Πανεπιστήμιο Ιωαννίνων Τμήμα

Πληροφορικής και Τηλεπικοινωνιών

Τεχνικές Κρυπτογράφησης και Blockchain

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Θεόδωρος Δρίτσας

Επιβλέπων καθηγητής: Χρυσόστομος Στύλιος

Φοιτητής: Θεόδωρος Δρίτσας

Α.Μ. 10729

2019

Περίληψη

Σκοπός της παρούσας πτυχιακής εργασίας είναι η περιγραφή της νεοεμφανιζόμενης τεχνολογίας Blockchain, των εργαλείων που εφαρμόζει και το πώς αυτές οι τεχνολογίες χρησιμοποιούνται από ένα κατανεμημένο δίκτυο Blockchain, καθώς και πως ξεκίνησε μέσω του Bitcoin αλλά και που εφαρμόζεται.

Έπειτα γίνεται αναφορά στην κρυπτογράφηση, στην διαδικασία δηλαδή της μετατροπής μιας πληροφορίας (κειμένου) σε ένα ακατανόητο κείμενο (κρυπτογράφημα). Στο πως εξελίχθηκε με το πέρασμα των χρόνων ως μυστικό εργαλείο και έφτασε στην εποχή μας να αποτελεί απαραίτητο στοιχείο ασφάλειας σε διάφορους τομείς των επικοινωνιών και των υπολογιστικών συστημάτων. Όπως επίσης και τον τύπο κρυπτογράφησης που χρησιμοποιεί το Bitcoin και το Blockchain.

Επιπλέον αναφέρονται οι περιπτώσεις χρήσης της τεχνολογίας του Blockchain στον τομέα της υγείας, της ενεργειακής αγοράς, στην διαχείριση των αλυσίδων

ανεφοδιασμού των εταιρειών και στην ρευστοποίηση ακίνητων περιουσιακών στοιχείων.

Στη συνέχεια γίνεται λόγος για τη λειτουργία και την αρχιτεκτονική του Hyperledger αλλά και στη διαδικασία της συναίνεσης, η οποία προσφέρει εγγύτητα σε στις συναλλαγές.

Επιπροσθέτως περιγράφεται η λειτουργία της πλατφόρμας Hyperledger Fabric, πως διαφοροποιείται από άλλες κατανεμημένες πλατφόρμες καθώς και τα κίνητρα για τις αρχιτεκτονικές του αποφάσεις.

Στο τέλος παρουσιάζεται ένα project το οποίο είναι ένα demo όπου υλοποιείται ένα σενάριο χρήσης, με χρήστες που θα μπαίνουν στο δίκτυο και ο ένας εκ των οποίων θα εκτελεί μια συναλλαγή που θα μπορούν να βλέπουν όλοι οι χρήστες του δικτύου. Στην περίπτωση μας είναι η αποστολή ενός μη κωδικοποιημένου mail το οποίο κωδικοποιείται μέσω της τεχνολογίας του Hyperledger Fabric.

Λέξεις κλειδιά: αλυσίδα από block, κρυπτογραφημένα δεδομένα, κρυπτογράφηση

Abstract

The purpose of this thesis is to describe the emerging Blockchain technology, the tools that are being deployed, and how these technologies are used by a distributed Blockchain network, as well as how it was launched through Bitcoin but also implemented.

Then reference is made to encryption in the process of converting a text into an incomprehensible text (cryptogram). How it has evolved over the years as a secret tool and has come to be an essential element of security in various areas of communications and computing. As well as the type of encryption used by Bitcoin and Blockchain.

In addition, Bitcoin's technology is being used in health, energy, supply chain management, and real estate liquidation.

It then discusses the operation and architecture of Hyperledger, but also the process of consensus, which offers proximity to a transaction.

In addition, the Hyperledger Fabric platform is described as being differentiated from other distributed platforms as well as incentives for its architectural decisions.

Finally, there is a project that is a demo that implements a usage scenario with users entering the network and one of which will perform a transaction that all network users can see. In our case, we are sending an uncoded mail encoded by Hyperledger Fabric technology.

Keywords: blockchain, cryptographic data, cryptography

ΕΥΧΑΡΙΣΤΙΕΣ

Για την έως τώρα σταδιοδρομία μου θα ήθελα να ευχαριστήσω τους γονείς και τον αδερφό μου, που είναι πάντα δίπλα μου και με στηρίζουν σε όλες τις επιλογές μου. Καθώς δίχως εκείνους δεν θα ήμουν εδώ που βρίσκομαι σήμερα. Επίσης ευχαριστώ την Ιωάννα για την στήριξη, την βοήθεια και την υπομονή της.

Ευχαριστώ την κύριο Χρυσόστομο Στύλιο για την πολύτιμη καθοδήγηση του κατά την διάρκεια των σπουδών μου στο τμήμα, καθώς και για την ανάθεση της πολύ ενδιαφέρουσας πτυχιακής εργασίας. Τον ξάδελφο μου μαθηματικό Ιωάννη Τσακανίκα για τις γνώσεις του και την πολύτιμη βοήθεια του, δίχως τις οποίες το έργο μου θα ήταν πολύ δυσκολότερο.

Τέλος, ευχαριστώ όλους τους καθηγητές του τμήματος που με τις γνώσεις τους διδάσκουν και εμπνέουν τους φοιτητές.

Θεόδωρος Δρίτσας
Φεβρουάριος 2018

Περιεχόμενα

Κεφάλαιο 1

1.1 Ορισμός

Blockchain[1] (στα ελληνικά ο αγγλικός όρος αποδίδεται ποικιλοτρόπως, ως «αλυσίδα μπλοκ» ή «μπλοκ αλυσίδας»,[2][3] «αλυσίδα συστοιχιών»,[4][5] «τεχνολογία κατανεμημένης εγγραφής», «αλυσίδα ομάδων συναλλαγών»,[6], «αλυσίδα κοινοποιήσεων»[7][8][9][10][11][12][13][14][15][16][17][18]) είναι μια νέα τεχνολογία η οποία παρουσιάζεται ως μία δημόσια, μη δυνατόν να τροποποιηθεί το ιστορικό της[19], διανεμημένη σειρά δεδομένων[20], ομαδοποιημένων σε χρονικά αριθμημένα «τμήματα», «συστοιχίες» (blocks). Η πρώτη ιστορικά, εφαρμογή της τεχνολογίας πραγματοποιήθηκε στον χώρο των ψηφιακών νομισμάτων, και ήταν η περίπτωση του bitcoin.

Η τεχνολογία αυτή μπορεί να εφαρμοστεί σε ένα πλήθος επιπλέον περιοχών της ανθρώπινης δραστηριότητας, όπως ενδεικτικά η καταμέτρηση ψήφων[21][22], η Παιδεία[23][24], η Υγεία[25], η διαφύλαξη και διαφάνεια ιστορικών, πολιτιστικών, δημοσιονομικών και άλλων αρχείων[26][27], η πιστοποίηση προϊόντων και υπηρεσιών[28][29], τα κοινωνικά δίκτυα[30][31].

1.2 Δίκτυο και κανόνες

Η τεχνολογία blockchain προκύπτει από ένα δίκτυο ανθρώπων που δημιουργούν και μοιράζονται κάτι κοινό[31]. Το κύριο χαρακτηριστικό του δικτύου αυτού που χρησιμοποιείται στην τεχνολογία της αλυσίδας και στην γλώσσα τον υπολογιστών ανήκει στην κατηγορία δικτύων υπό τον τίτλο δίκτυο ομότιμων κόμβων.

Το δίκτυο είναι αποκεντρωμένο και διανεμημένο ισόποσα. Αυτό σημαίνει ότι δεν υπάρχει κάποιο πρόσωπο του δικτύου που να υπερέχει έναντι κάποιου άλλου προσώπου κατ' οποιονδήποτε τρόπο, οπότε υπάρχει απουσία προτεραιότητας (όποιου είδους), κάποιου προσώπου έναντι κάποιου άλλου. Τα πρόσωπα των συμμετεχόντων στο δίκτυο δεν είναι ίδια, αλλά είναι ίσα μεταξύ τους αναφορικά με οποιαδήποτε διαδικασία εκλογής ή/και επιλογής μεταξύ αυτών. Στατιστικά μιλώντας, εάν τεθεί θέμα εκλογής κάποιου προσώπου, η εκλογή αυτή θα δίνει ίσα ποσοστά επιτυχίας σε κάθε ένα από αυτά τα πρόσωπα και αυτή θα εκτελείται τυχαία.

Όλα τα πρόσωπα του δικτύου blockchain, δημιουργούν και μοιράζονται από κοινού ένα αρχείο. Η διαδικασία δημιουργίας και διαφύλαξης του αρχείου αυτού καθορίζεται και ελέγχεται από ένα Σύνταγμα κανόνων, που ονομάζεται πρωτόκολλο συναίνεσης. Οι κανόνες αυτοί συντάσσονται με βασικό γνώμονα την κατ'εξαίρεση ανάγκη ύπαρξης εμπιστοσύνης ανάμεσα στα πρόσωπα αυτά. Αυτό που εννοεί η παραπάνω φράση αναφέρεται στην ανάγκη για απόδειξη ύπαρξης εμπιστοσύνης μεταξύ των προσώπων του δικτύου μόνο σε εξαιρετικές περιπτώσεις και μάλιστα αν είναι δυνατόν καθόλου[31]. Η σύνταξη ενός συμπαγούς πρωτοκόλλου συναίνεσης απομακρύνει την δημιουργία συνθηκών οι οποίες να οδηγούν στην ανάγκη να αποδείξουν τα πρόσωπα του δικτύου την τιμιότητά τους αναφορικά με την συμμετοχή τους στο δίκτυο, και έτσι ακολούθως, το δικαίωμα συνύπαρξης τους σε αυτό.

1.3 Ιστορία

Η πρώτη ιστορικά εφαρμογή της τεχνολογίας blockchain ήταν το ψηφιακό νόμισμα Bitcoin του Σατόσι Νακαμότο. Στην εργασία αυτή προτεινόταν μια λύση σε ένα διάσημο πρόβλημα των Μαθηματικών με εφαρμογή της λύσης αυτής στον χρηματοοικονομικό τομέα. Ήταν δυνατόν μία κοινότητα ανθρώπων να κτίσουν ένα

δίκτυο από υπολογιστές και μέσω του δικτύου αυτού να εκτελούν χρηματοοικονομικές συναλλαγές μεταξύ τους με αποδεδειγμένη ασφάλεια διαφύλαξης των περιουσιών τους και ταυτόχρονα να μην υπάρχει κεντρική εξουσία που να μπορεί να επέμβει με οποιοδήποτε τρόπο θα ήθελε, στους κανονισμούς οι οποίοι διέπουν την πραγματοποίηση ή όχι όλων αυτών των συναλλαγών. Οι κανονισμοί αυτοί σχεδιάστηκαν από τον προγραμματιστή του πρωτοκόλλου αυτού και αποτελούν το πρωτόκολλο συναίνεσης του Bitcoin, το οποίο χρησιμοποιεί έναν αλγόριθμο απόδειξης μόχθου. Σήμερα χρησιμοποιούνται και άλλοι αλγόριθμοι όπως ο αλγόριθμος απόδειξης μερισμάτων στο ψηφιακό νόμισμα Ethereum.

1.4 Λειτουργία

Όλα τα πρόσωπα που συμμετέχουν στην δημιουργία μιας αλυσίδας κοινοποιήσεων κατέχουν ξεχωριστά και από κοινού ταυτόχρονα ένα πανομοιότυπο αντίγραφο από ένα κοινό αρχείο. Το αρχείο αυτό δεν είναι στατικό, αλλά εμπλουτίζεται συνεχώς με καινούργιο περιεχόμενο. Η ειδοποιός διαφορά του αρχείου blockchain σε αντίθεση με οποιουδήποτε άλλου είδους αρχείο, έγκειται στο ότι σε αυτό απουσιάζει η δυνατότητα διαγραφής δεδομένων σε αυτό.

Πρόκειται για μια αλυσίδα νέων κοινοποιημένων εγγραφών πάνω στο αρχείο αυτό, εγγραφών ομαδοποιημένων σε ομάδες που ονομάζονται τμήματα δεδομένων (datablocks), μπλοκ που αντιστοιχούν και θυμίζουν τους κρίκους μιας αλυσίδας. Και όπως οι κρίκοι μιας αλυσίδας, έτσι και αυτά τα ομαδοποιημένα δεδομένα ή αλλιώς τμήματα (blocks), συγκολλούνται χρονικά το ένα μετά το άλλο δημιουργώντας μια αλυσίδα κατασκευασμένη από κοινού και απευθυνόμενη προς το κοινό, δηλαδή μια αλυσίδα κοινό-ποιήσεων. Η διαδικασία συγκόλλησης επιτυγχάνεται με την λειτουργία μιας συνάρτησης κατακερματισμού πάνω σε ομάδες αυτών, τα λεγόμενα μπλοκ και την δημιουργία κρυπτογραφικών αποτυπωμάτων αυτών.

1.5 Η φύση των ομαδοποιημένων δεδομένων (τμημάτων)

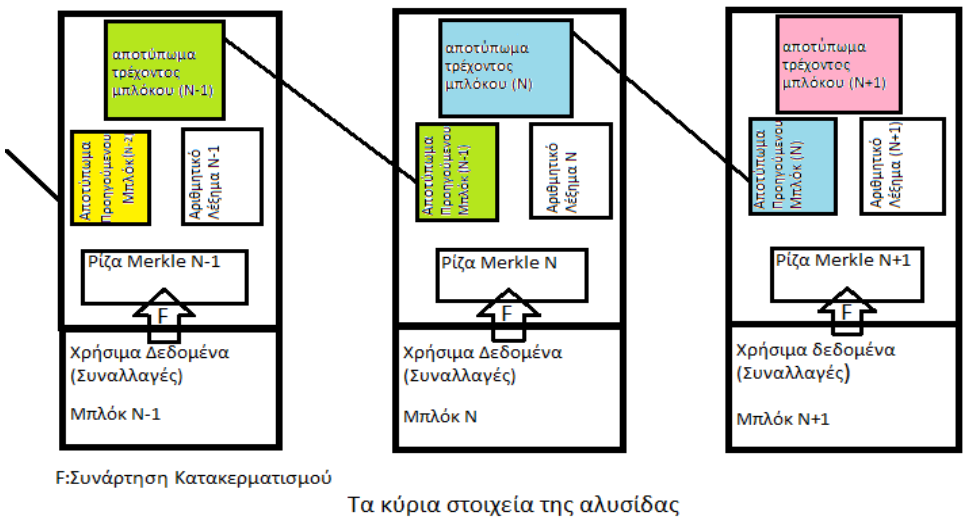
Η φύση των δεδομένων που κοινοποιούνται σε μια αλυσίδα κοινοποιήσεων καθορίζεται από την ύπαρξη ή όχι μιας συγκεκριμένης λειτουργίας των δεδομένων αυτών. Υπάρχουν τα δεδομένα που εγγυώνται την διαδικασία με την οποία όλα (συμπεριλαμβανομένων και των ιδίων) τα ομαδοποιημένα δεδομένα ή μπλοκ, συναρμολογούν μια αλυσίδα κοινοποιήσεων και υπάρχουν και τα δεδομένα που δεν έχουν αυτή την ιδιότητα. Ας ονομάσουμε τα πρώτα αυτά "Σημαντικά Δεδομένα" ή "Δεδομένα Ελέγχου". Τα σημαντικά δεδομένα εγγυώνται την απρόσκοπτη λειτουργία ενός blockchain σύμφωνα με το πρωτόκολλο συναίνεσης που έχει θεσπιστεί για την αλυσίδα αυτή. Τα υπόλοιπα δεδομένα αναφέρονται σε δεδομένα με ανθρώπινο εννοιολογικό περιεχόμενο και για αυτόν ακριβώς τον λόγο είναι αξιόλογα και χρήσιμα για τους κατόχους των δεδομένων αυτών. Ας τα ονομάσουμε "Εννοιολογικά Δεδομένα" ή "Χρήσιμα Δεδομένα".

Στην περίπτωση του Bitcoin τα δεδομένα αυτά περιγράφουν την κατάσταση ενός από κοινού τραπεζικού χαρτοφυλακίου. Εάν θα μιλάγαμε για δεδομένα που περιγράφουν την καταμέτρηση ψήφων, τότε στο τέλος της, η αλυσίδα αυτή θα περιείχε ένα ανόθευτο εκλογικό αποτέλεσμα, εάν πάλι τα δεδομένα αυτά αναφέρονταν σε περιουσίες ακινήτων, θα μιλάγαμε για την ανόθευτη αλυσίδα κοινοποιήσεων του Εθνικού Κτηματολογίου. Με εφαρμογές όπως στην από κοινού πιστοποίηση προϊόντων, στην από κοινού διαφύλαξη πολιτιστικών, ιστορικών, δημοσιονομικών εγγράφων, στην από κοινού διεξαγωγή ανόθευτων και συνάμα τυχερών παιχνιδιών, στην από κοινού σύνταξη συμβολαίων παντός είδους και οποιοδήποτε συνθηκών (τα λεγόμενα έξυπνα συμβόλαια), στην ελεύθερη και ταυτόχρονα ελεγχόμενη από κοινού, διακίνηση ιδεών και πληροφοριών.

1.6 Ρόλοι και αρμοδιότητες

Σε μια Blockchain τα πρόσωπα διακρίνονται και παίρνουν το όνομά τους με βάση τις αρμοδιότητές τους[37]. Μία αρμοδιότητα αναφέρεται στην κατοχή και συνεχή ενημέρωση μέρους ή του συνόλου του αρχείου της αλυσίδας και μια δεύτερη αρμοδιότητα αναφέρεται στο δικαίωμα υποβολής υποψηφιότητας νέων block στην αλυσίδα. Όσοι κόμβοι διαφυλάσσουν μέρος της αλυσίδας ονομάζονται απλά κόμβοι, ενώ οι κόμβοι που διαφυλάσσουν το σύνολο της αλυσίδας, ονομάζονται διαχειριστές-κόμβοι (masternodes). Αμφότεροι χρησιμοποιούν τοπικά τον αποθηκευτικό τους χώρο. Όσοι διαχειριστές-κόμβοι εκτελούν και την δεύτερη αρμοδιότητα ονομάζονται εξορύχοι (miners) και η διαδικασία αυτή ονομάζεται εξόρυξη (mining). Όλοι οι κόμβοι είναι επιφορτισμένοι με το καθήκον του ελέγχου νομιμότητας των μπλοκ που διοχετεύονται σε αυτούς και επιπλέον την προώθηση τους στους γειτονικούς τους κόμβους. Χρήστες του δικτύου ονομάζονται όσοι κόμβοι ή μη, δημιουργούν και διοχετεύουν χρήσιμα δεδομένα σε αυτό.

1.7 Το μπλοκ. Ορισμός και δομή



Τα κύρια στοιχεία της αλυσίδας

Εικόνα 1. Δομή του Block
https://upload.wikimedia.org/wikipedia/commons/thumb/8/8b/%CE%91%CE%BB%CF%85%CF%83%CE%AF%CE%B4%CE%B1_%CE%9A%CE%BF%CE%B9%CE%BD%CE%BF%CF%80%CE%BF%CE%B9%CE%AE%CF%83%CE%B5%CF%89%CE%BD_2.png/220px-%CE%91%CE%BB%CF%85%CF%83%CE%AF%CE%B4%CE%B1_%CE%9A%CE%BF%CE%B9%CE%BD%CE%BF%CF%80%CE%BF%CE%B9%CE%AE%CF%83%CE%B5%CF%89%CE%BD_2.png

Η βασική δομή κάθε μπλοκ περιέχει τις παρακάτω ομάδες δεδομένων.

α) Το κρυπτογραφικό αποτύπωμα του προηγούμενου στην αλυσίδα, μπλοκ (previousblockhash). Τα δεδομένα αυτά ανήκουν στην κατηγορία των σημαντικών δεδομένων. Πρόκειται για έναν δείκτη που καθορίζει την μοναδική ταυτότητα του προηγούμενου μπλοκ.

β)Το κρυπτογραφικό αποτύπωμα που προκύπτει από την λειτουργία μιας συνάρτησης κατακερματισμού πάνω στο σύνολο των εισαχθέντων και ξεχωριστών συναλλαγών(transactions) στο εν λόγω μπλοκ. Στην περίπτωση του bitcoin, κάθε ομάδα συναλλαγών αναφέρεται και περιγράφει μία νομισματική συναλλαγή (cointransaction). Οι συναλλαγές ανήκουν στην κατηγορία των χρήσιμων δεδομένων, ενώ το κρυπτογραφικό τους αποτύπωμα ανήκει στην κατηγορία των σημαντικών δεδομένων. Τα δεδομένα αυτά εντάσσονται στο μπλοκ σε μια διάταξη που στην γλώσσα των υπολογιστών ονομάζεται δέντρο Merkle (Merkletree), και θυμίζει ένα ανεστραμμένο δέντρο. Η κορυφή του ανεστραμμένου αυτού δέντρου ονομάζεται ρίζα Merkle (Merkleroot). Η ρίζα Merkle λοιπόν προκύπτει και περιέχει πληροφοριακά το σύνολο των ενταγμένων στο μπλοκ, συναλλαγών. Να σημειωθεί ότι κάθε Κόμβος

που λαμβάνει μέρος στη διαδικασία υποβολής νέου μπλοκ προς ένταξη στην αλυσίδα blockchain, δεν συμπεριλαμβάνει απαραίτητα τα ίδια χρήσιμα δεδομένα. Προϋπόθεση για την συμπερίληψη μιας συναλλαγής σε ένα υποψήφιο προς ένταξη στην αλυσίδα μπλοκ, είναι η παρουσία των δεδομένων αυτών στον διαχειριστή-κόμβο καθώς σχετίζεται με το επισυναπτόμενο σε αυτήν, κόμιστρο (transactionfee). Το κόμιστρο είναι κλάσμα του ψηφιακού νομίσματος που χρησιμοποιεί η εκάστοτε αλυσίδα. Όσο υψηλότερο είναι το επισυναπτόμενο από τον χρήστη της συναλλαγής κόμιστρο, τόσο υψηλότερα θα βρίσκεται στην λίστα συμπερίληψης συναλλαγών, αυξάνοντας τις πιθανότητες συντομότερης κοινοποίησης.

γ)Την χρονική του σφραγίδα ή χρόνο-σφραγίδα (timestamp). Πρόκειται για τον αριθμό των δευτερολέπτων που έχουν μεσολαβήσει από την 1η Ιανουαρίου του 1970 μέχρι την στιγμή της παραγωγής της χρονο-σφραγίδας.

δ)Την απόδειξη μόχθου του μπλοκ (cryptographic nonce). Πρόκειται για ένα μοναδικά δημιουργημένο αριθμητικό λέξημα. Είναι μια σειρά σημαντικών δεδομένων που παράγεται με τυχαία διεργασία από τον κόμβο-διαχειριστή. Τα δεδομένα ενός αριθμητικού λεξήματος σε ένα μπλοκ που τηρεί τις προϋποθέσεις ένταξης σε μια αλυσίδα blockchain έχουν την εξής ιδιότητα. Η λειτουργία μιας συνάρτησης κατακερματισμού στο σύνολο των δεδομένων των προηγούμενων τριών ομάδων ενός μπλοκ συμπεριλαμβανομένου και του αριθμητικού λεξήματος αυτού, δημιουργεί την τελευταία ομάδα δεδομένων του μπλοκ, ήτοι το

ε)Κρυπτογραφικό αποτύπωμα του εν λόγω μπλοκ. Όπως και στην περίπτωση της ομάδας (α) το αποτύπωμα αυτό καθορίζει την μοναδική ταυτότητα του μπλοκ αυτού. Να σημειωθεί ότι εάν ένα υποψήφιο προς ένταξη μπλόκ στην αλυσίδα blockchain πετύχει να ενταχθεί σε αυτήν, το κρυπτογραφικό του αποτύπωμα θα αποτελέσει την ομάδα (α) του επόμενου από αυτό, μπλοκ.

1.8 Ασφάλεια και ώθηση(κίνητρο)

Blockchain. Η βασική δομή.

Στην τρίτη ομάδα δεδομένων ενός μπλοκ, βρίσκεται το κλειδί της σταθερότητας και ασφαλής λειτουργίας μιας αλυσίδας blockchain. Η εύρεση του κατάλληλου αριθμητικού λεξήματος βασίζεται εξ ολοκλήρου σε τυχαίους παράγοντες και για αυτόν τον λόγο έχει άμεση εξάρτηση με την υπολογιστική ισχύ του εκάστοτε διαχειριστή-κόμβου. Ο σχεδιασμός του πρωτοκόλλου του bitcoin συγκεκριμένα, επιτρέπει επιπροσθέτως την δημιουργία επεξεργαστών σχεδιασμένων κατάλληλα στην κατεύθυνση βελτιστοποίησης των εργασιών τους. Η ιδιότητα αυτή του πρωτοκόλλου του bitcoin το καθιστά ευάλωτο, παρέχοντας ταυτόχρονα υπολογιστική προτεραιότητα στους κατόχους τέτοιων επεξεργαστών δίνει τροφή για κριτική του πρωτοκόλλου[37]. Σε άλλα ψηφιακά νομίσματα, όπως για παράδειγμα το ψηφιακό νόμισμα Monero(XMR), η δυνατότητα εύρεσης τέτοιων στοχευόμενων αναφορικά με την λειτουργία τους επεξεργαστών, απομακρύνεται. Η εύρεση ενός λειτουργικού αριθμητικού λεξήματος αποτελεί την defacto απόδειξη μόχθου στην διαδικασία προσθήκης νέων μπλοκ σε μια αλυσίδα blockchain αφού χρειάζονται αστρονομικά νούμερα παραγωγής και ελέγχου τυχαίων λεξημάτων μέχρι την εύρεση ενός που να λειτουργεί ικανοποιώντας την συνθήκη δυσκολίας του εκάστοτε πρωτοκόλλου. Επιχειρώντας έναν παραλληλισμό, θα λέγαμε ότι η διαδικασία εύρεσης ενός λειτουργικού αριθμητικού λεξήματος μοιάζει με την ρίψη ενός ζαριού με

αστρονομικά μεγάλο αριθμό όψεων, από τις οποίες μόνο ένα πολύ μικρό σύνολο, διασκορπισμένων τυχαία, όψεων αυτού, θεωρούνται επιτυχείς. Όσες περισσότερες οι ρίψεις, τόσες μεγαλύτερη η πιθανότητα εύρεσης κατάλληλου αριθμο-λεξήματος. Η διαδικασία αυτή, της προσπάθειας ανεύρεσης κατάλληλου αριθμο-λεξήματος, είναι στην ουσία αυτό που ονομάζεται εξόρυξη(mining), και είναι αναγκαία η κατανόηση της διαδικασίας αυτής για να μπορέσουμε να καταλάβουμε πώς επιτυγχάνεται ισορροπία στην αλυσίδα ταυτόχρονα με την μη ανάγκη ύπαρξης εγγυήσεων αμοιβαίας εμπιστοσύνης μεταξύ των συμμετεχόντων στο δίκτυο. Να σημειώσουμε ότι η διαδικασία της εξόρυξης κοστίζει με όρους πραγματικής οικονομίας.[37]

Κίνητρο είναι η απόκτηση κλάσματος του νομίσματος της εκάστοτε αλυσίδας, κλάσμα που ορίζεται από το πρωτόκολλο του δικτύου και αποδίδεται αυτόματα στον κόμβο που επιτυγχάνει την ένταξη του μπλοκ που παρήγαγε, στην αλυσίδα blockchain καθιστώντας το, νόμιμο κομμάτι αυτής. Επιπροσθέτως καρπώνονται και τα κόμιστρα των συναλλαγών που ενέταξαν στο μπλοκ τους. Για ευνόητους λόγους, η πρώτη στην λίστα των χρήσιμων δεδομένων συναλλαγή, περιγράφει την ανταμοιβή του μπλοκ.

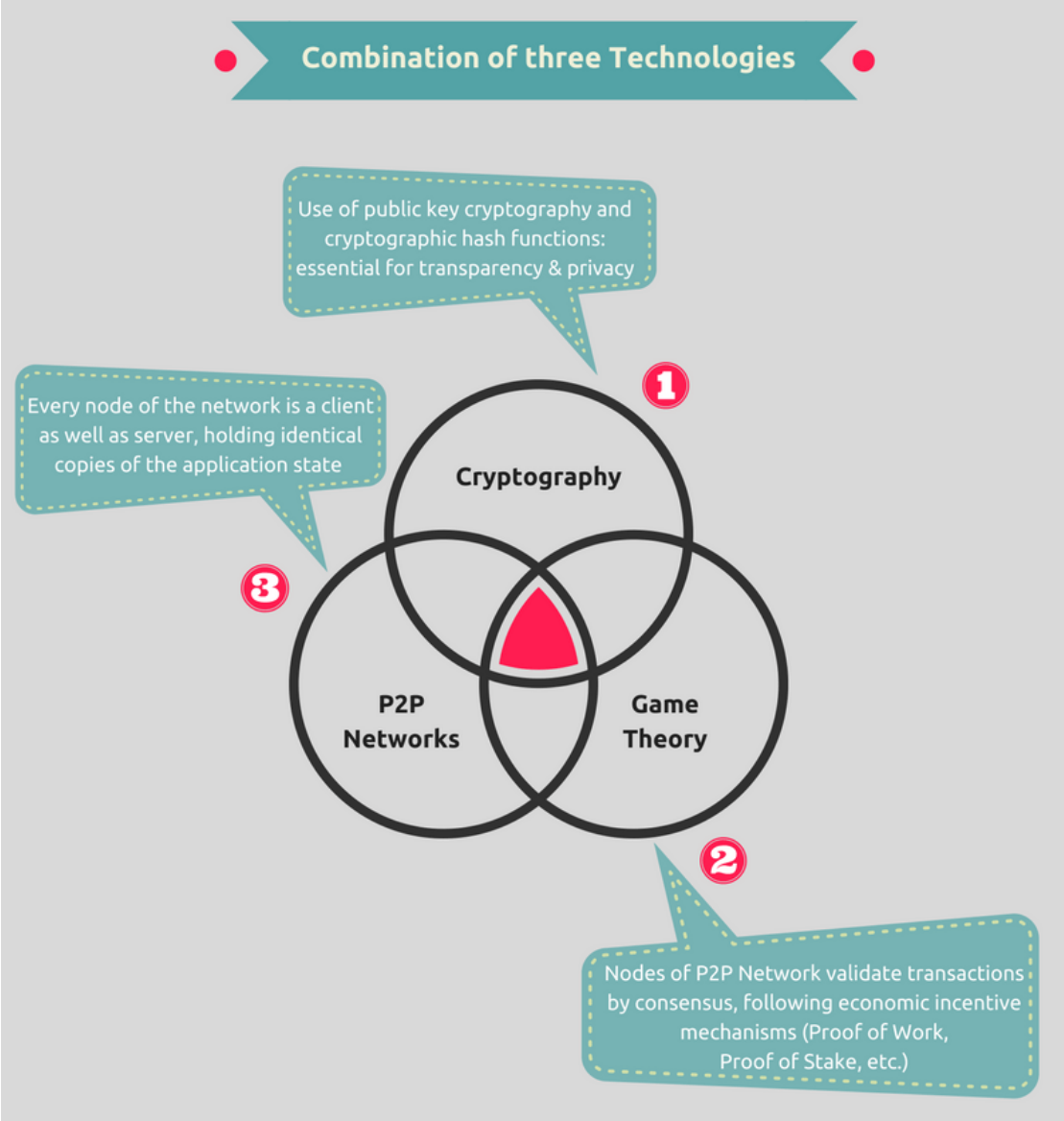
Κεφάλαιο 2

2.1 Κρυπτογραφία & Blockchain

Από πού προέρχεται η κρυπτογράφηση ή κρυπτοσυχνότητα;

Το αρχικό πρωτόκολλο BitcoinBlockchain εισήγαγε την έννοια της Cryptoeconomics, ενός συνδυασμού κρυπτογραφίας και οικονομικών για τη δημιουργία αξιόπιστων, ανεκτικών σε σφάλματα και ανθεκτικών σε προσβολές αποκεντρωμένων δικτύων P2P. Ενώ η κρυπτογραφία χρησιμοποιείται για τη διατήρηση της ιδιωτικής ζωής και της διαφάνειας, χρησιμοποιούνται οικονομικά κίνητρα για την ενθάρρυνση της επιθυμητής συμπεριφοράς των φορέων του δικτύου που δεν εμπιστεύονται ή γνωρίζουν ο ένας τον άλλον, ούτε έχουν νομικά δεσμευτικές συμφωνίες μεταξύ τους[38].

Blockchains όπως το Bitcoin, το Ethereum και παρόμοια πρωτόκολλα βασίζονται στον συνδυασμό τριών τεχνολογιών: δίκτυα P2P, κρυπτογραφία και θεωρία παιγνίων. Στόχος είναι να διασφαλιστεί ότι ένα ανόμοιο δίκτυο παραγόντων, οι οποίοι δεν γνωρίζουν ή δεν εμπιστεύονται ο ένας τον άλλον, καταλήγουν σε συναίνεση ως προς το ποια συναλλαγή είναι σωστή, χωρίς τη βοήθεια ενός κεντρικού διαχειριστή[38]. Αυτός είναι ο λόγος για τον οποίο αναφέρεται επίσης ως πρωτόκολλο ελέγχου . Αυτός ο μοναδικός συνδυασμός μας επιτρέπει να έχουμε πραγματικές συναλλαγές P2P χωρίς οργανισμούς εκκαθάρισης.[38]



Εικόνα 2. Αρχιτεκτονική Cryptography&Blockchain – Part 1https://blockchainhub.net/blog/blog/cryptography-blockchain-part-1/

Το BlockchainBitcoin χρησιμοποιεί κρυπτογραφίες δημόσιου κλειδιού και κρυπτογραφικές λειτουργίες κατακερματισμού για την επίτευξη αυτού του στόχου.

Αλλά ας δούμε λεπτομερώς: τι είναι η κρυπτογραφία και πώς λειτουργεί;

2.2 Ιστορία της κρυπτογραφίας

Η κρυπτογραφία είναι η πρακτική και η μελέτη τεχνικών για ασφαλή επικοινωνία παρουσία τρίτων. Η βιβλιογραφία της κρυπτογραφίας συχνά χρησιμοποιεί το όνομα Alice "A" για τον αποστολέα, τον Bob "B" για τον αποδέκτη και την Eve "Eavesdropper" για τον αντίπαλο. Το ιστορικό της κρυπτογράφησης χρονολογείται από την εμφάνιση του αναλογικού κειμένου και έχει εξελιχθεί σημαντικά στην εποχή του υπολογιστή[38].

Μέχρι τις σύγχρονες εποχές, η κρυπτογραφία αναφέρεται σχεδόν αποκλειστικά στην κρυπτογράφηση , η οποία είναι η διαδικασία της μετατροπής μιας πληροφορίας (κειμένου) σε ένα ακατανόητο κείμενο (κρυπτογράφημα). Το Cyphertext είναι κρυπτογραφημένη ή κωδικοποιημένη πληροφορία που περιέχει μια μορφή του αρχικού κειμένου, αλλά δεν μπορεί να διαβαστεί από έναν άνθρωπο ή υπολογιστή χωρίς το κατάλληλο κρυπτογραφημένο κώδικα για να αποκρυπτογραφηθεί .

Οι Cyphers ήταν μία από τις πρώτες τεχνικές κρυπτογράφησης που αναπτύχθηκαν για την κρυπτογράφηση απλού κειμένου με κρυπτογράφηση αντικατάστασης.

Η αποκρυπτογράφηση είναι η αντίστροφη, με άλλα λόγια, μετακινώντας από το ακατανόητο κρυπτογράφημα πίσω στο απλό κείμενο. Ένας κρυπτογράφος είναι ένα ζεύγος αλγορίθμων που δημιουργούν την κρυπτογράφηση καθώς και την αποκρυπτογράφηση αναστροφής: Είναι εύκολο να κρυπτογραφήσετε ένα μήνυμα, αλλά είναι πολύ δύσκολο να το αντιστρέψετε αν δεν γνωρίζετε τον κώδικα. Με την

εφεύρεση των υπολογιστών οι κλασικοί κρυπτόγραφοι(ciphers) έγιναν περιττοί επειδή ήταν πολύ εύκολο να μαντέψουν με απλές βίαιες επιθέσεις , όπου ένας αλγόριθμος ηλεκτρονικού υπολογιστή τρέχει όλους τους πιθανούς συνδυασμούς, μέχρι να μαντέψει τον σωστό κώδικα. Η παλαιότερη γνωστή χρήση της κρυπτογραφίας είναι κάποιο σκαλιστό κρυπτογράφημα σε πέτρα στην Αίγυπτο. Στο Ινδία (Kautiliyam και Mulavediya), SassanidPersia, από τους Αρχαίους Έλληνες, τους Ρωμαίους, τους Εβραίους, χρησιμοποιήθηκαν διαφορετικές μορφές κρυφών ψηφίων, για να αναφέρουμε μόνο λίγους[38].

Πριν από τις αρχές του 20ου αιώνα, κρυπτογραφία αφορούσε κυρίως γλωσσικά και λεξικογραφικά σχέδια. Από την ανάπτυξη των μηχανών κρυπτογράφησης στον Α 'Παγκόσμιο Πόλεμο και την έλευση των υπολογιστών στον Β' Παγκόσμιο Πόλεμο, οι μέθοδοι που χρησιμοποιούνται για την εκτέλεση της κρυπτολογίας έχουν γίνει όλο και πιο πολύπλοκες και η εφαρμογή τους πιο διαδεδομένη. Η έμφαση έχει μετατοπιστεί και η κρυπτογραφία υπάρχει στη διασταύρωση των μαθηματικών, της επιστήμης των υπολογιστών, της ηλεκτρολογίας, της επικοινωνιακής επιστήμης και της κβαντικής φυσικής. Με την έλευση του κβαντικού υπολογιστή υπάρχει επίσης ενεργός έρευνα που εξετάζει τη σχέση μεταξύ των κρυπτογραφικών προβλημάτων και της κβαντικής φυσικής[38]

Οι υπολογιστές και τα ηλεκτρονικά στοιχεία όχι μόνο βελτίωσαν τις δυνατότητες κρυπτοανάλυσης (σπάσιμο της κρυπτογράφησης), αλλά και καθιστούσαν δυνατούς πιο περίπλοκους κρυπτογράφους. Οι υπολογιστές εισήγαγαν επίσης νέες μορφές κρυπτογράφησης κάθε είδους ψηφιακών πληροφοριών, όχι μόνο των γλωσσικών κειμένων. Οι πιθανές επιπτώσεις της κβαντικής πληροφορικής εξετάζονται ήδη από ορισμένους σχεδιαστές κρυπτογραφικών συστημάτων που αναπτύσσουν μετα-κβαντική κρυπτογραφία . η επικείμενη εφαρμογή μικρών εφαρμογών αυτών των

μηχανών μπορεί να κάνει την ανάγκη για αυτή την προληπτική προσοχή μάλλον παρά απλώς κερδοσκοπική[38].

Οι κρυπτογραφικοί αλγόριθμοι σχεδιάζονται γύρω από υποθέσεις υπολογιστικής σκληρότητας: ενώ θεωρητικά είναι δυνατόν να σπάσουν ένα τέτοιο σύστημα, έχουν σχεδιαστεί ώστε να μην μπορούν να σπάσουν με κανένα γνωστό πρακτικό μέσο (χρόνο ή / και χρήμα)[38].

Η ανάπτυξη της κρυπτογραφικής τεχνολογίας έχει προκαλέσει μια σειρά νομικών ζητημάτων στην εποχή της πληροφόρησης. Το δυναμικό της κρυπτογραφίας ως εργαλείου για κατασκοπεία έχει οδηγήσει πολλές κυβερνήσεις να το ταξινομήσουν ως όπλο και να περιορίσουν ή ακόμη και να απαγορεύσουν τη χρήση και την εξαγωγή τους. Σε ορισμένες περιπτώσεις όπου η χρήση της κρυπτογραφίας είναι νόμιμη, οι νόμοι επιτρέπουν στους ανακριτές να υποχρεώνουν την αποκάλυψη κλειδιών κρυπτογράφησης για έγγραφα που σχετίζονται με μια έρευνα.

Επιπλέον οι ερωτήσεις σχετικά με τα ανθρώπινα δικαιώματα σε μια ψηφιακή εποχή και ο τρόπος με τον οποίο πρέπει να ερμηνευθεί το συνταγματικό δικαίωμα στην ιδιωτική ζωή της επικοινωνίας ("μυστικότητα της επιστολής") και αν αντιστοιχεί ή όχι στο δικαίωμα κρυπτογραφημένης επικοινωνίας, πρέπει να αντιμετωπιστεί δημοσίως και γενικά σε όλο τον κόσμο[38].

2.3 Σύγχρονη κρυπτογραφία

Η πρώιμη κρυπτογράφηση προσπάθησε να εξασφαλίσει μυστικότητα στις επικοινωνίες, όπως εκείνες των κατασκόπων, των στρατιωτικών ηγετών και των διπλωματών. Τις τελευταίες δεκαετίες, το πεδίο έχει επεκταθεί πέρα από τις ανησυχίες περί εμπιστευτικότητας ώστε να περιλαμβάνει τεχνικές ηλεκτρονικού εμπορίου, κάρτες πληρωμών με τσιπ, ψηφιακά νομίσματα, διαχείριση ψηφιακών δικαιωμάτων, διαχείριση κωδικών πρόσβασης, έλεγχος ακεραιότητας μηνυμάτων, έλεγχος ταυτότητας αποστολέα / παραλήπτη, ψηφιακές υπογραφές και ασφαλείς υπολογισμοί. Υπάρχουν δύο είδη κρυπτοσυστημάτων: συμμετρικά και ασύμμετρα[38] .

Συμμετρική κρυπτογραφία.

Δύο μέρη συμφωνούν σε ένα μυστικό κλειδί (ιδιωτικό κλειδί) και χρησιμοποιούν το ίδιο κλειδί για κρυπτογράφηση και αποκρυπτογράφηση. Το πρόβλημα με αυτή την προσέγγιση είναι ότι αυτή η μέθοδος δεν κλιμακώνεται. Αν θέλατε να επικοινωνήσετε ιδιωτικά με κάποιον θα χρειαστεί συναντηθείτε και να συμφωνήσετε σε ένα μυστικό κλειδί. Στον κόσμο των σύγχρονων επικοινωνιών, όπου πρέπει να συντονίσουμε με πολλούς παράγοντες, τέτοιες μέθοδοι δεν θα ήταν εφικτές. Επί πλέον ο χειρισμός δεδομένων σε συμμετρικά συστήματα είναι ταχύτερος από τα ασύμμετρα συστήματα, καθώς χρησιμοποιούνται ευρέως.[38].

Από την άλλη πλευρά, η κρυπτογράφηση αρχείων και μηνυμάτων με ασύμμετρους αλγορίθμους μπορεί να μην είναι πάντα πρακτική. Ο κύριος λόγος είναι η απόδοση. Η κρυπτογράφηση συμμετρικού κλειδιού είναι πολύ ταχύτερη και χειρίζεται

καλύτερα την κρυπτογράφηση μεγάλων αρχείων και βάσεων δεδομένων, επομένως, εξακολουθεί να χρησιμοποιείται ευρέως.

Ασύμμετρη κρυπτογραφία (κρυπτογραφία δημόσιου κλειδιού).

Τα ασύμμετρα συστήματα χρησιμοποιούν ένα δημόσιο κλειδί για την κρυπτογράφηση ενός μηνύματος και ένα ιδιωτικό κλειδί για την αποκρυπτογράφηση του. Η χρήση ασύμμετρων συστημάτων ενισχύει την ασφάλεια της επικοινωνίας. Παραδείγματα ασύμμετρων συστημάτων περιλαμβάνουν RSA (Rivest-Shamir-Adleman) και ECC (κρυπτογράφηση ελλειπτικής καμπύλης)[38].

Τα ιδιωτικά κλειδιά θα πρέπει να παραμένουν μυστικά και ένα δημόσιο κλειδί θα μπορεί να διανεμηθεί ελεύθερα μεταξύ των μερών. Σε ένα ασύμμετρο σενάριο κρυπτογράφησης, δύο μέρη θα διανέμουν τα δημόσια κλειδιά τους και θα επιτρέψουν σε οποιονδήποτε να κρυπτογραφήσει μηνύματα χρησιμοποιώντας τα συγκεκριμένα δημόσια κλειδιά. Λόγω του πώς ένα μαθηματικό ζεύγος κλειδιών λειτουργεί είναι αδύνατο να αποκρυπτογραφήσει ένα μήνυμα το οποίο αποκτήθηκε κρυπτογραφημένο με ένα δημόσιο κλειδί[38]. Το μήνυμα αυτό μπορεί να ταξιδέψει με ασφάλεια στον ιδιοκτήτη του ιδιωτικού κλειδιού και μόνο αυτός / αυτή θα είναι σε θέση να αποκρυπτογραφήσει το μήνυμα χρησιμοποιώντας το ιδιωτικό κλειδί που συνδέεται με το δημόσιο κλειδί (λουκέτο). Αυτή η μέθοδος λειτουργεί αντίστροφα. Οποιοδήποτε μήνυμα κρυπτογραφείται με ιδιωτικό κλειδί μπορεί να αποκρυπτογραφηθεί μόνο με το αντίστοιχο δημόσιο κλειδί. Αυτή η μέθοδος αναφέρεται επίσης ως ψηφιακή υπογραφή.

Κεφάλαιο 3

3.1 Blockchain και Bitcoin

Παρακάτω θα δούμε τις λεπτομέρειες του τύπου κρυπτογράφησης που χρησιμοποιείται στο Bitcoin και παρόμοια πρωτόκολλα Blockchain. Άλλα Blockchains ενδέχεται να χρησιμοποιούν εναλλακτικούς κρυπτογραφικούς αλγόριθμους. Ορισμένες αλυσίδες μπλοκ, για παράδειγμα, χρησιμοποιούν περισσότερη κρυπτογράφηση που δίνει έμφαση στην προστασία της ιδιωτικής ζωής, όπως για παράδειγμα το Zcash (αποδείξεις μηδενικής γνώσης), το Monero (RingSignatures)[39].

3.2 Τύπος κρυπτογραφίας που χρησιμοποιείται στο Bitcoin

Το πρωτόκολλο BlockchainBitcoin χρησιμοποιεί κρυπτογράφηση δημόσιου κλειδιού για ψηφιακές υπογραφές και κρυπτογραφικές λειτουργίες κατακερματισμού, λεπτομέρειες των οποίων θα εξηγηθούν παρακάτω[39]. Ο κρυπτογραφικός αλγόριθμος που χρησιμοποιείται στο Bitcoin ονομάζεται κρυπτογράφηση ελλειπτικής καμπύλης . Είναι ένας τύπος ασύμμετρης κρυπτογραφίας που θεωρείται πιο αποδοτικός σε σύγκριση με την κλασσική κρυπτογραφία RSA. Ενώ η κρυπτογραφία ελλειπτικής καμπύλης παρέχει το ίδιο επίπεδο ασφάλειας όπως το RSA, επίσης χρειάζεται μικρότερο υπολογισμό και μικρότερο μέγεθος κλειδιού , μειώνοντας έτσι τις απαιτήσεις αποθήκευσης και μετάδοσης.

3.3 Κρυπτογραφία δημόσιου κλειδιού: Κρυπτογραφικά κλειδιά

Εάν δύο ή περισσότεροι άνθρωποι επιθυμούν να πραγματοποιήσουν ασφαλείς συναλλαγές μέσω του διαδικτύου, μπορούν να χρησιμοποιήσουν ασύμμετρη κρυπτογραφία που επίσης αναφέρεται ως κρυπτογραφία δημόσιου-ιδιωτικού κλειδιού. Αυτή η τεχνολογία τους επιτρέπει να αποδείξουν την ταυτότητά τους με ένα σύνολο κρυπτογραφικών κλειδιών: ένα ιδιωτικό κλειδί και ένα δημόσιο κλειδί.

Ο συνδυασμός αυτών δημιουργεί μια ψηφιακή υπογραφή. Ο κύριος σκοπός της χρήσης κρυπτογραφίας δημόσιου-ιδιωτικού κλειδιού για το BlockchainBitcoin είναι η δημιουργία ασφαλούς ψηφιακής αναφοράς σχετικά με την ταυτότητα ενός χρήστη. Επομένως, η ταυτότητα ενός κατόχου πορτοφολιού βασίζεται στην κατοχή ενός συνδυασμού ιδιωτικών και δημόσιων κρυπτογραφικών κλειδιών. Οι ψηφιακές υπογραφές αποδεικνύουν την κατοχή των περιουσιακών στοιχείων του χρήστη και του επιτρέπουν να ελέγχει τα κεφάλαιά του.[39]

Παρόμοια με μια χειρόγραφη υπογραφή, χρησιμοποιείται μια ψηφιακή υπογραφή για να υπάρξει βεβαίωση ότι ο χρήστης είναι αυτός που λέει ότι είναι. Στο Bitcoin και σε άλλα Blockchains, οι ψηφιακές υπογραφές είναι μαθηματικές λειτουργίες που αντιστοιχούν σε ένα συγκεκριμένο πορτοφόλι . Πρόκειται για ψηφιακή αναγνώριση ενός πορτοφολιού. Προσθέτοντας μια ψηφιακή υπογραφή σε μια συναλλαγή, κανείς δεν μπορεί να αμφισβητήσει ότι η συναλλαγή αυτή προήλθε από το πορτοφόλι από το οποίο φέρεται να προέρχεται και ότι το πορτοφόλι δεν μπορεί να μιμηθεί άλλο πορτοφόλι[39].

Το ιδιωτικό κλειδί χρησιμοποιείται για την κρυπτογράφηση των συναλλαγών, ενώ το δημόσιο κλειδί χρησιμοποιείται για την αποκρυπτογράφηση. Το ιδιωτικό κλειδί πρέπει να διατηρείται ιδιωτικό ανά πάσα στιγμή καθώς ενεργεί ως "κωδικός πρόσβασης". Το δημόσιο κλειδί προορίζεται να μοιραστεί με τρίτους και εξασφαλίζει ότι είστε ιδιοκτήτης μιας διεύθυνσης που μπορεί να λάβει χρήματα. Τον αποστολέα τον κρυπτογραφεί η συναλλαγή με το ιδιωτικό κλειδί του, το οποίο μπορεί να αποκρυπτογραφηθεί από τον παραλήπτη μόνο με το δημόσιο κλειδί του αποστολέα. Εάν το δημόσιο κλειδί του αποστολέα δεν λειτουργεί για να αποκρυπτογραφήσει τη συναλλαγή, αυτό σημαίνει ότι η συναλλαγή δεν είναι από το ίδιο πορτοφόλι. Το δημόσιο και το ιδιωτικό κλειδί είναι απαραίτητα για την υπογραφή των συναλλαγών από τους χρήστες.

3.4 Bitcoin πορτοφόλι

Σε αντίθεση με την κοινή πεποίθηση, ένα πορτοφόλι κρυπτογράφησης δεν αποθηκεύει νομίσματα, αλλά μόνο το ζεύγος δημόσιου-ιδιωτικού κλειδιού που σχετίζεται με τη διεύθυνση bitcoin σας. Το ίδιο ισχύει και για άλλα πορτοφόλια με κρυπτογράφηση. Ένα πορτοφόλι λειτουργεί απλά ως ασφαλές κλειδί αποθήκευσης και ως εργαλείο επικοινωνίας με το blockchain. Όταν στέλνουμε ή λαμβάνουμε Bitcoin, χρησιμοποιούμε το πορτοφόλι κρυπτογράφησης για να υπογράψουμε τη συναλλαγή με το δημόσιο-ιδιωτικό κλειδί που έχει αποθηκεύτει στο πορτοφόλι. Στη συνέχεια, το προσωπικό μας Bitcoin βρίσκεται σε λειτουργία[39].

3.5 Διεύθυνση Bitcoin

Μια διεύθυνση Bitcoin είναι σαν μια διεύθυνση ηλεκτρονικού ταχυδρομείου που μπορούν να αποσταλούν τα χρήματα. Το δημόσιο κλειδί χρησιμοποιείται από το πορτοφόλι για τη δημιουργία μιας διεύθυνσης Bitcoin.

Οι διευθύνσεις μπορούν να ληφθούν δωρεάν, χρησιμοποιώντας οποιοδήποτε είδος παρόχου πορτοφολιών. Ένα πορτοφόλι στο πλαίσιο του Bitcoin είναι μια εφαρμογή που αποθηκεύει το ιδιωτικό κλειδί του χρήστη, το δημόσιο κλειδί, την διεύθυνση Bitcoin και αλληλεπιδρά με το BitcoinBlockchain. Αυτό το λογισμικό πορτοφολιών μπορεί να εκτελεστεί στον υπολογιστή του ή στο κινητό του τηλέφωνο (όπως το BitcoinCore, Electrum) ή μια ειδική συσκευή υλικού (όπως Tezos, Ledger κ.λπ.)[39]

Τα δημόσια και τα ιδιωτικά κλειδιά είναι κρυμμένα εκτός αν εξάγονται με το χέρι. Ο χρήστης πρέπει να βεβαιωθεί ότι έχει εξαγάγει τα κλειδιά και τη διεύθυνσή του. Εάν χάσει το πορτοφόλι του, χωρίς να έχει εφεδρικό αντίγραφο της διεύθυνσης και του ιδιωτικού κλειδιού του, θα χάσει την πρόσβαση στα χρήματά του. Όπως για παράδειγμα υποθέτοντας ότι κάποιος στέλνει κάποια χρήματα στη διεύθυνση bitcoin ενός χρήστη, αλλά ο υπολογιστής του έσπασε με την εφαρμογή πορτοφολιού.

3.6 Hashes, ψηφιακές υπογραφές και πορτοφόλια

Το BitcoinNetwork χρησιμοποιεί χτύπημα σε συνδυασμό με ψηφιακές υπογραφές για να προστατεύσει την ακεραιότητα των δεδομένων που ρέουν μέσα από το Blockchain. Όταν ξεκινάει για πρώτη φορά, ένα πορτοφόλι κρυπτογράφησης παράγει ένα ζεύγος κλειδιών. Αυτό το ζεύγος κλειδιών αποτελείται από ένα ιδιωτικό κλειδί και ένα αντίστοιχο δημόσιο κλειδί . Το ιδιωτικό κλειδί (κωδικός πρόσβασης) είναι ένας ακέραια δημιουργούμενος ακέραιος 256-bit. Το δημόσιο κλειδί προέρχεται από

το ιδιωτικό κλειδί και ενεργεί όπως ο αριθμός του τραπεζικού λογαριασμού του χρήστη. Τόσο το ιδιωτικό κλειδί όσο και το δημόσιο κλειδί δεν εμφανίζονται ποτέ στον χρήστη εκτός εάν εξάγονται. Το ιδιωτικό κλειδί πρέπει πάντα να μένει μυστικό και να μην μοιράζεται ποτέ με άλλους ανθρώπους.

Υπάρχει μια μαθηματική σχέση μεταξύ των δύο πλήκτρων. Η σχέση μεταξύ δημόσιων και ιδιωτικών κλειδιών καθορίζεται από μονόδρομους κρυπτογραφικούς αλγορίθμους. Στην επιστήμη των υπολογιστών, μια λειτουργία μονής κατεύθυνσης είναι μια λειτουργία που είναι εύκολο να υπολογιστεί σε κάθε είσοδο, αλλά είναι δύσκολο να αντιστραφεί δεδομένης της εικόνας μιας τυχαίας εισόδου. Αυτό σημαίνει ότι το δημόσιο κλειδί προέρχεται μαθηματικά από το ιδιωτικό του κλειδί, αλλά χρησιμοποιώντας αντίστροφα μαθηματικά για να αντλήσει το ιδιωτικό κλειδί θα έπαιρνε τον πιο ισχυρό υπερυπολιστή τρισεκατομμυρίων ετών για να σπάσει, καθιστώντας το πρακτικά αδύνατο.

Υπάρχουν κάποια πρόσθετα βήματα πριν από την εμφάνιση της τελικής έκδοσης του δημόσιου κλειδιού. Για τη δημιουργία της διεύθυνσης Bitcoin, το δημόσιο κλειδί χρησιμοποιεί το RIPEMD160 (RACE IntegrityPrimitivesEvaluationMessageDigest) και το SHA-256 (SHA: SecureHashAlgorithm). Η δημιουργούμενη συμβολοσειρά είναι το μόνο πράγμα που βλέπει ο χρήστης στο πορτοφόλι του[39].

3.7 Hashing στο Bitcoin

Ο κρυπτογραφικός κατακερματισμός είναι μια μέθοδος μετατροπής μεγάλων ποσοτήτων δεδομένων σε μικρούς αριθμούς που είναι δύσκολο να μιμηθούν. Τα hashes χρησιμοποιούνται κυρίως σε συνδυασμό με ψηφιακές υπογραφές. Αυτές οι λειτουργίες διασφαλίζουν την ακεραιότητα των δεδομένων. Το δίκτυο Bitcoin χρησιμοποιεί SHA (SecureHashAlgorithm) όπως το SHA-256. Με λίγα λόγια, τα

hashes είναι κρυπτογραφικές λειτουργίες μονής κατεύθυνσης που λαμβάνουν κάθε τύπο εισόδου (συμβολοσειρά, αρχεία, κλπ.). Μια σημαντική ιδιότητα των hashes είναι ότι αν αλλάξει μια μικρή ποσότητα δεδομένων εισόδου, η έξοδος αλλάζει σημαντικά[39].

Η αντίστοιχη SHA-256 της φράσης " Πώς να αγοράσετε το Bitcoin; "Μοιάζει με αυτό:

156aedcfab1d49f73abddd89faf78d9930e4b523ab804026310c973bfa707d37

Εάν αφαιρέσουμε μόνο ένα σύμβολο - για παράδειγμα το ερωτηματικό ";" - το hash του " Πώς να αγοράσετε Bitcoin " μοιάζει με αυτό: 4314d903f04e90e4a5057685243c903fbcfa4f8ec75ec797e1780ed5c891b1bf[39]

Όπως μπορούμε να δούμε, παράγεται ένα εντελώς διαφορετικό hash, όταν αλλάζουμε μόνο ένα γράμμα. Βασίζεται στο λεγόμενο "εφέ χιονοστιβάδας" και είναι χρήσιμο για την εύκολη παροχή της ακεραιότητας των δεδομένων.

Εάν έχουμε hash, το υπάρχον hash εδώ είναι το αποτέλεσμα:

4c9622e1148ff0b855de50e62999d194039eb2faa9e715cc9d9ef604015aa1fe[39]

Και πάλι εντελώς διαφορετική συμβολοσειρά αλλά πάντα το ίδιο μήκος.

Hashing χρησιμοποιείται για τέσσερις διαδικασίες:

- Κωδικοποίηση διευθύνσεων πορτοφολιού
- Κωδικοποίηση των συναλλαγών μεταξύ πορτοφολιών
- Επαλήθευση και επικύρωση των ισοζυγίων λογαριασμών των πορτοφολιών.
- Εξόρυξη ή ‘’Απόδειξη’’ της εργασίας

3.8 Ψηφιακές υπογραφές

Τα hashes χρησιμοποιούνται συχνά σε συνδυασμό με υπογραφές. Τα Blockchains χρησιμοποιούν υπογραφές για την υπογραφή συναλλαγών. Οι υπογραφές χρησιμοποιούνται για να αποδείξουν ότι για παράδειγμα, ένας συγκεκριμένος χρήστης είναι ο ιδιοκτήτης των εισροών που αντιστοιχούν σε ένα συγκεκριμένο hash. Οι είσοδοι υπογραφής δεν είναι αποδοτικές, επομένως οι υπογραφές χρησιμοποιούνται για την υπογραφή των τιμών hash. Σε γενικές γραμμές, η υπογραφή γίνεται κάπως έτσι[39]:

Ένας hash μιας συναλλαγής παράγεται από το χρήστη Α.

Με την χρήση του ιδιωτικού κλειδιού Α κρυπτογραφεί τον κατακερματισμό υπογράφοντας έτσι το έγγραφο.

Το υπογεγραμμένο hash αποστέλλεται στο χρήστη Β μαζί με το δημόσιο κλειδί του χρήστη Α.

Ο χρήστης Β παίρνει τις εισροές που χρησιμοποιήθηκαν πριν δημιουργηθεί το hash και επαναδημιουργεί το hash. Αυτός ο κατακερματισμός θα χρησιμοποιηθεί ως σύγκριση.

Χρησιμοποιώντας έναν κρυπτογραφικό αλγόριθμο ο χρήστης Β είναι σε θέση να αποκρυπτογραφήσει το υπογεγραμμένο hash από τον χρήστη Α με το παρεχόμενο δημόσιο κλειδί.

Ο χρήστης Β συγκρίνει τα hashes και επαληθεύει ότι ο χρήστης Α είναι ο ιδιοκτήτης των εισροών.

Σε αυτό το σύστημα, το δημόσιο κλειδί διανέμεται ελεύθερα και συνδυάζεται κρυφά με ένα ιδιωτικό κλειδί. Δεν είναι πρόβλημα εάν ένα δημόσιο κλειδί είναι γνωστό,

αλλά το ιδιωτικό κλειδί πρέπει πάντα να είναι μυστικό. Παρόλο που οι δύο είναι συνδυασμένες, ο υπολογισμός του ιδιωτικού κλειδιού κάποιου χρήστη με βάση το δημόσιο κλειδί είναι τόσο υπολογιστική και τόσο δύσκολη ώστε είναι οικονομικά και τεχνικά ανέφικτη. Αν ο χρήστης χάσει το ιδιωτικό του κλειδί, χάνει και τα χρήματα του. Η προστασία του κλειδιού είναι το κύριο μειονέκτημα αυτής της μεθόδου.

3.9 Αλγόριθμος εξόρυξης

Η εξόρυξη Bitcoin περιλαμβάνει επίσης κρυπτογραφικούς αλγόριθμους. Η πράξη εξόρυξης στο δίκτυο Bitcoin, ενθαρρύνει τους χρήστες ενός δικτύου (που ονομάζονται επίσης Miners) να επικυρώνουν αληθινά τις συναλλαγές Bitcoin και τους παροτρύνουν με το Bitcoin. Το Hashing χρησιμοποιείται για τη δημιουργία μαθηματικών πάζλ που πρέπει να λυθούν για να δημιουργηθεί ένα μπλοκ[39].

Πώς λειτουργεί λεπτομερώς;

Όλοι οι miners ανταγωνίζονται μεταξύ τους για να δημιουργήσουν ένα έγκυρο μπλοκ συναλλαγών. Αυτός ο διαγωνισμός οδηγείται από ένα κρυπτογραφικό πάζλ όπου όλοι ανταγωνίζονται για να βρουν πρώτα μια λύση σε ένα μαθηματικό πρόβλημα, τον ανταγωνισμό για να βρουν μια είσοδο που δίνει μια συγκεκριμένη τιμή κατακερματισμού. Με αυτόν τον τρόπο, εκτελούν υπολογιστική εργασία για να λύσουν το πάζλ, γι 'αυτό η διαδικασία αναφέρεται ως Απόδειξη Εργασίας (POW) με βάση την ιδέα του AdamBack και Hashcash[39] . Η επίλυση του μαθηματικού προβλήματος απαιτεί να συγκεντρώνει όλες τις πρόσφατες συναλλαγές, να επαληθεύει τις συναλλαγές και να εκτελεί όλα τα δεδομένα μέσω ενός αλγορίθμου SHA256. Ο miner πρέπει να βρει έναν αριθμό που ταιριάζει με έναν προκαθορισμένο από τον αλγόριθμο.

Για να γίνει αποδεκτό ένα μπλοκ από τους συμμετέχοντες στο δίκτυο, οι miners πρέπει να βρουν αυτή την ειδική τιμή κατακερματισμού, και με αυτόν τον τρόπο καλύπτουν όλα τα δεδομένα του μπλοκ. Ο πρώτος που βρίσκει τον αριθμό, κερδίζει τον ανταγωνισμό. Αυτό δημιουργεί ένα νέο μπλοκ συναλλαγών, το οποίο αντιπροσωπεύει μια δέσμη των πρόσφατων συναλλαγών που στάλθηκαν μέσω του δικτύου.

Όλες οι συναλλαγές που περιλαμβάνονται σε ένα μπλοκ είναι έγκυρες. Κάθε φορά που δημιουργείται ένα έγκυρο μπλοκ, οι συμμετέχοντες λαμβάνουν μια ανταμοιβή υπό μορφή νεοαποκτηθέντος BTC. Η κωδικοποίηση του αλγορίθμου Blockchain ρυθμίζεται για να επιβραβεύει το άτομο για την εξόρυξη και έτσι να συμβάλλει στην επαλήθευση των συναλλαγών Blockchain διατηρώντας παράλληλα το δίκτυο ασφαλές. Κάθε φορά που περισσότεροι εντάσσονται στο δίκτυο, οι αλγόριθμοι ρυθμίζουν τη δυσκολία του δικτύου[39].

Η δυσκολία αυτής της εργασίας προσαρμόζεται έτσι ώστε να περιορίζεται ο ρυθμός με τον οποίο μπορούν να δημιουργηθούν νέα μπλοκ από το δίκτυο σε μία κάθε 10 λεπτά. Αυτή η μέθοδος καθιστά απρόβλεπτο να γνωρίζουμε ποιος υπολογιστής στο δίκτυο θα είναι σε θέση να δημιουργήσει το επόμενο μπλοκ. Κάθε νέα μπλοκ που παράγεται περιέχει το hash του προηγούμενου μπλοκ, έτσι κάθε μπλοκ έχει μια αλυσίδα από μπλοκ που μαζί περιέχουν μια μεγάλη ποσότητα εργασίας. Έτσι δικαιολογείται ο όρος Blockchain.

Η αλλαγή των δεδομένων σε ένα μπλοκ συνεπώς απαιτεί από έναν εισβολέα να αναδημιουργήσει όλα τα διαδοχικά μπλοκ και να επαναλάβει την υπολογιστική εργασία που περιέχει. Αυτό είναι εφικτό, αλλά θα απαιτούσε μια μη εφικτή ποσότητα

υπολογιστικής ισχύος, η οποία προστατεύει το Blockchain από τις προσπάθειες χειραγώγησης.

Δεδομένου ότι η συνάρτηση κατακερματισμού που χρησιμοποιείται είναι κρυπτογραφικά ασφαλής, ο μόνος τρόπος για να βρεθεί μια λύση στο πρόβλημα αυτό είναι να δοκιμάσουμε όλους τους δυνατούς συνδυασμούς (βίαιη δύναμη). Ο επικυρωτής (ορυχείο) ο οποίος είναι ο ταχύτερος για να λύσει το μαθηματικό πάζλ, είναι ο νικητής και μπορεί να επιλέξει το επόμενο μπλοκ που θα προστεθεί στο Blockchain[39].

Μια κακόβουλη επίθεση στο δίκτυο είναι δυνατή, αλλά θα κοστίσει πολύ, λόγω του υψηλού κόστους του υλικού, της ενέργειας και των πιθανών κερδών εξόρυξης που χάθηκαν.

Επομένως, η απόδειξη της εργασίας παρέχει την απαιτούμενη ασφάλεια του δικτύου και έχει αποδειχθεί ότι καθιστά το δίκτυο Bitcoin και άλλα δίκτυα ανθεκτικά σε επίθεση (χωρίς χειρισμούς από εξωτερικούς επιτιθέμενους) μέχρι στιγμής.

Κεφάλαιο 4

4.1 Χρήσεις του Blockchain

Οι αλυσίδες μπλοκ μπορούν να επιτρέψουν σε πολλούς χρήστες να διεξάγουν συναλλαγές με διαφάνεια χωρίς την ανάγκη ενός αξιόπιστου διαμεσολαβητή [40].

Οι πιο συναρπαστικές περιπτώσεις χρήσης βρίσκονται σε περιοχές της υπάρχουσας βιομηχανίας, όπου οι αξιόπιστοι διαμεσολαβητές υποχρεούνται να καταγράφουν, να επικυρώνουν και να συμβιβάζουν τις συναλλαγές χωρίς πραγματικά να προσθέτουν πρόσθετη αξία στην αρχική συναλλαγή.

4.2 Αποκωδικοποίηση περιουσιακών στοιχείων

Μία από τις πιο συναρπαστικές περιπτώσεις χρήσης είναι η εφαρμογή στις χρηματοπιστωτικές υπηρεσίες και ειδικότερα η τιτλοποίηση περιουσιακών στοιχείων σε χρηματοοικονομικά και ακίνητα περιουσιακά στοιχεία. Με τη χρήση τεχνολογίας blockchain, τα μη ρευστοποιήσιμα στοιχεία μπορούν τώρα να μετατραπούν σε διακεκομμένη μορφή και να αποσπαστούν με αποτελεσματικό τρόπο, έπειτα να διαπραγματευτούν και τέλος να εγκατασταθούν στην αλυσίδα. Αυτό μπορεί να ξεκλειδώσει τη ρευστότητα για τους ιδιοκτήτες. Επιπλέον αυτό σημαίνει ότι η πρόσβαση σε επενδύσεις που προηγουμένως ήταν προσβάσιμες μόνο από θεσμικούς επενδυτές μπορεί να είναι προσπελάσιμη και σε ιδιώτες επενδυτές. Το AlphaPoint εκτιμά ότι η συνολική αξία των μη ρευστοποιήσιμων περιουσιακών στοιχείων, συμπεριλαμβανομένου του χρυσού, των ακινήτων και άλλων, είναι 11 τρισεκατομμύρια δολάρια[40].

Το Alphapoint , το Polymath , το SmartVarlor και το Harbour εργάζονται σε πλατφόρμες για τον διαχωρισμό των περιουσιακών στοιχείων.

4.3 Διαχείριση αλυσίδας εφοδιασμού

Η δεύτερη πιο συναρπαστική περίπτωση χρήσης για Blockchain είναι στον τομέα της διαχείρισης της αλυσίδας εφοδιασμού. Ένα από τα μεγαλύτερα προβλήματα που αντιμετωπίζουν οι εταιρείες όταν διαχειρίζονται την αλυσίδα εφοδιασμού τους είναι το ζήτημα της διαφάνειας. Οι αλυσίδες του μπλοκ επιτρέπουν σε πολλά μέρη να έχουν πρόσβαση σε μια βάση δεδομένων για να λειτουργούν ως η μόνη πηγή αλήθειας. Οι καταγεγραμμένες συναλλαγές είναι αμετάβλητες, επισυναπτόμενες και παρέχουν μια διαδρομή ελέγχου στο χρόνο[40]. Οι αλυσίδες μπλοκ επιτρέπουν την τεκμηρίωση ενός προϊόντος σε πραγματικό χρόνο καθώς μετακινείται από την αρχική του προέλευση και όλα τα σημεία επαφής του. Η τεχνολογία Blockchain συμβάλλει στην ενίσχυση της διαφάνειας σε ένα αδιαφανές δίκτυο, βοηθά στην παύση των κλοπών, μειώνει τη γραφειοκρατία και το κόστος.

Από την άποψη του καταναλωτή, οι αλυσίδες μπλοκ μπορούν να εξουσιοδοτήσουν τους τελικούς καταναλωτές να ανακαλύψουν με ακρίβεια εάν τα προϊόντα είναι αυτό που ισχυρίζονται ότι είναι.

Παραδείγματα σχεδίων που εργάζονται σε αυτό περιλαμβάνουν το Vechain και το OriginTrail[40] .

4.4 Ενεργειακή αγορά

Μια άλλη περίπτωση χρήσης για την τεχνολογία Blockchain είναι ο ρόλος που μπορεί να διαδραματίσει για την αποκέντρωση της αγοράς ενέργειας, η οποία ελέγχεται συνήθως από μερικές μεγάλες εταιρείες σε κάθε αγορά. Η τεχνολογία Blockchain επιτρέπει την καταγραφή, διαπραγμάτευση και διακανονισμό της ευφυούς μέτρησης της ηλεκτρικής ενέργειας που παράγεται από τους ηλιακούς συλλέκτες ενός κατόχου. Εάν η ηλεκτρική ενέργεια μπορεί να αποτελέσει αντικείμενο συναλλαγής όπως οποιοδήποτε άλλο εμπόρευμα, οι τιμές της ενέργειας αντί να είναι μια σταθερή ρυθμιζόμενη τιμή, θα ανταποκρίνονται στις δυνάμεις ζήτησης και προσφοράς σε μια πλήρως λειτουργική αγορά ηλεκτρικής ενέργειας. Αυτό επιτρέπει στα άτομα να είναι τόσο παραγωγοί όσο και καταναλωτές ενέργειας, γεγονός που μπορεί να μειώσει το κόστος και να βελτιώσει την αποτελεσματικότητα, χωρίς να χρειάζεται να βασίζεται σε κεντρικό δίκτυο[40]

Παραδείγματα συναλλαγών ενέργειας περιλαμβάνουν το LedgerPower και το Grid + .

4.5 Φροντίδα υγείας

Στην τρέχουσα κατάσταση της υγειονομικής περίθαλψης, τα δεδομένα των ασθενών κρατούνται σε διαφορετικά ιδρύματα και σε διάφορες μορφές και πρότυπα, καθιστώντας την ανταλλαγή δεδομένων ακατάλληλη στην επιθυμία του σύγχρονου χρήστη για στιγμιαία πρόσβαση.

Η χρήση τεχνολογίας Blockchain για την καταγραφή πληροφοριών ασθενούς σε κατανεμημένο ημερολόγιο μπορεί να επιτρέψει σε διάφορους ενδιαφερόμενους να έχουν πρόσβαση υπό όρους σε μία μόνο πηγή αλήθειας, όπου κάθε αλληλεπίδραση με τα δεδομένα υγείας ενός ασθενούς μπορεί να καταγραφεί σε ένα ημερολόγιο ως μια συναλλαγή με ένα χρονικά διαβαθμισμένο ίχνος ελέγχου. Αυτό καθιστά

ασφαλέστερη την πρόσβαση στις πληροφορίες για την υγεία του ασθενούς (κρυπτογραφημένα δεδομένα ασθενών), μπορούν να εξαλείψουν τις ανεπάρκειες με τις τρέχουσες πρακτικές διαχείρισης δεδομένων και να προσφέρουν στους ασθενείς περισσότερο έλεγχο των δεδομένων τους (συμπεριλαμβανομένης της δημιουργίας εσόδων από δικά τους προσωπικά δεδομένα υγείας για ερευνητικούς σκοπούς)[40].

Παραδείγματα πλατφόρμων ανταλλαγής δεδομένων για την υγειονομική περίθαλψη περιλαμβάνουν το Medicalchain .

Κεφάλαιο5

5.1 Λειτουργία Hyperledger

Σε γενικές γραμμές, το Blockchain είναι ένας αμετάβλητος τίτλος συναλλαγών, που διατηρείται μέσα σε ένα κατανεμημένο δίκτυο το οποίο απαρτίζεται από κατανεμημένους κόμβων. Αυτοί οι κόμβοι διατηρούν ένα αντίγραφο του ημερολογίου εφαρμόζοντας συναλλαγές που έχουν επικυρωθεί από ένα πρωτόκολλο συναίνεσης , ομαδοποιημένο σε μπλοκ που περιλαμβάνουν ένα hash που δεσμεύει κάθε μπλοκ με το προηγούμενο μπλοκ[41].

Στην ουσία ο κατακερματισμός σημαίνει τη λήψη μιας αλυσίδας εισόδου οποιουδήποτε μήκους και την παράδοση μιας εξόδου σταθερού μήκους . Στο πλαίσιο των κρυπτοσυχνοτήτων όπως το Bitcoin, οι συναλλαγές λαμβάνονται ως είσοδος και τρέχουν μέσω ενός αλγόριθμου κατακερματισμού (Το Bitcoin χρησιμοποιεί SHA-256) που δίνει μια παραγωγή σταθερού μήκους.

INPUT	HASH
Hi	639EFCD08ABB273B1619E82E78C29A7DF02C1051B1820E99FC395DCAA3326B8
Welcome	53A53FC9E2A03F9B6E66D84BA701574CD9CF5F01FB498C41731881BCDC68A7C8

Εικόνα 3. **https://blockgeeks.com/guides/hashingexample**

Όπως φαίνεται από την εικόνα 3, στην περίπτωση του SHA-256 , ανεξάρτητα από το πόσο μεγάλη ή μικρή είναι η είσοδος , η έξοδος θα έχει πάντα σταθερό μήκος 256 bits. Αυτό γίνεται κρίσιμο όταν πρόκειται για ένα τεράστιο όγκο δεδομένων και συναλλαγών. Έτσι, βασικά, αντί να θυμάται τα δεδομένα εισόδου που θα μπορούσαν να είναι τεράστια, μπορεί απλά να θυμηθεί το hash για να τα παρακολουθεί .

Κρυπτογραφικές λειτουργίες κατακερματισμού

Μια κρυπτογραφική συνάρτηση κατακερματισμού είναι μια ειδική κλάση λειτουργιών κατακερματισμού η οποία έχει διάφορες ιδιότητες καθιστώντας την ιδανική για κρυπτογραφία. Υπάρχουν ορισμένες ιδιότητες που χρειάζεται μια κρυπτογραφική λειτουργία κατακερματισμού προκειμένου να θεωρηθεί ασφαλής. Ακόμα κι αν γίνει μια μικρή αλλαγή στις εισροές , οι αλλαγές που θα αντικατοπτρίζονται στο hash θα είναι τεράστιες.

Καθώς η δημοτικότητα του Bitcoin, του Ethereum και μερικές άλλες παράγωγες τεχνολογιών αυξήθηκαν, το ενδιαφέρον για την εφαρμογή της βασικής τεχνολογίας του Blockchain, του κατανεμημένου βιβλίου και της κατανεμημένης πλατφόρμας εφαρμογής σε πιο καινοτόμες περιπτώσεις χρήσης των επιχειρήσεων αυξήθηκε επίσης. Ωστόσο, πολλές περιπτώσεις χρήσης σε επιχειρήσεις απαιτούν χαρακτηριστικά απόδοσης που οι τεχνολογίες Blockchain χωρίς άδεια δεν μπορούν (προς το παρόν) να παραδώσουν. Επιπλέον σε πολλές περιπτώσεις χρήσης, η ταυτότητα των συμμετεχόντων είναι μια δύσκολη απαίτηση, όπως στην περίπτωση των χρηματοπιστωτικών συναλλαγών στις οποίες πρέπει να ακολουθούνται οι κανονισμοί του Know-Your-Customer (KYC) και της καταπολέμησης της νομιμοποίησης εσόδων από παράνομες δραστηριότητες (AML)[41].

Το Hyperledger Fabric έχει σχεδιαστεί επιχειρηματική χρήση. Οι ακόλουθες ενότητες περιγράφουν τον τρόπο με τον οποίο το Hyperledger Fabric (Fabric) διαφοροποιείται από άλλες πλατφόρμες και περιγράφει μερικά από τα κίνητρα για τις αρχιτεκτονικές του αποφάσεις.

Αρχιτεκτονική Hyperledger

Το HyperledgerFabric είναι μια πλατφόρμα τεχνολογίας κατανεμημένου λογιστικού καταλόγου (DLT), ανοικτού κώδικα, δηλαδή μια βάση δεδομένων που η οποία δεν είναι αποθηκευμένη σε μια κεντρική τοποθεσία αλλά κατανεμημένη σε ένα δίκτυο πολλών υπολογιστών. Η πλατφόρμα αυτή έχει σχεδιαστεί για να χρησιμοποιείται σε επιχειρηματικά περιβάλλοντα και προσφέρει ορισμένες βασικές δυνατότητες, οι οποίες την διαφοροποιούν από άλλες δημοφιλείς κατανεμημένες πλατφόρμες [41].

Πιο συγκεκριμένα, ένα βασικό σημείο που τη διαφοροποιεί είναι πως το Hyperledger ιδρύθηκε στο πλαίσιο του LinuxFoundation, το οποίο έχει μια μακρά και πολύ επιτυχημένη ιστορία στη δημιουργία πρότζεκτ ανοιχτού κώδικα υπό ανοιχτή διακυβέρνηση που αναπτύσσουν ισχυρές κοινότητες στήριξης και ακμάζοντα οικοσυστήματα.

Το Hyperledger διοικείται από μια πολυσύνθετη τεχνική επιτροπή διαχείρισης και το πρότζεκτ Hyperledger Fabric το διαχειρίζεται ένα εξίσου σύνθετο σύνολο διαχειριστών αποτελούμενο από πολλούς οργανισμούς. Έχει μια αναπτυξιακή κοινότητα, η οποία από την πρώτη της δέσμευση [41] έχει εξαπλωθεί σε πάνω από 35 οργανισμούς και σε περίπου 200 προγραμματιστές .

Όλα τα πρότζεκτ του Hyperledger ακολουθούν μια φιλοσοφία σχεδιασμού που περιλαμβάνει μια σπονδυλωτή επεκτάσιμη διαλειτουργικότητα με έμφαση σε άκρως ασφαλείς λύσεις. Ένα token-αγνωστικιστής προσέγγισης χωρίς εγγενή κρυπτονόμισμα και την ανάπτυξη μιας πλούσιας και εύχρηστης Διασύνδεσης εφαρμογών προγραμματισμού (API). Η αρχιτεκτονική Hyperledger Working Group(WG) έχει ξεχωρίσει καθώς εφαρμόζει τα ακόλουθα επιχειρηματικά blockchain στοιχεία:[42]

- **Consensus Layer** - υπεύθυνο για τη σύναψη συμφωνίας καθορίζοντας και επιβεβαιώνοντας την ορθότητα του συνόλου των συναλλαγών που αποτελούν ένα μπλοκ.
- **Smart Contract Layer**-είναι υπεύθυνο για την επεξεργασία των αιτήσεων προκειμένου να εκτελεστούν οι συναλλαγές, επίσης προσδιορίζει εάν οι συναλλαγές αυτές είναι έγκυρες εκτελώντας επιχειρηματική λογική.
- **Communication Layer**-είναι υπεύθυνο για τη μεταφορά μηνυμάτων μεταξύ των κατανεμημένων χρηστών στους κόμβους που συμμετέχουν σε ένα κοινόχρηστο μητρώο ledger.
- **Data Store Abstraction**-επιτρέπει διαφορετικές βάσεις δεδομένων να χρησιμοποιηθούν από άλλα δομοστοιχεία(modules).
- **Crypto Abstraction**-επιτρέπει διαφορετικούς αλγόριθμους κρυπτογράφησης να ανταλλαχθούν χωρίς να επηρεαστούν άλλα δομοστοιχεία.

- **Identity Services**-επιτρέπει την δημιουργία εμπιστοσύνης(Root of Trust) κατά τη διάρκεια της εγκατάστασης μιας περίπτωσης blockchain. Επίσης επιτρέπει την εγγραφή και την καταχώριση των ταυτοτήτων ή οργανισμών του συστήματος κατά τη διάρκεια λειτουργίας του δικτύου. Επίσης, παρέχει επαλήθευση και εξουσιοδότηση στους χρήστες.
- **Policy Services**-είναι υπεύθυνο για τη διαχείριση των διαφόρων πολιτικών που καθορίζονται στο σύστημα, όπως η πολιτική υποστήριξης. έγκρισης και συναίνεσης. Διασυνδέεται και εξαρτάται από άλλα modules για να εφαρμόσει τις ποικίλες πολιτικές του.
- **APIs**-επιτρέπει στους πελάτες και στις εφαρμογές να διασυνδεθούν με τα blockchains.
- **Interoperation**-υποστηρίζει τη διαλειτουργικότητα μεταξύ διαφορετικών περιπτώσεων blockchain.[42]

Συναίνεση (consensus)

Η συναίνεση είναι η διαδικασία με την οποία ένα δίκτυο κόμβων παρέχει μια εγγυημένη παραγγελία συναλλαγών και επικυρώνει το μπλοκ των συναλλαγών.
Η συναίνεση πρέπει να παρέχει τις ακόλουθες λειτουργίες.[42]

- Επιβεβαιώνει την ορθότητα όλων των συναλλαγών σε ένα προτεινόμενο μπλοκ, σύμφωνα με τις πολιτικές επικύρωσης και συναίνεσης.

- Συμφωνεί σχετικά με την σειρά και την ορθότητα, άρα συνεπώς και με τα αποτελέσματα της εκτέλεσης(αυτό συνεπάγεται συμφωνία σε παγκόσμιο επίπεδο).

- Διασύνδεει και εξαρτάται από το Smart Contract Layer για να επαληθεύσει την ορθότητα ενός ταξινομημένου συνόλου συναλλαγών σε ένα μπλοκ.[42]

Ιδιότητες της συναίνεσης

Η συναίνεση πρέπει να ικανοποιεί δύο ιδιότητες για να εγγυηθεί τη συμφωνία μεταξύ των κόμβων: **ασφάλεια** και **ζωτικότητα**.

- **Ασφάλεια** σημαίνει ότι κάθε κόμβος εγγυάται την ίδια σειρά εισόδων και αποτελεσμάτων στην ίδια έξοδο για κάθε κόμβο. Όταν οι κόμβοι λάβουν μια ίδια σειρά από συναλλαγές, οι ίδιες αλλαγές θα προκύψουν σε κάθε κόμβο. Ο αλγόριθμος πρέπει να συμπεριφέρεται πανομοιότυπα σε ένα σύστημα κόμβων που εκτελεί κάθε συναλλαγή ατομικά κάθε φορά.

- **Ζωτικότητα** σημαίνει ότι κάθε μη ελαττωματικός κόμβος θα λάβει τελικά κάθε συναλλαγή που έχει υποβληθεί, υποθέτοντας ότι η επικοινωνία δεν είναι επιτυχής.[42]

Η συναίνεση στο Hyperledger Fabric

Η συναίνεση στο Hyperledger Fabric χωρίζεται σε 3 φάσεις: στην **έγκριση**, την **ταξινόμηση** και την **επικύρωση**.[42]

- Η **έγκριση** είναι η πολιτική κατά την οποία οι συμμετέχοντες εγκρίνουν τη συναλλαγή.

- Η φάση της **ταξινόμησης** αποδέχεται τις εγκριθείσες συναλλαγές και συμφωνεί με την εντολή να αποθηκευτούν στο μητρώο.
- Η **επικύρωση** παίρνει ένα μπλοκ από ταξινομημένες συναλλαγές και επικυρώνει την ορθότητα των αποτελεσμάτων, επιπλέον ελέγχει και την πολιτική έγκρισης στην οποία οι συμμετέχοντες υποστηρίζουν μια συναλλαγή αλλά και της διπλής δαπάνης(double-spending).[42]

  Ο όρος διπλή δαπάνη χρησιμοποιείται όταν ένας κακόβουλος χρήστης επιχειρήσει να ξοδέψει τα bitcoin του για παράδειγμα σε δύο διαφορετικούς παραλήπτες την ίδια στιγμή, αυτό ονομάζεται double-spending.[44] Για να αποφευχθεί αυτό το πρόβλημα έχει δημιουργηθεί μια συναίνεση στο δίκτυο σχετικά με το ποια από τις συναλλαγές θα επιβεβαιωθεί και θα θεωρηθεί έγκαιρη.

Το Hyperledger Fabric υποστηρίζει pluggable εξυπηρέτηση συναίνεσης και για τα τρία στάδια. Οι εφαρμογές μπορούν να προσθέτουν διαφορετικές εγκρίσεις παραγγελίας και μοντέλα επικύρωσης ανάλογα με τις απαιτήσεις τους. Η υπηρεσία παραγγελιών, δηλαδή το λογισμικό Διασύνδεσης Εφαρμογών Προγραμματισμού (API) που επιτρέπει την επικοινωνία μεταξύ των εφαρμογών αποτελείται από δύο βασικές λειτουργίες: **Μετάδοση** και **παράδοση**.[42]

- **Μετάδοση**: ένας πελάτης καλεί το συγκεκριμένο API το οποίο χρησιμοποιείται για την αποστολή συναλλαγών στην υπηρεσία παραγγελιών προς επεξεργασία.

- **Παράδοση**: η υπηρεσία παραγγελιών καλεί το API για να ζητήσει από τον διαχειριστή πληροφορίες, όπως διαμορφώσεις καναλιών.[42]

Hypeledger Fabric

Το Fabric είναι η πρώτη κατανεμημένη πλατφόρμα για την υποστήριξη έξυπνων συμβολαίων που συντάσσονται σε γλώσσες προγραμματισμού γενικού σκοπού, όπως είναι η Java, η Go και η Node.js. Αυτό σημαίνει ότι οι περισσότερες επιχειρήσεις διαθέτουν ήδη το απαιτούμενο σύνολο δεξιοτήτων για την ανάπτυξη έξυπνων συμβάσεων, χωρίς να απαιτείται πρόσθετη κατάρτιση για να μάθουν μια νέα γλώσσα.[41].

Επίσης, η πλατφόρμα Fabric είναι εξουσιοδοτημένη, γεγονός που σημαίνει ότι, αντίθετα με ένα δημόσιο δίκτυο, οι συμμετέχοντες είναι γνωστοί μεταξύ τους και όχι ανώνυμοι, και συνεπώς πλήρως αξιόπιστοι. Με άλλα λόγια, ακόμη κι αν οι συμμετέχοντες δεν έχουν εμπιστοσύνη ο ένας στον άλλον, το δίκτυο μπορεί να λειτουργήσει κάτω από ένα μοντέλο διακυβέρνησης το οποίο είναι χτισμένο μακριά από το τι είδους εμπιστοσύνης υπάρχει μεταξύ των συμμετεχόντων, όπως συμβαίνει σε μια νομική συμφωνία ή σε ένα πλαίσιο για τη διεκπεραίωση διαφορών [41].

Ένα άλλο στοιχείο που διαφοροποιεί την πλατφόρμα από άλλες είναι πως υποστηρίζει πρωτόκολλα συναίνεσης, τα οποία της επιτρέπουν να προσαρμόζεται πιο αποτελεσματικά, προκειμένου να ταιριάζει σε συγκεκριμένες περιπτώσεις χρήσης.

Για παράδειγμα, όταν αναπτύσσεται μέσα σε μία επιχείρηση ή λειτουργεί μέσα από μια αξιόπιστη αρχή, η συνολική συναίνεση για αντοχή σε βλάβες μπορεί να θεωρηθεί περιττή και να οδηγήσει σε υπερβολική συσσώρευση της απόδοσης [41].

Σε τέτοιες καταστάσεις, ένα πρωτόκολλο συναίνεσης για την ανοχή σε σφάλματα όπως το Crash fault tolerance (CFT) διαθέτοντας ένα επίπεδο ανθεκτικότητας, όπου το σύστημα μπορεί ακόμα να φτάσει σωστά στη συναίνεση σε περίπτωση αποτυχίας, μπορεί να είναι κάτι περισσότερο από επαρκές. Ενώ σε άλλες περιπτώσεις μπορεί να απαιτηθεί ένα πρωτόκολλο συναίνεσης όπως το Byzantine Fault Tolerance(BFT) το οποίο είναι πιο περίπλοκο και ασχολείται με συστήματα που μπορεί να είναι κακόβουλα[41].

Το Fabric μπορεί να αξιοποιήσει τα πρωτόκολλα συναίνεσης που δεν απαιτούν κρυπτογράφηση για να εισέλθουν σε δαπανηρή εξόρυξη ή για να τροφοδοτήσουν την εκτέλεση έξυπνων συμβολαίων. Η αποφυγή κρυπτογράφησης μειώνει ορισμένους σημαντικούς παράγοντες κινδύνου και ρίσκου, μιας και η απουσία κρυπτογραφικών δραστηριοτήτων εξόρυξης σημαίνει ότι η πλατφόρμα μπορεί να αναπτυχθεί με το ίδιο περίπου λειτουργικό κόστος, όπως και οποιοδήποτε άλλο κατανεμημένο σύστημα [41].

Ο συνδυασμός αυτών των διαφορετικών χαρακτηριστικών καθιστά την Fabric μία από τις πλέον αποδοτικές πλατφόρμες που διατίθενται σήμερα τόσο από πλευράς επεξεργασίας συναλλαγών όσο και από πλευράς επιβεβαίωσης συναλλαγών. Επιπλέον επιτρέπει την ιδιωτικότητα, την εμπιστευτικότητα των συναλλαγών και των έξυπνων συμβολαίων.

5.2 Modularity

Το Hyperledger Fabric έχει σχεδιαστεί ειδικά για να διαθέτει αρθρωτή αρχιτεκτονική. Είτε πρόκειται για πρωτόκολλα συναίνεσης, πρωτόκολλα διαχείρισης ταυτότητας, ή πρωτόκολλα διαχείρισης κλειδιών..

Σε ένα υψηλό επίπεδο, το Fabric αποτελείται από τα ακόλουθα στοιχεία[41]:

- Μια υπηρεσία παραγγελιών δημιουργεί συναίνεση για τη σειρά συναλλαγών και στη συνέχεια μεταδίδει μπλοκ στους χρήστες.
- Ένας πάροχος υπηρεσιών προσβασιμότητας είναι υπεύθυνος για τη συσχέτιση φορέων στο δίκτυο με κρυπτογραφικές ταυτότητες.
- Μια προαιρετική υπηρεσία μεταξύ χρηστών διαδίδει την έξοδο των μπλοκ, μέσω της υπηρεσίας ταξινόμησης σε άλλους χρήστες.
- Τα έξυπνα συμβόλαια ("chaincode") εκτελούνται μέσα σε ένα περιβάλλον περιεκτή (π.χ. Docker). Μπορούν να γραφτούν σε τυπικές γλώσσες προγραμματισμού, αλλά δεν έχουν άμεση πρόσβαση στην κατάσταση μητρώου.
- Το μητρώο μπορεί να διαμορφωθεί έτσι ώστε να υποστηρίζει μια ποικιλία εφαρμογών λογισμικού που επιτρέπει στον χρήστη να αλληλεπιδράσει με μια βάση δεδομένων.
- Μια πολιτική έγκρισης και επικύρωσης που μπορεί να ρυθμιστεί ανεξάρτητα ανά εφαρμογή.

Υπάρχει δίκαιη συμφωνία στον κλάδο ότι δεν υπάρχει "ένα Blockchain για να τους κυβερνήσεις όλους". Το Hyperledger Fabric μπορεί να διαμορφωθεί με πολλούς τρόπους για να ικανοποιήσει τις ποικίλες προαπαιτούμενες ανάγκες σε πολλές περιπτώσεις βιομηχανικής χρήσης.

5.3 Δεσμευμένα και μη μπλόκ

Σε ένα μη δεσμευμένο Blockchain, σχεδόν οποιοσδήποτε μπορεί να συμμετάσχει και κάθε συμμετέχων είναι ανώνυμος. Σε ένα τέτοιο πλαίσιο, δεν μπορεί να υπάρξει καμία εμπιστοσύνη πέρα από το γεγονός ότι η κατάσταση του Blockchain, προτού φτάσει σε ένα ορισμένο βάθος είναι αμετάβλητη[41]. Προκειμένου να μετριαστεί αυτή η απουσία εμπιστοσύνης, τα αδέσμευτα μπλοκ συνήθως εφαρμόζουν τέλη συναλλαγών προκειμένου να αντισταθμίσουν το υπερβολικό κόστος συμμετοχής και ένα πρωτόκολλο συναίνεσης βασισμένο στην "απόδειξη εργασίας" [41].

Οι δεσμευμένες αλυσίδες μπλοκ από την άλλη πλευρά, δραστηριοποιούνται σε ένα Blockchain που απαρτίζεται από ένα σύνολο γνωστών, αναγνωρισμένων και συχνά ελεγμένων συμμετεχόντων που λειτουργούν με ένα μοντέλο διακυβέρνησης το οποίο αποδίδει ένα ορισμένο βαθμό εμπιστοσύνης. Ένα δεσμευμένο Blockchain μπορεί να εξασφαλίσει τις αλληλεπιδράσεις μεταξύ μιας ομάδας οντοτήτων που έχουν κοινό στόχο, αλλά που μπορεί να μην εμπιστεύονται πλήρως. Βασιζόμενοι στις ταυτότητες των συμμετεχόντων, ένα δεσμευμένο Blockchain μπορεί να χρησιμοποιήσει πρωτόκολλα συναίνεσης για την ανοχή σε σφάλματα όπως το Crash fault tolerance

(CFT) ή το Byzantine Fault Tolerance(BFT) που δεν απαιτούν δαπανηρή εξόρυξη[41].

Επιπλέον, σε ένα τέτοιο πλαίσιο, ο κίνδυνος ενός συμμετέχοντος που εισάγει σκόπιμα κακόβουλο κώδικα μέσω ενός έξυπνου συμβολαίου μειώνεται. Αυτό συμβαίνει καθώς οι συμμετέχοντες είναι γνωστοί αναμεταξύ τους.

Έτσι όποια ενέργεια εκτελείται, είτε πρόκειται για μια υποβολή αίτησης συναλλαγών ή για τροποποίηση του δικτύου είτε ακόμα και για την αξιοποίηση ενός έξυπνου συμβολαίου, καταγράφονται ακολουθώντας μια πολιτική επικύρωσης που θεσπίστηκε στο δίκτυο και τον σχετικό τύπο συναλλαγής στο Blockchain.

Επομένως αντί ο κακόβουλος χρήστης να είναι εντελώς ανώνυμος, μπορεί να εντοπιστεί εύκολα και το περιστατικό να αντιμετωπιστεί σύμφωνα με τους όρους του μοντέλου διακυβέρνησης[41].

5.4 Έξυπνα συμβόλαια

Ένα έξυπνο συμβόλαιο ή αυτό που το Fabric Hyperledger ονομάζει "chaincode", λειτουργεί ως μια αξιόπιστη κατανεμημένη εφαρμογή όπου η ασφάλεια και η εμπιστοσύνη του εξασφαλίζεται από το blockchain αλλά και από την συναίνεση μεταξύ των μελών. [41]

Πρόκειται για την επιχειρηματική λογική μιας εφαρμογής blockchain.

Υπάρχουν τρία βασικά σημεία, τα οποία ισχύουν για τα έξυπνα συμβόλαια, ειδικά όταν εφαρμόζονται σε μια πλατφόρμα:

- πολλά έξυπνα συμβόλαια τρέχουν ταυτόχρονα στο δίκτυο
- μπορούν να αναπτυχθούν δυναμικά και σε πολλές περιπτώσεις από οποιονδήποτε
- ο κώδικας της εφαρμογής θα πρέπει να αντιμετωπίζεται ως μη αξιόπιστος, ακόμη κι ως κακόβουλος [41]

Οι περισσότερες από τις υπάρχουσες πλατφόρμες blockchain, οι οποίες εκτελούν "έξυπνα συμβόλαια" (smart contracts), ακολουθούν μια αρχιτεκτονική εκτέλεσης παραγγελιών στην οποία το πρωτόκολλο συναίνεσης:

- επικυρώνει τις συναλλαγές,
- κατόπιν τις μεταδίδει σε όλους τους εγκεκριμένους χρήστες,
- στη συνέχεια κάθε χρήστης εκτελεί τις διαδοχικά τις συναλλαγές.[41]

Τα έξυπνα συμβόλαια

Η αρχιτεκτονική εκτέλεσης εντολών order- execute architecture[45] βρίσκεται σχεδόν σε όλα τα υπάρχοντα συστήματα blockchain, χρησιμοποιώντας πλατφόρμες όπως είναι η Ethereum[43] η οποία είναι υπεύθυνη για την δημιουργία έξυπνων συμβολαίων. Τα έξυπνα συμβόλαια γράφονται με τη χρήση της γλώσσας προγραμματισμού Solidity. Κάθε συναλλαγή που γίνεται μέσω των έξυπνων συμβολαίων καταγράφεται και ενημερώνεται από το δίκτυο. Έτσι όλοι όσοι

εμπλέκονται με το συμβόλαιο είναι υπεύθυνοι για τις πράξεις τους και κάθε τους ενέργεια είναι ορατή σε ολόκληρο το δίκτυο.

Τα έξυπνα συμβόλαια που εκτελούνται σε ένα blockchain πρέπει να είναι καθοριστικά διαφορετικά δεν είναι εφικτό να πραγματοποιηθεί ποτέ συναίνεση.

Αυτό δυσκολεύει τους προγραμματιστές που γράφουν τα "έξυπνα συμβόλαια", να χρησιμοποιούν μια νέα γλώσσα, γεγονός που μπορεί να τους οδηγήσει σε προγραμματιστικά σφάλματα.

Το γεγονός ότι ο κώδικας για τα "έξυπνα συμβόλαια" εκτελείται σε κάθε κόμβο του συστήματος είναι κάτι που απαιτεί να ληφθούν πολύπλοκα μέτρα. Στόχος είναι η προστασία του συνολικού συστήματος από δυνητικά κακόβουλες συμβάσεις, προκειμένου να διασφαλιστεί η ανθεκτικότητα του συνολικού συστήματος.[41]

5.5 Transaction Flow(Ροή Συναλλαγών)

Στο παρόν κεφάλαιο θα περιγράψουμε τους μηχανισμούς συναλλαγών που λαμβάνουν χώρα κατά τη διάρκεια μιας τυπικής ανταλλαγής αγαθών. Στην συγκεκριμένη περίπτωση περιλαμβάνονται δύο πελάτες, Α και Β, που αγοράζουν και πωλούν ραπανάκια. Ο κάθε πελάτης διαθέτει από έναν κατανεμημένο χρήστη στο δίκτυο όπου στέλνει τις συναλλαγές του και αλληλεπιδρά με το μητρώο

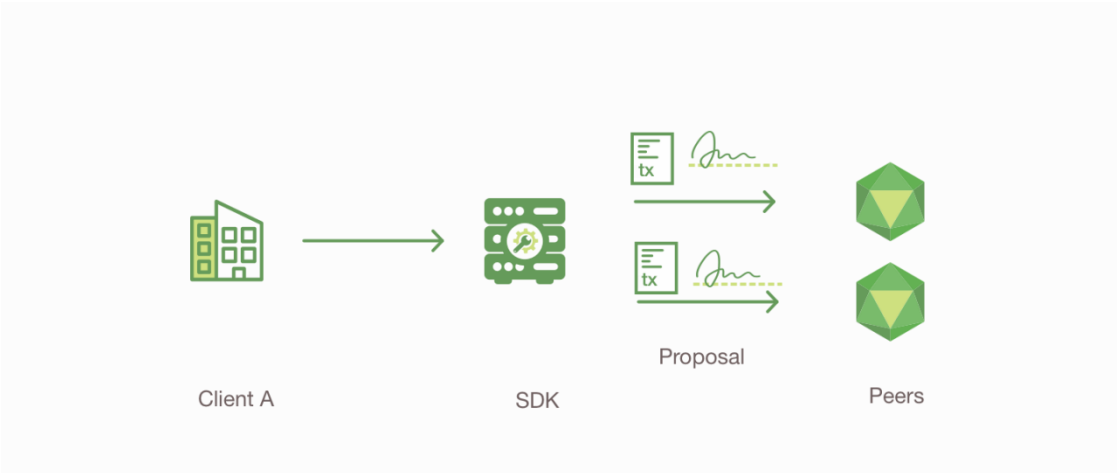
ledger.[41]

Υποθέσεις

Ας ξεκινήσουμε με την υπόθεση ότι ένα κανάλι έχει ρυθμιστεί και εκτελείται. Ο χρήστης της εφαρμογής έχει εγγραφεί στον οργανισμό έκδοσης ψηφιακών πιστοποιητικών(CA) και έλαβε πίσω το απαραίτητο κρυπτογραφικό κλειδί το οποίο χρησιμοποιείται για να πιστοποιηθεί η αυθεντικότητα του στο δίκτυο.

Ο αλγόριθμος chaincode που είναι γνωστός και ως έξυπνο συμβόλαιο συμπεριλαμβάνει ένα σύνολο από ζεύγη κλειδιών-τιμών, είναι εγκατεστημένος στους κατανεμημένους χρήστες του δικτύου και ενσωματωμένος στο κανάλι. Το κανάλι επιτρέπει στους συμμετέχοντες να δημιουργήσουν ξεχωριστό μητρώο συναλλαγών. Οι συναλλαγές είναι ορατές μόνο από τα μέλη του καναλιού.

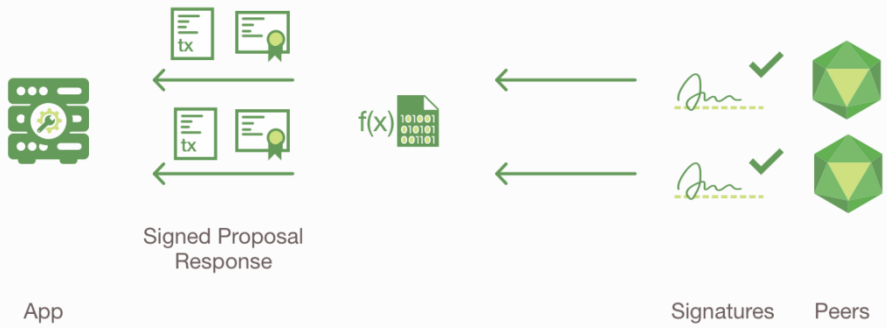
Ο αλγόριθμος καθορίζει ένα σύνολο οδηγιών για τις συναλλαγές και την τιμή που έχει συμφωνηθεί για ένα ραπανάκι. Μια πολιτική επικύρωσης έχει καθοριστεί επίσης για τον αλγόριθμο προκειμένου να συμφωνηθεί μια τιμή πώλησης για το προϊόν , δηλώνοντας στους κατανεμημένους χρήστες ότι πρέπει να εγκρίνουν κάθε συναλλαγή.[41]



1. **Ο πελάτης Α ξεκινάει μια συναλλαγή**

Εδώ βλέπουμε τι συμβαίνει όταν ξεκινάει μια συναλλαγή. Στο παράδειγμα μας ο Πελάτης Α στέλνει ένα αίτημα για να αγοράσει ραπανάκια. Το αίτημα έχει ως προορισμό τους κατανεμημένους χρήστες που εκπροσωπούν τον Πελάτη Α και τον Πελάτη Β. Η πολιτική έγκρισης δηλώνει ότι και οι δύο χρήστες πρέπει να εγκρίνουν οποιαδήποτε συναλλαγή και επομένως η αίτηση πηγαίνει ξεχωριστά στον κάθε χρήστη.

Στη συνέχεια, φτιάχνεται η πρόταση συναλλαγής. Έπειτα αξιοποιείται ένα εργαλείο ανάπτυξης λογισμικού(SDK) και χρησιμοποιεί μια από τα διαθέσιμες διεπαφές προγραμματισμού(API) οι οποίες με τη σειρά τους δημιουργούν την πρόταση συναλλαγής. Η πρόταση συναλλαγής καλεί μια συνάρτηση chaincode, έτσι ώστε τα δεδομένα να μπορούν να διαβαστούν ή/και να εγγραφούν στο μητρώο, δηλαδή να κρυπτογραφηθούν τα πιστοποιητικά. Το λογισμικό SDK με τη σειρά του παίρνει τα κρυπτογραφικά πιστοποιητικά για να δημιουργήσει μια ψηφιακή υπογραφή για αυτήν την πρόταση συναλλαγής.[41]



2. **Οι κατανεμημένοι χρήστες επιβεβαιώνουν την εγκυρότητα των ψηφιακών υπογραφών και εκτελούν την συναλλαγή**

Στη συνέχεια οι κατανεμημένοι χρήστες ακολουθούν κάποια βήματα για να επιβεβαιώσουν τα εγκυρότητα των υπογραφών.

(1) ότι η πρόταση συναλλαγής έχει σχηματιστεί σωστά

(2) ότι δεν έχει υποβληθεί ξανά στο παρελθόν (replay attack protection),δηλαδή ότι το κρυπτογραφημένο μήνυμα δεν έχει υποβληθεί ξανά. Διότι εάν υποβλήθηκε ξανά στο παρελθόν, ίσως να το είχε στην κατοχή του ένας εισβολέας και να

μπορούσε να το στείλει ξανά προκειμένου να αποσπάσει μεγάλα χρηματικά ποσά από ένα τραπεζικό λογαριασμό.

(3) ότι η υπογραφή είναι έγκυρη χρησιμοποιώντας τον φορέα παροχής υπηρεσιών(MSP). Ο συγκεκριμένος φορέας είναι ένα δομικό στοιχείο που διαθέτουν οι χρήστες, που τους επιτρέπει να επαληθεύουν τις αιτήσεις συναλλαγών των πελατών. Έτσι καθορίζουν ποιοι χρήστες έχουν το δικαίωμα να υποβάλουν μια συναλλαγή.

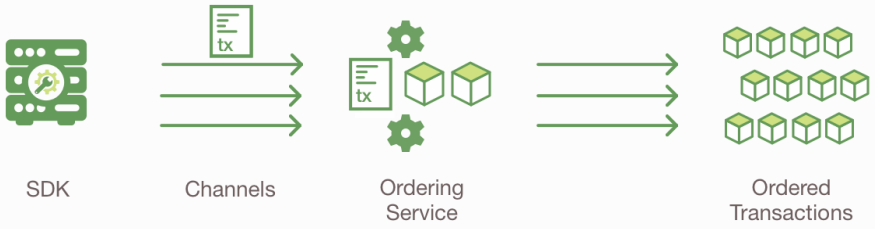
(4) Και τέλος ότι ο υποβάλλων (Πελάτης Α, στο παράδειγμα μας) έχει την εξουσιοδότηση να εκτελέσει την προτεινόμενη διαδικασία σε αυτό το δίκτυο.

Οι εγκεκριμένοι χρήστες παίρνουν προτάσεις συναλλαγών προκειμένου να καλέσουν τη συνάρτηση chaincode, η οποία έπειτα εκτελείται για να παράγει τα αποτελέσματα των συναλλαγών. Τα αποτελέσματα των συναλλαγών είναι τα μοναδικά κλειδιά του read set και οι τιμές του write set. Σε αυτό το σημείο να αναφέρουμε ότι δεν γίνεται καμία ανανέωση στο μητρώο ledger. Ο ορισμός αυτών των τιμών, μαζί με την υπογραφή των χρηστών μεταβιβάζονται ως “πρόταση απάντησης” στην εφαρμογή SDK. [41]

3. **Ελέγχονται οι προτάσεις απάντησης**

Η εφαρμογή επαληθεύει τις ψηφιακές υπογραφές των χρηστών και συγκρίνει τις προτάσεις απάντησης για να αποφασίσει εάν είναι οι ίδιες. Εάν ο αλγόριθμος chaincode υποβάλλει ερώτημα μόνο στο μητρώο ledger, τότε η εφαρμογή θα εξετάσει την απάντηση του ερωτήματος και πιθανόν να μην υποβάλλει την συναλλαγή στην Υπηρεσία Παραγγελιών. Εάν η εφαρμογή του πελάτη σκοπεύει να υποβάλει την συναλλαγή στην Υπηρεσία Παραγγελιών προκειμένου να ενημερώσει το μητρώο, τότε η εφαρμογή επιθεωρεί εάν οι χρήστες A και B αντίστοιχα το εγκρίνουν.

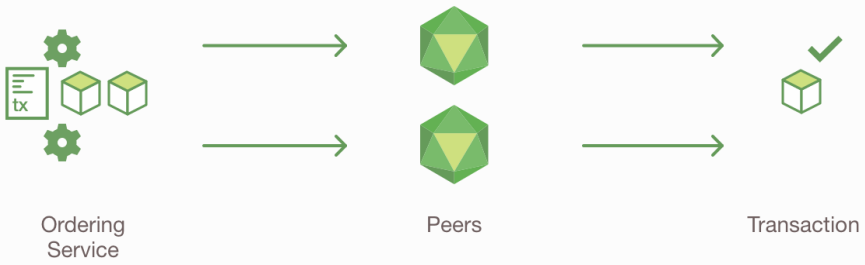
Η αρχιτεκτονική του είναι τέτοια που ακόμα και αν μια εφαρμογή επιλέξει να μην επιθεωρήσει τις απαντήσεις ή αλλιώς να μην προωθήσει μια συναλλαγή που δεν έχει εγκριθεί, τότε η πολιτική έγκρισης θα εξακολουθεί να επιβάλλεται από τους χρήστες και να τηρηθεί κατά τη φάση της επικύρωσης.[41]



4. **Ο πελάτης συγκεντρώνει τις εγκρίσεις σε μια συναλλαγή**

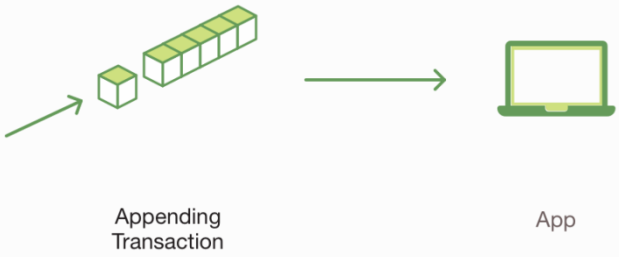
Η εφαρμογή "μεταδίδει" την πρόταση συναλλαγής και ανταποκρίνεται με ένα "μήνυμα συναλλαγής" στην υπηρεσία παραγγελιών. Έπειτα η συναλλαγή θα περιλαμβάνει τα κλειδιά και τα ορίσματα των read/write set ,τις επικυρωμένες υπογραφές των χρηστών και την ταυτότητα του καναλιού. Η υπηρεσία παραγγελιών με τη σειρά της δεν χρειάζεται να επιθεωρήσει ολόκληρο το

περιεχόμενο μιας συναλλαγής προκειμένου να λειτουργήσει. Απλά λαμβάνει συναλλαγές από όλα τα κανάλια του δικτύου, τις ταξινομεί χρονολογικά ανά κανάλι και δημιουργεί μπλοκ συναλλαγών ανά κανάλι. [41]



5. **Η συναλλαγή είναι επικυρωμένη και δεσμευμένη**

Στη συνέχεια τα μπλοκ των συναλλαγών "παραδίδονται" σε όλους τους χρήστες του καναλιού. Οι συναλλαγές εντός του μπλοκ είναι επικυρωμένες προκειμένου να εξασφαλίσουν ότι πληρείται η πολιτική έγκρισης, αλλά και ότι δεν έχουν υπάρξει αλλαγές στο μητρώο ledger για τις ρυθμίσεις ανάγνωσης read set, καθώς οι ρυθμίσεις ανάγνωσης είχαν δημιουργηθεί στο στάδιο της εκτέλεσης συναλλαγής. Τέλος οι συναλλαγές στο μπλοκ χαρακτηρίζονται ως έγκυρες ή μη έγκυρες. [41]



6. **Το μητρώο ledger ενημερώνεται**

Κλείνοντας να αναφέρουμε ότι κάθε κατανεμημένος χρήστης συνδέει το μπλοκ στην αλυσίδα του καναλιού και για κάθε έγκυρη συναλλαγή οι ρυθμίσεις γραφής write set δεσμεύονται στην βάση δεδομένων. Έπειτα η εφαρμογή του πελάτη ενημερώνεται ότι η συναλλαγή έχει προστεθεί στην αλυσίδα καθώς επίσης ενημερώνεται εάν επικυρώθηκε ή ακυρώθηκε.[41]

Κεφάλαιο 6

6.1 Παραμετροποίηση

Στην παρούσα εργασία ακλουθήσαμε την υλοποίηση του Hyperledger όπως περιγράφεται και στην επίσημη ιστοσελίδα.

Πριν ξεκινήσουμε, εγκαταστήσαμε όλα τα απαραίτητα εργαλεία στην πλατφόρμα στην οποία θα αναπτύξουμε εφαρμογές Blockchain ή το Hyperledger Fabric.

Αυτά είναι

- Τεκμηρίωση του SDK και του κόμβου SDK Hyperledger Fabric SDK .
- Hyperledger Fabric Java SDK .

Αφού τα εγκαταστήσαμε στη συνέχεια εγκαταστήσαμε το HyperLedger Fabric και είμαστε έτοιμη να φτιάξουμε ένα μικρό demo του Blockchain

Στην εφαρμογή μας θα δημιουργήσουμε ένα σενάριο χρήσης με χρήστες που θα μπαίνουν στο δίκτυο , ο ένας θα εκτελεί μια συναλλαγή (όπως για παράδειγμα μια αποστολή κειμένου όπως τιμολόγιο) και όλοι οι συμμετέχοντες θα βλέπουν την συναλλαγή σαν γεγονός αλλά μόνος αυτός που θα είναι ορισμένος στο συμβόλαιο με κατάλληλα δικαιώματα θα το βλέπει.

6.2 Τεχνικές Λεπτομέρειες Υλοποίησης HYPERLEDGER FABRIC

1. Εγκατάσταση προαπαιτούμενων εργαλείων

Για τη δημιουργία του project χρησιμοποιήθηκαν τα εξής εργαλεία:

Χρησιμοποιήθηκε το περιβάλλον Linux με εγκατεστημένα τα Ubuntu 16.04,καθώς οι νεώτερες εκδόσεις Linux δεν λειτουργουν σωστα με το Hyperledger Fabric.

- **Ubuntu 16.04**

Χρησιμοποιήθηκε το περιβάλλον Ubuntu 16.04 για το project.Στο λειτουργικό σύστημα βρίσκεται εγκατεστημένη η γλωσσά προγραμματισμού Python 3.5.1.

Το Hyperledger Fabric απαιτεί να εγκατασταθεί η Python 2.7 προκειμένου τα πακέτα npm να εγκατασταθούν με επιτυχία.

Πληκτρολογώντας την εντολή sudo apt install python στο terminal προστίθεται η Python 2.7.

- **Python 2.7**

Επίσης χρειάζονται να εγκατασταθούν τα ακόλουθα εργαλεία στην πλατφόρμα στην οποία θα λειτουργήσει στο το Hyperledger Fabric:

- **Docker**
- **Docker Compose**

πληκτρολογώντας στο terminal sudo apt install docker.io και sudo apt install docker-compose.

Συχνά, όταν μια εφαρμογή πάει σε επίπεδο production, δηλαδή σε ένα κεντρικό υπολογιστή. Εκεί υπάρχει μία σύγχυση με τους πόρους, τις βιβλιοθήκες καθώς δύναται να υπάρχουν για παράδειγμα άλλες εκδόσεις. Κατά συνέπεια, αντί να χρησιμοποιείται ένα ολόκληρο λειτουργικό σύστημα, δύναται η δυνατότητα να αφαιρεθούν τα περιττά στοιχεία του εικονικού λειρουργικού σύστηματος ώστε να δημιουργηθεί μια ελαχιστοποιημένη έκδοση του (container).

Το Docker αποτελεί ένας μηχανισμός ανοιχτού κώδικα, βασικός στόχος του οποίου είναι η αυτοματοποίηση της διανομή εφαρμογών μέσα σε δοχεία λογισμικού και την

αυτοματοποίηση του Virtualization των μικρο-υπηρεσιών του λειτουργικού συστήματος στο Linux.

Εγκαταστάθηκε η πιο πρόσφατη έκδοση του εργαλείου cURL με την εντολή

sudo apt install curl. Το cURL αποτελεί ένα πολυεργαλείο που μπορεί να κατεβάσει περιεχόμενο από το διαδίκτυο. Επίσης, το cURL τροφοδοτείται από την βιβλιοθήκη libcurl.

- **Curl**

Το εργαλείο Git για το Linux περιβάλλον. Το Git είναι ένα κατανεμημένο σύστημα ελέγχου εκδόσεων που σημαίνει ότι:

1. επιτρέπει την παράλληλη εργασία πολλαπλών ατόμων σε ένα έργο ακόμα και χωρίς την ύπαρξη σύνδεσηςσε κεντρικό δίκτυο.
2. είναι δωρεάν, σύμφωνα με την άδεια GPLv2
3. είναι γρήγορο και υποστηρίζει πολύ μεγάλα projects π.χ. LinuxKernel
4. είναι ασφαλές καθώς ο κώδικας είναι κρυπτογραφικά επικυρωμένος.

Εγκαταστάθηκε με την εντολή sudo apt tinstall git

- **Git**

Το εργαλείο Node.js αποτελεί μια πλατφόρμα ανάπτυξης λογισμικού (κυρίως διακομιστών) δομημένη σε περιβάλλον Javascript και σκοπός του είναι η παροχή εύκολου τρόπου δημιουργίας διαδικτυακών εφαρμογών.

Εγκαταστάθηκε με την εντολή sudo apt tinstall nodejs.

- **Node.js**

Το εργαλείο NPM με την εντολή sudo apt install npm

- **NPM**

Εκτελούνται οι ακόλουθες εντολές στο terminal χωρις την εντολή sudo για να διευκολύνουμε την ανάπτυξη του λογισμικού όπως επισημαίνει το Hyperledger Fabric.

- npm install -g composer-cli
- npm install -g composer-rest-server
- npm install -g composer-playground
- npm install -g yo generator-hyperledger-composer

2. Για την εγκατάσταση ενός τοπικό δίκτυο του Hyperledger Fabric εκτελούνται οι παρακάτω εντολές

1) mkdir ~/fabric-dev-servers
2) cd ~/fabric-dev-servers
3) curl --O https://raw.githubusercontent.com/hyperledger/composer-tools/master/packages/fabricdev-servers/fabric-dev-servers.tar.gz
4) tar -xvf fabric-dev-servers.tar.gz
5) export FABRIC_VERSION=h1fv12
6) ./downloadFabric.sh
7) ./startFabric.sh
8) ./createPeerAdminCard.sh

Και έτσι δημιουργήθηκε ένα τοπικό δίκτυο του Hyperledger Fabric

3. Στη συνέχεια για τη δημιουργία του project υλοποιήσαμε ένα business network

Εγκαθιστόντας το πακέτο yo και το generator-hyperledger-composer.

- yohyperledger-composer

Έπειτα έγινε η μοντελοποίηση του project όπου υλοποιήθηκαν/τροποποιήθηκαν τα παρακάτω:

- Assets
- Participants

- Transactions
- Events

Προστέθηκε η λογική με javascript στο αρχείο logic.js και τροποποιήθηκαν τα κατάλληλα permissions για τις ανάγκες του project. Τέλος υλοποιήθηκαν δυο pythonscript setup.py και run.py για την αυτόματη εκκίνηση του network και την εγγραφή του project στο δίκτυο.

6.3 Σενάριο Χρήσης

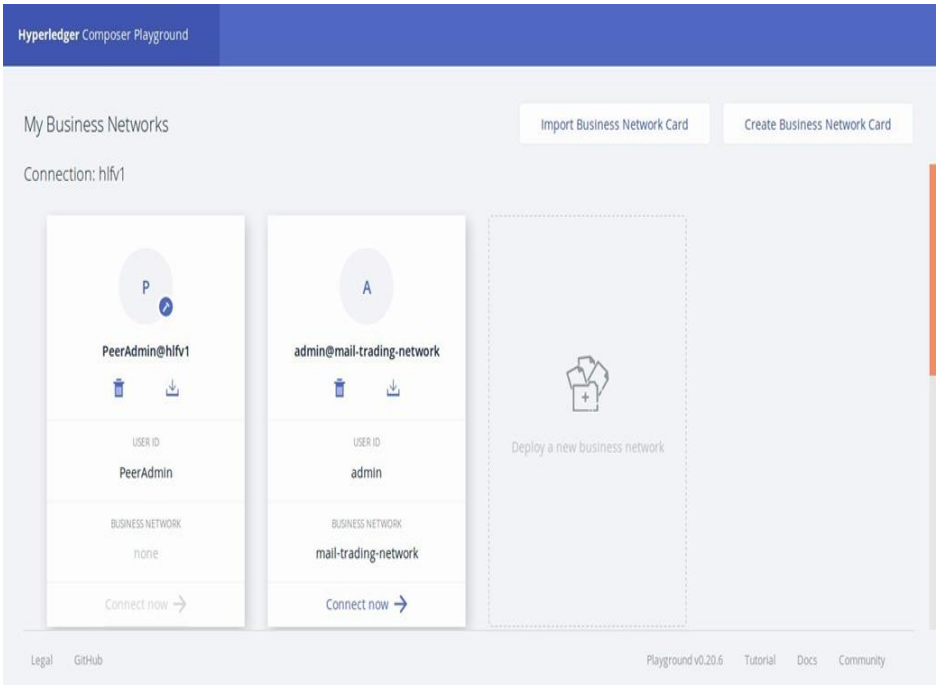
mail-trading-network

Ξεκινόντας ακολουθούμε τα παρακάτω βήματα προκειμένου να ανοίξει το demo του Hylerledger που έχουμε δημιουργήσει:

- Ανοίγουμε το virtual machine
- Ανοίγουμε το terminal και πληκτρολογούμε cd mail-trading-network
- έπειτα πληκτρολογούμε python setup.py && python run.py
- τέλος θα δούμε ότι ανοίγει ο browser στο playground.

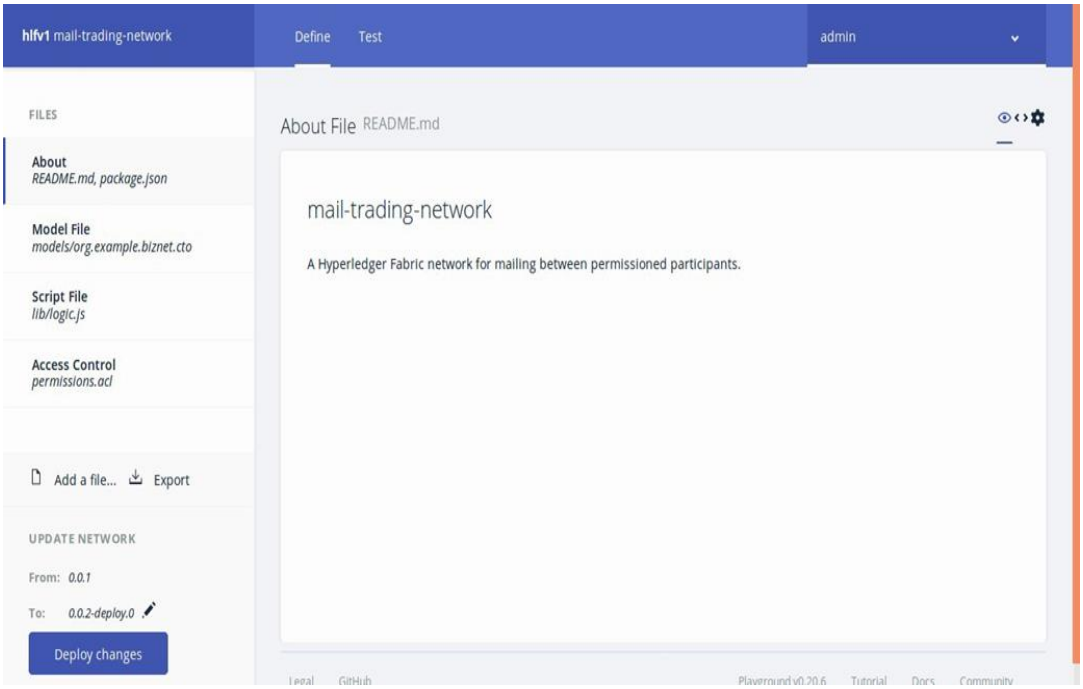
1. Στην αρχική σελίδα πατάμε στο κουτάκι με την επιλογή admin@ mail - trading-network

και στη συνέχεια πατάμε την επιλογή Connect now



Εικόνα 1 Σύνδεση με δίκτυο Blockchain

2. Αυτό είναι το menu του blockchain και πατάμε στην επιλογή Test.

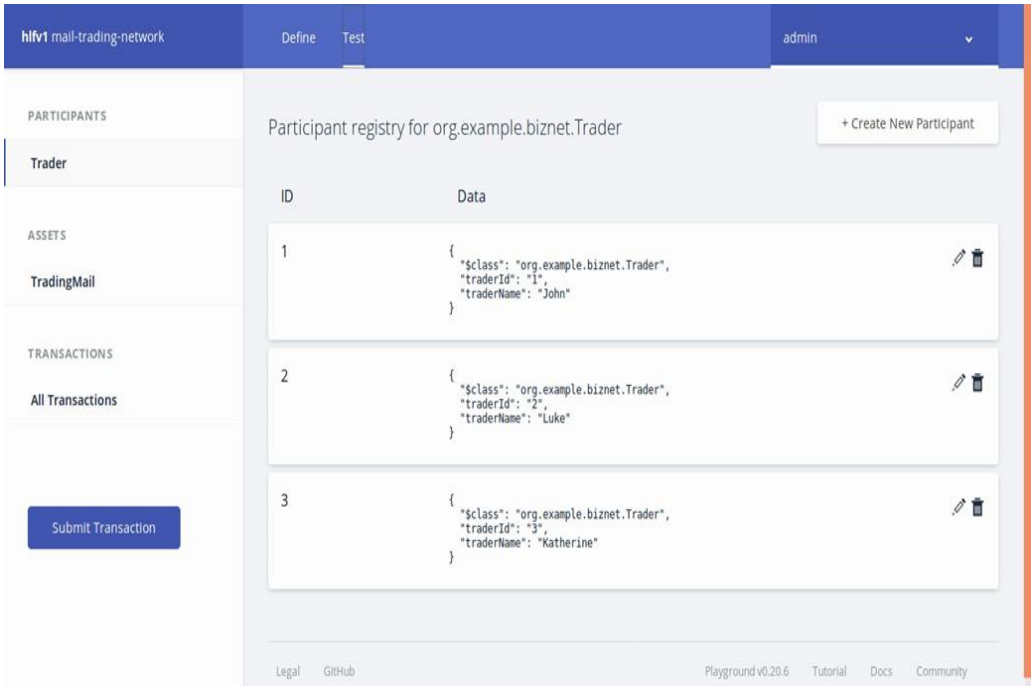


Εικόνα 2Σύνδεση με demoAPP

Έπειτα μας μεταφέρει στο τομέα των χρηστών για να δημιουργήσουμε ένα νέο χρήστη.

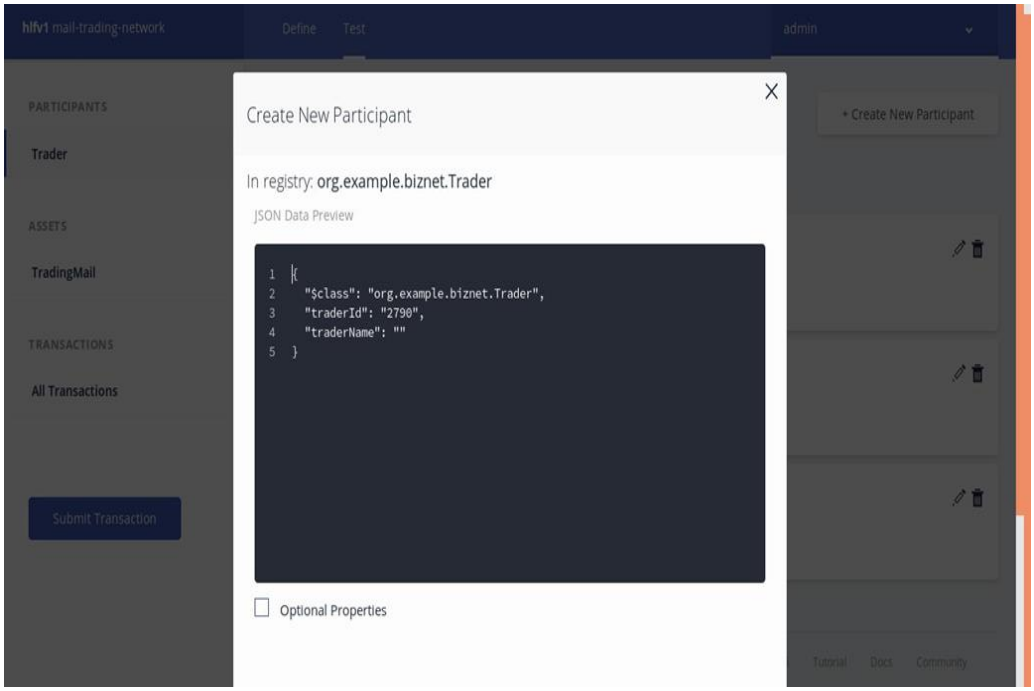
3. Έπειτα μας μεταφέρει στο τομέα των χρηστών. Εδώ εισάγουμε το χρήστη σε μορφή json.

   Αυτό είναι το μενού των χρηστών και πατάμε create new participant για να δημιουργήσουμε έναν νέο χρήστη.



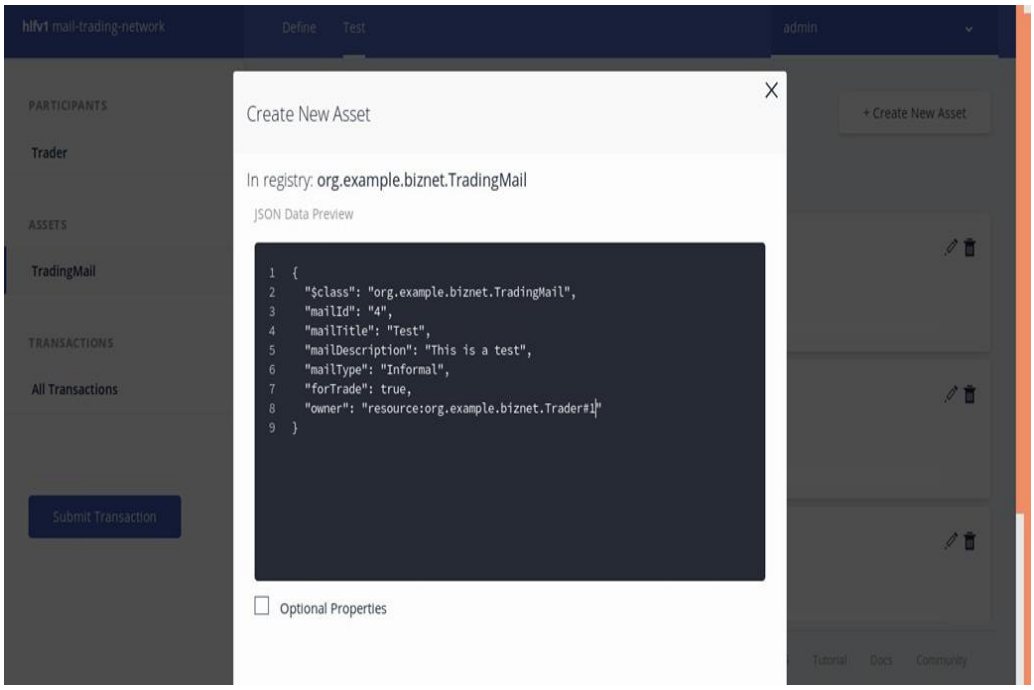
Εικόνα 3 Μενού δημιουργίας συμμετεχόντων

4. Για παράδειγμα βάζουμε τα στοιχεία όπως φαίνεται traderId : “1” traderName:”John” και πατάμε create.



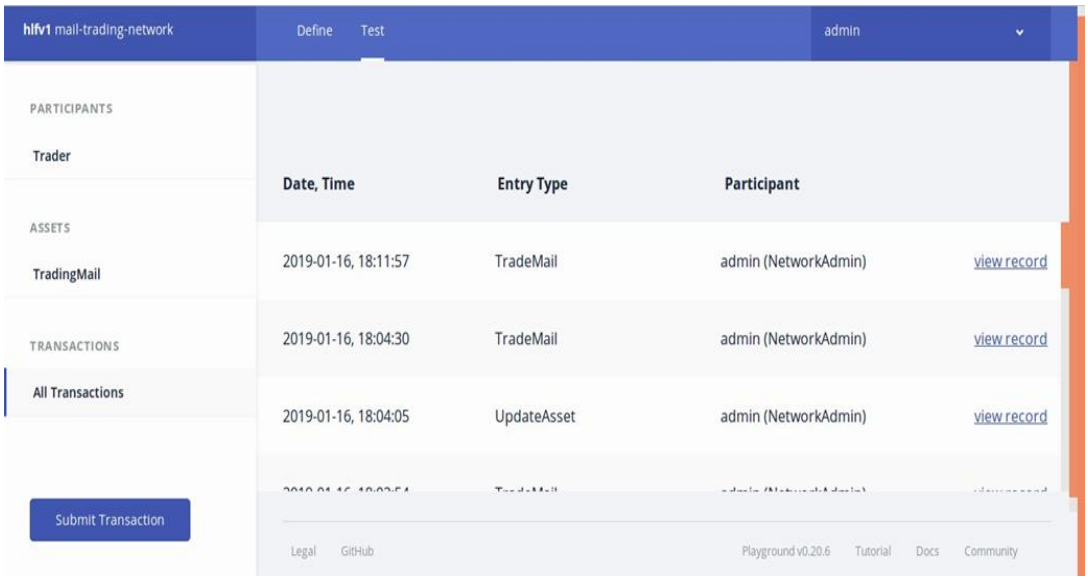
Εικόνα 4 Δημιουργία Χρήστη

5. Στη συνέχεια πατάμε στο trading mail στη δεξιά μπάρα και πατάμε create new asset για να δημιουργήσουμε ένα mail όπως φαίνεται στην εικόνα.



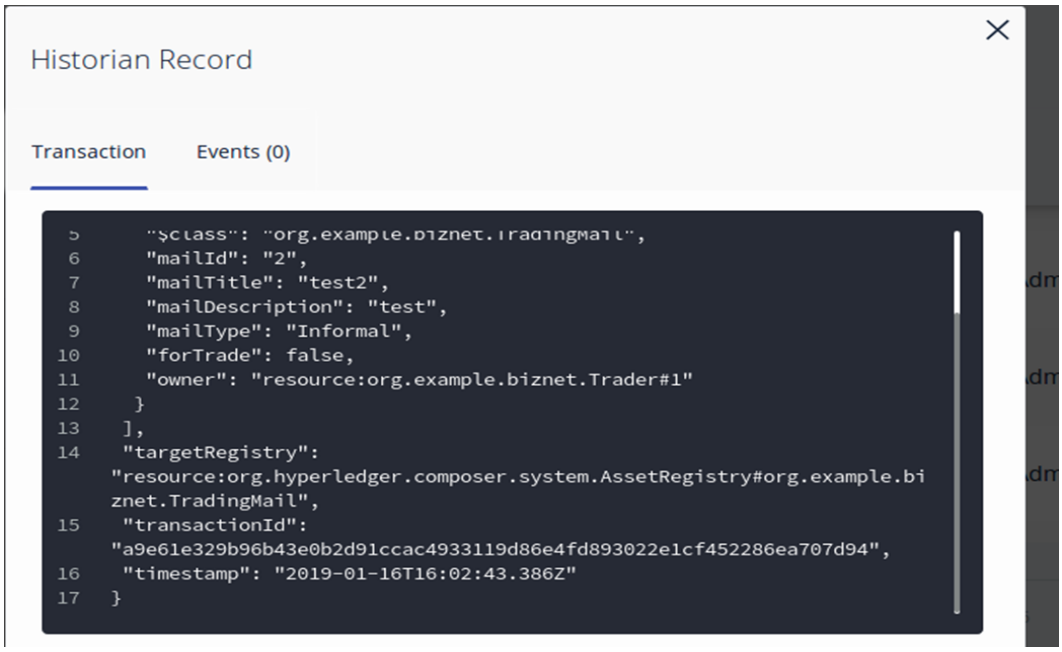
Εικόνα 5 Δημιουργία mail (asset)

6. Πατάμε All transactions στη δεξιά μπάρα και μπορούμε να δούμε όλα τα records του app μας



Εικόνα 6 Λίστα εγγραφών

7. Τελος πατάμε στο view record σε οποιοιδήποτε στοιχείο υπάρχει στη λίστα και μας εμφανίζει όλες τις πληροφορίες και ειδικά το hash, δηλαδή το transactionid όπως φαίνεται στην εικόνα.



Έτσι υλοποιήθηκε ένα blockchain για ανταλλαγή mail που μπορούν να δουν μόνο οι χρηστές με πρόσβαση στο δίκτυο.

Συμπεράσματα

Σκοπός της παρούσας πτυχιακής εργασίας ήταν οι τεχνικές κρυπτογράφησης και η περιγραφή της τεχνολογίας Blockchain των εργαλείων που εφαρμόζει και το πώς αυτές οι τεχνολογίες χρησιμοποιούνται από ένα κατανεμημένο δίκτυο.

Η τεχνολογία του Blockchain ενώ αρχικά δημιουργήθηκε για τη λειτουργία του Bitcoin, στην πορεία έγινε τεχνολογία αιχμής καθώς προσφέρει μεγάλες δυνατότητες.

Ταυτόχρονα παρέχει ασφάλεια καθώς όλες οι συναλλαγές είναι κρυπτογραφημένης στο Blockchain.

Επιπλέον καταργεί την ύπαρξη μεσάζοντα και οι συναλλασσόμενοι οφείλουν να δείξουν εμπιστοσύνη στον αλγόριθμο.

Επίσης είναι ένα αποκεντρωμένο δίκτυο και έτσι οι τράπεζες μπορούν να εξοικονομήσουν μεγάλα χρηματικά ποσά αλλά και να μειώσουν τη γραφειοκρατία και τους χρόνους διακανονισμού που απαιτούνται, όπως για μια τυπική τραπεζική συναλλαγή.

Τέλος παρέχει ασφάλεια καθώς τα αντίγραφα των καταχωρημένων συναλλαγών είναι πολύ δύσκολο να τροποποιηθούν και βρίσκονται αποθηκευμένα από τους κατανεμημένους χρήστες του δικτύου στο μητρώο ledger. Επιπροσθέτως υπάρχει διαφάνεια διότι το μητρώο ledger είναι δημόσιο και μπορούν όλοι όσοι συμμετέχουν να έχουν πρόσβαση. Έτσι στο Blockchain όλες οι συναλλαγές είναι μόνιμες και αμετάβλητες.

Βέβαια για την υλοποιηθεί το σενάριο χρήσης αντιμετωπίσαμε αρκετές δυσκολίες. Όπως για παράδειγμα μια μεταβλητή (COMPOSE_PROJECT_NAME),δημιούργησε πρόβλημα στην εκτέλεση του αλυσιδωτού κώδικα σε ένα διαφορετικό δίκτυο. Επιπλέον το όνομα του δικτύου μας δεν ταίριαζε με το όνομα του δικτύου της αλυσίδας.

Υπήρξε δυσκολία στην υλοποίηση της γλώσσας προγραμματισμού ανοιχτού κώδικα Go.

Όπως επίσης και με το Docker σε περιβάλλον Windows. Καθώς κατά την αντιγραφή αρχείων με μεγάλες διαδρομές, ορισμένα από τα αρχεία πιστοποιητικών είχαν μακρά ονόματα. Όταν αντιγράφηκαν τέτοια αρχεία μέσα στο Docker, η διαδικασία αντιγραφής έληξε απότομα χωρίς σαφή λόγο. Έτσι προτιμήσαμε το περιβάλλον των Linux. Τέλος οι πηγές στο διαδίκτυο όπως και στους δημοφιλείς πόρους ήταν πολύ λίγες, εκτός από αρκετά περιορισμένα έγγραφα στην ίδια την πλατφόρμα. Η υπάρχουσα τεκμηρίωση ήταν ανεπαρκής για την επίλυση των προβλημάτων.

Κλείνοντας μπορούμε να συμπεράνουμε ότι η τεχνολογία Blockchain και το εργαλείο Hyperledger Fabric που αναλύσαμε στην παρούσα πτυχιακή εργασία προσφέρουν πολλές δυνατότητες, αλλά δεν είναι αρκετά φιλική σε χρήστες που δεν διαθέτουν γνώσεις προγραμματισμού.

Βέβαια η τεχνολογία του Blockchain δείχνει το μέλλον για μια αποκεντρωμένη οικονομία και την δυνατότητα να εφαρμοστεί εκτός από τα κρυπτονομίσματα σε τραπεζικούς, ασφαλιστικούς, ψυχαγωγικούς και κυβερνητικούς τομείς. Αυτό έχει επίσης ως αποτέλεσμα την βελτίωση της καθημερινότητας των πολιτών προσφέροντας τους ταχύτητα, οικονομία, ασφάλεια και διαφάνεια.

Βιβλιογραφία

[1]«Τεχνολογίες Blockchain και Αποκεντρωμένες Εφαρμογές». Ανακτήθηκε στις 22 Δεκεμβρίου 2018.

[2]«ΦΕΚ. Τεύχος Β’ 1756/22.05.2017». Εφημερίδα της Κυβερνήσεως: 17803, 17805, 17807 κ.ε.. 22 Μαΐου 2017.

[3]Βλ. και εφαρμογή της τεχνολογίας “Αλυσίδα των Μπλοκ” για τη δημιουργία ενός περιβάλλοντος εμπιστοσύνης στο Διαδίκτυο των Πραγμάτων», Εθνικό Μετσόβειο Πολυτεχνείο. Ανακτήθηκε στις 2018-12-23.

[4]«Πώς μπορεί η νέα τεχνολογία να μεταμορφώσει τις χρηματοπιστωτικές αγορές;», Ευρωπαϊκή Κεντρική Τράπεζα, 19 Απριλίου 2017. Ανακτήθηκε στις 2018-12-23.

[5]Σταμπέρνας, Σωτήριος (2018). Τεχνολογίες αλυσίδας συστοιχιών και έξυπνα συμβόλαια στο πλαίσιο του Διαδικτύου των Πραγμάτων. Πανεπιστήμιο Πειραιώς (μεταπτυχιακή διατριβή). Ανακτήθηκε στις 2018-12-23.

[6]«Αυθεντικά πτυχία με τεχνολογία blockchain - Συνέντευξη του Γ.Γ. Ψηφιακής Πολιτικής, Στ. Ράλλη, στην εφ. Νέα Σελίδα». www.mindigital.gr. Ανακτήθηκε στις 2018-12-22.

[7]«Η τεχνολογία θα αυξήσει το παγκόσμιο εμπόριο κατά 1,8 έως 2 ποσοστιαίες μονάδες». Capital.gr. 2018-10-03.

[8]«ΦΕΚ. Τεύχος Β' 3488/21.08.2018. 44103 κ.ε.. .». Εφημερίδα της Κυβερνήσεως. 2018-08-21.

[9]«ΦΕΚ. Τεύχος Β' 3273/08.08.2018. 41093 κ.ε.». Εφημερίδα της Κυβερνήσεως. 2018-08-08.

«Greektranslation». GitHub.

[10]«Το Παράδοξο της σχέσης GDPR και Blockchain». BLUEVALUE.

[11]«ΠΟΕ: Πώς η τεχνολογία στηρίζει το παγκόσμιο εμπόριο». naftemporiki.gr.

«Blockchain». GREEKCOIN.

[12]«ΠΡΌΓΡΑΜΜΑ ΤΕΛΩΝΕΊΑ» (PDF). Ευρωπαϊκή Επιτροπή.

[13]«ΠΡΟΓΡΑΜΜΑ FISCALIS» (PDF). Ευρωπαϊκή Επιτροπή.

[14]«Η τεχνολογία αναμένεται να αυξήσει το παγκόσμιο εμπόριο κατά το ένα τρίτο έως το 2030». ypaithros.gr.

[15]«Blockchain – Η τεχνολογία του σήμερα με απλά λόγια». IMPOSSIBLE WORKS.

[16]«Τεχνολογία Αλυσίδας Κοινοποιήσεων και Εφαρμογές». ΠανεπιστήμιοΠειραιώς. Ανακτήθηκεστις 2018-12-23.

[17]«Blockchain Enhances Privacy, Security and Conveyance of Data». SCIENTIFIC AMERICAN.2016-06-23.

[18]«This is blockchain and here's why it matters». CNN BUSINESS.2018-10-06.

[19]«Is Blockchain The Answer To Election Tampering?». Forbes. 2018-11-02.

[20]«A secure online voting system using blockchain». BusinessTech.2018-04-13.

[21]«Many Scientific Studies Are Bogus, but Blockchain Can Help». SCIENTIFIC AMERICAN.2018-04-11.

[22]«Oxford academics open budget 'Uber of universities'». The Times.2018-06-19.

[23]«U.S. Health Care Companies Begin Exploring Blockchain Technologies». SCIENTIFIC AMERICAN. 2018-07-19.

[23]«Blockchain: Η τεχνολογία που αλλάζει για πάντα οικονομία και διαδίκτυο». insider.gr. 2018-03-06.

[24]«Ohio becomes the first state to allow businesses to pay taxes with Bitcoin». CNN WORLD.2018-11-26.

[25]«Blockchain tracks food all the way from farm to table». The Times.2018-01-25.

[26]«Enterprise Ethereum: Blockchain Use Cases and Applications by Industry». Medium.

[27]«Facebook boss Mark Zuckerberg plots to launch own 'currency'». The Times.2018-05-13.

[28]«Why Blockchain Needs A Community Now More Than Ever». Forbes. 2018-12-20.

[29]«Οι 50 μεγαλύτερες εισηγμένες που εξερευνούν τις δυνατότητες του blockchain». Capital.gr. 2018-07-04.

[30]«On cusp of a new finance revolution». The Times.2018-07-13.

[31]«Blockchain revolution in mutual fund trades». The Times.2018-12-03.

[32]«Blockchain system promises sea change in insurance market». The Times.2017-09-06.

[33]«Industry executives see blockchain becoming disruptive force in auto sector». The Economic Times.2018-12-23.

[34]«How Blockchain Allows A Data-Driven Approach To Investing In Startups». Forbes. 2018-12-22.

[35]«Swiss Post and Swisscom launch a 100% Swiss infrastructure for blockchain applications». Swisscom.2018-12-06.

[36]«JPMorgan widens blockchain payments to more than 75 banks». Financial Times.2018-09-25.

[37]«Banks complete first syndicated loan on blockchain». FinancialTimes.2018-11-06.

[38]Cryptography&Blockchain–Part1https://blockchainhub.net/blog/blog/cryptography-blockchain-part-1/Δεκ 2017

[39]Cryptography&Blockchain–Part2 https://blockchainhub.net/blog/blog/cryptography-blockchain-part-2/ Δεκ 2017

[40]Top-5-Most-Compelling-Use-Cases-For-Blockchainhttps://medium.com/bitfwd/top-5-most-compelling-use-cases-for-blockchain-technology-d198e500e3d3 Emily Su 22 Ιουνίου 2018

[41]https://hyperledger-fabric.readthedocs.io/en/release-1.3/whatis.html

[42]https://www.hyperledger.org/wp-content/uploads/2017/08/Hyperledger_Arch_WG_Paper_1_Consensus.pdf

[43]https://www.ethereum.org/

[44]https://www.mycryptopedia.com/double-spending-explained/ / /Δεκ 2018

[45]https://www.ibm.com/blogs/research/2018/02/architecture-hyperledger-fabric/

/Φεβ 2018