



ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΤΕΧΝΟΛΟΓΙΑΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

Αξιοποίηση τεχνολογιών Blockchain σε εφαρμογές κρίσιμης
αποστολής: μια μελέτη περίπτωσης στο οικοσύστημα Hyperledger
*Using Blockchain technologies in mission-critical applications: a
case study, based on the Hyperledger ecosystem*

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Νάκου Χριστίνα

Επιβλέπων : Βασίλειος Βεσκούκης

Καθηγητής Ε.Μ.Π.

Αθήνα, Οκτώβριος 2019

Αθήνα, Οκτώβριος 2019



ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΤΕΧΝΟΛΟΓΙΑΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

Αξιοποίηση τεχνολογιών Blockchain σε εφαρμογές κρίσιμης
αποστολής: μια μελέτη περίπτωσης στο οικοσύστημα Hyperledger
*Using Blockchain technologies in mission-critical applications: a
case study, based on the Hyperledger ecosystem*

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Νάκου Χριστίνα

Επιβλέπων : Βασίλειος Βεσκούκης
Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την .. Νοεμβρίου 2019.

.....
Βασίλειος Βεσκούκης
Καθηγητής Ε.Μ.Π.

.....
Νικόλαος Παπασπύρου
Καθηγητής Ε.Μ.Π.

.....
Νικόλαος Δουλάμης
Καθηγητής Ε.Μ.Π.

Αθήνα, Οκτώβριος 2019

.....

Χριστίνα Νάκου

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Copyright © Χριστίνα Νάκου, 2019

Με επιφύλαξη παντός δικαιώματος. All rights reserved.

Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας εργασίας, εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Ερωτήματα που αφορούν τη χρήση της εργασίας για κερδοσκοπικό σκοπό πρέπει να απευθύνονται προς τον συγγραφέα.

Οι απόψεις και τα συμπεράσματα που περιέχονται σε αυτό το έγγραφο εκφράζουν τον συγγραφέα και δεν πρέπει να ερμηνευθεί ότι αντιπροσωπεύουν τις επίσημες θέσεις του Εθνικού Μετσόβιου Πολυτεχνείου.

Περίληψη

Το διαδίκτυο αποτελεί αναμφισβήτητα μια από τις σπουδαιότερες εφευρέσεις του περασμένου αιώνα κι έχει αναχθεί πλέον σε αναπόσπαστο κομμάτι της καθημερινότητας για μεγάλο μέρος του πληθυσμού. Έφερε μια επανάσταση στον τρόπο που οι άνθρωποι και οι οργανισμοί αλληλεπιδρούν. Πρόσφατα έχει δημιουργηθεί μια νέα τάση αποκεντροποίησης της διαχείρισης των διαδικτυακών εφαρμογών. Προς αυτήν την κατεύθυνση συντελεί και η ανάπτυξη τεχνολογιών όπως το Blockchain και ο σημασιολογικός ιστός. Η τεχνολογία Blockchain έχει αρκετά παραδείγματα εφαρμογής παρέχοντας επικοινωνίες, κυβερνοασφάλεια και στήριξη στις συναλλαγές σε αρκετούς κλάδους, όπως τα χρηματοοικονομικά, η υγεία, η εφοδιαστική αλυσίδα και η δημόσια διοίκηση.

Είναι μια καινούργια τεχνολογία που διαρκώς εξελίσσεται και ανοίγεται σε καινούργιους ορίζοντες, όπως για παράδειγμα η ανάπτυξη ασφαλών πλατφόρμων επικοινωνίας. Το blockchain επιτρέπει τη δημιουργία αμετάβλητων αρχείων που αποθηκεύονται σε πακέτα (blocks). Τα πακέτα επαληθεύονται και αντιγράφονται από κόμβους μέσα στο δίκτυο blockchain. Επειδή δεν υπάρχει μια ενιαία κεντρική βάση δεδομένων, τα αρχεία του blockchain είναι απολύτως ασφαλή από παρεμβάσεις, καθώς όλα αντιγράφονται και διατηρούνται σε αλυσιδωτή μορφή(chaincode). Συνεπώς, οι λύσεις blockchain επιτρέπουν στις εταιρείες, στους προμηθευτές και στις επιχειρήσεις ενεργειακών υπηρεσιών να προστατεύουν, να δημιουργούν και να μεταδίδουν δεδομένα αποδοτικά σε ένα ασφαλές περιβάλλον, βοηθώντας και στη μείωση του κόστους.

Ο σκοπός της παρούσας εργασίας είναι η διερεύνηση της τεχνολογίας Blockchain και η δημιουργία μιας αποκεντρωμένης πλατφόρμας επικοινωνίας για την πραγματοποίηση μιας αεροδιακομιδής ασθενών που βασίζεται στο Hyperledger Blockchain. Σκοπός της εφαρμογής είναι η παροχή μιας ποιοτικής και αδιάβλητης πληροφορίας στην αεροδιακομιδή, από το σημείο της αίτησης μέχρι την διεκπεραίωσή της. Με την εφαρμογή οι φορείς που εμπλέκονται στην αεροδιακομιδή θα έχουν τη δυνατότητα να επικοινωνούν απευθείας μέσα από την πλατφόρμα ενώ παράλληλα θα επιτρέπεται σε άλλους κρατικούς φορείς να αποτελέσουν τον ελεγκτικό παράγοντα στην πλατφόρμα ώστε να διευκρινιστεί ποιοι λόγοι επέφεραν την αποτυχία της αποστολής. Μέσω της αδιαβλητότητας της πληροφορίας, η αξιοπιστία της επικοινωνίας μεταξύ των φορέων είναι πραγματική και έτσι δεν θα τίθεται θέμα εμπιστοσύνης ή δολιοφθοράς.

Στο πλαίσιο της εκπόνησης της εργασίας αναλύθηκαν οι έννοιες και οι λειτουργίες των έξυπνων συμβολαίων και των αλγορίθμων συναίνεσης. Επίσης, μελετήθηκε σε βάθος η τεχνολογία και ο τρόπος υλοποίησης του Hyperledger και σε αυτόνομο περιβάλλον και σε περιβάλλον πολλαπλών μηχανημάτων. Και τέλος, ερευνήθηκε ο σημερινός τρόπος λειτουργίας των εμπλεκόμενων φορέων μιας αεροδιακομιδής για να αναπτυχθεί ο τρόπος επικοινωνίας μέσω της τεχνολογίας Blockchain, καθώς καταγράφηκαν τα συνολικά οφέλη και οι επεκτάσεις αυτής της τεχνολογίας.

Λέξεις κλειδιά: Blockchain, Hyperledger Fabric, Hyperledger Composer, αεροδιακομιδή ασθενών, έξυπνα συμβόλαια, αλγόριθμοι συναίνεσης.

Abstract

Undoubtedly the internet is one of the most important innovations of the previous century and it has become an integral part of our everyday life. It has revolutionized the way people and organizations interact. There has been a recent trend to create decentralized web applications. The development of cutting-edge technologies such as the Blockchain and the semantic web also contributes to this direction. Blockchain technology has several application examples providing communications, cybersecurity and transaction support across a variety of industries, such as finance, health, supply chain and public administration.

Blockchain is a new technology constantly evolving and broaden our horizons, such as the development of secure communication platforms. Blockchain allows you to create unchanged files stored in blocks. The packets are verified and copied from nodes within the blockchain network. Because there is no single central database, blockchain files are completely safe from tampering, as they are all copied and stored in a chaincode. Thus, Blockchain solutions enable companies, suppliers and service providers to protect, create and transmit data efficiently in a secure environment, while also helping to reduce costs.

The purpose of the current dissertation is to research Blockchain technology as well as to develop a decentralized communication platform for the realization of an air medical transportation based on the Hyperledger Blockchain. The purpose of the application is to provide quality and immutable information in air medical transportation from the point of request to its completion. The organizations who are involved in air medical transportation will be able to communicate directly through the platform, allowing other government agencies to be a check on the platform in order to clarify the reasons for the failure of the mission. Through the impartiality of information, the credibility of the communication between the organizations is real and thus there won't be a matter of trust or undermining.

During the development of this research study, the concepts and functions of smart contracts and consensus algorithms were analyzed. Furthermore, I studied in depth the technology and the implementation of Hyperledger Blockchain both in standalone and multiple machines environments. Finally, I investigated the current mode of communication between the organizations for the air medical transportation in order to develop the new way of communication through Blockchain technology, as the overall benefits and extensions of this technology were recorded.

Key words: Blockchain, Hyperledger Fabric, Hyperledger Composer, air medical transportation, smart contracts, consensus algorithms.

Ευχαριστίες

Με την ευκαιρία της ολοκλήρωσης της διπλωματικής μου εργασίας, θα ήθελα να εκφράσω τις πιο θερμές μου ευχαριστίες προς τον κ. Βασίλειο Βεσκούκη, Αναπληρωτή Καθηγητή Ε.Μ.Π., για τη δυνατότητα που μου παρείχε να εργαστώ ερευνητικά στον τομέα των Blockchain, καθώς και για την πολύτιμη καθοδήγησή του σε όλη την πορεία διεκπεραίωσης της εργασίας.

Ακόμη, ευχαριστώ τον κ. Αντώνη Βιτωράτο, πιλότο της Αεροπορίας Στρατού και υποψήφιο διδάκτορα ΕΜΠ για τις συμβουλές του και τις πληροφορίες που μου παρείχε σχετικά με τον σημερινό τρόπο αεροδιακομιδής.

Θέλω, επίσης, να ευχαριστήσω την μητέρα μου και την αδερφή μου για την αγάπη, την υπομονή και την αμερόληπτη υποστήριξη τους στην εκπόνηση της εργασίας αλλά και σε όλη τη διάρκεια των σπουδών μου.

Τέλος, θα ήθελα να προσθέσω ένα ευχαριστώ στους φίλους μου και τους συμφοιτητές μου για την συνεργασία και την αλληλοϋποστήριξη όλα αυτά τα χρόνια της φοίτησής μου.

Περιεχόμενα

Περίληψη	5
Abstract.....	7
Ευχαριστίες	9
Κεφάλαιο 1. Γενικά για τεχνολογίες Blockchain.....	15
1.1 Τι είναι Blockchain.	15
1.2 Blockchain και «παραδοσιακό» μοντέλο διασφάλισης εμπιστοσύνης.....	17
1.2.1 Το παραδοσιακό μοντέλο που βασίζεται σε αρχές πιστοποίησης («μεσάζοντες», τρίτα έμπιστα μέρη).....	17
1.2.2 Το Blockchain όπου καθένας είναι η αρχή πιστοποίησης	18
1.3 Βασικές αρχές και έννοιες	19
1.3.1 Consensus algorithms	19
1.3.2 Smart contracts.....	20
1.4 Χαρακτηριστικοί consensus algorithms.....	22
1.4.1 Proof of Work Algorithm.....	22
1.4.2 Proof of Stake Algorithm	23
1.4.3 Practical Byzantine Fault Tolerance	23
1.4.4 Άλλοι αλγόριθμοι.....	25
1.4.5 Σύγκριση των consensus αλγορίθμων.....	27
1.5 Θεματικές περιοχές εφαρμογών Blockchain	29
1.5.1 Κρυπτονομίσματα	29
1.5.2 Υγεία	30
1.5.3 Εφοδιαστική αλυσίδα.....	31
1.5.4 Διακίνηση εγγράφων.....	32
1.5.5 Δημόσια διοίκηση και ασφάλεια.....	32
1.5.6 Δημοκρατία.....	33
1.5.7 Άλλοι τομείς.....	34
1.6 Περιβάλλοντα εργασίας Blockchain.....	35
1.6.1 Hyperledger.....	35
1.6.2 Ethereum	35
1.6.3 Άλλα Blockchain Δίκτυα	36
Κεφάλαιο 2. Το οικοσύστημα Hyperledger.....	37
2.1 Γενικά.....	37
2.1.1 Ιστορία	37
2.1.2 Γενικά χαρακτηριστικά, πλαίσια και εργαλεία	38
2.1.3 Περιβάλλον εκτέλεσης.....	40
2.1.4 Πηγές πληροφοριών.....	41

2.2	Αντιστοίχιση εννοιών Blockchain στο Hyperledger.....	42
2.2.1	Consensus algorithms	42
2.2.2	Smart contracts.....	44
2.2.3	Πρόσθετες έννοιες	45
2.3	Εγκατάσταση Hyperledger σε αυτόνομο περιβάλλον.....	47
2.3.1	Βήματα.....	47
2.3.2	Σημεία που χρήζουν προσοχής	68
2.4	Προγραμματισμός σε περιβάλλον Hyperledger.....	71
2.4.1	Υποστηριζόμενα περιβάλλοντα προγραμματισμού	71
2.4.2	Δομές δεδομένων	73
2.4.3	Υλοποίηση smart contracts	73
2.4.4	Υλοποίηση consensus algorithms	76
Κεφάλαιο 3. Εφαρμογές κρίσιμης αποστολής σε Blockchain		77
3.1	Γενικά χαρακτηριστικά και απαιτήσεις	77
3.1.1	Εφαρμογές κρίσιμης αποστολής	77
3.1.2	Γιατί Blockchain	78
3.2	Μελέτη περίπτωσης: εφαρμογή επείγουσας αεροδιακομιδής ασθενών	79
3.2.1	Εμπλεκόμενοι φορείς (οργανισμοί)	79
3.2.2	Ροή ενεργειών που λαμβάνουν χώρα.....	80
3.2.3	Τεχνολογίες που χρησιμοποιούνται.....	81
3.2.4	Υλοποίηση ασφάλειας	83
3.2.5	Ακεραιότητα δεδομένων που ανταλλάσσονται.....	84
3.2.6	Περιορισμοί από το θεσμικό πλαίσιο.....	85
3.2.7	Απαιτήσεις ακεραιότητας καταγραφής γεγονότων και περιεχομένων επικοινωνιών ...	87
3.2.8	Σημεία που χρήζουν προσοχής – αδυναμίες του σημερινού συστήματος	87
3.3	Αρχιτεκτονική πολλαπλών οργανισμών στο Hyperledger.....	89
3.3.1	Μια αρχιτεκτονική με Blockchain	89
3.3.2	Ρυθμίσεις και ρόλοι.....	91
3.3.3	Αντιστοίχιση ενεργειών και αρμοδιοτήτων σε περιβάλλον Blockchain.....	92
3.3.4	Βήματα υλοποίησης στο Hyperledger	93
3.3.5	Σημεία προσοχής.....	99
3.4	Κρίσιμες επιχειρησιακές λειτουργίες σε περιβάλλον Blockchain	100
3.4.1	Καταγραφή (logging) επικοινωνιών	100
3.4.2	Παράδειγμα ανταλλαγής κρίσιμων δεδομένων.....	100
3.5	Θέματα συνεργασίας με προϋπάρχοντα “legacy” πληροφοριακά συστήματα	101
3.5.1	Ενδεικτικές αρχιτεκτονικές integration.....	101
3.5.2	Σημεία που χρήζουν προσοχής	103

Κεφάλαιο 4. Συμπεράσματα	104
4.1 Σύνοψη εργασίας	104
4.2 Σχετικά με τις τεχνολογίες Blockchain.....	104
4.3 Blockchain και εφαρμογές κρίσιμης αποστολής	105
4.4 Σχετικά με το περιβάλλον Hyperledger	105
4.5 Επόμενα βήματα	106
Βιβλιογραφία	107
Παραρτήματα.....	115
Παράρτημα 1. Δημιουργία νέου VM και επικοινωνία με τον κεντρικό υπολογιστή.....	115
Παράρτημα 2. Εγκατάσταση των προαπαιτούμενων για το Hyperledger Fabric και Composer ...	124
Παράρτημα 3. Μελέτη περίπτωσης αεροδιακομιδής: Διάγραμμα Business Process Model (BPM)	129

Πίνακας Σχημάτων

Εικόνα 1 Trusted Blockchain, Rebuilding Community Confidence.....	16
Εικόνα 2 Objectives of Consensus mechanism.....	20
Εικόνα 3 Utility of smart contracts	21
Εικόνα 4 Flow of Proof of Work	22
Εικόνα 5 Flow of Proof of Stake.....	23
Εικόνα 6 Process of PBFT	24
Εικόνα 7 Hyperledger Fabric-high level transaction flow	43
Εικόνα 8 Vehicle chaincode Diagram.....	45
Εικόνα 9 Hyperledger Composer Architecture.....	75
Εικόνα 10 Τρόπος επικοινωνίας με τον σημερινό τρόπο λειτουργίας.....	81
Εικόνα 11 Business model diagram: Επικοινωνία με Blockchain.....	89
Εικόνα 12 Αρχιτεκτονική του Hyperledger Fabric στην αεροδιακομιδή	90
Εικόνα 13 Insertion of a block into a chaincode.....	90
Εικόνα 14 Communication Diagram: Τρόπος επικοινωνίας οργανισμών για αεροδιακομιδή με blockchain σύστημα.....	92
Εικόνα 15 Τοπολογία συστήματος Hyperledger Fabric για δύο οργανισμούς.....	93
Εικόνα 16 Activity Diagram: Μελέτη περίπτωσης επικοινωνίας ΕΚΑΒ με ΓΕΑ.....	101
Εικόνα 17 Τρόποι ενσωμάτωσης του Blockchain στα συμβατικά πληροφοριακά συστήματα.....	102

Κεφάλαιο 1. Γενικά για τεχνολογίες Blockchain

1.1 Τι είναι Blockchain.

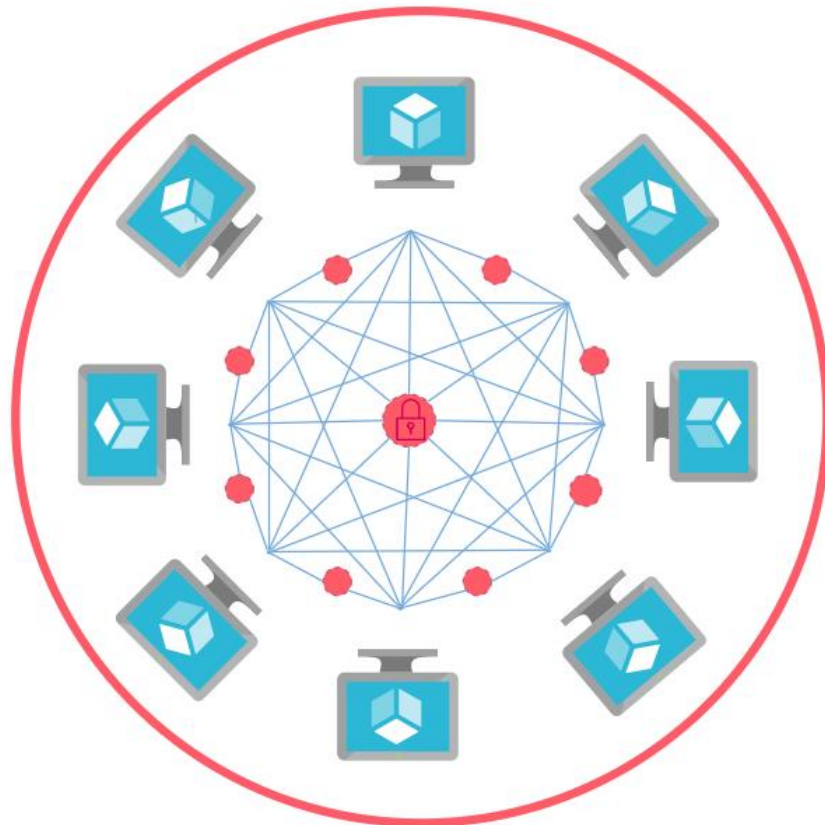
Το Blockchain είναι μια κατανεμημένη δομή δεδομένων σε ένα δίκτυο όπου δεν υπάρχει κεντρική οντότητα που να είναι υπεύθυνη για τη διαχείριση των δεδομένων που καταγράφονται. Αποτελεί μια σειρά από αμετάβλητα δεδομένα, τα οποία τα διαχειρίζονται πολλές συστάδες υπολογιστών και όχι μια συγκεκριμένη οντότητα. Κάθε μπλοκ πληροφοριών είναι ασφαλές και εξαρτώμενο από άλλα μπλοκ καθώς περιέχει ένα hash του προηγούμενου μπλοκ, δημιουργώντας έτσι μια αλυσίδα από μπλοκ, από όπου προκύπτει και το όνομα Blockchain.

Η ιδέα του Blockchain αποτελεί έναν τρόπο μεταφοράς δεδομένων από τον χρήστη Α στον χρήστη Β με μια απόλυτα αυτοματοποιημένη και ασφαλή διαδικασία, χωρίς εξάρτηση από τον τρίτο ή τον μεσάζοντα. Κατά τη δημιουργία κάθε μπλοκ χιλιάδες ή και εκατομμύρια υπολογιστές σε ολόκληρο το δίκτυο επικυρώνουν αυτό το μπλοκ. Το επικυρωμένο μπλοκ προστίθεται στην αλυσίδα, η οποία είναι μοναδική. Η παραποίηση των δεδομένων μιας καταγραφής, προϋποθέτει την παραποίηση ολόκληρης της αλυσίδας, το οποίο είναι πρακτικά αδύνατο, διότι κάτι τέτοιο θα απαιτούσε πρόσβαση σε ολόκληρο το δίκτυο. Το σύστημα επικύρωσης μπλοκ έχει ως αποτέλεσμα τα νέα δεδομένα που προστίθενται να είναι αμετάβλητα κι απαραβίαστα καθώς και τα παλιά να διατηρούνται για πάντα, δίνοντας την δυνατότητα της διαφάνειας και της αντοχής τους στο χρόνο. Κάθε κόμβος στο δίκτυο διατηρεί ένα αντίγραφο του blockchain, επιτρέποντας στον χρήστη να επαληθεύσει την εγκυρότητα κάθε συναλλαγής, έτσι ώστε να μην υπάρχει ποτέ διπλή μέτρηση.

Το blockchain μπορεί επίσης να θεωρηθεί ως προσέγγιση σχεδίασης λογισμικού που δεσμεύει έναν αριθμό υπολογιστές που υπόκεινται συνήθως στην ίδια διαδικασία συναίνεσης για την δημοσιοποίηση ή καταγραφή των πληροφοριών που κατέχουν και όπου όλες οι σχετικές αλληλεπιδράσεις επαληθεύονται από κρυπτογράφηση. Για τους προγραμματιστές, ένα blockchain είναι πρωτίστως ένα σύνολο τεχνολογιών λογισμικού. Το blockchain περιλαμβάνει τεχνολογίες για την κατασκευή μιας νέας γενιάς εφαρμογών, που θα είναι αποκεντρωμένες και κρυπτογραφικά ασφαλείς. Συνεπώς, blockchain είναι ένας νέος τρόπος ανάπτυξης εφαρμογών και αποτελεί μια επανάσταση στο κόσμο της επικοινωνίας. (Shermin Voshmgir, 2019)

Το Blockchain διακρίνεται σε τρία είδη, το public ή permissionless blockchain, το private ή permissioned blockchain και το hybrid blockchain. Τα public blockchain δίκτυα επιτρέπουν στον οποιοδήποτε να συμμετέχει στο δίκτυο, ως χρήστες, miners, developers, μέλη κοινότητας. Όλες οι συναλλαγές διαδραματίζονται με διαφάνεια και σαφήνεια και όλοι μπορούν να τις ελέγξουν. Τα δίκτυα είναι σχεδιασμένα απκεντρωμένα και χωρίς κανένα ατομικό ή κεντρικό έλεγχο των συναλλαγών. Στα private blockchain δίκτυα οι συμμετέχοντες χρειάζονται συγκατάθεση για να συμμετάσχουν στα δίκτυα. Οι συναλλαγές είναι ιδιωτικές και είναι διαθέσιμες μόνο σε συμμετέχοντες στο οικοσύστημα στους οποίους έχει δοθεί άδεια να ενταχθούν στο δίκτυο. Τα ιδιωτικά blockchains είναι πιο συγκεντρωτικά από τα δημόσια blockchain δίκτυα. Τα ιδιωτικά blockchains είναι πολύτιμα για τις επιχειρήσεις που επιθυμούν να συνεργαστούν και να μοιραστούν τα δεδομένα, αλλά δεν θέλουν τα ευαίσθητα επιχειρηματικά τους δεδομένα να είναι ορατά σε ένα δημόσιο blockchain. Αυτά τα δίκτυα, από τη φύση τους, είναι πιο συγκεντρωμένα, οι φορείς που δημιουργούν το δίκτυο έχουν σημαντικό έλεγχο των συμμετεχόντων και των δομών διοίκησης. Τα hybrid blockchain δίκτυα συνδυάζουν τα οφέλη των private και public blockchains, δίνοντας στις επιχειρήσεις την ευελιξία να επιλέγουν ποια δεδομένα θα είναι δημόσια και διαφανή και ποια θα είναι ιδιωτικά.

Τέλος, ένα ακόμη είδος blockchain είναι το consortium blockchain το οποίο διαφέρει από τα private δίκτυα στο γεγονός ότι ο έλεγχος των δεδομένων δεν γίνεται από μία οντότητα αλλά από μια ομάδα. Αυτό το συνεργατικό μοντέλο προσφέρει μερικές από τις καλύτερες περιπτώσεις χρήσης για τα οφέλη του blockchain, καθώς τα μέλη της ομάδας θα έχουν μεγαλύτερη ελευθερία στην συνεργασία τους. Έτσι, οι συμμετέχοντες σε αυτό το δίκτυο θα μπορούν να συμπεριλάβουν οποιοδήποτε από τις κεντρικές τράπεζες, τις κυβερνήσεις και τις αλυσίδες εφοδιασμού. (Dragonchain Team, 2019)



Εικόνα 1 Trusted Blockchain, Rebuilding Community Confidence

1.2 Blockchain και «παραδοσιακό» μοντέλο διασφάλισης εμπιστοσύνης

1.2.1 Το παραδοσιακό μοντέλο που βασίζεται σε αρχές πιστοποίησης («μεσάζοντες», τρίτα έμπιστα μέρη)

Οι παραδοσιακές βάσεις δεδομένων χρησιμοποιούν την αρχιτεκτονική δικτύου πελάτη-διακομιστή (client-server). Στο μοντέλο αυτό ένας χρήστης (γνωστός ως πελάτης) μπορεί να τροποποιήσει δεδομένα, τα οποία είναι αποθηκευμένα σε έναν κεντρικό υπολογιστή. Ο κεντρικός διακομιστής πρέπει πάντα να είναι ενεργός και να εξυπηρετεί αιτήσεις για υπηρεσίες από άλλους υπολογιστές δηλαδή τους πελάτες. Ο ρόλος του διακομιστή είναι καθοριστικός για την λειτουργία αυτού του είδους δικτύων, ο οποίος πιστοποιεί τα διαπιστευτήρια ενός πελάτη πριν από την παροχή πρόσβασης στη βάση δεδομένων. Δηλαδή αποθηκεύει τόσο τις πληροφορίες επικοινωνίας όσο και τις πληροφορίες λογαριασμού χρήστη. Οι περισσότερες πλατφόρμες άμεσων μηνυμάτων χρησιμοποιούν ένα κεντρικό (centralized) δίκτυο. Δεδομένου ότι ο εξυπηρετητής είναι υπεύθυνος για τη διαχείριση της βάσης δεδομένων, εάν διακυβεύεται η ασφάλεια του, τα δεδομένα μπορούν να τροποποιηθούν, να διαγραφούν. (Goyal, 2018)

Οι client-server αρχιτεκτονικές είναι ευάλωτες στις Denial of Service και Distributed Denial of Service (DoS / DDoS) επιθέσεις, επειδή παρέχουν στους επιτιθέμενους έναν μόνο στόχο να χτυπήσουν. Παράλληλα, δεδομένου των μεμονωμένων σημείων αποτυχίας, το client-server σύστημα μπορεί να προκαλέσει παραβίαση δεδομένων. Οι υπηρεσίες που διαχειρίζονται τους εξυπηρετητές οφείλουν να διασφαλίσουν την ακεραιότητα και την ασφάλεια των δεδομένων καθώς και την εύρυθμη λειτουργία του εκάστοτε διακομιστή.

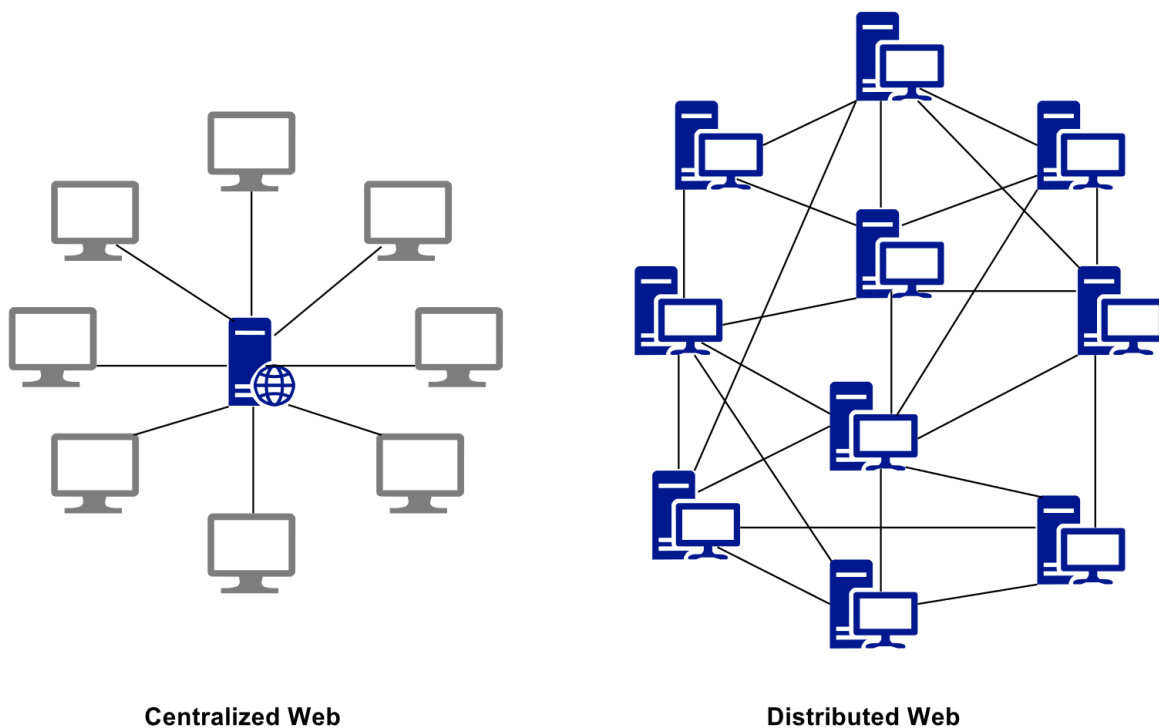
Ακόμη, οι client-server αρχιτεκτονικές προκαλούν σοβαρά προβλήματα προστασίας της ιδιωτικής ζωής. Οι χρήστες έχουν ελάχιστη ή καθόλου ιδέα για το τι συμβαίνει πίσω από τους περιφραγμένους χώρους των κεντρικών υπηρεσιών. Επομένως, δεν γνωρίζουν με ακρίβεια πόσα δεδομένα συλλέγουν αυτές οι υπηρεσίες για αυτούς και το απώτερο σκοπό χρήσης τους. Ένα τέτοιο παράδειγμα αποτελούν τα μέσα κοινωνικής δικτύωσης όπως το Facebook, που συχνά γνωρίζει περισσότερα για τους χρήστες από ότι οι ίδιοι. Υπάρχει επίσης το ζήτημα σε ποιον οι εν λόγω υπηρεσίες μοιράζονται τα δεδομένα των χρηστών τους. Όλες οι μεγάλες εταιρίες διαδικτύου έχουν την υποχρέωση να αποκαλύπτουν πληροφορίες χρηστών σε κυβερνητικούς οργανισμούς χωρίς να αποκτούν τη συγκατάθεσή τους ή να τις πωλούν σε τρίτους. (Nikhil, 2018)

1.2.2 Το Blockchain όπου καθένας είναι η αρχή πιστοποίησης

Το Blockchain είναι ένα σύστημα συνδεδεμένων κατακευματισμένων ομότιμων κόμβων (P2P network). Κάθε κόμβος συμμετέχει στη διοίκηση, όλοι οι κόμβοι επαληθεύουν νέες προσθήκες στο blockchain και είναι σε θέση να εισάγουν νέα δεδομένα στη βάση δεδομένων. Για να γίνει μια προσθήκη στο blockchain, η πλειονότητα των κόμβων πρέπει να φτάσει σε συναίνεση (consensus). Το Blockchain μπορεί να αντιμετωπίσει ένα μεγάλο αριθμό κινδύνων που θα εμφανίζονταν αν αποθηκεύουμε τα πάντα σε ένα κεντρικό κόμβο.

Αρχικά με αυτόν τον τρόπο εξαλείφεται ο κίνδυνος κάποιας βλάβης του κεντρικού κόμβου. Επίσης είναι δυσκολότερες οι επιθέσεις από κακοποιά στοιχεία καθώς δεν μπορούν να επιτεθούν σε κάποια κεντρική οντότητα, αλλά αντίθετα σε έναν τεράστιο αριθμό κόμβων-υπολογιστών. Επιπρόσθετα, με τη χρήση αλγορίθμων κρυπτογραφίας δημοσίου κλειδιού, καθιστά στην ουσία τις πληροφορίες που είναι αποθηκευμένες στην αλυσίδα αμετάβλητες.

Κάθε κόμβος στο αποκεντροποιημένο σύστημα κατέχει ένα αντίγραφο του blockchain. Με αυτόν τον τρόπο προστατεύεται η εγκυρότητα των δεδομένων που διατηρείται από την τεράστια αναπαραγωγή αντιγράφων. Κάθε κόμβος και κατ'επέκταση κάθε χρήστης έχει τα ίδια δικαιώματα. (William, 2016) (Shaan, 2017)



Εικόνα 2 Web3 Centralized vs Distributed

1.3 Βασικές αρχές και έννοιες

Σε αυτό το κεφάλαιο θα αναπτύξουμε τις βασικές αρχές και έννοιες της Blockchain τεχνολογίας. Η πρώτη αρχή που αντιπροσωπεύει την αρχιτεκτονική των ομότιμων κόμβων είναι η διαδικασία της συνέναισης (consensus), στην οποία πρέπει να καταλήγουν όλοι οι συνδεδεμένοι κόμβοι που ανήκουν σε ένα Blockchain δίκτυο. Ενώ εξίσου σημαντική είναι η δημιουργία έξυπνων συμβολαίων (smart contracts), στα οποία ορίζονται οι κανόνες με οποίους καθορίζονται όλες οι αλληλεπιδράσεις μεταξύ των κόμβων.

1.3.1 Consensus algorithms

Ο αλγόριθμος συναίνεσης (consensus) είναι ένας αλγόριθμος συνεργατικής διαδικασίας που καθορίζει τον τρόπο επίτευξης συναίνεσης μεταξύ όλων των κόμβων του Blockchain και προσδιορίζει την εγκυρότητα των εγγραφών. Τα μέλη του blockchain το χρησιμοποιούν για να διαπραγματευτούν πότε η συναλλαγή είναι έγκυρη και να διατηρούν τον συγχρονισμό του ledger¹. Κάθε κόμβος στο blockchain επαληθεύει και επιβεβαιώνει τα δεδομένα σύμφωνα με τον consensus αλγόριθμο. Μετά από επιβεβαίωση από έναν ορισμένο αριθμό κόμβων, τα έγκυρα δεδομένα μπορούν να εγγραφούν στην αλυσίδα.

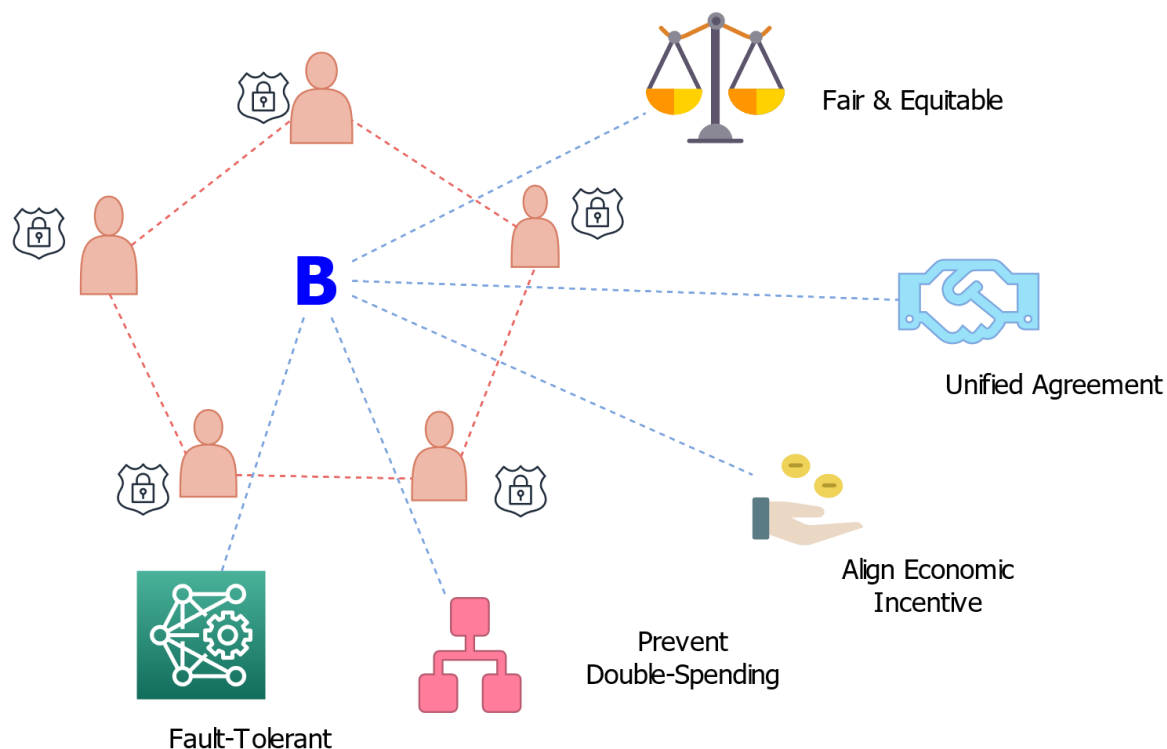
Οι αλγόριθμοι συναίνεσης έχουν σχεδιαστεί για να επιτυγχάνουν αξιοπιστία σε ένα δίκτυο που περιλαμβάνει πολλαπλούς αναξιόπιστους κόμβους. Η επίλυση αυτού του ζητήματος - γνωστό ως πρόβλημα συναίνεσης - είναι σημαντικό για συστήματα καταναμεμημένων υπολογιστών και πολλαπλών κόμβων.

Το πρόβλημα συναίνεσης σύμφωνα με τον Vincent Gramoli (Gramoli, 2017), μπορεί να οριστεί από τρεις ιδιότητες που πρέπει να επιτευχθούν, την συμφωνία, κατά την οποία δύο σωστές διαδικασίες δεν αποδέχονται διαφορετικά μπλοκ, την ισχύ, όπου το αποδεχθέν μπλοκ πρέπει να έχει προταθεί από κάποιες διεργασίες του συστήματος και τον τερματισμό, στο τέλος δηλαδή όλες οι διεργασίες πρέπει να έχουν καταλήξει στην επιλογή ενός μπλοκ.

Οι αλγόριθμοι συναίνεσης προϋποθέτουν κατά ανάγκη ότι ορισμένες διαδικασίες και συστήματα δεν θα είναι διαθέσιμα και ότι ορισμένες επικοινωνίες θα χαθούν. Ως αποτέλεσμα, για να αντιμετωπιστεί αυτή η αδυναμία οι αλγόριθμοι συναίνεσης πρέπει να είναι ανεκτικοί σε σφάλματα (fault tolerant). Συνήθως υποθέτουν, για παράδειγμα, ότι μόνο ένα τμήμα κόμβων θα ανταποκριθεί, αλλά απαιτεί μια απόκριση από αυτό το τμήμα, όπως το 51%, στο ελάχιστο.

Οι πιο συνηθισμένοι συναινετικοί αλγόριθμοι είναι οι: Proof of Work, Proof of Stake, Delegated Proof of Stake και Practical Byzantine Fault Tolerance που θα αναλύσουμε σε επόμενα κεφάλαια.

¹ Το ledger επίσης γνωστό ως shared ledger ή distributed ledger technology (DLT) είναι μια συναίνεση των αναπαραγόμενων, κοινόχρηστων και συγχρονισμένων ψηφιακών δεδομένων γεωγραφικά καταναμεμημένων σε πολλαπλές τοποθεσίες, χώρες ή ιδρύματα. Δεν υπάρχει κεντρικός διαχειριστής ή κεντρική αποθήκευση δεδομένων. (UK Government, Office for Science, 2016)



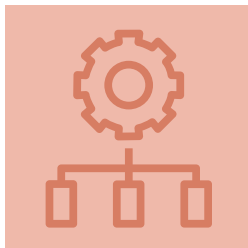
Εικόνα 2 Objectives of Consensus mechanism

1.3.2 Smart contracts

Ο όρος των έξυπνων συμβολαίων χρησιμοποιήθηκε αρχικά από τον Αμερικάνο επιστήμονα πληροφορικής και κρυπτογράφο Nick Szabo (Szabo, 1996). Χαρακτηριστικά αναφέρει το παράδειγμα της ενοικίασης ενός αυτοκινήτου με έξυπνο συμβόλαιο έτσι ώστε να αποτραπεί η κλοπή του αν δεν ικανοποιηθεί το πρωτόκολλο παράδοσης. Το ίδιο θα μπορούσε να συμβεί σε μία περίπτωση τραπεζικού δανείου για αγορά αυτοκινήτου όπου ο ιδιοκτήτης δεν μπορούσε να πραγματοποιήσει τις πληρωμές, το έξυπνο συμβόλαιο αυτομάτως θα έκανε κατάσχεση επιστρέφοντας τα κλειδιά του αυτοκινήτου στην τράπεζα. Τα έξυπνα συμβόλαια είναι μικρά αυτόνομα προγράμματα που λαμβάνουν μια συναλλαγή ως είσοδο, επεξεργάζονται και παράγουν μια νέα έξοδο. Η εκτέλεσή τους ξεκινάει αυτόματα, υπό συγκεκριμένες συνθήκες και παράγει ένα αποτέλεσμα. Αυτό πραγματοποιείται στο επίπεδο του blockchain όπου ζει η επιχειρηματική λογική και συγκεκριμένες προγραμματικές λειτουργίες που εξυπηρετούν μια περίπτωση χρήσης. Τα κυριότερα οφέλη του συμβολαίου είναι ότι το blockchain εγγυάται πως οι συμβατικοί όροι δεν μπορούν να τροποποιηθούν και είναι αδύνατη η παραβίαση τους. Με την εφαρμογή αυτών αναμένεται να μειωθεί το κόστος εκτέλεσης, επαλήθευσης, ελέγχου και αποφυγής απάτης μια σύμβασης. Τέλος, με τα έξυπνα συμβόλαια ξεπερνιέται το πρόβλημα του ηθικού κινδύνου.



Smart Contracts are written as code and committed to the blockchain. The code and conditions in the contract are publicly available on the ledger.



When an event outlined in the contract is triggered, like an expiration date or an asset's target price is reached, the code executes.



Regulators can watch contract activity on the blockchain to understand the market while still maintaining the privacy of individual actors

Εικόνα 3 Utility of smart contracts

Η χρήση έξυπνων συμβολαίων σε ένα blockchain ξεκίνησε με το Bitcoin, το οποίο προσέφερε μια περιορισμένη ψευδό-γλώσσα (scripting language). Αυτή η γλώσσα έχει «κλαδευτεί» ακόμη περισσότερο κατά την χρήση της καθώς εντοπίστηκαν ασάφειες όταν εκτελούνταν ορισμένες λειτουργίες. Το Ethereum επέκτεινε την έννοια των έξυπνων συμβολαίων με την επεξεργασία των συναλλαγών σε μια ειδικά δημιουργημένη εικονική μηχανή. Τα έξυπνα συμβόλαια γράφονται σε γλώσσα υψηλότερου επιπέδου, πιο συχνά την Solidity, τα οποία στη συνέχεια μεταγλωττίζονται σε ψηφιακό κώδικα Ethereum Virtual Machine (EVM). Η λογική του συμβολαίου και ο κώδικας διαμοιράζεται στο δίκτυο ούτως ώστε να χρησιμοποιηθεί από τους συμμετέχοντες για να επικυρώσουν και να επεξεργαστούν τις συναλλαγές. Το αποτέλεσμα των λειτουργιών που ορίζονται μέσω του συμβολαίου γράφεται αυτόματα και υπόλοιποι διατηρούν αντίγραφα.

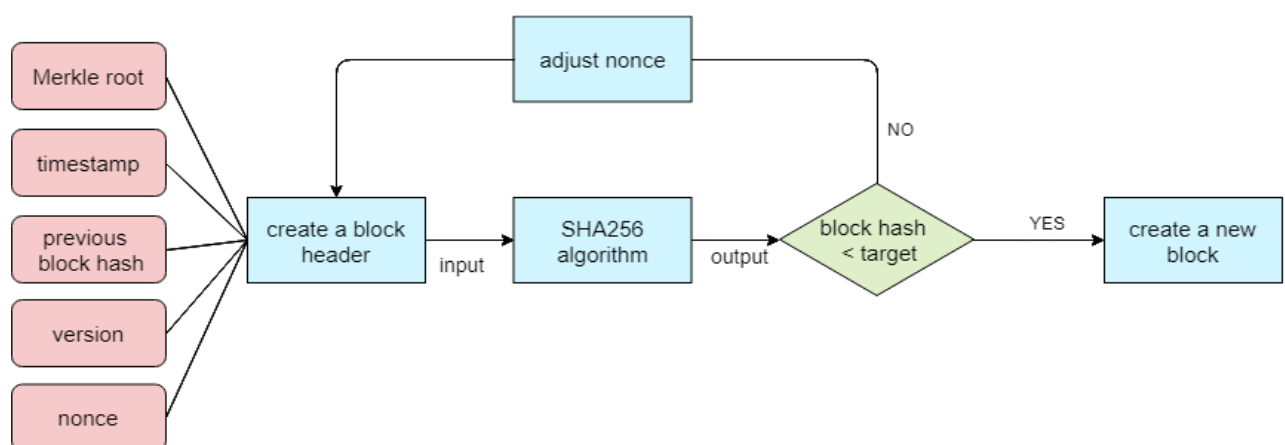
1.4 Χαρακτηριστικοί consensus algorithms

1.4.1 Proof of Work Algorithm

Το πρώτο είδος αλγόριθμου συναίνεσης που θα συζητήσουμε είναι ο αλγόριθμος Proof of Work (PoW). Ο Proof of Work αλγόριθμος στο Bitcoin και στο Ethereum χρησιμοποιείται για την επεξεργασία μπλοκ συναλλαγών και την προσθήκη τους στο blockchain. Οι κόμβοι μέσα στο δίκτυο επαληθεύουν κάθε μπλοκ πριν προστεθεί στο blockchain. Με άλλα λόγια, ο αλγόριθμος Proof of Work χρησιμοποιείται για την παραγωγή μπλοκ.

Η διαδικασία δημιουργίας σωστών αποδεικτικών στοιχείων για την προσθήκη ενός μπλοκ στο blockchain είναι γνωστή ως «mining» και οι κόμβοι που συμμετέχουν στη διαδικασία mining είναι γνωστοί ως «miners». Η πρώτη εφαρμογή ενός κατανεμημένου και διαπιστευμένου αλγόριθμου συναίνεσης είναι το Bitcoin Proof of Work (PoW). Το PoW απαιτεί από τους miners να λύσουν σύνθετα κρυπτογραφικά προβλήματα προτού να μπορέσουν να προσθέσουν ένα μπλοκ στο blockchain.

Το PoW επιλέγει έναν κόμβο για να δημιουργήσει ένα νέο μπλοκ σε κάθε γύρο συναίνεσης με ανταγωνισμό υπολογιστικής δύναμης. Στον ανταγωνισμό αυτό, οι miners χρειάζεται να λύσουν το κρυπτογραφικό πρόβλημα. Ο miner που έχει λύσει πρώτος το πρόβλημα, έχει το δικαίωμα να δημιουργήσει ένα νέο μπλοκ. Η ροή της δημιουργίας μπλοκ σε PoW παρουσιάζεται στο Εικόνα 4. Η διαδικασία εύρεσης λύσης του προβλήματος είναι δύσκολη. Οι κόμβοι πρέπει να συνεχίσουν να προσαρμόζουν την τιμή του nonce² για να πάρουν τη σωστή απάντηση, η οποία απαιτεί μεγάλη υπολογιστική δύναμη. Είναι εφικτό για ένα κακόβουλο και επιτιθέμενο κόμβο να ανατρέψει ένα μπλοκ σε μια αλυσίδα, αλλά καθώς τα έγκυρα μπλοκ στην αλυσίδα αυξάνονται, ο έγκυρος όγκος δεδομένων συσσωρεύεται και επικρατεί σε σχέση με τα κακόβουλα μπλοκ. Επομένως, η ανατροπή μιας μακράς αλυσίδας απαιτεί τεράστια υπολογιστική δύναμη. Το PoW ανήκει στα consensus πρωτόκολλα πιθανότητας γνωστά ως «Probabilistic-finality Consensus Protocols» και εγγυάται τελικά την συνέπεια. (Zhang & Lee, 2019)



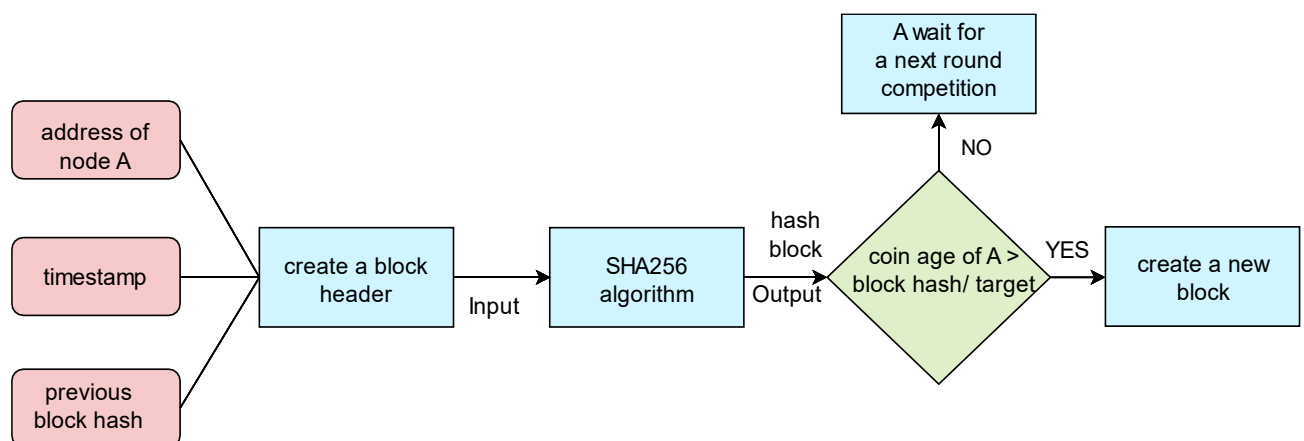
Εικόνα 4 Flow of Proof of Work

² Το nonce είναι ένας τυχαίος αριθμός που χρησιμοποιείται ως διάνυσμα αρχικοποίησης σε μια διαδικασία κρυπτογραφίας. Στο PoW χρησιμοποιείται για να μεταβάλλει την είσοδο στην συνάρτηση κατακερματισμού έτσι ώστε να επιτευχθεί η επιθυμητή τιμή. (Rouse, 2019)

1.4.2 Proof of Stake Algorithm

Ο αλγόριθμος Proof of Stake είναι ένας σχετικά διαφορετικός και νέος τρόπος να δημιουργηθούν μπλοκ μέσα σε ένα blockchain (mining), διαφορετικό από αυτό του αλγορίθμου Proof of Work. Η διασφάλιση της συνέπειας στο Proof of Stake βασίζεται στην οικονομική κατάσταση ενός κόμβου του Blockchain δικτύου. Όλοι οι κόμβοι ή αλλιώς «επικυρωτές» (validators) κατέχουν ένα σύνολο ψηφιακών κερμάτων (bitcoins) και ανάλογα με την ποσότητα κερμάτων (stake), που απαιτείται να έχουν για συγκεκριμένο χρονικό διάστημα, μπορούν να συμμετέχουν στη διαδικασία επικύρωσης. Με άλλα λόγια οι πιθανότητες εκλογής ενός κόμβου ως validator του επόμενου μπλοκ είναι ανάλογες με το ποσό πονταρίσματος που έχει διαθέσει. Έτσι, οι κόμβοι πάλι έχουν να λύσουν ένα κρυπτογραφικό πρόβλημα, αλλά το κλειδί στη λύση είναι το ποσό του στοιχήματος που έχει διαθέσει ο κόμβος και το χρονικό διάστημα που έχει παρέλθει από το ποντάρισμα.

Η διαδικασία mining σε PoS δεν είναι η προσαρμογή του nonce στην σωστή απάντηση κι έτσι δεν απαιτείται υπολογιστική δύναμη, εξοικονομώντας ενέργεια καθώς αξιοποιεί το νομισματικό κίνητρο (Stake) που διαθέτει. Η ροή του PoS φαίνεται στην εικόνα 5. Επιπλέον, ο αλγόριθμος PoS είναι απρόσβλητος σε μια επίθεση κατά 51%, λόγω των προστίμων που επιβάλλονται στους validators για οποιαδήποτε ψευδή διαδικασία επαλήθευσης. Ο επιτιθέμενος πρέπει επίσης να κρατήσει αρκετά bitcoins για πολύ καιρό πριν επιτεθεί στο δίκτυο, αυξάνοντας έτσι τη δυσκολία της επίθεσης. (Zhang & Lee, 2019)



Εικόνα 5 Flow of Proof of Stake

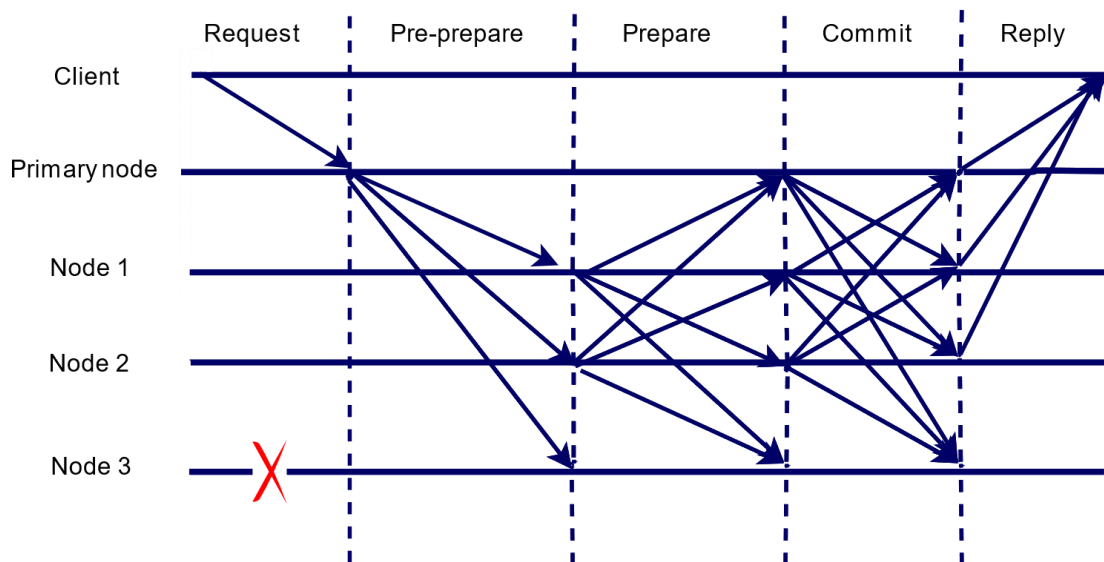
1.4.3 Practical Byzantine Fault Tolerance

Αυτός ο αλγόριθμος Practical Byzantine Fault Tolerance προτάθηκε από τους Miguel Castro και Barbara Liskov για τον μετριασμό του Byzantine Fault που συμβαίνει λόγω μιας αποτυχίας συναίνεσης που οδηγεί στο Byzantine Generals Problem (BGP). Το γενικό πρόβλημα των Blockchain δικτύων είναι η επίτευξη συμφωνίας μέσω μη αξιόπιστων κόμβων. Στο σενάριο αυτό ένας εισβολέας μπορεί να επωφεληθεί, να χειριστεί τους επλεκόμενους κόμβους και να επικυρώσει μια ψευδή κακόβουλη συναλλαγή.

Το επίκεντρο του PBFT είναι να παράσχει μια πρακτική αναπαράσταση της Byzantine State μηχανής για την ανοχή του Byzantine Fault και μιας ψηφοφορίας με αντίγραφα των συλλαγών.

Αυτός ο αλγόριθμος βελτιστοποιείται ώστε να λειτουργεί σε ασύγχρονο σύστημα, να είναι υψηλής απόδοσης και να απαιτεί χαμηλό κόστος. Η απόφαση συναίνεσης επιτυγχάνεται μετά από μια σειρά φάσεων. Η κύρια λειτουργία είναι η επιλογή ενός κόμβου ως πρωτεύον και οι υπόλοιποι αναλαμβάνουν να δημιουργούν αντίγραφα ασφαλείας των συναλλαγών. Ο αλγόριθμος PBFT επεξεργάζεται τις αιτήσεις συναλλαγών με υψηλή ταχύτητα, αλλά απαιτεί $3n+1$ αντίγραφα των συναλλαγών για να αντιμετωπίσει n αποτυχημένους κόμβους. (Baliga, 2017) Επιπλέον, η ταυτότητα του συστήματος είναι πιθανόν να διακυβεύεται εξαιτίας του τρόπου με τον οποίο σχεδιάστηκε ο αλγόριθμος. Είναι επίσης δύσκολο να χρησιμοποιηθεί αυτός ο αλγόριθμος στο δημόσιο περιβάλλον, καθώς είναι υποχρεωτικός ο προσδιορισμός του πλήθους των κόμβων προτού αρχίσει η λειτουργία του δικτύου και εκτέλεσης του αλγορίθμου. (Alsunaidi & Alhaidari, 2019)

Ο PBFT αλγόριθμος περιέχει συγκεκριμένα πέντε φάσεις request, pre-prepare, prepare, commit και reply. Στη εικόνα 6 περιγράφεται ο τρόπος λειτουργίας του PBFT. Στην πρώτη φάση ο πελάτης στέλνει την συναλλαγή στον πρωτεύον κόμβο, ο οποίος επιβεβαιώνει χρονολογικά το αίτημα αυτό και στη συνέχεια προωθεί το μήνυμα στους άλλους τρεις κόμβους. Για τη συμμετοχή του αιτήματος στα στάδια αυτά οι υπόλοιποι κόμβοι πρέπει να συγκεντρώσουν την αποδοχή των ψήφων των $2/3$ του υπόλοιπου δικτύου, ενώ ο πρωτεύον κόμβος συντονίζει τις ενέργειες της διαδικασίας. Στην περίπτωση που ο τρίτος κόμβος συντριβεί, δεν δημιουργείται πρόβλημα καθώς τα $2/3$ του δικτύου συνεχίζουν να λειτουργούν και το μήνυμα περνάει από τις πέντε φάσεις για να επιτευχθεί συναίνεση μεταξύ των υπόλοιπων κόμβων. Τελικά, αυτοί οι κόμβοι απαντούν στον πελάτη για να ολοκληρωθεί ένας γύρος της consensus διαδικασίας. Το PBFT εγγυάται ότι οι κόμβοι διατηρούν μια κοινή κατάσταση-απόφαση και αναλαμβάνουν μια συγκεκριμένη συμπεριφορά σε κάθε γύρο της συμφωνίας. Το PBFT επιτυγχάνει το στόχο της ισχυρής συνέπειας, έτσι θεωρείται ως ένα absolute-finality consensus πρωτόκολλο. (Zhang & Lee, 2019)



Εικόνα 6 Process of PBFT

1.4.4 Άλλοι αλγόριθμοι

Αναλύσαμε τους τρεις κυριότερους consensus αλγόριθμους που αναπτύχθηκαν για την επίτευξη συμφωνίας σε κατανεμημένα συστήματα κόμβων. Από την εμφάνιση του Bitcoin μέχρι σήμερα, υπάρχουν περισσότεροι από 30 αλγόριθμοι συναίνεσης, οι περισσότεροι από τους οποίους βασίζονται στους παραπάνω τρεις αλγόριθμους συναίνεσης. Ενδεικτικά αναφέρουμε τους Ripple, Proof of Elapsed Time, Simplified Byzantine Fault Tolerance, Delegated Byzantine Fault Tolerance, Delegated Proof-of-Stake, Leased Proof-Of-Stake, Proof-of-Activity, Proof-of-Importance, Proof-of-Burn.

Η διαδικασία συναίνεσης στο Ripple εκτελείται με την επικύρωση κόμβων, κάθε ένα από τα οποία κατέχει μια λίστα με αξιόπιστους κόμβους, που ονομάζεται UNL (Unique Node List). Κάθε κόμβος δημοσιοποιεί τις υπό έγκριση συναλλαγές στους υπόλοιπους κόμβους της UNL, οι οποίες συναλλαγές συλλέγονται σε μία δομή δεδομένων (candidate set). Οι κόμβοι που ανήκουν στο UNL μπορούν να ψηφίσουν τις συναλλαγές που υποστηρίζουν. Όταν η συναλλαγή παίρνει περισσότερο από το 50% των ψήφων, αυτή η συναλλαγή θα επαναληφθεί στον επόμενο γύρο. Η ομοφωνία επιτυγχάνεται σε πολλαπλούς γύρους ψηφοφορίας, στους οποίους για να θεωρηθούν έγκυρες οι συναλλαγές πρέπει να συγκεντρώσουν το 80% των ψήφων αποδοχής σε κάθε UNL. Τελικά οι συναλλαγές με ποσοστό άνω του 80% των ψήφων θα καταγραφούν στο ledger. (Zhang & Lee, 2019)

Το Proof of Elapsed Time αλγόριθμος χρησιμοποιεί το σύστημα Software Guard Extensions για να γίνεται δίκαια η επιλογή των μπλοκ στο ledger. Στον αλγόριθμο αυτό καταργείται η ανάγκη του mining και αντικαθιστάται από ένα τυχαίο σύστημα χρονοδιακόπτη για τους συμμετέχοντες στο δίκτυο, που παρέχεται από την επέκταση λογισμικού (SGX) της Intel. Έτσι όλοι οι συμμετέχοντες του δικτύου γίνονται ηγέτες και παράγουν νέα μπλοκ για συγκεκριμένο χρονικό διάστημα που καθορίζεται από το χρονόμετρο. (Anwar, 2018)

Το Simplified Byzantine Fault Tolerance χρησιμοποιεί μια γεννήτρια παραγωγής μπλοκ που συλλέγει όλες τις συναλλαγές, τις ταξινομεί σε ένα μπλοκ και τις επικυρώνει όλες μαζί, σύμφωνα με ορισμένους κανόνες. Μόλις ολοκληρωθεί η δημιουργία του μπλοκ προστίθεται η υπογραφή της επικύρωσής τους. Έτσι κάθε μπλοκ περιέχει συναλλαγές με την υπογραφή τους. Για αυτό το λόγο αν κάποιο μπλοκ χάσει μια υπογραφή συναλλαγών, τότε θα απορριφθεί. (Anwar, 2018)

Το Delegated Byzantine Fault Tolerance είναι παρόμοιο με το DPoS, καθώς κάθε χρήστης του δικτύου ψηφίζει και διορίζει έναν αντιπρόσωπο που εκπροσωπεί τα συμφέροντά του. Οι εκλεγμένοι αντιπρόσωποι ψηφίζουν ποια μπλοκ είναι έγκυρα και ποια κακόβουλα. Όταν ένα μπλοκ αποκτήσει το 66% των ψήφων, το μπλοκ υποβάλλεται σε επεξεργασία και οι συναλλαγές καταγράφονται στο ledger. Διαφορετικά απορρίπτεται και ο ίδιος κύκλος επαναλαμβάνεται.

Ο Delegated Proof of Stake είναι μια παραλλαγή του τυπικού αλγορίθμου Proof of Stake. Το ζήτημα της συμφωνίας αντιμετωπίζεται με ένα δημοκρατικό τρόπο και όχι με την χρηματική υπεροχή. Κάθε κόμβος μπορεί να πάρει μέρος στον ανταγωνισμό. Οι κόμβοι εδώ επικαλούνται αντιπρόσωποι (delegates) αντί για «miners». Τέλος, το σύστημα αυτό σχεδιάστηκε για να εξασφαλίσει όλα τα επίπεδα προστασίας από προβλήματα ρυθμίσεων. (Anwar, 2018)

Το Leased Proof-Of-Stake σχεδιάστηκε για να αντιμετωπίσει τους περιορισμούς που έθετε ο αρχικός αλγόριθμος PoS, κατά τον οποίο μόνο οι κόμβοι με μεγάλα κεφάλαια μπορούσαν να

συμμετέχουν στο ποντάρισμα. Με το νέο αλγόριθμο μπορούν πλέον και οι χαμηλοί οικονομικά κόμβοι μπορούν να ποντάρουν και να επωφεληθούν από το στοίχημα, καθώς μισθώνονται κεφάλαια των πλουσιότερων κόμβων, οι οποίοι λαμβάνουν αναλογικά μέρος των τελών που εισπράττονται από τα blocks. (Anwar, 2018)

Ο Proof of Activity αλγόριθμος είναι ένας συνδυασμός αλγορίθμων PoW και PoS. Παρέχει ένα καλό επίπεδο ασφάλειας, χαμηλή επιβάρυνση στο δίκτυο και δεν απαιτεί μεγάλο χώρο αποθήκευσης. Αυτός ο αλγόριθμος συγχρονίζει τις συναλλαγές με τρόπο αρκετά σαφή και υψηλό επίπεδο ασφάλειας. Είναι δύσκολο για τον επιτιθέμενο να μονοπωλήσει τη διαδικασία δημιουργίας μπλοκ επειδή αυτό απαιτεί ένα μεγάλο μέρος των συνολικών νομισμάτων που έχουν δημιουργηθεί. (Alsunaidi & Alhaidari, 2019)

Το Proof of Importance καθορίζει ποιοι κόμβοι είναι κατάλληλοι να προσθέσουν ένα μπλοκ στο blockchain. Αυτός ο αλγόριθμος βασίζεται στην ανάλυση του τρόπου συναλλαγής για τη συγκέντρωση των κόμβων. Με άλλα λόγια, οι κόμβοι εκλέγονται με βάση το πλήθος των συναλλαγών που έχουν ολοκληρώσει ή τη φήμη του κόμβου και άλλες παραμέτρους. Χρησιμοποιώντας αυτή τη μέθοδο, θα δοθεί προτεραιότητα στους πιο σημαντικούς κόμβους με βάση την αξιολόγηση αυτών των κόμβων. (Alsunaidi & Alhaidari, 2019)

Ο αλγόριθμος Proof of Burn (PoB) χρησιμοποιεί τους miners που στέλνουν τα bitcoin τους σε μια απροσδιόριστη διεύθυνσή, με σκοπό να «κάψουν» το bitcoin για πάντα. Αυτό πρακτικά σημαίνει πως τα νομίσματα αυτά δεν μπορούν πλέον να χρησιμοποιηθούν από κανέναν άλλον, ενώ ο κάθε κόμβος μπορεί να δημιουργήσει ένα μπλοκ ανάλογα με το πόσα νομίσματα έχει κάψει. Επιπλέον οι κόμβοι ανάλογα με το ποσό των νομισμάτων που έχουν θυσιάσει στην διαδικασία του PoB λαμβάνουν και τις αντίστοιχες αμοιβές πολύ αργότερα σε PoB coins. Ολόκληρη η ιδέα πίσω από τον PoB αλγόριθμο στηρίζεται στο ότι ενθαρρύνοντας τους κόμβους να κάψουν όλο και περισσότερα νομίσματα, επιδιώκει να ενισχύσει την σταθερότητα και την αποκέντρωση δημιουργώντας ένα ιδανικά διανεμημένο δίκτυο συναλλαγών. (CoinBundle Team, 2018)

1.4.5 Σύγκριση των consensus αλγορίθμων

Μερικοί από τους προτεινόμενους αλγόριθμους συναίνεσης όπως PoI, DBFT, SBFT και PBFT πρέπει να επαληθεύσουν την ταυτότητα των κόμβων που θα συμμετέχουν στη διαδικασία επικύρωσης μπλοκ. Αυτοί οι αλγόριθμοι είναι κατάλληλοι για τα ιδιωτικά ή κοινοπραξιακά δίκτυα Blockchain, λόγω της δυσκολίας εντοπισμού των κόμβων σε δημόσια δίκτυα. Αλγόριθμοι όπως PoW, PoS, DPoS και PoA είναι πιο κατάλληλοι για δημόσια δίκτυα Blockchain, όπου οι κόμβοι μπορούν να ενταχθούν ελεύθερα στο δίκτυο.

Ο αλγόριθμος που καταναλώνει περισσότερο ενέργεια είναι ο PoW. Όπου η εκλογή ενός miner σε αυτόν τον αλγόριθμο εξαρτάται από την ταχύτητα επίλυσης του κρυπτογραφικού προβλήματος, το οποίο απαιτεί την εκτέλεση διαδοχικών υπολογισμών για να επιτευχθεί η τιμή στόχου κατακερματισμού, με αποτέλεσμα την κατανάλωση μιας μεγάλης ποσότητας ηλεκτρικής ενέργειας. Ωστόσο, το σύνολο των υπολογισμών είναι μικρότερο στις PoS, DPoS και PoA, πράγμα που τους καθιστά λιγότερο καταναλωτικούς από το PoW. Η ηλεκτρική ισχύς διατηρείται σημαντικά σε αλγόριθμους που δεν εκτελούν mining μέθοδο όπως PoI, Ripple και PBFT. (Alsunaidi & Alhaidari, 2019)

Ένα ακόμη μέτρο σύγκρισης για τους αλγόριθμους συναίνεσης είναι το Verification speed, που υποδεικνύει τον απαιτούμενο χρόνο σε δευτερόλεπτα για να ολοκληρωθεί μια διαδικασία επικύρωσης συναλλαγής. Κυρίως, ο τύπος δικτύου Blockchain και η ταχύτητα της υπολογιστικής μονάδας θα επηρεάσουν αυτόν τον παράγοντα. Στον πίνακα 1 αναφέρεται το όριο της ταχύτητας επικύρωσης για κάθε αλγόριθμο.

Σε συνάρτηση με την απόδοση (throughput), δηλαδή με τον αριθμό των συναλλαγών που υποβάλλονται σε επεξεργασία το δευτερόλεπτο, ο πίνακας 1 μας δείχνει ότι ο ρυθμός απόδοσης των ιδιωτικών δικτύων είναι καλύτερος από αυτό των δημόσιων δικτύων.

Η δυνατότητα κλιμάκωσης (scalability) είναι μια από τις προκλήσεις στο Blockchain δίκτυο. Εντοπίζει τον αριθμό των συναλλαγών που μπορούν να επεξεργαστούν ταυτόχρονα και το μέγεθος του μπλοκ που μπορεί να δημιουργηθεί από ένα κόμβο. Οι περισσότεροι αλγόριθμοι παρατηρούμε ότι έχουν ισχυρή κλιμακωσιμότητα εκτός από τον PBFT. (Zhang & Lee, 2019)

Ένας άλλος παράγοντας είναι η επέκταση, που καθορίζει την έκταση στην οποία το δίκτυο μπορεί να επεκταθεί αυξάνοντας τον αριθμό των κόμβων. Το PoW και το PoS θεωρούνται ως μη επεκτάσιμοι εξαιτίας του τρόπου με τον οποίο επιλέγεται ο miner με την πάροδο του χρόνου. Επίσης, οι αλγόριθμοι που χρησιμοποιούνται στο ιδιωτικό δίκτυο δεν μπορούν να επεκταθούν λόγω της ανάγκης ταυτοποίησης των κόμβων προτού ξεκινήσει η εργασία στο δίκτυο. Ωστόσο, η αύξηση του μεγέθους του δικτύου είναι αναπόφευκτο γεγονός. Επομένως, πρέπει να εργαστούμε για την παροχή αλγορίθμων που παρέχουν την καλύτερη απόδοση για διαφορετικά σενάρια. (Alsunaidi & Alhaidari, 2019)

Όλοι οι προτεινόμενοι αλγόριθμοι έχουν εντοπίσει ένα ορισμένο ποσοστό ικανότητα αντοχής σφάλματος του δικτύου που μπορεί να ανήκει σε έναν αντίπαλο (fault tolerance) για να επιτευχθεί στην ασφάλεια του δικτύου ή μια απώλεια ενός από τους εμπλεκόμενους κόμβους. Το υψηλότερο ποσοστό ήταν 50%, ενώ η χειρότερη περίπτωση που διαπιστώθηκε ως ποσοστό ήταν 20%. Ωστόσο, αυτές οι αναλογίες δεν είναι αξιόπιστες σε όλες τις περιπτώσεις. (Xiao, et al., 2019)

Όλα τα παραπάνω φαίνονται στον παρακάτω πίνακα (Πίνακας 1).

Πίνακας 1. Comparison of Blockchain Consensus Algorithms

	Node- Entity management	Fault Tolerance	Power consumption	Extensible	Scalability	Verification speed	TPS*	Applications
PoW	Public	50%	Large	No	Strong	<100s	<100	Cryptocurrency Smart Contracts
PoS	Public	50%	Less	No	Strong	>100s	<1000	Cryptocurrency Smart Contracts
PoET	Public	Depend of finalization	N/A	No	Strong	N/A	N/A	Cryptocurrency BitShares
DPoS	Public	50%	Less	Yes	Strong	>100s	<1000	Cryptocurrency BitShares
LPoS	Public	50%	N/A	No	N/A	N/A	N/A	Cryptocurrency
PoA	Public	Depend of finalization	Less	Yes	Strong	N/A	N/A	Cryptocurrency
PoI	Consortium	50%	Negligible	Yes	Strong	N/A	N/A	Real-world like IoT
PoB	Public	N/A	Less	N/A	N/A	N/A	N/A	Cryptocurrency
Ripple	N/A	20%	Negligible	N/A	Strong	N/A	>1500	N/A
PBFT	Private	33%	Negligible	No	Weak	>10s	<2000	Smart Contracts
DBFT	Private	33%	Negligible	N/A	N/A	N/A	N/A	Smart Contracts
SBFT	Private	N/A	N/A	N/A	N/A	N/A	N/A	Smart Contracts

*N/A: Not Available, *TPS: Throughput (Transaction per Second)

1.5 Θεματικές περιοχές εφαρμογών Blockchain

Το Bitcoin ξεκίνησε και μέχρι σήμερα χρησιμοποιεί την Blockchain τεχνολογία αποκλειστικά και μόνο για χρηματοοικονομικές συναλλαγές, αποδεικνύοντας ότι το δίκτυο τεχνολογίας blockchain περιγράφει μια στρατηγική όσον αφορά την ιδιοκτησία ψηφιακών στοιχείων και τη διαχείρισή τους. Μπορεί δηλαδή να παρέχει βελτιωμένη ακρίβεια και πληροφόρηση στο οικοσύστημα χρηματοοικονομικών υπηρεσιών μιας τράπεζας. Η εξέλιξη όμως της τεχνολογίας του Blockchain επιτρέπει την ανάπτυξη διαφόρων εφαρμογών και σε άλλους τομείς.

1.5.1 Κρυπτονομίσματα

Τα κρυπτονομίσματα θεωρούνται ως μέσο συναλλαγής που βασίζονται όμως στην κρυπτογραφία για να εξασφαλίσουν τη ιδιοκτησία και τη δημιουργία νέων μονάδων νομίσματος. Ανήκουν στην κατηγορία των εναλλακτικών νομισμάτων. Η κεντρική ευρωπαϊκή τράπεζα (ECB) έχει θεωρήσει ως κρυπτονομίσματα το σύνολο εικονικών νομισμάτων, τα οποία είναι μια μορφή μη ελεγχόμενων ψηφιακών χρημάτων, εκδίδονται και ελέγχονται από τους προγραμματιστές και χρησιμοποιούνται και επικυρώνονται από τα μέλη μιας συγκεκριμένης ψηφιακής κοινότητας δηλαδή ενός Blockchain δικτύου. (Houben & Snyers, 2018)

Σήμερα υπάρχουν περισσότερα από 300 διαφορετικά κρυπτονομίσματα, όπως Bitcoin, Litecoin, Ethereum, Ripple, MaidSafe, Monero, HayekGold και άλλα. Το πρώτο γνωστό κρυπτονόμισμα είναι το Bitcoin, που όρισε ο Satoshi Nakamoto το 2008 (Nakamoto, n.d.). Με την χρήση του Bitcoin έχουμε τη δυνατότητα συναλλαγών χωρίς υποβολή προσωπικών δεδομένων, την διεκπεραίωσή τους από οποιονδήποτε και οπουδήποτε με πολύ μικρό κόστος αποστολής. Επίσης παρέχεται η δυνατότητα συμμετοχής όλων που ανήκουν στο δίκτυο στην έκδοση νομισμάτων και περιορισμός και γνωστοποίηση του χρηματικού αποθέματος. Όμως μειονεκτήματα του Bitcoin όπως η άγνωστη ταυτότητα του δημιουργού ενός κρυπτονομίσματος ή το ιστορικό χρήσης του νομίσματος για παράνομες αγορές, οδήγησαν στη δημιουργία άλλων κρυπτονομισμάτων. (Vigna & Casey, 2016)

Το Ether είναι το πιο διαδεδομένο κρυπτονόμισμα τον τελευταίο καιρό και σίγουρα ότι πιο ενδιαφέρον έχουμε δει από τη δημιουργία του bitcoin και μετά. Πρόκειται περί της προγραμματιστικής πλατφόρμας Ethereum, η οποία συμπεριλαμβάνει μέσα της και το κρυπτονόμισμα Ether.

Το Litecoin είναι ένα από τα πρώτα κρυπτονομίσματα που κατάφεραν να κερδίσουν μεγάλο κοινό και επενδυτές, χάρη στις πολύ πιο γρήγορες συναλλαγές (2 λεπτά αντί για 10). Έχει συχνά αναφερθεί ως το “ασήμι” σε σχέση με το bitcoin που συχνά παρομοιάζεται με τον χρυσό.

Το Ripple εκτός από κρυπτονόμισμα είναι και μία ολοκληρωμένη πλατφόρμα συναλλαγών που έχει και αυτή ως βάση την τεχνολογία blockchain και το αποκεντρωμένο μοντέλο με την διαφορά ότι ο χρήστης έχει τη δυνατότητα να επιλέξει σε τι μορφή θα είναι τα κεφάλαια που θα διαχειρίζεται, έχοντας να επιλέξει ανάμεσα σε Ευρώ, Δολάρια, χρυσό, bitcoin, Ripple και ανάμεσα σε άλλα.

Το MaidSafe είναι μια προσπάθεια δημιουργίας ενός οικοσυστήματος όπου οι χρήστες έχουν τη δυνατότητα να διαθέσουν υπολογιστικούς πόρους, όπως αποθηκευτικό χώρο, υπολογιστική δύναμη, ευρηζωνηκότητα (bandwidth), τους οποίους χρησιμοποιούν ως αντάλλαγμα πληρωμής από άλλους χρήστες, οι οποίοι χρειάζονται αυτούς τους πόρους.

Το Monero έχει ως πρώτη προτεραιότητα την ιδιωτικότητα και την ανωνυμία. Χρησιμοποιώντας μια πολύ εξειδικευμένη ιδιότητα της κρυπτογραφίας (ring signatures), που καθιστά τις συναλλαγές σχεδόν απίθανο να ανιχνευθούν. Το HayekGold είναι ένα κρυπτονόμισμα που έχει ως βάση τον χρυσό και κάθε μονάδα αντιστοιχεί στην αξία ενός γραμμαρίου χρυσού, το οποίο είναι αποθηκευμένο σε χώρο της εταιρίας που εκδίδει νόμισμα μέσω της πλατφόρμας Counterparty. (Houben & Snyers, 2018)

1.5.2 Υγεία

Στον τομέα της υγειονομικής περίθαλψης, η χρήση τεχνολογίας blockchain θα μπορούσε να επιτρέψει στα νοσοκομεία, τους πληρωτές και άλλους φορείς να μοιραστούν την πρόσβαση στα δίκτυά τους χωρίς να διακυβεύουν την ασφάλεια και την ακεραιότητα των δεδομένων. Ο διαμοιρασμός των δεδομένων θα σήμαινε υψηλότερη πιθανότητα ακριβούς διάγνωσης, αποτελεσματικών θεραπειών και αυξημένη ικανότητα στα συστήματα υγείας να προσφέρουν οικονομική και αποδοτική φροντίδα. Με άλλα λόγια η διαλειτουργικότητα στο παραδοσιακό σύστημα καταχώρησης ιατρικών δεδομένων εμποδίζεται λόγω της κεντρικής αποθήκευσης των δεδομένων στα ιατρικά κέντρα. Τα αρχεία που είναι διασκορπισμένα σε διάφορα νοσοκομεία μπορεί να χαθούν και τα δεδομένα που περιέχονται δεν μπορούν να προσεγγιστούν από τον ασθενή. Επομένως, η δημιουργία μιας πλατφόρμας Blockchain θα έδινε την δυνατότητα στους ασθενείς να έχουν πρόσβαση στο ιατρικό τους ιστορικό από οπουδήποτε παγκοσμίως, διευκολύνοντας την πρόσβαση στα ιατρικά δεδομένα και παροχή καλύτερων υπηρεσιών. Παράδειγματα Blockchain εφαρμογών στον τομέα της υγείας είναι το MedRec, το Patientory, το Medibloc, το Modum.

Το MedRec αποτελεί ασφαλή και εύκολη πρόσβαση σε διάσπαρτα ιατρικά δεδομένα, για την παροχή του πλήρους ηλεκτρονικού φακέλου Υγείας στους ασθενείς. Εύκολη διαχείριση των δεδομένων από τους ίδιους τους ασθενείς. Ενίσχυση της ιατρικής έρευνας μέσω των αμοιβών “mining” με ανώνυμα ιατρικά δεδομένα. (Ekblaw, et al., 2016)

Το Patientory επίσης προσφέρει ασφαλή και εύκολη πρόσβαση στο πλήρες ιατρικό φάκελο του ασθενούς και μηχανισμούς για την εύκολη συνδιαλλαγή τους με το ιατρικό σύστημα και τους γιατρούς, καθώς και μηχανισμούς για την προσφορά πληροφοριών από ασθενείς σε ερευνητές. Διαφέρει με τη MedRec ως προς την ασφάλεια λόγω του διαφορετικού τρόπου αποθήκευσης της πληροφορίας. (Patientory Inc, 2018)

Το Medibloc πρόκειται για μια πλατφόρμα με περισσότερες δυνατότητες. Προσφέρει τις υπηρεσίες των παραπάνω εφαρμογών, ωστόσο αποτελεί ένα περιβάλλον στο οποίο μπορούν να αναπτυχθούν πολλές διαφορετικές εφαρμογές ιατρικού ενδιαφέροντος. (Medibloc Team, 2019)

Η Modum δραστηριοποιείται σε έναν διαφορετικό κλάδο του τομέα της υγείας, προσφέροντας υπηρεσίες για εξοικονόμηση και ασφάλεια στον εφοδιασμό φαρμάκων, καθόλη την αλυσίδα εφοδιασμού από την φαρμακοβιομηχανία μέχρι το φαρμακείο και τον καταναλωτή. (Modum Team, 2017)

1.5.3 Εφοδιαστική αλυσίδα

Ο αμετάβλητος χαρακτήρας της τεχνολογίας blockchain την καθιστά κατάλληλη για σκοπούς όπως η παρακολούθηση των προϊόντων καθώς αλλάζουν κατοχή στην εφοδιαστική αλυσίδα. Καταχωρήσεις στην βάση της 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.

Οι σημερινοί γνωστοί τρόποι διαχείρισης των προϊόντων είναι η χρήση barcode και μια αναπτυσσόμενη τεχνολογία ραδιοσυχνικής αναγνώρισης ή ταυτοποίησης μέσω ραδιοσυχνοτήτων (Radio Frequency Identification - RFID). Η τελευταία αναφέρεται σε μια τεχνολογία αυτόματης αναγνώρισης προϊόντων, μέσω της οποίας τα ψηφιακά δεδομένα που έχουν καταγραφεί από τον αναγνώστη, μέσω ραδιοκυμάτων, κωδικοποιούνται σε RFID ετικέτες. Το σύστημα αυτό καλύπτει την ανάγκη ταχύτερης και πιο αυτοματοποιημένης εισαγωγής στοιχείων από αυτή που μπορούν να προσφέρουν τα barcodes. Όμως, το υψηλό κόστος (κόστος απόκτησης ετικέτας, τοποθέτησης ετικέτας στο προϊόν, κόστος αγοράς και εγκατάστασης αναγνώστών, κόστος αναβάθμισης υπάρχοντος εξοπλισμού και κόστος εκπαίδευσης προσωπικού), η δυσπιστία ως προς τη διασφάλιση του απορρήτου του περιεχομένου των ηλεκτρονικών ετικετών, θέματα ακρίβειας που ανακύπτουν από δυσμενείς περιβαλλοντικούς παράγοντες ή παρεμβολή ηλεκτρολογικού και βιομηχανικού εξοπλισμού, πιθανά προβλήματα συμβατότητας αναγνώρισης αντικειμένων μεταξύ διαφορετικών χωρών, λόγω απουσίας ενός παγκόσμιου και αποδεκτού φάσματος συχνοτήτων εμποδίζουν την χρήση των RFID ετικετών. (Δανιά, 2015)

Το αποκεντρωμένο Blockchain εξαλείφει τα παραπάνω πλεονεκτήματα μειώνοντας κυριολεκτικά το κόστος και την απόσταση των προϊόντων. Επιπλέον, οι 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, κατά τη διαδικασία της μεταφοράς τους στην παγκόσμια αγορά. Σύμφωνα με έρευνα της Deloitte και του σωματείου εταιρειών μηχανογράφησης κι εφοδιαστικής αλυσίδας στις Η.Π.Α το 2016, παρόμοιοι αισθητήρες χρησιμοποιούνταν ήδη σχεδόν από τις μισές εταιρείες του χώρου ενώ η υιοθέτησή τους προβλέπεται να είναι σχεδόν καθολική τα επόμενα χρόνια. 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. (Δρόσος, 2019)

1.5.4 Διακίνηση εγγράφων

Με παρόμοιο τρόπο, που η αλυσίδα εφοδιασμού γίνεται όλο και πιο συνηθισμένη, η διαδικασία της εξασφάλισης και της διαχείρισης των εγγράφων γίνεται όλο και πιο δημοφιλής στον χώρο του blockchain. Η ψηφιοποίηση των εγγράφων είναι ζωτικής σημασίας στη σύγχρονη εποχή, με την αναποτελεσματικότητα του τυπωμένου χαρτιού να είναι αισθητή σε πολλούς διαφορετικούς τομείς.

Η ίδια η φύση του blockchain διευκολύνει τη διαθεσιμότητα και τη διανομή των εγγράφων, καθώς παρακολουθεί τη διαδικασία ελέγχου των αλλαγών σε αυτές, επιτρέποντας σε κάθε συμμετέχοντα στο δίκτυο να λαμβάνει πάντοτε μια αποδεκτή και αναθεωρημένη έκδοση των εγγράφων που τον ενδιαφέρουν. Μόλις ένα έγγραφο καταχωρηθεί στο σύστημα είναι άμεσα διαθέσιμο σε όλα τα ενδιαφερόμενα μέρη του δικτύου και αυτομάτως φροντίζουν να διατηρήσουν ένα ενημερωμένο το ledger δημιουργώντας αντίγραφα στο blockchain.

Αυτό είναι αναμφίβολα πολύ πιο αποτελεσματικό από τη φυσική διανομή των εγγράφων με ταχυδρομική αλληλογραφία ή ψηφιακά με συμβατικό τρόπο του κεντρικού συστήματος, όπου ο κεντρικός διακομιστής είναι συνήθως υπεύθυνος για τη συνολική διαχείριση των εγγράφων. Δηλαδή αναλαμβάνει το πρόσθετο καθήκον της αποστολής ενημερωτικών ειδοποιήσεων σε κάθε πελάτη και από την άλλη μεριά, οι πελάτες προκαλούν κορεσμό του διακομιστή με αιτήματα για συνεχή ενημέρωση. Με το νέο σύστημα εξαλείφονται όλες αυτές οι ανταλλαγές μηνυμάτων αφού δεν είναι πλέον αναγκαίες.

Επιπλέον, η χρήση του blockchain επιτρέπει στο σύστημα να μην εξαρτάται μόνο από μια μεγάλη βάση δεδομένων που αποθηκεύει όλες τις πληροφορίες των συναλλαγών, έχοντας μεγάλο φόρτο εργασίας και καταναλώνοντας ένα μεγάλο ποσό χώρο εντός του εξοπλισμού δικτύου, γεγονός που μεταφράζεται σε πιθανή μείωση του κόστους απόκτησης και συντήρησης διακομιστών βάσεων δεδομένων σε αντίθεση με ένα παραδοσιακό κεντρικό σύστημα διαχείρισης εγγράφων. (Solarte-Rivera, et al., 2018)

1.5.5 Δημόσια διοίκηση και ασφάλεια

Καθώς η τεχνολογία blockchain αποτελεί ουσιαστικά έναν νέο τρόπο καταχώρησης και αποθήκευσης πληροφοριών με τέτοιο τρόπο ώστε να δημιουργείται μία αλληλένδετη αλυσίδα δεδομένων, αποτρέποντας διπλές εγγραφές, κακόπιστες καταχωρήσεις κ.ά, η πιο προφανής εφαρμογή της είναι η τήρηση μητρώων, όπως το κτηματολόγιο, το ληξιαρχείο, μητρώο εταιρειών, φορολογικό μητρώο, μητρώο δικαιωμάτων διανοητικής ιδιοκτησίας κλπ. Επιπλέον, η τεχνολογία θα μπορούσε να εφαρμοστεί σε λογιστικές καταχωρήσεις εταιρειών, καθώς μειώνει σημαντικά την πιθανότητα σφαλμάτων και εξασφαλίζει, τουλάχιστον σε βαθμό μεγαλύτερο από τις σημερινές πρακτικές, την ακεραιότητα των εγγράφων. Η τροποποίηση των εγγράφων από την στιγμή που θα καταχωρηθούν στην βάση δεδομένων blockchain θα είναι εξαιρετικά δύσκολη, αν όχι αδύνατη, ακόμη και από εκείνον που τηρεί το μητρώο /αρχείο.

Σε όλες τις παραπάνω περιπτώσεις, η καταχώριση δεδομένων μπορεί να συνδυαστεί με επιπρόσθετες λειτουργικές δυνατότητες οι οποίες ενσωματώνονται στην εκάστοτε πλατφόρμα. Για παράδειγμα, σε μία πειραματική εφαρμογή της τεχνολογίας από το χρηματιστήριο του NASDAQ το 2016, καταχωρήθηκε η κυριότητα κινητών αξιών των χρηστών, όπως τηρείται

από την κεντρική αρχή (CSD), και στη συνέχεια αποδόθηκαν δικαιώματα ψήφου μέσω tokens³, ώστε οι χρήστες να μπορούν να «ξοδεύουν» tokens και να ψηφίζουν στις συνελεύσεις εφόσον ήταν και φορείς του αντίστοιχου δικαιώματος ψήφου.

Έτσι θα μπορούσε να ψηφιοποιηθεί η κοινωνική ασφάλιση, οι πληρωμές ιατρικών παροχών και οι εγγώριες και διεθνείς ενισχύσεις. Οι προκαταβολικές και αυτοματοποιημένες πληρωμές θα μπορούσαν να αυτοματοποιηθούν μέσω των Smart Contracts. Στο πλαίσιο αυτό με την παρακολούθηση και πληρωμή διαφόρων προμηθευτών, τη διαχείριση αγοράς και την παρακολούθηση της απόδοσης δημοσίων προγραμμάτων, θα μπορούσε να επιτρέψει την απόλυτη διαφάνεια των δημόσιων δαπάνων.

Μεγάλη σημασία μπορεί να έχει η νέα τεχνολογία στην καταχώρηση δικαιωμάτων διανοητικής ιδιοκτησίας όπου η απόδειξη της κυριότητας και της χρονικής προτεραιότητας μπορεί να είναι δυσχερής και δαπανηρή, σε αντίθεση με την τεχνολογία blockchain η οποία μπορεί να προσφέρει βεβαιότητα για τις εν λόγω καταχωρήσεις. Οι πληροφορίες αυτές μπορούν να είναι εξαιρετικά χρήσιμες και στην αντιμετώπιση των απομιμητικών προϊόντων επιτρέποντας τη χρήση ασφαλών και μη τροποποιήσιμων πιστοποιητικών από τις τελωνειακές και αστυνομικές αρχές.

Ιδιαίτερα, ένα από τα βασικά ζητήματα στον τομέα της διαχείρισης δικαιωμάτων πνευματικής ιδιοκτησίας είναι η περιπλοκότητα των δικαιωμάτων κτήσης, η κατανομή των αμοιβών και η διαφάνεια λειτουργίας των οργανισμών συλλογικής διαχείρισης. Η τεχνολογία blockchain σε συνδυασμό με τα έξυπνα συμβόλαια μπορεί να παρέχει μία πλήρη και ακριβή βάση δεδομένων δικαιωμάτων πνευματικής ιδιοκτησίας εξασφαλίζοντας διάφανη κατανομή των αμοιβών σε πραγματικό χρόνο σε όλους τους δικαιούχους σε διαφορετικά επίπεδα. Η χρήση ψηφιακών νομισμάτων για την άμεση καταβολή των αμοιβών από τους χρήστες θα διευκολύνει ακόμη περισσότερο την βέλτιστη διαχείριση των εν λόγω δικαιωμάτων. (Λογαράς, 2018)

1.5.6 Δημοκρατία

Η ψηφιακή διακυβέρνηση και ηλεκτρονική ψηφοφορία καθίσταται πλέον πολύ πιο ασφαλής καθώς εκτός από την κρυπτογράφηση των δεδομένων με μέθοδο που καθιστά εξαιρετικά δύσκολη την παραποίηση τους, διασφαλίζεται και η διαφάνεια αφού οι συμμετέχοντες είναι σε θέση να επιβεβαιώσουν ότι οι ψήφοι τους μετρήθηκαν και ότι το περιεχόμενό τους δεν αλλοιώθηκε.

Η τεχνολογία blockchain διαθέτει όλα εκείνα τα χαρακτηριστικά που θα αναζητούσε κανείς σε μία πλατφόρμα διαδικτυακής ψηφοφορίας. Δεν επιτρέπει αλλαγές του παρελθόντος, αλλοιώσεις του παρόντος, ούτε και τροποποίηση του τρόπου πρόσβασης στο σύστημα. Κυρίως όμως, κάθε κόμβος με πρόσβαση στο σύστημα μπορεί να «βλέπει» τα ίδια αποτελέσματα και

³ Το token είναι μια μορφή δικαιώματος που παρέχει πρόσβαση σε συγκεκριμένες λειτουργίες του Blockchain δικτύου (στην ιδιοκτησία ή τις υπηρεσίες κάποιου άλλου ή συλλογικού αγαθού). (Shermin Voshmgir, 2019)

κάθε ψήφος μπορεί να αναχθεί με βεβαιότητα στην πηγή της, χωρίς διακυβεύεται η ανωνυμία των ψηφοφόρων.

Ένας άλλος τομέας στον οποίο η νέα τεχνολογία θα έβρισκε σημαντικές εφαρμογές είναι αυτός των μη κερδοσκοπικών οργανισμών, αφού οι δωρητές θα είναι σε θέση να διαπιστώνουν με βεβαιότητα και διαφάνεια πού χρησιμοποιούνται τα χρήματά τους. Πέραν αυτού, το blockchain διευκολύνει την πιο αποτελεσματική διανομή των κεφαλαίων κι ενισχύει τις δυνατότητες παρακολούθησής τους. (Λογαράς, 2018)

1.5.7 Άλλοι τομείς

Η τεχνολογία Blockchain έχει τη δυνατότητα να επηρεάσει τα συστήματα σε ένα ευρύ φάσμα βιομηχανιών και ο εκπαιδευτικός τομέας δεν αποτελεί εξαίρεση όταν τα εκπαιδευτικά δεδομένα αποθηκεύονται με ασφάλεια στο blockchain και μοιράζονται μεταξύ των αποδεκτών χρηστών. Στον τομέα της εκπαίδευσης, μπορούν να γίνουν διαχειρήσιμες οι διαδικασίες έκδοσης πιστοποιητικών και επαλήθευσής τους. Θα μπορεί αυτόματα να ελεγχεί αν κάποιος έχει έγκυρο πτυχίο ή πιστοποιητικό εκπαίδευσης. Επίσης το Blockchain θα διευκολύνει τον έγκυρο διαμοιρασμό αρχείων μεταξύ εκπαιδευτικών και φοιτητών. Προς αυτή την κατεύθυνση, η Sony Global Education έχει δημιουργήσει μια εκπαιδευτική πλατφόρμα σε συνεργασία με την IBM. Η πλατφόρμα επιτρέπει στους εκπαιδευτικούς να ανταλλάσσουν πληροφορίες σχετικά με την πρόοδο των μαθητών και τα επιτεύγματά τους. (Tapscott & Kaplan, 2019)

Η υπηρεσία «κοινοπραξίας οχημάτων» (ride-sharing) μπορεί να λειτουργήσει με μια τεχνολογία Blockchain και να διευκολύνει όλες τις συναλλαγές. Οι οδηγοί και οι επιβάτες έχουν τη δυνατότητα να επικοινωνούν μέσω μιας εφαρμογής φιλική προς το χρήστη αλλά και ταυτόχρονα με αυτόματες συναλλαγές με την βοήθεια ενός κατανεμημένου ledger. Ένα τέτοιο σύστημα είναι η πρωτοπορία Arcade city, στο οποίο οι οδηγοί ορίζουν τις δικές τους τιμές και αποκτούν δική τους βάση δεδομένων με τους πελάτες. Ένα άλλο σύστημα blockchain είναι το La'zooz, στο οποίο παρέχεται η δυνατότητα της επιβράβευσης με μάρκες σε χρήστες που εισάγουν νέα άτομα στο δίκτυο. Τέλος, το Snagride είναι μια blockchain εφαρμογή που παρέχει αρκετές διευκολύνσεις στον τρόπο πληρωμής και την δυνατότητα σε απλούς χρήστες να είναι εκτός από πελάτες και οδηγοί. (KryptoGraphe Team, 2018)

1.6 Περιβάλλοντα εργασίας Blockchain

1.6.1 Hyperledger

Το Hyperledger είναι μάλλον κάτι σαν hub⁴ για την ανάπτυξη ανοικτών βιομηχανικών blocks. Στην επίσημη ιστοσελίδα του Hyperledger δηλώνεται ότι: «Το Hyperledger είναι μια συνεργατική προσπάθεια ανοιχτής πηγής που δημιουργήθηκε για να προωθήσει τις διεπαγγελματικές τεχνολογίες blockchain. Πρόκειται για μια παγκόσμια συνεργασία, που φιλοξενείται από το ίδρυμα του Linux Foundation, συμπεριλαμβανομένων των ηγετών στον τομέα της χρηματοδότησης, της τραπεζικής, του Διαδικτύου των πραγμάτων, των αλυσίδων εφοδιασμού, της κατασκευής και της τεχνολογίας ».

Το Hyperledger δεν υποστηρίζει Bitcoin ή οποιαδήποτε άλλη κρυπτογράφηση. Έχει τη δυνατότητα να «οικοδομήσει» μια νέα γενιά εφαρμογών που δημιουργούν την εμπιστοσύνη, τη λογοδοσία και τη διαφάνεια στον πυρήνα τους, ενώ παράλληλα η τεχνολογία αυτή υποσχέθηκε μια ευρύτερη και πιο θεμελιώδη επανάσταση από την τεχνολογία blockchain, δηλαδή την ροή των επιχειρηματικών διαδικασιών και των νομικών περιορισμών. (Rosic, 2017)

1.6.2 Ethereum

Το δίκτυο Ethereum παρέχει ένα πιο ευέλικτο αναπτυξιακό περιβάλλον από το Bitcoin Blockchain και άλλα Blockchain δίκτυα ειδικού σκοπού. Πρόκειται για ένα δίκτυο Peer to Peer (P2P) που μπορεί να επεξεργαστεί κάθε είδους έξυπνη σύμβαση, η οποία μπορεί εύκολα να δημιουργηθεί με λίγες γραμμές κώδικα και χωρίς να χρειάζεται να δημιουργήσετε τη δική σας υποδομή αποκλειστικής χρήσης.

Η βασική καινοτομία του Ethereum, η εικονική μηχανή Ethereum (EVM) είναι ένα πλήρες λογισμικό της Turing που λειτουργεί στο δίκτυο Ethereum. Επιτρέπει σε οποιονδήποτε να εκτελέσει οποιοδήποτε πρόγραμμα, ανεξάρτητα από τη γλώσσα προγραμματισμού που δίνει αρκετό χρόνο και μνήμη. Η εικονική μηχανή Ethereum καθιστά τη διαδικασία δημιουργίας εφαρμογών blockchain πολύ πιο εύκολη και αποτελεσματική από ποτέ. Αντί να χρειαστεί να χτίσει ένα εντελώς πρωτότυπο blockchain για κάθε νέα εφαρμογή, η Ethereum επιτρέπει την ανάπτυξη δυνητικά χιλιάδων διαφορετικών εφαρμογών σε μία πλατφόρμα.

Το Ethereum μπορεί επίσης να χρησιμοποιηθεί για την κατασκευή Αποκεντρωμένων Αυτόνομων Οργανισμών (Decentralized Autonomous Organization, DAO). Ένας DAO είναι μια πλήρως αυτόνομη, αποκεντρωμένη οργάνωση χωρίς μοναδικό ηγέτη. Τα DAO λειτουργούν με κώδικα προγραμματισμού, σε μια συλλογή έξυπνων συμβολαίων που γράφονται στο μπλοκ του Ethereum. Ο κώδικας έχει σχεδιαστεί για να αντικαταστήσει τους κανόνες και τη δομή μιας παραδοσιακής οργάνωσης, εξαλείφοντας την ανάγκη για τους ανθρώπους και τον κεντρικό έλεγχο. Ένα DAO ανήκει σε όσους αγοράζουν μάρκες, αλλά αντί για κάθε κρυπτογραφικό token που αντιστοιχεί σε μετοχές και ιδιοκτησία μετοχών, οι μάρκες λειτουργούν ως εισφορές που δίνουν στους ανθρώπους δικαιώματα ψήφου. (Rosic, 2016)

⁴ Ο επαγωγέας ή hub είναι μια συσκευή δικτύωσης που συνδέει πολλούς υπολογιστές ή άλλες συσκευές δικτύου. (Computer Hope, 2019)

1.6.3 Άλλα Blockchain Δίκτυα

Το Amazon Managed Blockchain είναι μια πλήρως διαχειριζόμενη υπηρεσία για τη δημιουργία και διαχείριση δικτύων blockchain χρησιμοποιώντας πλαίσια ανοιχτού κώδικα. Επί του παρόντος υποστηρίζεται το πλαίσιο ανοιχτού κώδικα Fabric Hyperledger. Το Blockchain επιτρέπει τη δημιουργία εφαρμογών, όπου πολλά μέρη μπορούν να διεξάγουν με ασφάλεια και διαφάνεια τις συναλλαγές και να μοιράζονται δεδομένα χωρίς την ανάγκη μιας έμπιστης κεντρικής αρχής.

Το Amazon Quantum Ledger Database (QLDB) είναι μια βάση δεδομένων πλήρους διαχείρισεως, η οποία παρέχει ένα διαφανές, αμετάβλητο και κρυπτογραφικά επαληθεύσιμο αρχείο συναλλαγών που ανήκει σε μια κεντρική έμπιστη αρχή. Το Amazon QLDB παρακολουθεί κάθε αλλαγή των δεδομένων εφαρμογής και διατηρεί ένα πλήρες και επαληθεύσιμο ιστορικό αλλαγών με την πάροδο του χρόνου.

Το Mastercard Blockchain διευκολύνει νέες ευκαιρίες εμπορίου για την ψηφιακή μεταφορά αξίας επιτρέποντας στις επιχειρήσεις και τα χρηματοπιστωτικά ιδρύματα να πραγματοποιούν συναλλαγές σε κατανεμημένο βιβλίο. Η τεχνολογία αυτή μπορεί να τροφοδοτήσει πολλαπλές περιπτώσεις χρήσης και μπορεί να βοηθήσει στην απομάκρυνση των οικονομικών ροών από το χρόνο, το κόστος και τον κίνδυνο.

Η Azure παρέχει μια πλατφόρμα γρήγορης, χαμηλού κόστους, χαμηλού κινδύνου και αποτυχίας για να συνεργαστούν οι οργανισμοί μέσω πειραματισμού με νέες επιχειρηματικές διαδικασίες και όλα υποστηρίζονται από μια πλατφόρμα σύννεφων με το μεγαλύτερο χαρτοφυλάκιο συμμόρφωσης στον κλάδο. (G2 Team, 2019)

Κεφάλαιο 2. Το οικοσύστημα Hyperledger

2.1 Γενικά

Η κύρια ιδέα του Hyperledger είναι η ανάπτυξη ενός συστήματος που θα συμβάλλει στην συνεργασία μεταξύ διαφόρων επιχειρήσεων και οργανισμών χωρίς τη χρήση δημόσιων blockchain εφαρμογών όπως το Bitcoin και το Ethereum. Αντί κάθε μεμονωμένος οργανισμός να δημιουργεί τη δική του blockchain λύση, χρησιμοποιείται μια κοινά αποδεκτή πλατφόρμα αποτελούμενη από επιμέρους τμήματα, τα οποία μπορούν να επιλεγθούν και να συνδυαστούν έτσι ώστε να παρέχουν λύσεις σε κάθετα πεδία εφαρμογών. (Hyperledger , 2017)

2.1.1 Ιστορία

Το Hyperledger είναι ένα σύστημα συνδεδεμένων ομότιμων κόμβων (P2P network), μια πλατφόρμα που δημιουργήθηκε από την αιγίδα του Linux Foundation τον Δεκέμβριο του 2015, ώστε να στηρίξει την ανάπτυξη αποκεντρωμένων ledgers (ημερολόγια) βασισμένων στην blockchain τεχνολογία. Με το Hyperledger, το Linux Foundation στοχεύει να δημιουργήσει ένα περιβάλλον στο οποίο οι κοινότητες προγραμματιστών λογισμικού και οι εταιρείες συναντιούνται και συντονίζονται για να δημιουργήσουν πλαίσια blockchain. Έτσι, πρόκειται για μια υποδομή στην οποία αναπτύσσονται συνεχιζόμενα και μελλοντικά έργα σχετιζόμενα με το blockchain.

Σήμερα η Hyperledger διαθέτει μια εντυπωσιακή λίστα με περισσότερα από 100 μέλη. Ο κατάλογος καλύπτει ένα ευρύ φάσμα γνωστών ηγετών της βιομηχανίας. Περιλαμβάνει εταιρείες τεχνολογίας κινητικότητας όπως η Airbus και η Daimler, εταιρείες πληροφορικής όπως η IBM, η Fujitsu, η SAP, η Huawei, η Nokia, η Intel και η Samsung, χρηματοπιστωτικά ιδρύματα όπως Deutsche Börse, American Express, JP Morgan, BBVA, BNP Paribas και Well Fargo. ως νεοσυσταθέντες όπως Blockstream, Netki, Lykke, Factom, bloq και Consensys. Πολλές από τις μεγαλύτερες εταιρείες στον κόσμο της τεχνολογίας και του χρηματοπιστωτικού τομέα συναντώνται στο Hyperledger με μερικά από τα καλύτερα blockchain startups.

Το σύνολο των διοικητικών στελεχών του Hyperledger είναι μια επιτροπή ηγετών. Αποτελείται από περισσότερα από 10 στελέχη, τα περισσότερα με δεκαετίες εμπειρίας στο Open Source και στενές συνδέσεις με διάφορες βιομηχανίες. Βρίσκονται επικεφαλής του Ιδρύματος Apache και της Κοινοπραξίας του W3C, καθώς και μηχανικοί της IBM και πολλούς άλλους. Ορισμένα από τα μέλη του Hyperledgers, όπως ο Richard Brown και ο Tamas Blumer, έχουν ήδη εργαστεί με το Blockchain εδώ και χρόνια. Για τα μέλη της, το Hyperledger δεν παρέχει μόνο τεχνικές γνώσεις και πλαίσια λογισμικού αλλά και διάφορες επαφές με βιομηχανίες και προγραμματιστές.

Σχετικά νωρίς στην ιστορία του Hyperledger, το έργο έπρεπε να πάρει μια σημαντική απόφαση. Ο γενικός διευθυντής Brian Behlendorf ρωτήθηκε αν θα υπάρξει ένα «Hyperledger Coin», μια νομισματική μονάδα που θα τρέχει στα μπλοκ Hyperledger. Ο Behlendorf απάντησε ότι το ίδιο το έργο Hyperledger ποτέ δεν θα χτίσει τη δική του κρυπτογράφηση. Η απόφαση αυτή διαμόρφωσε έντονα τους στρατηγικούς στόχους του Hyperledger για την ανάπτυξη βιομηχανικών εφαρμογών της τεχνολογίας blockchain και την απότομη εξαίρεσή

της από τα πλουσιότερα σχέδια που συνήθως εξελίσσονται από τα blockchain με βάση το νόμισμα.

Συνεπώς, ένα από τα πιο σημαντικά χαρακτηριστικά του Hyperledger είναι η δημιουργία και η ανάπτυξη μη κερδοσκοπικών εφαρμογών. Κάνουμε λόγο για ένα παγκόσμιο κίνημα, που ξεκίνησε από το Linux Foundation και με επικεφαλής γνωστούς ανθρώπους της τεχνολογίας, του ανοιχτού κώδικα και του κόσμου δεδομένων με πολυετή εμπειρία και την υποστήριξη από εταιρείες και οργανισμούς και συμβάλλει στην ανάπτυξη μη κερδοσκοπικών blockchain εφαρμογών στον επιχειρηματικό κόσμο. (Rosic, 2017)

2.1.2 Γενικά χαρακτηριστικά, πλαίσια και εργαλεία

Στο πλαίσιο του Hyperledger φιλοξενείται και προωθείται μια σειρά επιχειρηματικών Blockchain τεχνολογιών, πλαισίων, βιβλιοθηκών, διεπαφών και εφαρμογών. Το Hyperledger είναι ο κύριος ιδρυτής των ακόλουθων έργων. (Rosic, 2017)

Hyperledger Iroha

Το Hyperledger Iroha χρησιμοποιείται στην Cambodia για να δημιουργήσει ένα νέο σύστημα πληρωμών παράλληλα με την εθνική τράπεζα της Cambodia, καθώς επίσης πολλές Ιαπωνικές εταιρίες συνεργάζονται στο πλαίσιο του Iroha για προγράμματα στην υγειονομική περίθαλψη, την χρηματοδότηση και τη διαχείριση της ταυτότητας.

Hyperledger Sawtooth

Sawtooth περιλαμβάνει ένα δυναμικό χαρακτηριστικό συναίνεσης που επιτρέπει αλγόριθμους συναίνεσης συναλλαγών σε ένα τρέχον δίκτυο. Μεταξύ των επιλογών συναίνεσης είναι ένα πρωτότυπο πρωτόκολλο συναίνεσης γνωστό ως "Proof of Elapsed Time", ένα πρωτόκολλο συναινετικής σχεδίασης που έχουμε αναλύσει στο προηγούμενο κεφάλαιο. Το Sawtooth υποστηρίζει τα έξυπνα συμβόλαια του Ethereum μέσω του "seth" (έναν επεξεργαστή συναλλαγών Sawtooth που ενσωματώνει τη λειτουργία του εικονικού μηχανήματος Hyperledger Burrow EVM). (Benjamin, 2017)

Hyperledger Fabric

Αντί ένα ενιαίο blockchain το Fabric είναι μια βάση για την ανάπτυξη λύσεων βασισμένων σε blockchain με μια αρχιτεκτονική μοντέλου. Με το Fabric διαφορετικά εξαρτήματα των Blockchains, όπως η συναίνεση και οι υπηρεσίες προσχώρησης μπορούν να γίνουν «plug-and-play», δηλαδή να ενταχθούν και τρέξουν εύκολα στο μοντελοποιημένο σύστημα. Το Fabric έχει σχεδιαστεί για να παρέχει ένα πλαίσιο με το οποίο οι επιχειρήσεις μπορούν να δημιουργήσουν το δικό τους, μεμονωμένο δίκτυο blockchain που μπορεί να κλιμακωθεί γρήγορα σε πάνω από 1.000 συναλλαγές ανά δευτερόλεπτο.

Hyperledger Caliper

Το Hyperledger Caliper είναι ένα εργαλείο συγκριτικής αξιολόγησης και ένα από τα έργα του Hyperledger που φιλοξενείται από το The Linux Foundation. Το Hyperledger Caliper επιτρέπει στους χρήστες να μετρήσουν την απόδοση μιας συγκεκριμένης εφαρμογής blockchain με ένα σύνολο προκαθορισμένων περιπτώσεων χρήσης. Το Hyperledger Caliper θα παράγει

αναφορές που θα περιλαμβάνουν ορισμένους δείκτες απόδοσης, όπως TPS (Transactions Per Second), λανθάνουσα κατάσταση συναλλαγών, χρήση πόρων κλπ. Στόχος είναι τα αποτελέσματα του Caliper να χρησιμοποιηθούν από άλλα έργα του Hyperledger, καθώς αναπτύσσουν τα πλαίσια τους και αναφορές στην υποστήριξη της επιλογής μιας εφαρμογής blockchain κατάλληλης για τις συγκεκριμένες ανάγκες ενός χρήστη. Στο Hyperledger Caliper είχαν αρχικά συμβάλει προγραμματιστές από την Huawei, Hyperchain, Oracle, Bitwise, Soramitsu, IBM και το Πανεπιστήμιο Τεχνολογίας και Οικονομικών της Βουδαπέστης. (Hyperledger Team, 2018)

Hyperledger Cello

Το Hyperledger Cello στοχεύει να φέρει το μοντέλο ανάπτυξης «on-the-service» στο οικοσύστημα blockchain για να μειώσει την προσπάθεια που απαιτείται για τη δημιουργία, τη διαχείριση και τον τερματισμό μπλοκ αλυσίδων. Παρέχει μια υπηρεσία αλυσίδας πολλαπλών μισθωτών αποτελεσματικά και αυτόματα πάνω από διάφορες υποδομές, π.χ. baremetal, εικονική μηχανή και περισσότερες πλατφόρμες εμπορευματοκιβωτίων. Στο Hyperledger Cello συνεισέφερε αρχικά η IBM, με χορηγούς τους Soramitsu, Huawei και Intel. (Hyperledger Team, 2018)

Hyperledger Explorer

Σχεδιασμένο για να δημιουργήσει μια φιλική προς το χρήστη εφαρμογή Ιστού, το Hyperledger Explorer μπορεί να προβάλλει, να επικαλείται, να αναπτύσσει και να υποβάλλει ερωτήματα σε μπλοκ, συναλλαγές και συναφή δεδομένα, πληροφορίες δικτύου (όνομα, κατάσταση, λίστα κόμβων), αλυσιδωτούς κωδικούς και οικογένειες συναλλαγών και σχετικές πληροφορίες που είναι αποθηκευμένες στο ledger. Στην αρχιτεκτονική του Hyperledger Explorer συνεισέφεραν αρχικά η IBM, η Intel και η DTCC. (Hyperledger , 2018)

Hyperledger Quilt

Το Hyperledger Quilt προσφέρει διαλειτουργικότητα μεταξύ λογιστικών συστημάτων εφαρμόζοντας το πρωτόκολλο Interledger (επίσης γνωστό ως ILP), το οποίο είναι πρωτίστως πρωτόκολλο πληρωμών και έχει σχεδιαστεί για να μεταφέρει την αξία σε διανεμημένους καταλόγους και μη κατανεμημένους καταλόγους. Το πρωτόκολλο Interledger παρέχει ατομικές αντισταθμίσεις μεταξύ των ledgers (ακόμη και μη κατανεμημένων καταλόγων) και ένα ενιαίο χώρο ονομάτων για όλους τους λογαριασμούς εντός κάθε ledger. Με την προσθήκη του Quilt στο Hyperledger, το ίδρυμα Linux Foundation φιλοξενεί σήμερα τις εφαρμογές Java (Quilt) και JavaScript (Interledger.js) Interledger. (Hyperledger, 2018)

Hyperledger Composer

Το Hyperledger Composer είναι ένα σύνολο εργαλείων συνεργασίας για την οικοδόμηση δικτύων επιχειρηματικών δεσμών, τα οποία καθιστούν απλό και γρήγορο για τους ιδιοκτήτες επιχειρήσεων και προγραμματιστές να δημιουργούν έξυπνες συμβάσεις και εφαρμογές αποκλεισμού για την επίλυση επιχειρηματικών προβλημάτων. (Kuhrt & Huseby, 2019)
Το Hyperledger Composer υποστηρίζει και διαμένει στην κορυφή της υπάρχουσας υποδομής και χρόνου εκτέλεσης του Hyperledger Fabric Blockchain. Το Hyperledger Composer παρέχει μια απλοποιημένη γλώσσα μοντελοποίησης συγκεκριμένου τομέα για

τη μοντελοποίηση επιχειρηματικού δικτύου και τη JavaScript για την λογική εφαρμογή των συναλλαγών. (Haardik, 2018)

2.1.3 Περιβάλλον εκτέλεσης

Η αποστολή του Hyperledger είναι να δημιουργήσει ένα επιχειρηματικό επίπεδο, ένα διανεμημένο πλαίσιο λογισμικού ανοιχτού κώδικα και μια βάση κώδικα, μέσω της οποίας οι χρήστες μπορούν να δημιουργήσουν και να εκτελέσουν ισχυρές εφαρμογές, πλατφόρμες και συστήματα λογισμικού για τη στήριξη των επιχειρηματικών συναλλαγών.

Η δημιουργία μιας τεχνικής κοινότητας ανοιχτού κώδικα ωφελεί το οικοσύστημα των παρόχων και χρηστών λύσεων Hyperledger, εστιάζοντας σε περιπτώσεις κοινών χρηστών που θα λειτουργούν σε διάφορες βιομηχανικές λύσεις. Προωθείται η συμμετοχή των κυριότερων μελών του οικοσυστήματος, συμπεριλαμβανομένων των προγραμματιστών, των παρόχων υπηρεσιών και των τελικών χρηστών. Τέλος, παραχωρεί ένα ουδέτερο χώρο για κοινοτική υποδομή, συναντήσεις, εκδηλώσεις και συνεργατικές συζητήσεις.

Στο πλαίσιο αυτό τον Απρίλιο του 2017, η IBM συνεργάστηκε με το Mizuho Financial Group της Ιαπωνίας και την Mizuho Bank για τη δημιουργία μιας πλατφόρμας βασισμένης σε blockchain για τη χρηματοδότηση του εμπορίου. Σύμφωνα με την ιαπωνική τράπεζα, η τεχνολογία blockchain τους βοήθησε να συντομεύσουν τον χρόνο επεξεργασίας των συμφωνιών από μερικές ημέρες σε μόλις δύο ώρες, επιτρέποντας επίσης να εξοικονομήσουν το κόστος εργασίας, αυξάνοντας ταυτόχρονα τη διαφάνεια μέσω της ψηφιοποίησης εγγράφων.

Επιπλέον, η Mizuho Financial Group συνεργάζεται με την IBM για την τελική διεξαγωγή όλων των συναλλαγών τους στο Hyperledger Fabric. Σύμφωνα με το επίσημο δελτίο Τύπου της IBM, το σύστημα αυτό θα επιτρέψει σε όλα τα μέρη να δουν τα πιο πρόσφατα δεδομένα αποστολής, τα οποία θα μειώσουν δραστικά την εμπορική συναλλαγή και το κόστος επεξεργασίας.

Σε συνεργασία με τις TenneT, Sonnen και Vandebron, η IBM έχει αναπτύξει μια κατανομημένη βάση δεδομένων για τη διαχείριση του ηλεκτρικού δικτύου στην Ολλανδία και τη Γερμανία. Το έργο θα έχει τεράστιο αντίκτυπο στην μελλοντική χρήση ενεργειακών πηγών παγκοσμίως, δεδομένου ότι αποσκοπεί στον εντοπισμό περιοχών που δεν διαθέτουν ηλεκτρική ενέργεια ή υποφέρουν από συχνές διακοπές ενέργειας και θα καλύπτει τα κενά αυτά με την παροχή ηλεκτρικής ισχύς από άλλες ηλεκτρικές πηγές, συμπεριλαμβανομένων των ηλεκτρικών αυτοκινήτων και των ηλεκτρικών στηλών (σε περιοχές που έως τώρα δεν διαθέτουν παρόμοια μέσα), μέσω ενός αποκλειστικού δικτύου blockchain που χρησιμοποιεί Hyperledger Fabric.

Το παγκόσμιο εμπόριο έχει αυξηθεί ραγδαία, με αύξηση 246,15% στις πωλήσεις ηλεκτρονικού εμπορίου παγκοσμίως και αναμένεται να αυξηθεί περαιτέρω, φθάνοντας τα 4,5 τρισεκατομμύρια δολάρια το 2021. Με την κατασκευαστική δραστηριότητα που λαμβάνει χώρα σε ολόκληρο τον κόσμο, η παρακολούθηση εμπορευμάτων σε πραγματικό χρόνο είναι ζωτικής σημασίας.

Για να ικανοποιήσει τη ζήτηση, τον Δεκέμβριο του 2017 ο μεγάλος πολυεθνικός λιανοπωλητής Walmart συνεργάστηκε με την IBM για να δημιουργήσει ένα σύστημα αποκλειστικής επιχείρησης Hyperledger Fabric, το οποίο παρακολουθεί τη μεταφορά των τροφίμων από τον

προμηθευτή στο ράφι. Η λύση για την ασφάλεια τροφίμων της Walmart χρησιμοποιεί την τεχνολογία IBM Food Trust, η οποία επιτρέπει την πλήρη συνεργασία όλων των εμπλεκόμενων και τη σχέση τους με τα τρόφιμα. Επιπλέον, περισσότεροι μεγάλοι λιανοπωλητές εξέφρασαν πρόσφατα την επιθυμία τους να συνεργαστούν, όπως η Dole, η Driscoll, η Golden State Foods, η Kroger, η McCormick and Company, η McLane Company, η Nestlé, η Tyson Foods και η Unilever. Ωστόσο, το σύστημα της αλυσίδας εφοδιασμού που βασίζεται στο Hyperledger δεν είναι αποκλειστικά για τη βιομηχανία τροφίμων και οι επόμενες εταιρείες που την υιοθέτησαν είναι φαρμακεία σε ολόκληρο τον κόσμο, δεδομένου ότι απαιτείται από το νόμο να διατηρούν την αλυσίδα φύλαξης για κάθε φάρμακο. (Yafimava, 2018)

2.1.4 Πηγές πληροφοριών

Για το Hyperledger μπορούμε να αντλήσουμε πολλές πληροφορίες στο διαδίκτυο τόσο για την χρησιμότητά του όσο και για τον τρόπο υλοποίησής του. Στην επίσημη σελίδα του Hyperledger (Hyperledger, 2019) μπορούμε να βρούμε αναφορές των διαφόρων εργαλείων και εφαρμογών που φιλοξενούνται, καθώς και ένα σύνολο από παραπομπές πηγών έρευνας όπως webinars, tutorials, videos, publications, training και certification, industries και universities.

Υπάρχουν πλατφόρμες που στοχεύουν στην εκμάθηση Blockchain εφαρμογών, στις οποίες δίνεται και η δυνατότητα απόκτησης πιστοποιητικών μέσα από αυτά τα μαθήματα δίνοντας ένα χρηματικό ποσό. Φυσικά, υπάρχει και η επιλογή της απλής παρακολούθησης των μαθημάτων δωρεάν χωρίς το πιστοποιητικό για όσους δεν ενδιαφέρονται να το αποκτήσουν. Ένα παράδειγμα τέτοιας πλατφόρμας είναι το Coursera (Coursera Team, 2019).

Στην σελίδα του Coursera μπορούμε να παρακολουθήσουμε διάφορα διαδικτυακά μαθήματα, τα οποία καλύπτουν τα βασικά χαρακτηριστικά των τεχνολογιών Blockchain και των διαφοροποιήσεων μεταξύ των διαφόρων Blockchain έργων αλλά και την καθοδήγηση για την υλοποίησή τους. Ένα από αυτά είναι το «Blockchain: Essentials for developers», το οποίο δημιουργήθηκε από την IBM και τους έμπειρους συνεργάτες της για να προσφέρει στους ενδιαφερόμενους τη δυνατότητα να χτίσουν ένα δικό τους σύστημα Hyperledger με πλήρη κατανόηση των τεχνολογιών που χρησιμοποιούν. (IBM Team, 2018)

Παρόμοια λειτουργούν η Udacity (Udacity, 2019) και η Udemy (Udemy, 2019), στις οποίες μπορούμε να δημιουργήσουμε ένα λογαριασμό και να παρακολουθήσουμε μαθήματα για Blockchain εφαρμογές με δυνατότητα υποβολής ερωτημάτων προς τον διδάσκοντα και άμεσης ανταπόκρισής του. Ακόμη και σε περιπτώσεις που δεν υπάρχει αλληλεπίδραση με τον ιδρυτή του, τα μαθήματα περιέχουν ερωτήσεις και ασκήσεις για την εκτίμηση της κατανόησης των περιεχομένων ενός μαθήματος.

Δύο ακόμη χρήσιμες ηλεκτρονικές πηγές είναι η πλατφόρμα Blockgeeks (Blockgeeks, 2019), η οποία περιέχει διάφορες αναφορές, άρθρα, βίντεο και σχεδιαγράμματα για την κατανόηση των εννοιών του Hyperledger και άλλων Blockchain εφαρμογών, αλλά και η πλατφόρμα Medium (Medium Team, 2019), η οποία είναι μια πιο γενικού ενδιαφέροντος πηγή πληροφοριών, αλλά περιέχει επίσης σημαντικά tutorials με οδηγίες για την υλοποίηση εφαρμογών του Blockchain. Ένα επιπλέον σημαντικό στοιχείο αυτών των σελίδων είναι ότι δημιουργώντας ένα λογαριασμό σε αυτές δίνεται η δυνατότητα του σχολιασμού και της

κατάθεσης ερωτήσεων προς τον συγγραφέα του άρθρου, ο οποίος με τη σειρά του απαντά. Τις περισσότερες ιστοσελίδες για πληροφορίες θα βρείτε και στην βιβλιογραφία.

2.2 Αντιστοίχιση εννοιών Blockchain στο Hyperledger

2.2.1 Consensus algorithms

Επειδή οι απαιτήσεις των Blockchain των επιχειρήσεων ποικίλουν, η κοινότητα του Hyperledger χρησιμοποιεί διάφορους μηχανισμούς συναίνεσης ανάλογα με τον τρόπο που αναπτύσσεται το μοντέλο κάθε εφαρμογής ή αλλιώς πλαισίου.

Consensus στο Fabric

Η συναίνεση στο Hyperledger Fabric χωρίζεται σε 3 φάσεις: την πρόταση(Endorsement), που καθοδηγείται από μια πολιτική που ακολουθούν οι συμμετέχοντες να εγκρίνουν μια συναλλαγή, την παραγγελία (Ordering), που δέχεται τις εγκεκριμένες συναλλαγές και συμφωνεί αν η πρόταση να μπορεί να εγγραφεί στο ledger και την επικύρωση (Validation), που λαμβάνει ένα μπλοκ από εντολές και επικυρώνει την ορθότητα του αποτελέσματος, συμπεριλαμβανομένου του ελέγχου της πολιτικής επικύρωσης και της διπλής δαπάνης.

Συγκεκριμένα, κάθε συναλλαγή ή ενημέρωση του ledger ακολουθεί την εξής ροή (Εικόνα 7):

(1) Ο πελάτης χρησιμοποιεί το SDK για να σχηματίσει μια πρόταση συναλλαγής, η οποία περιλαμβάνει: το όνομα του καναλιού, το όνομα του αλυσωτού κώδικα και τις παραμέτρους εισόδου του κώδικα που πρόκειται να εκτελεστεί. Στη συνέχεια, ο πελάτης στέλνει πρόταση συναλλαγής σε όλους τους υποψήφιους συνοδούς για να ικανοποιήσει την πολιτική επικύρωσης του συγκεκριμένου αλυσιδωτού κώδικα.

(2) Οι peers⁵ προσομοιώνουν τη συναλλαγή με βάση τις παραμέτρους που λαμβάνονται από τον πελάτη, αλληλεπιδρώντας πραγματικά με τον αλυσιδωτό κώδικα για να καταγράψουν τις ενημερώσεις και να παράγουν αποτελέσματα με τη μορφή συνόλου ανάγνωσης και εγγραφής ακολουθώντας την υπογραφή του συνόλου και επιστρέφοντας τα αποτελέσματα πίσω στον πελάτη.

(3) Ο πελάτης συλλέγει τις απαντήσεις από όλους τους peers, επικυρώνει ότι τα αποτελέσματα είναι συνεπή, π.χ. όλοι οι υποψήφιοι που έχουν προσυπογράψει όλοι το ίδιο ωφέλιμο φορτίο. Ακολουθεί η συνένωση όλων των υπογραφών των peers μαζί με τα σύνολα ανάγνωσης-εγγραφής και η δημιουργία μιας συναλλαγής που υποβάλλεται στο ordering service.

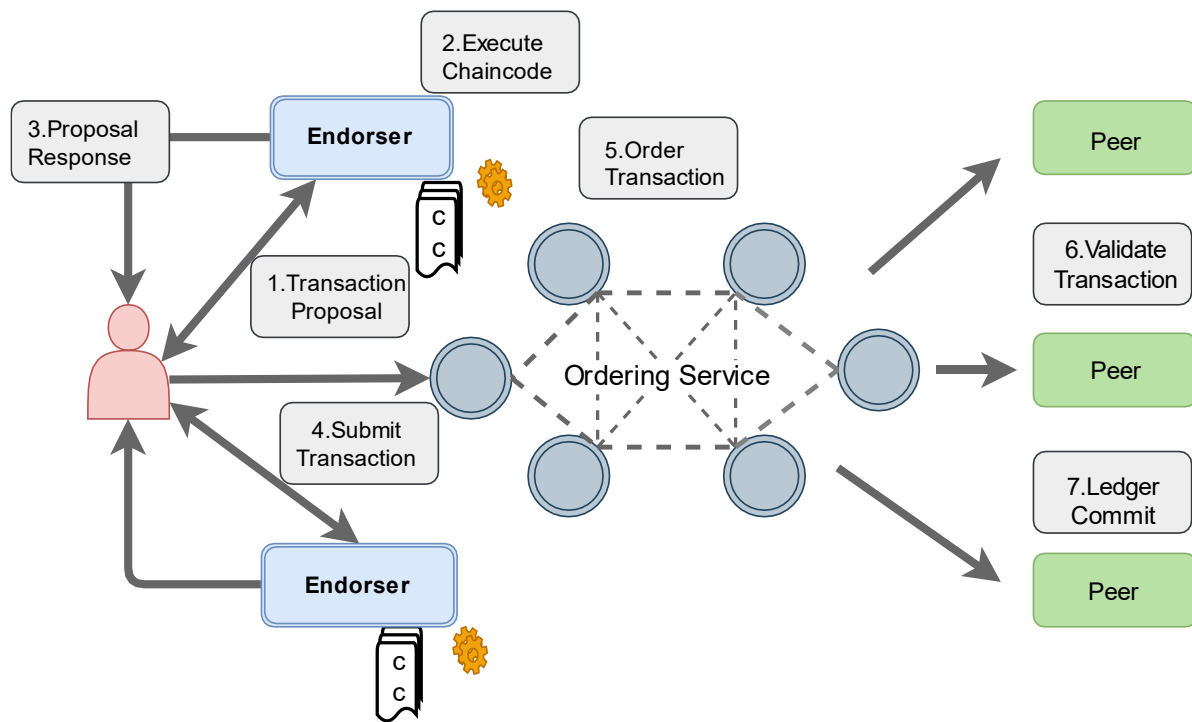
⁵ Ο peer είναι κόμβος του δικτύου που περιέχει αντίγραφα των ledgers και των smart contracts. Παράλληλα, οι peers έχουν το ρόλο του υποστηρικτή (endorser), όπου όταν λάβει μια πρόταση από ένα πελάτη την υποστηρίζει και την παραθέτει στο ordering service για να εγκριθεί η πρόταση και από τα υπόλοιπα μέλη του δικτύου.

(4) Το ordering service⁶ συλλέγει όλες τις εισερχόμενες συναλλαγές, τις κατατάσσει σε ένα πλαίσιο του καναλιού και περιοδικά διαιρεί τα πλαίσια σε μπλοκ που περιλαμβάνουν όλες αυτές παραγγελίες.

(5) Οι peers κάθε οργανισμού, τραβούν νέα μπλοκ από την υπηρεσία παραγγελιών και διαδίδουν στη συνέχεια με τη χρήση κλιμακούμενου ενδιαμέσου λογισμικού την αναπαραγωγή του ledger σε όλο το δίκτυο, η εφαρμογή του οποίου βασίζεται σε πρωτόκολλο γνωστό ως μέθοδος «κουτσομπολιού» .

(6) Κάθε peer, όταν λάβει ένα νέο μπλοκ, επαναλαμβάνει τις συναλλαγές για να επικυρώσει: πρώτον την πολιτική επικύρωσης, δηλ. εάν το σύνολο των υπογραφών peers ικανοποιεί την πολιτική επικύρωσης που σχετίζεται με τον αλυσιδωτό κωδικό και δεύτερον, εκτελεί ταυτόχρονα ελέγχους πολλαπλών τιμών.

(7) Μόλις ολοκληρωθεί η επικύρωση της συναλλαγής, ο peer προσθέτει το μπλοκ στο ledger και ενημερώνει την κατάστασή του βάσει έγκυρων συναλλαγών. Μετά την δέσμευση του μπλοκ εκπέμπει συμβάντα για την ενημέρωση του συνδεδεμένου πελάτη. (Hyperledger Fabric, 2019)



Εικόνα 7 Hyperledger Fabric-high level transaction flow

Το ordering service χρησιμοποιεί consensus αλγόριθμους βασισμένους στο Byzantine Fault Tolerance, συμπεριλαμβανομένων των BFT Smart, Simplified BFT, Honey Badger of BFT, Kafka, Raft, Solo κ.λ.π. Περισσότερα για τους τρεις τελευταίους μπορούμε να βρούμε στην επίσημη σελίδα του Fabric (Hyperledger Fabric, 2019).

⁶ Οι orderers είναι οι κόμβοι που λαμβάνουν τις προτάσεις συναλλαγών των peers, τις οριοθετούν σε blocks (σελίδες) και στέλνουν τα αντίγραφα των blocks σε όλους τους peers του ίδιου καναλιού.

Η εφαρμογή Solo της ordering service διαθέτει μόνο έναν μοναδικό κόμβο παραγγελίας. Ως αποτέλεσμα, δεν είναι, και ποτέ δεν θα είναι, ανεκτικός σε λάθη. Για το λόγο αυτό, οι υλοποιήσεις Solo δεν μπορούν να ληφθούν υπόψη για την παραγωγή, αλλά είναι μια καλή επιλογή για δοκιμές εφαρμογών και έξυπνων συμβολαίων ή για τη δημιουργία αποδείξεων έννοιας.

Το Raft είναι μια υπηρεσία παραγγελίας ανεκτική σε σφαλμάτα (Crash Fault Tolerant, CFT) που υλοποιείται με βάση την εφαρμογή του πρωτοκόλλου Raft. Το Raft πρωτόκολλο ακολουθεί ένα μοντέλο «leader and follower», όπου εκλέγεται ένας κόμβος ηγέτη (ανά κανάλι) και οι αποφάσεις του αντιγράφονται από τους οπαδούς. Οι Raft ordering services πρέπει να είναι ευκολότερες στη δημιουργία και τη διαχείριση των blocks από τις ordering services που βασίζονται στο Kafka και ο σχεδιασμός τους επιτρέπει σε διαφορετικούς οργανισμούς να συνεισφέρουν στο ordering service.

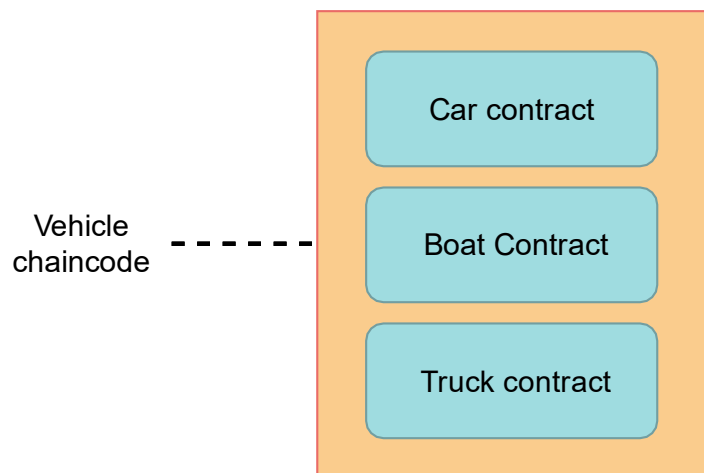
Παρόμοια με το Raft, το Apache Kafka είναι μια εφαρμογή του CFT που παράγει κόμβους με βάση το μοντέλο «leader and follower». Ο Kafka χρησιμοποιεί ένα σύνολο ZooKeeper για σκοπούς διαχείρισης. Το ordering service Kafka είναι διαθέσιμο από την έκδοση του Fabric v1.0.

Consensus στα υπόλοιπα πλαίσια

Η συναίνεση στο Hyperledger Indy βασίζεται στον αλγόριθμο Redundant Byzantine Fault Tolerance (RBFT). Όπως το PBFT, το RBFT χρειάζεται τουλάχιστον $3n + 1$ κόμβους για να χειριστεί n ελαττωματικούς κόμβους. Όλες οι προτάσεις τίθενται στο ordering service αλλά μόνο αυτές που έχουν μια κύρια ιδιότητα επικυρώνονται. Το Hyperledger Iroha εισάγει ένα νέο αλγόριθμο βασισμένο στο BFT, τον Sumeragi, στο οποίο οι διαδικασίες των συναλλαγών ολοκληρώνονται σε δευτερόλεπτα. Τέλος, το Hyperledger Sawtooth χρησιμοποιεί τον αλγόριθμο Proof of Elapsed Time, που έχουμε αναλύσει σε προηγούμενο κεφάλαιο. (Hyperledger, 2017)

2.2.2 Smart contracts

Οι χρήστες του Hyperledger Fabric χρησιμοποιούν συχνά τους όρους smart contract και chaincode εναλλακτικά. Σε γενικές γραμμές, ένα έξυπνο συμβόλαιο ορίζει τη λογική συναλλαγής που ελέγχει τον κύκλο ζωής ενός επιχειρησιακού αντικειμένου. Στη συνέχεια ταξινομείται σε αλυσιδωτή μορφή (chaincode) και ο αλυσιδωτός κώδικας αξιοποιείται από το δίκτυο. Καταλαβαίνουμε λοιπόν, ότι τα smart contracts ορίζουν τον τρόπο με το οποίο γίνονται οι συναλλαγές ενώ το chaincode τον τρόπο με τον οποίο ταξινομούνται τα smart contracts για την αξιοποίησή τους. Ας κατανοήσουμε καλύτερα αυτή τη λογική με ένα παράδειγμα.



Εικόνα 8 Vehicle chaincode Diagram

Στο διάγραμμα (εικόνα 8) μπορούμε να δούμε έναν αλυσιδωτό κωδικό οχήματος που περιέχει τρία έξυπνα συμβόλαια: αυτοκίνητα, σκάφη και φορτηγά. Μια έξυπνη σύμβαση ορίζεται σε έναν αλυσιδωτό κωδικό. Πολλαπλές έξυπνες συμβάσεις μπορούν να οριστούν μέσα στον ίδιο αλυσιδωτό κωδικό. Όταν αναπτύσσεται ένας αλυσιδωτός κώδικας, όλα τα έξυπνα συμβόλαια μέσα σε αυτόν διατίθενται σε εφαρμογές. Ένα έξυπνο συμβόλαιο είναι ένα πρόγραμμα συγκεκριμένου τομέα που σχετίζεται με συγκεκριμένες επιχειρησιακές διαδικασίες, ενώ ένας αλυσωτός κώδικας είναι ένα τεχνικό container μιας ομάδας σχετικών έξυπνων συμβολαίων για εγκατάσταση και δημιουργία παραδειγμάτων. (Hyperledger Fabric, 2019)

2.2.3 Πρόσθετες έννοιες

Ledger

Το ledger στο Fabric περιέχει την τρέχουσα κατάσταση μιας επιχείρησης ως ημερολόγιο συναλλαγών. Ένα ledger δεν αποθηκεύει κυριολεκτικά επιχειρησιακά αντικείμενα, αλλά αποθηκεύει δεδομένα για αυτά τα αντικείμενα. Όταν λέμε ότι «αποθηκεύουμε ένα επιχειρηματικό αντικείμενο σε ένα ledger» αυτό που πραγματικά εννοούμε είναι ότι καταγράφουμε τα γεγονότα σχετικά με την τρέχουσα κατάσταση ενός αντικειμένου και τα γεγονότα σχετικά με την ιστορία των συναλλαγών που οδήγησαν στην τρέχουσα κατάσταση. Στην περίπτωση ενός ψηφιακού αντικειμένου, είναι πιθανό ότι ζει σε ένα εξωτερικό datastore. Οι πληροφορίες που αποθηκεύουμε στο ledger μας επιτρέπουν να προσδιορίσουμε την τοποθεσία του μαζί με άλλα βασικά χαρακτηριστικά για αυτό. Ενώ τα γεγονότα σχετικά με την τρέχουσα κατάσταση ενός επιχειρηματικού αντικειμένου μπορεί να αλλάξουν, το ιστορικό των γεγονότων γι' αυτό είναι αμετάβλητο, μπορεί να προστεθεί, αλλά δεν μπορεί να αλλάξει αναδρομικά.

Ένα ledger αποτελείται από δύο ξεχωριστά, αν και σχετικά μέρη, μια World state και ένα Transaction log. Κάθε ένα από αυτά αντιπροσωπεύει ένα σύνολο γεγονότων σχετικά με ένα σύνολο επιχειρηματικών αντικειμένων.

Η World state αποτελεί μια βάση δεδομένων που κρατά μια κρυφή μνήμη των τρεχουσών τιμών ενός συνόλου καταστάσεων. Η World state καθιστά εύκολο για ένα πρόγραμμα να αποκτήσει άμεση πρόσβαση στην τρέχουσα τιμή μιας κατάστασης αντί να το ψάξει διαβάζοντας ολόκληρο το αρχείο καταγραφής συναλλαγών. Οι καταστάσεις ενός ledger εκτυπώνονται ως ζεύγη κλειδιών-τιμών. Η World state μπορεί να αλλάζει συχνά, καθώς οι καταστάσεις μπορούν να δημιουργηθούν, να ενημερωθούν και να διαγραφούν.

Ένα Transaction log είναι ένα αρχείο καταγραφής συναλλαγών που καταγράφει όλες τις αλλαγές που έχουν οδηγήσει στη σημερινή World state. Οι συναλλαγές συλλέγονται μέσα σε μπλοκ που είναι προσαρτημένα στο blockchain, επιτρέποντάς την προβολή του ιστορικού των αλλαγών που έχουν οδηγήσει στην τρέχουσα world state. Η δομή δεδομένων blockchain σε αντίθεση με την World state, είναι αμετάβλητη. (Hyperledger Fabric, 2019)

Membership Service Provider (MSP)

Επειδή το Fabric βασίζεται στο permissioned blockchain, επιτρέπει την πρόσβαση μόνο στα εξουσιοδοτημένα μέλη και περιορίζει οποιονδήποτε να συνδεθεί στο δίκτυο, να έχει πρόσβαση στα δεδομένα του ledger ή να επιτελέσει μια συναλλαγή. Οι υπηρεσίες Membership Service Provider (MSP) εκδίδουν τα πιστοποιητικά εγγραφής και συναλλαγής που απαιτούνται για την πρόσβαση στο ledger. Αναλυτικά, οι υπηρεσίες αυτές διαχωρίζονται σε τοπικές (local ή peer ή orderer) που αφορούν το επίπεδο των μελών, σε καναλιών (channel) οι οποίες αφορούν το επίπεδο καναλιού και σε δικτύων (network) που αφορούν το επίπεδο δικτύου.

Οι τοπικές υπηρεσίες MSP προσδιορίζουν ποιες αρχικές και ενδιάμεσες Certificate Authorities (CAs) είναι αξιόπιστες για να καθορίσουν εμπιστοσύνη ανάμεσα στα μέλη, όπως σε έναν οργανισμό. Ο προσδιορισμός γίνεται είτε με καταγραφή των ταυτοτήτων των μελών είτε με καθορισμό ποιών CAs έχουν εξουσιοδοτηθεί να εκδίδουν έγκυρες ταυτότητες για τα μέλη τους είτε με συνδυασμό και των δύο τρόπων. Παράλληλα, μια τοπική MSP εντοπίζει συγκεκριμένους ρόλους για κάθε μέλος του δικτύου και ορίζει τα προνόμια πρόσβασης και αλληλεπίδρασης με τα δεδομένα στο πλαίσιο του δικτύου. Με αυτό τον τρόπο πιστοποιείται η ταυτότητα αλλά και οι ρόλοι των μελών στο blockchain δίκτυο.

Οι channel MSP ορίζουν τα διοικητικά και συμμετοχικά δικαιώματα σε επίπεδο καναλιού. Κάθε οργανισμός πρέπει να έχει οριστεί από ένα τοπικό MSP και οι peers και οι orderers που συμμετέχουν στο ίδιο κανάλι θα πρέπει να μοίραζονται ένα κοινό channel MSP ώστε να είναι σε θέση να πιστοποιήσουν ορθά όλους τους συμμετέχοντες στο κανάλι. Δηλαδή, κάθε οργανισμός που επιθυμεί να ενταχθεί σε ένα κανάλι θα πρέπει να συμπεριληφθεί στο channel MSP ώστε να ενσωματωθεί στην αλυσίδα εμπιστοσύνης των υπόλοιπων μελών. Διαφορετικά, οι συναλλαγές που θα προέρχονται από την ταυτότητα αυτού του οργανισμού θα απορριφθούν.

Το network MSP ορίζει ποιοι είναι οι συμμετέχοντες στο δίκτυο, που όπως έχουμε αναφέρει είναι ένα σύνολο καναλιών. Επίσης ορίζει ποιά μέλη είναι εξουσιοδοτημένα να εκτελούν διοικητικές εργασίες όπως η δημιουργία ενός καναλιού. (Hyperledger Fabric, 2019)

2.3 Εγκατάσταση Hyperledger σε αυτόνομο περιβάλλον

2.3.1 Βήματα

Για την υλοποίηση του Hyperledger Fabric σε ένα μηχάνημα κάναμε χρήση του εύκολου εργαλείου Hyperledger Composer. Για το συγκεκριμένο αναπτυξιακό περιβάλλον χρειάστηκε να εγκαταστήσουμε διάφορα εργαλεία. Ξεκινώντας από ένα εγκατεστημένο εικονικό μηχάνημα με λειτουργικό σύστημα Linux Ubuntu 16.04 or 18.04 LTS (64bit) που η εγκατάσταση θα περιγραφεί στο παράρτημα 1, εγκαθιστούμε τα εξής προαπαιτούμενα:

- Docker Engine: Version 17.03 ή μεγαλύτερο
- Docker-Compose: Version 1.8 ή μεγαλύτερο
- Node: 8.9 ή μεγαλύτερο (το version 9 δεν υποστηρίζεται)
- npm: v5.x
- git: 2.9.x ή μεγαλύτερο
- Την προγραμματιστική γλώσσα Python: 2.7.x
- Go Language

Σύμφωνα με την επίσημη σελίδα του Hyperledger Composer (Hyperledger Composer , 2019) τα προαπαιτούμενα μπορούν να εγκατασταθούν, αν δουλεύουμε σε Linux σύστημα με τις εξής εντολές στο command line:

```
curl -O https://hyperledger.github.io/composer/v0.19/prereqs-ubuntu.sh
```

για λήψη του script αρχείου που εγκαθιστά τα εργαλεία

```
chmod u+x prereqs-ubuntu.sh
```

για ενεργοποίηση των δικαιωμάτων εκτέλεσης του script

```
./prereqs-ubuntu.sh
```

και εκτέλεση του script (.sh)

Σε περίπτωση που υπάρξει πρόβλημα παραθέτουμε στο παράρτημα 2 όλες τις οδηγίες για την εγκατάσταση όλων των εργαλείων, το καθένα ξεχωριστά.

Εκτός από τα προαπαιτούμενα είναι απαραίτητη και η εγκατάσταση των βασικών στοιχείων του Hyperledger Composer που είναι τα CLI εργαλεία:

- composer-cli, το οποίο περιέχει όλες τις βασικές λειτουργίες του composer και η εντολή εγκατάστασης είναι:

```
npm install -g composer-cli@0.19
```

- generator-hyperledger-composer, που χρησιμοποιείται για τη δημιουργία assets στο πρόγραμμά μας

```
npm install -g composer-rest-server@0.19
```

- composer-rest-server, που αποτελεί βοηθητικό πρόγραμμα για την εκτέλεση ενός διακομιστή REST στο μηχανήμά σας για να εκθέσετε τα δίκτυα των επιχειρήσεων σας ως RESTful API

```
npm install -g generator-hyperledger-composer@0.19
```

- Yeoman, είναι ένα εργαλείο για τη δημιουργία εφαρμογών, το οποίο χρησιμοποιεί το generator-hyperledger-composer

```
npm install -g yo
```

Σημειώνουμε ότι δεν πρέπει να τρέξουμε τις προηγούμενες εντολές με su ή sudo αλλά ως απλός χρήστης.

Για την εγκατάσταση του GUI Playground μπορούμε να τρέξουμε την εντολή:

```
npm install -g composer-playground@0.19
```

Για την εγκατάσταση του Hyperledger Fabric, δηλαδή των απαιτούμενων βιβλιοθηκών και εργαλείων του, δημιουργούμε ένα φάκελο και πηγαίνουμε στα περιεχόμενά του, κατεβάζουμε το συμπιεσμένο αρχείο με κατάληξη .tar.gz και το αποσυμπιέζουμε:

```
mkdir fabric-dev-servers && cd ~/fabric-dev-servers  
curl -O https://raw.githubusercontent.com/hyperledger/composer-tools/master/packages/fabric-dev-servers/fabric-dev-servers.tar.gz  
tar -xvf fabric-dev-servers.tar.gz
```

Προσέχουμε ώστε να τρέξουμε αυτές τις τρεις εντολές όλες μαζί.

Χρησιμοποιούμε τα scripts αρχεία που μόλις κατεβάσαμε για να καταβάσουμε το τοπικό Hyperledger Fabric v1.1 runtime:

```
cd ~/fabric-dev-servers  
export FABRIC_VERSION=hlfv12  
./downloadFabric.sh
```

Την πρώτη φορά που ξεκινάμε ένα νέο runtime, πρέπει να εκτελέσουμε το start script και στην συνέχεια να παράγουμε ένα PeerAdmin Card:

```
cd ~/fabric-dev-servers  
export FABRIC_VERSION=hlfv12  
./startFabric.sh
```



```
./createPeerAdminCard.sh
```

Το αποτέλεσμα της τελευταίας εντολής πρέπει να είναι:

```
Successfully imported business network card
Card file: /tmp/PeerAdmin@hlfv1.card
Card name: PeerAdmin@hlfv1

Command succeeded

The following Business Network Cards are available:

Connection Profile: hlfv1
```

Card Name	UserId	Business Network
PeerAdmin@hlfv1	PeerAdmin	

```
Issue composer card list --card <Card Name> to get details a specific card

Command succeeded

Hyperledger Composer PeerAdmin card has been imported, host of fabric specified as 'localhost'
```

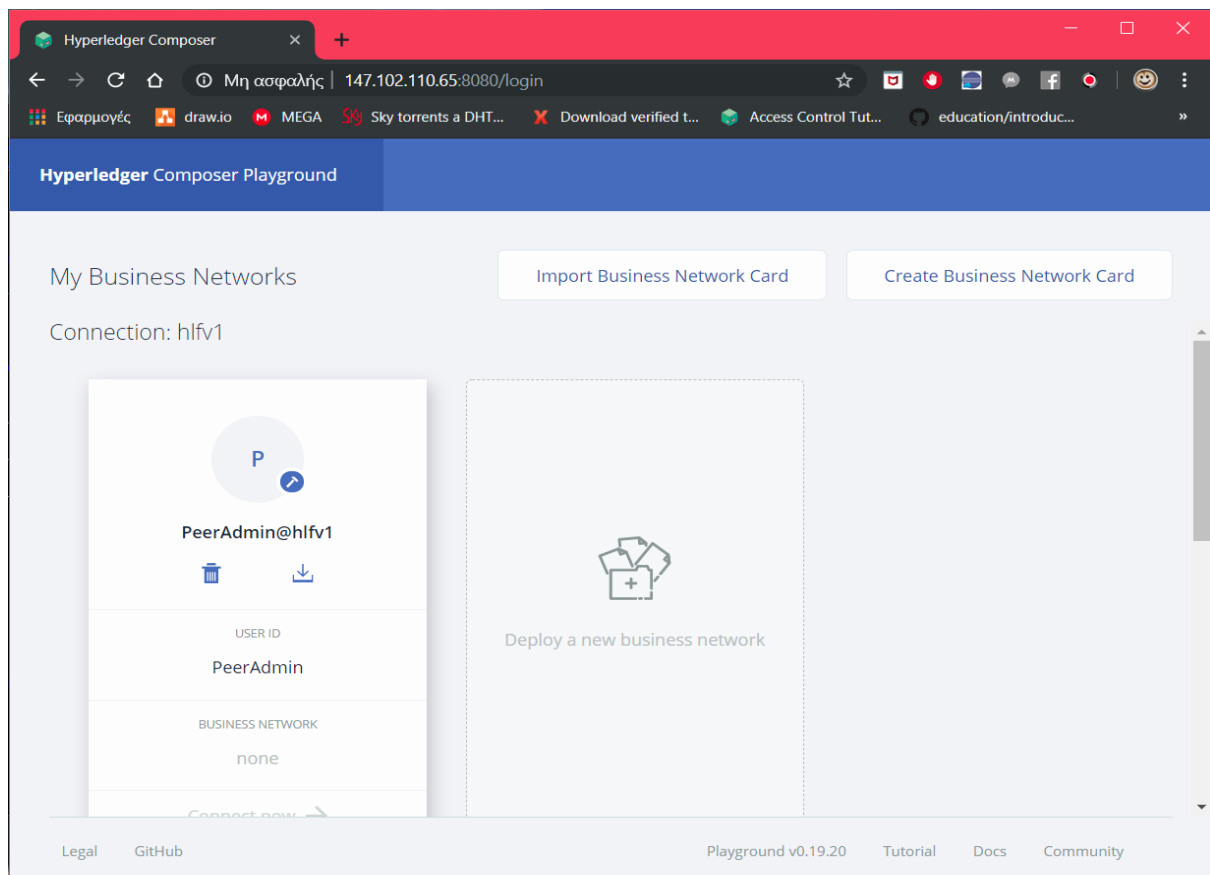
Για να εκκινήσουμε την Web εφαρμογή Playground αρκεί να τρέξουμε την εντολή:

```
composer-playground
```

Για να δούμε τη σελίδα που έχει δημιουργηθεί ανοίγουμε το browser μας και γράφουμε το εξής link:

<http://<ip-του virtual machine>:8080/login>

Στην σελίδα αυτή θα πρέπει να βλέπουμε το PeerAdmin@hlfv1 Card που έχουμε δημιουργήσει με το script createPeerAdminCard. Σε περίπτωση που δεν εμφανίζεται η προαναφερόμενη κάρτα στην σελίδα, σημαίνει ότι κάτι δεν έχει εγκατασταθεί σωστά.



Τώρα, που έχουμε ολοκληρώσει την εγκατάσταση του Hyperledger Composer οικοσυστήματος, ξεκινάμε να δημιουργήσουμε ένα επιχειρησιακό δίκτυο (business network) στο οποίο θα συμμετέχουν δύο οργανισμοί, το δίκτυο αυτό θα τρέχει σε δικό του container (περιβάλλον προγραμματισμού) και στην συνέχεια θα κοινοποιηθεί σε ένα κοινό ledger που θα έχουν πρόσβαση και οι δύο οργανισμοί.

Δημιουργία business network

Καρταρχήν, δημιουργούμε ένα σκελετό του business network με τη βοήθεια του εργαλείου Yeoman:

```
yo hyperledger-composer:businessnetwork
```

Και συμπληρώνουμε τα παρακάτω πεδία:

```
Welcome to the business network generator
? Business network name: tutorial-network
? Description: my first network
? Author name: orguser
? Author email: orguser@gmail.com
? License: Apache-2.0
? Namespace: org.example.mynetwork
? Do you want to generate an empty template network? No: generate a populated sample network
```

Στην συνέχεια, ορίζουμε το αρχιτεκτονικό μοντέλο που θέλουμε να έχει το δίκτυό μας, δηλαδή τα assets, participants και transactions.

Ανοίγουμε το αρχείο `org.example.mynetwork.cto` και αντικαθιστούμε το περιεχόμενο με τις παρακάτω εντολές:

```
/**
 * My commodity trading network
 */
namespace org.example.mynetwork
asset Commodity identified by tradingSymbol {
  o String tradingSymbol
  o String description
  o String mainExchange
  o Double quantity
  --> Trader owner }
participant Trader identified by tradeId {
  o String tradeId
  o String firstName
  o String lastName }
transaction Trade {
  --> Commodity commodity
  --> Trader newOwner}
```

Ακολουθούν, τα υπόλοιπα αρχεία, στα οποία αντικαθιστούμε τα αντίστοιχα παρακάτω περιεχόμενα.

Το `logic.js`:

```
/**
 * Track the trade of a commodity from one trader to another
 * @param {org.example.mynetwork.Trade} trade - the trade to be processed
 * @transaction
 */
async function tradeCommodity(trade) {
```

```
trade.commodity.owner = trade.newOwner;

let assetRegistry = await getAssetRegistry('org.example.mynetwork.Commodity');

await assetRegistry.update(trade.commodity); }
```

To permissions.acl:

```
/**
 * Access control rules for tutorial-network
 */
rule Default {
  description: "Allow all participants access to all resources"
  participant: "ANY"
  operation: ALL
  resource: "org.example.mynetwork.*"
  action: ALLOW}
rule SystemACL {
  description: "System ACL to permit all access"
  participant: "ANY"
  operation: ALL
  resource: "org.hyperledger.composer.system.*"
  action: ALLOW }
```

Σε όλα τα αρχεία αποθηκεύουμε τις αλλαγές.

Τέλος, μεταφερόμαστε στα περιεχόμενα του tutorial-network υποφακέλου, που έχει δημιουργηθεί και δημιουργούμε το τελικό αρχείο με το business network, το [tutorial-network@0.0.1.bna](#), με την εντολή:

```
composer archive create -t dir -n
```

```
Found:
  Description: my first network
  Name: tutorial-network
  Identifier: tutorial-network@0.0.1

Written Business Network Definition Archive file to
  Output file: tutorial-network@0.0.1.bna

Command succeeded
```

Ανάπτυξη του business network για δύο οργανισμούς

Τρέχουμε τις επόμενες εντολές για να διαγράψουμε τυχόν προηγούμενα Composer περιβάλλοντα:

```
cd ~/fabric-dev-servers
export FABRIC_VERSION=hlfv12
./stopFabric.sh
./teardownFabric.sh
```

Στην συνέχεια, αντιγράφουμε από το github.com το repository fabric-samples.git

```
git clone https://github.com/mahoney1/fabric-samples.git
```

Μεταφερόμαστε στο φάκελο αυτό και τρέχουμε την παρακάτω εντολή για να έχουμε στο περιβάλλον μας τις βιβλιοθήκες του Hyperledger Fabric:

```
curl -sSL http://bit.ly/2ysbOFE | bash -s 1.2.1 1.2.1 0.4.10
```

Μόλις ολοκληρωθεί η εγκατάσταση τρέχουμε την εντολή:

```
git checkout multi-org
```

για να χρησιμοποιήσουμε την έκδοση multi-org από τα αρχεία στο github.com

Στην συνέχεια μεταφερόμαστε στο φάκελο first-network και τρέχουμε τις εντολές:

```
cd first-network
./byfn.sh -m generate
./byfn.sh -m up -s couchdb -a
```

Ωστε να ξεκινήσει το default BYFN δίκτυο και μάλιστα και με την χρήση της βάσης CouchDB.

Το αποτέλεσμα πρέπει να είναι:

```
===== Query successful on peer1.org2 on channel 'mychannel' =====  
===== All GOOD, BYFN execution completed =====  
  
END
```

Επόμενο βήμα, διαγράφουμε τυχόν προηγούμενες κάρτες που έχουμε δημιουργήσει:

```
composer card delete -c PeerAdmin@byfn-network-org1  
composer card delete -c PeerAdmin@byfn-network-org2  
composer card delete -c alice@trade-network  
composer card delete -c bob@trade-network  
composer card delete -c admin@trade-network  
composer card delete -c PeerAdmin@fabric-network
```

Χρησιμοποιούμε τα αρχεία με τις άδειες (CAs) που υπάρχουν στις εξής τοποθεσίες:

Για το κόμβο του orderer και τους άλλους δύο οργανισμούς:

crypto-config/ordererOrganizations/example.com/orderers/orderer.example.com/tls/ca.crt

crypto-config/peerOrganizations/org1.example.com/peers/peer0.org1.example.com/tls/ca.crt

crypto-config/peerOrganizations/org2.example.com/peers/peer0.org2.example.com/tls/ca.crt

Επίσης τις τοποθεσίες για τα δημόσια και ιδιωτικά κλειδιά:

crypto-config/peerOrganizations/org1.example.com/users/Admin@org1.example.com/msp

crypto-config/peerOrganizations/org2.example.com/users/Admin@org2.example.com/msp

Για να τα αξιοποιήσουμε κατάλληλα, δημιουργούμε ένα composer φάκελο στο ήδη υπάρχον temp φάκελο του συστήματός μας και δύο υποφακέλους για τους δύο οργανισμούς με τις εντολές:

```
mkdir -p /tmp/composer/org1  
mkdir -p /tmp/composer/org2
```

Στην συνέχεια δημιουργούμε ένα αρχείο byfn-network.json το οποίο θα περιγράφει τη πρόσβαση των δύο οργανισμών στο δίκτυο και θα περιλαμβάνει:

```
{
```

```
"name": "byfn-network",
"x-type": "hlfv1",
"version": "1.0.0",
"channels": {
  "mychannel": {
    "orderers": [
      "orderer.example.com"
    ],
    "peers": {
      "peer0.org1.example.com": {
        "endorsingPeer": true,
        "chaincodeQuery": true,
        "eventSource": true
      },
      "peer1.org1.example.com": {
        "endorsingPeer": true,
        "chaincodeQuery": true,
        "eventSource": true
      },
      "peer0.org2.example.com": {
        "endorsingPeer": true,
        "chaincodeQuery": true,
        "eventSource": true
      },
      "peer1.org2.example.com": {
        "endorsingPeer": true,
        "chaincodeQuery": true,
        "eventSource": true
      }
    }
  }
}
```

```

    }
  },
  "organizations": {
    "Org1": {
      "mspid": "Org1MSP",
      "peers": [
        "peer0.org1.example.com",
        "peer1.org1.example.com"
      ],
      "certificateAuthorities": [
        "ca.org1.example.com"
      ]
    },
    "Org2": {
      "mspid": "Org2MSP",
      "peers": [
        "peer0.org2.example.com",
        "peer1.org2.example.com"
      ],
      "certificateAuthorities": [
        "ca.org2.example.com"
      ]
    }
  },
  "orderers": {
    "orderer.example.com": {
      "url": "grpc://localhost:7050",
      "grpcOptions": {
        "ssl-target-name-override": "orderer.example.com"
      },

```



```

        "tlsCACerts": {
            "pem": "INSERT_ORDERER_CA_CERT"
        }
    },
    "peers": {
        "peer0.org1.example.com": {
            "url": "grpcs://localhost:7051",
            "grpcOptions": {
                "ssl-target-name-override": "peer0.org1.example.com"
            },
            "tlsCACerts": {
                "pem": "INSERT_ORG1_CA_CERT"
            }
        },
        "peer1.org1.example.com": {
            "url": "grpcs://localhost:8051",
            "grpcOptions": {
                "ssl-target-name-override": "peer1.org1.example.com"
            },
            "tlsCACerts": {
                "pem": "INSERT_ORG1_CA_CERT"
            }
        },
        "peer0.org2.example.com": {
            "url": "grpcs://localhost:9051",
            "grpcOptions": {
                "ssl-target-name-override": "peer0.org2.example.com"
            },
            "tlsCACerts": {

```

```

        "pem": "INSERT_ORG2_CA_CERT"
    }
},
"peer1.org2.example.com": {
    "url": "grpc://localhost:10051",
    "grpcOptions": {
        "ssl-target-name-override": "peer1.org2.example.com"
    },
    "tlsCACerts": {
        "pem": "INSERT_ORG2_CA_CERT"
    }
}
},
"certificateAuthorities": {
    "ca.org1.example.com": {
        "url": "https://localhost:7054",
        "caName": "ca-org1",
        "httpOptions": {
            "verify": false
        }
    },
    "ca.org2.example.com": {
        "url": "https://localhost:8054",
        "caName": "ca-org2",
        "httpOptions": {
            "verify": false
        }
    }
}
}
}

```

Στο αρχείο αυτό πρέπει στις εντολές : INSERT_ORG1_CA_CERT,

INSERT_ORG2_CA_CERT, INSERT_ORDERER_CA_CERT να προστεθούν τα CAs που βρίσκονται στις προηγούμενες τοποθεσίες. Για να γίνει όμως ορθά και με ασφάλεια να μην χαθούν αυτά τα αρχεία, πρέπει να αντιγραφούν σε μορφή .txt αυτό γίνεται με τις εντολές:

```
awk 'NF {sub(/\r/, ""); printf "%s\\n",$0;}' crypto-config/peerOrganizations/org1.example.com/peers/peer0.org1.example.com/tls/ca.crt > /tmp/composer/org1/ca-org1.txt
awk 'NF {sub(/\r/, ""); printf "%s\\n",$0;}' crypto-config/peerOrganizations/org2.example.com/peers/peer0.org2.example.com/tls/ca.crt > /tmp/composer/org2/ca-org2.txt
awk 'NF {sub(/\r/, ""); printf "%s\\n",$0;}' crypto-config/ordererOrganizations/example.com/orderers/orderer.example.com/tls/ca.crt > /tmp/composer/ca-orderer.txt
```

Από αυτά τα αρχεία που βρίσκονται πλέον στους φακέλους: /tmp/composer/org1, /tmp/composer/org2 και /tmp/composer/ αντίστοιχα μπορούμε πλέον να αντιγράψουμε τα περιεχόμενα στις αντίστοιχες εντολές στο byfn-network.json αρχείο.

Στη συνέχεια, δημιουργούμε δύο αντίγραφα του byfn-network.json αρχείου με ονόματα:

byfn-network-org1.json, byfn-network-org2.json, μέσα στους αντίστοιχους υποφακέλους και μέσα στα νέα αρχεία ανάμεσα στις εντολές του «version» και «channel» προσθέτουμε τις παρακάτω εντολές, ώστε η τελική μορφή τους να είναι:

Για το byfn-network-org1.json:

```
...
"version": "1.0.0",
"client": {
  "organization": "Org1",
  "connection": {
    "timeout": {
      "peer": {
        "endorser": "300",
        "eventHub": "300",
        "eventReg": "300"
      },
      "orderer": "300"
    }
  }
}
```

```
}  
},  
"channel": {  
...  
}
```

Ενώ για το byfn-network-org2.json:

```
...  
"version": "1.0.0",  
"client": {  
  "organization": "Org2",  
  "connection": {  
    "timeout": {  
      "peer": {  
        "endorser": "300",  
        "eventHub": "300",  
        "eventReg": "300"  
      },  
      "orderer": "300"  
    }  
  }  
},  
"channel": {  
...  
}
```

Τέλος πρέπει στους δύο φακέλους να προστεθούν τα κλειδιά για τους δύο οργανισμούς με τις εντολές:

Για τον πρώτο οργανισμό:

```
export ORG1=crypto-config/peerOrganizations/org1.example.com/users/Admin@org1.example.com/msp
```

```
cp -p $ORG1/signcerts/A*.pem /tmp/composer/org1
cp -p $ORG1/keystore/*_sk /tmp/composer/org1
```

Για τον δεύτερο οργανισμό:

```
export ORG2=crypto-config/peerOrganizations/org2.example.com/users/Admin@org2.example.com/msp
cp -p $ORG2/signcerts/A*.pem /tmp/composer/org2
cp -p $ORG2/keystore/*_sk /tmp/composer/org2
```

Ολοκληρώνονται αυτές τις ρυθμίσεις, τρέχουμε τις παρακάτω εντολές για να δημιουργήσουμε τις composer κάρτες, που δηλώνουν τα προφίλ των δύο οργανισμών στο δίκτυο.

```
composer card create -p /tmp/composer/org1/byfn-network-org1.json -u PeerAdmin -c /tmp/composer/org1/Admin@org1.example.com-cert.pem -k /tmp/composer/org1/*_sk -r PeerAdmin -r ChannelAdmin -f PeerAdmin@byfn-network-org1.card
composer card create -p /tmp/composer/org2/byfn-network-org2.json -u PeerAdmin -c /tmp/composer/org2/Admin@org2.example.com-cert.pem -k /tmp/composer/org2/*_sk -r PeerAdmin -r ChannelAdmin -f PeerAdmin@byfn-network-org2.card
```

Και τις εισάγουμε στο composer wallet⁷, για να μπορούν να χρησιμοποιηθούν αργότερα από το δίκτυο:

```
composer card import -f PeerAdmin@byfn-network-org1.card --card PeerAdmin@byfn-network-org1
composer card import -f PeerAdmin@byfn-network-org2.card --card PeerAdmin@byfn-network-org2
```

Εγκαθιστούμε τις κάρτες στο δίκτυο που έχουμε δημιουργήσει, η εντολή μπορεί να θέλει αλλαγή με το όνομα του αρχείου .bna που έχουμε δημιουργήσει (φυσικά το αρχείο αυτό πρέπει να υπάρχει στο φάκελο που τρέχουμε αυτές τις εντολές, αν βρίσκεται αλλού το αντιγράφουμε):

⁷ Το wallet είναι ένας κατάλογος στο σύστημα αρχείων που περιέχει κάρτες επιχειρηματικών δικτύων.

```
composer network install --card PeerAdmin@byfn-network-org1 --archiveFile trade-  
network.bna  
  
composer network install --card PeerAdmin@byfn-network-org2 --archiveFile trade-  
network.bna
```

Αποτέλεσμα των εντολών αυτών είναι:

```
testuser@test:~/fabric-dev-servers/fabric-samples/first-network$ composer network install --card PeerAdmin@byfn-network-  
org1 --archiveFile trade-network@0.0.1.bna  
[i] Installing business network. This may take a minute...  
Successfully installed business network trade-network, version 0.0.1  
  
Command succeeded  
  
testuser@test:~/fabric-dev-servers/fabric-samples/first-network$ composer network install --card PeerAdmin@byfn-network-  
org2 --archiveFile trade-network@0.0.1.bna  
[i] Installing business network. This may take a minute...  
Successfully installed business network trade-network, version 0.0.1  
  
Command succeeded
```

Έπειτα, ορίζουμε τα δικαιώματα που θα έχει κάθε οργανισμός στο δίκτυο στο αρχείο endorsement-policy.json, δημιουργούμε λοιπόν αυτό το αρχείο στο φάκελο /tmp/composer/ και προσθέτουμε τα παρακάτω:

```
{  
  "identities": [  
    {  
      "role": {  
        "name": "member",  
        "mspld": "Org1MSP"  
      }  
    },  
    {  
      "role": {  
        "name": "member",  
        "mspld": "Org2MSP"  
      }  
    }  
  ],  
}
```

```
"policy": {  
  "2-of": [  
    {  
      "signed-by": 0  
    },  
    {  
      "signed-by": 1 }] } }
```

Και τρέχουμε τις παρακάτω εντολές για να ανακτήσουμε τις άδειες των δύο οργανισμών και να δώσουμε μια ταυτότητα στους διαχειριστές (στο σημείο αυτό μπορούμε να βάλουμε όποιο όνομα θέλουμε):

```
composer identity request -c PeerAdmin@byfn-network-org1 -u admin -s adminpw -d  
alice  
composer identity request -c PeerAdmin@byfn-network-org2 -u admin -s adminpw -d  
bob
```

Εγκατάσταση των οργανισμών στο δίκτυο.

Ξεκινάμε το δίκτυο με την εντολή:

```
composer network start -c PeerAdmin@byfn-network-org1 -n trade-network -V 0.0.1 -o  
endorsementPolicyFile=/tmp/composer/endorsement-policy.json -A alice -C alice/ad-  
min-pub.pem -A bob -C bob/admin-pub.pem
```

```
testuser@test:~/fabric-dev-servers/fabric-samples/first-network$ composer network
n trade-network -V 0.0.1 -o endorsementPolicyFile=/tmp/composer/endorsement-pol
-A bob -C bob/admin-pub.pem
Starting business network trade-network at version 0.0.1

Processing these Network Admins:
    userName: alice
    userName: bob

Starting business network definition. This may take a minute...
Successfully created business network cards:
    Filename: alice@trade-network.card
    Filename: bob@trade-network.card

Command succeeded
```

Δημιουργούμε κάρτες του δικτύου trade-network και τις προσθέτουμε στο δίκτυο:

Για τον πρώτο οργανισμό:

```
composer card create -p /tmp/composer/org1/byfn-network-org1.json -u alice -n trade-
network -c alice/admin-pub.pem -k alice/admin-priv.pem

composer card import -f alice@trade-network.card

composer network ping -c alice@trade-network
```

```
testuser@test:~/fabric-dev-servers/fabric-samples/first-network$ composer network ping -c alice@trade-network
The connection to the network was successfully tested: trade-network
    Business network version: 0.0.1
    Composer runtime version: 0.20.9
    participant: org.hyperledger.composer.system.NetworkAdmin#alice
    identity: org.hyperledger.composer.system.Identity#54923602c0058dc957d782d043a9df8700235e72257317225fb9c

Command succeeded
```

Για να προσθέσουμε ένα νέο συμμετέχοντα με όνομα Jo Doe, τρέχουμε την εντολή:

```
composer participant add -c alice@trade-network -d '{"$class":"org.example.mynet-
work.Trader","tradelid":"trader1-org1", "firstName":"Jo","lastName":"Doe"}'

composer identity issue -c alice@trade-network -f jo.card -u jdoe -a "resource:org.ex-
ample.mynetwork.Trader#trader1-org1"
```

Το αποτέλεσμα είναι:


```
testuser@test:~/fabric-dev-servers/fabric-samples/first-network$ composer identity issue -c
ce@trade-network -f jo.card -u jdoe -a "resource:org.example.mynetwork.Trader#trader1-org1"
Issue identity and create Network Card for: jdoe

❏ Issuing identity. This may take a few seconds...

Successfully created business network card file to
    Output file: jo.card

Command succeeded
```

```
composer card import -f jo.card
composer network ping -c jdoe@trade-network
```

Τώρα, δημιουργούμε ένα asset:

```
composer transaction submit --card jdoe@trade-network -d '{"$class": "org.hyperledger.composer.system.AddAsset", "targetRegistry" : "resource:org.hyperledger.composer.system.AssetRegistry#org.example.mynetwork.Commodity", "resources": [{"class": "org.example.mynetwork.Commodity", "tradingSymbol": "EMA", "description": "Corn commodity", "mainExchange": "EURONEXT", "quantity": "10", "owner": "resource:org.example.mynetwork.Trader#trader1-org1"}]}'
```

Τέλος, τρέχουμε την παρακάτω εντολή για να επιβεβαιώσουμε τα παραγόμενα στοιχεία που δημιουργήσαμε.

```
composer network list -c jdoe@trade-network
```

Το αποτέλεσμα αυτή της εντολής είναι:

```

scripts:
- lib/logic.js
registries:
  org.example.mynetwork.Commodity:
    id: org.example.mynetwork.Commodity
    name: Asset registry for org.example.mynetwork.Commodity
    registryType: Asset
    assets:
      EMA:
        $class: org.example.mynetwork.Commodity
        tradingSymbol: EMA
        description: Corn commodity
        mainExchange: EURONEXT
        quantity: 10
        owner: resource:org.example.mynetwork.Trader#trader1-org1
  org.example.mynetwork.Trader:
    id: org.example.mynetwork.Trader
    name: Participant registry for org.example.mynetwork.Trader
    registryType: Participant
    assets:
      trader1-org1:
        $class: org.example.mynetwork.Trader
        tradeId: trader1-org1
        firstName: Jo
        lastName: Doe

```

Για τον δεύτερο οργανισμό ομοίως:

```

composer card create -p /tmp/composer/org2/byfn-network-org2.json -u bob -n trade-
network -c bob/admin-pub.pem -k bob/admin-priv.pem
composer card import -f bob@trade-network.card
composer network ping -c bob@trade-network

```

Προσθέτουμε ένα νέο συμμετέχοντα με όνομα Dave Lowe:

```

composer participant add -c bob@trade-network -d '{"$class":"org.example.mynet-
work.Trader","tradeId":"trader2-org2", "firstName":"Dave","lastName":"Lowe"}'
composer identity issue -c bob@trade-network -f dave.card -u dlowe -a "re-
source:org.example.mynetwork.Trader#trader2-org2"
composer card import -f dave.card
composer network ping -c dlowe@trade-network

```

Και πραγματοποιούμε μια συναλλαγή, αλλάζοντας την ιδιοκτησία του asset που φτιάξαμε προηγουμένως από τον Jo Doe στον Dave Lowe, με την εντολή:

```
composer transaction submit --card jdoe@trade-network -d '{"$class":"org.example.mynetwork.Trade","commodity":"resource:org.example.mynetwork.Commodity#EMA","newOwner":"resource:org.example.mynetwork.Trader#trader2-org2"}'
composer network list -c dlowe@trade-network
```

Αντίστοιχα, το αποτέλεσμα είναι:

```
- lib/logic.js
registries:
  org.example.mynetwork.Commodity:
    id: org.example.mynetwork.Commodity
    name: Asset registry for org.example.mynetwork.Commodity
    registryType: Asset
    assets:
      EMA:
        $class: org.example.mynetwork.Commodity
        tradingSymbol: EMA
        description: Corn commodity
        mainExchange: EURONEXT
        quantity: 10
        owner: resource:org.example.mynetwork.Trader#trader2-org2
  org.example.mynetwork.Trader:
    id: org.example.mynetwork.Trader
    name: Participant registry for org.example.mynetwork.Trader
    registryType: Participant
    assets:
      trader1-org1:
        $class: org.example.mynetwork.Trader
        tradeId: trader1-org1
        firstName: Jo
        lastName: Doe
      trader2-org2:
        $class: org.example.mynetwork.Trader
        tradeId: trader2-org2
        firstName: Dave
        lastName: Lowe
Command succeeded
```

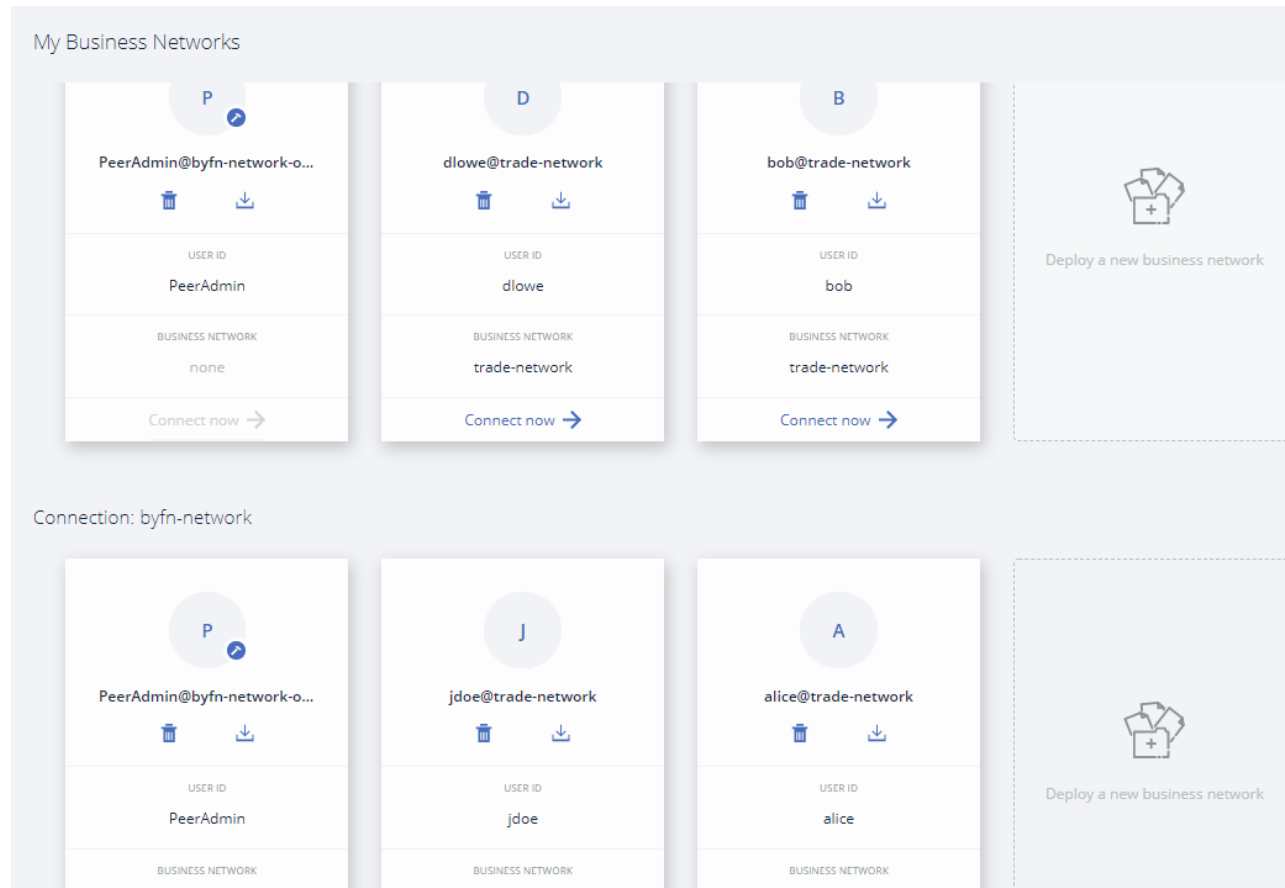
Φυσικά, μπορούμε να δούμε και τα αποτελέσματα, τρέχοντας την εντολή:

composer-playground

την οποία μπορούμε να τρέξουμε σε όποιο σημείο της διαδικασίας θέλουμε για να δούμε τι έχουμε δημιουργήσει και μεταβαίνουμε στην σελίδα:

`http://<ip του υπολογιστή>:8080`

Το αποτέλεσμα φαίνεται παρακάτω:



2.3.2 Σημεία που χρήζουν προσοχής

Το βασικότερο που πρέπει να προσέξουμε είναι οι εκδόσεις που ορίζουν οι οδηγίες εγκατάστασης των εργαλείων. Δεν πρέπει να παραλείψουμε αυτό το σημείο διότι στην συνέχεια παρουσιάζονται προβλήματα που δεν διορθώνονται εύκολα και δεν γνωρίζουμε ότι προκλήθηκαν λόγω των διαφορετικών εκδόσεων. Ακολουθώντας ακριβώς ότι αναφέρεται στις οδηγίες θα έχουμε λιγότερα προβλήματα.

Ένα ακόμη σημαντικό στοιχείο που διευκολύνει την όλη διαδικασία, αν τρέχουμε το Composer σε εικονικό μηχάνημα, είναι να κρατάμε στιγμιότυπα (εκδόσεις του μηχανήματός μας), ώστε αν κάνουμε κάποιο λάθος βήμα και δεν διορθώνεται, να γυρίσουμε σε μια προηγούμενη κατάσταση χωρίς να χρειάζεται να διαγράψουμε όλο το μηχάνημα και να το δημιουργήσουμε απο την αρχή.

Αν στην αρχή της εγκατάστασης των προαπαιτούμενων προκύψει το παρακάτω πρόβλημα:

```
Reading package lists... Done
E: Could not get lock /var/lib/apt/lists/lock - open (11: Resource temporarily unavailable)
E: Unable to lock directory /var/lib/apt/lists/
```

Τρέχουμε την εντολή (Prakash, 2019):

```
ps aux | grep -i apt
```

για να δούμε τι αποτέλεσμα θα βγάλει, αν βγεί:

```
root      25394  0.1  0.1  4504  636 ?        Ss   13:59   0:00 /bin/sh /usr/lib/apt/apt.systemd.daily update
root      25401  0.0  0.2  4504  1424 ?        S    13:59   0:00 /bin/sh /usr/lib/apt/apt.systemd.daily lock_is_held updat
ate
root      25435  0.7  1.7  61780  8832 ?        S    13:59   0:00 apt-get -qq -y update
root      25731  0.0  0.8  61780  4012 ?        S    14:00   0:00 apt-get -qq -y update
root      25749  62.7  6.1 117184 30116 ?        DN   14:00   0:37 /usr/bin/python3 /usr/lib/update-notifier/apt-check --h
uman-readable
orguser   25792  0.0  0.1  14224   960 pts/0    S+   14:01   0:00 grep --color=auto -i apt
orguser@org2:~$ lsof /var/lib/dpkg/lock-frontend
```

Τρέχουμε με την σειρά τις εντολές:

```
lsof /var/lib/dpkg/lock
lsof /var/lib/apt/lists/lock
lsof /var/cache/apt/archives/lock
```

Αν κάποια απο αυτές τις εντολές βγάλει αποτέλεσμα διαγράφουμε τις διαδικασίες με την εντολή:

```
sudo kill -9 «PID της διαδικασίας»
```

Στην συνέχεια τις εντολές:

```
sudo rm /var/lib/apt/lists/lock
sudo rm /var/cache/apt/archives/lock
sudo rm /var/lib/dpkg/lock
lsof /var/lib/dpkg/lock-frontend
sudo rm /var/lib/dpkg/lock-frontend
sudo dpkg --configure -a
```

Ολοκληρώνοντας τις εντολές αυτές ξαναεπαναλαμβάνουμε την εγκατάσταση των προαπαιτούμενων.

Επίσης, όταν τελειώσει χωρίς προβλήματα η εγκατάσταση κάνουμε logout και login και ελέγχουμε, αν έχουν εγκατασταθεί σωστά τα εργαλεία με τις παρακάτω εντολές:

```
docker version
docker-compose version
node -v
npm -v
git --version
go version
python --version
```

Γενικά, επειδή κάθε υπολογιστής ή εικονικό μηχάνημα έχει δικές του ρυθμίσεις και προβλήματα είναι λογικό να παρουσιάζονται σφάλματα και κάποιες εντολές να μην τρέχουν. Σε περίπτωση που βγεί ένα σφάλμα το οποίο δεν έχει εμφανιστεί στην παρούσα εργασία, αναζητήστε τη λύση στο ιστό της google, σίγουρα κάποιος θα έχει αντιμετωπίσει παρόμοιο σφάλμα.

Στην ανάπτυξη του business network σε δύο οργανισμούς καλό είναι να προηγηθεί η ανάπτυξη δικτύου για έναν οργανισμό που η επίσημη σελίδα του Composer περιγράφει αναλυτικά βήμα-βήμα την υλοποίηση του για πλήρη κατανόηση των μηχανισμών που χρησιμοποιούνται.

Επίσης, είναι σημαντικό πριν ξεκινήσετε την ανάπτυξη του δικτύου στους δύο οργανισμούς να έχετε ανοίξει τις πόρτες: 7050,7051,7053,7054,8051,8053,8054,9051,9053,10051,10053 που είναι απαραίτητες για την σύνδεση με τους default οργανισμούς: orderer.example.com org1.example.com, org2.example.com που ακούν σε αυτές τις πόρτες. Αυτό γίνεται με τις εντολές:

```
sudo ufw enable, ενεργοποίηση του firewall
sudo ufw allow XXXX(port number), εντολή ενεργοποίησης πόρτας
sudo ufw status, προβολή της κατάστασης του firewall
```

2.4 Προγραμματισμός σε περιβάλλον Hyperledger

2.4.1 Υποστηρίζόμενα περιβάλλοντα προγραμματισμού

Τα κύρια εργαλεία που έχουμε χρησιμοποιήσει είναι το πλαίσιο Hyperledger Fabric, το Hyperledger Composer, το Docker Engine, το Docker Compose και εργαλεία που αυτά υποστηρίζουν καθώς και γλώσσες προγραμματισμού όπως η Python και η Go Language.

Το Hyperledger Fabric, που έχουμε αναλύσει και σε προηγούμενο κεφάλαιο αποτελεί την υποδομή του blockchain δικτύου, περιλαμβάνει το αρχιτεκτονικό μοντέλο, προσδιορίζει τους ρόλους μεταξύ των κόμβων, δημιουργεί smart contracts (έξυπνα συμβόλαια) σε αλυσιδωτή μορφή (chaincode) και υλοποιεί την συναίνεση και τις υπηρεσίες των κόμβων-μελών (endorsement policies). (Hyperledger Fabric, 2019)

Το Hyperledger Composer παρέχει μια απλοποιημένη γλώσσα μοντελοποίησης συγκεκριμένου τομέα για τη μοντελοποίηση επιχειρηματικού δικτύου και τη JavaScript για την λογική εφαρμογή των συναλλαγών. Επίσης, περιλαμβάνει τον composer-rest-server (βασισμένο στην τεχνολογία Loopback) για την αυτόματη δημιουργία του REST API στο επιχειρηματικό δίκτυο και του hyperledger composer plugin για τη δημιουργία της Angular εφαρμογής. Το Hyperledger Composer διαθέτει επίσης ένα πλούσιο σύνολο εφαρμογών API JavaScript για τη δημιουργία εγγενών εφαρμογών Node.js. (Hyperledger Composer, 2019)

Το Node.js είναι ένα περιβάλλον εκτέλεσης ανοικτού JavaScript κώδικα. Είναι ένα δημοφιλές εργαλείο για σχεδόν οποιοδήποτε είδος έργου. Το Node.js εκτελεί τη μηχανή JavaScript V8, τον πυρήνα του Google Chrome, έξω από το πρόγραμμα περιήγησης. Αυτό επιτρέπει στο Node.js να είναι πολύ αποδοτικό. Μια εφαρμογή Node.js εκτελείται σε μια ενιαία διαδικασία, χωρίς να δημιουργείται ένα νέο νήμα (thread) για κάθε αίτημα. (Node.js Foundation, 2019)

Το Docker είναι μια πλατφόρμα για προγραμματιστές που θέλουν να αναπτύξουν, να στείλουν και να εκτελέσουν εφαρμογές. Το Docker επιτρέπει να συναρμολογούνται γρήγορα εφαρμογές από τα εξαρτήματα και να εξαλείφονται οι τριβές που μπορεί να προκύψουν κατά την αποστολή ενός κώδικα. (Docker Inc, 2019)

Η Docker μηχανή δημιουργεί μια διαδικασία daemon⁸ από την πλευρά του διακομιστή που φιλοξενεί εικόνες, containers⁹, δίκτυα και volumes αποθήκευσης. Διαθέτει μια REST API που καθορίζει τις διεπαφές που μπορούν να χρησιμοποιήσουν τα προγράμματα για να μιλήσουν στην daemon διαδικασία και να της δώσουν οδηγίες για το τι πρέπει να κάνει. Παρέχει επίσης μια διεπαφή γραμμής εντολών πελάτη (Command Line Interface) που επιτρέπει στους χρήστες να αλληλεπιδρούν με το REST API του Docker Engine. Το Docker είναι δηλωτικό, πράγμα που σημαίνει ότι ο διαχειριστής προγραμματίζει ένα συγκεκριμένο σύνολο συνθηκών ως την επιθυμητή κατάσταση. Το Docker ρυθμίζει αυτόματα τις ρυθμίσεις και τις συνθήκες, ώστε να διασφαλίζει ανά πάσα στιγμή την πραγματική κατάσταση και τον επιθυμητό αγώνα κατάστασης. (Hale, 2019)

⁸ Το Docker Daemon είναι ένας διακομιστής Docker που ακούει τα αιτήματα του Docker API. Το Docker Daemon διαχειρίζεται εικόνες, containers, δίκτυα και volumes.

⁹ Ένα docker container είναι μια στιγμή εκτέλεσης (runtime) μια docker εικόνας. Αποτελείται από: μια εικόνα Docker, ένα περιβάλλον εκτέλεσης, ένα τυποποιημένο σύνολο οδηγιών. Το container ορίζει ένα πρότυπο για την αποστολή λογισμικού.

Οι εικόνες Docker αποτελούν τη βάση των containers. Μια εικόνα είναι μια ταξινομημένη συλλογή των αλλαγών του συστήματος, των αρχικών αρχείων και των αντίστοιχων παραμέτρων εκτέλεσης για χρήση μέσα σε ένα runtime container. Μια εικόνα τυπικά περιέχει μια ένωση των αρχείων του συστήματος σε συστάδες στοιβαγμένα το ένα πάνω στο άλλο. Μια εικόνα δεν έχει κατάσταση και δεν αλλάζει ποτέ.

Τα Docker volumes είναι ο καλύτερος τρόπος αποθήκευσης των επίμονων δεδομένων που καταναλώνουν και δημιουργούν τα Docker containers, επειδή το volume δεν αυξάνει το μέγεθος των containers που το χρησιμοποιούν και τα περιεχόμενα του volume υπάρχουν εκτός του κύκλου ζωής ενός συγκεκριμένου container. Ενώ τα bind mounts (μια εναλλακτική προβολή ενός δέντρου καταλόγου) εξαρτώνται από τη δομή του καταλόγου του κεντρικού υπολογιστή, τα volumes ελεγχθούν πλήρως από το Docker.

Το Docker Compose είναι ένα εργαλείο που διευκολύνει την εκτέλεση εφαρμογών που απαιτούν πολλαπλά Docker containers. Το Docker Compose μας επιτρέπει να μεταφέρουμε εντολές σε ένα αρχείο που μπορεί να αναπαραχθεί και να επαναχρησιμοποιηθεί οπουδήποτε. Στη συνέχεια μπορούμε να καθορίσουμε τις υπηρεσίες που συνθέτουν την εφαρμογή μας στο docker-compose.yml αρχείο, ώστε να τρέξουν όλες μαζί σε ένα απομονωμένο περιβάλλον. Και εκτελούμε την εντολή docker-compose up που εκκινεί και εκτελεί ολόκληρη την εφαρμογή μας. Επιπλέον, η διεπαφή γραμμής εντολών Docker Compose (CLI) διευκολύνει στην συνέχεια την αλληλεπίδραση με την εφαρμογή μας. (Kerner, 2019)

Το Node Package Manager (NPM) είναι ένα πρόγραμμα διαχείρισης πακέτων της γλώσσας Javascript και το προκαθορισμένο πρόγραμμα διαχείρισης πακέτων του προγραμματιστικού περιβάλλοντος Node.js. Εκτός από πακέτα, στο αρχείο του npm υπάρχουν αρχεία node modules που χρησιμοποιούνται στο server-side προγραμματισμό. (Npm Community, 2019)

Το Git είναι ένα ελεύθερο και ανοικτού κώδικα σύστημα ελέγχου έκδοσεων έργων που έχει σχεδιαστεί για να διαχειρίζεται τα πάντα, από μικρά έως πολύ μεγάλα έργα με ταχύτητα και αποτελεσματικότητα. Σε μια κατανεμημένη αρχιτεκτονική, το Git είναι ένα παράδειγμα ενός DVCS (Distributed Version Control System). Αντί να υπάρχει μόνο μία τοποθεσία για το ιστορικό πλήρους έκδοσης του λογισμικού, όπως συμβαίνει με τα δημοφιλέστερα συστήματα ελέγχου έκδοσης όπως το CVS ή το Subversion (SVN), στο Git, το αντίγραφο του κώδικα κάθε προγραμματιστή είναι ένας ξεχωριστός αποθηκευτικός χώρος (repository) που μπορεί να περιέχει το πλήρες ιστορικό όλων των αλλαγών, που έχουν εφαρμοστεί στον κώδικα. Στην συγκεκριμένη εργασία το git θα χρησιμοποιηθεί και για την μεταφορά αρχείων και εργαλείων που είναι δημοσιευμένα στην ανοιχτή πλατφόρμα του github. (Atlassian, 2019) (Git Community, 2019)

2.4.2 Δομές δεδομένων

Το αρχείο model είναι υπεύθυνο για την περιγραφή της δομής του δικτύου. Έχει τρία βασικά στοιχεία: assets, participants και transactions.

Assets

Τα assets είναι υλικοί ή πνευματικοί πόροι, υπηρεσίες ή περιουσιακά στοιχεία, τα αρχεία των οποίων διατηρούνται σε μητρώα. Τα assets μπορούν να αντιπροσωπεύουν σχεδόν οτιδήποτε σε ένα επιχειρηματικό δίκτυο, όπως ένα σπίτι για πώληση, κατάθεση προς πώληση, πιστοποιητικό εγγραφής για αυτό το σπίτι, ενώ τα ασφαλιστικά έγγραφα για το σπίτι μπορεί να είναι περιουσιακά στοιχεία σε ένα ή περισσότερα επιχειρηματικά δίκτυα. Τα assets πρέπει να έχουν μοναδικό αναγνωριστικό (identifier), αλλά μπορούν επίσης να περιέχουν οποιεσδήποτε ιδιότητες που τα προσδιορίζουν.

Participants

Οι participants μπορούν να συσχετίζονται με ένα ή περισσότερα assets. Μπορούν να έχουν πρόσβαση στις συναλλαγές τους με βάση το ρόλο τους ως αγοραστής, πωλητής ή μεσίτης. Ο μεσίτης μπορεί στη συνέχεια να δημιουργήσει μια εφαρμογή για να παρουσιάσει τους αγοραστές και τους πωλητές με μια απλή διεπαφή χρήστη για την προβολή ανοιχτών λιστών και την πραγματοποίηση προσφορών. Αυτό το επιχειρηματικό δίκτυο θα μπορούσε επίσης να ενσωματωθεί με το υπάρχον σύστημα απογραφής, προσθέτοντας νέα σπίτια ως περιουσιακά στοιχεία και αφαιρώντας τις ιδιότητες που πωλούνται. Τα σχετικά άλλα μέρη μπορούν να καταχωρηθούν ως συμμετέχοντες, για παράδειγμα ένα κτηματολόγιο μπορεί να αλληλεπιδράσει με έναν αγοραστή για να μεταβιβάσει την ιδιοκτησία της γης. (Hyperledger Composer, 2019)

Transactions

Η συναλλαγή (transaction) είναι ο μηχανισμός αλληλεπίδρασης των συμμετεχόντων με τα assets. Ο ορισμός της δηλώνει επίσης τη διαδικασία κατασκευής ή οποιασδήποτε συναλλαγής ενός επιχειρηματικού δικτύου, δηλαδή την αναφορά δημιουργίας ενός assets, συμμετοχής ενός participant στο επιχειρηματικό δίκτυο αλλά και η ολοκλήρωση μιας συναλλαγής, δηλαδή μια δημοπρασία ή μια ανταλλαγή ενός asset.

2.4.3 Υλοποίηση smart contracts

Όπως ορίσαμε και στην λογική του Hyperledger Fabric, τα smart contracts ορίζουν τον τρόπο με τον οποίο γίνονται οι συναλλαγές και ότι περιλαμβάνεται στις συναλλαγές αυτές, δηλαδή περιγράφονται assets, participants και transactions μεταξύ των δύο πρώτων στοιχείων.

Τα αρχεία που συμπεριλαμβάνουν τα smart contracts είναι:

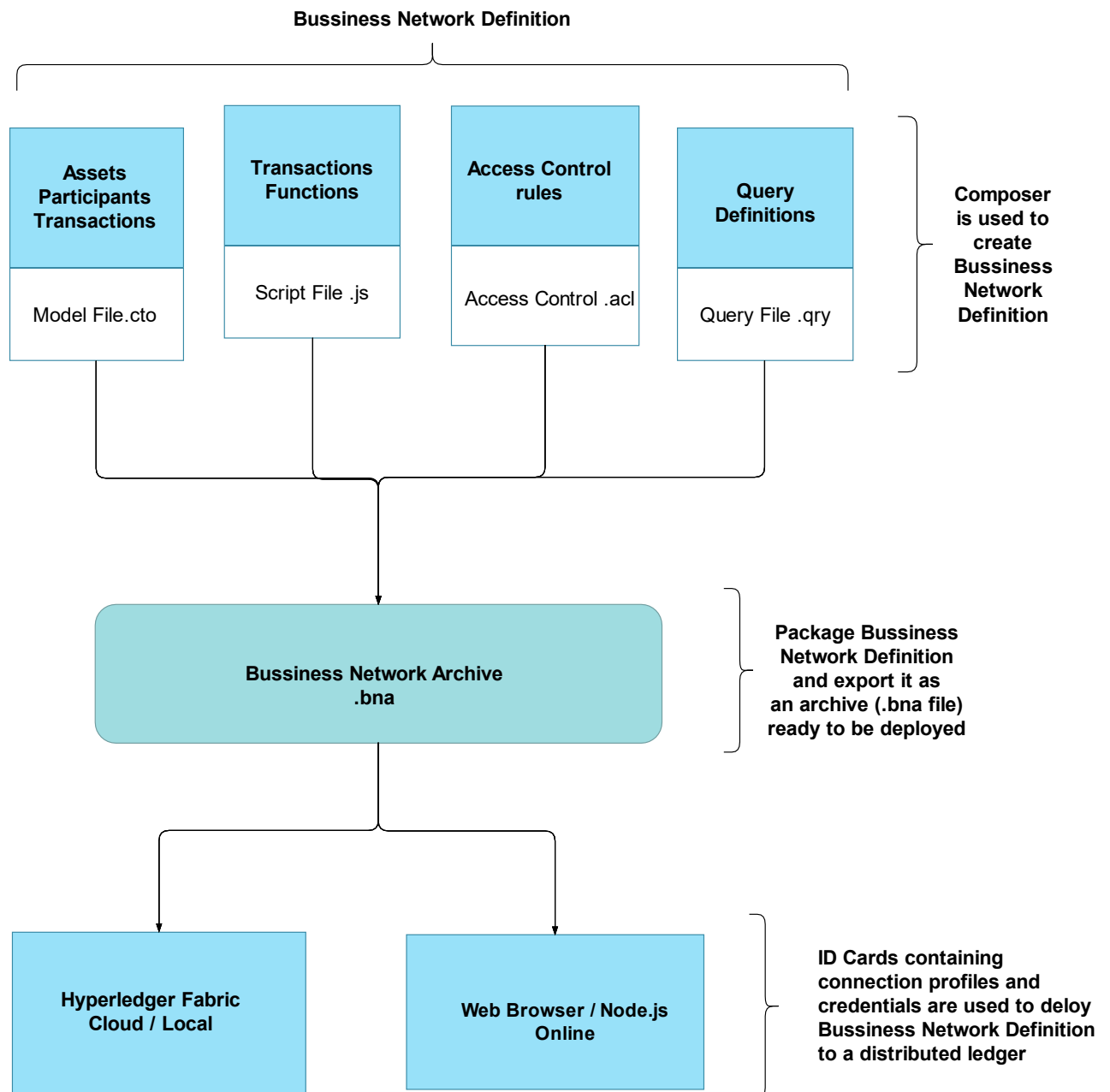
Το αρχείο script file ορίζει διάφορες λειτουργίες συναλλαγών στο δίκτυο. Είναι γραμμένο σε JavaScript και χειρίζεται τη λογική συναλλαγών, συμπεριλαμβανομένων των τύπων των μελών που συμμετέχουν (καθώς ανάλογα με τον ρόλο που έχουν οι συμμετέχοντες έχουν διαφορετικά δικαιώματα πρόσβασης στο δίκτυο) και τα είδη των δεδομένων που μεταφέρονται.

Το αρχείο access control περιγράφει τα πεδία των χρηστών που έχουν πρόσβαση στο επιχειρηματικό δίκτυο. Σε αυτό το αρχείο περιγράφεται ο ρόλος του χρήστη (συμμετέχων), προσδιορίζοντας τον ρόλο του στη δημιουργία, ανάγνωση, ενημέρωση ή διαγραφή δεδομένων του δικτύου.

Το αρχείο query ορίζει τη δομή και τη λειτουργία των ερωτημάτων σε αυτό το δίκτυο. Τα ερωτήματα μπορούν να οριστούν για την προβολή ορισμένων είναι όλων των συναλλαγών από τον ιστορικό, το οποίο αποτελεί ένα κατάλογο όλων των προηγούμενων συναλλαγών στο σύστημα.

Μόλις καθοριστεί το δίκτυο, μπορεί να εξαχθεί ως αρχείο archive (.bna file), να μεταφορτωθεί και να εκτελεστεί σε άλλο μηχάνημα. Για τη σύνδεση στο σύστημα χρησιμοποιείται μια κάρτα δικτύου. Οι κάρτες δικτύου μπορούν να λάβουν το είδος της κάρτας συμμετέχοντος ή ενός διαχειριστή. Οι κάρτες συμμετεχόντων έχουν γενικά πιο ελεγχόμενο πεδίο πρόσβασης στο δίκτυο, ενώ ο διαχειριστής μπορεί να εκτελεί περισσότερες λειτουργίες υψηλής απόδοσης, όπως η προσθήκη νέων συμμετεχόντων ή η διαγραφή συμμετεχόντων. Η ιδιότητα μιας κάρτας ορίζει την ταυτότητα του κόμβου που χρησιμοποιεί την κάρτα για να συνδεθεί στο δίκτυο και έτσι περιγράφει το είδος του ρόλου που παίζει ο κόμβος.

Η όλη αρχιτεκτονική του Hyperledger Composer φαίνεται στο παρακάτω σχήμα (εικόνα 9).



Εικόνα 9 Hyperledger Composer Architecture

2.4.4 Υλοποίηση consensus algorithms

Η πολιτική της συναίνεσης ορίζεται στο αρχείο endorsement-policies.json, στο οποίο ορίσαμε τα δικαιώματα κάθε οργανισμού στο δίκτυο. Οι πολιτικές εγκρίσεων χρησιμοποιούνται για να καθοδηγήσουν έναν peer για τον τρόπο με τον οποίο μπορεί να αποφασίσει κατά πόσον μια συναλλαγή έχει εγκριθεί σωστά. Όταν ένας peer χρήστης λαμβάνει μια συναλλαγή, καλεί το VSCC (Chaincode System Validation) που σχετίζεται με τον Chaincode της συναλλαγής ως μέρος της ροής επικύρωσης συναλλαγής για να καθορίσει την εγκυρότητα της συναλλαγής.

Επίσης, σύμφωνα με την επίσημη σελίδα του Hyperledger Fabric (Hyperledger Fabric, 2019) μια υπηρεσία Solo ordering είναι μια καλή επιλογή κατά την ανάπτυξη δικτύων δοκιμών, ανάπτυξης ή δοκιμών. Για το λόγο αυτό, είναι η προεπιλεγμένη υπηρεσία παραγγελίας που αναπτύσσεται στο Build our First Tutorial Network, καθώς, από την πλευρά άλλων εξαρτημάτων του δικτύου, μια υπηρεσία παραγγελιών Solo επεξεργάζεται συναλλαγές πανομοιότυπα με τις πιο περίπλοκες εφαρμογές Kafka και Raft, που χρησιμοποιούνται για δίκτυα πολλαπλών κόμβων και ομάδων. Άρα χρησιμοποιήσαμε την default επιλογή του Solo, που φαίνεται και στο αρχείο configtx.yaml στο σημείο του OrdererType είναι:

```
#####  
Orderer: &OrdererDefaults  
  
# Orderer Type: The orderer implementation to start  
# Available types are "solo" and "kafka"  
OrdererType: solo  
  
Addresses:  
- orderer.example.com:7050
```

Κεφάλαιο 3. Εφαρμογές κρίσιμης αποστολής σε Blockchain

3.1 Γενικά χαρακτηριστικά και απαιτήσεις

Με τον όρο διαχείριση κρίσιμων αποστολών ή αλλιώς έκτακτων αναγκών εννοούμε μια διαδικασία λήψης αποφάσεων για την εντιμετώπιση μιας έκτακτης κατάστασης με στόχο την ελαχιστοποίηση ανθρώπινων απωλειών, φυσικών καταστροφών, καταστροφών σε υποδομές και αποδιοργάνωση κοινωνικής και οικονομικής ζωής γενικά. (Βεσκούκης, 2008)

3.1.1 Εφαρμογές κρίσιμης αποστολής

Στο πλαίσιο της διαχείρισης κρίσιμων αποστολών έχουν αναπτυχθεί εφαρμογές για την αυτοματοποίηση των λειτουργιών του συστήματος προστασίας σε βαθμό που είναι εφικτό. Παραδείγματα τέτοιων εφαρμογών έχουν εφαρμοστεί σε περιπτώσεις πυρκαγιάς και σεισμών.

Ένα ολοκληρωμένο σύστημα διαχείρισης κρίσεων δασικών πυρκαγιών είναι το σύστημα Firementor, το οποίο αναπτύχθηκε από το Εθνικό Μετσόβιο Πολυτεχνείο και ιδιωτικούς φορείς και περιλαμβάνει τη χρήση αισθητήρων στις δασικές περιοχές για ανίχνευση κινδύνου και την χαρτογράφησή τους, την προσομοίωση της πυρκαγιάς με ενεργοποίηση τους συστήματος είτε από αισθητήρες είτε από έναν χρήστη, την επικοινωνία με μετεωρολογικούς σταθμούς για την ενημέρωση των καιρικών συνθηκών της περιοχής. Επίσης, περιέχει ένα σύστημα δρομολόγησης και κατανομής των τοπικών υπηρεσιών επέμβασης στο σημείο της πυρκαγιάς, όπως πυροσβεστικά, ασθενοφόρα, ομάδες εθελοντών. Υπολογίζει τις συνθήκες των δρόμων για την διαχείριση εκκένωσης σε περιπτώσεις που κρίνεται απαραίτητη. Ακόμη, χρησιμοποιεί σενάρια κρίσεων πυρκαγιάς με εξαγωγή αποτελεσμάτων και ταξινόμησή τους, ώστε οι λειτουργίες του συστήματος να χρησιμοποιηθούν ως οδηγός επιχειρήσεων πυρκαγιάς τόσο για την προετοιμασία απόκρισης μιας αποστολής και λήψη αποφάσεων πριν την κρίση πυρκαγιάς, όσο και την έγκαιρη ενημέρωση του γενικού πληθυσμού. Το σύστημα αυτό αναπτύχθηκε προκειμένου να βελτιστοποιηθεί ο χρόνος απόκρισης, η αποτελεσματικότερη χρήση των μέσων, μείωση κόστους και αύξηση της κάλυψης των αναγκών γενικά. Μπορεί ταυτόχρονα να αποτελέσει ένα εργαλείο εκπαιδευτικού υλικού για πυροσβέστες, εθελοντές κλπ. (Βεσκούκης, 2008)

Ένα νέο σύστημα έγκαιρης προειδοποίησης επερχόμενου σεισμού και της επικινδυνότητας αυτού είναι το Shields, το οποίο αναπτύχθηκε από τον Καθηγητή Άκη Τσελέντη και τους συνεργάτες του σε συνεργασία με το Πανεπιστήμιο Πατρών. Έχει ήδη ξεκινήσει η πιλοτική ανάπτυξη και εφαρμογή του στην περιοχή της Αττικής για την προστασία του δικτύου φυσικού αερίου. Σε γενικές γραμμές το σύστημα αποτελείται από αισθητήρες της έντασης του σεισμού, υπολογιστικό σύστημα για τους απαραίτητους υπολογισμούς της έντασης και καταστροφικότητας του σεισμού, ένα δίαυλο επικοινωνίας ασύρματο ή ενσύρματο (συμπεριλαμβανομένου και των οπτικών ινών), στον οποίο η ταχύτητα διάδοσης των πληροφοριών είναι μεγαλύτερη από την ταχύτητα των σεισμικών κυμάτων και τέλος συσκευές πληροφόρησης και ελέγχου που βρίσκονται στον υπό προστασία χώρο και του παρέχουν ενδείξεις (οπτικές, ηχητικές και ηλεκτρικές) σχετικά με την άφιξη και την ένταση του επερχόμενου σεισμού. Το σύστημα αυτό προβλέπεται να προειδοποιεί αυτόματα τους φορείς προστασίας του πολίτη, τα σχολεία και τα νοσοκομεία της συγκεκριμένης περιοχής καθώς και

αυτόματο κλείσιμο ηλεκτρονικών βαλβίδων, στάση ανελκυστήρων για αποφυγή εγκλωβισμών και αυτόματη τροχοπέδηση σειρμών για αποφυγή εκτροχιασμών. (Τσελέντης, 2002)

Όσο αναφορά την ενημέρωση των πολιτών έχουν δημιουργηθεί πολλές εφαρμογές για κινητά τηλέφωνα και websites, οι οποίες ειδοποιούν για φυσικές καταστροφές, ακραία καιρικά φαινόμενα, προσφέροντας πλήρη ενημέρωση των προγνώσεων και της πιθανής εξέλιξης των καταστροφών. Στις εφαρμογές αυτές δίνεται και η δυνατότητα επικοινωνίας με κοντινά πρόσωπα ή με εξειδικευμένη υπηρεσία παροχής βοήθειας. Τέτοιες εφαρμογές είναι το Disaster Alert, Zello PTT Walkie Talkie, Earthquake network-Realtime alerts. Το μειονέκτημα αυτών των εφαρμογών είναι η υποχρεωτική χρήση δικτύου (2G το ελάχιστο), που καθιστά αδύνατη την ενημέρωση σε περίπτωση απώλειας σήματος. (SecNews , 2017)

3.1.2 Γιατί Blockchain

Το όφελος του blockchain στην διαχείριση έκτακτης ανάγκης είναι ότι παρέχει διαλειτουργικότητα και διαφάνεια. Από την άποψη της διαλειτουργικότητας, το blockchain μπορεί να υιοθετηθεί ως ένα καθολικό σύστημα σε όλους τους οργανισμούς - παρόμοιο με το διαδίκτυο - και να επιτρέψει σε πολλά μέρη σε αυτό το σύστημα να συντονίσουν τους πόρους σε περίπτωση έκτακτης ανάγκης. Σε ένα σενάριο διάσωσης από καταστροφές, πολλά μέρη συμβάλλουν συχνά σε πόρους για να βοηθήσουν μια πληγείσα περιοχή. Εάν όλα τα εμπλεκόμενα σε αυτό το σενάριο μέρη υιοθετήσουν κοινό σύστημα αρχειοθέτησης βασισμένο σε blockchain, θα μπορούσαν να συντονίσουν αποτελεσματικότερες λύσεις σε καταστροφές, διασφαλίζοντας ότι οι πόροι διατέθηκαν στις περιοχές όπου χρειάζονται οι περισσότερες. Το Κέντρο Ελέγχου Ασθενειών-Center for Disease Control (CDC) εξετάζει τώρα το πιλοτικό πεδίο της περίπτωσης χρήσης της παρακολούθησης δεδομένων για τη δημόσια υγεία, όπου θα συλλέγει και θα κοινοποιεί δεδομένα σε φορείς που αντιμετωπίζουν ασθενείς σε σενάρια διάσωσης, συμπεριλαμβανομένων τοπικών υπηρεσιών δημόσιας υγείας, νοσοκομείων και φαρμακείων. (Torres, 2018)

Όσον αφορά τη διαφάνεια στο σενάριο διάσωσης από καταστροφές, το blockchain θα μπορούσε να προσφέρει μια αμετάβλητη αναφορά, προσβάσιμη από όλους, για να καταδείξει τους πόρους που έχουν αφιερωθεί σε μια περιοχή και από ποιον. Αυτή η διάφανη καταχώρηση θα μείωνε τη δυνατότητα εκτροπής πόρων και διαφθοράς σε αυτούς τους τύπους σεναρίων. Πάνω από όλα, η ικανότητα μιας πόλης να συλλέγει, να αναλύει και να επικοινωνεί με δεδομένα είναι κρίσιμη για την αποτελεσματική και αποδοτική διαχείριση έκτακτων περιστατικών. Η τεχνητή νοημοσύνη, το Internet of Things και το blockchain είναι οι τεχνολογίες που επιτρέπουν πιο εξελιγμένες διαδικασίες παραγωγής δεδομένων και μπορούν να βελτιώσουν την ικανότητα και την αποτελεσματικότητα του προσωπικού έκτακτης ανάγκης.

3.2 Μελέτη περίπτωσης: εφαρμογή επείγουσας αεροδιακομιδής ασθενών

Ως αεροδιακομιδή ορίζεται η μεταφορά οξέως ή και βαρέως πάσχοντων ασθενών σε υγειονομική μονάδα ή από μία υγειονομική μονάδα σε μια άλλη με αεροπορικά μέσα υπό ιατρικό έλεγχο και φροντίδα από συνοδευόμενο ιατρό. Επίσης, θεωρείται και η μεταφορά ιατρών και εξοπλισμού για παροχή πρώτων βοηθειών εφόσον κρίνεται αναγκαίο. (Air ambulance, 2019)

Η αεροδιακομιδή αποτελεί ισχυρή ανάγκη στον ελληνικό χώρο λόγω της μη ύπαρξης υποδομής πρωτοβάθμιας περίθαλψης στις ακριτικές περιοχές. Για παράδειγμα, μέσα σε μια μέρα πραγματοποιήθηκαν επτά αεροδιακομιδές από την ακριτική Ελλάδα προς μεγάλες νοσοκομειακές μονάδες στην ηπειρωτική Ελλάδα συνολικής διάρκειας δεκαοκτώ ωρών πτήσεως. Πιο συγκεκριμένα στις 20/4/19 και συμφώνως με τα στοιχεία που δημοσιοποίησε το ΓΕΑ πραγματοποιήθηκαν οι ακόλουθες πτήσεις: Ένα μεταφορικό αεροσκάφος C-27J Spartan της 354 Μοίρας Τακτικών Μεταφορών (354 MTM) μετέφερε 1 ασθενή από τη Γαλλία στην Ελευσίνα. Ένα μεταφορικό αεροσκάφος C-130H Hercules της 356 Μοίρας Τακτικών Μεταφορών (356 MTM) μετέφερε 4 ασθενείς από την Κω, τη Ρόδο και τη Μύκονο στη Ρόδο και στην Ελευσίνα, στη διάρκεια μιας πτήσεως με διαδοχικές αποπροσγειώσεις. Ένα άλλο αεροσκάφος C-130H της 356 MTM μετέφερε 1 νεογνό από τη Σάμο στην Ελευσίνα. Ένα ελικόπτερο Super Puma της 384 Μοίρας Ερεύνης – Διασώσεως (384 ΜΕΔ) μετέφερε 1 ασθενή από την Κάρπαθο στη Ρόδο. Συνολικώς, τα πτητικά μέσα της ΠΑ μετέφεραν τους 7 ασθενείς σε 4 αποστολές. (Μπλαβέρης, 2019)

3.2.1 Εμπλεκόμενοι φορείς (οργανισμοί)

Σε έκτακτα περιστατικά ασθενειών ή τραυματισμών και εφόσον ο γιατρός διαγνώσει την κρισιμότητα της κατάστασης ενημερώνει τηλεφωνικά το Εθνικό Κέντρο Άμεσης Βοήθειας (ΕΚΑΒ) για αναγκαιότητα αεροδιακομιδής. Το ΕΚΑΒ αφού καταγράψει την κλήση, προχωρά σε αξιολόγηση και διαβαθμίζει ως προς τον βαθμό του επείγοντος. Στην συνέχεια σε συνεργασία με το Γενικό Επιτελείο της Αεροπορίας εκτελεί αν είναι εφικτή την αεροδιακομιδή. Επίσης, το ΕΚΑΒ ενημερώνει την υγειονομική μονάδα υποδοχής για την κατάσταση του ασθενούς και τα μέτρα που πρέπει να ληφθούν για την καλύτερη δυνατή αντιμετώπιση του περιστατικού. Κατά τη διάρκεια της μεταφοράς τηρούνται όλοι οι προβλεπόμενοι κανόνες ασφαλείας που αφορούν και τον ασθενή και τους διασώστες, ενώ παράλληλα διατηρείται συνεχής επικοινωνία με το ΕΚΑΒ.

Λόγω της ιδιομορφίας του εδάφους της χώρας μας και της ύπαρξης πολλών νησιών που συνήθως δεν έχουν την κατάλληλη υγειονομική υποδομή για την αντιμετώπιση δύσκολων περιστατικών, η αεροδιακομιδή είναι σημαντικός παράγοντας στον τομέα της υγείας. Η οργάνωση του Συστήματος Αεροδιακομιδών, η εποπτεία της σωστής λειτουργίας και ο συντονισμός απαιτούν τη δημιουργία συντονιστικών Κέντρων Επιχειρήσεων από τους βασικούς φορείς λήψης αποφάσεων. Οι φορείς αυτοί είναι το Εθνικό Κέντρο Άμεσης Βοήθειας (ΕΚΑΒ), το Γενικό Επιτελείο Αεροπορίας (ΓΕΑ) με την Εθνική Μετεωρολογιακή Υπηρεσία (ΕΜΥ) και το Γενικό Επιτελείο Στρατού (ΓΕΣ)

3.2.2 Ροή ενεργειών που λαμβάνουν χώρα

Αρχικά, το ΕΚΑΒ λαμβάνει το αίτημα της αεροδιακομιδής ενός ασθενούς και προχωρά στην αποστολή εγκριτικού φαξ προς το ΓΕΑ. Κατόπιν αυτής της ειδοποίησης, το ΓΕΑ προχωρεί στην άμεση ενημέρωση των εμπλεκόμενων φορέων όπως για παράδειγμα το πλήρωμα του ελικοπτέρου, το οποίο με τη σειρά του ελέγχει τις καιρικές συνθήκες που επικρατούν στις περιοχές αναχώρησης και προορισμού, για τις οποίες ενημερώνεται από την εθνική μετεωρολογική υπηρεσίας (ΕΜΥ) και το Αρχηγείο της Τακτικής Αεροπορίας (ΑΤΑ). Παράλληλα, εξετάζονται η ύπαρξη και η καταλληλότητα αεροδρομίου με δεδομένα καθώς και άλλες απαιτήσεις για τη δυνατότητα εκτέλεσης της αεροδιακομιδής από το ΓΕΑ. Μόλις συγκεντρωθούν όλα τα δεδομένα λαμβάνεται η απόφαση για την εκτέλεση ή μη της αεροδιακομιδής από το ΓΕΑ. Σε περίπτωση έγκρισης, εκπληρώνεται η διαδικασία της μεταφοράς από το ΓΕΑ και εκδίδεται ένα έγγραφο με τη διαταγή της αεροδιακομιδής.

Εφόσον η απάντηση στο αίτημα είναι αρνητική από το ΓΕΑ, αυτό αποστέλλεται στο Κέντρο Επιχειρήσεων του Γενικού Επιτελείου Στρατού (ΓΕΣ/ΚΕΠΙΧ) με φαξ. Το ΚΕΠΙΧ ενημερώνει με τη σειρά του, τους δικούς του εμπλεκόμενους φορείς και το αίτημα μεταφέρεται σε διάφορες υπηρεσίες του ΓΕΣ και καταγράφεται στην βάση δεδομένων του. Στη συνέχεια, μετατρέπεται σε εντολή προς διερεύνηση που διαβιβάζεται στην πρώτη Μεραρχία Πεζικού (1ΜΠ). Το αρμόδιο τμήμα μετατρέπει την εντολή σε διαταγή για διερεύνηση και τη μεταβιβάζει τηλεφωνικά και έγγραφως στην ΤΑΞΑΣ. Όπου καταγράφεται η ώρα και η ημέρα που έλαβε χώρα η διαταγή. Ενημερώνεται τηλεφωνικά το πλήρωμα που αναλαμβάνει τον έλεγχο για την δυνατότητα πραγματοποίησης της αεροδιακομιδής. Συγκεκριμένα, ελέγχουν τις μετεωρολογικές συνθήκες και την καταλληλότητα του αεροδρομίου για την εκτέλεση της διακομιδής καθώς και την κατάσταση του πληρώματος.

Όταν δεν είναι εφικτή η αποστολή, στέλνονται όλες οι λεπτομέρειες της μη δυνατότητας στο ΚΕΠΙΧ. Το ΚΕΠΙΧ εκδίδει ένα διαβιβαστικό με τις λεπτομέρειες της μη αποδοχής και στέλνει ένα φαξ μη αποδοχής στο ΓΕΣ. Το ΓΕΣ λαμβάνει τα δεδομένα με φαξ και τα καταγράφει στη βάση δεδομένων του, ενώ ταυτόχρονα ενημερώνει το ΓΕΑ, το οποίο με την σειρά του στέλνει την απόρριψη στο ΕΚΑΒ.

Όταν είναι εφικτή η αεροδιακομιδή, η ΤΑΞΑΣ ενημερώνει τηλεφωνικά και στη συνέχεια εκδίδει διαβιβαστικό αποδοχής της αποστολής που προωθείται στην 1 ΜΠ. Η πρώτη Μεραρχία Πεζικού ενημερώνει τηλεφωνικά για κέρδος χρόνου τη Διεύθυνση Αεροπορίας Στρατού για την αποδοχή. Στη συνέχεια ενημερώνονται τα αρμόδια στελέχη και η ηγεσία στο ΓΕΣ, οι οποίοι αξιολογώντας τα δεδομένα και τα στοιχεία για την ασφάλεια και την επιτυχία της αποστολής λαμβάνουν την απόφαση για την έγκριση ή μη της αεροδιακομιδής.

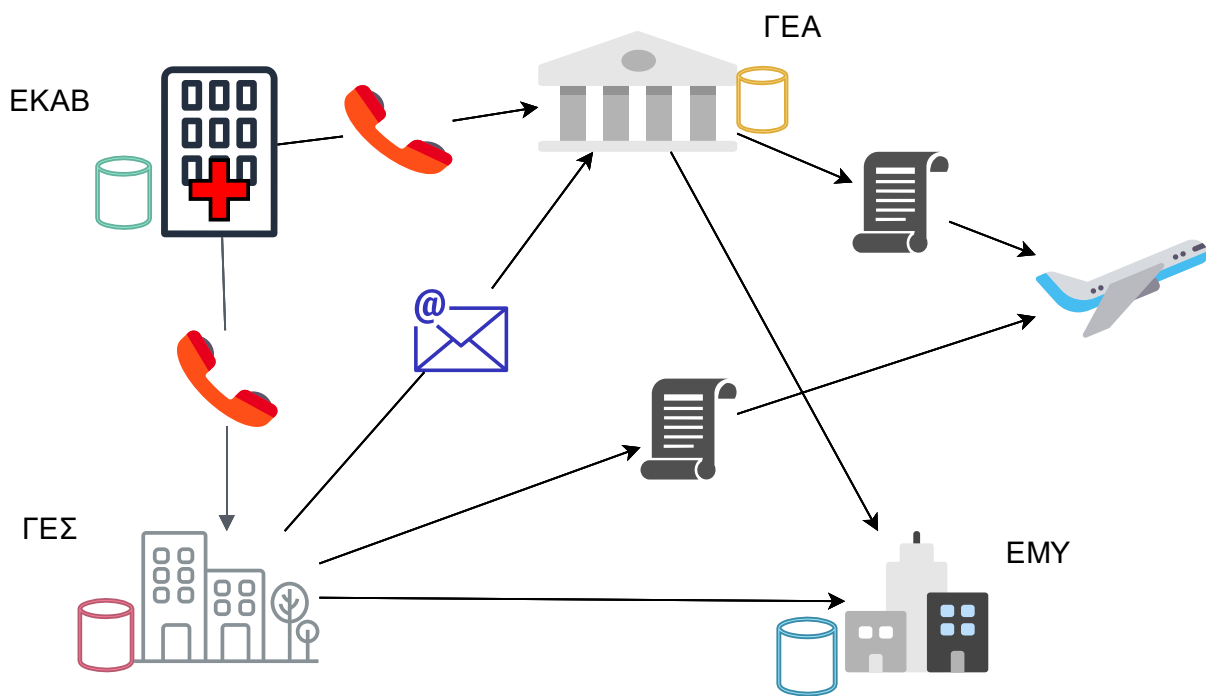
Στην περίπτωση που η ηγεσία δεν αποδεχτεί την αεροδιακομιδή, ενημερώνεται το ΚΕΠΙΧ και στην συνέχεια το ΓΕΑ, το οποίο αναλαμβάνει να καταγράψει την απόρριψη και να ενημερώσει το ΕΚΑΒ.

Με την έγκριση της αποστολής ενημερώνεται το ΚΕΠΙΧ, που καταγράφει την ώρα έγκρισης και ενημερώνει προφορικά το ΔΑΣ. Ο αρμόδιος προϊστάμενος της ΔΑΣ λαμβάνοντας την έγκριση εκδίδει διαβιβαστικό διαταγής εκτέλεσης, την οποία στέλνει στην πρώτη Μεραρχία Στρατού. Ακολουθούν αντίστοιχες διαταγές από όλους τους φορείς για την εκτέλεση της αποστολής. Τέλος ενημερώνεται η ΤΑΞΑΣ με όλες τις πληροφορίες για την διακομιδή, ώστε να ξεκινήσει η προετοιμασία για την εκτέλεση της αποστολής. Παράλληλα, ειδοποιείται το

ΕΚΑΒ τηλεφωνικά και άμεσα από το ΓΕΑ και απο το ΚΕΠΙΧ μετά την έγκριση της ηγεσίας για την έναρξη της προετοιμασίας της αποστολής που πρέπει να ολοκληρωθεί εντός μιας ώρας.

Μετά την ολοκλήρωση της αποστολής, η ΤΑΞΑΣ εκδίδει έγγραφο με όλα τα δεδομένα για το πέρας της αποστολής που διαβιβάζεται σε όλους τους φορείς και όλοι οι εμπλεκόμενοι φορείς με τη σειρά τους εκδίδουν αντίστοιχες διαταγές με τα στοιχεία της αεροδιακομιδής και τα έγγραφα καταχωρούνται.

Σε όλα τα στάδια επικοινωνίας δημιουργούνται έγγραφα, μηνύματα, φαξ, χάρτες, τηλεφωνικές κλήσεις και μετεωρολογικά δεδομένα, τα οποία στέλνονται επικυρωμένα απο τον έναν φορέα στον άλλο καθώς και μεταξύ των υπηρεσιών μέσα στον ίδιο φορέα.



Εικόνα 10 Τρόπος επικοινωνίας με τον σημερινό τρόπο λειτουργίας

3.2.3 Τεχνολογίες που χρησιμοποιούνται

Στην επικοινωνία μεταξύ των αρμόδιων φορέων χρησιμοποιούνται τηλεφωνικά κέντρα τελευταίας τεχνολογίας, καθώς και μηνύματα μέσω του ηλεκτρονικού ταχυδρομείου ή φαξ. Το τηλέφωνο, το ραδιοτηλέφωνο, ο ασύρματος, το τηλέτυπο, το τηλεομοιοτυπικό (γνωστότερο ως φαξ) αποτελούν κύριες τηλεπικοινωνιακές συσκευές, που χρησιμοποιούνται για την συνναλλαγή δεδομένων μεταξύ υπηρεσιών. Ενδεικτικά, στην Εθνική Μετεωρολογιακή Υπηρεσία εξάγονται προγνώσεις καιρού για τις περιοχές ενδιαφέροντος σε μορφή χαρτών, διαγραμμάτων και στατιστικών ως δεδομένα που αποστέλλονται συνήθως με φαξ στις αρμόδιες υπηρεσίες.

Σε κάθε συντονιστικό κέντρο λειτουργεί ένα πληροφοριακό σύστημα μέσω του οποίου αντλούνται πληροφορίες από την βάση δεδομένων του. Ένα πληροφοριακό σύστημα μπορεί να διαθέτει πληροφορίες σχετικά με τα αεροδρόμια και την κατάστασή τους σε πραγματικό χρόνο. Παράλληλα, έχει καταχωρημένα στοιχεία που αφορούν τα εναέρια μέσα, διαθεσιμότητα, τον εξοπλισμό, καθώς και ιστορικό συντήρησης και βλαβών. Επίσης, ενημερώνεται καθημερινά με αναλυτική κατάσταση των πληρωμάτων βάρδιας και των πιθανών αλλαγών. Στο ιστορικό των αιτημάτων αεροδιακομιδής καταχωρούνται όλα τα δεδομένα που αφορούν την μελέτη έγκρισης ή απόρριψης της αποστολής και διαταγές και ενημερώσεις που εκδίδονται αντιστοίχως. Αναλυτικά, αποθηκεύονται όλες οι ενέργειες, οι επικοινωνίες (με καταγραφή ώρας), οι εντολές, οι διαταγές, τα διαβιβαστικά έγγραφα και τα συνοδευτικά τους. Σε περίπτωση εκτέλεσης της αεροδιακομιδής καταχωρούνται με λεπτομέρειες οι ώρες έναρξης και λήξης, η διάρκεια εκτέλεσης, οι τόποι αναχώρησης και προορισμού, οι αναφορές των συμμετεχόντων και η έκβαση της αποστολής.

Οι γνωστές σε όλους τεχνολογίες που βοήθησαν σημαντικά και χρησιμοποιούνται μέχρι σήμερα από τα συντονιστικά κέντρα κατά τη διάρκεια μελέτης σχετικά με την εκτέλεση μιας αεροδιακομιδής αλλά και κατά την διάρκεια πραγματοποιήσής της είναι οι ασύρματες τηλεπικοινωνίες και τα συστήματα ραντάρ. Παράλληλα, μπορεί να διατίθεται πραγματική εικόνα καιρού από δορυφόρο για την συνεχή πρόγνωση και μεταβολή των καιρικών συνθηκών.

Οι επικοινωνίες φωνής μεταξύ του πιλότου του αεροσκάφους και του ελεκτή του τμήματος εναέριας κυκλοφορίας διακρίνονται σε υψηλές συχνότητες (high-frequency, HF), πολύ υψηλές συχνότητες (very-high-frequency, VHF) και δορυφορικές επικοινωνίες SATCOM. Η HF ζώνη χρησιμοποιείται σε περιπτώσεις προβλημάτων σε επικοινωνίες VHF, ενώ οι δορυφορικές αποτελούν μια πιο εξελιγμένη τεχνολογία. Δύο κύρια συστήματα επικοινωνίας που στηρίζονται σε κανάλια VHF είναι το aircraft communications addressing and reporting system (ACARS) και τη ζεύξη δεδομένων controller pilot data link communications (CPDLC), με τα οποία ανταλλάσσονται δεδομένα από το σύστημα του αεροπλάνου και αντίστοιχα από τον πιλότο στον ελεγκτή εναέριας κυκλοφορίας και αντίστροφα. Οι δορυφορικές επικοινωνίες έχουν βελτιώσει τις υπηρεσίες που αφορούν τη διαχείριση της εναέριας κυκλοφορίας, τόσο για τη ζεύξη δεδομένων CPDLC όσο και την επιτήρηση των αεροσκαφών κατά τις πτήσεις τους. Τέλος, οι ζεύξεις δεδομένων που βασίζονται σε δορυφόρους αποτελούν το σημαντικότερο τμήμα ελέγχου εναέριας κυκλοφορίας αφού ίσως είναι ο μόνος τρόπος να διασφαλιστεί η αξιοπιστία των ζεύξεων δεδομένων πάνω από ωκεανούς. (Παπαζαχαρίας, 2015) Σε περιπτώσεις γενικής πτώσης της επικοινωνίας ή ενός επίγειου σταθμού μπορούν να χρησιμοποιηθούν συχνότητες από εφεδρικά συστήματα ραδιοεπικοινωνίας, αλλά και τηλεφωνική επικοινωνία μέσω του συστήματος TELEPHON BACK-UP VCS. (Παρδάλη, 2010)

Επιπροσθέτως, το ραντάρ είναι ένα σύστημα που χρησιμοποιεί τα ραδιοκύματα για να ανιχνεύσει, να καθορίσει την απόσταση και να χαρτογραφήσει αντικείμενα. Τα συστήματα ραντάρ ανάλογα με τον φορέα και τον επιθυμητό χώρο ραδιοεντοπισμού διακρίνονται σε: (1) τα ραντάρ Ανιχνεύσεως επιφάνειας ή αλλιώς ραντάρ Ναυσιπλοΐας, που ανιχνεύουν την επιφάνεια της θάλασσας, αλλά και τον εναέριο χώρο σε μικρό ύψος, (2) τα ραντάρ Ανιχνεύσεως Αέρα που ως σκοπό έχουν να ανιχνεύουν τον εναέριο χώρο σε μεγάλες αποστάσεις και σε μεγάλα ύψη, (3) τα ραντάρ Ελέγχου Προσγειώσεως Αεροσκαφών που έχουν μικρή εμβέλεια, αλλά μεγάλη ακρίβεια και παρέχουν πληροφορίες αποστάσεως, ύψους, κατευθύνσεως διαδρόμου προσγειώσεως και ίχνους καθόδου, (4) τα Υψομετρικά ραντάρ

εγκαθίστανται σε αεροσκάφη και εξασφαλίζουν ακριβή μέτρηση του ύψους πτήσεώς τους, (5) τα Μετεωρολογικά ραντάρ που με αυτά εξασφαλίζεται ο έγκαιρος εντοπισμός και η παρακολούθηση των επερχομένων καταιγίδων και κυκλώνων, (6) τα ραντάρ Ανίχνευσης Κίνησης ανιχνεύουν κινήσεις σε σταθερούς χώρους και ενεργοποιούν συναγερμούς, φώτα και διάφορους άλλους μηχανισμούς. (Σάγος, 2018)

3.2.4 Υλοποίηση ασφάλειας

Η ασφάλεια υπολογιστικών συστημάτων αφορά την προστασία των υπολογιστών, των δικτύων που τους διασυνδέουν και των δεδομένων σε αυτά τα συστήματα, αποτρέποντας τη μη εξουσιοδοτημένη πρόσβαση ή χρήση τους. Συγκεκριμένα, η ασφάλεια ενός υπολογιστικού συστήματος (computer system security) θέτει ως στόχο τη διαφύλαξη των υπολογιστικών πόρων από μη εξουσιοδοτημένη χρήση και τη προστασία πληροφορίας από ακούσια ή σκόπιμη βλάβη, αποκάλυψη ή τροποποίησή της. Ενώ η ασφάλεια κατά την επικοινωνία (communication security) στοχεύει στη προστασία δεδομένων κατά τη μετάδοση σε δίκτυα υπολογιστών και καταναμεμημένα συστήματα.

Στόχος ενός συστήματος πολιτικής ασφάλειας είναι ο περιορισμός επικινδυνότητας σε αποδεκτό επίπεδο. Το σύστημα περιλαμβάνει αξιολόγηση της επικινδυνότητας και περιορισμό του αποδεκτού επιπέδου ασφαλείας, ανάπτυξη και εφαρμογή μιας πολιτικής ασφαλείας καθώς και δημιουργία κατάλληλου οργανωτικού πλαισίου και εξασφάλιση των απαιτούμενων πόρων για την εφαρμογή της πολιτικής ασφαλείας. Τα είδη των πολιτικών ασφαλείας ενός φορέα είναι: (α) τα τεχνικά (computer oriented) δηλαδή τα συστήματα πληροφοριών, τα λειτουργικά συστήματα και τα δίκτυα υπολογιστών (β) τα οργανωτικά (human oriented) και (γ) τα ατομικά (individual security policies). Περιλαμβάνει αποσπασματική διαχείριση της ασφάλειας πληροφοριακών συστημάτων και μεγάλη πολυπλοκότητα στη συντήρηση ενώ είναι αποτελεσματική σε αυτόνομες εφαρμογές και υπολογιστικά συστήματα που δεν συνδέονται μεταξύ τους.

Βασικές αρχές στις οποίες στηρίζεται η ασφάλεια των πληροφοριακών συστημάτων είναι η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα. Η εμπιστευτικότητα είναι η αποφυγή μη εξουσιοδοτημένης αποκάλυψης της πληροφορίας και σε ένα σύστημα εμπιστοσύνης οι πόροι ενός συστήματος πρέπει να είναι προσπελάσιμοι μόνο από εξουσιοδοτημένες οντότητες. Οι υπηρεσίες που διασφαλίζουν την εμπιστευτικότητα είναι η υπηρεσία Εμπιστευτικότητας Επιλεγμένου Πεδίου (Selected Field Confidentiality Service), που παρέχει εμπιστευτικότητα συγκεκριμένων πεδίων στα δεδομένα μιας σύνδεσης ή σε μεμονωμένα τμήματά τους και η υπηρεσία Εμπιστευτικότητας Ροής Κίνησης (Traffic Flow Confidentiality Service), που προστατεύει πληροφορίες που μπορεί να αποκαλυφθούν από επιθέσεις τύπου ανάλυσης κίνησης (traffic analysis). Η διαθεσιμότητα είναι η εξασφάλιση ότι οι υπολογιστές, τα δίκτυα και τα δεδομένα θα είναι προσπελάσιμα χωρίς αδικαιολόγητη καθυστέρηση σε εξουσιοδοτημένους χρήστες. Άλλες βασικές αρχές είναι η αυθεντικότητα δηλαδή η διαβεβαίωση για την ταυτότητα μιας οντότητας, ο έλεγχος πρόσβασης που είναι η προστασία από μη εξουσιοδοτημένη χρήση των πόρων ενός υπολογιστικού συστήματος, η εξουσιοδότηση, η απονομή ευθυνών και η μη αποποίηση δηλαδή η προστασία από την δόλια άρνηση μιας οντότητας ότι έλαβε μέρος σε μια ανταλλαγή πληροφοριών. Η ασφάλεια ενός πληροφοριακού συστήματος είναι μια αλυσίδα και είναι τόσο ασφαλές όσο ο πιο αδύναμος κρίκος αυτής της αλυσίδας. (Μαυρίδης, 2015)

3.2.5 Ακεραιότητα δεδομένων που ανταλλάσσονται

Η ακεραιότητα (Integrity) είναι μια ακόμη βασική αρχή της ασφάλειας των συστημάτων που αναφέρεται στη διατήρηση των δεδομένων ενός πληροφοριακού συστήματος σε μια γνωστή κατάσταση χωρίς ανεπιθύμητες τροποποιήσεις, αφαιρέσεις ή προσθήκες από μη εξουσιοδοτημένα άτομα, καθώς και την αποτροπή της πρόσβασης ή χρήσης των υπολογιστών και δικτύων του συστήματος από άτομα χωρίς άδεια. Τα δεδομένα πρέπει να διασώζονται σε περιπτώσεις βλαβών υλικού και δυσλειτουργιών του λογισμικού στο μέτρο που είναι εφικτό. Οι τροποποιήσεις πρέπει να γίνονται μόνο από εξουσιοδοτημένους χρήστες και κάθε φορά να επιστρέφονται τα δεδομένα που έχουν αποθηκευτεί. Αν υπάρξει οποιαδήποτε παράβαση της ακεραιότητας, οι ενδιαφερόμενοι χρήστες πρέπει τουλάχιστον να ειδοποιούνται.

Πιο συγκεκριμένα, τα δεδομένα ενός συστήματος πρέπει να είναι προστατευμένα από φυσικά προβλήματα όπως πτώση τάσης ρεύματος, ούτως ώστε να είναι δυνατή η επανάκτηση των δεδομένων μετά από μια φυσική καταστροφή. Το σύστημα παρέχει μηχανισμούς, ώστε κατόπιν εμφάνισης τέτοιων περιστατικών να είναι δυνατή η ανάκαμψη από το σφάλμα και η ανάκτηση των δεδομένων. Η τήρηση εφεδρικών αντιγράφων είναι ένας σημαντικός μηχανισμός υποστήριξης της φυσικής ακεραιότητας των δεδομένων, αντιγράφοντας τα περιεχόμενα των δίσκων της βάσης δεδομένων σε άλλα φυσικά μέσα αποθήκευσης όπως δισκέτες, CD, εξωτερικούς δίσκους κλπ. Για τα εφεδρικά αντίγραφα είναι σημαντικό να μπορούν να λαμβάνονται όταν η βάση δεδομένων βρίσκεται σε λειτουργία, με άλλα λόγια να είναι δυνατόν να διενεργούνται δοσοληψίες στη βάση δεδομένων όσο διαρκεί η λήψη του εφεδρικού αντιγράφου. Επίσης, είναι απαραίτητο να υπάρχουν ταχείες διαδικασίες ανάκαμψης μέχρι να τεθεί το σύστημα σε πλήρη διαθεσιμότητα να είναι κατα το δυνατόν μικρότερος.

Με κύριο στόχο την ανάκτηση των δεδομένων έχουν αναπτυχθεί και υπηρεσίες που διασφαλίζουν την έγκυρη μετάδοση των δεδομένων, οι οποίες είναι: (1) η υπηρεσία Ακεραιότητας Σύνδεσης Επιλεγμένου Πεδίου (Selected Field Connection Integrity Service), που διατηρεί την ακεραιότητα μεμονωμένων πεδίων δεδομένων μιας σύνδεσης, (2) η υπηρεσία Ακεραιότητας Άνευ Εγκατάστασης Σύνδεσης (Connectionless Integrity Service), η οποία παρέχει ακεραιότητα μεμονωμένων τμημάτων δεδομένων, (3) η υπηρεσία Ακεραιότητας Επιλεγμένου Πεδίου Άνευ Εγκατάστασης Σύνδεσης (Selected Field Connectionless Integrity Service), η οποία εξασφαλίζει ακεραιότητα συγκεκριμένων πεδίων σε μεμονωμένα τμήματα δεδομένων, (4) η υπηρεσία Ακεραιότητας Σύνδεσης με Αποκατάσταση (Connection Integrity Service With Recovery), που εξασφαλίζει ακεραιότητα των δεδομένων μιας σύνδεσης, ενώ σε περίπτωση απώλειας της ακεραιότητας είναι δυνατή η ανάκτησή της και (5) η υπηρεσία Ακεραιότητας Σύνδεσης Χωρίς Αποκατάσταση (Connection Integrity Service Without Recovery), η οποία παρέχει μόνον ακεραιότητα δεδομένων χωρίς να είναι εφικτή η ανάκτηση της ακεραιότητας σε περίπτωση απώλειάς της. (Μαυρίδης, 2015)

3.2.6 Περιορισμοί από το θεσμικό πλαίσιο

Το ΕΚΑΒ αποκτά υπόσταση ως νομικό πρόσωπο δημοσίου δικαίου το 1985 (ιδρυτικός Ν.1579/85 άρθρο 7, ΦΕΚ217/Α/28-12-1985). Οι αεροδιακομιδές ωστόσο ως σύστημα δεν προβλέπονται σε κανένα από τα δυο προαναφερθέντα νομοθετήματα. Σκοπός του ΕΚΑΒ όπως καθορίζεται από τον συγκεκριμένο νόμο, είναι ο συντονισμός της παροχής σε έκτακτες περιπτώσεις άμεσης βοήθειας και επείγουσας ιατρικής φροντίδας στους πολίτες και η μεταφορά των πολιτών αυτών σε μονάδες παροχής υπηρεσιών υγείας.

Το άρθρο 31 του Ν.2072/1992 (ΦΕΚ125/Α/23-07-1992) καθορίζει λεπτομέρειες που αφορούν τη δαπάνη μεταφοράς βαρέως πασχόντων ασθενών. Αναφέρεται για πρώτη φορά η ανάγκη καθορισμού τρόπου μεταφοράς και παραπέμπει ο νομοθέτης σε επικείμενη Υπουργική Απόφαση.

Εκδίδεται στις 20.09.1994 η 9239 Υπουργική Απόφαση (ΦΕΚ727/Β/27-09-1994) η οποία καθορίζει την ανάθεση των Αεροδιακομιδών στο ΕΚΑΒ σε συνεργασία με το Αερογειονομικό του Ελληνικού και τη Διεύθυνση Υγιεινής της Νομαρχίας Πειραιά. Δίνεται στην παράγραφο Β η δυνατότητα στο ΕΚΑΒ για ναύλωση εναέριων ή πλωτών μέσων για την μεταφορά βαρέως πασχόντων. Το ΕΚΑΒ συνεργάζεται με την Ολυμπιακή Αεροπορία/Αεροπλοΐα, συνεπικουρούμενο όταν και όποτε χρειάζεται από τα ιπτάμενα μέσα της Π.Α. και του Πολεμικού Ναυτικού (Π.Ν.)για την αεροδιακομιδή ασθενών.

Η Υπουργική Απόφαση 9196/09.10.1995 (ΦΕΚ874/Β/20-0-1995) τροποποιεί την προαναφερθείσα ως προς την παράγραφο Α, καταργώντας το Αερογειονομικό του Ελληνικού και την συνεργασία με τη Διεύθυνση Υγιεινής της Νομαρχίας Πειραιά. Προκύπτει από τη λήξη της συνεργασίας αυτής η ανάγκη για δομές που θα συντονίζουν τις Αεροδιακομιδές εκ μέρους του ΕΚΑΒ. Δημιουργείται το Συντονιστικό Κέντρο το οποίο έδρευε στο παλιό Αεροδρόμιο του Ελληνικού.

Το 2000 το ΕΚΑΒ παραλαμβάνει 5 ελικόπτερα A-109E Augusta με αποκλειστικό ρόλο την διακομιδή ασθενών. Για την εκμετάλλευσή τους υπογράφει σύμβαση με την Helitalia. Τα τρία μείζονα ατυχήματα έως και το 2003 (Βλέπε Παράρτημα "ΣΤ" σελ.101) οδηγούν σε απόφαση ενσωμάτωσης των ελικοπτέρων στην Π.Α. για την Επιχειρησιακή εκμετάλλευσή τους. Δημιουργείται το Σμήνος Ελικοπτέρων Άμεσης Βοήθειας (ΣΕΑΒ) με τα τρία A-109E, το οποίο εντάσσεται στην 358ΜΕΔ (358 Μοίρα Έρευνας Διάσωσης) η οποία επανδρώνεται και με ελικόπτερα S.Puma.

Ουσιαστικά και μέχρι την πλήρη αξιοποίηση των ελικοπτέρων, το έργο των Αεροδιακομιδών αναλαμβάνει η Πολεμική Αεροπορία με ελικόπτερα S.Puma και αεροσκάφη C-130, γεγονός το οποίο δεν επρόκειτο να αλλάξει αφού αποφασίζεται η ΜΗ χρήση των ελικοπτέρων A-109E σε νυχτερινές αποστολές. Την αλλαγή αυτή στον τρόπο εκτέλεσης του έργου των Αεροδιακομιδών νομιμοποιεί και τυπικά Υπουργική Απόφαση, ΦΕΚ746/02.06.2005, σύμφωνα με το Άρθρο 1 της οποίας, το έργο των αεροδιακομιδών ανατίθεται στον Αρχηγού του Γενικού Επιτελείου Αεροπορίας (Α/ΓΕΑ) επ' ωφελεία ΕΚΑΒ. Η δυνατότητα ανάθεσης αρμοδιοτήτων πηγάζει από τον Ν.1558/1985 (ΦΕΚ 136/Α/26.07.1985, μεταβίβαση αρμοδιοτήτων από τον Υπουργό Εθνικής Άμυνας προς προϊσταμένους) και τον Ν.2292/1995 (ΦΕΚ 35/Α/15.02.1995 περί Οργάνωσης και λειτουργίας Υπουργείου Εθνικής Άμυνας). Τα πτητικά μέσα τα οποία δύναται να χρησιμοποιηθούν είναι κατ' αρχήν της Π.Α. και αν απαιτηθεί του Γενικού Επιτελείου Εθνικής Άμυνας (ΓΕΕΘΑ).

Το 2015 με σκοπό την επικαιροποίηση του συστήματος των αεροδιακομιδών, εκδίδεται Υπουργική Απόφαση ΦΕΚ 2758/Β/18.12.2015 σύμφωνα με το Άρθρο 1 της οποίας ανατίθεται στον Α/ΓΕΑ η οργάνωση της διάθεσης των μέσων, ο συντονισμός και η εκτέλεση του πτητικού έργου των αεροδιακομιδών υγείας επ' ωφελεία ΕΚΑΒ.

Δύο είναι οι σημαντικές αλλαγές από την προηγούμενη Υπουργική Απόφαση του 2005:

α. Προστίθενται πτητικά μέσα του Πυροσβεστικού Σώματος (Π.Σ.) και του Λιμενικού Σώματος (Λ.Σ.) πλέον αυτών της Π.Α. και του ΓΕΕΘΑ. Για την αξιοποίηση των διατιθέμενων από το Π.Σ. πτητικών μέσων υπογράφηκε Μνημόνιο Συνεργασίας μεταξύ Π.Α. και Π.Σ.27. Τα πτητικά μέσα του Λ.Σ. σε αντίθεση με τις προβλέψεις του προαναφερθέν νόμου δεν διατέθηκαν για σκοπούς αεροδιακομιδών.

β. Στο Άρθρο 2 παρ 1 αναφέρεται ότι η διάθεση και χρήση των μέσων των φορέων θα καθορισθεί με μνημόνιο συνεργασίας που θα συναφθεί μεταξύ των εμπλεκόμενων μερών. Αναφορά στα μνημόνια συνεργασίας θα γίνει σε παράγραφο που ακολουθεί και αφορά την Οργάνωση και Λειτουργία των Αεροδιακομιδών.

Η πιο πρόσφατη Κοινή Υπουργική Απόφαση ΦΕΚ 205/Α/31-10-2016 στο Άρθρο 61 ρυθμίζει κυρίως θέματα δαπανών του Υπουργείου Υγείας. Το κόστος των αποστολών αεροδιακομιδής, όπως αυτό υπολογίζεται βάσει του ΦΕΚ 2808/Β/08.11.2013 (Κοστολόγηση Παρεχομένων Υπηρεσιών και Οικονομική Τακτοποίηση των Δοσοληψιών των Κλάδων των Ε.Δ.), βαρύνει τον Εθνικό Οργανισμό Παροχής Υπηρεσιών Υγείας (ΕΟΠΥΥ) για τους δικαιούχους περίθαλψης, τους ανασφάλιστους και τους οικονομικά αδύνατους. Στην περίπτωση αεροδιακομιδής αλλοδαπών, το κόστος βαρύνει τον ασθενή ή τον ασφαλιστικό του φορέα αυτού (ιδιωτικό ή δημόσιο) μέσω πρεσβειών. Ειδικά για Ευρωπαίους πολίτες ισχύει η ΟΔΗΓΙΑ 2011/24/ΕΕ του ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ και του ΣΥΜΒΟΥΛΙΟΥ της 9ης Μαρτίου 2011 περί εφαρμογής των δικαιωμάτων των ασθενών στο πλαίσιο της διασυνοριακής υγειονομικής περίθαλψης. Η Οδηγία διευκρινίζει τα δικαιώματα των ασθενών για πρόσβαση σε ασφαλή και καλής ποιότητας περίθαλψη σε διασυνοριακή βάση εντός της Ευρωπαϊκής Ένωσης και καθορίζει θέματα οικονομικής φύσης. Σημαντική είναι η δυνατότητα που δίνεται στο ΕΚΑΒ, κατόπιν έγκρισης του Υπουργού Υγείας, για σύναψη σύμβασης με αεροπορικές εταιρίες ή άλλες εταιρίες μεταφορών για μίσθωση μέσων στην περίπτωση που τα δικά του μέσα δεν επαρκούν για την κάλυψη των αναγκών του. Με αυτή την παράγραφο ανοίγει ο δρόμος για χρήση του ιδιωτικού μοντέλου στο σύστημα αεροδιακομιδών. (Κοτρέτσου, 2017)

3.2.7 Απαιτήσεις ακεραιότητας καταγραφής γεγονότων και περιεχομένων επικοινωνιών

Ως λειτουργικές απαιτήσεις, το σύστημα πρέπει να είναι εύχρηστο και φιλικό στο χρήστη ώστε να μπορεί γρήγορα και εύκολα να καταχωρεί δεδομένα. Αρχικά, πρέπει ο χρήστης να δηλώσει όνομα χρήστη και κωδικό για να αποκτήσει πρόσβαση στο σύστημα. Κατόπιν εισαγωγής στο σύστημα, να επιβεβαιωθεί από τους μηχανισμούς διαπίστευσης χρηστών ότι ο λογαριασμός του είναι υπαρκτός, δηλαδή καταχωρημένος στον πίνακα χρηστών της βάσης δεδομένων, έγκυρος με όλα τα στοιχεία του σωστά καταχωρημένα στο σύστημα και ενεργός, δηλαδή δεν έχει απενεργοποιηθεί από τον διαχειριστή. Στη συνέχεια, ο χρήστης πρέπει να μπορεί να αναγνωρίσει ποιες ενέργειες μπορεί να εκτελέσει στο σύστημα είτε με το να εμφανίζονται μόνο τα πεδία που μπορεί να προσπελάσει και έχει δικαιώματα πρόσβασης είτε να εμφανίζονται προειδοποιητικά μηνύματα σε περίπτωση που θελήσει να προχωρήσει σε ενέργεια που δεν είναι εξουσιοδοτημένος να κάνει. Αυτός ο περιορισμός ισχύει και για προβολή δεδομένων από τη βάση αλλά και για την τροποποίηση τους. Θα πρέπει επίσης να υπάρχει ξεχωριστή σελίδα που να περιγράφει τα δικαιώματα στατικά ή δυναμικά που παραχωρούνται στον εκάστοτε χρήστη. Ακόμη, οι φόρμες που θα συμπληρώνει ο χρήστης πρέπει να είναι εύχρηστες και καθοδηγούμενες με υποδείξεις λαθών, ώστε να υπάρχει έλεγχος των δεδομένων που εισάγονται στην βάση. Έτσι μειώνεται η πιθανότητα λάθους του χρήστη που καλείται να καταχωρήσει έναν τεράστιο όγκο δεδομένων σε σύντομο χρονικό διάστημα. (Σαϊδης, 2017-2018)

Ως μη λειτουργικές απαιτήσεις εννοούνται η διαθεσιμότητα, η ασφάλεια, η πληρότητα, η αποδοτικότητα και η υποστήριξη διεθνών προτύπων, η επικοινωνία, η οργάνωση, η σχεδίαση και φυσικές απαιτήσεις συσκευών και περιβάλλοντος λειτουργίας. Όπως έχουμε προαναφέρει τα δεδομένα πρέπει να είναι διαθέσιμα στους εξουσιοδοτημένους χρήστες σε πραγματικό χρόνο. Η έννοια της ασφάλειας των δικτύων και των πληροφοριακών συστημάτων περιλαμβάνει την φυσική ασφάλεια των δικτύων, που αποβλέπει στην μέγιστη δυνατή ακεραιότητα και διαθεσιμότητα των υποδομών και των αντίστοιχων υπηρεσιών, την διασφάλιση του απορρήτου των πληροφοριών και σχετικών δεδομένων που διακινούνται μέσω των δικτύων και την διασφάλιση των προσωπικών δεδομένων των χρηστών των δικτύων. Το πληροφοριακό περιεχόμενο της βάσης δεδομένων είναι αποδεκτό μόνο όταν ικανοποιούνται συνθήκες πληρότητας των καταχωρημένων στοιχείων. Το σύστημα πρέπει να κάνει καλή διαχείριση του αποθηκευτικού χώρου και όχι αλόγιστη χρήση των πόρων του συστήματος, να είναι γρήγορο και αξιόπιστο. Όσο αναφορά την οργάνωση των δεδομένων να διεκπεραιώνει πολλές δοσοληψίες και να εξυπηρετεί αποδοτικά πολλούς χρήστες ταυτόχρονα. Ακόμη, πρέπει να είναι μεταφέρσιμο, να μπορεί να εγκατασταθεί σε διάφορα συστήματα και να συνεργάζεται με άλλα συστήματα, συσκευές ή λογισμικά. (Βεσκούκης, 2015)

3.2.8 Σημεία που χρήζουν προσοχής – αδυναμίες του σημερινού συστήματος

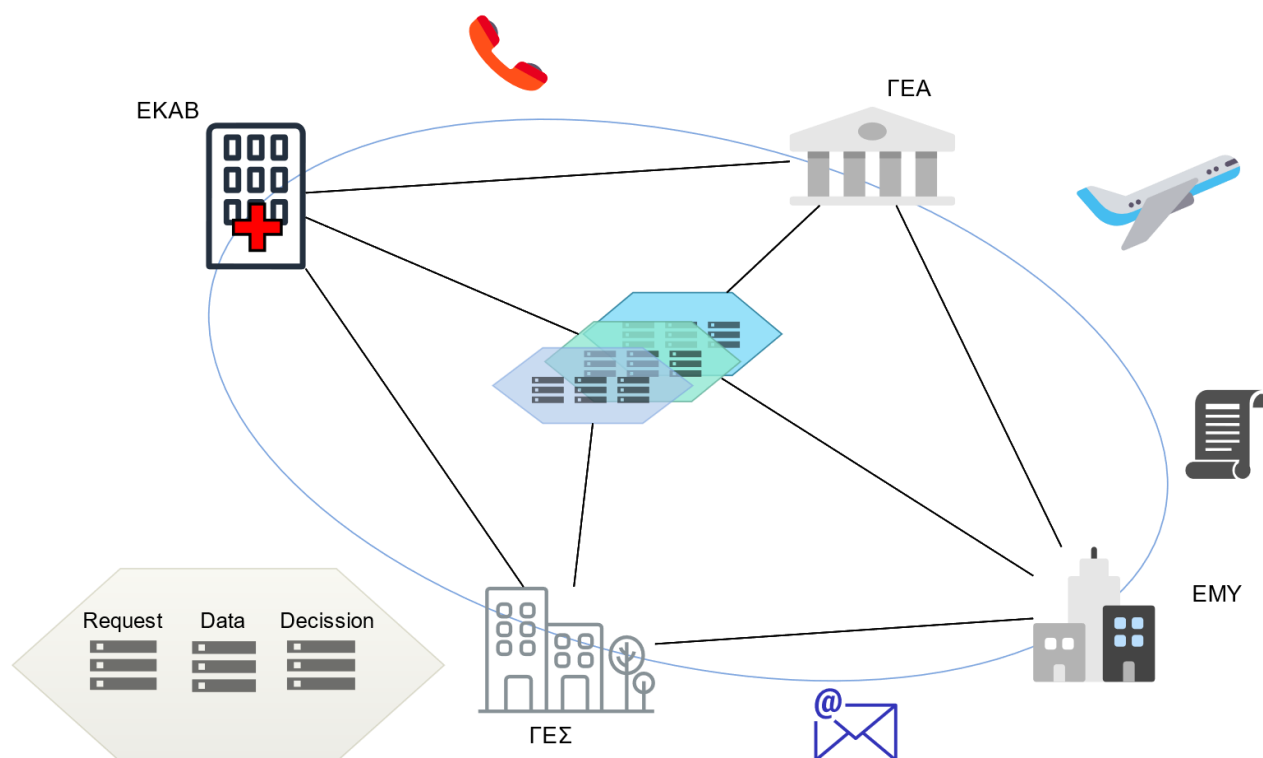
Το σημερινό σύστημα πολιτικής προστασίας που αναλαμβάνει τον χειρισμό έκτακτων αναγκών όπως είναι η αεροδιακομιδή παρουσιάζει αρκετές αδυναμίες που χρήζουν βελτίωσης. Βασίζεται στην λειτουργία πολλών συστημάτων συντονισμού ανά υπηρεσία που είναι δύσκολο να επικοινωνήσουν άμεσα και να δώσουν αποτελεσματική λύση στο εκάστοτε περιστατικό. Απαιτείται μεγάλο χρονικό διάστημα για την επικοινωνία των φορέων μεταξύ τους, την συλλογή δεδομένων και πληροφοριών από τα διάφορα πληροφοριακά συστήματα

και τις υπηρεσίες, ώστε να καταστεί δυνατή η λήψη απόφασης αντιμετώπισης του προβλήματος. Σε κάθε υπηρεσία εμπλέκονται πολλά άτομα, προϊστάμενοι, προσωπικό βάρδιας, συντονιστές που πρέπει να επεξεργαστούν τις συλλεγόμενες πληροφορίες και να ενημερώσουν για τα δεδομένα εξουσιαδοτημένα μέλη άλλων αρμόδιων φορέων. Ο καθολικός συντονισμός λοιπόν είναι δύσκολος, χρονοβόρος και αναποτελεσματικός, γεγονός που συμβάλλει στην άδικη απώλεια ανθρώπινων ζώων.

Σημαντική είναι και η έλλειψη ασφάλειας στις βάσεις δεδομένων που διατηρεί κάθε υπηρεσία για λογαριασμό της. Αδυναμία θεωρείται ένα τρωτό σημείο στο λογισμικό, το υλικό ή τις διαδικασίες ενός συστήματος το οποίο μπορεί να επιτρέψει την πρόσβαση σε μη εξουσιοδοτημένους χρήστες στις πληροφορίες του συστήματος ή να οδηγήσει στην απώλεια δεδομένων λόγω λάθους χειρισμού από κάποιο χρήστη. Το σύστημα μπορεί να δεχτεί απειλές ακούσιες ή εκούσιες. Ακούσιες είναι οι απειλές που δεν έχουν προκληθεί σκόπιμα αλλά απο λάθη στο σχεδιασμό ή τη χρήση συστημάτων ή ακόμα από καταστροφές και η αντιμετώπιση των οποίων δεν έχει προβλεφθεί όπως για παράδειγμα μια φυσική καταστροφή. Εκούσιες είναι οι απειλές που σχεδιάζονται και υλοποιούνται απο ένα πρόσωπο με σκοπό τη διάρκεια στην ασφάλεια ενός συστήματος βάσεων δεδομένων. Σύμφωνα με τις τελευταίες εκθέσεις ασφάλειας, οι hackers θεωρούν τα τρωτά σημεία μιας βάσης δεδομένων ως τα κύρια ελαττώματα που μπορούν να εκμεταλλευτούν προκειμένου να παρακάμψουν την άμυνα του στόχου τους.

Συνέπεια όλων των παραπάνω είναι η έλλειψη διαφάνειας στους χειρισμούς των φορέων κατά την αντιμετώπιση του περιστατικού, καθώς και στους πόρους που διατίθενται για την αντιμετώπισή του. Αναλυτικά, δεν υπάρχει αμετάβλητη μεταφορά των δεδομένων, των συντονιστικών ενεργειών, των επικοινωνιών και των αποφάσεων που λαμβάνονται καθώς και καταγραφή όλη της ροής απο την πηγή στον προορισμό ώστε να ελέγχονται σε όλα τα στάδια μεταφοράς τους. Το γεγονός ότι δεν καταγράφονται καθολικά όλες οι απαραίτητες πληροφορίες δεν δίνει τη δυνατότητα ελέγχου στο καταμερισμό ευθυνών σε περιπτώσεις κακού συντονισμού. Τέλος, δεν εξασφαλίζεται η διαφάνεια στην διαχείριση των πόρων που απαιτούνται για τον χειρισμό έκτακτων αναγκών, δεν υπάρχει δυνατότητα καταχώρησης από πού προέρχονται και πού και πώς χρησιμοποιούνται. Και αυτό θα μπορούσε εύκολα να οδηγήσει σε φαινόμενα διαφθοράς.

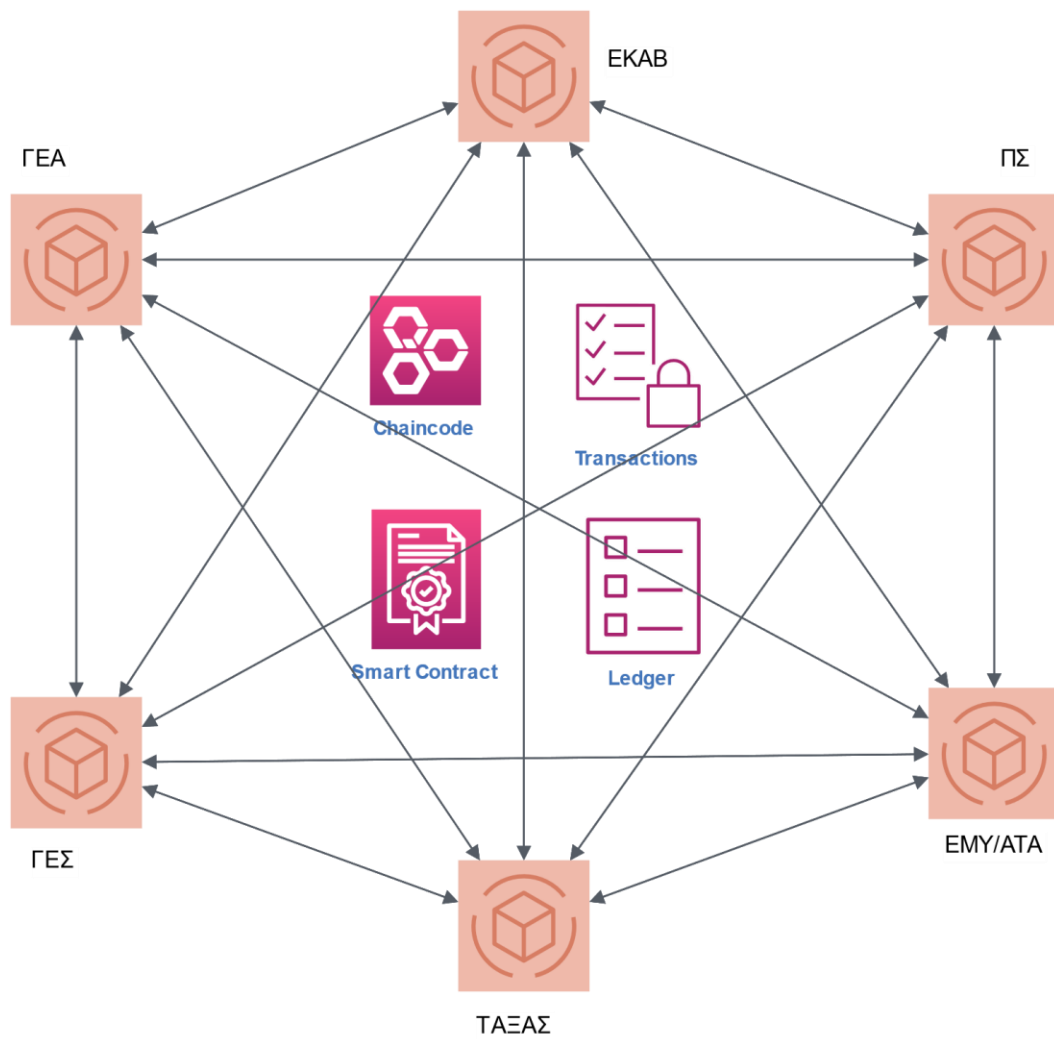
3.3 Αρχιτεκτονική πολλαπλών οργανισμών στο Hyperledger



Εικόνα 11 Business model diagram: Επικοινωνία με Blockchain

3.3.1 Μια αρχιτεκτονική με Blockchain

Στο παρακάτω διάγραμμα (εικόνα 12) οι οργανισμοί αναπαρίστανται ως κόμβοι του δικτύου. Συγκεκριμένα, οι αρμόδιοι φορείς που εμπλέκονται στο Blockchain δίκτυο για αεροδιακομιδή είναι το Κέντρο Άμεσης Βοήθειας (ΕΚΑΒ), το Γενικό επιτελείο Αεροπορίας (ΓΕΑ), η Εθνική Μετεωρολογική Υπηρεσία (ΕΜΥ), το Γενικό Επιτελείο Στρατού (ΓΕΣ), το Πυροσβεστικό Σώμα (ΠΣ) και την την Ταξιαρχία Αεροπορίας Στρατού (ΤΑΞΑΣ). Όπως συμβαίνει σε κάθε Blockchain δίκτυο δημιουργούν μεταξύ τους έξυπνα συμβόλαια (smart contracts), στα οποία καθορίζονται οι ρόλοι, τα όρια και τα δικαιώματα που έχει ο κάθε κόμβος στο δίκτυο. Τα smart contracts στη συνέχεια ταξινομούνται σε blocks, τα οποία αποθηκεύονται στο blockchain δίκτυο σε αλυσιδωτή μορφή (chaincode), όπως φαίνεται στη εικόνα 13. Κάθε φορά που επιτελείται μια συναλλαγή μεταξύ δύο κόμβων διατηρούν ένα αντίγραφο της συναλλαγής στο ledger ο καθένας με όλες τις σχετικές λεπτομέρειες. Αντίθετα, οι υπόλοιποι κόμβοι έχουν πρόσβαση μόνο στην σελίδα που περιέχει την λίστα των συναλλαγών με καταγραφή ημερομηνίας και ώρας χωρίς αναλυτικές λεπτομέρειες. Με αυτό το τρόπο εξασφαλίζεται το απόρρητο στις ιδιωτικές συναλλαγές ανάμεσα σε μέλη που ανήκουν στο ίδιο δίκτυο Blockchain.



Εικόνα 12 Αρχιτεκτονική του Hyperledger Fabric στην αεροδιακομιδή



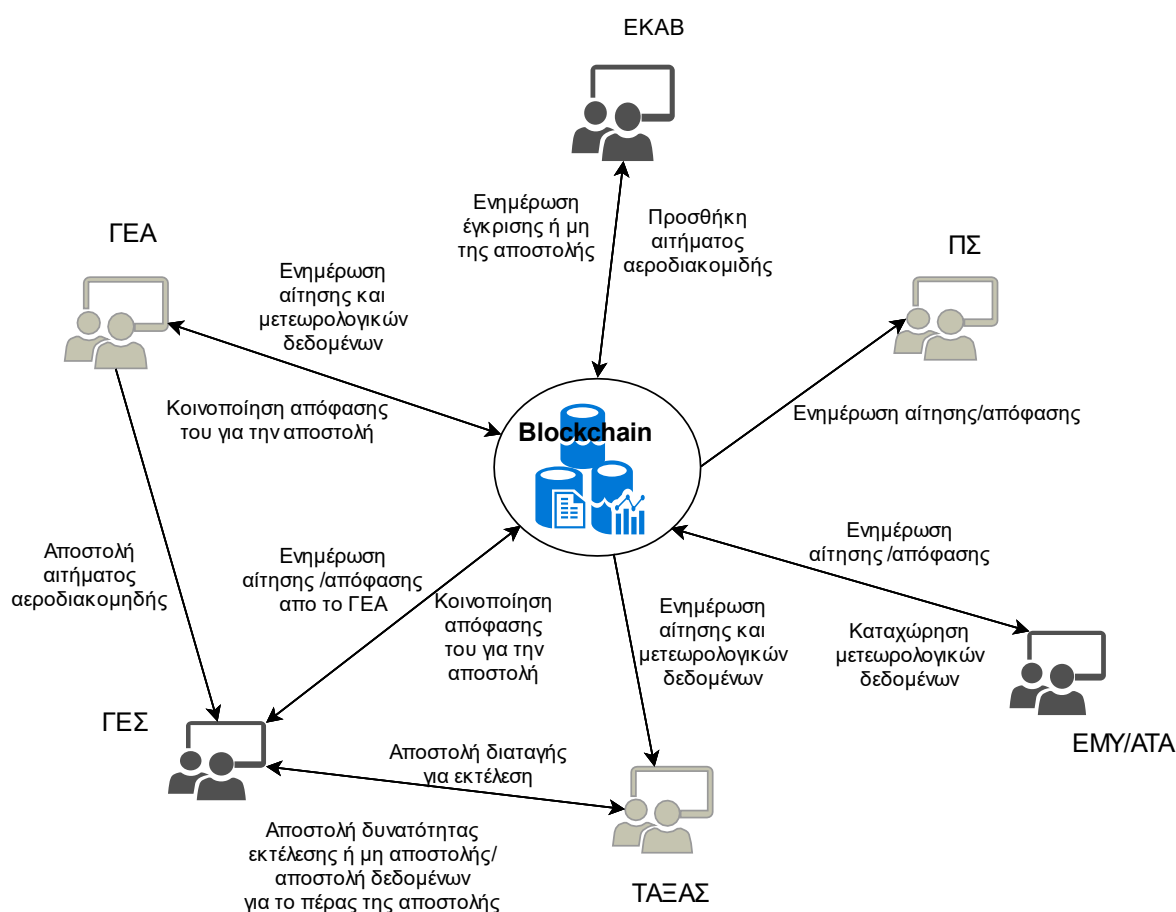
Εικόνα 13 Insertion of a block into a chaincode

3.3.2 Ρυθμίσεις και ρόλοι

Οι ρυθμίσεις και οι ρόλοι σε ένα δίκτυο Blockchain καθορίζονται από τα smart contracts. Τα smart contracts είναι τα ψηφιακά συμβόλαια που δημιουργούνται και εκτελούνται στο Blockchain. Όπως έχουμε προαναφέρει, πρόκειται ουσιαστικά για μια σύμβαση που κωδικοποιείται με υπολογιστή και έχει συγκεκριμένους όρους που καθορίζονται σε αυτήν (όπως ένα συμβατικό συμβόλαιο) και όταν εκπληρωθεί δημιουργείται μια συναλλαγή ή άλλο αποτέλεσμα (ενημέρωση ή ειδοποίηση) όπως έχουν συμφωνήσει τα μέλη που το δημιούργησαν. Σε ένα Blockchain δίκτυο για αεροδιακομιδές, τα μέλη ΕΚΑΒ, ΓΕΑ, ΕΜΥ, ΓΕΣ, ΠΣ, ΤΑΞΑΣ συνάπτουν smart contracts που καθορίζουν τις αρμοδιότητες του κάθε μέλους, τον αριθμό και τα διαπιστευτήρια των χρηστών (ώστε να είναι εξειδικευμένοι οι αρμόδιοι χρήστες του συστήματος), τις πληροφορίες που πρέπει να διατίθενται στην πλατφόρμα, τον χρόνο απόκρισης, τα χρονικά όρια για την εξέταση του αιτήματος της αεροδιακομιδής, τον βαθμό πρόσβασης στα δεδομένα και τη διασφάλιση του απορρήτου ιδιαίτερων πληροφοριών ή συναλλαγών. Συνήθως, τα smart contracts περιέχουν και οικονομικές ρήτρες και ως προς τις συναλλαγές ανάμεσα στα μέλη αλλά και οικονομικές υποχρεώσεις των μελών προς το δίκτυο. Στην συγκεκριμένη περίπτωση όμως επειδή τα μέλη είναι κρατικοί φορείς και ο σκοπός λειτουργίας του δικτύου είναι κοινωφελής δεν υπάρχουν οικονομικές υποχρεώσεις και ρήτρες, κι έτσι αναπτύσσεται σε περιβάλλον Hyperledger Fabric.

Ως προς την ανάλυση των ρόλων στο Blockchain της αεροδιακομιδής, το ΕΚΑΒ καταχωρεί τα αιτήματα των αεροδιακομιδών με υποχρέωση να δίνει αναλυτικά τα στοιχεία της βαρύτητας του περιστατικού, του βαθμού προτεραιότητας, τους τόπους αναχωρήσεως και προορισμού, καθώς και χρονικά περιθώρια. Η ΕΜΥ εφόσον λάβει γνώση για ένα αίτημα καλείται να παραδώσει όλα τα μετεωρολογικά δεδομένα για τις περιοχές που πρέπει να καλύψει η αεροδιακομιδή με την μεγαλύτερη δυνατή έγκυρη πρόγνωση και παράλληλα να δώσει στοιχεία με χάρτες, στατιστικά και εικόνες από δορυφόρο. Το ΓΕΑ κατόπιν του αιτήματος και των δεδομένων από την ΕΜΥ, αξιολογεί την δυνατότητα που έχει και εγκρίνει ή όχι την αεροδιακομιδή. Έχει πρόσβαση σε όλα τα δεδομένα που έχουν εισαχθεί στο ledger μέχρι τώρα και την δυνατότητα να εκτελέσει ιδιωτική συναλλαγή. Το ΓΕΣ και το ΤΑΞΑΣ έχουν παρόμοια προσβασιμότητα ως προς τα δεδομένα και τις ιδιωτικές συναλλαγές. Το ΠΣ ενημερώνεται από το δίκτυο σχετικά με την έκβαση του αιτήματος.

3.3.3 Αντιστοίχιση ενεργειών και αρμοδιοτήτων σε περιβάλλον Blockchain



Εικόνα 14 Communication Diagram: Τρόπος επικοινωνίας οργανισμών για αεροδιακομιδή με blockchain σύστημα

Η λειτουργία του συστήματος επικοινωνίας ανάμεσα στους οργανισμούς που σχετίζονται με μια αεροδιακομιδή εικονίζεται στο παραπάνω διάγραμμα. Όλοι οι κόμβοι επικοινωνούν με το Blockchain δίκτυο, από το οποίο λαμβάνουν γνώση αρχικά για το αίτημα αεροδιακομιδής από το ΕΚΑΒ. Οι πρώτοι που κινητοποιούνται είναι το ΓΕΑ και η ΕΜΥ. Η ΕΜΥ κοινοποιεί τις μετεωρολογικές προγνώσεις στις ζητούμενες περιοχές από κάθε αίτημα που δέχεται το Blockchain. Το ΓΕΑ λαμβάνοντας όλα τα δεδομένα αποφασίζει αν θα εκτελέσει ή όχι την αεροδιακομιδή. Αν η αεροδιακομιδή εγκριθεί, το ΓΕΑ ενημερώνει το Blockchain και μετά την πραγματοποίηση της αεροδιακομιδής καταχωρούνται όλα τα στοιχεία της εκτέλεσής της που παραμένουν στο ιστορικό του ledger.

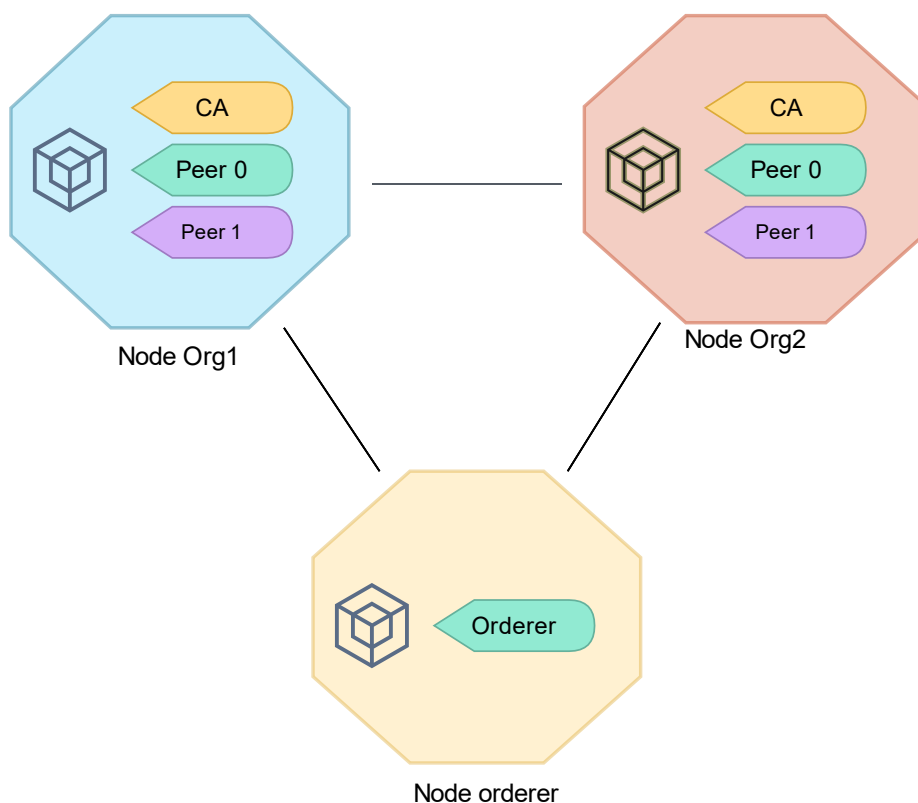
Σε περίπτωση απόρριψης του αιτήματος, το ΓΕΑ ενημερώνει το Blockchain και στέλνει ιδιωτικό αίτημα διερεύνησης αεροδιακομιδής στο ΓΕΣ. Το ΤΑΞΑΣ ενημερώνεται για την αποστολή αιτήματος του ΓΕΑ προς το ΓΕΣ από το Blockchain. Εξετάζει τις μετεωρολογικές προγνώσεις που λαμβάνει μέσω του Blockchain και τα δεδομένα από την βάση του για την καταλληλότητα του αεροδρομίου, τα ιπτάμενα μέσα και τα πληρώματα και αποδέχεται την δυνατότητα πραγματοποίησης της αεροδιακομιδής ή όχι. Πραγματοποιείται ιδιωτική συναλλαγή του ΤΑΞΑΣ και του ΓΕΣ με όλα τα δεδομένα της δυνατότητας ή μη της πραγματοποίησης της αποστολής. Στην συνέχεια, το ΓΕΣ αποφασίζει αν θα εγκρίνει το αίτημα

της αεροδιακομιδής ή όχι και ενημερώνει το Blockchain. Αν η απόφαση είναι αρνητική η διαδικασία ολοκληρώνεται και όλα τα δεδομένα καταχωρούνται στο ιστορικό του ledger. Διαφορετικά, το ΓΕΣ στέλνει ιδιωτικά διαταγή στο ΤΑΞΑΣ να εκτελέσει την αποστολή και κοινοποιεί την αποδοχή του αιτήματος στο Blockchain. Τέλος, τα δεδομένα για το πέρας της αποστολής προστίθενται στο ιστορικό του ledger.

Σε όλη τη διάρκεια της διαδικασίας οι κόμβοι που πραγματοποιούν ιδιωτικές συναλλαγές διατηρούν αντίγραφα των συναλλαγών στο ledger. Οι υπόλοιποι κόμβοι ενημερώνονται για κάθε συναλλαγή μόνο μέσω της πλατφόρμας του Blockchain με την ημερομηνία και την ώρα καταχώρησης χωρίς τη δυνατότητα προβολής λεπτομερειών, καθώς υπάρχει ξεχωριστή λίστα με όλο το ιστορικό των συναλλαγών, στην οποία έχουν πρόσβαση όλοι.

3.3.4 Βήματα υλοποίησης στο Hyperledger

Ένα σύστημα πολλαπλών οργανισμών μπορεί να προσομοιωθεί με τη δημιουργία ενός συστήματος Blockchain μεταξύ διαφορετικών εικονικών μηχανημάτων. Για δύο οργανισμούς χρειαζόμαστε τρία εικονικά μηχανήματα τα οποία περιγράφεται πως δημιουργούνται στο παράρτημα 1.



Εικόνα 15 Τοπολογία συστήματος Hyperledger Fabric για δύο οργανισμούς

Σύμφωνα με τις οδηγίες για την εγκατάσταση ενός συστήματος Blockchain σε δύο οργανισμούς (Sarvepalli, 2018), η τοπολογία του συστήματος(εικόνα 15) ορίζει στο πρώτο εικονικό μηχάνημα να είναι ο orderer, στο δεύτερο μηχάνημα να λειτουργεί ο πρώτος οργανισμός (εν συντομία org1) και να περιέχει την πιστοποίηση ταυτότητα (CA1) και τους συμμετέχοντες peers (org1peer0, org1peer1) και στο τελευταίο μηχάνημα να εντάσσεται ο δεύτερος οργανισμός (org2) με πιστοποίηση ταυτότητας (CA2) και αντίστοιχους peers (org2peer0, org2peer1).

Τα προαπαιτούμενα σε αυτό το σύστημα πρέπει να εγκατασταθούν σε όλα τα μηχανήματα και είναι:

- Λειτουργικό σύστημα Ubuntu-16.04
- Hyperledger Fabric – version1.2
- προγραμματιστική γλώσσα Go – version 1.9.3 ή μεγαλύτερο
- Docker – version 18.03.1-ce ή μεγαλύτερο
- Docker-Compose – version 1.18.0 ή μεγαλύτερο
- Node – version 8.11.3

Και στην συνέχεια να πραγματοποιήσουμε σε όλα τα μηχανήματα τις παρακάτω ρυθμίσεις:

Εγκατάσταση των αρχείων από την σελίδα του github:

```
git clone -b release-1.2 https://github.com/hyperledger/fabric-samples
```

Μετάβαση στα περιεχόμενα του φακέλου fabric-samples:

```
cd fabric-samples
```

Εγκατάσταση των εργαλείων και των βιβλιοθηκών του Hyperledger fabric:

```
curl -sSL http://bit.ly/2ysbOFE | bash -s 1.2.0
```

Αντιγραφή των αρχείων για τη δημιουργία συστήματος σε πολλαπλούς οργανισμούς από την σελίδα του github:

```
git clone https://github.com/mallikprojects/fabric-multi-network
```

Και μετάβαση στον υποφάκελο fabric-multi-network:

```
cd fabric-multi-network
```

Στην συνέχεια, για τη δημιουργία των κρυπτογραφημένων δεδομένων και των πιστοποιητικών ταυτοποίησης και των δύο οργανισμών, τρέχουμε στο πρώτο μηχάνημα την εντολή:

```
./bymn.sh generate crypto-config.yaml
```

Από την οποία παράγονται οι φάκελοι: crypto-config και channel-artifacts, οι οποίοι πρέπει να αντιγραφούν σε όλα τα μηχανήματα, καθώς επίσης και τα παρακάτω αρχεία:

docker-compose-orderer.yaml, που πρέπει να αντιγραφτεί στο πρώτο μηχάνημα

docker-compose-org1.yaml, που πρέπει να αντιγραφτεί στο δεύτερο μηχάνημα

docker-compose-org2.yaml, που πρέπει να αντιγραφτεί στο τρίτο μηχάνημα

Σε περίπτωση λάθους, ανοίγουμε το αρχείο configtx.yaml και αντικαθιστούμε την ενότητα Profiles από την αρχή στο τέλος του αρχείου. Και επαναλαμβάνουμε την εντολή

```
./bymn.sh generate crypto-config.yaml
```

Ολοκληρώνοντας την παραπάνω διαδικασία, ορίζουμε τις παρακάτω μεταβλητές περιβάλλοντος μέσα στο αρχείο bymn.sh ανάλογα με τα hostname που έχουν τα αντίστοιχα μηχανήματα και τέλος να βεβαιωθούμε ότι αυτές οι μεταβλητές είναι ορισμένες ίδια σε όλα τα μηχανήματα. Οι μεταβλητές μέσα στο αρχείο ορίζονται όπως παρακάτω:

```
export ORDERER_HOSTNAME=<host name of PC-1>
export ORG1_HOSTNAME= <host name of PC-2>
export ORG2_HOSTNAME=<host name of PC-3>
export SWARM_NETWORK="fabric"
```

την εντολή αυτή την αλλάζουμε αν επιθυμούμε να αλλάξουμε το όνομα του δικτύου docker swarm που θα δημιουργήσουμε στην συνέχεια

```
export DOCKER_STACK="fabric"
```

την εντολή αυτή την αλλάζουμε αν επιθυμούμε να αλλάξουμε το όνομα του δικτύου docker swarm που θα δημιουργήσουμε στην συνέχεια

Για την ενημέρωση του hostname ενός μηχανήματος αρκεί να τρέξουμε την εντολή:

```
hostname
```

στο εκάστοτε μηχάνημα.

Έπειτα, δημιουργούμε και ρυθμίζουμε το δίκτυο docker swarm. Ξεκινώντας τη διαδικασία, πρέπει να τρέξουμε στο πρώτο μηχάνημα τις εντολές:

```
docker swarm init --advertise-addr <PC-1 IP address>
docker swarm join-token manager
```

Τρέχοντας την δεύτερη εντολή, η οποία δηλώνει την επιθυμία της ένταξης μελών στο δίκτυο ως managers, παράγεται ένας κωδικός (token), οποίος πρέπει να συμπεριληφθεί στην παρακάτω εντολή από τα υπόλοιπα μηχανήματα για να εισέλθουν στο δίκτυο:

```
docker swarm join --token SWMTKN-1-
3anjn4oxwcn278hie3413zaakr4higjdqr2x89r5605p1dosui-a4u407pt6c5ta2ont7pqdnm
137.116.147.36:2377 --advertise-addr <PC-2 Ip Address>
```

```
docker swarm join --token SWMTKN-1-3anjn4oxwcn278hie3413zaakr4higjdqr2x89r5605p1dosui-a4u407pt6c5ta2ont7pqdnm137.116.147.36:2377 --advertise-addr <PC-3 Ip Address>
```

Παρόμοιες εντολές βγαίνουν και στο δικό μας μηχάνημα και πρέπει να τρέξουμε αυτές προσθέτοντας την επιλογή του `--advertise-addr <PC Ip Address>`, αντίστοιχα για κάθε μηχάνημα, ώστε να πάρουμε το token το δικό μας για να μπορεί να επιτύχει η εντολή.

Για να ελέγξουμε ότι έχει ολοκληρωθεί η σύζευξη των μηχανημάτων τρέχουμε την παρακάτω εντολή σε όποιο μηχάνημα επιθυμούμε:

```
docker node ls,
```

η οποία έχει το εξής αποτέλεσμα:

```
orgauser@orgA:~$ docker node ls
ID                                HOSTNAME    STATUS    AVAILABILITY    MANAGER STATUS    ENGINE VERSION
7xey887ge026e7t0eb5k424s4 *    orgA        Ready     Active           Leader            19.03.1
19383pyvtayvr1q6p4js00iaa      orgB        Ready     Active           Reachable         19.03.1
jdx182p35u71xk4r8q6n9yayb      orgC        Ready     Active           Reachable         19.03.1
orgauser@orgA:~$
```

Στα παρακάτω αποτελέσματα βλέπουμε ότι ο αρχηγός είναι ο πρώτος υπολογιστής με hostname να είναι orgA ενώ και οι υπόλοιποι δύο υπολογιστές με hostnames orgB και orgC αντίστοιχα, να έχουν ενταχθεί σωστά στο δίκτυο (έχουν βρεθεί στο κοινό δίκτυο).

Εφόσον έχουν ενταχθεί όλα τα μηχανήματα σε ένα δίκτυο, ορίζουμε το κοινό δίκτυο ως overlay network και του δίνουμε ένα όνομα μόνο στο πρώτο μηχάνημα:

```
docker network create --attachable --driver overlay fabric
```

που βγαίνει ως αποτέλεσμα η ταυτότητα του δικτύου με όνομα fabric.

Για την εκκίνηση των υπηρεσιών του orderer τρέχουμε στο πρώτο μηχάνημα την εντολή :

```
./bymn.sh up -f docker-compose-orderer.yaml
```

Και αντίστοιχα για τις υπηρεσίες των δύο οργανισμών στα άλλα δύο μηχανήματα τις εντολές:

```
./bymn.sh up -f docker-compose-org1.yaml
./bymn.sh up -f docker-compose-org2.yaml
```

Ολοκληρώνοντας αυτές τις εντολές, για να ελέγξουμε ότι όλα τα services λειτουργούν κανονικά τρέχουμε την εντολή:

```
docker service ls
```


που βγάζει αποτέλεσμα:

```
orgauser@orgA:~$ docker service ls
ID                NAME                MODE                REPLICAS            IMAGE
2hugq4k9fij1     fabric_ca1          replicated          1/1                 hyperledger/fabric-ca:1.1.0
vjxgm8vgfkkv     fabric_ca2          replicated          1/1                 hyperledger/fabric-ca:1.1.0
qb8r1k19o090     fabric_orderer      replicated          1/1                 hyperledger/fabric-orderer:1.1.0
qwl5bdas8prw     fabric_org1cli      replicated          1/1                 hyperledger/fabric-tools:1.1.0
8g6y318t3qdk     fabric_org1peer0    replicated          1/1                 hyperledger/fabric-peer:1.1.0
vhkqw60jav       fabric_org1peer1    replicated          1/1                 hyperledger/fabric-peer:1.1.0
w20rqgiwehd5     fabric_org2cli      replicated          1/1                 hyperledger/fabric-tools:latest
xnyw1gr8ac0b     fabric_org2peer0    replicated          1/1                 hyperledger/fabric-peer:1.1.0
hh0bekmioz2      fabric_org2peer1    replicated          1/1                 hyperledger/fabric-peer:1.1.0
```

Όταν τα αντίγραφα είναι 1/1 σημαίνει ότι όλα λειτουργούν σωστά, αν κάποιο είναι 0/1 τότε τρέξτε την εντολή:

```
docker service ps --no-trunc {name of service/ id of service}
```

Και ελέγξε τα αποτελέσματά του.

Γενικά, εαν τρέξετε τις τρεις προηγούμενες εντολές παράλληλα στα τρία μηχανήματα δεν θα αντιμετωπίσετε προβλήματα.

Για να τεστάρουμε ότι έχουν ολοκληρωθεί όλες οι ρυθμίσεις δικτύου και μπορούμε να δημιουργήσουμε μια αλυσίδα. Μπορούμε να τρέξουμε τη διεργασία μέσα στο shell ενός container που έχει δημιουργηθεί στο τρίτο μηχάνημα. Για να βρούμε τα containers τρέχουμε στο τρίτο μηχάνημα την εντολή:

```
docker ps
```

η οποία βγάζει όλα τα containers που έχουν δημιουργηθεί στο τρίτο μηχάνημα

```
orgcuser@orgC:~$ docker ps
CONTAINER ID   IMAGE                                COMMAND                  CREATED        STATUS
PORTS
db6889107e21   hyperledger/fabric-peer:1.1.0     "peer node start"      53 minutes ago Up 53 minutes
0.0.0.0:8051->7051/tcp, 0.0.0.0:8053->7053/tcp
3299827a16e1   hyperledger/fabric-peer:1.1.0     "peer node start"      53 minutes ago Up 53 minutes
0.0.0.0:7051->7051/tcp, 0.0.0.0:7053->7053/tcp
8ebdb539a328   hyperledger/fabric-ca:1.1.0       "sh -c 'fabric-ca-se..." 53 minutes ago Up 53 minutes
0.0.0.0:7054->7054/tcp
56868f993cfb   hyperledger/fabric-tools:latest    "/bin/bash"            53 minutes ago Up 53 minutes
fabric_org2cli.1.gb587np6o9d14zwvm3xkrvoh7
```

Για να ανοίξουμε το shell του container, επιλέγουμε το container με το όνομα fabric_org2cli και τρέχουμε την εντολή:

```
docker exec -it <docker cli name> bash
```

με όνομα αυτό που έχει βγει.

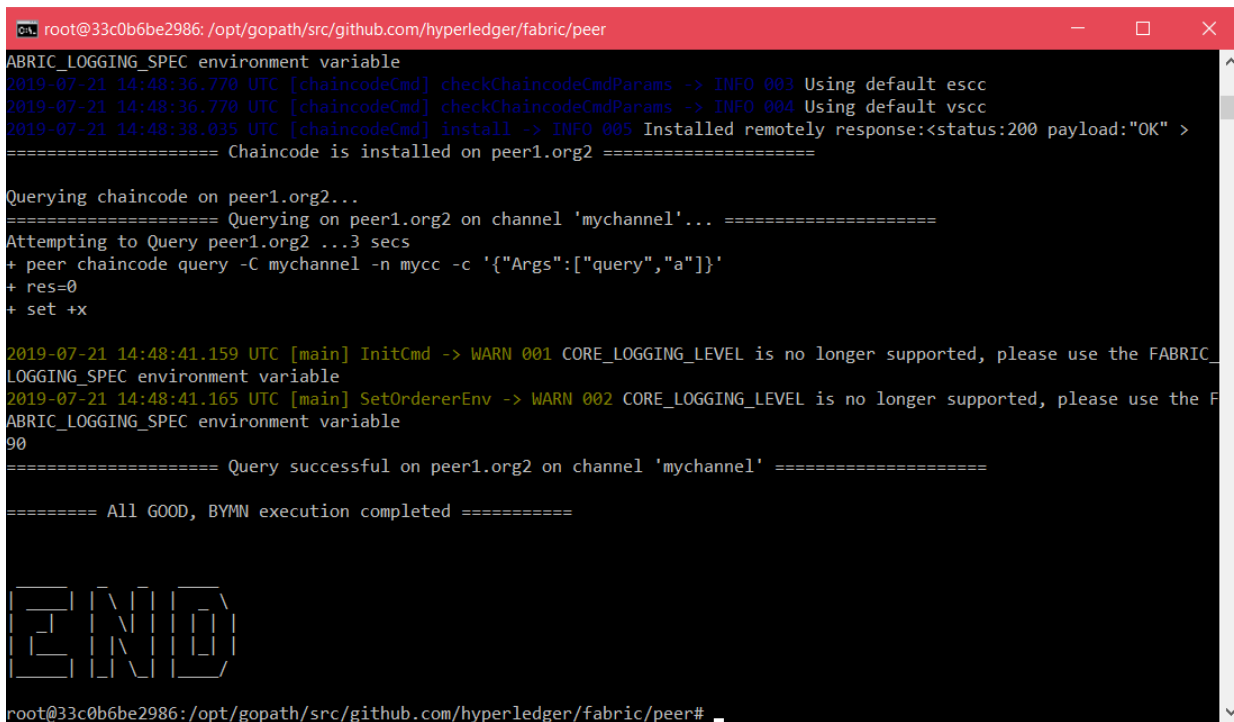
Στο νέο shell, τρέχουμε την εντολή ls για να δούμε ότι έχουν αντιγραφεί οι φάκελοι από το μηχανήμα μας μέσω των προηγούμενων εντολών και πρέπει να βγει το παρακάτω αποτέλεσμα:

```
orgcuser@orgC:~$ docker exec -it fabric_org2cli.1.gb587np6o9d14zwvm3xkrvoh7 bash
root@56868f993cfb:/opt/gopath/src/github.com/hyperledger/fabric/peer# ls
channel-artifacts  crypto  scripts
root@56868f993cfb:/opt/gopath/src/github.com/hyperledger/fabric/peer#
```

Τέλος, τρέχουμε την εντολή μέσα στο νέο shell:

```
scripts/script.sh
```

Διαβάζοντας το αρχείο script.sh, καταλαβαίνουμε ότι δημιουργείται ένα κανάλι στο οποίο συμμετέχουν και οι δύο οργανισμοί και εγκαθίσταται μια default αλυσίδα κώδικα (chaincode) και στους δύο οργανισμούς, επιτελείται μια default συνναλλαγή μεταξύ των δύο οργανισμών και ελέγχεται με ερώτηση (query) αν έγινε επιτυχώς η συνναλλαγή. Ολοκληρώνοντας όλη αυτή τη διαδικασία η εντολή πρέπει να βγάλει το παρακάτω αποτέλεσμα:



```
root@33c0b6be2986:/opt/gopath/src/github.com/hyperledger/fabric/peer
ABRIC_LOGGING_SPEC environment variable
2019-07-21 14:48:36.770 UTC [chaincodeCmd] checkChaincodeCmdParams -> INFO 003 Using default escc
2019-07-21 14:48:36.770 UTC [chaincodeCmd] checkChaincodeCmdParams -> INFO 004 Using default vscc
2019-07-21 14:48:38.035 UTC [chaincodeCmd] install -> INFO 005 Installed remotely response:<status:200 payload:"OK" >
===== Chaincode is installed on peer1.org2 =====

Querying chaincode on peer1.org2...
===== Querying on peer1.org2 on channel 'mychannel'... =====
Attempting to Query peer1.org2 ...3 secs
+ peer chaincode query -C mychannel -n mycc -c '{"Args":["query","a"]}'
+ res=0
+ set +x

2019-07-21 14:48:41.159 UTC [main] InitCmd -> WARN 001 CORE_LOGGING_LEVEL is no longer supported, please use the FABRIC
LOGGING_SPEC environment variable
2019-07-21 14:48:41.165 UTC [main] SetOrdererEnv -> WARN 002 CORE_LOGGING_LEVEL is no longer supported, please use the F
ABRIC_LOGGING_SPEC environment variable
90
===== Query successful on peer1.org2 on channel 'mychannel' =====

===== All GOOD, BYMN execution completed =====

END

root@33c0b6be2986:/opt/gopath/src/github.com/hyperledger/fabric/peer#
```

Με το παραπάνω αποτέλεσμα βλέπουμε ότι όλες οι διεργασίες έχουν ενεργοποιηθεί και λειτουργούν κανονικά και ότι όλοι οι κόμβοι είναι συνδεδεμένοι στο σύστημα.

3.3.5 Σημεία προσοχής

Όπως έχουμε επισημάνει και στο αυτόνομο σύστημα Hyperledger πρέπει πρώτα απο όλα να ελέγξουμε να είναι σωστές οι εκδόσεις και του συστήματος του μηχανήματος που δημιουργούμε. Δεύτερον, είναι απαραίτητο να ενημερωθούμε ότι και όλα τα εργαλεία έχουν εγκατασταθεί σωστά και έχουν τις εγκεκριμένες εκδόσεις. Ακολουθώντας ακριβώς τα πρότυπα των οδηγιών δεν θα αντιμετωπίσουμε κανένα σοβαρό ή μη αντιμετωπίσιμο πρόβλημα.

Επιπροσθέτως, πρέπει να πριν απο όλες τις εγκαταστάσεις να έχουμε ενεργοποιημένες τις πόρτες:

1. PC-1

Orderer (orderer.example.com) -port 7050

2. PC-2

CA1 (ca.org1.example.com) -port 7054

Org1 Peer0 (peer0.org1.example.com) -port 7051,8051

Org1 Peer1 (peer1.org1.example.com) -port 7053,8053

3. PC-3

CA2 (ca.org2.example.com) -port 7054

Org2 Peer0 (peer0.org2.example.com) -port 7051,8051

Org2 Peer1(peer1.org2.example.com) -port 7053,8053

Καθώς και τις πόρτες : 2377,7946,4789 για την υλοποίηση του docker swarm.

Επίσης, σε όλα τα στάδια πρέπει να προσέξουμε πολύ την υλοποίηση αυτού του συστήματος, καθώς διαφορετικές εντολές τρέχουν στα διαφορετικά μηχανήματα, ενώ κάποιες τρέχουν σε όλα τα μηχανήματα. Δεν πρέπει να κάνουμε βεβαιωμένες κινήσεις και να βεβαιωνόμαστε ότι βγαίνουν τα επιθυμητά αποτελέσματα απο κάθε εντολή.

Τέλος, στην σελίδα οδηγιών που ακολουθούμε στην παρούσα εργασία (Sarvepalli, 2018) αναφέρεται μια παραπομπή για την αναπαράσταση του δικτύου που δημιουργήσαμε σε πλατφόρμα με χρήση του εργαλείου Hyperledger Explorer. Έγινε προσπάθεια για την υλοποίηση αυτής της πλατφόρμας, αλλά η ολοκλήρωσή της δεν ήταν εφικτή λόγω των βημάτων που δεν περιγράφονται με σαφήνεια, όπως το παρόν tutorial. Δημιουργήθηκαν πολλά προβλήματα, καθώς ζητούσε την εγκατάσταση πρόσθετων εργαλείων χωρίς την επεξήγηση της χρησιμότητάς τους και οι οδηγίες για την ρύθμισή τους δεν ήταν επαρκής. Τελικά, λύνοντας πολλά σφάλματα που προκλήθηκαν αποδείχτηκε ότι οι υπάρχουσες εκδόσεις του Hyperledger Explorer και των αρχείων (configuration files) δεν αντιστοιχούν στις εκδόσεις που αναφέρονται στα αρχεία που δίνονται και περιγράφονται σε αυτό το φύλλο οδηγιών.

3.4 Κρίσιμες επιχειρησιακές λειτουργίες σε περιβάλλον Blockchain

3.4.1 Καταγραφή (logging) επικοινωνιών

Από την λειτουργία του Blockchain καταλαβαίνουμε πόσο χρήσιμο και αποτελεσματικό εργαλείο μπορεί να αποδειχθεί σε κρίσιμες και επείγουσες επιχειρησιακές λειτουργίες όπως είναι μια αεροδιακομιδή. Με μια απλή αναζήτηση έχουμε όλη τη λίστα των συναλλαγών-επικοινωνιών μεταξύ των κόμβων- οργανισμών με καταγεγραμμένη ημερομηνία και ώρα. Παράλληλα στο ιστορικό μπορούμε να δούμε με λεπτομέρειες το περιεχόμενο αυτών των επικοινωνιών αν αυτές είναι κοινές, ενώ οι αρμόδιοι μπορούν να δούν το περιεχόμενο και των ιδιωτικών συναλλαγών. Το περιεχόμενο των επικοινωνιών καταχωρείται αυτούσιο και αμετάβλητο χωρίς να μπορεί κάποιος να το αμφισβητήσει. Δεν αφήνει περιθώρια λάθους, υποκλοπής ή παραβίασης και δολιοφθοράς.

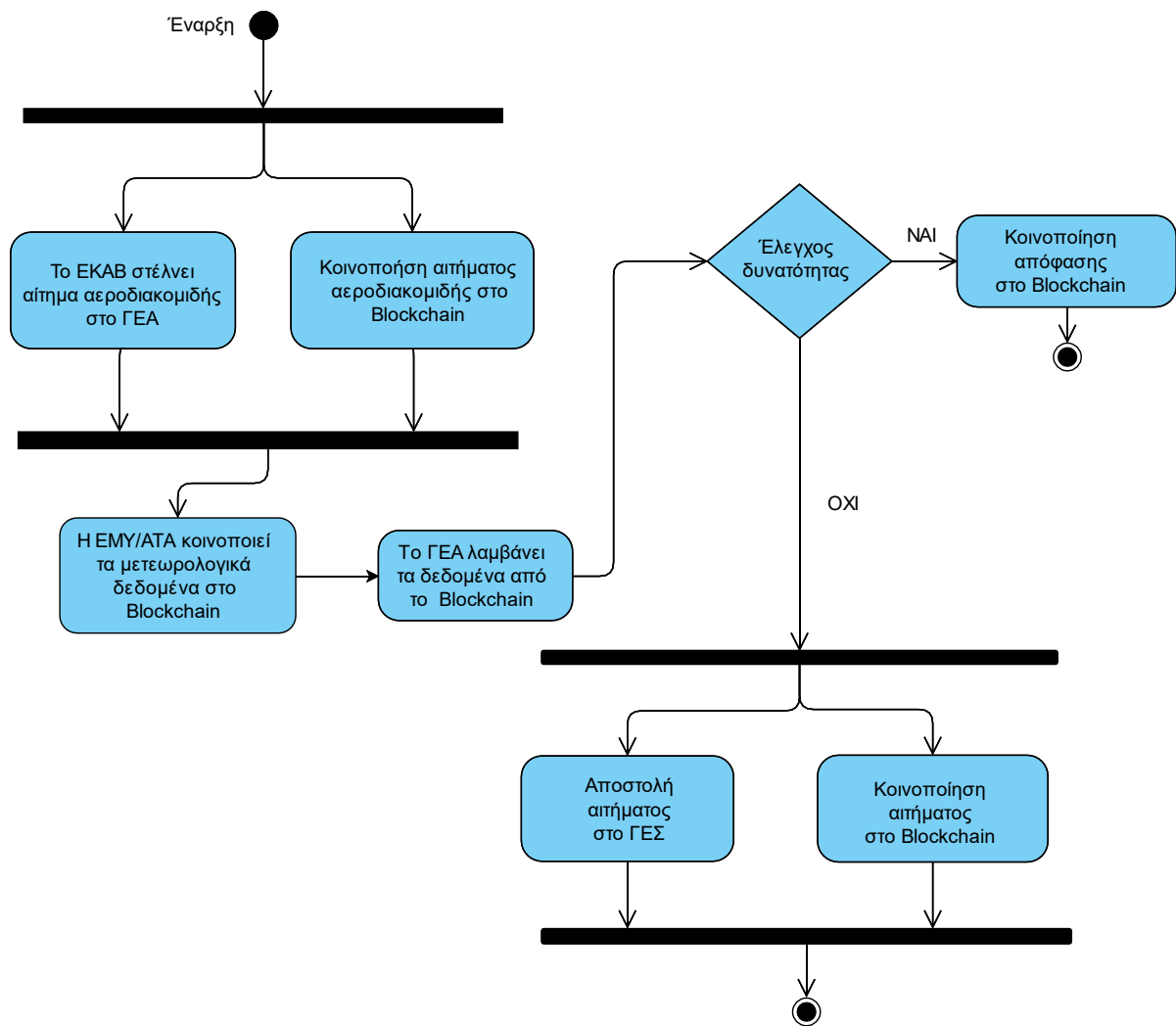
Με ιδιαίτερη ευκολία βάση αυτών των δεδομένων μπορεί να πραγματοποιηθεί έλεγχος στην ετοιμότητα, στον σωστό συντονισμό και στην έγκαιρη αντιμετώπιση μιας επείγουσας κατάστασης. Αρκεί να εισέλθει στο δίκτυο του Blockchain ο νέος ελεγκτικός κόμβος με ρόλο και δικαιώματα που θα καθορίζονται από νέο smart contract στο οποίο θα δίνονται δικαιώματα διαχειριστή για να έχει την πλήρη προσβαση των δεδομένων.

3.4.2 Παράδειγμα ανταλλαγής κρίσιμων δεδομένων

Ενδεικτικά, σε ένα αίτημα αεροδιακομιδής αναλύεται η επικοινωνία του ΕΚΑΒ με το ΓΕΑ στο παρακάτω διάγραμμα (εικόνα 16). Αρχικά, το ΕΚΑΒ πραγματοποιεί αίτημα αεροδιακομιδής στο ΓΕΑ και κοινοποιεί το αίτημα στο δίκτυο του Blockchain.

Στην συνέχεια, η ΕΜΥ που ενημερώνεται για το αίτημα από το δίκτυο, καταχωρεί στην πλατφόρμα του Blockchain τα μετεωρολογικά δεδομένα (σε μορφή χαρτών, προγνώσεων και στατιστικών) που αφορούν τις περιοχές που πρόκειται να λάβει χώρα η αεροδιακομιδή. Στην συνέχεια το ΓΕΑ μελετά τα δεδομένα που συλλέγει από το Blockchain (πληροφορίες αιτήματος, μετεωρολογικά δεδομένα) και πληροφορίες από την βάση δεδομένων του (στοιχεία για τα αεροδρόμια, την καταλληλότητά τους, τα ιπτάμενα μέσα, πληρώματα κλπ) και αποφασίζει αν θα εγκρίνει την αεροδιακομιδή ή όχι.

Αν το αίτημα γίνει αποδεκτό, κοινοποιείται στο Blockchain ότι η αεροδιακομιδή θα πραγματοποιηθεί από το ΓΕΑ. Μετά το πέρας της αποστολής συλλέγονται όλα τα δεδομένα για την εκτέλεσή της και καταχωρούνται στο ledger. Αν το αίτημα απορριφθεί, κοινοποιείται στο Blockchain από το ΓΕΑ και παράλληλα στέλνει το αίτημα της αεροδιακομιδής στο ΓΕΣ.



Εικόνα 16 Activity Diagram: Μελέτη περίπτωσης επικοινωνίας ΕΚΑΒ με ΓΕΑ

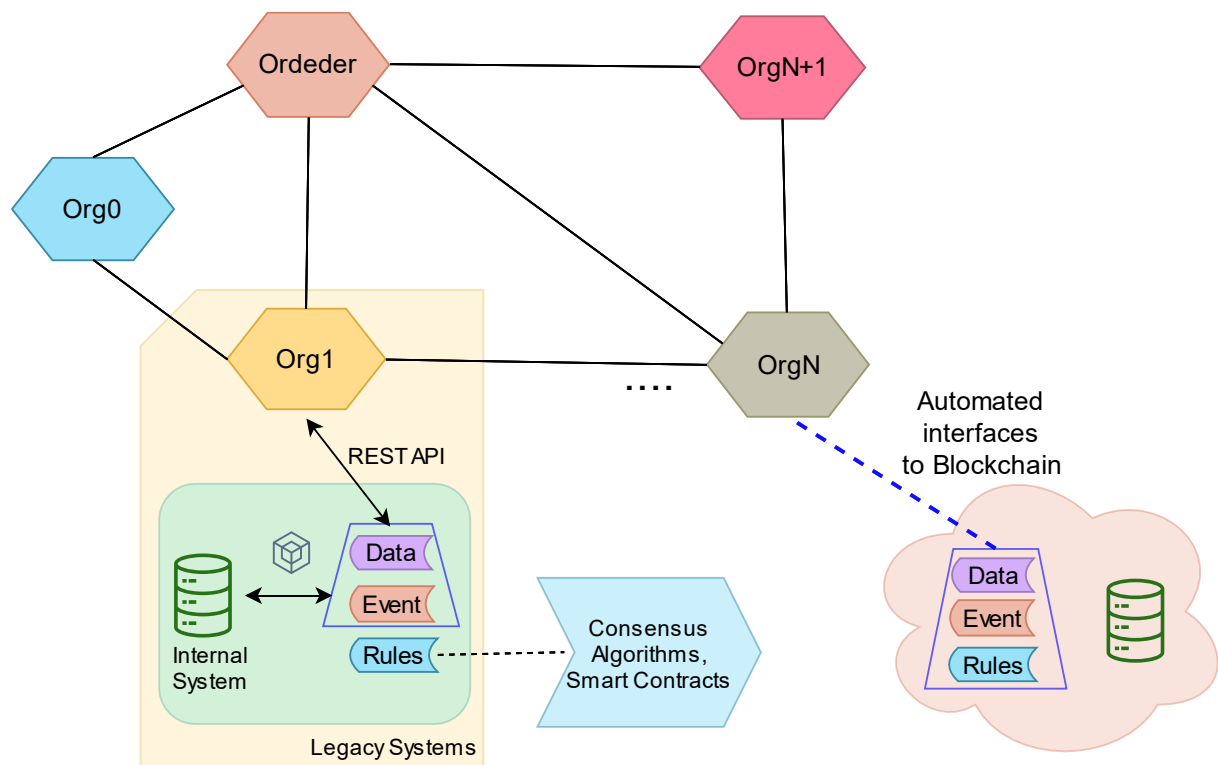
3.5 Θέματα συνεργασίας με προϋπάρχοντα “legacy” πληροφοριακά συστήματα

3.5.1 Ενδεικτικές αρχιτεκτονικές integration

Καθοριστική για την επέκταση και την εύρυθμη λειτουργία ενός Blockchain συστήματος στην επικοινωνία και τον συντονισμό μιας κρίσιμης αποστολής είναι η ένταξή του στα συμβατικά συστήματα πληροφόρησης και επικοινωνίας μεταξύ των εμπλεκόμενων. Μια απλή αρχιτεκτονική ενσωμάτωσης ενός Blockchain συστήματος στον τρόπο επικοινωνίας μεταξύ των οργανισμών είναι η ανάπτυξη Rest API εφαρμογών. Οι εφαρμογές αυτές δίνουν την δυνατότητα στους υπεύθυνους των φορέων να συμπληρώνουν απλές φόρμες για την ένταξη πληροφοριών και νέων δεδομένων που ανταλλάσσονται σε μια επικοινωνία μεταξύ τους. Η σημερινή ιεραρχία και οι ρόλοι που καθορίζονται μέσα από αυτήν θα ενσωματωθούν στο blockchain με την μορφή των smart contracts και οι συμφωνίες μεταξύ των οργανισμών θα υλοποιούνται με consensus αλγόριθμους. Συγκεκριμένα σε μια αεροδιακομιδή, ο κάθε

εμπλεκόμενος φορέας θα έχει τον προσωπικό του λογαριασμό και θα εισέρχεται στο σύστημα με χρήση κωδικού πρόσβασης. Στη συνέχεια θα μπορεί να εισάγει στο σύστημα όλα τα δεδομένα και τις πληροφορίες που αφορούν τον ρόλο του στην αποστολή και παράλληλα θα έχει πρόσβαση στα δεδομένα που έχουν καταθέσει οι υπόλοιποι φορείς ανάλογα με τα δικαιώματά του, που θα καθορίζονται από τα smart contracts.

Επίσης, μια επαναστατική μέθοδος ενσωμάτωσης αποτελεί η δημιουργία συστημάτων αυτόματης εισαγωγής δεδομένων προερχόμενων από τα συμβατικά συστήματα πληρόρησης χωρίς την εμπλοκή του ανθρώπινου παράγοντα. Μέσω αυτών των συστημάτων θα καθορίζονται πάλι εξ αρχής οι ρόλοι και τα δικαιώματα του κάθε φορέα στο σύστημα, αλλά τα δεδομένα θα εισάγονται αυτόματα χωρίς την ύπαρξη κάποιου χειριστή. Στα συστήματα αυτά θα διασφαλίζεται η πηγή και ο όγκος των πληροφοριών ώστε να αφορούν μια συγκεκριμένη αποστολή κάθε φορά μέσω των smart contracts και των consensus αλγορίθμων. Αυτή η πρωτοποριακή καινοτομία θα μπορούσε να μηδενίσει το χρόνο απόκρισης και συντονισμού των φορέων σε μια κρίσιμη αποστολή, εξασφαλίζοντας την επιτυχία της. Παράλληλα, διασφαλίζεται η καθολική και απόλυτη ακεραιότητα των δεδομένων, αφού θα εξαλείφει την αδυναμία του ανθρώπινου παράγοντα.



Εικόνα 17 Τρόποι ενσωμάτωσης του Blockchain στα συμβατικά πληροφοριακά συστήματα

3.5.2 Σημεία που χρήζουν προσοχής

Ο φιλόδοξος σχεδιασμός που αφορά την ένταξη του blockchain συστήματος στα σημερινά συστήματα επικοινωνίας των φορέων δεν έχει καταφέρει ακόμα να υλοποιηθεί και βρίσκεται σε ερευνητικό επίπεδο. Η τεχνολογία Blockchain είναι ιδιαίτερα συνδεδεμένη με τον οικονομικό τομέα και τα κρυπτονομίσματα, έτσι έχουν αναπτυχθεί ενδελεχώς αρκετές πλατφόρμες που εξυπηρετούν αυτούς τους σκοπούς, όπως για παράδειγμα το Ethereum. Εκρεμεί σε μεγάλο βαθμό το ενδιαφέρον και η μελέτη για την ανάπτυξη εφαρμογών σε άλλους τομείς και πολύ περισσότερο για κοινοφελής σκοπούς.

Ήδη όμως το ερευνητικό πεδίο διευρίνεται και σύντομα θα αποδώσει καρπούς. Παράλληλα, πρέπει να ενημερωθούν και οι κρατικοί φορείς για τα πλεονεκτήματα της επικοινωνίας με ένα σύστημα blockchain, καθώς τώρα το αντιμετωπίζουν πολύ επιφυλακτικά, αφού για ιδεολογικούς κυρίως λόγους θέλουν να διατηρούν το απόρρητο των πληροφοριών τους στα δικά τους και μόνο πληροφοριακά συστήματα. Στην πραγματικότητα η αδιάβλητη ασφάλεια και η ακεραιότητα των δεδομένων αποτελούν τα κύρια προτερήματα του blockchain. Η πλήρη εφαρμογή ενός συστήματος blockchain σε κρίσιμες αποστολές θα διευκολύνει σε μεγάλο βαθμό όλες τις επικοινωνίες μεταξύ των φορέων και το αποτέλεσμα θα είναι άμεσα και ποιοτικά αναβαθμισμένο. Ειδικά στην περίπτωση μιας αεροδιακομιδής η άμεση και αποτελεσματική επέμβαση των αρμόδιων κρατικών φορέων μπορεί να σώσει πολλές ανθρώπινες ζωές.

Κεφάλαιο 4. Συμπεράσματα

4.1 Σύνοψη εργασίας

Η σύγχρονη τεχνολογία μπορεί να παράσχει τα απαραίτητα εργαλεία για την μετατροπή των λειτουργιών και την κάλυψη των σημερινών αλλά και των μελλοντικών αναγκών της ψηφιακής επικοινωνίας. Η αύξηση του όγκου και της ποιότητας των δεδομένων που παράγονται, σε ένα συνδεδεμένο περιβάλλον, έχουν ως αποτέλεσμα να εξελιχθούν οι δυνατότητες ανάλυσης και υπολογισμού για την κατανόηση των δεδομένων. Η τεχνολογία Blockchain για ανταλλαγή πληροφοριών επιτρέπει σε πολλαπλούς οργανισμούς να επαληθεύουν τις εγγραφές τους, ώστε να είναι αξιόπιστες και προσιτές σε εύκολη και γρήγορη πρόσβαση από τους χρήστες.

Στη παρούσα διπλωματική εργασία έγινε προσπάθεια να αναπτυχθεί μια πλατφόρμα για την ασφαλή, αξιόπιστη και διάφανη ροή πληροφοριών για την κρίσιμη αποστολή της αεροδιακομιδής ασθενών. Μελετώντας τον τρόπο με τον οποίο γίνεται σήμερα η επικοινωνία κατόπιν ενός αιτήματος αεροδιακομιδής, αποδεικνύεται χρονοβόρα και χωρίς άμεσο συντονισμό με πιθανό αποτέλεσμα την απώλεια ανθρώπινης ζωής. Είναι άμεση η ανάγκη λοιπόν να εξακολουθήσει η έρευνα στο σχετικό πεδίο ώστε να επιλυθούν τα προβλήματα και να μπορέσει να λειτουργήσει η πλατφόρμα του Blockchain στην αεροδιακομιδή. Η νέα εφαρμογή θα δώσει λύση στα σημερινά προβλήματα καθιστώντας γρήγορο και καθολικό συντονισμό όλων των ενεργειών σε ένα έκτακτο περιστατικό.

4.2 Σχετικά με τις τεχνολογίες Blockchain

Αναλύθηκαν πολλές διαφορετικές τεχνολογίες Blockchain, όπως το Bitcoin, το Ethereum και το Hyperledger κ.α. Η κάθε μια από αυτές τις τεχνολογίες ανάλογα με το είδος του δικτύου (δημόσιο ή ιδιωτικό) εφαρμόζεται σε διάφορους τομείς, όπως στην οικονομία, την υγεία, την εφοδιαστική αλυσίδα, την εκπαίδευση, την δημόσια διοίκηση κλπ. Βασικά στοιχεία του Blockchain αποτελούν τα έξυπνα συμβόλαια (smart contracts), το αρχείο καταγραφής συναλλαγών (ledger) και οι αλγόριθμοι συναίνεσης (consensus algorithms) που το καθιστούν αξιόπιστο και ευέλικτο, καθώς μέσω των consensus αλγόριθμων επιτυγχάνεται η επιβεβαίωση και η επαλήθευση των δεδομένων, ενώ τα smart contracts καθορίζουν τους ρόλους και τα όρια των χρηστών. Επομένως, δεν υπάρχουν αντικρουόμενα συμφέροντα και σχέσεις αμφισβήτησης αλλά σχέσεις συνεργασίας και εμπιστοσύνης για τον διαμοιρασμό της πληροφορίας μεταξύ τους.

Έτσι όπως είναι σχεδιασμένη η αρχιτεκτονική της λύσης αυτής, κάθε χρήσιμη κίνηση, στις διαδικασίες των συμμετεχόντων, καταγράφεται. Οι πληροφορίες είναι αμετάβλητες καθώς κάθε πρότερη καταγραφή κίνησης δεν μπορεί να διαγραφεί. Με αυτόν τον τρόπο διατίθεται όλη η ιστορικότητα των κινήσεων διότι κάθε συναλλαγή αφήνει πάντοτε το αποτύπωμά της. Παράλληλα, χρησιμοποιούνται συστήματα που προϋπάρχουν και προσθέτοντας νέες web υπηρεσίες (api services) επιτυγχάνεται ο αυτοματισμός της συλλογής πληροφοριών. Στην εφαρμογή μιας κρίσιμης αποστολής όπως είναι η αεροδιακομιδή αξιολογήθηκε και επιλέχθηκε η αποκεντρωμένη τεχνολογία Hyperledger Fabric, καθώς είναι ιδανική για επιχειρησιακές λύσεις χωρίς οικονομικά κίνητρα, περιλαμβάνει δικαιώματα χρηστών και διαθέτει φιλικό

περιβάλλον προς τον χρήστη. Επίσης, είναι η πιο δημοφιλής υλοποίηση σε permissioned blockchain.

4.3 Blockchain και εφαρμογές κρίσιμης αποστολής

Ο στόχος της εργασίας ήταν να βρεθούν τρόποι ώστε να αντιμετωπιστούν τα ισχύοντα μέχρι σήμερα προβλήματα που προκαλούνται με το σημερινό σύστημα επικοινωνίας μεταξύ των εμπλεκόμενων φορέων. Τα βασικά κριτήρια που έπρεπε να καλυφθούν για την πλατφόρμα ενοποίησης κι ανταλλαγής πληροφοριών στην αεροδιακομιδή ασθενών ήταν η αποκέντρωση, η διαφάνεια, η ασφάλεια και η αδιαβλητότητα των πληροφοριών. Ιδανική τεχνολογία για αυτή τη λύση κρίθηκε όπως είδαμε το Hyperledger Blockchain.

Με την χρήση των έξυπνων συμβολαίων υλοποιήθηκε η επιχειρηματική λογική για τον κάθε συμμετέχοντα κρίκο (εμπλεκόμενοι φορείς, πληρώματα, υπηρεσίες). Η εφαρμογή αυτή φέρνει μια σύγχρονη εποχή με την ριζική αλλαγή των σχέσεων μεταξύ των συμμετεχόντων της επικοινωνίας για την πραγματοποίηση αεροδιακομιδής. Πλέον το τελικό προϊόν διαθέτει τη σωστή και όσο το δυνατόν ολοκληρωμένη πληροφορία η οποία είναι αποτέλεσμα σύνθεσης τμημάτων αδιάβλητης πληροφόρησης κάθε σταδίου. Η εφαρμογή προσεγγίζει τη λύση από την αρχική αίτηση του ΕΚΑΒ για αεροδιακομιδή έως την ολοκλήρωση της αποστολής.

Στα συμβατικά συστήματα που υπάρχουν η διαδικασία για την λήψη απόφασης εκτέλεσης ή μη της αεροδιακομιδής διαρκεί αρκετό χρονικό διάστημα και εξαρτάται από το επίπεδο συνεννόησης και πληροφόρησης του κάθε φορέα. Οι αυτοματοποιημένες ειδοποιήσεις και ενέργειες έχουν σαν αποτέλεσμα τη μείωση του απαιτούμενου προσωπικού στην βάρδια και εξοικονόμηση του κόστους λειτουργίας. Επίσης, οδηγούν στην εξάλειψη της απώλειας χρησίων δεδομένων απο λάθος και την μείωση του χρόνου συντονισμού των φορέων. Ο κάθε οργανισμός επενδύει, μέσω της εφαρμογής, όχι μόνο στην παροχή γρήγορων αποτελεσμάτων που οδηγούν στην διάσωση ανθρώπινης ζωής αλλά και στην παροχή μιας πιο αποτελεσματικής και ποιοτικής συνολικής υπηρεσίας.

4.4 Σχετικά με το περιβάλλον Hyperledger

Γεγονός είναι πως η τεχνολογία του Blockchain είναι μια σχετικά νέα τεχνολογία της οποίας οι εφαρμογές δεν έχουν ακόμη δοκιμαστεί εκτενώς. Ανοίγοντας αυτόν τον νέο δρόμο σε πολλές υλοποιήσεις, δεν υπάρχουν σαφείς βέλτιστες πρακτικές. Ακόμα μια συνιστάμενη της πολυπλοκότητας αυτής είναι η ανάγκη για πλήρη απεικόνιση όλων των επιχειρησιακών λειτουργιών, ο μεγάλος αριθμός των εμπλεκόμενων φορέων και των πολλαπλών παραμέτρων σε κάθε τμήμα της επικοινωνίας για την αεροδιακομιδή ασθενών.

Στην προσπάθεια της συγκεκριμένης εργασίας θελήσαμε το έργο αυτό να ανταποκρίνεται στην πραγματικότητα (τουλάχιστον έξι εμπλεκόμενοι φορείς – κόμβοι του δικτύου) και για το λόγο αυτό επιχειρήσαμε να το εγκαταστήσουμε σε ένα δίκτυο πολλαπλών μηχανημάτων. Η εξέλιξη όμως αυτού του έργου βρίσκεται σε πειραματικό στάδιο, γιατί δεν υπάρχει έγκυρη και ολοκληρωμένη βιβλιογραφία που να δίνει πληροφορίες για την ανάπτυξη μια τέτοιας πλατφόρμας. Σε συνεργασία με ερευνητές και σε άλλα πανεπιστήμια αναμένονται εξελίξεις και αποτελέσματα που θα οδηγήσουν στην λειτουργία ενός τέτοιου συστήματος. Η παρούσα

εργασία έχει επιτύχει την δημιουργία ενός Blockchain δικτύου για δύο εμπλεκόμενους φορείς κάνοντας χρήση του εργαλείου Hyperledger Fabric που λειτουργεί με τρία εικονικά μηχανήματα.

Η εμφάνιση της πλατφόρμας δεν ολοκληρώνεται, καθώς οι πρόσθετες ρυθμίσεις και η εγκατάσταση επιπλέον εργαλείων που οδηγούν στην τελική πλατφόρμα, δεν μπορούν να πραγματοποιηθούν λόγω της μη ύπαρξης σαφών οδηγιών, καθώς η υλοποίηση αυτή βρίσκεται ακόμη υπο έρευνα. Παράλληλα, η διαρκής ανανέωση των εκδόσεων των εργαλείων που χρησιμοποιούνται ακυρώνει τις προηγούμενες εκδόσεις και είναι ασύμβατες με τα δεδομένα του συστήματος (πχ. configuration files, βιβλιοθήκες κλπ). Το γεγονός αυτό έχει ως αποτέλεσμα να απαιτείται συνεχώς από τους προγραμματιστές να διορθώνουν τα σφάλματα που δημιουργούνται λόγω των διαφορετικών εκδόσεων με τα εργαλεία και τις ρυθμίσεις που έχουν μέχρι στιγμής εγκαταστήσει και να μην προχωρά η πραγματοποίηση του έργου. Το Blockchain και συγκεκριμένα το Hyperledger είναι σχετικά πολύ νέες όχι ακόμα ώριμες και ραγδαία αναπτυσσόμενες τεχνολογίες. Αυτό έχει ως συνέπεια να υπάρχει διαρκής εξέλιξη, αλλαγή και σε κάποιες περιπτώσεις ακόμη και κατάργηση σχετικών εργαλείων αλλά και να μην υπάρχει ακόμη υποστήριξη από μια μεγάλη κοινότητα προγραμματιστών που να ασχολούνται με τον κλάδο των αποκεντρωμένων εφαρμογών.

4.5 Επόμενα βήματα

Επενδύοντας κάποιος οργανισμός στο blockchain είναι σαν να συντηρεί έναν ζωντανό οργανισμό ο οποίος τροφοδοτείται συνεχώς με νέες προοπτικές. Οι τεχνολογίες πάνω στις οποίες βασίζεται η εφαρμογή παρότι είναι καινούργιες, αλλάζουν συνεχώς.

Μια ενδιαφέρουσα μελλοντική επέκταση της πλατφόρμας θα μπορούσε να είναι η προσθήκη Internet of Things (IoT) συσκευών. Η εφαρμογή των IoT συσκευών στην επικοινωνία και τον συντονισμό των εμπλεκόμενων φορέων σε κρίσιμες αποστολές, για παράδειγμα σε μια αεροδιακομιδή, θα παίξει καθοριστικό ρόλο αντικαθιστώντας όλα τα προϋπάρχοντα συστήματα (όπως τηλέφωνο, φαξ, e-mail, ρανταρ, ασύρματος κλπ).

Ο συνδυασμός του blockchain με IoT, τεχνητή νοημοσύνη, Big Data και αυτόματα ρομπότ αποτελεί μια ακόμη επέκταση που θα μπορούσε να έχει θαυμάσια αποτελέσματα. Με την σωστή ανάλυση και τον συνδυασμό αυτών των τεχνολογιών μπορεί να επιτευχθεί βελτίωση της ακρίβειας των προβλέψεων, αυξημένη επίτευξη στόχων των αεροδιακομιδών και να δημιουργηθούν μαθηματικά μοντέλα που θα φέρουν νέες μορφές αυτοματισμού κ.α.

Η ανάπτυξη μιας πρόσθετης λειτουργίας στο Blockchain θα μπορούσε να οδηγήσει στην εξάλειψη χρήσης των web εφαρμογών για καταχωρήσεις πληροφοριών από ανθρώπους, καθιστώντας πιο αυστηρές και αυτόματες τις συναλλαγές.

Το Blockchain και οι αποκεντρωμένες εφαρμογές έχουν την δυναμική να αλλάξουν σε μεγάλο βαθμό αρκετούς τομείς της ζωής και συνεπώς θα τραβήξουν το ενδιαφέρον πολλών ερευνητών, προγραμματιστών, επιχειρήσεων και κρατικών φορέων.

Βιβλιογραφία

- Docker Inc, 2019. *Get Docker Engine - Community for Ubuntu*. [Ηλεκτρονικό]
Available at: <https://docs.docker.com/install/linux/docker-ce/ubuntu/#install-using-the-repository>
[Πρόσβαση 2 3 2019].
- KryptoGraphe Team, 2018. *Which are the Top 4 Blockchain-based Platforms for RideSharing?*. [Ηλεκτρονικό]
Available at: <https://www.kryptographe.com/ridesharing-platforms/>
[Πρόσβαση 28 9 2019].
- UK Government, Office for Science, 2016. *Distributed Ledger Technology: beyond block chain*. [Ηλεκτρονικό]
Available at:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf
[Πρόσβαση 17 8 2019].
- Air ambulance, 2019. *Air medical services*. [Ηλεκτρονικό]
Available at: https://en.wikipedia.org/wiki/Air_medical_services
[Πρόσβαση 10 10 2019].
- Alsunaidi, S. J. & Alhaidari, F. A., 2019. *A Survey of Consensus Algorithms for Blockchain Technology*, s.l.: IEEE.
- Anwar, H., 2018. *Consensus Algorithms: The Root Of The Blockchain Technology*. [Ηλεκτρονικό]
Available at: <https://101blockchains.com/consensus-algorithms-blockchain/>
[Πρόσβαση 29 9 2019].
- Atlassian, 2019. *What is Git*. [Ηλεκτρονικό]
Available at: <https://www.atlassian.com/git/tutorials/what-is-git>
[Πρόσβαση 6 9 2019].
- Baliga, D. A., 2017. *Understanding Blockchain*. [Ηλεκτρονικό]
Available at:
<https://pdfs.semanticscholar.org/da8a/37b10bc1521a4d3de925d7ebc44bb606d740.pdf>
[Πρόσβαση 18 9 2019].
- Benjamin, B., 2017. *Introduce a start for Burrow EVM as Sawtooth Transaction Processor*. [Ηλεκτρονικό]
Available at: <https://github.com/hyperledger/sawtooth-core/pull/415>
[Πρόσβαση 3 9 2019].
- Blockchain Team, 2019. *BITCOIN FOR BEGINNERS*. [Ηλεκτρονικό]
Available at: <https://www.blockchain.com/learning-portal/bitcoin-faq>
[Πρόσβαση 18 9 2019].
- CoinBundle Team, 2018. *Consensus Algorithms*. [Ηλεκτρονικό]
Available at: <https://medium.com/coinbundle/consensus-algorithms-dfa4f355259d#a76e>
[Πρόσβαση 30 9 2019].

Computer Hope, 2019. *Hub*. [Ηλεκτρονικό]

Available at: <https://www.computerhope.com/jargon/h/hub.htm>

[Πρόσβαση 3 10 2019].

Coursera Team, 2019. *Coursera- Your Course to Success*. [Ηλεκτρονικό]

Available at: <https://www.coursera.org/>

[Πρόσβαση 4 10 2019].

DigitalOcean Community, 2017. *How To Install Docker Compose on Ubuntu 16.04*. [Ηλεκτρονικό]

Available at: <https://www.digitalocean.com/community/tutorials/how-to-install-docker-compose-on-ubuntu-16-04>

[Πρόσβαση 15 6 2019].

DigitalOcean Community, 2018. *How To Install and Use Docker on Ubuntu 16.04*. [Ηλεκτρονικό]

Available at: <https://www.digitalocean.com/community/tutorials/how-to-install-and-use-docker-on-ubuntu-16-04>

[Πρόσβαση 15 6 2019].

DigitalOcean Community, 2018. *How To Install Node.js on Ubuntu 16.04*. [Ηλεκτρονικό]

Available at: <https://www.digitalocean.com/community/tutorials/how-to-install-node-js-on-ubuntu-16-04>

[Πρόσβαση 15 6 2019].

Dragonchain Team, 2019. *What Different Types of Blockchains are There?*. [Ηλεκτρονικό]

Available at: <https://dragonchain.com/blog/differences-between-public-private-blockchains>

[Πρόσβαση 30 9 2019].

Ekblaw, A., Azaria, A., Halamka, J. D. & Lippman, A., 2016. *A Case Study for Blockchain in Healthcare*.

[Ηλεκτρονικό]

Available at: https://www.healthit.gov/sites/default/files/5-56-onc_blockchainchallenge_mitwhitepaper.pdf

[Πρόσβαση 30 9 2019].

G2 Team, 2019. *Hyperledger Alternatives & Competitors*. [Ηλεκτρονικό]

Available at: <https://www.g2.com/products/hyperledger/competitors/alternatives>

[Πρόσβαση 4 10 2019].

Git Community, 2019. *Git --fast-version-control*. [Ηλεκτρονικό]

Available at: <https://git-scm.com/>

[Πρόσβαση 6 9 2019].

Gordon, S., 2018. *Installing Ubuntu Server in VirtualBox - Youtube*. [Ηλεκτρονικό]

Available at: <https://www.youtube.com/watch?v=7QIf4sf6DM0>

[Πρόσβαση 29 5 2019].

Goyal, S., 2018. *Centralized vs. Decentralized? The New Decentralized Internet Networks*.

[Ηλεκτρονικό]

Available at: <https://101blockchains.com/centralized-vs-decentralized-internet-networks/>

[Πρόσβαση 30 9 2019].

Gramoli, V., 2017. *From blockchain consensus back to Byzantine consensus, Future Generation Computer Systems*. [Ηλεκτρονικό]

Available at: <http://dx.doi.org/10.1016/j.future.2017.09.023>
[Πρόσβαση 28 9 2019].

Guoan, X., 2017. *How to Disable IPv6 on Ubuntu 16.04 and Ubuntu 17.04*. [Ηλεκτρονικό]
Available at: <https://www.linuxbabe.com/ubuntu/disable-ipv6-on-ubuntu>
[Πρόσβαση 18 6 2019].

Haardik, 2018. *How to build a blockchain network using Hyperledger Fabric and Composer*. [Ηλεκτρονικό]
Available at: <https://www.freecodecamp.org/news/how-to-build-a-blockchain-network-using-hyperledger-fabric-and-composer-e06644ff801d/>
[Πρόσβαση 23 7 2019].

Hale, J., 2019. *Learn Enough Docker to be Useful*. [Ηλεκτρονικό]
Available at: <https://towardsdatascience.com/learn-enough-docker-to-be-useful-1c40ea269fa8>
[Πρόσβαση 6 9 2019].

Houben, R. & Snyers, A., 2018. *Cryptocurrencies and*. [Ηλεκτρονικό]
Available at:
<http://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf>
[Πρόσβαση 1 10 2019].

Hyperledger , 2017. *HyperledgerArchitecture, Volume 1:Introduction to Hyperledger Business Blockchain*. [Ηλεκτρονικό]
Available at: [https://www.hyperledger.org/wp-content/uploads/2017/08/Hyperledger Arch WG Paper 1 Consensus.pdf](https://www.hyperledger.org/wp-content/uploads/2017/08/Hyperledger_Arch_WG_Paper_1_Consensus.pdf)
[Πρόσβαση 26 9 2019].

Hyperledger , 2018. *Hyperledger Explorer*. [Ηλεκτρονικό]
Available at: <https://www.hyperledger.org/projects/explorer>
[Πρόσβαση 16 9 2019].

Hyperledger Composer , 2019. *Hyperledger Composer Installing the development environment*. [Ηλεκτρονικό]
Available at: <https://hyperledger.github.io/composer/v0.19/installing/development-tools>
[Πρόσβαση 2 3 2019].

Hyperledger Composer, 2019. *Hyperledger Composer-Documentation*. [Ηλεκτρονικό]
Available at: <https://hyperledger.github.io/composer/latest/introduction/introduction.html>
[Πρόσβαση 18 7 2019].

Hyperledger Fabric, 2019. *Hyperledger Fabric*. [Ηλεκτρονικό]
Available at: <https://hyperledger-fabric.readthedocs.io/en/release-1.2/blockchain.html>
[Πρόσβαση 23 7 2019].

Hyperledger Team, 2018. *Hyperledger Cello*. [Ηλεκτρονικό]
Available at: <https://www.hyperledger.org/projects/cello>
[Πρόσβαση 28 9 2019].

Hyperledger Team, 2018. *Measuring Blockchain Performance with Hyperledger Caliper*. [Ηλεκτρονικό]
Available at: <https://www.hyperledger.org/blog/2018/03/19/measuring-blockchain-performance->

with-hyperledger-caliper
[Πρόσβαση 28 9 2019].

Hyperledger, 2018. *Hyperledger Quilt*. [Ηλεκτρονικό]
Available at: <https://www.hyperledger.org/projects/quilt>
[Πρόσβαση 27 9 2019].

Hyperledger, 2019. *Hyperledger – Open Source Blockchain Technologies*. [Ηλεκτρονικό]
Available at: <https://www.hyperledger.org/>
[Πρόσβαση 2 8 2019].

Kerner, S. M., 2019. *How Docker Engine Works to Enable Containers*. [Ηλεκτρονικό]
Available at: <https://www.serverwatch.com/server-news/how-docker-engine-works-to-enable-containers.html>
[Πρόσβαση 5 9 2019].

Kuhrt, T. & Huseby, D., 2019. *Hyperledger Composer*. [Ηλεκτρονικό]
Available at: <https://wiki.hyperledger.org/display/composer>
[Πρόσβαση 4 10 2019].

Medibloc Team, 2019. *MediBloc Technical Whitepaper*. [Ηλεκτρονικό]
Available at: https://github.com/medibloc/whitepaper/blob/master/TechnicalWhitepaper_ENG.md
[Πρόσβαση 2 10 2019].

Medium Team, 2019. *Medium*. [Ηλεκτρονικό]
Available at: <https://medium.com/>
[Πρόσβαση 7 3 2019].

Modum Team, 2017. *DATA INTEGRITY FOR SUPPLY CHAIN OPERATIONS*. [Ηλεκτρονικό]
Available at: <https://modum.io/sites/default/files/documents/2018-05/modum-whitepaper-v.-1.0.pdf>
[Πρόσβαση 1 10 2019].

Nakamoto, S., χ.χ. *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Ηλεκτρονικό]
Available at: <https://bitcoin.org/bitcoin.pdf>
[Πρόσβαση 30 8 2019].

Nikhil, R., 2018. *In What Ways Blockchain Will Disrupt Various Industries*. [Ηλεκτρονικό]
Available at: <https://hackernoon.com/in-what-ways-blockchain-will-disrupt-various-industries-be7aaee58927>
[Πρόσβαση 29 9 2019].

Node.js Foundation, 2019. *API Reference Documentation*. [Ηλεκτρονικό]
Available at: <https://nodejs.org/en/docs/>
[Πρόσβαση 5 9 2019].

Npm Community, 2019. *About npm*. [Ηλεκτρονικό]
Available at: <https://docs.npmjs.com/about-npm/index.html>
[Πρόσβαση 6 9 2019].

Patientory Inc, 2018. *Connecting your healthcare*. [Ηλεκτρονικό]
Available at: <https://patientory.com/technology/>
[Πρόσβαση 28 9 2019].

- Patrick Dahlke, 2017. *How to: Install Go 1.11.2 on Ubuntu*. [Ηλεκτρονικό]
Available at: <https://medium.com/@patdhlk/how-to-install-go-1-9-1-on-ubuntu-16-04-ee64c073cd79>
[Πρόσβαση 15 6 2019].
- Prakash, A., 2019. *Fix 'E: Could not get lock /var/lib/dpkg/lock' Error in Ubuntu*. [Ηλεκτρονικό]
Available at: <https://itsfoss.com/could-not-get-lock-error/>
[Πρόσβαση 5 4 2019].
- Rosic, A., 2016. *What is Ethereum? [The Most Comprehensive Step-by-Step-Guide!]*. [Ηλεκτρονικό]
Available at: <https://blockgeeks.com/guides/ethereum/>
[Πρόσβαση 27 9 2019].
- Rosic, A., 2017. *What Is Hyperledger? [The Most Comprehensive Step-by-Step Guide!]*. [Ηλεκτρονικό]
Available at: <https://blockgeeks.com/guides/hyperledger/>
[Πρόσβαση 24 8 2019].
- Rouse, M., 2019. *DEFINITION*. [Ηλεκτρονικό]
Available at: <https://searchsecurity.techtarget.com/definition/nonce>
[Πρόσβαση 1 10 2019].
- Sarvepalli, M., 2018. *Hyperledger Fabric 1.2 on Multiple Hosts using Docker Swarm and Compose*. [Ηλεκτρονικό]
Available at: <https://medium.com/@malliksarvepalli/hyperledger-fabric-1-2-on-multiple-hosts-using-docker-swarm-and-compose-11c13635e69e>
[Πρόσβαση 29 5 2019].
- SecNews , 2017. *7 Εφαρμογές για smartphones που θα σας προετοιμάσουν για φυσικές καταστροφές*. [Ηλεκτρονικό]
Available at: <https://www.secnews.gr/191720/7-smartphone-apps-for-disasters/>
[Πρόσβαση 8 10 2019].
- Shaan, R., 2017. *Blockchains versus Traditional Databases*. [Ηλεκτρονικό]
Available at: <https://hackernoon.com/blockchains-versus-traditional-databases-c1a728159f79>
[Πρόσβαση 29 9 2019].
- Shermin Voshmgir, 2019. *Tokenized Networks: Web3, the Stateful Web*. [Ηλεκτρονικό]
Available at: <https://blockchainhub.net/web3-decentralized-web/>
[Πρόσβαση 18 9 2019].
- Solarte-Rivera, J., Vidal-Zemanate, A., Chamorro-Lopez, J. A. & Cobos, C., 2018. *Document Management System Based on a Private Blockchain for the Support of the Judicial Embargoes Process in Colombia*. [Ηλεκτρονικό]
Available at:
https://www.researchgate.net/publication/325566733_Document_Management_System_Based_on_a_Private_Blockchain_for_the_Support_of_the_Judicial_Embargoes_Process_in_Colombia
[Πρόσβαση 2 10 2019].
- Sphinx, 2019. *Hyperledger Fabric-Documentation*. [Ηλεκτρονικό]
Available at: <https://hyperledger-fabric.readthedocs.io/en/release-1.4/blockchain.html>
[Πρόσβαση 17 9 2019].

- Szabo, N., 1996. *Smart Contracts: Building Blocks for Digital Markets*. [Ηλεκτρονικό]
Available at: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html
[Πρόσβαση 14 8 2019].
- Tapscott, D. & Kaplan, A., 2019. *Blockchain Revolution in Education and Lifelong Learning*. [Ηλεκτρονικό]
Available at: <https://www.ibm.com/downloads/cas/93DDVAKE>
[Πρόσβαση 30 9 2019].
- Torres, N., 2018. *Three Emerging Technologies To Improve Emergency Management*. [Ηλεκτρονικό]
Available at: <https://datasmart.ash.harvard.edu/news/article/three-emerging-technologies-improve-emergency-management>
[Πρόσβαση 7 10 2019].
- Udacity, 2019. *Udacity*. [Ηλεκτρονικό]
Available at: <https://www.udacity.com>
[Πρόσβαση 2 4 2019].
- Udemy, 2019. *Udemy*. [Ηλεκτρονικό]
Available at: <https://www.udemy.com/>
[Πρόσβαση 18 6 2019].
- Vigna, P. & Casey, M. J., 2016. *The Age of Cryptocurrency: How Bitcoin and the Blockchain Are Challenging the Global Economic Order*, s.l.: Ricador.
- William, M., 2016. *The Business Blockchain Promise, Practice, and Application of the Next Internet Technology*. New Jersey: Audible Studios on Brilliance Audio; Kindle edition (January 24, 2017).
- Xiao, Y., Zhang, N., Lou, W. & Y. T. H., 2019. *A Survey of Distributed Consensus Protocols for Blockchain*. [Ηλεκτρονικό]
Available at: <https://arxiv.org/pdf/1904.04098.pdf>
[Πρόσβαση 3 10 2019].
- Yafimava, D., 2018. *Hyperledger Enterprise Solutions: Top 5 Real Use Cases*. [Ηλεκτρονικό]
Available at: <https://openledger.info/insights/hyperledger-enterprise-solutions-top-5-real-use-cases/>
[Πρόσβαση 4 10 2019].
- Zhang, S. & Lee, J. H., 2019. *Analysis of the main consensus protocols of blockchain, ICT Express*. [Ηλεκτρονικό]
Available at: <https://doi.org/10.1016/j.icte.2019.08.001>
[Πρόσβαση 30 9 2019].
- Blockgeeks, 2019. *Blockchain for Developers*. [Ηλεκτρονικό]
Available at: <https://blockgeeks.com/guides/?tagfilter=true&filter=Blockchain%20for%20Developers>
[Πρόσβαση 15 9 2019].
- Βεσκούκης, Β., 2008. *Ολοκληρωμένα συστήματα διαχείρισης κρίσεων δασικών πυρκαγιών: το σύστημα firementor*. [Ηλεκτρονικό]
Available at: <https://docplayer.gr/1983157-Oloklirouena-systiuata-diaheirisis-kriseon-dasikon->

<pyrkagion-to-systiua-firementor.html>

[Πρόσβαση 9 10 2019].

Βεσκούκης, Β., 2015. *Στοιχεία Τεχνολογίας Λογισμικού*. [Ηλεκτρονικό]

Available at: https://repository.kallipos.gr/bitstream/11419/3160/1/61_vescoukis.pdf

[Πρόσβαση 12 10 2019].

Βιτωράτος, Α., 2019. *Business Process Model Diagram: Επικοινωνία μεταξύ των εμπλεκόμενων φορέων στην αεροδιακομιδή*. s.l.:s.n.

Δανιά, Α., 2015. *Διαχείριση Εφοδιαστικής*. [Ηλεκτρονικό]

Available at:

http://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/8747/Dania_Aikaterini.pdf?sequence=1&isAllowed=y

[Πρόσβαση 4 10 2019].

Δρόσος, Γ., 2019. *Industry-Logistics-Blockchain-Supply*. [Ηλεκτρονικό]

Available at:

http://www.boussiasconferences.gr/files/boussias_conferences_content/presentations/blockchain_supply_chain/2019/giorgos_drosos_blockchain_19.pdf

[Πρόσβαση 1 10 2019].

IBM Team, 2018. *Blockchain: Essentials of Developers*. [Ηλεκτρονικό]

Available at: <https://www.coursera.org/learn/ibm-blockchain-essentials-for-developers>

[Πρόσβαση 4 12 2018].

Κοτρέτσου, Σ., 2017. ΠΜΣ «Εφαρμοσμένη Γεωγραφία και Διαχείριση Χώρου»Α' Κατεύθυνση: «Διαχείριση Φυσικών και Ανθρωπογενών Κινδύνων και Καταστροφών» Οι Αεροδιακομιδές στον Ελλαδικό χώρο. [Ηλεκτρονικό]

Available at: <http://estia.hua.gr/file/lib/default/data/19605/theFile>

[Πρόσβαση 5 10 2019].

Λογαράς, Κ., 2018. *Η τεχνολογία Blockchain, οι εφαρμογές της και οι νομικές πτυχές της*.

[Ηλεκτρονικό]

Available at: <https://m.naftemporiki.gr/story/1363055>

[Πρόσβαση 3 10 2019].

Μαυρίδης, Ι., 2015. *Ασφάλεια Πληροφοριών στο Διαδίκτυο*. [Ηλεκτρονικό]

Available at:

https://repository.kallipos.gr/pdfviewer/web/viewer.html?file=/bitstream/11419/1024/2/00_master_document-KOY.pdf

[Πρόσβαση 13 10 2019].

Μπλαβέρης, Λ. Σ., 2019. *Επτά αεροδιακομιδές ασθενών μέσα σε μια μέρα από την Πολεμική Αεροπορία*. [Ηλεκτρονικό]

Available at: <http://newpost.gr/amyna/5cbb30cdabee9eb77065aad0/epta-aerodiakomides-asthenon-mesa-se-mia-mera-apo-tin-polemiki-aeroporia>

[Πρόσβαση 23 10 2019].

Παπαζαχαρίας, Δ., 2015. *Επικοινωνίες Δεδομένων και φωνής σε ιπτάμενα μέσα*. [Ηλεκτρονικό]

Available at: <http://artemis.cslab.ece.ntua.gr:8080/jspui/bitstream/123456789/12990/2/DT2015-0344.pdf>

[Πρόσβαση 14 10 2019].

Παρδάλη, Ε., 2010. *Ηλεκτρονική Ασύρματη Πλοήγηση και Επικοινωνίες στην Αεροπορία*.

[Ηλεκτρονικό]

Available at:

<http://apothetirio.teiep.gr/xmlui/bitstream/handle/123456789/4853/860.pdf?sequence=1>

[Πρόσβαση 14 10 2019].

Σάγος, Γ., 2018. *Συστήματα ραντάρ και Ηλεκτρονικού Πολέμου*. 1 επιμ. s.l.:Α. ΠΑΠΑΣΩΤΗΡΙΟΥ & ΣΙΑ Ι.Κ.Ε..

Σαϊδης, Κ., 2017-2018. *Ανάλυση Απαιτήσεων και Σχεδιασμός Λογισμικού*. [Ηλεκτρονικό]

Available at: <https://courses.softlab.ntua.gr/softeng/2017b/Slides/03.software-analysis-design.pdf>

[Πρόσβαση 15 10 2019].

Τσελέντης, Ά., 2002. *ΣΥΣΤΗΜΑ ΕΓΚΑΙΡΗΣ ΠΡΟΕΙΔΟΠΟΙΗΣΗΣ ΕΠΕΡΧΟΜΕΝΟΥ ΣΕΙΣΜΟΥ ΚΑΙ ΤΗΣ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ ΑΥΤΟΥ*. [Ηλεκτρονικό]

Available at: <http://seismo.geology.upatras.gr/SHIELDSWEB-GREEK.htm>

[Πρόσβαση 7 10 2019].

Παραρτήματα

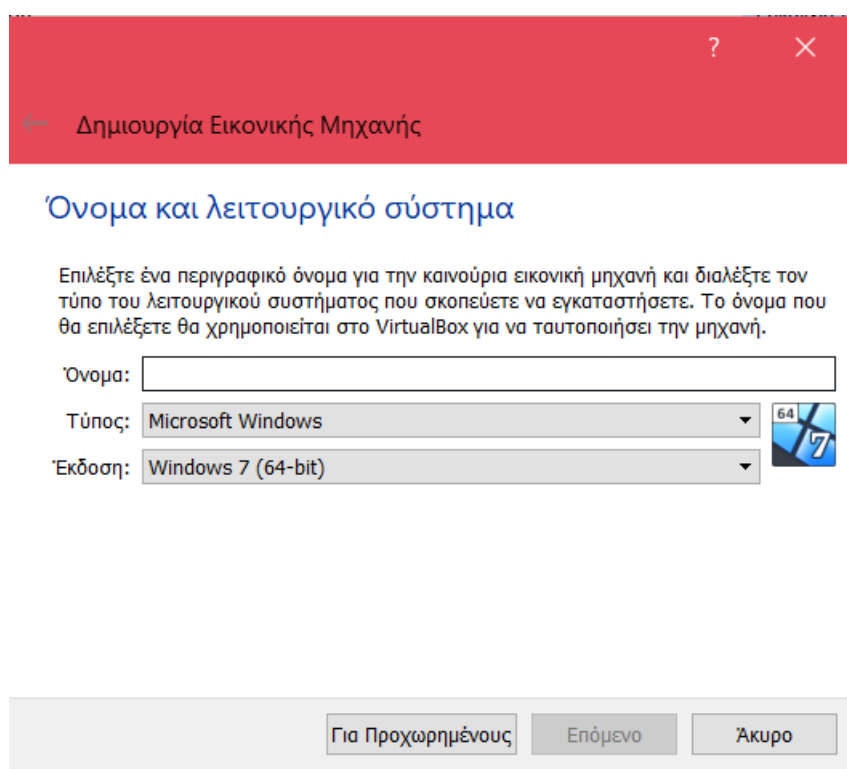
Παράρτημα 1. Δημιουργία νέου VM και επικοινωνία με τον κεντρικό υπολογιστή

Για την δημιουργία ενός νέου Vm-server εγκαθιστούμε ένα πρόγραμμα που δημιουργεί και ελέγχει τα vms, όπως το VirtualBox, που μπορούμε να το κατεβάσουμε και να το εκτελέσουμε απο την επίσημη σελίδα του Virtual Box: <https://www.virtualbox.org/>

Παράλληλα πρέπει να κατεβάσουμε το αρχείο οπτικού δίσκου (server): για ubuntu 16.04 LTS θα βρούμε όλες τις εκδόσεις στην σελίδα: <http://releases.ubuntu.com/16.04/> και σε αυτήν επιλέγουμε το αρχείο: ubuntu-16.04.06-server-amd64.iso ή για ubuntu 18.04 LTS, που θα βρούμε όλες τις εκδόσεις στην σελίδα: <http://old-releases.ubuntu.com/releases/18.04.2/> στην οποία επιλέγουμε το: ubuntu-18.04-server-amd64.iso

Ανοίγουμε τώρα το πρόγραμμα VirtualBox (την ελληνική έκδοση) και επιλέγουμε από το μενού την επιλογή «Νέα».

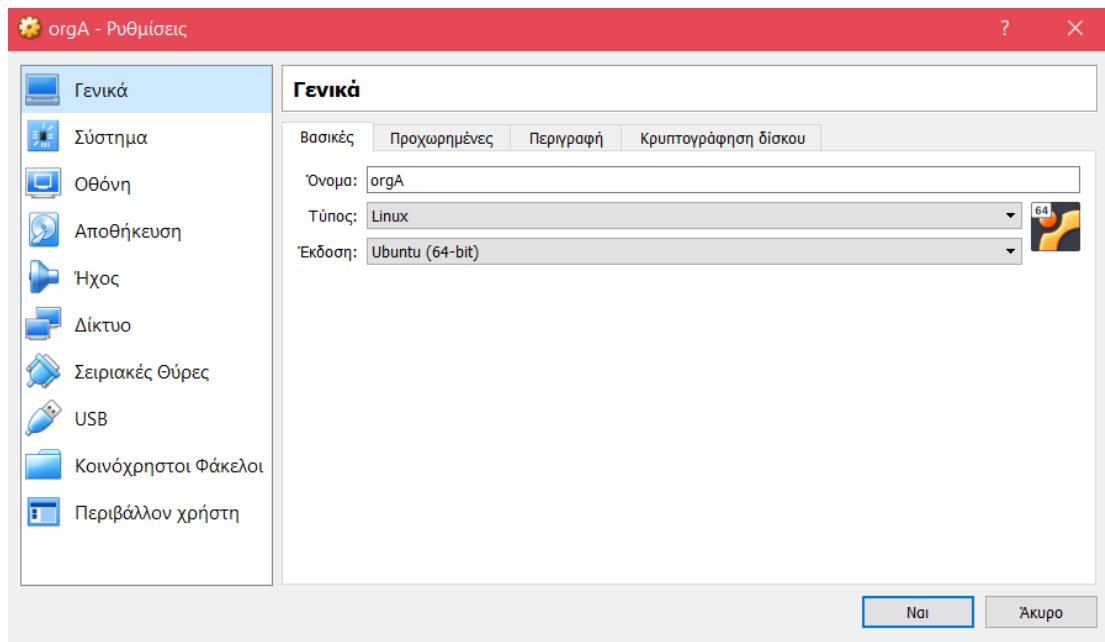
Στο νέο παράθυρο που εμφανίζεται:



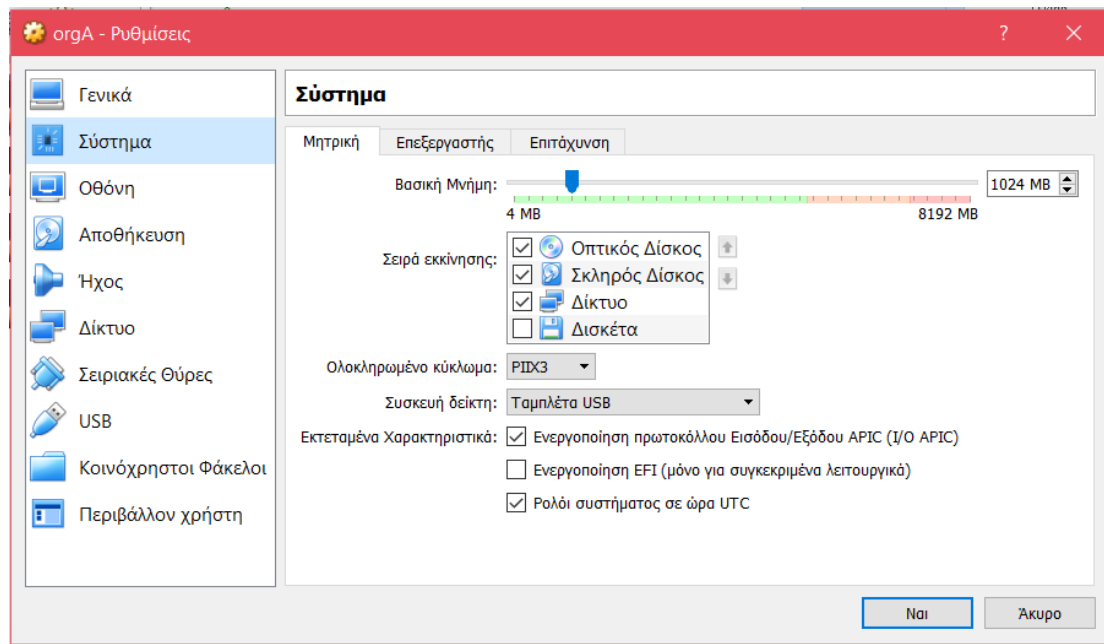
Συμπληρώνουμε στα πεδία το όνομα που θα θέλουμε να δώσουμε στο vm, συνήθως επιλέγουμε να είναι ίδιο με το hostname που θα δώσουμε στην συνέχεια. Δηλώνουμε τον τύπο να είναι Linux έκδοση ubuntu(64 bit) και επιλέγουμε «Επόμενο».

Στο νέο παράθυρο που αναφέρει το μέγεθος μνήμης αφήνουμε το προκαθορισμένο στα 1024MB και επιλέγουμε «Επόμενο». Για να το σκληρό δίσκο επιλέγουμε την επιλογή «Δημιουργήστε ένα εικονικό σκληρό δίσκο τώρα» και στην συνέχεια επιλέγουμε «Δημιουργία». Στο νέο παράθυρο που αναφέρει το τύπο αρχείου του σκληρού δίσκου αφήνουμε το προκαθορισμένο που είναι το «VDI» και στην αποθήκευση σε πραγματικό δίσκο επιλέγουμε την «Δυναμική εκχώριση». Επιλέγουμε την θέση που θέλουμε να έχουν τα αρχεία του vm(σκληρός δίσκος κλπ.) στον υπολογιστή μας και επιλέγουμε την επιλογή «Δημιουργήστε». Τώρα πλέον που έχει δημιουργηθεί το νέο vm και φαίνεται στην αρχική σελίδα του VirtualBox το επιλέγουμε και κάνοντας δεξί κλικ επιλέγουμε τις ρυθμίσεις.

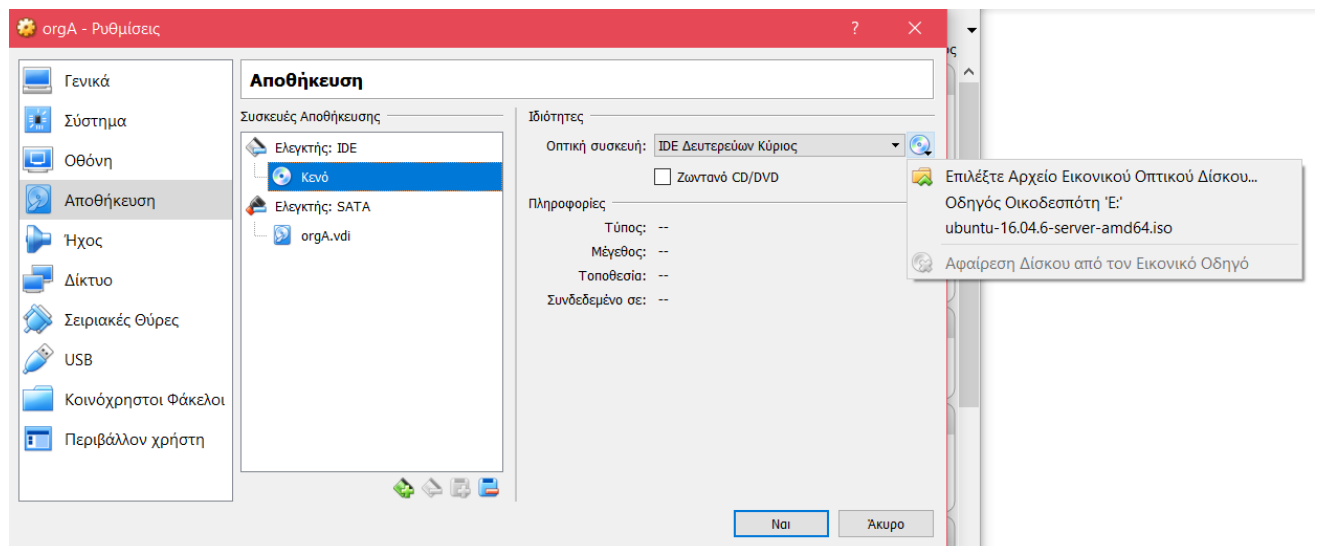
Στο νέο παράθυρο που έχει δημιουργηθεί



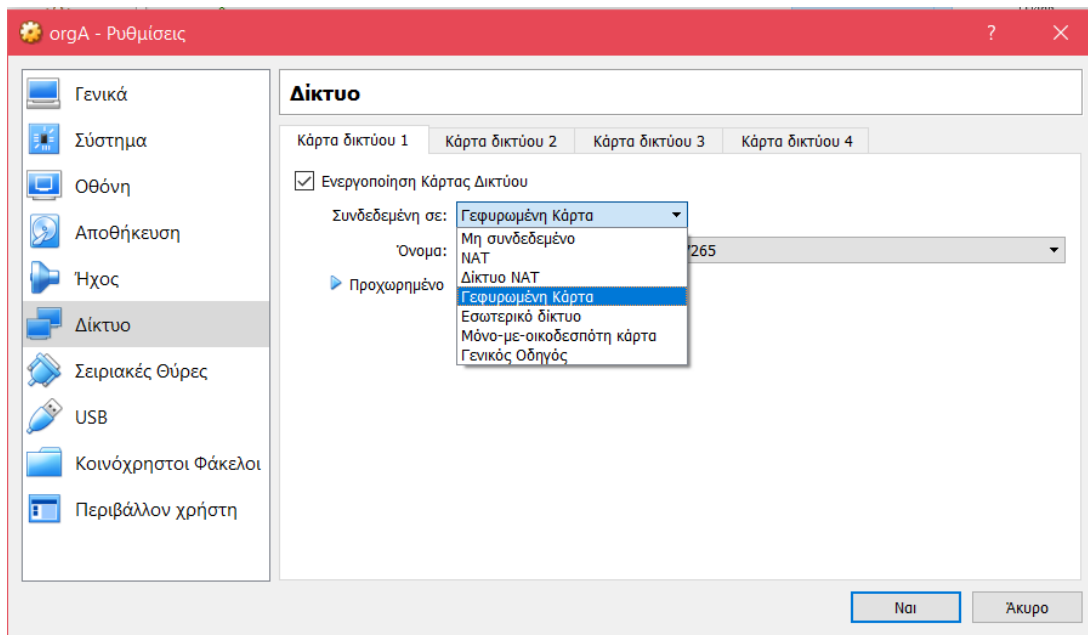
Επιλέγουμε την καρτέλα «Σύστημα» και σε αυτό επιλέγουμε στην σειρά εκκίνησης τα εξής στοιχεία(όλα εκτός από την δισκέτα):



Στην συνέχεια επιλέγουμε την καρτέλα «Αποθήκευση» στην οποία προσθέτουμε στον ελεκτή που είναι «Κενό», κάνοντας κλικ επάνω του το οπτικό αρχείο που έχουμε κατεβάσει, δηλαδή για εμάς το: ubuntu-16.04.6-server-amd64.iso

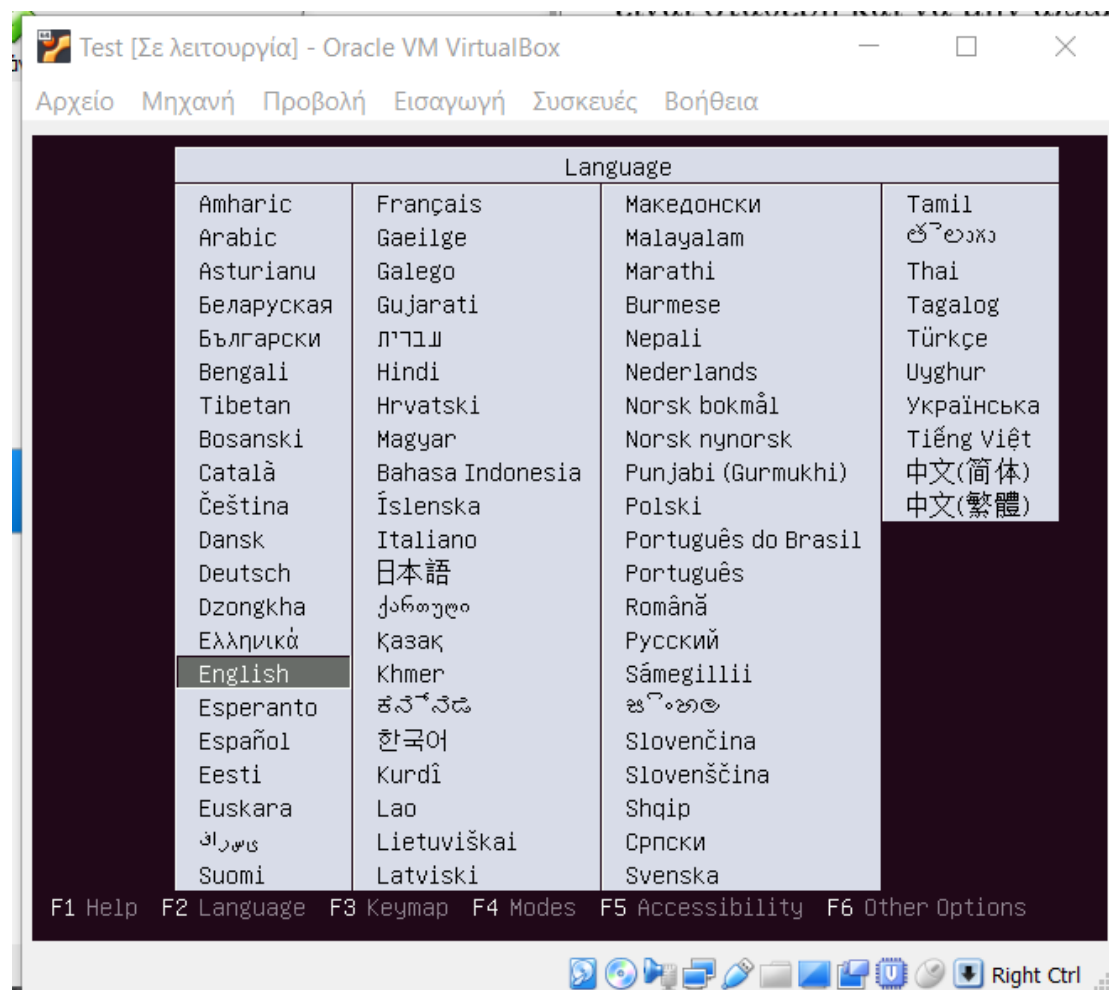


Τέλος επιλέγουμε την καρτέλα «Δίκτυο», στη επιλογή της συνδεδεμένης σε επιλέγουμε την επιλογή «Γεφρωμένη Κάρτα» ώστε η διεύθυνση-ip του vm μας να είναι σταθερή και να μην αλλάζει κάθε φορά που θα εκκινούμε το μηχανήμά μας.



Εφόσον έχουμε ολοκληρώσει όλες τις ρυθμίσεις επιλέγουμε το «Ναι» και στην συνέχεια εκκινούμε το νέο μας μηχάνημα με την επιλογή απο το μενού «Εκκίνηση».

Όταν η μηχανή ξεκινήσει απαιτεί νέες πρόσθετες ρυθμίσεις, όπως την γλώσσα, το hostname, το χρήστη, κωδικό πρόσβασης του χρήστη, και εγκατάσταση κάποιων βασικών εφαρμογών.



Ξεκινώντας λοιπόν, επιλέγουμε ως γλώσσα τα αγγλικά και πληκτρολογούμε «Enter» για να συνεχίσουμε.

Στην συνέχεια επιλέγουμε την προκαθορισμένη επιλογή «Install ubuntu server» και στο νέο παράθυρο πάλι ως γλώσσα τα αγγλικά και στην συνέχεια «United States». Για την επιλογή του keyboard επιλέγουμε «No». Και συνεχίζουμε με «Enter», όπου για την γλώσσα πληκτρολογίου επιλέγουμε το «English(US)».

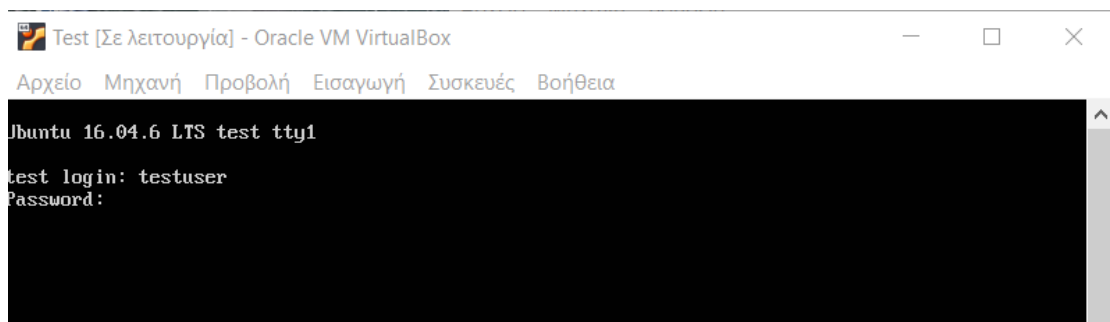
Όταν εμφανιστεί μετά από ένα διάστημα η επιλογή να πληκτρολογήσουμε το hostname που θέλουμε να δώσουμε στο μηχάνημα και πληκτρολογούμε το όνομα που είχαμε δώσει στην αρχή. Στην συνέχεια ορίζουμε ολόκληρο το όνομα που θέλουμε να δώσουμε στον βασικό χρήστη (μπορούμε να βάλουμε και το ονομά μας αλλά για ευκολία βάζουμε το ίδιο με τον username του λογαριασμού μας) και έπειτα το username και τέλος πληκτρολογούμε και το κωδικό που θα έχει ο νέος χρήστης. Στην επιλογή «Encrypt your home directory» επιλέγουμε το προκαθορισμένο «No».

Ακολουθεί ένα διάστημα για αποθήκευση των ρυθμίσεων και στην επιλογή για το time zone αν είναι «Europe/Athens» επιλέγουμε «Yes». Στην μέθοδο χωρισμού των δίσκων (Partition disks) επιλέγουμε το «Guided- use entire disk» και στην επιλογή του δίσκου αφήνουμε το σκληρό που εμφανίζεται. Στην επιλογή να γραφτούν οι αλλαγές στον δίσκο επιλέγουμε «Yes».

Μόλις εγκατασταθεί το σύστημα, στο ερώτημα «HTTP proxy information» το αφήνουμε κενό και συνεχίζουμε.

Στην συνέχεια στο ερώτημα πως να ελέγχουμε τα upgrades στο σύστημα επιλέγουμε το «No automatic updates» και στην συνέχεια απο τις επιλογές λογισμικού που παραθέτει επιλέγουμε τα: «standard system utilities» και «OpenSSH server» για την επιλογή τους πατάμε το «space».Τέλος, όταν εμφανιστεί η επιλογή να εγκατασταθεί το εργαλείο GRUB boot επιλέγουμε «Yes» και έπειτα «Continue». (Gordon, 2018)

Πλέον έχουμε ολοκληρώσει τις ρυθμίσεις που απαιτούνται για το σύστημα στο μηχάνημά μας. Και στο παράθυρο ζητείται να πληκτρολογήσουμε το username και password έχουμε ορίσει για το χρήστη μας.



Αν τα προσθέσουμε σωστά εμφανίζεται το παρακάτω:


```

Ubuntu 16.04.6 LTS test tty1

test login: testuser
Password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-142-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

124 packages can be updated.
30 updates are security updates.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

testuser@test:~$

```

Μπορούμε να τρέξουμε την εντολή: ifconfig για να ενημερωθούμε για την σταθερή ip που έχει αποκτήσει το vm μας.

Στην δική μου περίπτωση, είναι η διεύθυνση: 192.168.1.171

```

testuser@test:~$ ifconfig
enp0s3  Link encap:Ethernet  HWaddr 08:00:27:23:a3:31
        inet addr:192.168.1.171 Bcast:192.168.1.255 Mask:255.255.255.0
        inet6 addr: fe80::a00:27ff:fe23:a331/64 Scope:Link
        inet6 addr: 2a02:587:3f04:a600:a00:27ff:fe23:a331/64 Scope:Global
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:461 errors:0 dropped:0 overruns:0 frame:0
        TX packets:46 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:34168 (34.1 KB)  TX bytes:4301 (4.3 KB)

lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING  MTU:65536  Metric:1
        RX packets:176 errors:0 dropped:0 overruns:0 frame:0
        TX packets:176 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1
        RX bytes:13296 (13.2 KB)  TX bytes:13296 (13.2 KB)

testuser@test:~$

```

Για να έχουμε μια πιο εύκολη πρόσβαση στο μηχανήμά μας και να μπορούμε εύκολα να αντιγράψουμε εντολές από τις αναζητήσεις που θα κάνουμε στη συνέχεια, εφόσον έχουμε

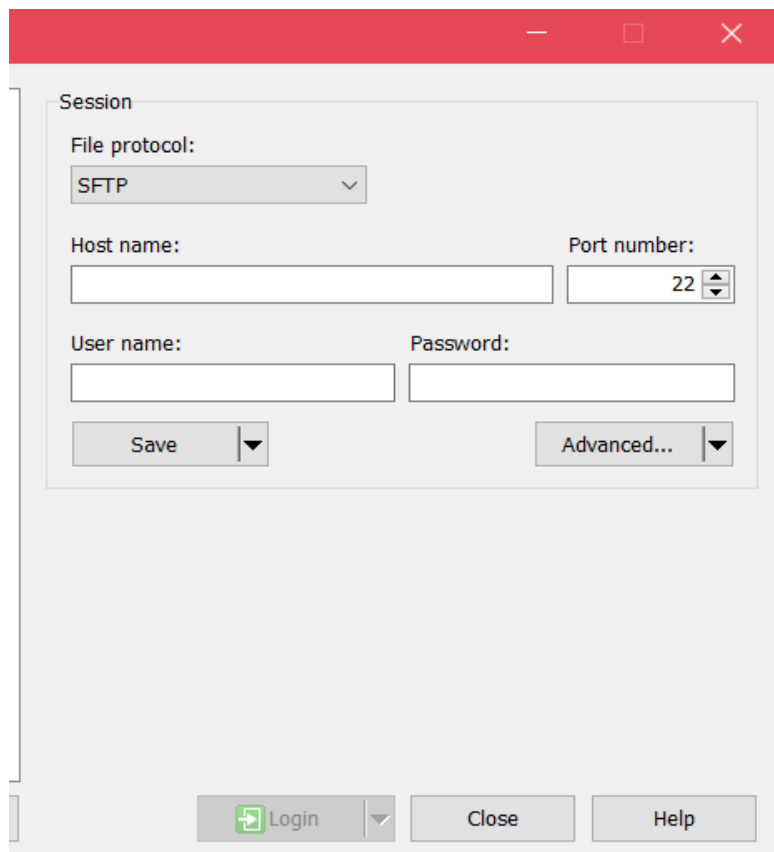
εγκαταστήσει από πριν το openSSH server, μπορούμε να ανοίξουμε το command line στον κεντρικό υπολογιστή μας και να πληκτρολογήσουμε την εντολή:

```
ssh username@«ip_του_vm»
```

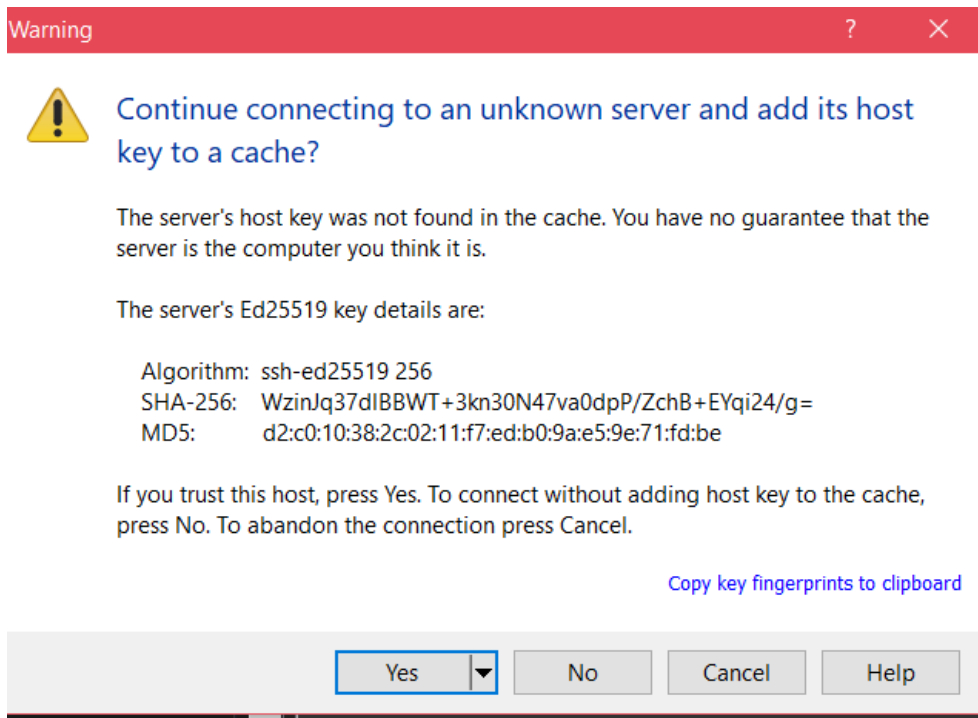
Και στην συνέχεια στο ερώτημα «Are you sure you want to continue connecting (yes/no)? » πληκτρολογούμε «Yes». Και ύστερα προσθέτουμε τον κωδικό. Πλέον έχουμε πρόσβαση στο μηχάνημα και απο το command line του υπολογιστή μας.

Επίσης για εύκολη πρόσβαση στα αρχεία του vm κατεβάζουμε το πρόγραμμα WinSCP, που ελέγχει και αντιγράφει αρχεία μεταξύ διαφορετικών vms αλλά και με τον κεντρικό υπολογιστή. Για την εγκατάστασή του πηγαίνουμε στην επίσημη σελίδα: <https://winscp.net/eng/download.php>

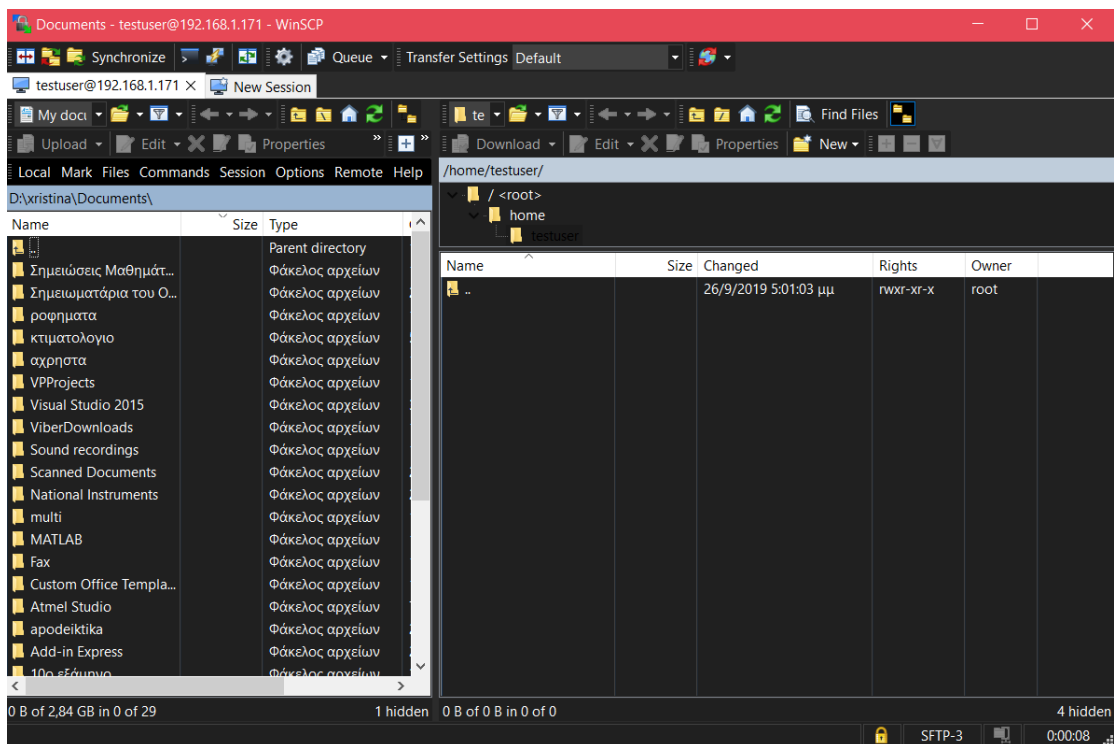
Όταν εγκαθιστούμε το πρόγραμμα στο υπολογιστή μας, το ανοίγουμε και επιλέγουμε το «New Site». Στο πλαϊνό μενού συμπληρώνουμε στο hostname για ευκολία την ip του νέου vm. Για username και password αυτά που έχουμε ορίσει και στην συνέχεια την επιλογή «Login».



Αν στην συνέχεια βγει το παρακάτω παράθυρο επιλέγουμε «Yes» για συνέχεια.



Έτσι τελικώς εμφανίζεται ένα παράθυρο με δύο καρτέλες. Στη αριστερή καρτέλα είναι τα αρχεία του κεντρικού υπολογιστή μας και στην δεξιά καρτέλα βλέπουμε τα αρχεία του vnc μας:



Παράρτημα 2. Εγκατάσταση των προαπαιτούμενων για το Hyperledger Fabric και Composer

Εγκατάσταση του Docker Engine (DigitalOcean Community, 2018)

Για την εγκατάσταση του docker θα χρησιμοποιήσουμε το Docker repository, δηλαδή το αρχείο για την εγκατάσταση του docker, αρχικά κατεβάζουμε το repository με τα πακέτα με τις εντολές:

```
sudo apt-get update
```

Σημειώνουμε ότι εάν έχουμε πρόβλημα όπως το παρακάτω, σημαίνει ότι πρέπει να απενεργοποιήσουμε την πρόσβαση σε IPv6 διευθύνσεις (Guoan, 2017):

```
"testuser@test:~$ sudo apt-get update
Get:1 https://download.docker.com/linux/ubuntu xenial InRelease [66.2 kB]
Get:2 https://download.docker.com/linux/ubuntu xenial/stable amd64 Packages [10.7 kB]
0% [Connecting to us.archive.ubuntu.com (2001:67c:1562::16)] [Connecting to security.ubuntu.com (2001:67c:1562::16)]
```

Σταμάταμε το τρέξιμο της προηγούμενης εντολής και τρέχουμε την εντολή:

```
sudo nano /etc/sysctl.d/99-sysctl.conf
```

για να έχουμε πρόσβαση στο config αρχείο του συστήματος και να προσθέσουμε τις εξής εντολές στο τέλος του αρχείου:

```
net.ipv6.conf.all.disable_ipv6 = 1
net.ipv6.conf.default.disable_ipv6 = 1
net.ipv6.conf.lo.disable_ipv6 = 1
```

Τέλος, εφόσον αποθηκεύσουμε και κλείσουμε το αρχείο, τρέχουμε την εντολή:

```
sudo sysctl -p
```

Και επαναλαμβάνουμε την εντολή:

```
sudo apt-get update
```

Προσθέτουμε τα αρχεία στο σύστημά μας με την εντολή:

```
sudo apt-get install \ apt-transport-https \ ca-certificates \ curl \ gnupg-agent \ software-properties-common
```

Και προσθέτουμε ακόμη το GPG official κλειδί με την εντολή:

```
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add -
```

Για να ελέγξουμε ότι έχουμε τον κλειδί με την υπογραφή, τρέχουμε την εντολή:

```
sudo apt-key fingerprint 0EBFCD88
```

Το αποτέλεσμα της εντολής είναι:

```
testuser@test:~$ sudo apt-key fingerprint 0EBFCD88
pub  4096R/0EBFCD88 2017-02-22
     Key fingerprint = 9DC8 5822 9FC7 DD38 854A  E2D8 8D81 803C 0EBF CD88
uid          Docker Release (CE deb) <docker@docker.com>
sub  4096R/F273FCD8 2017-02-22
```

Τέλος, η παρακάτω εντολή θα θέσει το repository να είναι αμετάβλητο:

```
sudo add-apt-repository \
    "deb [arch=amd64] https://download.docker.com/linux/ubuntu \
    $(lsb_release -cs) \
    stable"
```

Για να εγκαταστήσουμε το docker, τρέχουμε τις εντολές:

```
sudo apt-get update
sudo apt-get install docker-ce docker-ce-cli containerd.io
```

Για να ελέγξουμε ότι έχει εγκατασταθεί σωστά τρέχουμε την εντολή:

```
sudo docker version
```

```

testuser@test:~$ sudo docker version
[sudo] password for testuser:
Client: Docker Engine - Community
Version:      19.03.2
API version:  1.40
Go version:   go1.12.8
Git commit:   6a30dfc
Built:        Thu Aug 29 05:28:19 2019
OS/Arch:      linux/amd64
Experimental: false

Server: Docker Engine - Community
Engine:
Version:      19.03.2
API version:  1.40 (minimum version 1.12)
Go version:   go1.12.8
Git commit:   6a30dfc
Built:        Thu Aug 29 05:26:54 2019
OS/Arch:      linux/amd64
Experimental: false
containerd:
Version:      1.2.6
GitCommit:    894b81a4b802e4eb2a91d1ce216b8817763c29fb
runc:
Version:      1.0.0-rc8
GitCommit:    425e105d5a03fabd737a126ad93d62a9eeede87f
docker-init:
Version:      0.18.0
GitCommit:    fec3683
testuser@test:~$

```

Εγκατάσταση του Docker Compose

Για να εγκαταστήσουμε το docker compose (DigitalOcean Community, 2017), αρχικά αντιγράφουμε το repository με την εντολή:

```

sudo curl -L https://github.com/docker/compose/releases/download/1.18.0/docker-
compose-`uname -s`-`uname -m` -o /usr/local/bin/docker-compose

```

Στην συνέχεια επιτρέπουμε την εκτέλεση της εντολής με την εντολή:

```

sudo chmod +x /usr/local/bin/docker-compose

```

Και τέλος για να ελέγξουμε ότι έχει εγκατασταθεί σωστά τρέχουμε την εντολή:

```

docker-compose version

```

```

testuser@test:~$ docker-compose version
docker-compose version 1.18.0, build 8dd22a9
docker-py version: 2.6.1
CPython version: 2.7.13
OpenSSL version: OpenSSL 1.0.1t  3 May 2016
testuser@test:~$

```

Εγκατάσταση του node.js και του npm

Για να εγκαταστήσουμε το node.js και το npm με nvm (DigitalOcean Community, 2018), τρέχουμε αρχικά τις εντολές:

```
sudo apt-get update  
sudo apt-get install build-essential libssl-dev
```

Στην συνέχεια αντιγράφουμε το nvm repository με την εντολή:

```
curl -sL https://raw.githubusercontent.com/creationix/nvm/v0.33.8/install.sh -o in-  
stall_nvm.sh
```

Τώρα, εγκαθιστούμε το αρχείο στο σύστημά μας με τις εντολές:

```
bash install_nvm.sh  
source ~/.profile
```

Έπειτα, για να δούμε όλες τις διαθέσιμες εκδόσεις του nvm τρέχουμε την εντολή:

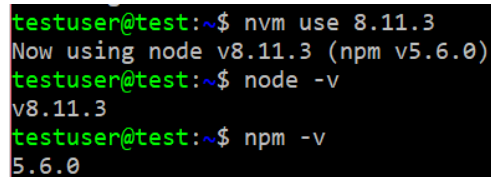
```
nvm ls-remote
```

Και τέλος, για να εγκαταστήσουμε την έκδοση v8.11.3 τρέχουμε την εντολή:

```
nvm install 8.11.3  
nvm use 8.11.3
```

Για να δούμε αν έχει εγκατασταθεί σωστά το node.js τρέχουμε την εντολή: node -v

Ενώ για το npm τρέχουμε την εντολή: npm -v



```
testuser@test:~$ nvm use 8.11.3  
Now using node v8.11.3 (npm v5.6.0)  
testuser@test:~$ node -v  
v8.11.3  
testuser@test:~$ npm -v  
5.6.0
```

Εγκατάσταση της προγραμματιστικής γλώσσας Python

Γίνεται απλά με τη εντολή:

```
sudo apt-get install python-minimal
```

Εγκατάσταση της γλώσσας Go Language

Αρχικά (Patrick Dahlke, 2017), κατεβάζουμε το go repository σε συμπιεσμένη μορφή με την εντολή:

```
curl -O https://storage.googleapis.com/golang/go1.9.3.linux-amd64.tar.gz
```

Έπειτα, αποσυμπιέζουμε το αρχείο με τις εντολές:

```
sha256sum go1.9.3.linux-amd64.tar.gz  
tar -xvf go1.9.3.linux-amd64.tar.gz
```

Και εγκαθιστούμε τα νέα αρχεία στην τοποθεσία /usr/local του vim με την εντολή:

```
sudo mv go /usr/local
```

Ύστερα, ανοίγουμε το αρχείο με την εντολή: `sudo vim ~/.profile` και να προσθέσει τις εντολές στο τέλος του αρχείου:

```
export GOPATH=$HOME/go  
export PATH=$PATH:/usr/local/go/bin:$GOPATH/bin
```

Και τέλος αποθηκεύουμε τις ρυθμίσεις στο σύστημα με την εντολή:

```
source ~/.profile
```

Για να ελέγξουμε ότι όλα εγκαταστάθηκαν σωστά τρέχουμε την εντολή:

```
go version
```

```
testuser@test:~$ source ~/.profile  
testuser@test:~$ go version  
go version go1.9.3 linux/amd64  
testuser@test:~$
```


Παράρτημα 3. Διάγραμμα Business Process Model για την αεροδιακομιδή

