξης, αλλά η υψηλή κατανάλωση ενέργειας και η αύξηση των τιμών στις κάρτες γραφικών λόγο της ζήτησης που είχαν, αύξανε τα έξοδα των miners.

FPGA (Field Programmable Gare Arrays)

Οι συσκευές FPGA είναι ένα ολοκληρωμένο κύκλωμα που μπορεί να προσαρμοστεί στις ανάγκες των χρηστών μετά την κατασκευή. Οι miners χρησιμοποιούν αυτά τα τσιπάκια, ώστε να ανταπεξέλθουν στις ανάγκες της εξόρυξης, αφού δουλεύουν πιο αποδοτικά με χαμηλότερη κατανάλωση ενέργειας. Το εύρος της ταχύτητας υπολογισμών είναι πολύ υψηλότερο από τις GPU, περίπου 100 MH/s έως 25 GH/s, συγκριτικά με τις GPU που είναι 200 MH/s έως 2 GH/s. [3]

ASIC (Application-Specific Integrated Circuits)

Η τέταρτη γενιά εμφανίστηκε στις αρχές του 2013 με την εισαγωγή ολοκληρωμένων κυκλωμάτων, που έχουν βελτιστοποιηθεί ώστε να εκτελεί υπολογισμούς hashing όσο τον δυνατόν αποτελεσματικότερα. Τα εργαστήρια Butterfly, ASICMiner και Avalon ήταν οι πρώτες εταιρίες που παρείχαν ASIC συσκευές για την εξόρυξη Bitcoin. Η ASICMiner στη αρχή δεν έστελνε συσκευές ASIC στους πελάτες, αλλά τους έτρεχε στα κέντρα δεδομένων τους ώστε να επωφεληθούν από το συνολικό hash rate του δικτύου. Οι συσκευές είναι ακριβές λόγο της εξειδικευμένης και χρονοβόρας κατασκευής. Οι υπολογισμοί ενός μοναδικού τσιπ κυμαίνονται από 5 GH/s έως 500 GH/s. [40]

Σήμερα, η εξόρυξη γίνεται με μια ομάδα ατόμων, που δουλεύουν στο ίδιο block, και ανταμείβονται ανάλογα με την συνεισφορά τους, στη λύση του προβλήματος (mining pool). Το ίδιο ισχύει και για άλλα κρυπτονομίσματα, όπως είναι το Ethereum και το Monero, αυτά ονομάζονται altcoins, τα εναλλακτικά κρυπτονομίσματα που ξεκίνησαν μετά την δημιουργία του Bitcoin και θεωρούνται καλύτερα υποκατάστατα του Bitcoin. [41]

Υπάρχου δύο εναλλακτικοί τρόπου που μπορεί να κάνει κάποιος εξόρυξη:

Cloud mining

Η εξόρυξη σε αυτή την περίπτωση γίνεται με την ενοικίαση υπολογιστικής ισχύς και η διαδικασία γίνεται σε μια απομακρυσμένη περιοχή. Αυτή η περίπτωση αποτελεί και την πιο οικονομική. Θετικό χαρακτηριστικό, της διαδικασίας αυτής είναι ότι ο χρήστης γλιτώνει χρήματα από την αγορά και την συντήρηση του εξοπλισμού και από την κατανάλωση ηλεκτρικής ενέργειας. Υπάρχει όμως και ένα αρνητικό, οι miners δεν αποτελούν μέλος της διαδικασίας, άρα δεν την ελέγχουν πλήρως και σε συνδυασμό με την μείωση των κερδών από τα έξοδα που επιβάλλονται στις νέες μονάδες Bitcoin, η μέθοδος αυτή δεν παίρνει την πρώτη θέση στη λίστα προτίμησής τους.

Mining pool

Η εξόρυξη αποτελεί μια διαδικασία, η οποία μπορεί να εκτελεστεί είτε μεμονωμένα, είτε συλλογικά. Το επίπεδο δυσκολίας ολοένα και αυξάνεται και παράλληλα αυξάνονται και οι πόροι που χρειάζονται. Και επειδή οι miners μεμονωμένα ξόδευαν πολλούς πόρους αλλά και χρόνο για την εύρεση ενός περιορισμένου αριθμού μπλοκ, οδήγησε στην δημιουργία ομάδων εξόρυξης. Μέσω της εξόρυξης συνεργασίας, διάφοροι miners συμμετέχουν στην επίλυση του ίδιου του προβλήματος και ανταμείβονται ανάλογα με την συνεισφορά τους.

5 Μεθοδολογία

Η τεχνολογία Blockchain λειτουργεί δημιουργώντας ένα περιβάλλον ασφαλές και διαφανές για τις οικονομικές συναλλαγές εικονικών αξιών όπως το Bitcoin. Οι κωδικοί κατακερματισμού κάθε μπλοκ διατηρούν τα αρχεία ασφαλή στο blockchain. Αυτό συμβαίνει κυρίως επειδή, ανεξάρτητα από το μέγεθος των πληροφοριών ή του εγγράφου, η μαθηματική συνάρτηση κατακερματισμού παρέχει έναν κωδικό κατακερματισμού του ίδιου μήκους για κάθε μπλοκ. Έτσι, η απόπειρα αλλαγής ενός μπλοκ πληροφοριών θα δημιουργούσε μια εντελώς νέα τιμή κατακερματισμού.

Ένα δίκτυο που είναι ανοιχτό για όλους και διατηρεί ταυτόχρονα την ανωνυμία των συμμετεχόντων, δημιουργεί προβλήματα εμπιστοσύνης. Για να εξασφαλιστεί αυτή η εμπιστοσύνη, θα πρέπει το κάθε μέλος να περνάει από κάποιους αλγόριθμους, όπως είναι το Proof of Work (PoW).

Το δίκτυο blockchain χρησιμοποιεί μια αποκεντρωμένη δομή που αποτελείται από διασκορπισμένους κόμβους που ελέγχουν και επικυρώνουν την αυθεντικότητα των νέων συναλλαγών που πρόκειται να πραγματοποιηθούν. Αυτή είναι και η διαδικασία της εξόρυξης (mining). Η διαδικασία της εξόρυξης δείχνει ότι κάθε κόμβος έχει περάσει από μια διαδικασία επίλυσης ενός μαθηματικού προβλήματος και αξίζει να λάβει ανταμοιβή ως αντάλλαγμα για την υπηρεσία του. Για την επικύρωση μιας συναλλαγής, το δίκτυο πρέπει να επιβεβαιώσει τις ακόλουθες προϋποθέσεις.

- Ο αποστολέας έχει αρκετές μονάδες BTC για την συναλλαγή που επιθυμεί να πραγματοποιήσει.
- Το ποσό που προορίζεται για μεταφορά δεν έχει σταλεί σε κάποιον άλλον παραλήπτη (double spending).

Μόλις μια συναλλαγή έχει επικυρωθεί από την πλειοψηφία των συμμετεχόντων, τότε προστίθεται στη βάση του blockchain.

Λειτουργία κατακερματισμού (Hash Function): Η συνάρτηση κατακερματισμού λαμβάνει μια είσοδο και επιστρέφει μια έξοδο σταθερού μήκους. Η έξοδος της λειτουργίας κατακερματισμού είναι διαφορετική για κάθε διαφορετικό μήνυμα και ίδια για την ίδια είσοδο. Η συνάρτηση κατακερματισμού έχει ορισμένες εσωτερικές καταστάσεις. Με βάση το μήνυμα που λαμβάνει (input), θα αλλάξει αυτές τις εσωτερικές καταστάσεις. Μέσω παραλλαγών και συνδυασμών, οι εσωτερικές καταστάσεις θα αλλάξουν με τέτοιο τρόπο που το καθιστά αδύνατο να μαντέψει κάποιος το μήνυμα εισόδου από την έξοδο κατακερματισμού. Ο κατακερματισμός ενός μπλοκ στην τεχνολογία blockchain απαιτεί μεγάλη υπολογιστική ισχύ.

5.1 Λειτουργικό δίκτυο συναλλαγών Fabric

Βασικά εργαλεία για να ξεκινήσει ένα πλήρως λειτουργικό δίκτυο συναλλαγών με το Hyperledger Fabric.

Chaincode
Ο κώδικας, που είναι αυτό-εκτελούμενο, κωδικοποιεί τους κανόνες για συγκεκριμένους τύπους συναλλαγών του δικτύου. Μπορεί να γραφτεί σε Java ή σε Go. Αλλά, είναι γραμμένο σε Go, επειδή η γλώσσα Go υποστηρίζεται περισσότερο από την Java. Ο κώδικας που χρησιμοποιείται είναι μια απλή πληρωμή ψηφιακών περιουσιακών στοιχείων από τον λογαριασμό A στον λογαριασμό B. Σκοπός είναι να δημιουργηθεί μια απλή εφαρμογή που βρίσκεται στα χρηματοοικονομικά η οποία δεν είναι πολύ υπολογιστική. Ο λόγος είναι ότι οι εφαρμογές που εκτελούνται αργά στους τοπικούς υπολογιστές θα εκτελούνται πιο αργά σε ένα δίκτυο Hyperledger Fabric.

Java SDK and Hyperledger Fabric
Ένας client έχει δημιουργηθεί για εκτελέσει ένα στρες τεστ, το οποίο περιλαμβάνει: την εγκατάσταση του κώδικα (chaincode), την δημιουργία λογαριασμών και να στείλει χιλιάδες αιτήματα επίκλησης στο δίκτυο. Το αίτημα επίκλησης μετακινεί στοιχεία από τον λογαριασμό A στον λογαριασμό B ή πιο συγκεκριμένα αφαιρεί ένα ποσό X από τον A και προσθέτει το ποσό X στον λογαριασμό του B.

Docker Network Configuration
Το Docker Compose χρησιμοποιείται για την εκκίνηση των containers του Fabric.

Cryptogen-tool
Αυτό το εργαλείο δημιουργεί το κρυπτογραφικό υλικό. Κάθε οντότητα που συμμετέχει στο δίκτυο θα πρέπει να είναι μέλος και αναγνωρίσιμος. Το εργαλείο αυτό δημιουργεί τα πιστοποιητικά και τα κλειδιά για τα μέλη (peers and orderers) ώστε να υπογράφουν ψηφιακά τις συναλλαγές αλλά και να για να αποδεικνύουν ότι αποτελούν μέλη του δικτύου.

Configtxgen-tool
Το δεύτερο εργαλείο χρησιμοποιείται για την δημιουργία του πρώτου μπλοκ (genesis block), της αλυσίδας, για την εκκίνηση του εντολέα (orderer) και για την διαμόρφωση του καναλιού. Το τεχνούργημα διαμόρφωσης του καναλιού το οποίο περιέχει τον ορισμό του δικτύου μας και παρουσιάζει την τοπολογία των στοιχείων του δικτύου.

Endorsement policy
Χρησιμοποιείται για να καθοδηγήσει έναν peer για το πως να αποφασίσει εάν η συναλλαγή έχει εγκριθεί σωστά. Ένα παράδειγμα πολιτικής είναι: AND(‘Org1.member’, ‘Org2.member’) σε αυτή την περίπτωση απαιτείται η υπογραφή ενός μέλους από κάθε οργανισμό, ενώ στην περίπτωση OR(‘Org1.member’, ‘Org2.member’), απαιτείται η υπογραφή από το ένα μέλους είτε του Org1

είτε του Org2. Για κρίσιμες συναλλαγές, π.χ για συναλλαγή διαμόρφωσης καναλιού θα θέλαμε πιθανώς έγκριση από έναν διαχειριστή δηλαδή, AND('Org1.admin', 'Org2.admin').

5.2 Εργαλείο αξιολόγησης Blockchain

Η κοινότητα Hyperledger παρέχει ένα εργαλείο που ονομάζεται ¨Hyperledger Caliper¨, για να ελέγχει την απόδοση των συστημάτων blockchain. Το Caliper, ξεκίνησε για πρώτη φορά από την Huawei τον Μάϊο του 2017. Το Hyperledger Caliper είναι ένα εργαλείο συγκριτικής αξιολόγησης blockchain που επιτρέπει την συνεχή παρακολούθηση των χαρακτηριστικών απόδοσης διαφορετικών συστημάτων blockchain. Επιτρέπει στους χρήστες να δοκιμάζουν διαφορετικές λύσεις blockchain με προκαθορισμένες περιπτώσεις χρήσης και να λαμβάνουν ένα σύνολο αποτελεσμάτων δοκιμών απόδοσης. Τα συστήματα blockchain που υποστηρίζονται επί τους παρόντος είναι: Hyperledger Burrow, Hyperledger Composer, Hyperledger Fabric, Hyperledger Iroha, Hyperledger Sawtooth. Οι δείκτες απόδοσης που υποστηρίζονται είναι: Ποσοστό επιτυχίας (Success Rate), Απόδοση συναλλαγών / ανάγνωσης (Transaction/Read Throughput), καθυστέρηση συναλλαγών / ανάγνωση (transaction / read latency), κατανάλωση πόρων (επεξεργαστή, μνήμη). Μέχρι το Caliper, δεν υπήρχε κανένα γενικό εργαλείο που να παρείχε αξιολογήσεις όσον αφορά τις αποδόσεις για διαφορετικές λύσεις blockchain, με βάση ένα σύνολο ουδέτερων και κοινώς αποδεκτών κανόνων.

Το Hyperledger Caliper παρέχει ένα λειτουργικό εργαλείο συγκριτικής αξιολόγησης που μπορεί να λειτουργήσει με πολλά πλαίσια Hyperledger. Η κοινότητα θα συνεχίσει να καθορίζει περαιτέρω δείκτες απόδοσης και περιπτώσεις αναφοράς. Η επιτυχία του έργου θα εξαρτηθεί από πολλά μέλη της κοινότητας που το χρησιμοποιούν ως εργαλείο αναφοράς.

Η αρχιτεκτονική του Hyperledger caliper περιλαμβάνει ένα **στρώμα προσαρμογής** (Adaptation Layer), **διεπαφή** (Intrerface), το **στρώμα του πυρήνα** (Core Layer), και το **στρώμα της εφαρμογής** (Application Layer). Το προσαρμοστικό στρώμα ενσωματώνει το υπάρχον σύστημα blockchain στο πλαίσιο του Caliper. Ο προσαρμογέας χρησιμοποιεί το SDK ή το RESTful API του blockchain για να εφαρμόσει τα "Caliper Blockchain NBIs". Το δεύτερο και τρίτο στρώμα υλοποιεί βασικές λειτουργίες και παρέχει διασυνδέσεις για εφαρμογές που περιλαμβάνουν: παρακολούθηση πόρων, αναλυτή απόδοσης, την γεννήτρια αναφορών. [9]

Οι περιπτώσεις δοκιμής του Hyperledger Caliper βρίσκονται στον φάκελο "benchmark /", το οποίο γράφεται από τον υπεύθυνο δοκιμών και διαμορφώνονται σε "test.rounds [.callback]" στο αρχείο διαμόρφωσης που καθορίζεται από το "-c". Κάθε υπόθεση δοκιμής περιέχει ένα αρχείο .js (όπως main.js, query.js) που καθορίζει τις συγκεκριμένες λειτουργίες και δύο αρχεία διαμόρφωσης (config.json και fabric.json). Το "config.json" είναι ένα αρχείο διαμόρφωσης αναφοράς, το οποίο καθορίζει τις παραμέτρους της δοκιμής αναφοράς, όπως κύκλους δοκιμών, φόρτο εργασίας κ.λπ. Το "Fabric.json" είναι ένα αρχείο διαμόρφωσης blockchain που καθορίζει τις απαραίτητες πληροφορίες για την αλληλεπίδραση με το Σύστημα που βρίσκεται υπό δοκιμή (SUT), δηλαδή τη διαμόρφωση του δικτύου blockchain, όπως ο αριθμός των μελών, ο αριθμός των πελατών και ούτω καθεξής. Αυτά τα δύο αρχεία διαμόρφωσης είναι πολύ σημαντικά. Το Caliper ελέγχεται σύμφωνα με τις ρυθμίσεις αυτών των δύο αρχείων διαμόρφωσης. Μπορούμε

επίσης να τροποποιήσουμε αυτά τα δύο αρχεία διαμόρφωσης για να προσομοιώσουμε διαφορετικά περιβάλλοντα δοκιμών. Το Caliper παρέχει έναν προεπιλεγμένο σύστημα συγκριτικής αξιολόγησης που είναι ενσωματωμένο και διαμορφώσιμο, καθιστώντας εύκολη την ενσωμάτωση νέων δοκιμών.

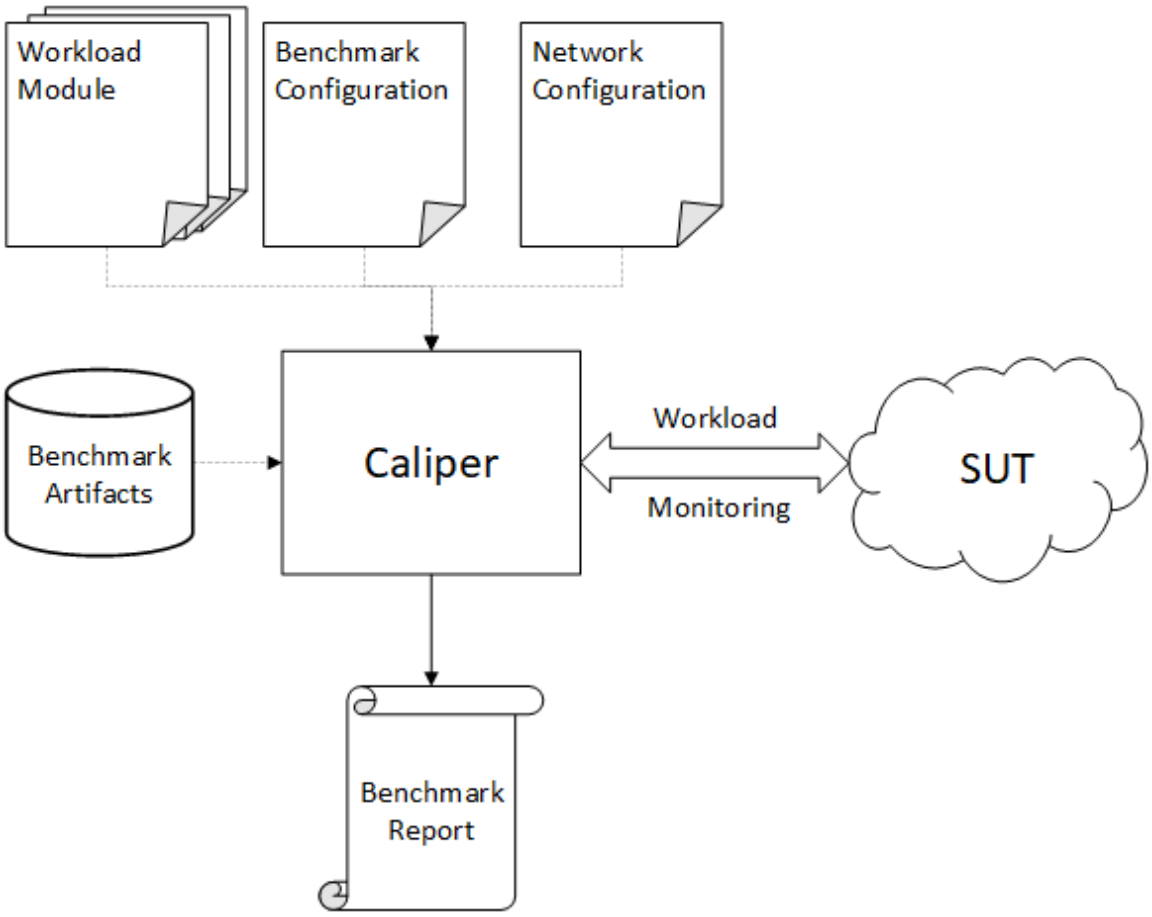
Σενάρια χρησιμότητας του Hyperledger Caliper:

1. Για τους υπεύθυνους λήψης αποφάσεων, που επιλέγουν τεχνολογία blockchain, το Caliper μπορεί να βοηθήσει:
   - Δοκιμή της απόδοσης με συγκεκριμένες περιπτώσεις, για να μάθει ποια ανταποκρίνεται καλύτερα στις ανάγκες του.
   - Μαθαίνει τις απαιτήσεις πόρων (CPU, μνήμης κλπ.) και εκτιμάτε το κόστος για την εγκατάσταση τους συστήματος

2. Για τους χειριστές συστημάτων, το Caliper μπορεί να βοηθήσει:
   - Αξιολόγηση της απόδοσης πολλών συνδυασμών διαμόρφωσης blockchain για την επιλογή του καλύτερου.
   - Γνώση για το πως η κατάσταση του δικτύου θα επηρεάσει την απόδοση.

3. Για προγραμματιστές, το Caliper Μπορεί να χρησιμοποιηθεί ως ένα εσωτερικό εργαλείο για:
   - Για της καλύτερη βελτίωση της απόδοσης μιας νέας έκδοσης.
   - Αξιολόγηση του αντίκτυπου των νέων δυνατοτήτων στην απόδοση.
   - Σύγκριση με άλλα συστήματα blockchain.

Στην πιο απλή μορφή του, το Caliper είναι μια υπηρεσία η οποία δημιουργεί εργασία ενάντια σε ένα συγκεκριμένο σύστημα που βρίσκεται υπό δοκιμή και παρακολουθεί συνεχώς τις αντιδράσεις του. Τέλος, το Caliper δημιουργεί μια αναφορά με βάση τις παρατηρήσεις του συστήματος που βρίσκεται υπό δοκιμή. Αυτό φαίνεται στη παρακάτω Εικόνα.



Εικόνα 16 Απεικόνιση του Caliper, **πηγή**: https://hyperledger.github.io/caliper/

Το Caliper απαιτεί αρκετές εισόδους για να τρέξει μια αξιολόγηση, ανεξάρτητα από το χρησιμοποιημένο SUT. Παρακάτω δίνεται εξήγηση για την κάθε μία είσοδο.

Αρχείο διαμόρφωσης αναφοράς (Benchmark Configuration File)
Το αρχείο διαμόρφωσης αναφοράς περιγράφει τον τρόπο εκτέλεσης της αναφοράς. Λέει στο Caliper, πόσους γύρους θα εκτελέσει και σε ποιο ρυθμό θα υποβληθούν οι συναλλαγές. Περιλαμβάνει επίσης ρυθμίσεις σχετικά με την παρακολούθηση του SUT

Αρχείο διαμόρφωσης δικτύου (Network Configuration File)
Το αρχείο αυτό είναι ειδικά διαμορφωμένο για το SUT. Το αρχείο περιγράφει την τοπολογία του SUT, που βρίσκονται οι κόμβοι, ποιες συσκευές υπάρχουν στο δίκτυο, και ποια έξυπνα συμβόλαια (Smart Contracts) πρέπει το Caliper να αναπτύξει ή να αλληλοεπιδράσει.

Κύκλωμα φόρτου εργασίας (Workload Module)
Είναι ο εγκέφαλος μιας αξιολόγησης. Δεδομένου ότι το Caliper είναι ένα γενικό πλαίσιο αναφοράς, δεν περιλαμβάνει συγκεκριμένη εφαρμογή αναφοράς. Όταν το Caliper προγραμματίζει τις συναλλαγές για έναν συγκεκριμένο γύρο, είναι καθήκον του κυκλώματος του

φόρτου εργασίας του γύρου να δημιουργήσει το περιεχόμενο των συναλλαγών και να το υποβάλει. Κάθε γύρος μπορεί να έχει διαφορετικό φόρτο. [42]

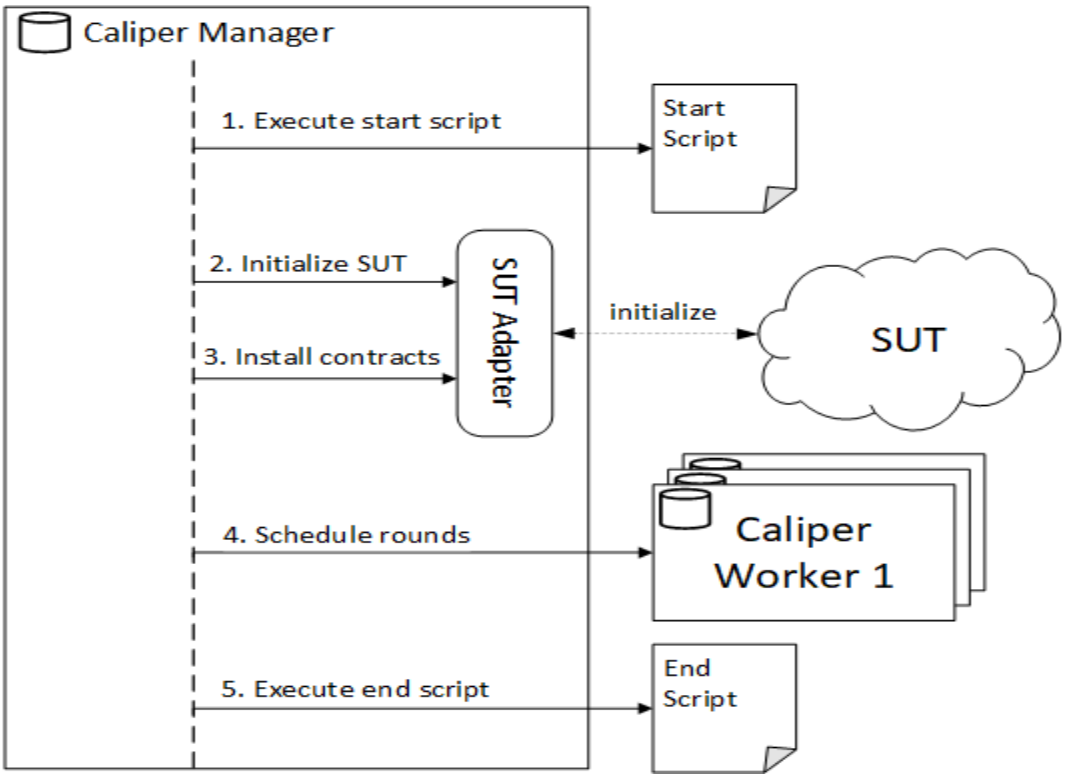
Τεχνικά κριτήρια (Benchmark Artifacts)

Μπορεί να υπάρχουν πρόσθετα αντικείμενα που είναι απαραίτητα για την εκτέλεση μιας αναφοράς που μπορεί να διαφέρει μεταξύ διαφορετικών αναφορών και εκτελέσεων. Αυτά συνήθως περιλαμβάνουν τα ακόλουθα:

- Κρυπτογραφικά υλικά απαραίτητα για την αλληλεπίδραση με το SUT.
- Ο πηγαίος κώδικας των έξυπνων συμβολαίων για Caliper για την ανάπτυξη.
- Αρχεία διαμόρφωσης χρόνου εκτέλεσης
- Προ-εγκατεστημένα πακέτα τρίτων για τα κυκλώματα φόρτου εργασίας.

5.2.1 Η κύρια διαδικασία

Στην παρακάτω εικόνα απεικονίζονται τα στάδια της κύριας διαδικασίας του Caliper.



Εικόνα 17 Στάδια κύριας διαδικασίας, **πηγή**: https://hyperledger.github.io/caliper/

1. Στο πρώτο στάδιο, το Caliper εκτελεί το σενάριο εκκίνησης (start script) εάν αυτό υπάρχει από το αρχείο διαμόρφωσης δικτύου. Αυτό το βήμα είναι κυρίως χρήσιμο για τοπικές εφαρμογές Caliper και του Συστήματος που βρίσκεται σε τεστ (SUT), καθώς παρέχει έναν βολικό τρόπο εκκίνησης του δικτύου και του Caliper σε ένα βήμα.

2. Στο δεύτερο στάδιο, το Caliper εφαρμόζει την αρχικοποίηση του SUT. Οι εργασίες που εκτελούνται εδώ εξαρτώνται σε μεγάλο βαθμό από τις δυνατότητες του SUT και του προσαρμογέα SUT. Για παράδειγμα, ο προσαρμογέας Hyperledger Fabric χρησιμοποιεί αυτό το στάδιο για τη δημιουργία / συμμετοχή καναλιών και την εγγραφή νέων χρηστών.

3. Στο τρίτο στάδιο, το Caliper αναπτύσσει τα έξυπνα συμβόλαια στο SUT, εάν το SUT και ο προσαρμογέας υποστηρίζουν τέτοια λειτουργία (όπως με τον προσαρμογέα Hyperledger Fabric)

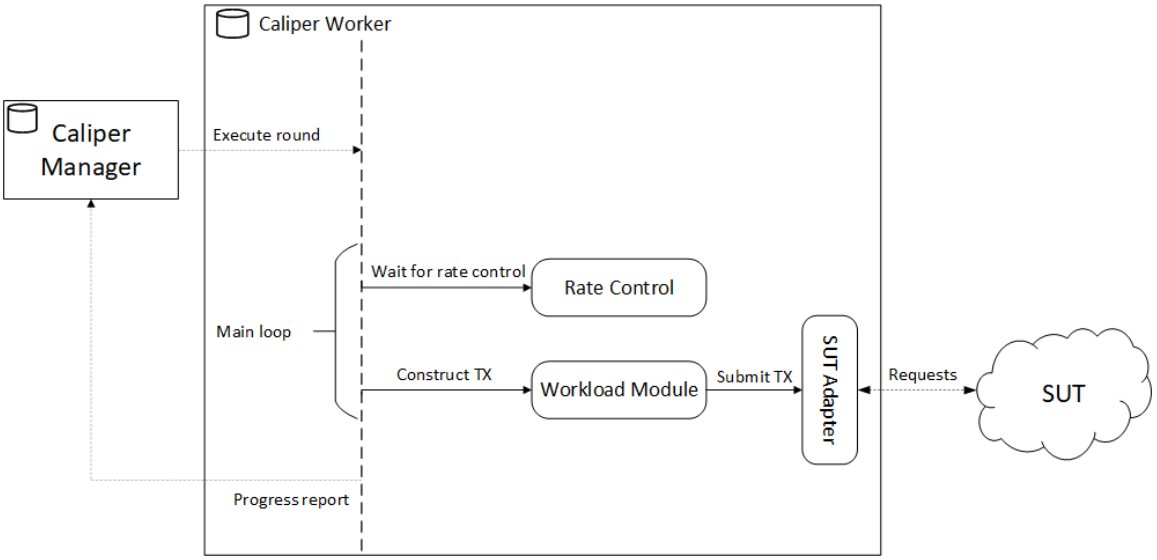
4. Στο τέταρτο στάδιο, το πρόγραμμα Caliper προγραμματίζει και εκτελεί τους διαμορφωμένους γύρους μέσω των διαδικασιών των εργαζομένων. Αυτό είναι το στάδιο όπου δημιουργείται η παραγωγή φόρτου εργασίας (μέσω των εργαζομένων).

5. Στο τελευταίο στάδιο, μετά την εκτέλεση των γύρων και τη δημιουργία της αναφοράς, το Caliper εκτελεί το σενάριο εκκαθάρισης (εάν υπάρχει) από το αρχείο διαμόρφωσης δικτύου. Αυτό το βήμα είναι κυρίως χρήσιμο για τοπικές εφαρμογές Caliper και SUT, καθώς παρέχει έναν βολικό τρόπο για να διαγράψει το δίκτυο και τυχόν προσωρινά αντικείμενα.

Εάν, το SUT, έχει ήδη αναπτυχθεί, τότε χρειάζεται μόνο το Caliper για να γίνει η εκτέλεση των γύρων και τίποτα άλλο.

5.2.2 Η διαδικασία του ¨εργαζομένου¨

Η διαδικασία ξεκινάει από τη στιγμή που η κύρια διαδικασία στέλνει ένα μήνυμα για την εκτέλεση του επόμενου γύρου (Βήμα 4^{ο} από την κύρια διαδικασία). Τα σημαντικά στοιχεία της διαδικασίας των ¨εργαζομένων¨ φαίνεται στην Εικόνα 18.



Εικόνα 18 Η διαδικασία των ¨εργαζομένων¨, **πηγή:** https://hyperledger.github.io/caliper/

Η παραπάνω διαδικασία περνάει τον περισσότερο χρόνο στον βρόχο δημιουργίας φόρτου εργασίας. Ο βρόχος αποτελείται από δύο σημαντικά βήματα:

1. Αναμένει τον ελεγκτή ρυθμού για την ενεργοποίηση της επόμενης συναλλαγής (TX). Ο ελεγκτής ρυθμού έχει τον ρόλο ενός κυκλώματος καθυστέρησης. Με βάση για το τι είδος ελεγκτή ρυθμού χρησιμοποιείται καθυστερεί ή διακόπτη την εκτέλεση του εργαζομένου πριν ενεργοποιηθεί η επόμενη συναλλαγή.

2. Μόλις ο ελεγκτής ρυθμού ενεργοποιήσει την επόμενη συναλλαγή, ο εργαζόμενος δίνει τον έλεγχο στη μονάδα φόρτου εργασίας. Η μονάδα φόρτου εργασίας συγκεντρώνει τις παραμέτρους της συναλλαγής και καλεί την απλή διεπαφή προγραμματισμού εφαρμογών (API) του προσαρμογέα του SUT, που αυτός με την σειρά του θα στείλει το αίτημα για την συναλλαγή στο SUT.

Κατά τη διάρκεια του βρόχου φόρτου εργασίας, η διαδικασία ¨εργαζόμενου¨ στέλνει ενημερώσεις προόδου στην κύρια διαδικασία.

5.3 Μοντέλα διανομής διεργασιών

Διακρίνονται τρία μοντέλα διανομής / ανάπτυξης με βάση τον τρόπο με τον οποίο ξεκινούν οι διαδικασίες εργαζομένων και ποια μέθοδος ανταλλαγής μηνυμάτων χρησιμοποιείται.

1. Αυτόματη αναπαραγωγή διεργασιών εργαζομένων στον ίδιο υπολογιστή με τη χρήση επικοινωνίας μεταξύ διεργασιών (Interprocess communication)

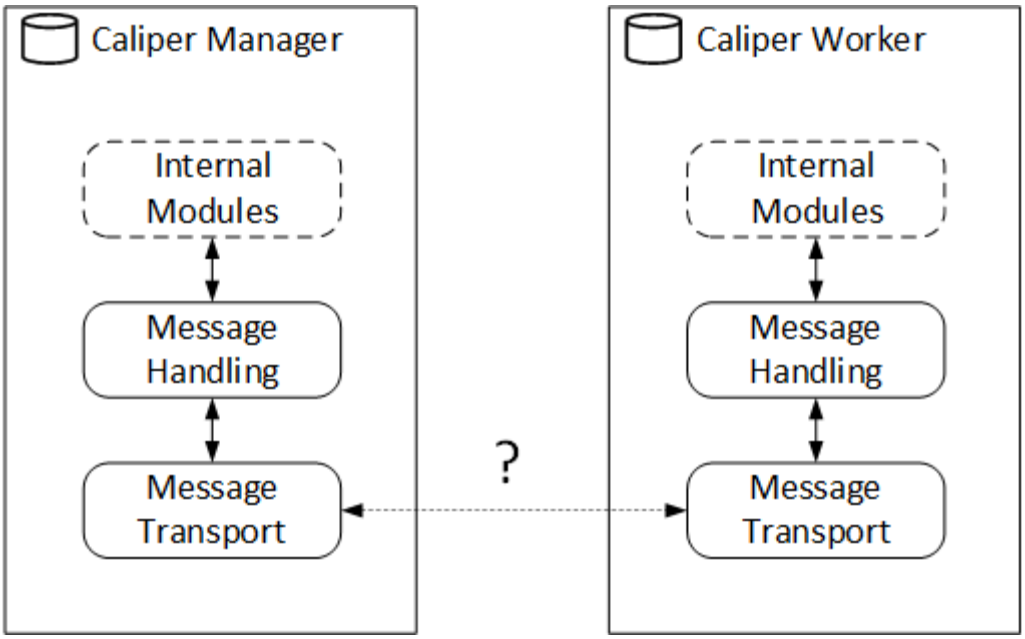
2. Αυτόματη αναπαραγωγή διεργασιών εργαζομένων στον ίδιο υπολογιστή, αυτή τη φορά με τη χρήση ενός απομακρυσμένου μηχανισμού ανταλλαγής μηνυμάτων με τη διαδικασία διαχειριστή (manager process)

3. Και το τρίτο μοντέλο είναι, η εκκίνηση εργασιών με μη αυτόματο τρόπο σε ένα αυθαίρετο αριθμό υπολογιστών, με τη χρήση ενός απομακρυσμένου μηχανισμού με τη διαδικασία του διαχειριστή.

Οι δύο πρώτοι τρόποι μπορούν να βοηθήσουν με την καλύτερη εξοικειώσει με το Hyperledger Caliper.

Αρθρωτή μεταφορά μηνυμάτων

Οι διαφορετικές προσεγγίσεις ανάπτυξης καθίστανται δυνατές από τον τρόπο με τον οποίο ο Caliper χειρίζεται τα μηνύματα εσωτερικά, όπως φαίνεται και στην παρακάτω Εικόνα.

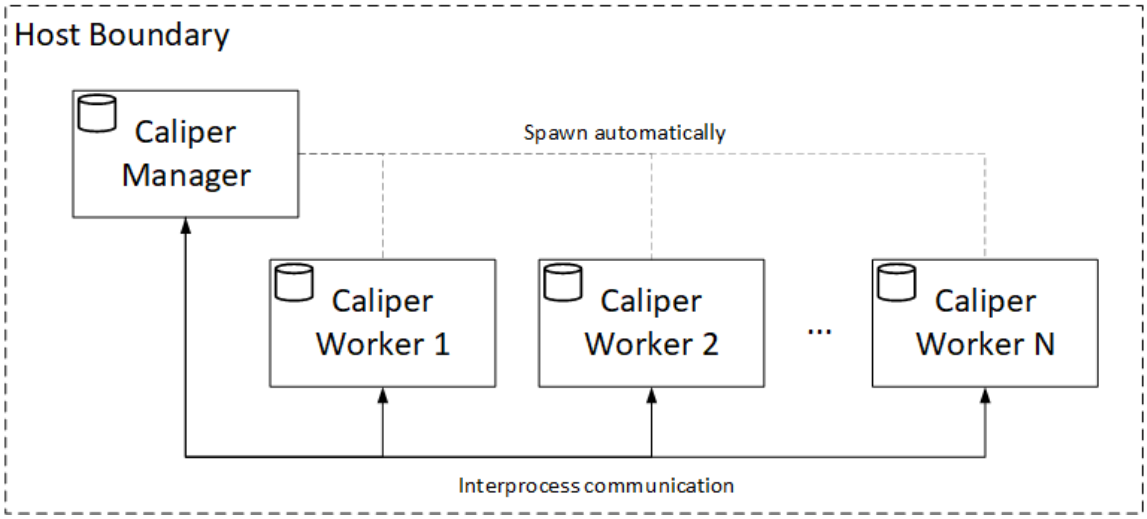


Εικόνα 19 Μεταφορά μηνυμάτων, **πηγή**: https://hyperledger.github.io/caliper/

Οι εσωτερικές μονάδες Caliper αφορούν μόνο προκαθορισμένα μηνύματα των οποίων το περιεχόμενο είναι ανεξάρτητο από τον τρόπο αποστολής των μηνυμάτων. Η ενότητα που στέλνει τα μηνύματα μεταξύ των διαδικασιών είναι εναλλακτική, επιτρέποντας έτσι διαφορετικές μεθόδους επικοινωνίας. [42]

Επικοινωνία μεταξύ διεργασιών

Η διαδικασία διαχειριστή ξεκινά με την εντολή caliper launch manager, η οποία με τη σειρά του θα δημιουργήσει αυτόματα τον διαμορφωμένο αριθμό διεργασιών εργαζομένου, όπως φαίνεται στη Εικόνα 20.

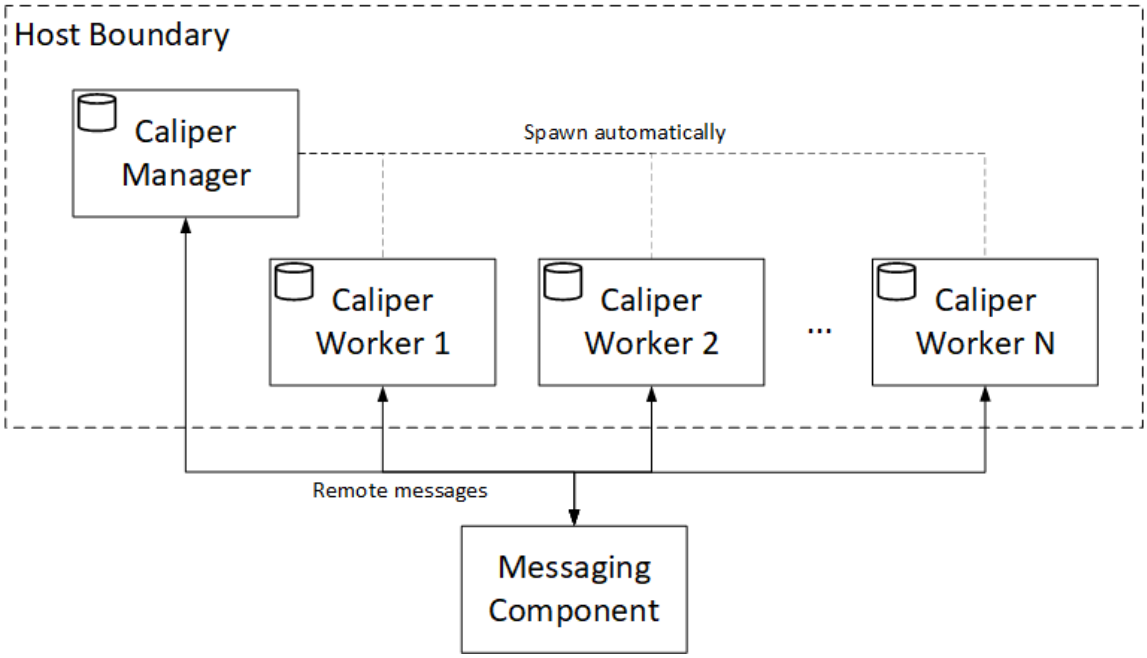


Εικόνα 20 Επικοινωνία μεταξύ διεργασιών, **πηγή:** https://hyperledger.github.io/caliper/

Αυτό αποτελεί το πιο απλό μοντέλο ανάπτυξης για το Caliper, το οποίο δεν απαιτεί επιπλέον διαμόρφωση και εφαρμογές μηνυμάτων τρίτων.

Τοπική επικοινωνία με μηνύματα μέσω τρίτων

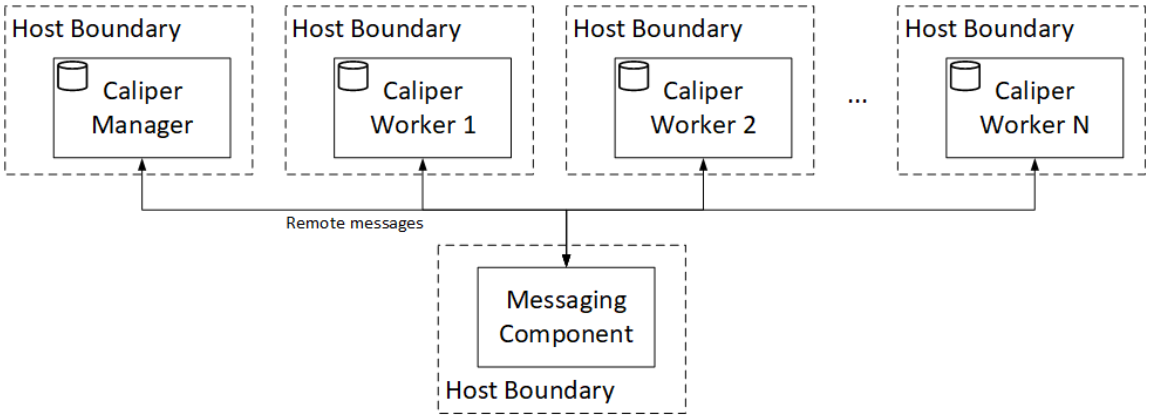
Το δεύτερο μοντέλο ανάπτυξης αντικαθιστά το IPC με την προσθήκη ενός τρίτου ανταλλαγής μηνυμάτων, και ταυτόχρονα αποκρύπτει τη διαχείριση της διαδικασίας των εργαζομένων από τον χρήστη, το οποίο φαίνεται στην Εικόνα 21.



Εικόνα 21 Τοπική επικοινωνία με μηνύματα μέσω τρίτων, **πηγή**: https://hyperledger.github.io/caliper/

Διανεμημένη επικοινωνία με μηνύματα μέσω τρίτων

Όταν η διαχείριση των εργασιών των εργαζομένων γίνεται από τον ίδιο τον χρήστη, τότε μπορεί να θέσει σε λειτουργία όσους εργαζόμενους σε όσους υπολογιστές επιθυμεί.



Εικόνα 22 Διανεμημένη επικοινωνία με μηνύματα μέσω τρίτων, **πηγή**: https://hyperledger.github.io/caliper/

Η πλήρως κατανεμημένη ανάπτυξη επιτρέπει την οριζόντια κλιμάκωση των εργασιών των εργαζομένων, αυξάνοντας σημαντικά τον επιτεύξιμο ρυθμό φόρτου εργασίας. [42]

6 ΛΕΙΤΟΥΡΓΙΑ HYPERLEDGER

Το Hyperledger Fabric είναι μια πλατφόρμα ανοιχτού κώδικα κατανεμημένης βάσης (DLT, distributed ledger technology), σχεδιασμένη για χρήση σε εταιρικά πλαίσια, η οποία παρέχει μερικές βασικές δυνατότητες διαφοροποίησης σε σχέση με άλλες δημοφιλείς τεχνολογίες κατανεμημένης βάσης.
Στην Ενότητα 2.3.1 , αναφέραμε ότι στη πλατφόρμα Fabric χρειάζεται άδεια κάποιος για να συμμετέχει στο δίκτυο, όπου σε αυτή την περίπτωση, όσοι συμμετέχουν γνωρίζονται.

Ένας από τους πιο σημαντικούς, από τους διαφοροποιητές της πλατφόρμας είναι η υποστήριξή τους για τα ενσωματωμένα πρωτόκολλα συναίνεσης που επιτρέπουν στην πλατφόρμα να προσαρμόζεται πιο αποτελεσματικά για να ταιριάζει σε συγκεκριμένες περιπτώσεις χρήσης και μοντέλα εμπιστοσύνης. Για παράδειγμα, όταν αναπτύσσεται σε μια μεμονωμένη επιχείρηση, ή λειτουργεί από μια αξιόπιστη αρχή, η πλήρως βυζαντινή ανοχή σε σφάλματα μπορεί να θεωρηθεί περιττή. Σε καταστάσεις όπως αυτό, ένα πρωτόκολλο συναίνεσης ανθεκτικό σε σφάλματα (CFT, crash fault-tolerant) μπορεί να είναι περισσότερο από επαρκές, ενώ, σε μια πολυμερή, αποκεντρωμένη περίπτωση χρήσης, μπορεί να απαιτεί ένα πιο παραδοσιακό βυζαντινό πρωτόκολλο ανεκτικότητας σε σφάλμα (BFT, Byzantine fault tolerant). [43]

Η Βυζαντινή Ανοχή Σφαλμάτων είναι το χαρακτηριστικό που καθορίζει ένα σύστημα που ανέχεται την κατηγορία των αποτυχιών που ανήκουν στο Βυζαντινό Πρόβλημα Στρατηγών. Η βυζαντινή αποτυχία είναι η πιο δύσκολη κατηγορία των τρόπων αποτυχίας. Δεν συνεπάγεται περιορισμούς και δεν κάνει παραδοχές σχετικά με το είδος της συμπεριφοράς που μπορεί να έχει ένας κόμβος. (π.χ. ένας κόμβος μπορεί να δημιουργήσει οποιοδήποτε είδος αυθαίρετων δεδομένων ενώ παρουσιάζεται ως έντιμος ηθοποιός).

Το Βυζαντινό Πρόβλημα των Στρατηγών περιγράφεται το 1982 από τους Lamport, Shostak και Pease, είναι μια γενικευμένη έκδοση του Προβλήματος των 2 Στρατηγών (Two Generals Problem), με μια επιπλοκή. Περιγράφει το ίδιο σενάριο, όπου περισσότεροι στρατηγοί πρέπει να συμφωνήσουν για την ώρα στην οποία θα επιτεθούν στον κοινό εχθρό τους. Η επιπλοκή σε αυτή την περίπτωση είναι ότι ένας ή περισσότεροι από τους στρατηγούς μπορεί να είναι προδότες, πράγμα που μπορούν να ψεύδονται για την απόφαση τους (π.χ λένε ότι θα επιτεθούν στις 0900 αλλά είπαν ψέματα). [44]

Το Fabric μπορεί να αξιοποιήσει πρωτόκολλα συναίνεσης που δεν απαιτούν εγγενή κρυπτονομίσματα για να ενθαρρύνουν την δαπανηρή εξόρυξη ή να τροφοδοτήσουν την έξυπνη εκτέλεση συμβολαίων (smart contracts).

6.1 Το μοντέλο του Hyperledger Fabric

Αυτή η ενότητα περιγράφει τα βασικά χαρακτηριστικά σχεδίασης του Hyperledger Fabric που οδηγούν σε ένα ολοκληρωμένο, αλλά και προσαρμόσιμο blockchain.

Περιουσιακά στοιχεία (Assets): Οι ορισμοί των περιουσιακών στοιχείων επιτρέπουν την ανταλλαγή για οτιδήποτε έχει χρηματική αξία, από τρόφιμα έως και υπηρεσίες.

Αλυσιδωτός κώδικας(Chaincode): Η εκτέλεση του κώδικα από την εντολή συναλλαγών περιορίζουν τα απαιτούμενα επίπεδα εμπιστοσύνης και επαλήθευσης από όλους του κόμβους, και βελτιστοποιώντας την επεκτασιμότητα και την απόδοση του δικτύου. [43]

Χαρακτηριστικά βάσης(Ledger features): Η αμετάβλητη κοινόχρηστη βάση κωδικοποιεί το ιστορικό συναλλαγών για κάθε κανάλι και δίνει την δυνατότητα να θέσει κάποιος ένα ερώτημα τύπου SQL για τον αποτελεσματικό έλεγχο.

Απόρρητο(Privacy): Τα κανάλια και οι ιδιωτικές συλλογές δεδομένων επιτρέπουν την εκτέλεση ιδιωτικών και εμπιστευτικών συναλλαγών συνήθως από ανταγωνιστικές επιχειρήσεις που ανταλλάσσουν περιουσιακά στοιχεία σε ένα κοινό δίκτυο. [43]

Ασφάλεια και Υπηρεσίες μέλους(Security & Membership Services): Η συμμετοχή με άδεια παρέχει ένα αξιόπιστο δίκτυο blockchain, όπου οι συμμετέχοντες γνωρίζουν ότι όλες οι συναλλαγές μπορούν να εντοπιστούν από εξουσιοδοτημένους ρυθμιστές και ελεγκτές. Το Hyperledger Fabric χρησιμοποιεί την υποδομή Δημόσιου Κλειδιού (PKI, Public Key Infrastructure) για τη δημιουργία του Membership Service Provider (MSP), η οποία στη συνέχεια χρησιμοποιείται για τη δημιουργία ψηφιακών πιστοποιητικών για τον προσδιορισμό και τη διαχείριση της ταυτότητας των μελών. [45]

Ομοφωνία(Consensus): Μια μοναδική προσέγγιση στη συναίνεση που επιτρέπει την ευελιξία και την επεκτασιμότητα που απαιτείται για την επιχείρηση. Η διαδικασία ομοφωνίας στο Hyperledger Fabric, είναι πιο γρήγορη σε σύγκριση με άλλα δημόσια blockchain.

Χαρακτηριστικά της βάσης του Fabric:

- Ερωτήματα και ενημέρωση της βάσης, αναζητήσεις με λέξεις κλειδιά και σύνθετα ερωτήματα
- Ερωτήματα μόνο για ανάγνωση χρησιμοποιώντας μια πλούσια γλώσσα ερωτημάτων (couchDB)
- Ερωτήματα ιστορικού μόνο για ανάγνωση – Ιστορικό της βάσης για ένα κλειδί
- Οι συναλλαγές αποτελούνται από τις εκδόσεις των κλειδιών/τιμών που διαβάστηκαν στον κώδικα αλυσίδας και κλειδιά/τιμές που γράφτηκαν στον κώδικα αλυσίδας
- Οι συναλλαγές περιέχουν τις υπογραφές κάθε μέλους (peer)
- Οι συναλλαγές ταξινομούνται σε μπλοκ και «παραδίδονται» σε κάθε μέλος του καναλιού
- Τα μέλη επικυρώνουν συναλλαγές έναντι πολιτικών έγκρισης και εφαρμόζουν τις πολιτικές

- Πριν την επικαιροποίηση ενός μπλοκ, πραγματοποιείται ένας έλεγχος για να διασφαλίσει ότι οι καταστάσεις για στοιχεία που έχουν διαβαστεί δεν έχουν αλλάξει από την ώρα εκτέλεσης του κώδικα αλυσίδας (chaincode)
- Δεν αλλάζει τίποτα από τη στιγμή που μια συναλλαγή εγκρίθηκε και πραγματοποιήθηκε
- Η βάση ενός καναλιού περιέχει ένα μπλοκ διαμόρφωσης που ορίζει πολιτικές, λίστες ελέγχου πρόσβασης και άλλες σχετικές πληροφορίες

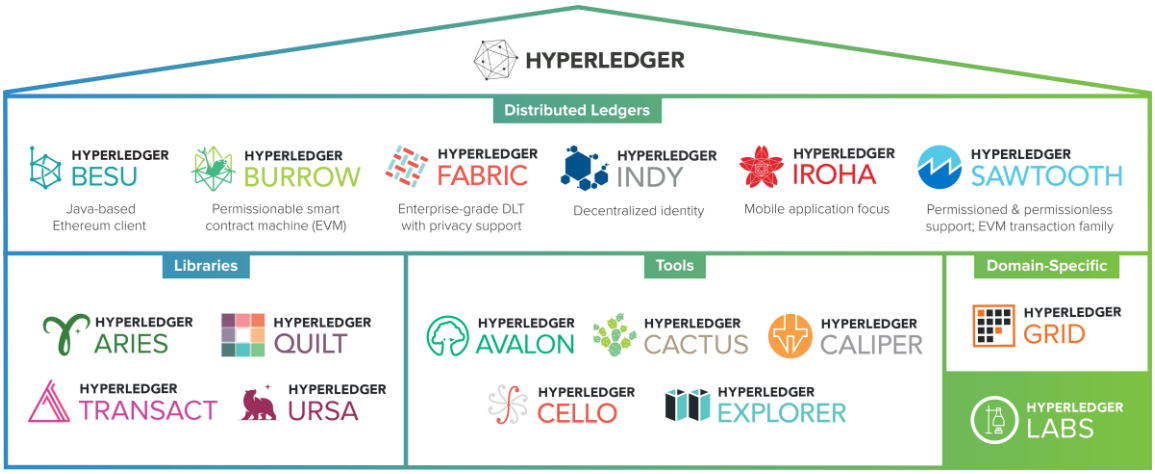
Το δίκτυο του Hyperledger αποτελείται κυρίως από 5 οντότητες.

1. **Πάροχος υπηρεσιών μέλους(MSP):** Εκδίδει και επικυρώνει πιστοποιητικά του χρήστη μετά την εκτέλεση του ελέγχου ταυτότητας χρήστη.
2. **Client:** Είναι μέλος που προτείνει συναλλαγές ώστε να ενημερωθούν στη βάση.
3. **Endorser:** Όταν ένα μέλος στέλνει ένα αίτημα συναλλαγής, αυτός είναι που θα κάνει τον έλεγχο της ταυτότητας του μέλους και τη πραγματοποίηση της προτεινόμενης συναλλαγής. [46]
4. **Orderer:** Αφού λάβει έναν αριθμό μη επιβεβαιωμένων συναλλαγών από τα μέλη, τότε συλλέγει ένα σύνολο συναλλαγών σε ένα μπλοκ και το μεταδίδει στο δίκτυο.
5. **Validator:** Ο ρόλος του είναι να επικυρώσει τις μη επιβεβαιωμένες συναλλαγές σε ένα μπλοκ και να ενημέρωση τη βάση σε περίπτωση επιτυχούς επικύρωσής.

6.2 Άλλες τεχνολογίες Blockchain

Υπάρχουν διάφορες τεχνολογίες blockchain επιχειρήσεων που έχουν αναπτυχθεί μέσα στο Hyperledger. Όλα τα έργα είναι ανοιχτού κώδικά, πράγμα που σημαίνει ότι ο καθένας μπορεί να κατεβάσει και να χρησιμοποιήσει οποιοδήποτε πρόγραμμα ανταποκρίνεται καλύτερα στις ανάγκες του.

Γενικά τα έργα τα οποία στηρίζονται στο Hyperledger έχουν μια αρθρωτή δομή και ανάλογα με την εφαρμογή επιλέγονται και εξειδικεύονται επιμέρους τμήματα του όπως φαίνονται και στην Εικόνα 23.



Εικόνα 23 Τμήματα του Hyperledger, **πηγή**: https://www.hyperledger.org/

Hyperledger Besu

Το Hyperledger Besu αποτελεί τεχνολογία blockchain ανοιχτού κώδικα με βάση τη γλώσσα προγραμματισμού Java και κάτω από την άδεια Apache 2.0, προσφέρει την πιο αξιόπιστη, επεκτάσιμη και εύχρηστη πλατφόρμα για το mainnet και τις επιχειρήσεις. Μπορεί να χρησιμοποιηθεί για την ανάπτυξη εταιρικών εφαρμογών οι οποίες έχουν ως κύρια απαίτηση την ασφαλή επεξεργασία συναλλαγών υψηλής απόδοσης σε ιδιωτικό δίκτυο. Το Besu περιλαμβάνει μια γραμμή εντολών (CLI), για την εκτέλεση, συντήρηση, τον εντοπισμό σφαλμάτων αλλά και την παρακολούθηση των κόμβων στο δίκτυο του Ethereum.

Hyperledger Burrow

Το Hyperledger Burrow είναι ένα ιδιωτικό blockchain που λειτουργεί ανάλογα με το blockchain του Ethereum. Η βασική του λειτουργία είναι η εκτέλεση έξυπνων συμβολαίων με αποδοτικό τρόπο. Το Burro αποτελεί ένα ολοκληρωμένο σύστημα blockchain και μια έξυπνη μηχανή εκτέλεσης έξυπνων συμβολαίων, μια κατανεμημένη βάση δεδομένων που εκτελεί κώδικα. Χρησιμοποιεί αλγόριθμο συναίνεσης Tendermint για τον συγχρονισμό.

Hyperledger Indy

Αποτελεί ένα κιτ ανάπτυξης λογισμικού (SDK), που επιτρέπει την αυτοκυρίαρχη ταυτότητα να ενσωματωθεί σε κατανεμημένα καθολικά. Αυτό το SDK αποτελεί περιτύλιγμα για πολλές γλώσσες για την προσθήκη νέων δυνατοτήτων και τη καλύτερη διαχείριση αποκεντρωμένων ταυτοτήτων. Παρέχει εργαλεία, βιβλιοθήκες και επαναχρησιμοποιήσιμα στοιχεία για την παροχή ψηφιακών ταυτοτήτων που έχουν τις ρίζες τους σε blockchain ή σε άλλες κατανεμημένες βάσεις, ώστε να είναι δια λειτουργικά μεταξύ των τομέων διαχείρισης. Το Indy είναι δια λειτουργικό με άλλα blockchain ή μπορεί η χρήση του να γίνει για την ενίσχυση της αποκέντρωσης της ταυτότητας. [47]

Hyperledger Iroha

Πρόκειται για ένα συνεκτικό σύνολο βιβλιοθηκών και στοιχείων που θα επιτρέψουν την υιοθέτηση κατανεμημένων βάσεων σε υπάρχουσες δομές. Η αποθήκευση δεδομένων και ο συγχρονισμός πραγματοποιούνται εκτός συσκευής και ένα προεπιλεγμένο πρόγραμμα κριτικής μεταξύ των χρηστών (Reputation System) εφαρμόζεται σε όλο το δίκτυο για να διασφαλίσουν επικυρωμένους κόμβους. Έχει σχεδιαστεί ώστε να είναι απλό και εύκολο για να ενσωματωθεί σε έργα υποδομής ή σε συσκευές που συνδέονται στο διαδίκτυο (IoT).

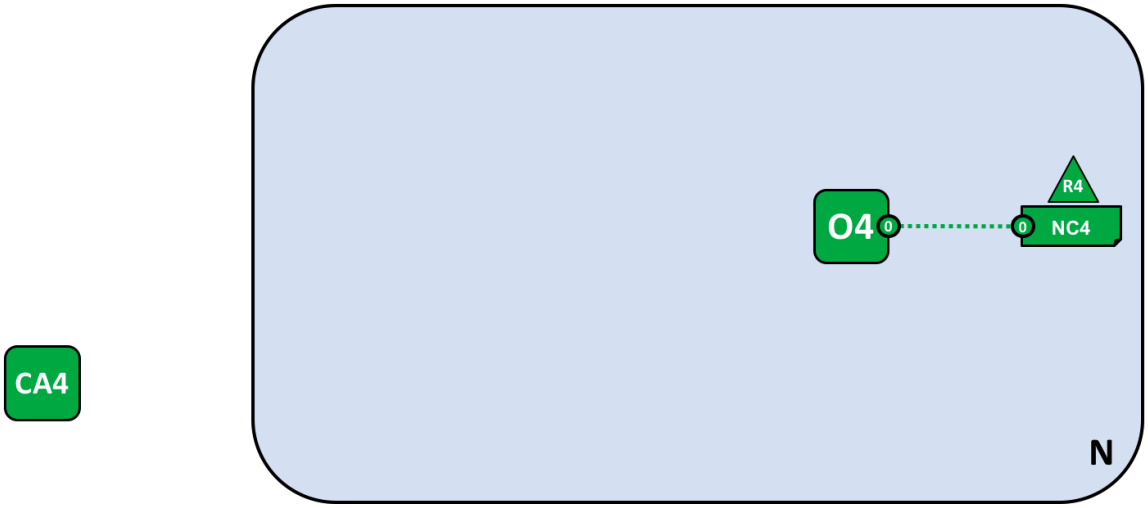
Hyperledger Sawtooth

Το Sawtooth αποτελεί μια προσπάθεια της Intel να δημιουργήσει ένα blockchain ανοιχτού κώδικα. Είναι μια πλατφόρμα για την κατασκευή, ανάπτυξη και λειτουργεία κατανεμημένων βάσεων. Περιέχει έναν νέο αλγόριθμο συναίνεσης που ονομάζεται Proof of Elapsed Time (PoET), που στοχεύει μεγάλους κατανεμημένους επικυρωτές με ελάχιστη κατανάλωση πόρων. [48]

6.3 Δίκτυο Blockchain

Παρακάτω θα γίνει η εξήγηση για τα βήματα που χρειάζεται να κάνουμε για την δημιουργία ενός λειτουργικού δικτύου blockchain.

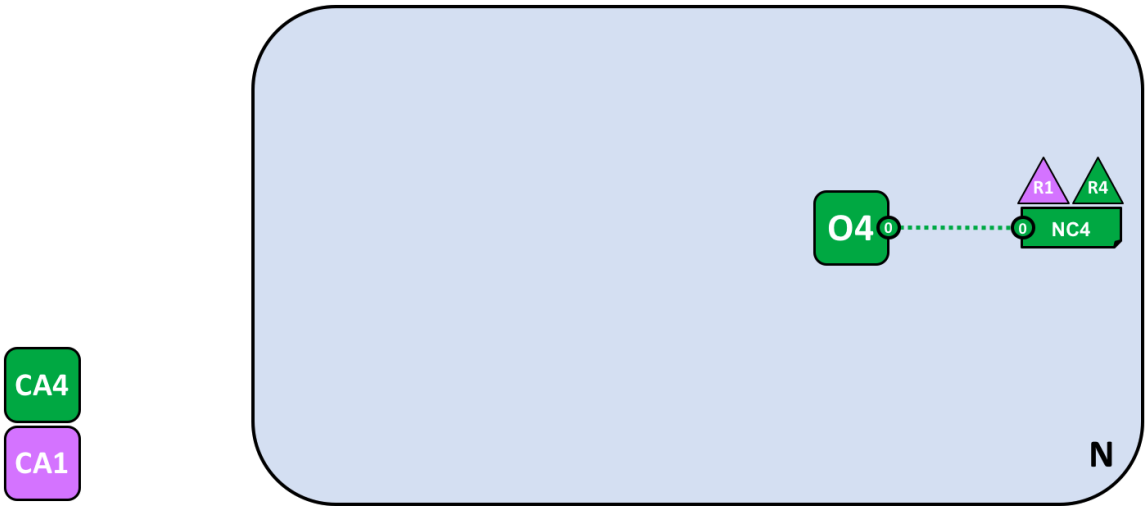
Θα αρχίσουμε από την δημιουργία του δικτύου, δηλαδή την βάση του.



Εικόνα 24 Δημιουργία Δικτύου, **πηγή**: https://hyperledger-fabric.readthedocs.io/

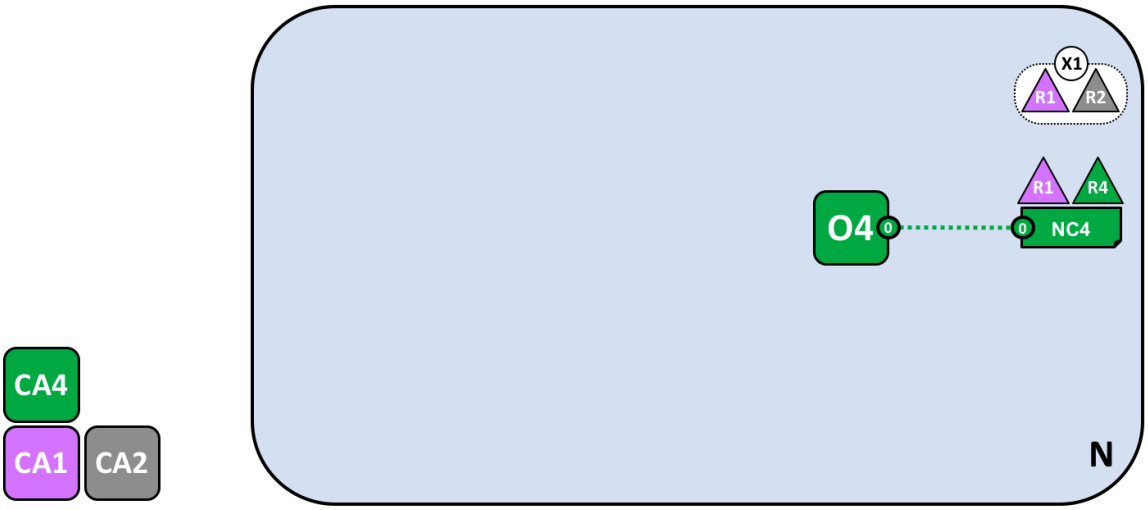
Με την δημιουργία ενός εντολέα (O4) σχηματίζεται και το δίκτυο μας. Το δίκτυο, στην παραπάνω εικόνα μας είναι το N, το οποίο περιλαμβάνει ένα μόνο κόμβο O4, ο οποίο αυτός ο κόμβος διαμορφώνεται σύμφωνα με μια διαμόρφωση δικτύου NC4). Επίσης φαίνεται η Αρχή Πιστοποιητικών (CA4), το οποίο χρησιμοποιείται για την έκδοση πιστοποιητικών σε διαχειριστές και κόμβους.

Στη συνέχεια θα προσθέσουμε στο δίκτυο διαχειριστές. Το NC4 έχει διαμορφωθεί έτσι ώστε να δώσει στους χρήστες του οργανισμού R4 δικαιώματα διαχειριστή, τώρα θα επιτραπεί στον Οργανισμό R1 να διαχειριστεί το δίκτυο. Αυτό φαίνεται στην παρακάτω Εικόνα.



Εικόνα 25 Προσθήκη διαχειριστών, **πηγή**: https://hyperledger-fabric.readthedocs.io/

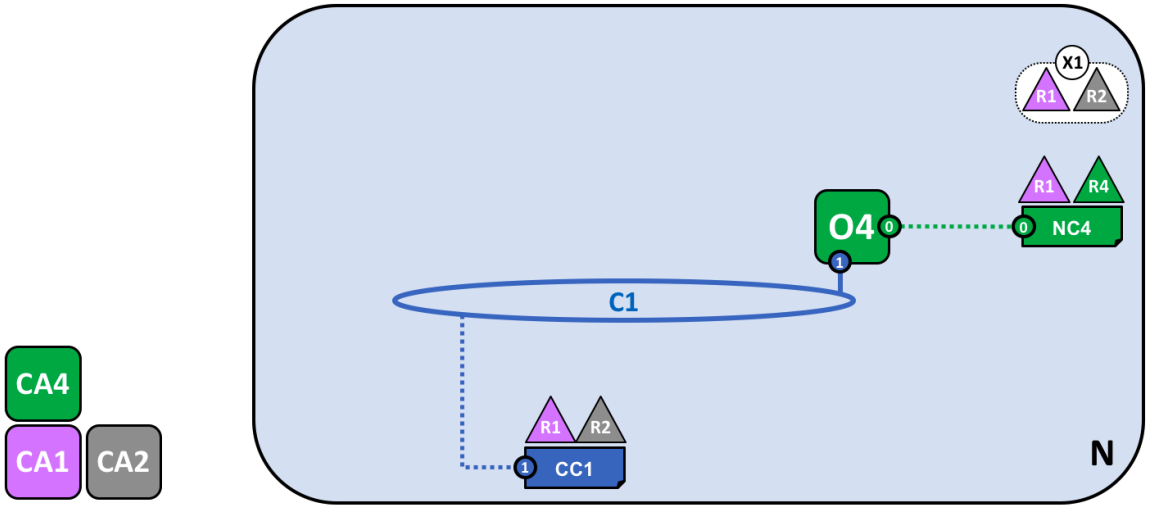
Ο οργανισμός R4 ενημερώνει το αρχείο διαμόρφωσης δικτύου ώστε να δώσει τα ίδια δικαιώματα διαχειριστεί στον οργανισμό R1. Τώρα που το δίκτυο διαχειρίζεται από τους οργανισμούς R1 και R4 δεν υπάρχουν πολλά να γίνουν, αυτό θα λυθεί με την δημιουργία μιας κοινοπραξίας, δηλαδή να μοιράζονται ένα κοινό μέλλον. Στην παρακάτω Εικόνα φαίνεται για το πως μιας κοινοπραξία καθορίζεται.



Εικόνα 26 Καθορισμός μιας κοινοπραξίας, **πηγή**: https://hyperledger-fabric.readthedocs.io/

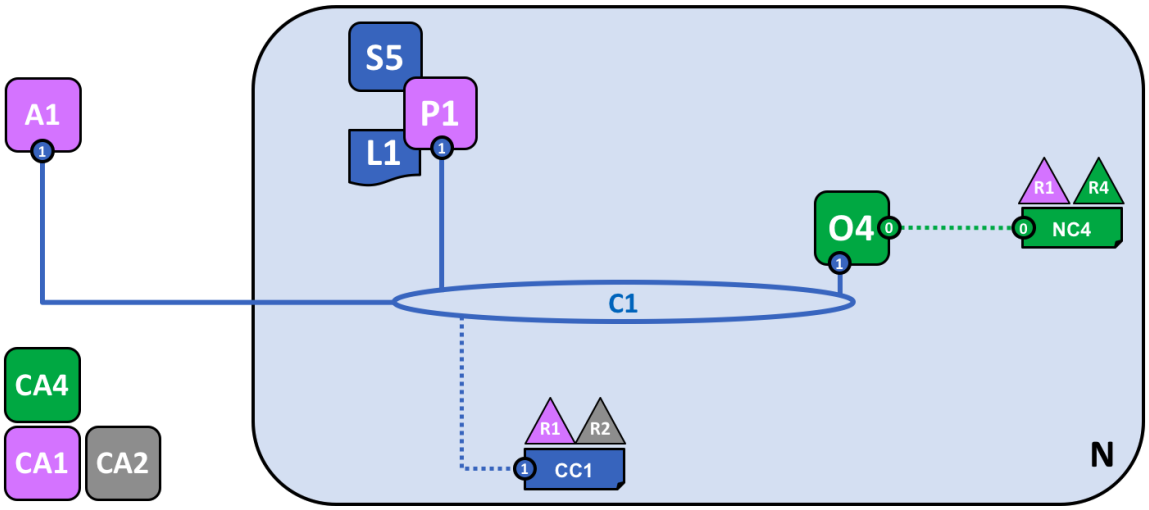
Η παραπάνω κοινοπραξία X1 δημιουργείται από τον διαχειριστή του δικτύου και περιλαμβάνει δύο μέλη, τον οργανισμό R1 και τον οργανισμό R2, αυτή η κοινοπραξία εμπεριέχεται στον NC4, το οποίο θα βοηθήσει στο επόμενο στάδιο ανάπτυξης του δικτύου. Οι R1 και R2 είναι οι μοναδικοί οργανισμοί που μπορούν να δημιουργήσουν μια κοινοπραξία και αυτό επειδή έτσι διαμορφώθηκε το NC4. Στο επόμενο βήμα θα δημιουργήσουμε το βασικό χαρακτηριστικό του δικτύου, το κανάλι, δηλαδή το μηχανισμό με το οποίο τα μέλη μιας κοινοπραξίας μπορούν να

επικοινωνούν το ένα με το άλλο. Στην παρακάτω Εικόνα φαίνεται η εισαγωγή του καναλιού C1. [43]



Εικόνα 27 Δημιουργία καναλιού για την κοινοπραξία, **πηγή**: https://hyperledger-fabric.readthedocs.io/

Το κανάλι C1 δημιουργήθηκε για την κοινοπραξία X1, το οποίο διέπετε από τον διαμορφωτή καναλιού CC1, το οποίο είναι διαφορετικό από το NC4. Το CC1 διαχειρίζεται από τους R1 και R2. Από την εικόνα παρατηρούμε ότι ο οργανισμός R4 δεν έχει κανένα δικαίωμα στο CC1.



Εικόνα 28 Δίκτυο N, **πηγή**: https://hyperledger-fabric.readthedocs.io/

Στην παραπάνω εικόνα προσθέσαμε ένα κόμβο-μέλος P1 και την βάση L1. Το P1, είναι μέλη στα οποία αποθηκεύονται αντίγραφα του L1. Όπως, βλέπουμε και πάνω ο P1 προστέθηκε το κανάλι C1, όπου ο P1 φιλοξενεί ένα αντίγραφο του L1. Ταυτόχρονα ένα έξυπνο συμβόλαιο S5 έχει

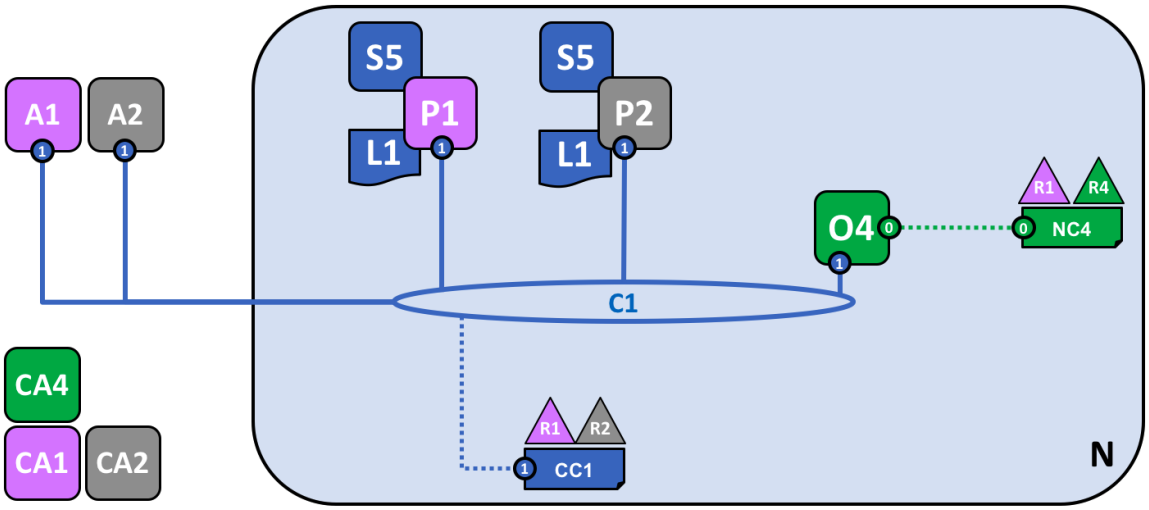
εγκατασταθεί στον P1, η εφαρμογή του συστήματος πελάτη A1 στον οργανισμό R1 μπορεί να χρησιμοποιήσει το S5 ώστε να έχει πρόσβαση στη βάση L1 μέσω του κόμβου P1. [43]

Ο διαχειριστής R1 πρέπει να δημιουργήσει ένα πακέτο αλυσιδωτού κώδικά και να το εγκαταστήσει στον P1, αφού το έξυπνο συμβόλαιο S5 έχει δημιουργηθεί. Αυτό αποτελεί μια απλή λειτουργία. Από την στιγμή που αυτή η λειτουργία έχει ολοκληρωθεί τότε ο P1 έχει πλήρη γνώση του S5. Όταν ένα δίκτυο έχει περισσότερα μέλη σε ένα κανάλι, μπορεί να διαλέξει τα μέλη στα οποία θα εγκαταστήσει τα έξυπνα συμβόλαια, δεν είναι υποχρεωτικό να εγκαταστήσει ένα έξυπνο συμβόλαιο σε κάθε μέλος.

Αν και ο αλυσιδωτός κώδικας έχει εγκατασταθεί στα μέλη των μεμονωμένων οργανισμών, διέπετε και λειτουργεί στο πλαίσιο ενός καναλιού. Κάθε οργανισμός πρέπει να εγκρίνει το καθορισμό ενός αλυσιδωτού κώδικα, αλλά και τις παραμέτρους με τους οποίους ο κώδικας θα χρησιμοποιείται στο κανάλι. Ένας οργανισμός θα πρέπει να εγκρίνει τον καθορισμό του κώδικα ώστε να μπορεί να χρησιμοποιήσει το εγκατεστημένο έξυπνο συμβόλαιο, ώστε να μπορεί να θέτει ερωτήματα στη βάση αλλά και για να εγκρίνει συναλλαγές. [43]

Το πιο σημαντικό κομμάτι πληροφοριών που περιέχονται στον ορισμό του αλυσιδωτού κώδικα είναι η **πολιτική έγκρισης**. Αυτή η πολιτική περιγράφει για το ποιοι οργανισμοί μπορούν να εγκρίνουν συναλλαγές προτού αποδεχθούν από άλλους οργανισμούς στο αντίγραφο της βάσης. Στο παραπάνω παράδειγμα, οι συναλλαγές μπορούν να αποδεχθούν στη βάση L1, αν και μόνο οι οργανισμοί R1 και R2 το εγκρίνουν.

Όταν ένα έξυπνο συμβόλαιο εγκατασταθεί σε ένα μέλος και καθοριστεί σε ένα κανάλι, μπορεί ένα σύστημα εφαρμογής πελάτη να το επικαλεστεί. Αυτό μπορεί να γίνει με το να στέλνει συναλλαγές στα μέλη που ανήκουν στους οργανισμούς οι οποίοι διευκρινίζονται στο έξυπνο συμβόλαιο πολιτικής έγκρισης. [43]



Εικόνα 29 Ολοκληρωμένο δίκτυο, **πηγή**: https://hyperledger-fabric.readthedocs.io/

Στη παραπάνω Εικόνα, φαίνεται για το πως έχει εξελιχθεί το δίκτυο. Ο οργανισμός R2 έχει προσθέσει ένα μέλος P2 το οποίο φιλοξενεί ένα αντίγραφο της βάσης L1, και τον αλυσιδωτό κώδικα S5. Ο P2 εγκρίνει τον ίδιο αλυσιδωτό με τον R1. Ταυτόχρονα, βλέπουμε ότι το κανάλι C1 φιλοξενεί και τον κόμβο P2 του οργανισμού R2. Το σύστημα εφαρμογής A2 και ο κόμβος P2 χρησιμοποιεί πιστοποιητικά από το CA2. Από αυτό βγαίνει το συμπέρασμα ότι το A1 και A2 μπορεί να ενεργοποιήσει το έξυπνο συμβόλαιο S5 στο κανάλι C1 είτε από τον κόμβο P1 ή από τον κόμβο P2.

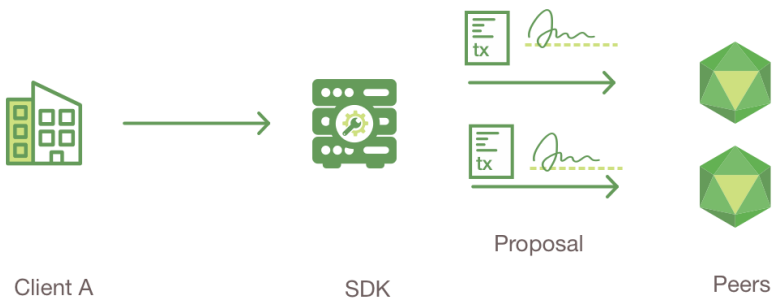
Ακόμη, βλέπουμε ότι ο κόμβος P2 που έχει προστεθεί από τον οργανισμό R2, φιλοξενεί ένα αντίγραφο του L1 και S5. Επίσης, ο οργανισμός R2 έχει προσθέσει το A2 το οποίο συνδέεται στο δίκτυο μέσω του καναλιού C1. Για να πετύχει αυτό, ένας διαχειριστής του οργανισμού R2 έχει δημιουργήσει τον κόμβο P2 και τον εισήγαγε στο κανάλι C1, όπως ακριβώς έγινε και με τον οργανισμό R1.

Δημιουργήσαμε ένα ολοκληρωμένο λειτουργικό δίκτυο. Σε αυτό το στάδιο, έχουμε ένα κανάλι στο οποίο οι οργανισμοί R1 και R2, μπορούν να αλληλοεπιδράσουν μεταξύ τους. Συγκεκριμένα, αυτό σημαίνει ότι οι εφαρμογές A1 και A2 μπορούν να δημιουργήσουν συναλλαγές χρησιμοποιώντας το έξυπνο συμβόλαιο S5 και τη βάση L1 στο κανάλι C1. [43]

6.4 Ροή Συναλλαγής

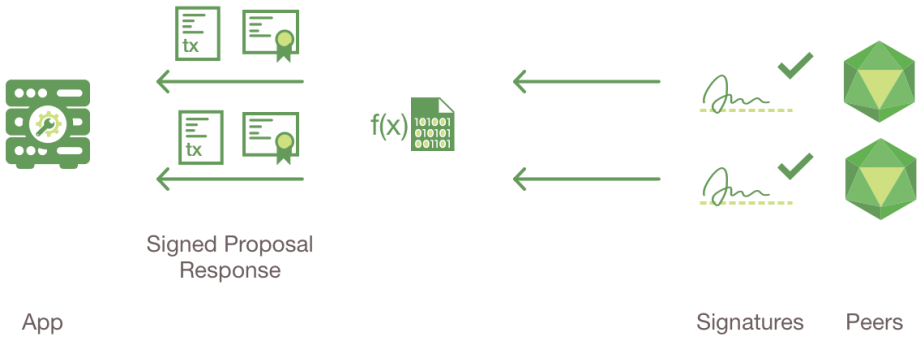
Υποθέσεις:

- Ένα κανάλι έχει δημιουργηθεί και τρέχει
- Ο χρήστης της εφαρμογής έχει εγγραφή στην Αρχή Πιστοποιητικών (CA, Certificate Authority) του οργανισμού
- Έχει λάβει το απαραίτητο κρυπτογραφικό υλικό για τον έλεγχο ταυτότητας
- Ο αλυσιδωτός κώδικας έχει εγκατασταθεί στα μέλη και λειτουργεί στο κανάλι, ακόμη περιέχει ένα σύνολο οδηγιών για την συναλλαγή και την συμφωνημένη τιμή για το προϊόν
- Έχει καθοριστεί μια πολιτική έγκρισης που δηλώνει ότι και τα δύο μέλη (peerA & peerB) πρέπει να εγκρίνουν οποιαδήποτε συναλλαγή



Εικόνα 30 Ο πελάτης A εκκινεί μια συναλλαγή, **πηγή:** www.hyperledger.org

1. Ο πελάτης A (clientA) στέλνει ένα αίτημα για την αγορά ενός προϊόντος. Το αίτημα έχει ως στόχο τα δύο μέλη (peers). Όπως έχουμε πει παραπάνω, η πολιτική έγκρισης δηλώνει ότι τα μέλη θα πρέπει να εγκρίνουν οποιαδήποτε συναλλαγή, οπότε το αίτημα απευθύνεται στον peerA και στον peerB.
   Στη συνέχεια, κατασκευάζεται η πρόταση συναλλαγής. Μια εφαρμογή που αξιοποιεί ένα υποστηριζόμενο SDK (Node, Java, Python) χρησιμοποιεί ένα από τα διαθέσιμα API για τη δημιουργία μιας πρότασης συναλλαγής. Η πρόταση είναι ένα αίτημα για εκκίνηση μιας λειτουργίας του αλυσιδωτού κώδικα με ορισμένες παραμέτρους εισόδου, με σκοπό την ανάγνωση ή / και την ενημέρωση της βάσης. [43]

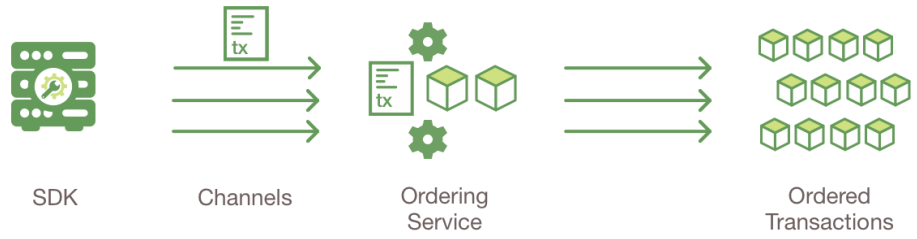


Εικόνα 31 Έγκριση υπογραφής και εκτέλεση συναλλαγής, **πηγή:** www.hyperledger.org

2. Τα μέλη επαληθεύουν, ότι η πρόταση συναλλαγής είναι σωστά διαμορφωμένη, δεν έχει υποβληθεί ήδη στο παρελθόν, η υπογραφή είναι έγκυρη (χρησιμοποιώντας το MSP), και ότι ο αποστολέας (clientA στο παράδειγμα) είναι εξουσιοδοτημένος να εκτελεί την προτεινόμενη λειτουργία σε αυτό το κανάλι. Τα μέλη λαμβάνουν τις εισόδους της πρότασης συναλλαγής ως μεταβλητές για την εκκίνηση του κώδικα αλυσίδας. Ο κώδικας αλυσίδας στη συνέχεια εκτελείται έναντι της τρέχουσας βάσης δεδομένων για την παραγωγή αποτελεσμάτων συναλλαγών που περιλαμβάνουν μια τιμή απόκρισης, ένα σύνολο ανάγνωσης και ένα σύνολο εγγραφής (δηλαδή ζεύγη κλειδιών/τιμών που ισοδυναμεί με ένα στοιχείο για δημιουργία ή ενημέρωση.

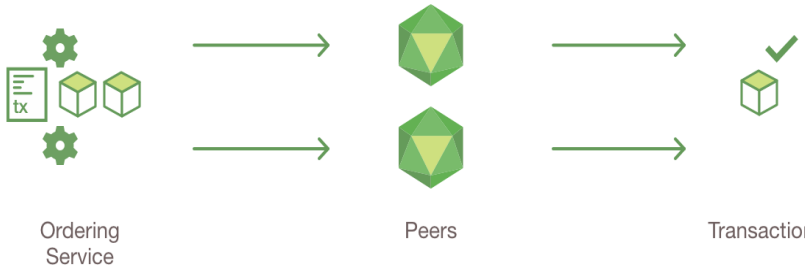
Εικόνα 32 Επιθεώρηση των απαντήσεων της πρότασης, **πηγή:** www.hyperledger.org

3. Η εφαρμογή επαληθεύει τις επικυρωμένες υπογραφές των μελών και συγκρίνει τις απαντήσεις της πρότασης για να προσδιορίσει εάν οι απαντήσεις της πρότασης είναι οι ίδιες. Εάν, ο αλυσιδωτός κώδικας θέτει ένα ερώτημα στη βάση, η εφαρμογή θα επιθεωρήσει μόνο την απάντηση στο ερώτημα και δεν θα υποβάλει τη συναλλαγή στο σύνολο των συναλλαγών που θα πάνε σε ένα μπλοκ. Εάν η εφαρμογή έχει ως στόχο η συναλλαγή να υποβληθεί σε ένα μπλοκ, τότε η εφαρμογή καθορίζει εάν η πολιτική έγκρισης έχει εκπληρωθεί (π.χ ο peerA και ο peerB, εγκρίνουν την συναλλαγή). Η αρχιτεκτονική είναι τέτοια που ακόμη και αν μια εφαρμογή επιλέξει να μην επιθεωρήσει τις απαντήσεις ή να προωθήσει με άλλον τρόπο μια συναλλαγή χωρίς έγκριση, η πολιτική έγκρισης θα εξακολουθεί να εφαρμόζεται από τα μέλη και να διατηρείται στη φάση επικύρωσης. [43]



Εικόνα 33 Ο πελάτης συγκεντρώνει τις εγκρίσεις σε μια συναλλαγή, **πηγή:** www.hyperledger.org

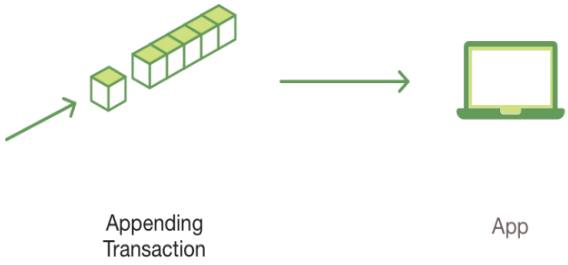
4. Η εφαρμογή «μεταδίδει» την πρόταση συναλλαγής και την απάντηση εντός ενός «μηνύματος συναλλαγής» στην υπηρεσία που συλλέγει τις συναλλαγές (ordering service). Η συναλλαγή θα περιέχει τα σύνολα ανάγνωσης/εγγραφής, τις υπογραφές των μελών και το αναγνωριστικό του καναλιού (channel ID). Η υπηρεσία δεν χρειάζεται να επιθεωρήσει ολόκληρο το περιεχόμενο μιας συναλλαγής για να εκτελέσει τη λειτουργία της, απλώς λαμβάνει συναλλαγές από όλα τα κανάλια στο δίκτυο, τα συγκεντρώνει χρονολογικά ανά κανάλι και δημιουργεί μπλοκ συναλλαγών ανά κανάλι. [43]



Εικόνα 34 Η συναλλαγή επικυρώνεται και δεσμεύεται, **πηγή:** www.hyperledger.org

5. Τα μπλοκ των συναλλαγών μεταδίδονται σε όλα τα μέλη του καναλιού. Οι συναλλαγές μέσα στο μπλοκ επικυρώνονται ώστε να διαβεβαιώσουν ότι πολιτική έγκρισης έχει εκπληρωθεί αλλά και για να διαβεβαιωθούν ότι δεν υπήρχαν αλλαγές στη κατάσταση της βάσης για το

σετ μεταβλητών ανάγνωσης καθώς το σετ ανάγνωσης δημιουργήθηκε από την εκτέλεση της συναλλαγής. Οι συναλλαγές στο μπλοκ επισημαίνονται ως έγκυρες ή μη.



Εικόνα 35 Η βάση ενημερώνεται, **πηγή:** www.hyperledger.org

6. Κάθε μέλος προσθέτει το μπλοκ στην αλυσίδα του καναλιού και για κάθε έγκυρη συναλλαγή τα σύνολα εγγραφής δεσμεύονται στην τρέχουσα κατάσταση βάσης δεδομένων. Ένα συμβάν εκπέμπεται από κάθε μέλος για να ειδοποιήσει την εφαρμογή πελάτη ότι η συναλλαγή έχει προσαρτηθεί αμετάβλητα στην αλυσίδα, καθώς και ειδοποίηση για το εάν η συναλλαγή έχει επικυρωθεί ή όχι.

6.5 Ανάπτυξη ενός δικτύου

Η διαδικασία ανάπτυξης ενός δικτύου Fabric είναι περίπλοκη και προϋποθέτει κατανόηση της υποδομής δημόσιου κλειδιού και τη διαχείριση κατανεμημένων συστημάτων. Χρειάζεται να γνωρίζει κάποιος τον τρόπο ανάπτυξης των δικτύων για την ανάπτυξη αποτελεσματικών έξυπνων συμβάσεων και εφαρμογών.

Παρακάτω δίνεται μια επισκόπηση των βημάτων που απαιτούνται για τη ρύθμιση των εξαρτημάτων παραγωγής και για την λειτουργία του δικτύου.
Βήμα 1ο: Απόφαση σχετικά με την διαμόρφωση του δικτύου
Βήμα 2ο: Ρύθμιση ενός συμπλέγματος για τους πόρους
Βήμα 3ο: Ρύθμιση των αρχών έκδοσης πιστοποιητικών (CA)
Βήμα 4ο: Χρήση των πιστοποιητικών (CA) για την δημιουργία ταυτοτήτων και των παροχών υπηρεσιών συνδρομής (MSP)
Βήμα 5ο: Ανάπτυξη κόμβων

- Δημιουργία μελών
- Δημιουργία ενός μέλους/εντολέα

Βήμα 1ο

Η δομή ενός δικτύου blockchain πρέπει να υπαγορεύεται από την περίπτωση χρήσης. Αυτές οι θεμελιώδεις επιχειρηματικές αποφάσεις θα διαφέρουν ανάλογα με τη περίπτωση χρήσης

Σε αντίθεση με τα περιβάλλοντα ανάπτυξης, η ασφάλεια, η διαχείριση πόρων και η υψηλή διαθεσιμότητα καθίστανται προτεραιότητα κατά τη λειτουργία στην παραγωγή. Πόσους κόμβους χρειάζεται για να ικανοποιήσει την υψηλή διαθεσιμότητα και σε ποια κέντρα δεδομένων θέλει ο χρήστης να τα αναπτύξει για να ικανοποιήσει τόσο τις ανάγκες ανάκτησης σε περίπτωση καταστροφής όσο και το μέρος που αποθηκεύονται τα δεδομένα; Πώς θα διασφαλιστούν ότι τα προσωπικά κλειδιά του χρήστη θα παραμείνουν ασφαλείς;

Σύμφωνα με τα παραπάνω, παρακάτω υπάρχουν μερικές αποφάσεις που θα χρειαστεί κάποιος να πάρει, πριν την έναρξη της διαδικασίας.

- **Διαμόρφωση αρχής έκδοσης πιστοποιητικών** (Certificate Authority configuration). Ως μέρος των συνολικών αποφάσεων που πρέπει να ληφθούν αναφορικά με τα μέλη (πόσοι θα είναι, πόσοι σε κάθε κανάλι και ούτω καθεξής) και για την υπηρεσία εντολών (ordering service, πόσους κόμβους, ποιοι θα τους κατέχουν), πρέπει επίσης να αποφασισθεί για το πως θα αναπτυχθούν τα πιστοποιητικά για τον οργανισμό.
- **Τύπος βάσης δεδομένων.** Ορισμένα κανάλια σε ένα δίκτυο ενδέχεται να απαιτούν τη μοντελοποίηση όλων των δεδομένων με τρόπο που το CouchDB μπορεί να κατανοήσει τη κατάσταση της βάσης δεδομένων, ενώ άλλα δίκτυα, που δίνουν προτεραιότητα στην ταχύτητα, ενδέχεται να αποφασίσουν ότι όλα τα μέλη θα χρησιμοποιήσουν το LevelDB.
- **Κανάλια και ιδιωτικά δεδομένα.** Ορισμένα δίκτυα ενδέχεται να αποφασίσουν ότι τα κανάλια είναι ο καλύτερος τρόπος για να διασφαλιστεί το απόρρητο και η απομόνωση για ορισμένες συναλλαγές. Άλλοι μπορεί να αποφασίσουν ότι ένα μόνο κανάλι, μαζί με τα ιδιωτικά δεδομένα, εξυπηρετεί καλύτερα την ανάγκη τους για προστασία της ιδιωτικής ζωής.
- **Χρήση των Κοντέινερ.** Διαφορετικοί χρήστες ενδέχεται επίσης να λάβουν διαφορετικές αποφάσεις σχετικά με τη χρήση των κοντέινερ τους, δημιουργώντας ξεχωριστά κοντέινερ για την διαδικασία των μελών της, είσοδος για τα μέλη, CouchDB, επικοινωνίες gRPC και τον κώδικα αλυσίδας, ενώ άλλοι χρήστες ενδέχεται να αποφασίσουν να συνδυάσουν ορισμένες από αυτές τις διαδικασίες.

Βήμα 2ο

Όπου κι αν επιλέξουμε να αναπτύξουμε τα στοιχεία μας, θα πρέπει να βεβαιωθούμε ότι έχουμε αρκετούς πόρους για να λειτουργούν αποτελεσματικά. Το μέγεθος εξαρτάται από την περίπτωση χρήσης. Εάν σκοπεύουμε να συμμετάσχουμε ένα μέλος σε πολλά κανάλια μεγάλου όγκου, θα χρειαστεί περισσότερη CPU και μνήμη από το να συνδέσουμε ένα μέλος σε ένα μονό κανάλι. Θα χρειαστεί να αφιερώσουμε τρείς φορές περισσότερους πόρους σε ένα μέλος, από ότι θα αφιερώναμε σε ένα κόμβο-εντολέα. Ομοίως, θα πρέπει να αφιερώναμε το ένα δέκατο σε ένα πιστοποιητικό από ότι θα αφιερώναμε σε ένα μέλος. Θα χρειαστεί να προστεθεί χώρος αποθήκευσης στο σύμπλεγμα.

Διαχείριση της υποδομής

- Χρήση μυστικών αντικειμένων για την ασφαλή αποθήκευση σημαντικών αρχείων διαμόρφωσης στο σύμπλεγμα.
- Θέματα συστάδων και μέγεθος κόμβων. Στο βήμα 2 παραπάνω, συζητήσαμε μια γενική περιγραφή για το πώς να σκεφτούμε τις διαστάσεις των κόμβων. Η περίπτωση χρήσης, είναι ο μόνος τρόπος που θα γνωρίζει κάποιος πόσο μεγάλοι θα πρέπει να είναι τα μέλη, οι κόμβοι-εντολών και τα Πιστοποιητικά Αρχής.
- Πώς θα γίνεται η παρακολούθηση των πόρων. Είναι σημαντικό να καθοριστεί μια στρατηγική και μια μέθοδο για την παρακολούθηση των πόρων που χρησιμοποιούνται από τους μεμονωμένους κόμβους και των πόρων που αναπτύσσονται στο σύμπλεγμα γενικά. Καθώς ενώνονται τα μέλη σε περισσότερα κανάλια, πιθανότατα θα χρειαστεί να αυξηθεί η κατανομή της CPU και της μνήμης. Ομοίως, θα πρέπει να βεβαιωθεί ο χρήστης, ότι έχει αρκετό χώρο αποθήκευσης για τη βάση δεδομένων.

Βήμα 3ο

Το πρώτο συστατικό που πρέπει να αναπτυχθεί σε ένα δίκτυο Fabric είναι το ΠΑ. Αυτό συμβαίνει επειδή τα πιστοποιητικά που σχετίζονται με έναν κόμβο (όχι μόνο για τον ίδιο τον κόμβο, αλλά και τα πιστοποιητικά που προσδιορίζουν ποιος μπορεί να διαχειριστεί τον κόμβο) πρέπει να δημιουργηθούν πριν από την ανάπτυξη του ίδιου του κόμβου. Αν και δεν είναι απαραίτητο να χρησιμοποιηθεί το Fabric CA για τη δημιουργία αυτών των πιστοποιητικών, το Fabric CA δημιουργεί επίσης δομές MSP που απαιτούνται για να καθοριστούν σωστά τα στοιχεία και οι οργανισμοί. Εάν ένας χρήστης επιλέξει να χρησιμοποιήσει μια CA διαφορετική από την Fabric CA, θα πρέπει να δημιουργήσει ο ίδιος τους φακέλους MSP.

Βήμα 4ο

Αφού δημιουργηθούν τα ΠΑ, μπορούν να χρησιμοποιηθούν για να δημιουργηθούν τα πιστοποιητικά για τις ταυτότητες και τα στοιχεία που σχετίζονται με τον οργανισμό (το οποίο αντιπροσωπεύεται από ένα MSP). Για κάθε οργανισμό, θα πρέπει τουλάχιστον:

- **Δημιουργία και εγγραφή μιας ταυτότητας διαχειριστή και η δημιουργία MSP.**
  Μετά τη δημιουργία της ΠΑ που θα συσχετιστεί με έναν οργανισμό, μπορεί να χρησιμοποιηθεί για την πρώτη εγγραφή μιας ταυτότητας. Στο πρώτο βήμα, ένα όνομα χρήστη και κωδικός πρόσβασης για την ταυτότητα εκχωρείται από τον διαχειριστή της ΠΑ. Μετά την καταχώριση της ταυτότητας, μπορεί να εγγραφεί χρησιμοποιώντας το όνομα χρήστη και τον κωδικό πρόσβασης. Η ΑΠ θα δημιουργήσει δύο πιστοποιητικά για αυτήν την ταυτότητα - ένα δημόσιο πιστοποιητικό (signcert) γνωστό στα άλλα μέλη του δικτύου και το ιδιωτικό κλειδί (αποθηκευμένο στο φάκελο keystore) που χρησιμοποιείται για την υπογραφή ενεργειών.
- **Δημιουργία και εγγραφή ταυτοτήτων κόμβων**
  Απόφαση σχετικά με το ρόλο του κόμβου(διαχειριστής, μέλος, εντολέας). Όπως και με τον διαχειριστή, μπορούν να εκχωρηθούν χαρακτηριστικά και συσχετισμοί για αυτήν την ταυτότητα. Η δομή MSP για έναν κόμβο είναι γνωστή ως "τοπικό MSP", καθώς τα δικαιώματα που εκχωρούνται στις ταυτότητες είναι σχετικά μόνο σε τοπικό επίπεδο. Αυτό το MSP δημιουργείται όταν δημιουργείται η ταυτότητα του κόμβου και χρησιμοποιείται κατά την εκκίνηση του κόμβου.

Βήμα 5ο
Μόλις συγκεντρωθούν όλα τα πιστοποιητικά και τα MSP που χρειάζονται, είμαστε σχεδόν έτοιμοι να δημιουργήσουμε έναν κόμβο. Ακόμη, θα πρέπει να καθορίσουμε και το μέγεθος του δικτύου μας.

Δημιουργία μελών
Για τη δημιουργία ενός μέλους, πρέπει πρώτα να προσαρμοστεί το αρχείο διαμόρφωσης του μέλους**.**
Υπάρχουν 2 επιλογές σχετικά με τη διαμόρφωση του αρχείου.

- Επεξεργασία του αρχείου YAML
- Χρήση περιβαλλοντικών μεταβλητών κατά την ανάπτυξη

Δημιουργία ενός κόμβου-εντολέα
Σε αντίθεση με τη δημιουργία ενός peer, θα πρέπει να δημιουργηθεί το αρχικό μπλοκ (genesis block).

6.6 Hyperledger Caliper

Το Hyperledger Caliper, είναι ένα εργαλείο αξιολόγησης και ένα από τα έργα Hyperledger που φιλοξενείται από το ίδρυμα Linux. Το Hyperledger Caliper επιτρέπει στους χρήστες να μετρούν την απόδοση μιας συγκεκριμένης εφαρμογής blockchain με ένα σύνολο προκαθορισμένων περιπτώσεων χρήσης. Το Caliper παράγει αναφορές που περιέχουν ένα αριθμό δεικτών απόδοσης, όπως τον δείκτη TPS (συναλλαγές ανά δευτερόλεπτο), την χρήση πόρων, την καθυστέρηση συναλλαγών κλπ.

Για την εκτέλεση του παραδείγματος που φαίνεται στην Εικόνα 36 εκτελούμε την εντολή **node benchmark/simple/main.js –c config-sawtooth.json –n sawtooth.json,** το οποίο θα τρέξει μια αξιολόγηση του δικτύου sawtooth, που ανήκει και αυτό στον Hyperledger. Στο **–c** καθορίζεται το αρχείο διαμόρφωσης, ενώ στο **–n** καθορίζεται το αρχείο διαμόρφωσης του δικτύου blockchain που βρίσκεται υπό δοκιμή (System Under Test).

Test	Name	Succ	Fail	Send Rate	Max Latency	Min Latency	Avg Latency	75%ile Latency	Throughput
1	open	1000	0	50 tps	1.23 s	0.10 s	0.66 s	0.91 s	49 tps
2	open	1000	0	100 tps	1.40 s	0.22 s	0.82 s	1.07 s	97 tps
3	open	1000	0	149 tps	1.81 s	0.45 s	1.15 s	1.40 s	138 tps
4	query	5000	0	100 tps	0.04 s	0.01 s	0.01 s	0.01 s	100 tps
5	query	5000	0	200 tps	0.08 s	0.01 s	0.01 s	0.01 s	200 tps

Εικόνα 36 Δείκτες απόδοσης (sawtooth)

Η στήλη **Succ** είναι ο αριθμός των συναλλαγών που έχουν προστεθεί επιτυχώς στη σκάλα δεδομένων.
Η στήλη **Send Rate** είναι ο αριθμός των συναλλαγών που υποβάλλονται ανά δευτερόλεπτο.
Η στήλη **Throughput** αντιπροσωπεύει τον αριθμό των συναλλαγών που έχει υποβληθεί σε επεξεργασία έναντι του ποσοστού αποστολής (**Send Rate**) που είναι ο ρυθμός ανά δευτερόλεπτο των συναλλαγών που υποβάλλονται στο blockchain.

TYPE	NAME	Memory(max)	Memory(avg)	CPU(max)	CPU(avg)	Traffic In	Traffic Out
Process	node local-client.js(avg)	100.6MB	99.9MB	18.60%	9.00%	-	-
Docker	dev-peer1.org2.example.co...le-v0	7.2MB	6.4MB	1.31%	0.89%	509.8KB	288.3KB
Docker	dev-peer0.org1.example.co...le-v0	7.3MB	6.9MB	3.46%	2.81%	1.4MB	826.6KB
Docker	dev-peer1.org1.example.co...le-v0	7.4MB	6.8MB	2.68%	1.84%	959.9KB	555.6KB
Docker	dev-peer0.org2.example.co...le-v0	7.4MB	7.0MB	4.26%	3.65%	1.8MB	1.1MB
Docker	peer1.org1.example.com	101.2MB	97.2MB	16.47%	13.19%	4.8MB	1.5MB
Docker	peer0.org1.example.com	88.9MB	86.3MB	19.08%	16.23%	5.4MB	5.9MB
Docker	peer1.org2.example.com	102.4MB	96.6MB	13.04%	10.37%	4.3MB	4.4MB
Docker	peer0.org2.example.com	88.3MB	84.5MB	22.36%	19.11%	6.0MB	13.9MB
Docker	ca_peerOrg1	5.0MB	5.0MB	0.00%	0.00%	0B	0B
Docker	ca_peerOrg2	5.2MB	5.2MB	0.01%	0.00%	0B	0B
Docker	couchdb	87.9MB	87.9MB	1.61%	0.35%	0B	0B
Docker	orderer.example.com	31.2MB	24.6MB	7.85%	6.21%	4.3MB	15.5MB

Εικόνα 37 Πόροι που καταναλώνουν οι peers

7 Επίλογος

Η τεχνολογία του blockchain, αν και υπήρχε το 1990, έγινε ευρέως γνωστό το 2008 με την έναρξη του Bitcoin. Όπως όλες οι καινούργιες αλλά και κυρίως οι καινοτόμες ιδέες, στην αρχή προσφέρουν μια δυσπιστία στους μελλοντικούς χρήστες, και αυτό είναι φυσικό, κανείς δεν μπορεί να είναι σίγουρος για κάτι καινοτόμο που μπαίνει στην αγορά του χρήματος, και ειδικότερα όταν εμπλέκονται έννοιες, όπως κρυπτογραφία, ανωνυμότητα και αποκεντροποίηση. Όλοι οι άνθρωποι, ότι χρησιμοποιούσαν όσον αφορά τα συστήματα πληρωμών, είχαν την κυβέρνηση να ελέγχει οποιαδήποτε συναλλαγή πραγματοποιούσαν. Αυτή είναι μια από τις κύριες και πιο σημαντικές καινοτομίες που εισήγαγε το Bitcoin, να εξαλείψει τον «μεγάλο αδερφό» από την χρήση των πληρωμών. Αλλά, ταυτόχρονα να αποτελεί και ένα μειονέκτημα, επειδή στη περίπτωση του Bitcoin οποιαδήποτε συναλλαγή πραγματοποιεί κάποιος, από τη στιγμή που οι μονάδες BTC φεύγουν από τον λογαριασμό του χρήστη, δεν μπορεί να τις ανακτήσει, και αυτό γιατί υπάρχει η ανωνυμότητα. Ενώ με τον παραδοσιακό ηλεκτρονικό τρόπο συναλλαγών (πχ. Τράπεζες), μπορεί να γνωρίζει σε ποιον λογαριασμό πήγαν, αφού ο λογαριασμός μιας τραπέζης λειτουργεί σαν ένα κλειδί που αντιστοιχεί σε ένα μόνο όνομα, όπως και ένα όνομα αντιστοιχεί σε έναν και μόνο λογαριασμό. Ενώ στην περίπτωση του Bitcoin, ένα ιδιωτικό κλειδί (private key) μπορεί να αντιστοιχεί σε πολλά δημόσια κλειδιά (public key) αλλά χωρίς να μπορεί να σε οδηγήσει το δημόσια κλειδί πίσω στο ιδιωτικό κλειδί.

7.1 Σύνοψη και συμπεράσματα

Η τεχνολογία blockchain αποτελεί μια επανάσταση στο τομέα των ηλεκτρονικών συναλλαγών και αυτό το είδαμε από την αρχή της εμφάνισης του μέχρι και τώρα. Κάνει την ζωή απλούστερη και ασφαλέστερη, αλλάζοντας τον τρόπο αποθήκευσης των προσωπικών δεδομένων. Η τεχνολογία blockchain δημιουργεί ένα μόνιμο και αμετάβλητο αρχείο κάθε συναλλαγής. Αυτή η αδιαπέραστη ψηφιακή βάση καθιστά αδύνατη την απάτη, την εισβολή, την κλοπή δεδομένων και την απώλεια πληροφοριών. Η τεχνολογία αυτή θα επηρεάσει κάθε βιομηχανία στον κόσμο, όπως είναι το σύστημα υγείας, τη κυβέρνηση, τα χρηματοπιστωτικά ιδρύματα και τις εταιρείες μεταφορών. [49]

Η τεχνολογία blockchain παρέχει αποτελεσματικότερη επαλήθευση. Αυτή η τεχνολογία είναι επίσης μια ισχυρή βάση δεδομένων που θα μπορούσε εύκολα να συνδυαστεί με μεγάλα δεδομένα (Big Data). Η τεχνολογία μπορεί να βοηθήσει στη μείωση τους κόστους αλλά και να κάνει πολλές υπηρεσίες πιο ανταγωνίστηκες. Ενώ η τεχνολογία blockchain έχει αναμορφώσει και αποκεντρώσει τα χρηματοπιστωτικά ιδρύματα, οι δυνατότητες εφαρμογής της είναι πολύ πιο ισχυρές. Εξετάζεται ενεργά από τις βιομηχανίες τροφίμων και ποτών, αυτοκινήτων, ηλεκτρονικών ειδών, αεροδιαστημικής και άμυνας για την εξασφάλιση πληροφοριών ποιότητας, ασφάλειας, και ιχνηλασιμότητας στις αλυσίδες εφοδιασμού. Εταιρείες όπως η IBM και η Microsoft παρέχουν λύσεις blockchain σε ορισμένες επιχειρήσεις. [50]

Το μέλλον του Blockchain διατηρεί σημαντικές εξελίξεις στην τεχνολογία. Ως μελλοντικό πεδίο εφαρμογής, πρωταρχική προτεραιότητα είναι ο χειρισμός των διαφόρων ζητημάτων ασφαλείας που προκύπτουν από διαφορετικούς τύπους δικτύου blockchain.

Επιπλέον, οι αλγόριθμοι συναίνεσης όπως το PoW που εφαρμόζονται στο blockchain έχουν πολλά μειονεκτήματα. Απαιτεί τεράστια ποσότητα ενέργειας για τον υπολογισμό της τιμής κατακερματισμού. Επομένως, η προσπάθεια ανάπτυξης βελτιωμένου αλγορίθμου συναίνεσης θα είχε ως αποτέλεσμα ένα πιο οικονομικό και αποδοτικότερο δίκτυο blockchain.

Συμπερασματικά, η τεχνολογία Blockchain αποτελεί μια ιδέα, απλή στο πως λειτουργεί, αλλά πολύπλοκη σχετικά με τις λειτουργίες τις. Αποτελεί, μια από τις πιο ασφαλείς βάσεις δεδομένων με συναλλαγές, αλλά όπως κάθε πρόγραμμα, δεν μπορεί να παρέχει 100% ασφάλεια ενάντια σε κακόβουλες επιθέσεις, αυτό το είδαμε στην περίπτωση του 51% Attack. Ακόμη, το σημαντικότερο πλεονέκτημα που μας παρέχει είναι η αποκεντροποιημένη του ιδιότητα, αφού καμία κυβέρνηση δεν μπορεί να επέμβει και να μεταβάλλει τα δεδομένα που περιέχει μέσα αυτή η βάση δεδομένων.

7.2 Μελλοντικές επεκτάσεις

Στην παρούσα εργασία, υπήρχαν εικονικοί peers, που δημιουργήθηκαν από τον ίδιο τον χρήστη, στο μέλλον θα μπορούσαν αυτοί οι χρήστες να αποτελούν πραγματικοί υπολογιστές με διαφορετικό Hardware, όπως για παράδειγμα, μερικοί να έχουν καλύτερες κάρτες γραφικών, άλλοι να έχουν καλύτερους επεξεργαστές, ακόμη μερικού να έχουν ένα ολοκληρωμένο κύκλωμα **FPGA** (Field Programmable Gate Arrays), αλλά και **ASIC** (Application-Specific Integrated Circuits), βέβαια τα δύο τελευταία θα καταστήσουν ακριβή την έρευνα, αλλά θα υπάρχουν και διαφορετικές μετρήσεις, λόγο του ότι τα δύο τελευταία (FPGA & ASIC) υπάρχουν γι' αυτό τον σκοπό, για να γίνεται η εξόρυξη. Με τη έννοια εξόρυξη, δεν εννοούμε την εξόρυξη μονάδων BTC, αλλά την δημιουργία νέων μπλοκ, που περιέχουν μέσα πληροφορίες και δεδομένα μέσω των συναλλαγών, όπως είχαμε δει και στην Ενότητα 2.2 .

Στην εργασία, η έρευνα θα διεξαγόταν με μια απλή συναλλαγή, η συναλλαγή μεταξύ δύο χρηστών που αφαιρείται ένα ποσό X και αυτό το ποσό προστίθεται στο λογαριασμό του δεύτερου. Στο μέλλον, θα μπορούσε να υπάρχει μια πιο πολύπλοκη συναλλαγή, όπως για παράδειγμα μεταξύ περισσοτέρων ατόμων. Ακόμη, αντί για συναλλαγές με χρήματα, θα μπορούσε να γίνει ένα μέσω ανταλλαγής μηνυμάτων, που θα διαθέτει όλα τα χαρακτηριστικά της τεχνολογίας blockchain, αλλά το κυρίως θα ήταν, ότι η συνομιλία θα είναι ασφαλής, που μόνο οι χρήστες που διαθέτουν ιδιωτικά κλειδιά θα έχουν πρόσβαση στο περιεχόμενο της συνομιλίας, αλλά ο τρόπος που θα πραγματοποιείται η δημιουργία νέων μπλοκ θα είναι ίδια, που αντί για μονάδες BTC, θα υπάρχει ένα μήνυμα, που θα αντιστοιχεί στο δημόσιο κλειδί του παραλήπτη, όπου το ιδιωτικό κλειδί του παραλήπτη θα είναι το μοναδικό που θα μπορεί να ανοίξει το μήνυμα.

Η τεχνολογία έχει επεκταθεί σε πολλούς τομείς, όπως χρηματοοικονομικούς και υγείας. Ακόμη, η τεχνολογία αυτή έχει τη δυνατότητα να μεταμορφώσει την εκπαιδευτική βιομηχανία(πχ. Academic certificate), και να κάνει τις διαδικασίες πιο αποτελεσματικές και ασφαλείς. [51] Παρακάτω αναφέρονται μελλοντικές επεκτάσεις της πλατφόρμας:

- Με την εισαγωγή και εφαρμογή IoT συσκευών σε διάφορες βιομηχανίες να παίξουν καθοριστικό ρόλο αντικαθιστώντας όλα τα προϋπάρχοντα συστήματα.

- Υλοποίηση πιλοτικού σε πραγματικές επιχειρήσεις, με τον ορισμό KPI's (Key Performance Indicator) για την αξιολόγηση της πλατφόρμας.

- Υιοθέτηση της τεχνολογίας στο σύστημα υγείας, ώστε ο φάκελος υγείας του ασθενή να μπορεί να είναι προσβάσιμος με το ιδιωτικό κλειδί του ασθενή, ή και ακόμη με την τεχνολογία NFC που χρησιμοποιούμε για τις ανέπαφες συναλλαγές μας.

- Η υιοθέτηση του blockchain θα φέρει σημαντικές αλλαγές στην εφοδιαστική αλυσίδα, αφού θα προσφέρει, διαφάνεια, διασφάλιση ποιότητας, μείωση του κόστους, αλλά θα ενισχύσει τον εντοπισμό των πακέτων.

8 Βιβλιογραφία

[1] A. Sherman, F. Javani, H. Zhang και E. Golaszewksi, « On the Origins and Variations of Blockchain Technologies,» IEEE Security & Privacy, τόμ. 17, αρ. 1, pp. 72-77, 2019.

[2] S. Haber και S. Stornetta, «How to Time-stamp a Digital Document,» Journal of Cryptology, 1991.

[3] D. L. K. CHUEN, HANDBOOK OF DIGITAL CURRENCY, 2015.

[4] D. R. Fernàndez-València, D. J. Caubet και A. Vila, «Cryptography Working Group Introduction to Blockchain Technology,» eurecat, 2018.

[5] M. Muzammal, Q. Qu και B. Nasrulin, «Renovating blockchain with distributed databases: An open source system,» Future Generation Computer Systems, pp. 105-117, 2019.

[6] Z. Zheng, S. Xie, H. Dai, X. Chen και H. Wang, «An Overview of Blockchain Technology: Architecture, Consensus, and Future Tools,» σε 6th International Congress on Big Data, 2017.

[7] B. Cao, Z. Zhang, D. Feng, S. Zhang, L. Zhang, M. Peng και Y. Li, «Performance analysis and comparison of PoW, PoS and DAG based blockchains,» Digital Communications and Networks, pp. 1-12, 2020.

[8] S. King και S. Nadal, PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake, 2012.

[9] W. Rui, K. Ye και X. Cheng-Zhong, «Performance Benchmarking and Optimization for Blockchain Systems: A Survey,» σε Blockchain – ICBC 2019, 2019, pp. 171-185.

[10] A. Kiayias, A. Russell, B. David και R. Oliynykov, «Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol,» σε Advances in Cryptology – CRYPTO 2017, Springer, Cham, 2017, pp. 357-388.

[11] M. Castro και B. Liskov, «Practical Byzantine Fault Tolerance,» Proceedings of the Third Symposium on Operating Systems Design and Implementation, p. 14, 02 1999.

[12] Y. Gilad, R. Hemo, S. Micali, G. Vlachos και N. Zeldovich, «Algorand: Scaling Byzantine Agreements for Cryptocurrencies,» σε SOSP '17: ACM SIGOPS 26th Symposium on Operating Systems Principles, Shanghai China, 2017.

[13] H. Michail, G. Athanasiou, G. Theodoridis, A. Gregoriades και C. Goutis, «Design and implementation of totally-self checking SHA-1 and SHA-256 hash functions' architectures,» Microprocessors and Microsystems, pp. 227-240, 2016.

[14] P. Franco, Understanding Bitcoin: Cryptography, Engineering and Economics, Wiley, 2014.

[15] E. Katsamakas και M. Xin, «Open source adoption strategy,» Electronic Commerce Research and Applications, pp. 1-9, 2019.

[16] C. Ma, X. Kong, Q. Lan και Z. Zhou, «The privacy protection mechanism of Hyperledger Fabric and its application in supply chain finance,» Cynersecurity, pp. 1-9, 2019.

[17] X. Xu, I. Weber και M. Staples, Architecture for Blockchain Applications, 2019.

[18] H. Hellani, H. El Ghor, A. Ellatif Samhat και C. Maroun, «On BlockChain Technology: Overview of Bitcoin and Future Insights,» 2018.

[19] V. Buterin, «A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM,» 2013.

[20] I.-C. Lin και T.-C. Liao, «A Survey of Blockchain Security Issues and Challenges,» International Journal of Network Security, pp. 653-659, 2017.

[21] M. Crawford Urban και D. Pineda, «Inside the Black Blocks,» Mowat Centre, 2018.

[22] P. Helo και Y. Hao, «Blockchains in operations and supply chains: A model and reference implementation,» Computers & Industrial Engineering, pp. 242-251, 2019.

[23] K. Francisco και D. Swanson, «The Supply Chain Has No Clothes: Technology Adoption of Blockchain for Supply Chain Transparency,» Digital Logistics, pp. 1-13, 2018.

[24] L. Chen , W.-K. Lee, C.-C. Chang, K.-K. R. Choo και N. Zhang, «Blockchain based searchable encryption for electronic health record sharing,» Future Generation Computer Systems, pp. 420-429, 2019.

[25] K. Mehboob Khan, J. Arshad και M. Mubashir Khan, «Investigating performance constraints for blockchain based secure e-Voting system,» Future Generation Computer Systems, pp. 13-26, 2020.

[26] Y. Chen και C. Bellavitis, «Blockchain disruption and decentralized finance: The rise of decentralized business models,» Journal of Business Venturing Insights, pp. 1-8, 2020.

[27] R. Ali, J. Barrdear, R. Clews και J. Southgate, «Innovations in payment technologies and the emergence of digital currencies,» Bank of England Quarterly Bulletin, pp. 262-275, 2014.

[28] Ν. Φίλλιπα και Μ. Ρούκη, «Το κρυπτονόμισμα Bitcoin θα είναι το νόμισμα της νέας ψηφιακής εποχής;,» Δελτίον Διοικήσεως Επιχειρήσεων, pp. 60-69, Μάιος - Ιούνιος 2016.

[29] D. G. WOOD, ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER, 2017.

[30] W.-M. Lee, Beginning Ethereum Smart Contracts Programming, Apress, 2019.

[31] «Ethereum,» [Ηλεκτρονικό]. Available: www.ethereum.org. [Πρόσβαση 19 08 2020].

[32] Z. Tu και C. Xue, «Effect of bifurcation on the interaction between Bitcoin and,» ELSEVIER, pp. 382-385, 2019.

[33] «Peercoin University,» 2015. [Ηλεκτρονικό]. Available: www.peercoin.net. [Πρόσβαση 2020].

[34] M. Haferkorn, «Seasonality and Interconnectivity Within Cryptocurrencies - An Analysis on the Basis of Bitcoin, Litecoin and Namecoin,» 2016.

[35] Z.-u.-h. U. author, «Invisible BlockChain and Plasticity of Money – Adam Smith Meets Darwin to Buy Crypto Currency,» 2019.

[36] S. Wan, M. Li , G. Liu και C. Wang, «Recent advances in consensus protocols for blockchain: a survey,» Wireless Network, 2019.

[37] J. Frankenfield, «Investopedia,» 23 09 2019. [Ηλεκτρονικό]. Available: www.investopedia.com. [Πρόσβαση 19 08 2020].

[38] P. Ciaian , M. Rajcaniova και A. Kanes, «The digital agenda of virtual currencies: Can BitCoin become a global currency?,» Information Systems and e-Business Management, pp. 883-919, 2016.

[39] O. Pal, B. Alam, V. Thakur και S. Singh, «Key management for blockchain technology,» ICT Express, pp. 1-5, 2019.

[40] H. Vranken, «Sustainability of bitcoin and blockchains,» Current Opinion in Environmental Sustainability, pp. 1-9, 2017.

[41] A. Toroghi Haghighat και M. Shajari, «Block withholding game among bitcoin mining pools,» Future Generation Computer Systems, pp. 482-491, 2019.

[42] «Hyperledger Caliper,» [Ηλεκτρονικό]. Available: https://hyperledger.github.io/caliper/. [Πρόσβαση 20 09 2020].

[43] «Hyperledger Fabric,» [Ηλεκτρονικό]. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.2/whatis.html#. [Πρόσβαση 19 08 2020].

[44] L. Lamport, R. Shostak και M. Pease, «The Byzantine Generals Problem,» ACM Transactions on Programming Languages and Systems, pp. 382-401, 1982.

[45] N. Lu, Y. Zhang, W. Shi, S. Kumari και K.-K. R. Choo, «A secure and scalable data integrity auditing scheme based on hyperledger fabric,» Computers & Security, pp. 1-16, 2020.

[46] N. Andola, Raghav, M. Gogoi, S. Venkatesan και S. Verma, «Vulnerabilities on Hyperledger Fabric,» Pervasive and Mobile Computing, pp. 1-13, 2019.

[47] «HYPERLEDGER,» [Ηλεκτρονικό]. Available: https://www.hyperledger.org/. [Πρόσβαση 08 10 2020].

[48] V. Dhillon, D. Metcalf και M. Hooper, Blockchain Enabled Applications, Berkeley, CA: Apress, 2017.

[49] M. Attaran και A. Gunasekaran, Applications of Blockchain Technology in Business: Challenges and Opportunities, 2019.

[50] E. Velasco-Castillo, «© Analysys Mason Limited 2016June 2016Nineblockchain opportunities that telecoms operatorsshould explore,» σε analysys mason, 2016.

[51] L. Rujia και W. Yifan , Blockchain based Academic CertificateAuthentication SystemOverview, 2017.

[52] D. L. K. CHUEN, HANDBOOK OF DIGITAL CURRENCY, 2015.

[53] [Ηλεκτρονικό]. Available: www.coinmarketcap.com.

[54] P. Franco, Understanding Bitcoin: Cryptography, Engineering and Economics, Wiley, 2014.