ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

BLOCKCHAIN KAI SMART CONTRACTS

ΦΟΙΤΗΤΗΣ: ΣΕΡΑΦΗΣ ΝΙΚΟΛΑΟΣ

ΒΑ11179

ΚΑΘΗΓΗΤΗΣ: ΧΑΡΑΚΤΙΝΙΩΤΗΣ ΣΤΕΦΑΝΟΣ

ΧΙΟΣ 2020

ΠΕΡΙΕΧΟΜΕΝΑ

Λίστα εικόνων

1. ***Εισαγωγή***

Η πρόοδος στην τεχνολογία συνεχίζει να μετασχηματίζει μια ευρεία γκάμα βιομηχανιών, συμπεριλαμβανομένης της τεράστιας βιομηχανίας της εφοδιαστικής αλυσίδας. Οι συνεχώς μεταβαλλόμενες και αυξανόμενες απαιτήσεις των καταναλωτών πλάθουν τη βιομηχανία αυτή σε άμεσα εξελισσόμενη ώστε να μπορεί να ανταποκρίνεται στις ανάγκες τους.

Η τεχνολογία Blockchain έγινε αρχικά γνωστή μέσα από την λειτουργία του Bitcoin. Σύντομα όμως οι χρήστες της συγκεκριμένης τεχνολογίας συνειδητοποίησαν ότι το Blockchain έχει πολύ μεγαλύτερες δυνατότητες, μέσα από τις οποίες μπορεί να αλλάξει ολόκληρο το διαδίκτυο. Χαρακτηριστική είναι η δήλωση των Tapscott και Tapscott (2016) οι οποίοι χαρακτηρίζουν το Blockchain ως το "έμπιστο πρωτόκολλο" που τόσα χρόνια έλειπε από το διαδίκτυο. Επίσης, αναφέρουν ότι τόσα χρόνια μέσα από το διαδίκτυο μπορούσαμε να μεταφέρουμε δεδομένα, ενώ τώρα μας δίνεται η δυνατότητα να μεταφέρουμε αξία (Tapscott & Tapscott, 2016).

Οι χρήσεις του blockchain σε βάθος χρόνου θα είναι αμέτρητες. Σύμφωνα με προβλέψεις ειδικών σε λιγότερο από 10 χρόνια οι εφαρμογές του blockchain θα εφαρμόζονται σε όλα τα φάσματα της ζωής του σύγχρονου ανθρώπου. Θα είναι εύκολο να γίνεται η συλλογή φόρων από τους πολίτες, οι μεταφορές χρημάτων από οποιοδήποτε μέρος του πλανήτη, θα υλοποιηθούν αυτόνομες επιχειρηματικές λειτουργίες, θα μπορούν άμεσα να ταυτοποιούνται τα άτομα με τα προσωπικά τους στοιχεία διασφαλίζοντας όμως τα προσωπικά τους δεδομένα. Ακόμα και οι οικονομικές απάτες θα μειωθούν καθώς κάθε συναλλαγή θα καταγράφεται σε ένα κατανεμημένο καθολικό. Η γραφειοκρατία θα μειωθεί μέσω της ψηφιοποίησης και αυτοματοποίησης των συστημάτων. Το blockchain είναι μία πηγή εμπιστοσύνης με παγκόσμια εμβέλεια.

Στα μέσα του 2018 παρουσιάστηκε μια πρωτοφανής έκρηξη της δημοτικότητας των τεχνολογιών του blockchain μέσω της αύξησης της ζήτησης του Bitcoin από τα τέλη του 2017 (Fiorillo, 2018). Η αυξημένη ζήτηση του

κρυπτονομίσματος εκτίναξε την τιμή αγοράς στα ανώτατα επίπεδα σε βάθος δεκαετίας. Παράλληλα υπήρξε η ολοένα και αυξανόμενη δημιουργία νέων κρυπτονομισμάτων τα ICO (Initial Coin Offering). Αυτό είχε σαν αποτέλεσμα οι κυβερνήσεις να προσπαθήσουν να βρουν λύσεις ώστε να καταφέρουν να ρυθμίσουν τη ροή και τη συγκέντρωση χρήματος ώστε να περιορίσουν τις οικονομικές απάτες, μπαίνοντας έτσι βαθύτερα στο χώρο του blockchain (O'Neal, 2018).

Σήμερα οι τεχνολογίες του blockchain εισάγονται στην καθημερινότητα σε διάφορους τομείς. Μεγάλες βιομηχανίες αυτοματοποιούν συστήματα, παραγωγής, ταυτοποίησης ποιότητας προϊόντος ακόμη και παροχής υπηρεσίας. Η τεχνολογία blockchain του Hyperledger έχει φτάσει τα 250 μέλη, δείχνοντας το μεγάλο ενδιαφέρων που υπάρχει για τις blockchain εφαρμογές. Εταιρείες κολοσσοί, όπως η Samsung, ενσωματώνουν εφαρμογές πορτοφολιών κρυπτονομισμάτων στα νέα μοντέλα κινητών (theverge.com, 2019), προσπαθώντας να προλάβουν τις εξελίξεις και να γίνουν μέρος αυτών. Άλλο ένα χαρακτηριστικό παράδειγμα είναι, η Wallmart, η μεγαλύτερη εταιρεία supermarket παγκοσμίως που ενσωμάτωσε στο δίκτυό της, τεχνολογίες blockchain με την εφαρμογή FoodTrust. Η υιοθέτηση αυτών των τεχνολογιών παρατηρείται από πλευράς επιχειρήσεων στην εφοδιαστική αλυσίδα, στα χρηματοοικονομικά, στον τομέα υγείας αλλά και σε κυβερνητικό επίπεδο.

Συνοπτικά υπάρχουν δύο βασικοί τύποι blockchain:

- Τα δημόσια (permissioinless) στα οποία ο καθένας μπορεί να διαβάσει και να γράψει. Είναι ανοιχτού κώδικα και όλοι μπορούν να λάβουν μέρος σε αυτά, να εξερευνήσουν και να στείλουν συναλλαγές ή συμβάσεις. Παραδείγματα δημοσίων blockchain είναι το Bitcoin και το Etherum. Τα ιδιωτικά blockchain (permissioned) στα οποία οι συμμετέχοντες είναι γνωστοί και αξιόπιστοι εκ των προτέρων.
- Τα δικαιώματα και η εγγραφή διατηρούνται κεντρικά σε έναν οργανισμό, ενώ για ανάγνωση είναι με περιορισμένη έκταση

Στην εφοδιαστική αλυσίδα για την διασφάλιση της καλής ποιότητας του

προϊόντος και της ασφαλούς κατανάλωσής του, πληρώντας τις απαραίτητες προϋποθέσεις υγιεινής, είναι χρήσιμο να εφαρμοστούν permissioned blockhain εφαρμογές. Οι εφαρμογές αυτές, θα φέρουν το μέγιστο δυνατό αποτέλεσμα σε κάθε στάδιο μέχρι το τελικό προϊόν να φτάσει στο ράφι του καταναλωτή.

Ωστόσο υπάρχουν και προκλήσεις από την χρήση της τεχνολογίας αυτής. Στα δημόσια δίκτυα το βασικότερο εμπόδιο για την ευρεία υιοθέτηση του blockchain είναι το κόστος της ενέργειας που απαιτείται. Ο όγκος των συναλλαγών και η αποθήκευση των δεδομένων είναι βασικές ανησυχίες για την επεκτασιμότητα του blockchain. Ο κίνδυνος από κυβερνοεπιθέσεις και το θεσμικό πλαίσιο στο οποίο λειτουργεί είναι δύο ακόμα παράγοντες που πρέπει να συνυπολογιστούν. Μια ακόμη μεγάλη πρόκληση για την υλοποίηση τέτοιων τεχνολογιών σε βιομηχανικό επίπεδο είναι η εναρμόνιση των διαφορετικών συμβαλλομένων, οι οποίοι έχουν πολύπλοκες και διαφορετικές διαδικασίες, σε μια ενιαία πατροναρισμένη ροή, η οποία απαιτεί την σωστή κατανόηση όλων των προηγούμενων σταδίων.

Παρά το γεγονός ότι η σταδιακή ανάπτυξη της ποιότητας των μεταποιημένων προϊόντων τα τελευταία χρόνια έχει δημιουργήσει μια ευκαιρία για την υλοποίηση ασφαλούς και καλής ποιότητας παραγωγής με βάση εναρμονισμένους νόμους της ΕΕ - οι καταναλωτές έχουν όλο και περισσότερες ανησυχίες και δίνουν μεγαλύτερη προσοχή στην ποιότητα των προϊόντων. Ωστόσο, η καλή ποιότητα των τροφίμων μπορεί να παραχθεί μόνο από υλικά καλής ποιότητας στα οποία γίνεται σωστή μεταχείριση σε όλα τα στάδια της εφοδιαστικής αλυσίδας.

2. ***Τεχνολογία blockchain***

2.1. Ορισμός blockchain

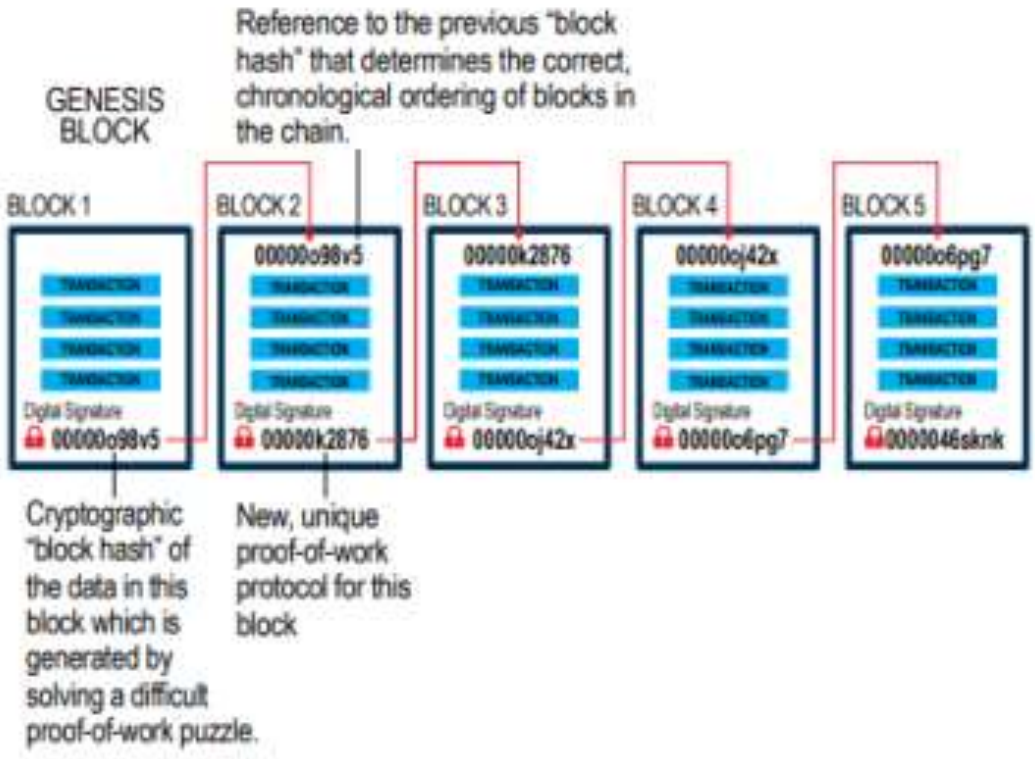
Το Blockchain είναι ένα αποκεντρωμένο και κατανεμημένο βιβλιάριο που χρησιμοποιείται για την καταγραφή δεδομένων σε ένα δίκτυο από ανεξάρτητους και άγνωστους μεταξύ τους χρήστες. Αυτό το κοινόχρηστο βιβλιάριο μπορεί να χρησιμοποιηθεί για την καταγραφή δεδομένων οποιασδήποτε μορφής. Στο σημείο αυτό θα πρέπει να διευκρινιστεί ότι τα δεδομένα διακρίνονται σε φυσικά και άυλα. Παραδείγματα φυσικών δεδομένων αποτελούν οι τίτλοι ιδιοκτησίας ενός σπιτιού ή ενός αυτοκινήτου ενώ ο όρος άυλο δεδομένο αναφέρεται στην πνευματική ιδιοκτησία (πνευματικά δικαιώματα και πατέντες). Στην πραγματικότητα, οτιδήποτε έχει αξία μπορεί να καταχωρηθεί και να διακινηθεί σε ένα δίκτυο Blockchain (Laurence, 2017 , Gupta, 2017 , Tapscott & Tapscott, 2016)

Η δομή δεδομένων blockchain είναι μια ταξινομημένη και αυξανόμενη λίστα συναλλαγών. Οι εγγραφές ονομάζονται μπλοκ και συνδέονται μεταξύ τους με κρυπτογραφία (Antonopoulos, 2017). Κάθε μπλοκ περιέχει ένα κρυπτογραφημένα κωδικό κατακερματισμού του προηγούμενου μπλοκ (hash), στίγματα χρόνου των συναλλαγών και δεδομένα. Το αρχείο συναλλαγών διατηρείτε σε διάφορους υπολογιστές οι οποίοι είναι συνδεδεμένοι σε ένα peer-to-peer (p2p) δίκτυο (Nakamoto, 2008). Έτσι η τεχνολογία Blockchain επιτρέπει να υπάρχουν κατανεμημένα και αμετάβλητα δεδομένα με ασφαλή και κρυπτογραφημένο τρόπο. Διασφαλίζοντας παράλληλα ότι οι συναλλαγές δεν μπορούν ποτέ να τροποποιηθούν.

2.2. Λειτουργία Blockchain

Αναφορικά με τον τρόπο λειτουργίας του Blockchain, θα πρέπει να αναφερθεί ότι στη συγκεκριμένη τεχνολογία χρησιμοποιείται κρυπτογράφηση των δεδομένων, η οποία περιλαμβάνει την ύπαρξη ενός ζεύγους κλειδιών (ενός δημόσιου και ενός ιδιωτικού) επιτρέποντας σε κάθε συμμετέχοντα οποιουδήποτε δικτύου να διαχειρίζεται το τμήμα πληροφορίας που του ανήκει, με ασφαλή τρόπο, χωρίς δηλαδή την ανάγκη κεντρικής αρχής. Η απαλοιφή της κεντρικής αρχής αποτελεί θεμελιώδη αρχή στο Blockchain. Άξιο αναφοράς κρίνεται επίσης ότι τα δεδομένα που καταγράφονται σε ένα Blockchain είναι εξαιρετικά δύσκολο να αλλάξουν ή να αφαιρεθούν, στοιχείο που εμφανίζεται για πρώτη φορά στην πληροφορική.

Το blockchain, όπως προαναφέρθηκε, είναι μια αποκεντρωμένη δομή δεδομένων στην οποία αποθηκεύονται ομάδες συναλλαγών σε ένα κατανεμημένο δίκτυο. Οι συμμετέχοντες του δικτύου έχουν πρόσβαση σε όλα τα ιστορικά δεδομένα και τις συναλλαγές, συμπεριλαμβανομένου της ώρας δημιουργίας των μπλοκ. Κάθε μπλοκ αποτελείται από συγκεκριμένες πληροφορίες, μια λίστα με τις συναλλαγές που έγιναν σε κάποιο χρονικό διάστημα, μια σφραγίδα του χρόνου δημιουργίας του και μια ψηφιακή αναφορά (hash) στο προηγούμενο μπλοκ. Με την πάροδο του χρόνου δημιουργείται μια ταξινομημένη σειρά από μπλοκ (βλ. Εικόνα 1). Για να επαληθευτεί η εγκυρότητα των μπλοκ χρησιμοποιούνται αλγόριθμοι συναίνεσης όπου μπορούν να το επιτύχουν σχεδόν σε πραγματικό χρόνο. Αυτό γίνεται σε συνδυασμό με την κρυπτογραφημένη αναφορά, το hash, που υπάρχει και τον αλγόριθμο που το επικυρώσει. Στα δημόσια blockchains η διαδικασία αυτή ονομάζεται εξόρυξη (mining) (Acheson, 2018). Η εξόρυξη περιλαμβάνει μια μορφή ανταμοιβής για κάποιον που θα επαληθεύσει ή θα επικυρώσει ένα μπλοκ. Για παράδειγμα στο Bitcoin όποιος επαληθεύσει ένα μπλοκ θα λάβει μια συγκεκριμένη αμοιβή από Bitcoin (Transaction Fees + Block Reword).



Εικόνα 1 Δομή blockchain

Αυτού του είδους η διαδικασία ονομάζεται απόδειξης της εργασίας (Proof-of-Work, PoW) και ο σκοπός της είναι να επικυρώσει ότι ο αλγόριθμος είναι αληθής και η συναλλαγή είναι νόμιμη (Wu, et al., 2017). Αν κάποιος προσπαθήσει να αλλάξει ή να παραβιάσει τις πληροφορίες συναλλαγής που καταγράφονται σε ένα μπλοκ, το hash για το συγκεκριμένο μπλοκ θα αλλάξει και δεν θα δείχνει πια το hash του προηγούμενου, επαληθευμένου μπλοκ. Τέλος, το πρώτο block που δημιουργείται στην αλυσίδα ονομάζεται Genesis μπλοκ, είναι ειδική περίπτωση, γι' αυτό δεν έχει κάποια αναφορά σε προηγούμενο μπλοκ και είναι γραμμένο στον κώδικα που ξεκινάει το blockchain.

Επίσης καινοτομία του Blockchain συνιστά η δυνατότητα διαχείρισης περιουσιακών στοιχείων χωρίς να χρειάζεται η παρέμβαση και πιστοποίηση από εξουσιοδοτημένες αρχές και οργανισμούς (Laurence, 2017 , Gupta, 2017). Στην περίπτωση που κάποιος θελήσει να προσθέσει μια εγγραφή (συναλλαγή ή καταχώρηση) σε ένα Blockchain, θα πρέπει τα δεδομένα να ελεγχθούν από έναν αλγόριθμο ο οποίος θα επιβεβαιώσειτην ακεραιότητα και την ορθότητα

της κάθε συναλλαγής, χωρίς να απαιτείται η περαιτέρω πιστοποίηση από κάποιον τρίτο οργανισμό (Laurence, 2017). Επιπρόσθετα, το Blockchain μπορεί να χρησιμοποιηθεί σε όλες τις περιπτώσεις στις οποίες απαιτείται αποθήκευση δεδομένων. Εντούτοις, ευρύτερη και σπουδαιότερη είναι η εφαρμογή του σε αναξιόπιστα δίκτυα στα οποία θέλουμε να εξασφαλίσουμε ότι τα δεδομένα και τα αρχεία μας δεν πρόκειται να παραποιηθούν ή να διαγραφούν. Επομένως το Blockchain ενισχύει σε σημαντικό βαθμό την εμπιστοσύνη σε ένα δίκτυο (Gupta, 2017).

- Το Blockchain αποτελείται από 3 διαφορετικούς τύπους. Η επιλογή του Blockchain τύπου που θα χρησιμοποιηθεί εξαρτάται από τους εξής παράγοντες: Αν το βιβλιάριο θα είναι κατανεμημένο ή όχι.
- Ποιοι χρήστες θα έχουν πρόσβαση σε αυτό.
- Ποιοι χρήστες θα επαληθεύουν και θα καταχωρούν τις συναλλαγές δεδομένων στο βιβλιάριο.

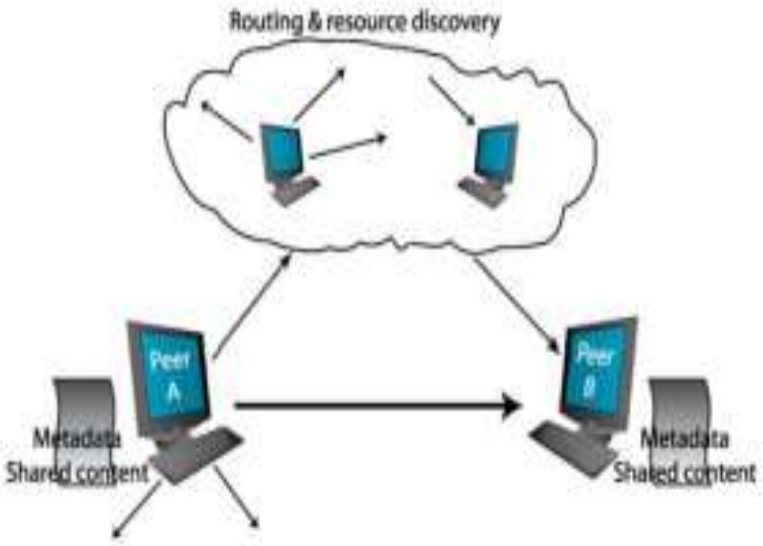
2.3. Χαρακτηριστικά blockchain

Το blockchain λόγω της αρχιτεκτονικής και του τρόπου που λειτουργεί έχει κάποια πολύ σημαντικά χαρακτηριστικά:

- Αμετάβλητο (Immutable) – (permanent and tamper-proof) Το blockchain είναι ένα μόνιμο αρχείο συναλλαγών. Εφόσον προστεθεί ένα block στον κόμβο δεν μπορεί να τροποποιηθεί. Αυτό οδηγεί στην ασφάλεια και στην εμπιστοσύνη των συναλλαγών.
- Αποκεντρωμένο – αυτό αποθηκεύετε σε ένα αρχείο το οποίο είναι προσβάσιμο και αντιγράφεται από οποιονδήποτε κόμβο του δικτύου. Το όποιο και δημιουργεί την αποκέντρωση.
- Διαφανές (Transparent) – (ολόκληρο ιστορικό συναλλαγών) κάθε μέρος μπορεί να έχει πρόσβαση και να ελέγχει τις συναλλαγές. Αυτό δημιουργεί την έννοια της προέλευσης και της παρακολούθησης ολόκληρης της ζωής του περιουσιακού στοιχείου.
- Βασίζεται στη Συναίνεση (Consensus Driven) – κάθε μπλοκ στο blockchain επαληθεύεται ανεξάρτητα μέσω μοντέλων συναίνεσης που παρέχουν κανόνες για την επικύρωση ενός μπλοκ. Πολύ συχνά στα δημόσια δίκτυα χρειάζονται πολλοί πόροι για να το πετύχουν αυτό (π.χ. επεξεργαστική ισχύ). Στο bitcoin η διαδικασία αυτή ονομάζεται εξόρυξη. Ο μηχανισμός αυτός λειτουργεί χωρίς κάποια κεντρική αρχή.

2.4. Δίκτυα peer to peer

Τα ομότιμα ή γνωστά ως peer-to-peer (P2P) δίκτυα επιτρέπουν δύο ή περισσότερους υπολογιστές να διαμοιράζουν ισοδύναμα τους πόρους τους. Λειτουργεί ταυτόχρονα ο κάθε υπολογιστής ως πελάτης και ως εξυπηρετητής (Schollmeier, 2002). Οι πληροφορίες που βρίσκονται στον κάθε κόμβο διαμοιράζονται και συγχρονίζονται κατ' επιλογή μεταξύ τους δίχως κεντρικό εξυπηρετητή. Αυτό διαφέρει από ένα μοντέλο κεντρικού διακομιστή που επιβραδύνεται όταν περισσότεροι χρήστες συμμετέχουν, καθώς το δίκτυο P2P μπορεί να βελτιώσει την ισχύ του με περισσότερες συσκευές ή κόμβους που ενώνουν το δίκτυο.



Εικόνα 2 Επικοινωνία peer to peer

Αυτή η μέθοδος μεταφοράς πληροφοριών αποτελεί σημαντικό συστατικό στοιχείο του blockchain επειδή τα δεδομένα δεν αποθηκεύονται σε ένα συγκεντρωτικό σημείο, καθιστώντας την, πολύ λιγότερο ευάλωτη σε εκμετάλλευση, αλλοίωση ή απώλεια. Για παράδειγμα στην Εικόνα 2 ο Peer A ζητάει κάποια δεδομένα που έχει ο Peer B. Πρώτα πρέπει μέσω του P2P δικτύου να εντοπίσει πως το B είναι αυτός που έχει τα δεδομένα. Στη συνέχεια εφόσον εντοπιστεί δημιουργείται απευθείας σύνδεση του Peer A με τον Peer B.

2.5. Private

Τα ιδιωτικά Blockchains τείνουν να είναι πολύ πιο μικρά σε αριθμό συμμετεχόντων σε σχέση με τους υπόλοιπους τύπους Blockchain. Ενδέχεται μάλιστα ο κόσμος να μην γνωρίζει καν την ύπαρξή τους επειδή τις περισσότερες φορές δεν είναι ορατά στο κοινό . Η συμμετοχή κάθε χρήστη είναι ελεγχόμενη από μια κεντρική αρχή. Ως προς τα χαρακτηριστικά τους θα πρέπει να αναφερθεί ότι είναι πολύ πιο γρήγορα από τους υπόλοιπους τύπους και ενδέχεται να μην παρουσιάζουν καμία καθυστέρηση στο χρόνο επικύρωσης των δεδομένων. Έχουν επίσης χαμηλό κόστος λειτουργείας, απεριόριστη χωρητικότητα και μπορούν να κατασκευαστούν σε πολύ γρήγορο χρονικό διάστημα. Εντούτοις τα περισσότερα ιδιωτικά Blockchain δεν χρησιμοποιούν κρυπτονόμισμα και δεν έχουν την ίδια ασφάλεια που παρέχει ένα αποκεντρωμένο Blockchain δίκτυο (Gupta, 2017 , Tapscott & Tapscott, 2016).

2.6. Public

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

επικύρωση των συναλλαγών τους, προκειμένου να ενθαρρύνει περισσότερους συμμετέχοντες να ενταχθούν σε αυτό και να χρησιμοποιήσουν το κρυπτονόμισμα.

Αξιοσημείωτο κρίνεται και το γεγονός ότι τα δημόσια Blockchains τείνουν να είναι πιο ασφαλή από τους υπόλοιπους τύπους Blockchain λόγω του ότι κανένας οργανισμός ή κυβέρνηση δεν ελέγχει το δίκτυο και η συμμετοχή γίνεται ανώνυμα. Ο κώδικας με τη σειρά του ανανεώνεται αποκλειστικά από την κοινότητα του κάθε Blockchain δικτύου στην οποία συμμετέχουν εθελοντικά προγραμματιστές.

Εξετάζοντας τα μειονεκτήματα των δημόσιων Blockchains καθίσταται φανερό ότι απαιτείται σημαντικό ποσό υπολογιστικής ισχύος για να επιτευχθεί ο συγχρονισμός και η διατήρηση του κατανεμημένου βιβλιαρίου. Επίσης το δημόσιο Blockchain είναι συχνά πιο αργό από τους υπόλοιπους τύπους Blockchain και με τη συνεχόμενη αύξηση των συναλλαγών αντιμετωπίζει προβλήματα αποθηκευτικού χώρου (Laurence, 2017).

2.7. Bitcoin και ethereum

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

κρυπτονόμισμα. Αξιοσημείωτο κρίνεται και το γεγονός ότι τα δημόσια Blockchains τείνουν να είναι πιο ασφαλή από τους υπόλοιπους τύπους Blockchain λόγω του ότι κανένας οργανισμός ή κυβέρνηση δεν ελέγχει το δίκτυο και η συμμετοχή γίνεται ανώνυμα. Ο κώδικας με τη σειρά του ανανεώνεται αποκλειστικά από την κοινότητα του κάθε Blockchain δικτύου στην οποία συμμετέχουν εθελοντικά προγραμματιστές.

Το Bitcoin δημιουργήθηκε το 2008 από έναν άνθρωπο ή ομάδα (The Economist, 2015) που αποκαλείται με το ψευδώνυμο Satoshi Nakamoto. Υλοποίησε ένα αποκεντρωμένο σύστημα ηλεκτρονικού νομίσματος βασισμένο στις Peer-to-Peer επικοινωνίες [8] [9]. Η υποκείμενη τεχνολογία με την οποία λειτουργεί το Bitcoin ονομάστηκε Blockchain. Η καινοτομία που παρείχε ο Satoshi είναι η ιδέα του να συνδυάσει ένα αποκεντρωμένο πρωτόκολλο συναίνεσης βασισμένο σε κόμβους που συλλέγουν συναλλαγές σε μπλοκ κάθε δέκα λεπτά. Έτσι δημιουργείται μια αυξανόμενη αλυσίδα από μπλοκ όπου με τον μηχανισμό απόδειξης της εργασίας οι κόμβοι κερδίζουν το δικαίωμα να συμμετέχουν στο δίκτυο. Ταυτόχρονα οι κόμβοι με μεγάλη υπολογιστική ισχύ έχουν αναλογικά μεγαλύτερη επιρροή. Με αυτό τον τρόπο επιτυγχάνεται η αξιόπιστη και η σωστή λειτουργία του αποκεντρωμένου νομίσματος, χωρίς κάποιο διαχειριστή ή μεσάζοντες, όπως κάποια κεντρική τράπεζα.

Το Ethereum είναι μια ανοιχτή πλατφόρμα blockchain η οποία δίνει τη δυνατότητα να δημιουργούνται, να εκτελούνται και να χρησιμοποιούνται αποκεντρωμένες εφαρμογές (DApps) και έξυπνα συμβόλαια (smart contracts) Χαρακτηριστική είναι η διευκόλυνση και η αυτοματοποίηση που προσφέρει στην αλληλεπίδραση μεταξύ των συμμετεχόντων του δικτύου. Όπως και με το Bitcoin, το Ethereum επιτρέπει τη δημιουργία ενός συστήματος πληρωμών χωρίς μεσάζοντες. Το ether (ETH) είναι το νόμισμα της πλατφόρμας και λειτουργεί επίσης ως αντίτιμο για τις εξορύξεις στο δίκτυο Ethereum. Για την κατασκευή των αποκεντρωμένων εφαρμογών, η πλατφόρμα προσφέρει μια ειδική γλώσσα προγραμματισμού turing-complete. Στη συνέχεια αυτή μεταφράζεται και τρέχει σε εικονικό σύστημα του (Ethereum Virtual Machine). Τεχνικά, λόγω του turing-complete συστήματος, το μεγάλο πλεονέκτημα είναι πως οι εφαρμογές και τα έξυπνα συμβόλαια που υποστηρίζει η πλατφόρμα

μπορούν να γραφτούν σε μια πληθώρα από σύγχρονες και παλιές γλώσσες προγραμματισμού, όπως C++, Python, Ruby, Go, Java, JavaScript, Rust κ.α..

2.8. Hyperledger project

Το Hyperledger Project ξεκίνησε το 2015 από το Linux Foundation. Είναι ένα σύνολο από blockchains και εργαλεία πάνω σε αυτό (βλ. Εικόνα 5) που έχουν ως στόχο να δημιουργήσουν σε επιχειρηματικό επίπεδο μια δομή ανοιχτού κώδικα για κατανεμημένα καθολικά (Distributed Ledger) (Cachin, 2016). Μέλη και υποστηρικτές σε αυτό το εγχείρημα είναι μεγάλες εταιρείες του κλάδου όπως η IBM, η Intel, η Cisco και η SAP.

Εικόνα 3 Blockchain frameworks και εργαλεία Hyperledger

Το Hyperledger Fabric είναι μια υλοποίηση πλατφόρμας κατανεμημένου καθολικού όπου τρέχει έξυπνα συμβόλαια, αξιοποιεί αποδεδειγμένες τεχνολογίες και έχει μια αρχιτεκτονική που επιτρέπει να «κουμπώνουν» και να υλοποιούνται διάφορες άλλες λειτουργίες. Γι' αυτό το λόγο είναι ευέλικτο για μια πληθώρα χρήσεων blockchain (Gaur, et al., 2018). Επίσης επιτρέπει την δημιουργία ξεχωριστών επιπέδων ασφαλείας και αδειοδοτεί μόνο πιστοποιημένους χρήστες. Λόγω της κρυπτογράφησης των συναλλαγών και σε συνδυασμό με τα προηγούμενα είναι ιδανικό για επιχειρηματικά περιβάλλοντα μιας και πετυχαίνει την εμπιστευτικότητα των συναλλαγών και

την επιλεκτική πρόσβαση μεταξύ των συμμετεχόντων. Για παράδειγμα σε μια υλοποίηση για βιομηχανίες αυτοκινήτων, οι διαφορετικές βιομηχανίες δεν θα έχουν πρόσβαση σε ανταγωνιστικές πληροφορίες. Αλλά μόνο σε αυτές που έχουν διαμοιράσει σε αυτούς που πρέπει και αμφίδρομα. Έτσι επιτυγχάνεται η εμπιστοσύνη των συμμετεχόντων στο διαμοιρασμό της πληροφορίας, σε συνδυασμό με όλα τα οφέλη του blockchain. Το Hyperledger Fabric βασίζεται στον αλγόριθμο συναίνεσης BTF (Byzantine Fault Tolerant) σε αντίθεση με το PoW του Bitcoin (Rilee, 2018). Η υπηρεσία εντολών (orderer) του Hyperledger πρέπει να ελέγχεται από κοινού, από τα μέλη του δικτύου, χρησιμοποιώντας έναν αλγόριθμο BFT που αντιστέκεται σε κακόβουλες δραστηριότητες (Gaur, et al., 2018).

2.9. Permissioned και Permissionless Blockchains

Το εξουσιοδοτημένο Blockchain διατηρεί και αυτό ένα κατανεμημένο βιβλιάριο δεδομένων, όμως η συμμετοχή σε αυτό ελέγχεται από μια κεντρική αρχή. Η κεντρική αυτή αρχή γνωρίζει τους συμμετέχοντες και δίνει το δικαίωμα επικύρωσης των συναλλαγών σε έμπιστα προς αυτούς άτομα. Αυτό το χαρακτηριστικό διευκολύνει την αύξηση του όγκου των συναλλαγών που πραγματοποιούνται ημερησίως και ταυτόχρονα τα εξουσιοδοτημένα δίκτυα μπορούν να είναι πολύ γρήγορα με μεγαλύτερη αποθηκευτική χωρητικότητα. Επίσης ο βασικός κώδικας του κάθε εξουσιοδοτημένου Blockchain μπορεί να εκδίδεται ανοιχτά προς όλους για να τον επιθεωρήσουν ή και όχι (Laurence, 2017 , Gupta, 2017 , Tapscott & Tapscott, 2016)

Όπως φαίνεται στις προηγούμενες ενότητες, υπάρχουν πολλές υλοποιήσεις blockchain. Αυτές μπορούν να κατηγοριοποιηθούν σε δύο μεγάλα σύνολα, τα δημόσια blockchains χωρίς δικαιώματα και τα ιδιωτικά ή επιχειρηματικά blockchains με δικαιώματα (Bauerle, 2017). Στα δημόσια οποιοσδήποτε ενδιαφερόμενος μπορεί να συμμετάσχει στο δίκτυο. Η πρόσβαση είναι ανοιχτή στα δεδομένα τους διαβάζοντας την αλυσίδα και επαληθεύοντας τα

μπλοκ δημιουργώντας διαφάνεια στην πληροφορία. Η επαλήθευση των μπλοκ γίνεται από τους εξορυκτές (miners) και υπάρχει η δυνατότητα να εξορύξουν όλοι αναζητώντας την ανταμοιβή τους. Έτσι επιτυγχάνεται η ασφαλής αποκέντρωση του συστήματος μιας και δεν χρειάζεται τα μέλη να εμπιστεύονται το ένα τον άλλο. Από την άλλη πλευρά ένα πρόβλημα για τις επιχειρήσεις προέκυψε λόγω του δημόσιου blockchains, οι συναλλαγές είναι εντελώς διαφανείς για όλους. Αυτό εξαλείφει την ανταγωνιστικότητα των επιχειρήσεων, επειδή δεν θέλουν να παρουσιάζουν όλες τις πληροφορίες τους (Terzi & Stamelos, 2018). Υπάρχουν πολλές περιπτώσεις εφαρμογών όπου οι συναλλαγές ή τα περιουσιακά στοιχεία δεν πρέπει να κοινοποιούνται ή να είναι προσβάσιμα από όλους, αλλά από επιλεγμένους συμμετέχοντες, π.χ. συναλλαγές ανταγωνιστών, ιατρικό ιστορικό και μεταφορά αγαθών. Γι' αυτό το λόγο δημιουργήθηκαν τα ιδιωτικά blockchains. Είναι χρήσιμα σε περιπτώσεις όπου η ακεραιότητα του ίχνους δεν είναι το πιο σημαντικό και υπάρχει η ανάγκη να τυποποιηθεί η ανταλλαγή πληροφοριών με ασφαλή τρόπο μεταξύ εταίρων, όπως ανάμεσα στις βιομηχανίες.

Στον παρακάτω πίνακα (βλ. Πίνακας 1) (International Bank for Reconstruction and Development, 2017) παρατηρείται συνοπτικά η σύγκριση των κύριων χαρακτηριστικών ανάμεσα στα Blockchains με δικαιώματα και χωρίς. Ενώ παρακάτω (βλ. Πίνακας 2) συγκρίνονται τα βασικά χαρακτηριστικά από τρία μεγάλα blockchains, το Bitcoin, το Ethereum και το Hyperledger Fabric.

Πίνακας 1 Σύγκριση χαρακτηριστικών Permissioned με Permissionless Blockchains ***(International Bank for Reconstruction and Development, 2017)***

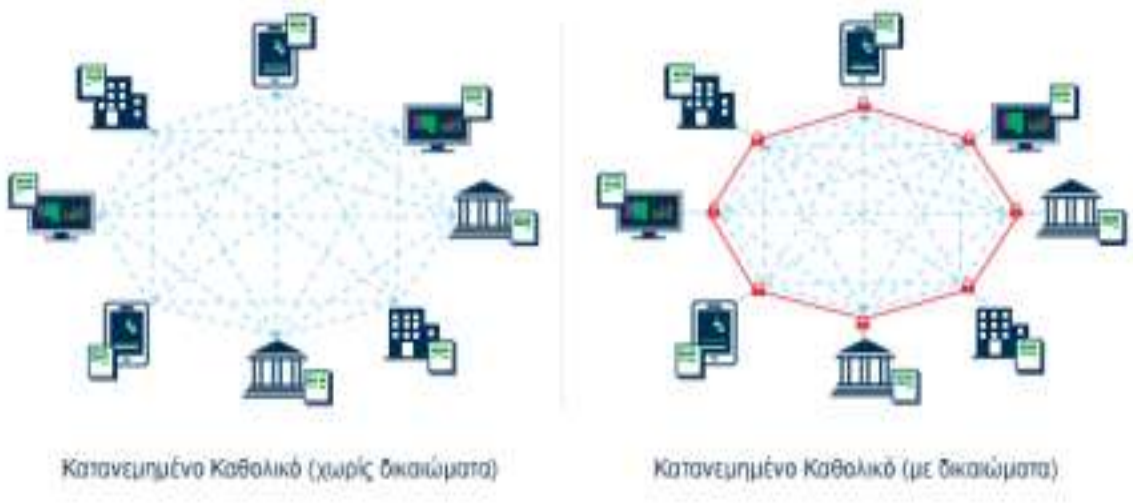
	Blockchains χωρίς δικαιώματα	**Blockchain με δικαιώματα**
Κεντρικό μέρος	Χωρίς κεντρικό ιδιοκτήτη ή διαχειριστή	Υπάρχει σε κάποιο βαθμό εξωτερικός διαχειριστής/ές ή έλεγχος
Πρόσβαση	Μπορεί οποιοσδήποτε να συμμετάσχει	Μόνο επιλεγμένοι συμμετέχοντες έχουν πρόσβαση στο δίκτυο
Επίπεδο εμπιστοσύνης	Δεν χρειάζεται τα μέλη του δικτύου να έχουν εμπιστοσύνη μεταξύ τους	Υψηλός βαθμός εμπιστοσύνης μεταξύ των μελών
Ανοιχτό	Το καθολικό είναι ανοιχτό και διαφανές αφου διαμοιράζεται μεταξύ όλων των συμμετεχόντων	Δυνατότητα σε διαφορετικό βαθμό ανοιχτού και διαφανές δικτύου
Ασφάλεια	Διαμέσου ευρείας κατανομής	Έλεγχος πρόσβασης σε συνδυασμό με τεχνολογία κατανεμημένου καθολικού
Ταχύτητα	Αργή επεξεργασία συναλλαγών	Γρήγορη επεξεργασία συναλλαγών
Ταυτότητα	Κυρίος ανώνυμα ή ψευδοανώνυμα	Ταυτότητα μέσω ιδιοκτήτη ή διαχειριστή
Συναίνεση (Consensus)	Δυσκολίας Proof-of-Work (συνήθως)	Διάφοροι αλγόριθμοι π.χ. PBFT, Kafka (τυπικά πιο εύκολοι από τον PoW)
Περιουσιακό στοιχείο	Συνήθως η φύση τους είναι κρυπτονομίσματα αλλά υπάρχει η δυνατότητα μέσω tokens να αντιπροσωπευθεί οποιοδήποτε περιουσιακό στοιχείο	Οποιοδήποτε περιουσιακό στοιχείο
Ιδιοκτησία	Υπάρχουν νομικά θέματα σχετικά με την ιδιοκτησία διότι κανένα νομικό πρόσωπο δεν ελέγχει ή κατέχει το καθολικό	Υπάρχει μεγαλύτερη νομική σαφήνεια ως προς την ιδιοκτησία. Συνήθως είναι ο ιδιοκτήτης ή ο διαχειριστής
Παραδείγματα	Bitcoin, Ethereum	Hyperledger Fabric

Πίνακας 2 Σύγκριση χαρακτηριστικών Bitcoin, Ethereum και Hyperledger ***(Friebe, 2017)***

Σύγκριση χαρακτηριστικών			
Χαρακτηριστικά	**Bitcoin**	**Ethereum**	**Hyperledger Fabric**
Πρόσβαση	Permissionless	Permissionless	Permissioned
Ιδιωτικότητα δεδομένων	Δημόσια	Δημόσια ή Ιδιωτικά	Ιδιωτικά
Συναίνεση	Proof-of-Work	Proof-of-Work	PBFT
Επεκτασιμότητα	Υψηλή κόμβου Χαμηλή απόδοσης	Υψηλή κόμβου Χαμηλή απόδοσης	Χαμηλή κόμβου Υψηλή απόδοσης
Κεντρικός έλεγχος	Χαμηλός, αποκεντρωμένες αποφάσεις που λαμβάνονται από την κοινότητα/miners	Μέτριος, κύρια ομάδα ανάπτυξης αλλά και EIP διαδικασία	Χαμηλός, ανοιχτής διακυβέρνησης μοντέλο βασισμένο στο μοντέλο Linux
Ανωνυμία	Ψευδοανωνυμία, χωρίς κρυπτογράφηση	Ψευδοανωνυμία, χωρίς κρυπτογράφηση	Όχι, με κρυπτογράφηση
Νόμισμα	Ναι, το bitcoin	Ναι, το ether	Όχι
Κόστος συναλλαγής	Ναι	Ναι	Όχι
Ψευδογλώσσα	Περιορισμένη δυνατότητα, stack-based	Υψηλή δυνατότητα, turing-complete, υψηλού επιπέδου	Υψηλή δυνατότητα, turing-complete, υψηλού επιπέδου

2.10. Κατανεμημένο καθολικό (Distributed Ledger)

Η τεχνολογία του κατανεμημένου καθολικού (distributed ledger technology ή DLT) είναι μια νέα τεχνολογία στα πρώτα στάδια ανάπτυξής της. Είναι ένας τύπος βάσης δεδομένων που έχει την ιδιότητα να αναπαράγει, να διαμοιράζεται και να συγχρονίζει τα δεδομένα του σε πολλαπλά σημεία, κόμβων και συσκευών (UK Office for Science, 2016). Χαρακτηριστικό του κατανεμημένου καθολικού είναι ότι δεν υπάρχει κεντρικός διαχειριστής ή κεντρική αποθήκευση δεδομένων. Μόλις υπάρξει η συναίνεση, το κατανεμημένο καθολικό ενημερώνεται και όλοι οι κόμβοι διατηρούν το δικό τους όμοιο αντίγραφο του (Bauerle, 2017).



Εικόνα 4 Κατανεμημένο καθολικό (International Bank for Reconstruction and Development, 2017)

Με το blockchain η τεχνολογία αυτή έκανε την πιο σημαντική της παρουσία εφόσον ανέδειξε τις δυνατότητες της. Υπάρχουν δημόσια και ιδιωτικά κατανεμημένα καθολικά (βλ. Εικόνα 6). Στα δημόσια ο κάθε κόμβος κατέχει ένα ολόκληρο αντίγραφο του καθολικού. Στα ιδιωτικά ο κάθε κόμβος έχει δικαιώματα, μέσα από τον έλεγχο πρόσβασης μπορεί να συνδεθεί στο δίκτυο και να κάνει αλλαγές στο καθολικό (International Bank for Reconstruction and Development, 2017).

3. ***Έξυπνα συμβόλαια***

Ένα συμβόλαιο με την παραδοσιακή του έννοια, είναι μια γραπτή συμφωνία με την οποία τα συμβαλλόμενα μέρη αναλαμβάνουν συγκεκριμένες δεσμεύσεις το ένα απέναντι στο άλλο. Κάθε συμβαλλόμενο μέρος πρέπει να εμπιστεύεται το άλλο μέρος ότι θα εκπληρώσει τις υποχρεώσεις του συμβολαίου. Τα έξυπνα συμβόλαια διαθέτουν το ίδιο είδος συμφωνίας, αλλά καταργούν την ανάγκη για εμπιστοσύνη μεταξύ των διαφόρων μερών. Αυτό οφείλεται στο γεγονός ότι ένα έξυπνο συμβόλαιο είναι ένα κομμάτι κώδικα που αποθηκεύεται σε ηλεκτρονικό υπολογιστή χωρίς να μπορεί κάποιος να το παραβιάσει και είναι σε θέση να εκτελέσει ή να επιβάλει μια προκαθορισμένη συμφωνία χρησιμοποιώντας ένα δίκτυο Blockchain, όταν και αν πληρούνται συγκεκριμένες προϋποθέσεις. Δηλαδή ο κώδικας περιέχει τη συμφωνία μεταξύ των διαφόρων μερών και καταργεί την ανάγκη εμπιστοσύνης, αφού κανείς δεν θα μπορεί να αλλάξει ή τροποποιήσει την συμφωνία και θα εκτελεστεί όταν θα πληρούνται οι προϋποθέσεις που έχουν συμφωνήσει.

Ένα έξυπνο συμβόλαιο χαρακτηρίζεται από τρία βασικά στοιχεία: την αυτονομία, την αυτάρκεια και την αποκέντρωση. Αυτονομία σημαίνει ότι μετά τη δρομολόγησή και τη λειτουργία του, το συμβόλαιο και τα συμβαλλόμενα μέρη δεν χρειάζεται να βρίσκονται σε περαιτέρω επαφή. Ο όρος αυτάρκεια αναφέρεται, με τη σειρά του, στη δυνατότητα των έξυπνων συμβολαίων να είναι αυτάρκη, να είναι δηλαδή ικανά να εκτελούν τις εσωτερικές τους λειτουργίες ανάλογα με τους πόρους που διαθέτουν. Τέλος, τα έξυπνα συμβόλαια είναι αποκεντρωμένα, δεδομένου ότι δεν έχουν έναν κεντρικό εξυπηρετητή αλλά εκτελούνται σε διάφορους κόμβους του Blockchain δικτύου.

Κύριος στόχος του έξυπνου συμβολαίου σε ένα Blockchain δίκτυο, είναι να επιτρέψει σε δύο ή περισσότερα μέρη να πραγματοποιήσουν μια αξιόπιστη συναλλαγή χωρίς να έχουν ανάγκη από μεσάζοντες. Το συμβόλαιο ενεργοποιείται αυτόματα όταν πληροί κάποιες προϋποθέσεις που έχουν

προσυμφωνεί από τα εμπλεκόμενα μέρη. Ένα παράδειγμα θα μπορούσε να ήταν: μόλις ένας άνθρωπος γίνει 18 ετών θα μεταφερθεί στο λογαριασμό του ένα ποσό που έχει συμφωνηθεί προηγουμένως στο συμβόλαιο. Όταν τα συμβόλαια ενεργοποιηθούν δεν μπορεί να διακοπεί η λειτουργία τους από τρίτα άτομα ούτε να αλλάξει η εκάστοτε συμφωνία. Τέλος ένα μικρό λάθος στον κώδικα μπορεί να έχει ως αποτέλεσμα την απώλεια των κρυπτονομισμάτων του έξυπνου συμβολαίου (Melanie Swan, 2015).

Ο όρος των έξυπνων συμβολαίων (smart contracts) χρησιμοποιήθηκε αρχικά από τον Αμερικάνο επιστήμονα πληροφορικής και κρυπτογράφο Nick Szabo (Szabo, 1997). Χαρακτηριστικά αναφέρει το παράδειγμα της ενοικίασης ενός αυτοκινήτου με έξυπνο συμβόλαιο έτσι ώστε να αποτραπεί η κλοπή του αν δεν ικανοποιηθεί το πρωτόκολλο παράδοσης (Szabo, 1996). 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 επισωρεύοντας 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. Το 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.

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 μετά την εισαγωγή της καθώς εντοπίστηκαν ευπάθειες όταν εκτελούνταν ορισμένες λειτουργίες. Το Ethereum επέκτεινε αυτή 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 μεταγλωτίζονται σε ψηφιακό κώδικα Ethereum Virtual Machine (EVM). Η λογική του συμβόλαιο και ο κώδικας διαμοιράζεται στο δίκτυο ούτος ώστε να χρησιμοποιηθεί από τους συμμετέχοντες για να επικυρώσουν και να επεξεργαστούν τις συναλλαγές. Το αποτέλεσμα της εσωτερικής κατάστασης του συμβολαίου γράφεται κατανεμημένα.

Εικόνα 5 Διάρκεια ζωής του οχήματος μέσω Smart Contracts σε blockchain. Παραγωγός-ΠελάτηςΑπόσυρση.

Σε σύγχρονες εφαρμογές blockchain για επιχειρήσεις αξιοποιείται μια ακόμα υλοποίηση από έξυπνα συμβόλαια, αυτά του Hyperledger Fabric. Έχει αναπτυχθεί ο chaincode που είναι ο κώδικας στον οποίο γράφονται τα έξυπνα συμβόλαια. Περιλαμβάνει την ερμηνεία αυτών σε λογική μεθόδων και αλγορίθμων μαζί με επιπρόσθετες λειτουργίες (Hyperledger Fabric Docs, 2018). Με συγκεκριμένες ρυθμίσεις στην πολιτική ορίζεται ποιοι ακριβώς κόμβοι ή χρήστες, ή πόσοι από αυτούς θα εκτελέσουν ένα smart contract.

Επομένως η κάθε συναλλαγή εκτελείται μόνο από ένα υποσύνολο κόμβων. Αυτό επιτρέπει παράλληλες εκτελέσεις, αυξάνοντας τη συνολική απόδοση και την κλίμακα του συστήματος. Η γλώσσα προγραμματισμού που μπορούν να συνταχθούν είναι είτε Go είτε Node.js. Παράλληλα υπάρχει η δυνατότητα ανάπτυξης εφαρμογών blockchain στο Hyperledger Composer όπου για την δημιουργία έξυπνων συμβολαίων χρησιμοποιείτε διερμηνέας σε γλώσσα

JavaScript που εκτελεί τη λογική για την επεξεργασία της συναλλαγής σε chaincode του HyperLedger Fabric (IBM, 2018). Στην Εικόνα 5 παρατηρείται ένα χαρακτηριστικό παράδειγμα της IBM (IBM, 2017) σχετικά με τον κύκλο ζωής των οχημάτων.

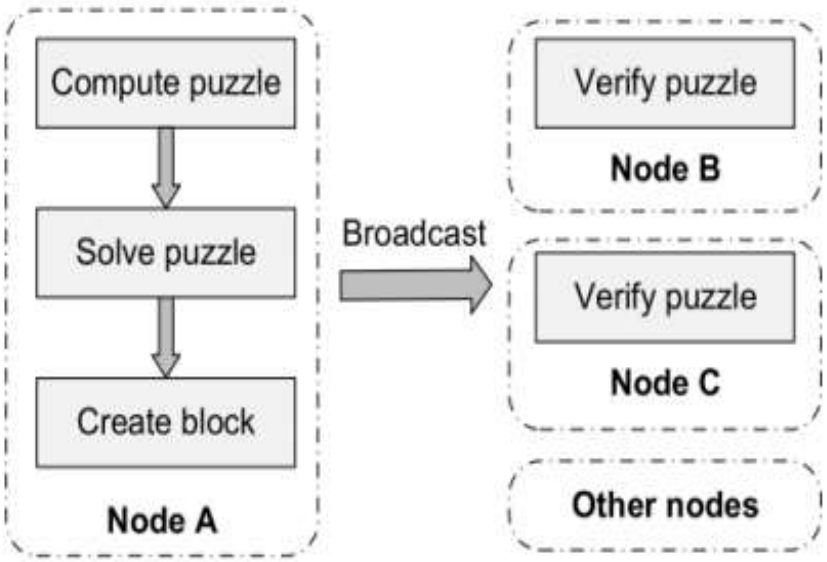
Πολλά μέρη εμπλέκονται στον κύκλο ζωής ενός οχήματος, συμπεριλαμβανομένου του κατασκευαστή, των αντιπροσώπων αυτοκινήτων, της ρυθμιστικής αρχής των οχημάτων, των ασφαλιστικών εταιρειών, των ιδιοκτητών και των αντιπροσώπων των απορριμμάτων. Όλα τα μέρη στο επιχειρηματικό δίκτυο επωφελούνται από την ύπαρξη αξιόπιστης, κατανεμημένης πηγής αλήθειας για την ιστορία και την ιδιοκτησία ενός οχήματος. Με την ενσωμάτωση της λογικής επιχειρηματικών αποφάσεων σε έξυπνες συμβάσεις που τρέχουν στο blockchain διαφαίνεται η αξία και η διαφάνεια μιας τέτοιας υλοποίησης.

3.1. Συναίνεση

Ως συναίνεση στην τεχνολογία αυτή ορίζεται η διαδικασία κατά την οποία επικυρώνεται η αξιοπιστία των συναλλαγών σε ολόκληρο το δίκτυο και η απόρριψη των ελαττωματικών διαδικασιών. Υπάρχουν πολλοί αλγόριθμοι συναινέσεις με διαφορετικά χαρακτηριστικά αλλά εξυπηρετώντας τον ίδιο σκοπό. Σε ένα ανοιχτό blockchain, όπως το bitcoin χρειάζεται μεγάλη επεξεργαστική ισχύ για τον PoW. Οι εξορυκτές (miners) ανταγωνίζονται μεταξύ τους για να ολοκληρώσουν τις συναλλαγές στο δίκτυο και να ανταμειφθούν (βλ. Εικόνα 6) (Li, et al., 2017).

Δείχνοντας μεγαλύτερη εμπιστοσύνη για τις επικυρώσεις των συναλλαγών, π.χ. το παγκόσμιο σύστημα χρηματοπιστωτικών συναλλαγών Ripple, επιλέγει μια λίστα επικυρωτών (validators) γνωστών ή μερικώς γνωστών. Κάθε λίγα δευτερόλεπτα εφαρμόζεται ο αλγόριθμος RPCA (Ripple Consensus Algorithm) από όλους τους κόμβους. Είναι βασισμένος στην έννοια του proof of correctness και είναι βελτιστοποιημένος και ταχύτερος από αυτόν του PoW

(Schwartz, et al., 2014).



Εικόνα 6 Μηχανισμός συναίνεσης PoW (Li, et al., 2017)

Ένα ακόμη διαδεδομένο μοντέλο κατανεμημένης συναίνεσης είναι το Proof-of-Stake, στο οποίο επιλέγεται ο δημιουργός του επόμενου μπλοκ βάση συνδυασμών τυχαίας επιλογής π.χ. πλούτου, ηλικίας. Αυτό είναι το ποντάρισμα (stake) για την επικύρωση του μπλοκ. Τέλος ακόμα ένας ευρέως διαδεδομένος αλγόριθμος είναι ο Byzantine Fault Tolerance (BFT) που εγγυάται την κάλυψη ή την ικανότητα να επιτύχει συναίνεση, ακόμα και αν υπάρχουν αντίπαλοι κόμβοι (κακόβουλοι) ή αν οι κόμβοι βρεθούν εκτός δικτύου. Δεν χρειάζεται εξορυκτές και βρίσκει μεγάλη εφαρμογή σε ιδιωτικά blockchain όπως το Hyperledger Fabric.

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

3.1.1. Proof of Work

Ο αλγόριθμος Proof-of-Work (PoW) έχει ως κύριο στόχο να διασφαλίσει την διαδικασία επικύρωσης των δεδομένων και την αποτροπή επιθέσεων στο δίκτυο. Η ιδέα του αλγορίθμου αυτού υπήρχε και πριν από το Bitcoin, αλλά ο Satoshi Nakamoto εφάρμοσε για πρώτη φορά αυτήν την τεχνική στο ψηφιακό νόμισμά bitcoin. Στην πραγματικότητα, η ιδέα του αλγορίθμου PoW δημοσιεύθηκε αρχικά από τους Cynthia Dwork και Moni Naor το 1992 με τίτλο "Pricing via Processing or Combatting Junk Mail". Αργότερα μια παρόμοια πρόταση που ονομάζεται Hashcash προτάθηκε το 1997 από τον Adam Back αλλά ο όρος "Proof-of-Work" δημιουργήθηκε από τους Markus Jakobsson και Ari Juels σε έγγραφο με ονομασία «Proofs of Work and Bread Pudding Protocols (Extended Abstract)» που δημοσιεύθηκε το 1999. Ο αλγόριθμος αυτός είναι ο πιο ευρέως χρησιμοποιούμενος αλγόριθμος στην τεχνολογία Blockchain.

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

Το πρωτόκολλο του Bitcoin θέτει αυτόματα ένα στόχο (Difficulty target). Ο στόχος είναι το επίπεδο δυσκολίας που χρειάζεται ένας κόμβος για να επικυρώσει το μπλοκ. Όλοι οι κόμβοι στο δίκτυο συναγωνίζονται για το ποιος

θα βρει πρώτος ένα αλφαριθμητικό Hash μικρότερο του στόχου. Το μόνο που μπορούν να κάνουν είναι κάθε φορά να αλλάζουν την τιμή του «nonce» και να τοποθετούνε το «Block + (καινούργιο)nonce» στον αλγόριθμο κρυπτογράφησης SHA256. Η διαδικασία της αλλαγής του «nonce» γίνεται αυτόματα και ο πρώτος κόμβος που θα βρει το σωστό αποτέλεσμα έχει επίσημα επικυρώσει τις συναλλαγές στο μπλοκ και κερδίζει ένα ποσό bitcoins. Τότε αποστέλλεται σε όλους τους υπόλοιπους κόμβους το «Block+ nonce + Hash» και αφού πιστοποιήσουν οι υπόλοιποι κόμβοι ότι είναι σωστή η λύση, τότε προσκολλάτε στην αλυσίδα του Blockchain. Μόλις ολοκληρωθεί η διαδικασία αυτή η οποία διαρκεί περίπου 10 λεπτά, οι κόμβοι αμέσως μαζεύουνε τις καινούργιες συναλλαγές και συναγωνίζονται πάλι για να βρούνε το σωστό «nonce» (Antonopoulos, 2017 , Vincenzo Morabito).

3.1.2. Proof of Stake

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

Σε αντίθεση με το Proof-of-Work όπου επικυρώνει τις συναλλαγές ο γρηγορότερος κόμβος, στο Proof-of-Stake, ο κόμβος που θα επικυρώσει τις συναλλαγές επιλέγεται με ντετερμινιστικό τρόπο. Οι κόμβοι δηλαδή, καταθέτουν στο δίκτυο ένα ποσό από τα κρυπτονομίσματα τους ως εγγύησή ότι θα επικυρώσουν τις συναλλαγές σε ένα μπλοκ. Το ποιος κόμβος τελικά θα επιλεγεί, καθορίζεται από το ποσό που έχει καταθέσει. Για παράδειγμα, εάν η Μαρία καταθέσει 60 κρυπτονομίσματα, η Άννα 30 και η Κατερίνα 10, η Μαρία έχει 60% πιθανότητα να επικυρώσει το μπλοκ, η Άννα έχει 30% και η Κατερίνα

10%. Έτσι στο PoS εμπιστευόμαστε την αλυσίδα με την υψηλότερη εγγύηση. Επίσης δεν υπάρχει ανταμοιβή για την επικύρωση του κάθε μπλοκ, όμως ο κόμβος που θα επικυρώσει το μπλοκ λαμβάνει ένα ποσό από την κάθε συναλλαγή (Ethan Buchman, 2016).

3.1.3. Practical Byzantine Fault Tolerance

Το 1999, οι Miguel Castro και Barbara Liskov εισήγαγαν τον αλγόριθμο "Practical Byzantine Fault Tolerance" (PBFT), που αποτέλεσε την πρώτη πρακτική λύση απέναντι στο πρόβλημα των Βυζαντινών Στρατηγών, η οποία έγινε αποδεκτή από όλους. Θα πρέπει να διευκρινιστεί στο σημείο αυτό ότι το πρόβλημα των Βυζαντινών Στρατηγών παρουσιάζεται όταν διαφορετικοί κόμβοι σε ένα αναξιόπιστο δίκτυο πρέπει να καταλήξουν σε μια τελική απόφαση, ελέγχοντας τα δεδομένα που ανταλλάζονται. Παράλληλα ο αλγόριθμος «PBFT» θεωρήθηκε ως ο πρώτος πρακτικός αλγόριθμος που είναι κατάλληλος για χρήση σε ασύγχρονα δίκτυα.

Ο συγκεκριμένος αλγόριθμος χρησιμοποιείται από εξουσιοδοτημένα Blockchain δίκτυα όπως το Hyperledger Fabric, Ripple, Stellar και απαιτεί ο κάθε κόμβος να είναι γνωστός στο δίκτυο. Κάθε φορά που πραγματοποιείται μια συναλλαγή, επικυρώνεται μέσω μιας συγκεκριμένης διαδικασίας. Πιο αναλυτικά, σε κάθε φάση της διαδικασίας, επιλέγεται με βάση ορισμένους κανόνες ένας κύριος εισηγητής κόμβος, ο οποίος είναι υπεύθυνος να εξετάσει αν τα δεδομένα είναι σωστά. Αφού εξετάσει τα δεδομένα στέλνει τα αποτελέσματα σε όλους τους υπόλοιπους κόμβους του δικτύου. Ο εισηγητής θα περάσει στην επόμενη φάση εξέτασης των δεδομένων, αν τα 2/3 όλων των κόμβων έχουν ψηφίσει ότι συμφωνούν μαζί του. Αν οι ψήφοι είναι λιγότεροι, τότε εκλέγεται ένας καινούργιος εισηγητής. Η διαδικασία ολοκληρώνεται σε 3 φάσεις, όπου κάθε φάση ακολουθείται η ίδια διαδικασία (Ethan Buchman, 2016)

4. ***Εφαρμογές blockchain στην εφοδιαστική αλυσίδα σήμερα***

Ο Christian Catalini, κύριος ερευνητής του MIT στον τομέα Digital Currencies Research Study, αναφέρει πως η τεχνολογία του blockchain έχει τη δυνατότητα να εξορθολογήσει και να απλοποιήσει την αλυσίδα εφοδιασμού, ιδίως στις περιπτώσεις όπου εμπλέκονται πολλές οντότητες, οι συμμετέχοντες είναι διασκορπισμένοι γεωγραφικά και υπάρχει συνολική πολυπλοκότητα (Catalini & Gans, 2017) (Church, 2017). Σε αυτή τη βιομηχανία παρατηρούνται σήμερα αρκετές υλοποιήσεις που στοχεύουν να λύσουν χρόνια προβλήματα.

Η πιο μεγάλη και γνωστή περίπτωση είναι η συνεργασία της IBM με την Walmart για την υλοποίησης του έργου «Food Safety». Τον Οκτώβριο του 2016 ξεκινάει η πιλοτική έρευνα της ιχνηλασιμότητας προϊόντων μέσω του blockchain (Kamath, 2018). Στόχος ήταν η επένδυση $24 εκατομμυρίων σε βάθος πέντε ετών για να ερευνηθεί η παγκόσμια ασφάλεια τροφίμων. Χρησιμοποιώντας την πλατφόρμα της IBM, το Hyperledger Fabric, ολοκλήρωσε με επιτυχία δύο πιλοτικά. Το χοιρινό κρέας στην Κίνα και τα μάνγκο στην Αμερική. Με έναν προσανατολισμό από την φάρμα στο τραπέζι πέτυχε την μείωση της ιχνηλασιμότητας σε όλο το εύρος της εφοδιαστικής αλυσίδας από επτά μέρες σε 2,2 δευτερότατα. Ενώ παράλληλα προώθησε την διαφάνεια της διαδικασίας σε όλα τα επίπεδα. Τον Αύγουστο του 2017 προχώρησε στην ενσωμάτωση μεγάλων κολοσσών όπως Dole, Nestlé, Unilever, Driscoll's, Golden State Foods, Kroger, McLane Company, και Tyson Foods (IBM, 2017).

Η Αμερικάνικη εταιρία IBM, σε ακόμα μια επένδυση της στο blockchain, συνεργάστηκε με την Maersk από την Δανία για να υλοποιήσει το «TradeLens». Η λύση αυτή ψηφιοποιεί και διαχειρίζεται το ίχνος χαρτιού του μεταφέρουν εμπορευματοκιβώτια σε ολόκληρο τον πλανήτη. Η αποστολή μεταξύ ηπείρων απαιτεί γραμματόσημα και εγκρίσεις από περισσότερα των 30 ατόμων και οργανώσεων, όπως τελωνειακές αρχές, μεταφορείς,

πράκτορες, φορτωτές κ.λπ. Επιπροσθέτως περιλαμβάνει πάνω από 200 επικοινωνίες μεταξύ διαφορετικών συμμετεχόντων (IBM, 2017). Τα γεγονότα, τα έγγραφα και τα δεδομένα της εφοδιαστικής αλυσίδας ανταλλάσσονται σε πραγματικό χρόνο. Η ψηφιακή υποδομή συνδέει τους συμμετέχοντες σε ένα οικοσύστημα, ενσωματώνοντας τις διαδικασίες και τους εταίρους της ναυτιλίας και δημιουργεί ένα πλαίσιο αξιοπιστίας, αυξημένες διαφάνειας και εμπιστοσύνης.

Τον Φεβρουάριο του 2018 το EXIMCHAIN κάνει το ντεμπούτο του ως κρυπτονόμισμα και καταφέρνει να συγκεντρώσει $20 εκατομμύρια ως ICO (Initial Coin Offering) (ICODROPS, 2018). Η αρχική ιδέα και η ανάπτυξη του ξεκίνησε το 2015, ενώ το 2016 ιδρύεται η startup. Ο σκοπός του είναι να παρέχει χρηματοοικονομικές λύσεις στην εφοδιαστική αλυσίδα μέσω ενός υβριδικού δημόσιου και ιδιωτικού blockchain. Στοχεύει μικρομεσαίες επιχειρήσεις που δραστηριοποιούνται στις αγορές και στις προμήθειες. Η πλατφόρμα παρέχει εργαλεία βελτιστοποίησης που ταιριάζουν στις ανάγκες του κλάδου. Μέσω των έξυπνων συμβολαίων δίνει την δυνατότητα προσιτών πηγών κεφαλαίου για να αναπτύξουν των επιχειρήσεων και δίνουν στους χρηματοδότες ορατότητα στην ταμειακή ροή της αλυσίδας εφοδιασμού (Huertas, et al., 2018).

Το κρυπτονόμισμα Tael γνωστό και ως WABI δημιουργήθηκε από την Κινεζική εταιρεία Techrock. Λειτουργεί ως μέσο επιβράβευσης για τον καταναλωτή και παράλληλα επιβεβαιώνει την αυθεντικότητα των προϊόντων. Οι καταναλωτές μπορούν να ξοδέψουν τα κέρματα τους με αγορές ασφαλών προϊόντων της Techrock (Techrock, n.d.). Η γένεση του συστήματος αυτού απορρέει από το σκάνδαλο του κινέζικού γάλακτος το 2008. Το σκάνδαλο περιλάμβανε το γάλα και τη βρεφική φόρμουλα μαζί με άλλα υλικά και συστατικά τροφίμων που είχαν αλλοιωθεί με μελαμίνη. Αυτό είχε σαν αποτέλεσμα να νοσηλευτούν 50.000 βρέφη, εκ των οποίων 6 κατέληξαν (Wikipedia, 2008). Ο στόχος της ομάδας είναι να αποτρέψει τους καταναλωτές από θάνατο ή σοβαρή κακουχία εξαιτίας αυτών των παραποιημένων αγαθών.

Τον Νοέμβριο του 2016 ιδρύθηκε το Waltonchain (WaltonChain, 2018). Είναι Κινεζικών και Κορεατικών συμφερόντων. Στόχος είναι ο συνδυασμός hardware

και software με την χρήση RFIDs και Blockchain. Το όραμα τους είναι να υλοποιήσουν αυτό που αποκαλούν Value Internet of Things (VIoT). Με την τεχνολογία του blockchain θέλουν να φέρουν στην ανθρωπότητα μια αξιόπιστη ψηφιακή ζωή, να οικοδομήσουν το Internet of Everything (IoE) και μια υγιή ανάπτυξη ενός οικοσυστήματος. Τα τσιπ RFID, που έχουν σχεδιαστεί από τους κατασκευαστές Waltonchain, αποθηκεύουν πληροφορίες σχετικά με τα φυσικά στοιχεία των προϊόντων. Η ομάδα ανέπτυξε επίσης ένα σαρωτή που διαβάζει δεδομένα από τα τσιπ RFID και μεταφορτώνει δεδομένα απευθείας στο blockchain. Τα τσιπ RFID και οι σαρωτές είναι πατενταρισμένη τεχνολογία. Υπήρξε υλοποίηση στην εφοδιαστική αλυσίδα του ρούχου. Πετυχαίνοντας υψηλής ποιότητας σύστημα ιχνηλασιμότητας και ελέγχου αυθεντικότητας των ενδυμάτων, όπως επίσης μείωση της επικοινωνίας, της ανάλυσης και του κόστους αποθήκευσης των δεδομένων.

Όπως λοιπόν γίνεται σαφές, η τεχνολογία του blockchain δημιουργήθηκε αρχικά για την λειτουργία του κρυπτονομίσματος Bitcoin, όμως, συνεχώς εξελίσσεται και τώρα το πεδίο εφαρμογής του έχει γίνει πολύ πιο ευρύ. Πρόκειται για μία σειρά καταχωρίσεων που αφορούν συναλλαγές, σε ένα δημόσιο σημειωματάριο (ledger) λαμβάνοντας χώρα σε ένα δημόσιο ή ιδιωτικό peer-to-peer δίκτυο. Εκτός από την λειτουργία κρυπτονομισμάτων, μπορεί να αποτελέσει πυλώνα για την δημιουργία και την λειτουργία αποκεντρωμένων εφαρμογών, που βασίζονται σε ένα κατανεμημένο δίκτυο ομότιμων κόμβων και όχι στους εξυπηρετητές κάποιου οργανισμού. Το blockchain μπορεί να έχει τεράστια επιρροή σε αυτοματοποιήσεις διεργασιών ανάμεσα σε επιχειρήσεις όταν συνδυάζεται με καινοτόμες τεχνολογίες όπως η μηχανική μάθηση, η τεχνητή νοημοσύνη και το Internet of Things. Η χρήση του ενεργοποιεί στη βιομηχανία της εφοδιαστικής αλυσίδας την διαφάνεια, τον καλύτερο διαμοιρασμό πληροφορίας και ενισχύει την ασφάλεια των τροφίμων. Ένα από τα χαρακτηριστικά παράδειγμα της χρήσης αυτής, είναι η εφαρμογή της IBM Food Trust για την εφοδιαστική αλυσίδα φρέσκου τροφίμου.

Σύμφωνα με όλα τα προαναφερθέντα, παρατηρείται πως η ιχνηλασιμότητα και η πληροφόρηση στην εφοδιαστική αλυσίδα είναι αναγκαία και σημαντική.

Ωστόσο, τα περισσότερα από τα σημερινά συστήματα είναι κεντρικοποιημένα και δεν υπάρχουν αποκεντρωμένα συστήματα στην αλυσίδα εφοδιασμού γαλακτοκομικών προϊόντων για την ασφάλεια των τροφίμων. Σε αυτή τη διπλωματική, αναπτύσσεται μια αποκεντρομένη πλατφόρμα διαμοιρασμού, παρακολούθησης πληροφοριών και ιχνηλασιμότητας για την εφοδιαστική αλυσίδα γαλακτοκομικών βασισμένη στις τεχνολογίες του blockchain.

Συγκριτικά με τα κεντρικά συστήματα, το νέο σύστημα θα μπορούσε να γίνει μια καινοτόμα πλατφόρμα που θα παρέχει πληροφορία για το γάλα με αξιοπιστία, διαφάνεια και ασφάλεια, από τους συμμετέχοντες μέχρι και τον τελικό καταναλωτή. Το σύστημα αυτό μπορεί να δώσει μια νέα προοπτική και ιδέα για το πως μπορεί να διαμοιραστεί η πληροφορία και να βελτιώσει σημαντικά την ασφάλεια των τροφίμων στις αλυσίδες εφοδιασμού.

5. ***Τεχνολογικό πλαίσιο***

Οι περισσότερες από τις καθημερινές εργασίες γίνονται με τη βοήθεια κάποιας τεχνολογίας, με αποτέλεσμα να υπάρχει μεγαλύτερη πρόσβαση σε χρήσιμη πληροφορία, η οποία χρειάζεται επεξεργασία. Ένα από τα βασικά χαρακτηριστικά του διαδικτύου, το οποίο έχει για μεγάλο χρονικό διάστημα σταθερότητα, είναι η κεντρικοποιημένη αρχιτεκτονική στην αμφίδρομη σχέση πελάτη-εξυπηρετητή με την οποία είναι φτιαγμένη η πλειοψηφία των εφαρμογών και των υπηρεσιών. Αυτή λοιπόν τη σχέση προσπαθούν να την αλλάξουν ορισμένες νέες τεχνολογίες, πρωταγωνιστικό ρόλο παίζει το blockchain με τον αποκεντρωμένο χαρακτήρα του. Σε αυτό το κεφάλαιο θα αναλυθούν οι τεχνολογίες που επιλέχθηκαν για την υλοποίηση της πλατφόρμας που προτείνεται.

5.1. Blockchain Technologies

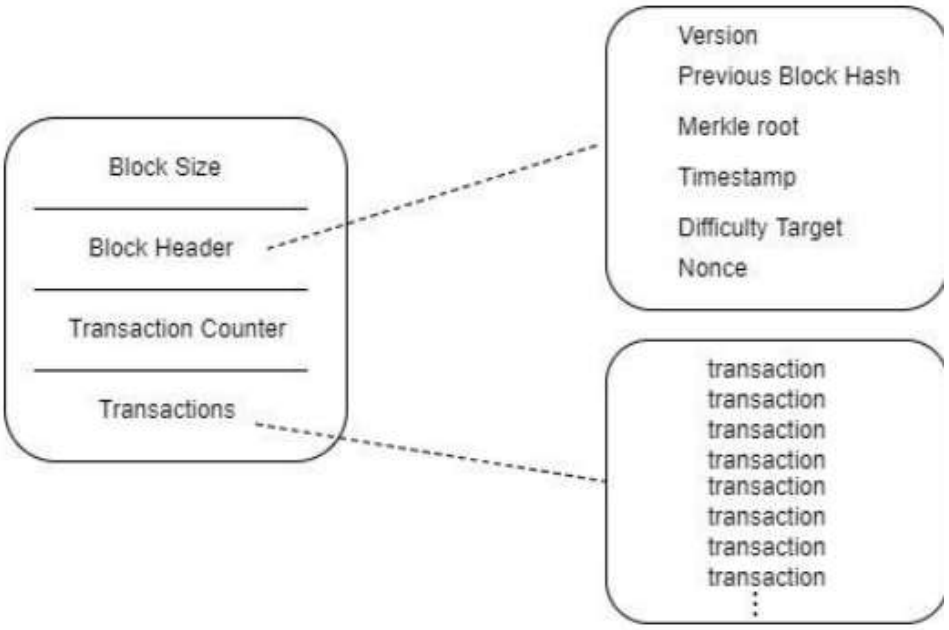
Μιλώντας γενικά, η εγκυρότητα των πληροφοριών βασίζεται στην εμπιστοσύνη της κεντρικοποιημένης μονάδας του συστήματος ή κάποιου τρίτου ισχυρού οργανισμού που την διαχειρίζεται. Ωστόσο, υπάρχει ασύμμετρη πληροφόρηση μεταξύ των οργανισμών και των συμμετεχόντων, η οποία και δημιουργεί μονοπώλιο στην κεντρικοποιημένη μονάδα. Αυτό έχει σαν αποτέλεσμα να γίνεται ευάλωτη και στόχος για hacking, δωροδοκία ή παραπληροφόρηση. Για παράδειγμα κάποιος διαχειριστής του κεντρικοποιημένου συστήματος μπορεί να δωροδοκηθεί για να αλλάξει έγκυρες πληροφορίες, με αποτέλεσμα να μετατρέψει σε αναξιόπιστο το σύστημα. Χάρη στο blockchain, αυτού του είδους τα προβλήματα μπορούν να επιλυθούν.

Το blockchain ουσιαστικά φαίνεται ως ένα τεχνικό σχήμα μιας αξιόπιστης βάσης δεδομένων, η οποία διατηρείται συλλογικά και αποκεντρωμένα με

αξιόπιστες μεθόδους. Η τεχνολογία του blockchain είναι παρόμοια με το NoSQL (Not Only Structured Query Language) (Meunier, 2016) και μπορεί να υλοποιηθεί με πολλά είδη γλωσσών προγραμματισμού όπως C++, Javascript, Python, Go, Solidity κ.α.. Η τεχνολογία του blockchain επιτρέπει την εμπιστοσύνη ακόμα και εκεί που δεν υπάρχει, την ασφάλεια και την ταυτοποίηση συστημάτων εφοδιαστικής αλυσίδας και ανταλλαγής αυτών. Λειτουργεί σε αποκεντρωμένο δίκτυο δίνοντας την δυνατότητα με τα έξυπνα συμβόλαια να αυτοματοποιούνται εκτελέσεις και επικυρώσεις διαδικασιών όταν συμβούν συγκεκριμένες συνθήκες.

5.1.1. Block

Σε ένα μπλοκ καταγράφονται οι πιο πρόσφατες συναλλαγές που έχουν γίνει σε ένα Blockchain δίκτυο. Συνεπώς, ένα μπλοκ είναι μια μόνιμη «αποθήκη δεδομένων», τα οποία, μόλις γραφτούν, δεν μπορούν να τροποποιηθούν ή να αφαιρεθούν. Τα μπλοκ όμως διαφέρουνε από Blockchain σε Blockchain και εκτός από τις συναλλαγές περιέχουνε κι,άλλα δεδομένα όπως αυτά που εξετάζονται στο μπλοκ του Bitcoin δικτύου. Παρακάτω παρουσιάζεται ένα παράδειγμα της δομής του μπλοκ στο Bitcoin δίκτυο το οποίο περιέχει τα εξής δεδομένα: το Block Size , το Block Header αποτελούμενο από 6 δεδομένα, το Transaction Counter και τις συναλλαγές (Transactions):



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

Block Header: Είναι η κεφαλίδα του μπλοκ η οποία αποτελείται από το:

Version: Είναι η έκδοσης του παρόν μπλοκ

Previous Block Hash: Είναι το Hash του προηγούμενου μπλοκ

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

Timestamp: Είναι ο χρόνος που δημιουργήθηκε αυτό το μπλοκ

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

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

Transaction Counter: Είναι ο συνολικός αριθμός των συναλλαγών στο μπλοκ

Transactions: Είναι όλες οι συναλλαγές που έχουν καταχωρηθεί στο μπλοκ, οι οποίες είναι περίπου 500 (Gupta, 2017, Antonopoulos, 2017).

5.1.2. Chain

Ο όρος αλυσίδα (Chain) σχετίζεται με τον τρόπο που είναι ταξινομημένα τα

μπλοκ σε ένα δίκτυο Blockchain. Σύμφωνα με τον Αντωνόπουλο (2017): "Η δομή των δεδομένων στο Blockchain είναι μια ταξινομημένη λίστα από μπλοκ συνδεδεμένη προς τα πίσω" (Antonopoulos, 2017). Αυτή η ταξινόμηση των μπλοκ σχηματίζει τελικά την αλυσίδα. Όπως προαναφέρθηκε, το Block Header αποτελείται από 6 δεδομένα και μέσα σε αυτά τα δεδομένα υπάρχει το Previous Block Hash το οποίο είναι αυτό που συνδέει αυτό το μπλοκ με το προηγούμενο μπλοκ στο Blockchain. Το Hash λοιπόν δημιουργείται πάντα από τα δεδομένα του προηγούμενου μπλοκ. Όπως αναφέρει η Laurence "Το Hash είναι η μαγική κόλλα που ενώνει τα μπλοκ μεταξύ τους και επιτρέπει εμπιστοσύνη με μαθηματική ακρίβεια" (Laurence, 2017). Για τη δημιουργία του Hash χρησιμοποιείται ο αλγόριθμος κρυπτογράφησης SHA-256, ο οποίος όταν κρυπτογραφεί τα δεδομένα επιστρέφει σχεδόν πάντα ένα μοναδικό αλφαριθμητικό 64 χαρακτήρων Hash. Η λειτουργία του αλγορίθμου χαρακτηρίζεται ως μη αντιστρέψιμη και λειτουργεί σαν ψηφιακό αποτύπωμα το οποίο είναι μοναδικό και δεν μπορεί να αποκρυπτογραφηθεί (Laurence, 2017 , Antonopoulos, 2017).

5.1.3. Digital Signatures

Η δημιουργία μιας συναλλαγής στο Blockchain απαιτεί ψηφιακή υπογραφή για τον έλεγχο και την εγκυρότητας της. Πιο αναλυτικά, για τη δημιουργία μιας ψηφιακής υπογραφής κάθε χρήστης χρησιμοποιεί ένα ζευγάρι κλειδιών, ένα ιδιωτικό και ένα δημόσιο. Το ιδιωτικό κλειδί, το οποίο γνωρίζει μόνο ο χρήστης χρησιμοποιείται για τη δημιουργία της ψηφιακής υπογραφής. Το δημόσιο κλειδί λειτουργεί σαν τις διευθύνσεις email, είναι δηλαδή ορατό προς όλους και χρησιμοποιείται για την επαλήθευση των δεδομένων.

Μια ψηφιακή υπογραφή περιλαμβάνει δύο φάσεις:

a) τη φάση υπογραφής και

b) τη φάση της επαλήθευσης.

Στην παρακάτω εικόνα παρουσιάζεται ένα παράδειγμα ψηφιακής υπογραφής. Παρατηρούμε λοιπόν ότι για να υπογράψει ο χρήστης,,Alice,, μια συναλλαγή

πρέπει να ακολουθήσει τα εξής βήματα:

i. Αρχικά δημιουργεί ένα Hash από τα δεδομένα της συναλλαγής χρησιμοποιώντας ένα αλγόριθμο κρυπτογράφησης.

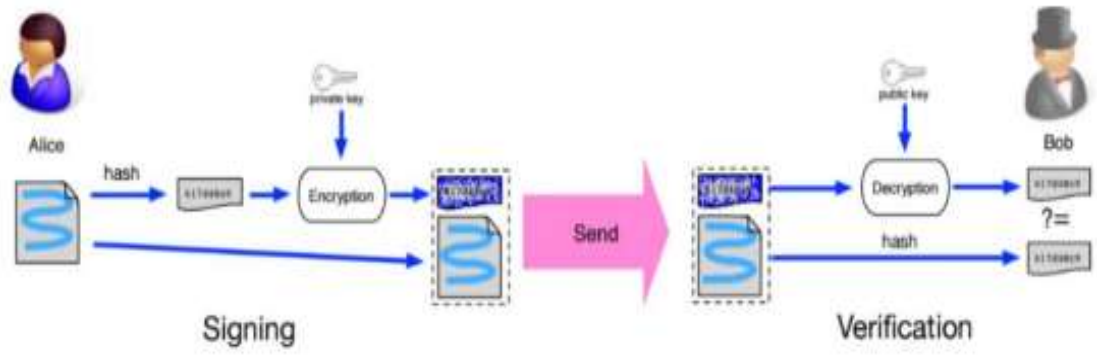
ii. Έπειτα δημιουργεί μια ψηφιακή υπογραφή αφού κρυπτογραφήσει την τιμή Hash χρησιμοποιώντας το ιδιωτικό κλειδί.

iii. Τέλος αποστέλλει στον χρήστη "Bob" την ψηφιακή υπογραφή μαζί με τα αρχικά δεδομένα της συναλλαγής.

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

i. να αποκρυπτογραφήσει την ψηφιακή υπογραφή με το δημόσιο κλειδί της Alice για να αποκτήσει το Hash

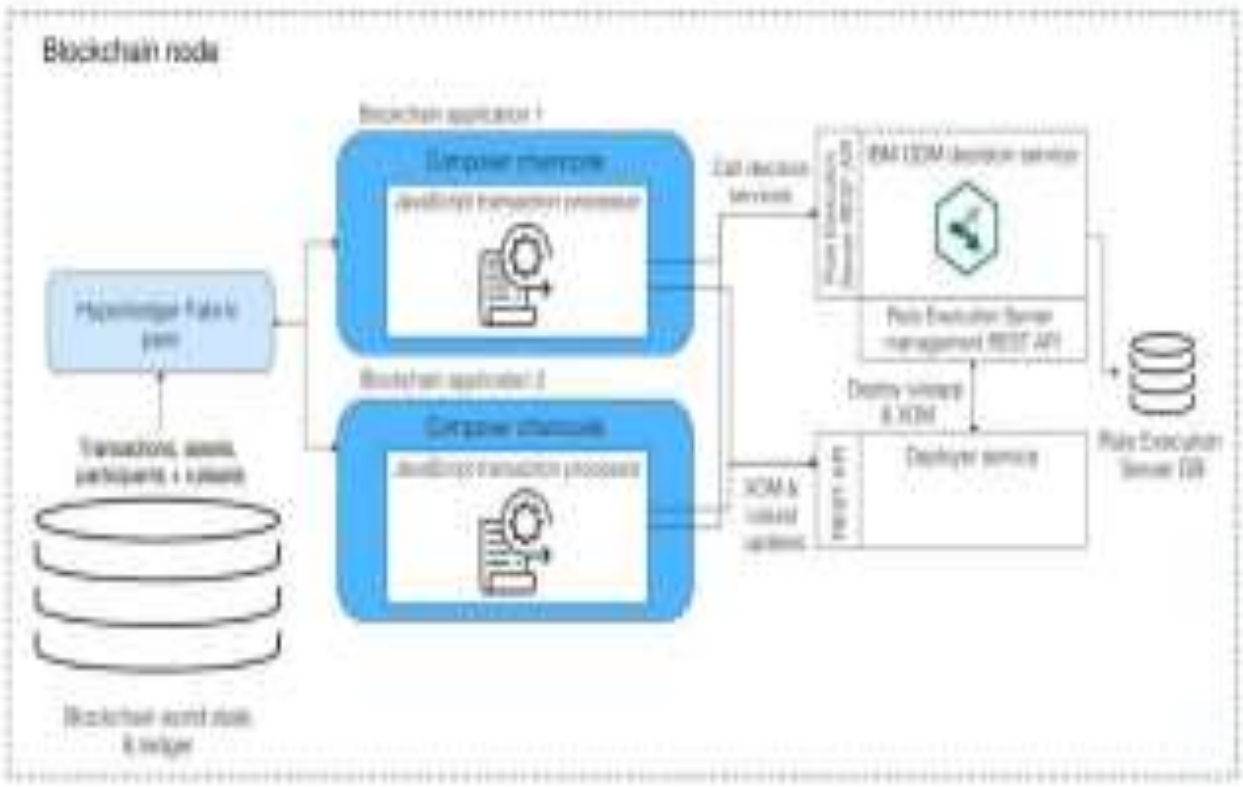
ii. να δημιουργήσει ένα 2 ο Hash από τα δεδομένα που του έχουνε σταλεί. Αν αυτά τα 2 Hash είναι ίδια τότε η συναλλαγή είναι έγκυρη (Antonopoulos, 2017: 61).



Εικόνα 7 Digital Signature Used in Blockchain. Ανακτήθηκε από www.researchgate.net: Άρθρο από τον Zibin Zheng και άλλους,

5.2. Hyperledger Fabric & Composer

Ένα blockchain που αναπτύσσεται χρησιμοποιώντας το Hyperleger Fabric αποθηκεύει δεδομένα με τη μορφή chaincode, έναν προγραμματικό κώδικα στο δίκτυο που λειτουργεί παρόμοια με έξυπνες συμβάσεις σε άλλα blockchains. Το δίκτυο υποστηρίζει επί του παρόντος τις Golang, node.js ή Java ως τις γλώσσες για τον chaincode.



Εικόνα 8 Διάγραμμα αρχιτεκτονικής ενός κόμβου που εξυπηρετεί διάφορες εφαρμογές blockchain. (IBM, 2018)

Από προεπιλογή, το δίκτυο δεν περιλαμβάνει το δικό του κρυπτονόμισμα. Ωστόσο, οι χρήστες μέσω του chaincode μπορούν να αναπτύξουν το δικό τους.

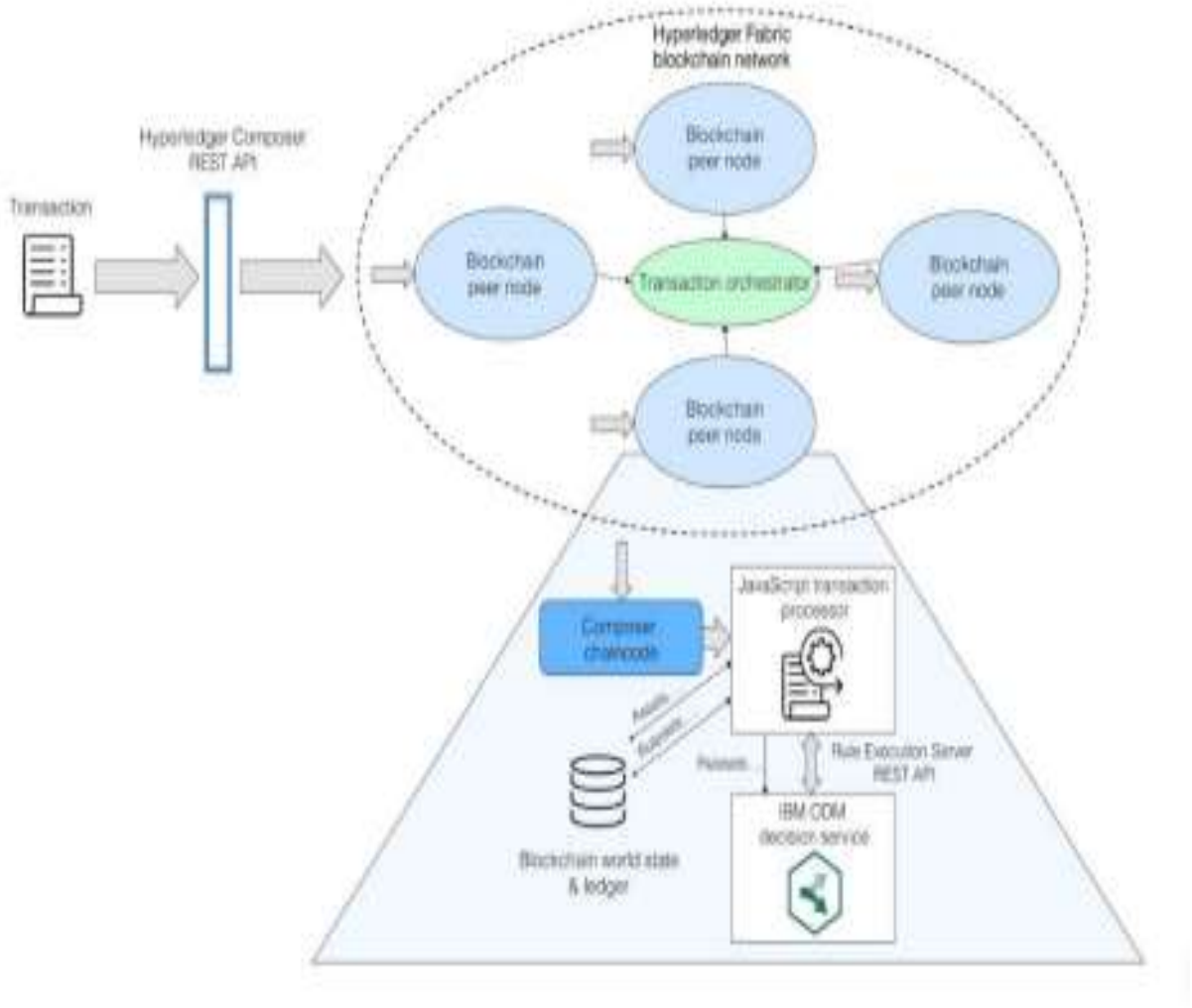
Το Hyperledger Composer είναι ένα σύνολο από εργαλεία που παρέχουν ένα αφαιρετικό επίπεδο για την υλοποίηση μια επαγγελματικής λύσης blockchain σε πραγματικές περιπτώσεις χρήσης .

Σε αυτό το πλαίσιο δημιουργούνται εφαρμογές blockchain και έξυπνα συμβόλαια. Το Composer εκτελείτε πάνω από το Hyperledger Fabric και σε συνδυασμό με τα εργαλεία του όπως είναι η JavaScript, node.js, npm,

Loopback API, CLI και δημοφιλή περιβάλλοντα ανάπτυξης κώδικα. Έτσι δίνει μια καλύτερη και εύχρηστη διαχείριση των τριών στοιχείων που ενδιαφέρουν μια επιχείρηση, τα περιουσιακά στοιχεία (assets), τις συναλλαγές (transactions) και του συμμετέχοντες (participants). Με αυτή την μοντελοποίηση ομαδοποιεί την διαχείριση των δεδομένων, τις λογικές λειτουργίες και την διαχείριση των μελών του δικτύου (Hyperledger Foundation, 2019) (IBM, 2018). Καταλήγοντας σε μια τυπική λειτουργία ενός κόμβου (βλ. Εικόνα 8) blockchain που λειτουργεί μέσα σε docker containers.

Ένα εξωτερικό σύστημα, που θα μπορούσε να είναι μια διαδικασία μιας επιχείρησης, ενεργοποιεί μια συναλλαγή μέσω του REST API (βλ. Εικόνα 9).

Η συναλλαγή κατανέμεται από το Hyperledger Fabric σε όλους τους κόμβους του blockchain. Ο κάθε κόμβος ενεργοποιεί το chaincode (έξυπνο συμβόλαιο) για να εφαρμοστεί η λογική πίσω από αυτό και να την ελέγξει. Το chaincode ενεργοποιεί την συναλλαγή του Hyperledger Composer όπου γίνεται η διερμηνεία του κώδικα JavaScript. Εκτελούνται οι απαραίτητες ενέργειες με της επιχειρηματικής λογικής και επιστρέφει μια απάντηση μέσω του REST API. Με αυτό τον τρόπο μπορούν να αυτοματοποιηθούν συναλλαγές της εφοδιαστικής αλυσίδας. Συλλέγονται οι πληροφορίες που αφορούν τις διαφορετικές εταιρείες της εφοδιαστικής που συμμετέχουν και δημιουργούνται γεγονότα που είναι το σημείο εκκίνησης κάποιας άλλης διαδικασίας. Επίσης με την συγκέντρωση πληροφοριών με αυτό τον τρόπο ενισχύεται η ορατότητα της ροής του προϊόντος.



Εικόνα 9 Η ροή της συναλλαγής στο Hyperledger

5.3. Παράλληλες Τεχνολογίες και Εργαλεία

Για να λειτουργήσει ένα ολοκληρωμένο σύστημα βασισμένο στο blockchain χρειάζονται πολλά εργαλεία και γλώσσες προγραμματισμού ώστε να συνδυαστούν και να δημιουργήσουν μια παραγωγική λύση. Έτσι θα αναλυθεί η σύγχρονη συλλογή εργαλείων που χρειάζεται από το Hyperledger Composer, όπως φαίνεται και στην εικόνα (βλ. Εικόνα 10). Συμβάλλοντας στην δόμηση του εμπρός, του πίσω και του ενδιάμεσου τμήματος μιας τέτοιας αρχιτεκτονικής υλοποίησης.

Εικόνα 10 Hyperledger Composer Tools-Stack

5.3.1. JavaScript

Η JavaScript είναι μια γλώσσα που πρωτοεμφανίστηκε το 1995 από την Netscape και Sun (Netscape Communications Corporation, 1995). Είναι μια γλώσσα υψηλού επιπέδου κατηγορίας διερμηνέα. Με τις τεχνολογικές εξελίξεις και την ραγδαία ανάπτυξη του internet και των browsers η JavaScript παράλληλα με την HTML και την CSS δομούν τεχνολογικά το World Wide Web. Ακολουθεί τις προδιαγραφές και εξελίσσεται με βάση το ECMAScript. Ενώ ταυτόχρονα έχει γνωρίσει μέσα στα χρόνια μεγάλες επεκτάσεις και υποκατάστατα όπως την VBScript από την Microsoft, την εκδοχή της Adobe, το Silverlight από την Microsoft, την εκδοχή της Google και φυσικά την TypeScript (Aston, 2015).

Η Angular είναι μια μοντέρνα cross-platform και ανοιχτού κώδικα γλώσσα για ανάπτυξη front-end web εφαρμογών. Είναι βασισμένη στην TypeScript και αναπτύσσεται από την Google. Ένα παράδειγμα αυτής, αποτελεί η παρούσα διπλωματική, στα πλαίσια της οποίας αναπτύχθηκαν δυο web εφαρμογές για τις επιχειρήσεις και για τον τελικό καταναλωτή. Παράλληλα υπάρχει το Node.JS όπου είναι ασύγχρονο περιβάλλον εκτέλεσης κώδικα JavaScript. Έχει σχεδιαστεί για την δημιουργία επεκτάσιμων εφαρμογών δικτύου. Το 2010 παρουσιάστηκε μαζί με το Node ο διαχειριστής πακέτων NPM. Ο οποίος διευκολύνει τους προγραμματιστές να δημοσιεύουν και να μοιράζονται πηγαίο κώδικα βιβλιοθηκών JavaScript. Στόχος του είναι να απλοποιεί την εγκατάσταση, την ενημέρωση και την απεγκατάσταση των βιβλιοθηκών.

Τέλος, σε γλώσσα JavaScript συντάσσεται όλη η επιχειρηματική λογική για τον ορισμό του δικτύου. Ο chaincode στο Hyperledger Composer έχει έναν διερμηνέα JavaScript που εκτελεί τη λογική για την επεξεργασία της συναλλαγής.

5.3.2. Web Playground

Το εργαλείο Composer Playground παρέχει μια web διεπαφή στον χρήστη για την διαμόρφωση, την εγκατάσταση και τις δοκιμές ενός επιχειρηματικού δικτύου blockchain. Έχει λειτουργίες που επιτρέπουν στους χρήστες να σχεδιάσουν τα επίπεδα ασφάλειας του δικτύου, να προσκαλούν συμμετέχοντες, να συνδέονται και να προσομοιώνουν πολλά blockchain .

5.3.3. CLI Utilities

Οι σύγχρονες τάσεις στον κώδικα ανοιχτού λογισμικού δεν θα μπορούσαν να λείπουν από εδώ. Υπάρχει μια πληθώρα εργαλείων και βιβλιοθηκών που συνθέτουν το περιβάλλον ανάπτυξης του blockchain. Τα εργαλεία CLI (command-line interface) έχουν σκοπό την αλληλεπίδραση προγραμμάτων όπου ο χρήστης δίνει εντολές με μορφή διαδοχικών γραμμών κειμένου, όπως σε μια κλασική κονσόλα. Μερικά από τα οποία είναι Yeoman Generator, που είναι γραμμένος σε Node.js, βοηθάει στην παραγωγή κώδικα με βάση κάποιο πρότυπο και τις δυναμικές παραμέτρους, για έλεγχο μονάδων κ.α. Μια σειρά από εργαλεία τα fabric-tools για την ρύθμιση και διαχείριση του Hyperledger Fabric. Τα πακέτα διαχειρίσεις του composer. Το composer-rest-server που είναι η εφαρμογή για το Backend API και τρέχει το Hyperledger Composer LoopBack Connector.\

5.3.4. VSCode και Extensions

Το Visual Studio Code είναι ένα ελεύθερο περιβάλλον ανάπτυξης λογισμικού, της Microsoft, το οποίο είναι ανοιχτού κώδικα. Στης εξέλιξή του έχει συμβάλει σημαντικά η κοινότητα των προγραμματιστών. Ένα δυνατό του σημείο είναι η υποστήριξη επεκτάσεων. Υπάρχει ειδική επέκταση από την Hyperledger για το Composer. Με αυτό τον τρόπο βοηθάει στης καλύτερη και ευκολότερη σύνταξη κώδικα. Προσφέρει επικύρωση, ορισμούς και δομή στον κώδικα. Επίσης αναφέρει τυχόν σφάλματα και εξετάζει να επικυρώσει τα αρχεία που δομούν την ασφάλεια και την πρόσβαση. Έτσι κατά την μοντελοποίηση μπορούν να αποφευχθούν λάθη και να βελτιστοποιηθεί ο χρόνος.

5.3.5. Docker

Το docker είναι ένα πρόγραμμα που πετυχαίνει εικονικότητα σε επίπεδο λειτουργικού συστήματος το οποίο ορίζεται ως containerization. Μέσω του docker δημιουργούνται και συνδέονται όλα τα κομμάτια του Blockchain όπως τα εργαλεία, η βάση δεδομένων CouchDB, ο orderer, η αρχή έκδοσης πιστοποιητικών (certificate authority), οι peers και ο chaincode. Το docker έχει μια σειρά από οφέλη όπως ασφάλεια και απομόνωση των κομματιών. Δίνει τη δυνατότητα για ταχεία και συνεχή ανάπτυξη κώδικα. Τέλος, δίνει ευελιξία στην ανάπτυξη και τις δοκιμές του κάθε τμήματος.

5.3.6. Debugging

Η διαδικασία του debugging είναι πολύπλοκη, προβληματική και περιορισμένη σε υλοποιήσεις blockchain. Στα έργα δικτύων blockchain η διαχείριση των σφαλμάτων του κώδικα είναι πολύ σημαντική (Stone, 2017). Ένα σφάλμα σε μια συναλλαγή μπορεί να σημαίνει απώλεια περιουσίας για τους συμμετέχοντες, την ακύρωση κάποιας σύμβασης ή το να παγώσουν κάποια εκατομμύρια δολάρια σε κρυπτονομίσματα. Ο κλασσικός τρόπος αποσφαλμάτωσης στις περισσότερες περιπτώσεις είναι δοκιμή και σφάλμα, με παρακολούθηση των logs για γραμμένες του κώδικα με εκτύπωση αναφορών, π.χ. τιμές μεταβλητών και καταστάσεων. Ευτυχώς, το Hyperledger Composer σε συνδυασμό με το Visual Studio Code έχουν αναπτύξει μια επικοινωνία για ζωντανή αποσφαλμάτωση με σημεία. Το μόνο που απαιτείται είναι μια λεπτομερής ρύθμιση παραμέτρων για να τρέξει.

6. ***Συμπεράσματα***

Η σύγχρονη τεχνολογία μπορεί να παράσχει τα απαραίτητα εργαλεία για την μετατροπή των λειτουργιών και την κάλυψη τον σημερινών αλλά και των μελλοντικών αναγκών της ψηφιακής οικονομίας. Σημαντικές τεχνολογίες πλέον βρίσκονται σε έξυπνες μονάδες παραγωγής και σε τμήματα αλυσίδων εφοδιασμού, όπου οι αισθητήρες και τα χειριστήρια είναι συνδεδεμένα μεταξύ τους. 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 ιδέα του Bitcoin και του Ethereum υιοθετήθηκε από τον κόσμο και διατάραξε τα νερά της οικονομίας με αποτέλεσμα μεγάλες τράπεζες και κυβερνήσεις να πολεμούν αυτά τα κρυπτονομίσματα. Ανήμπορες όμως οι τράπεζες και κυβερνήσεις να πάψουν την λειτουργία των κρυπτονομισμάτων άρχισαν να υποστηρίζουν την τεχνολογία Blockchain φτιάχνοντας τα δικά τους κρυπτονομίσματα και τις δικές τους υπηρεσίες βασισμένα σε αυτά. Καθίσταται έτσι φανερή η σπουδαιότητα και σοβαρότητα της νέας αυτής τεχνολογίας.

Ταυτόχρονα, κατά τη διεξαγωγή της έρευνάς μου κατανόησα απόλυτα ότι το Bitcoin και το Ethereum αποτελούν ένα μικρό μόνο δείγμα των δυνατοτήτων της τεχνολογίας Blockhain. Συνδυάζοντας λοιπόν παλιές και καινούργιες τεχνολογίες δημιουργήθηκε το Blockchain, το οποίο αποτελεί το έμπιστο πρωτόκολλο του Internet που τόσα χρόνια απουσίαζε αλλά ήταν τόσο αναγκαίο. Θα μπορούσε να υποστηριχθεί ότι η δημιουργία της τεχνολογίας Blockchain είναι αντίστοιχης σπουδαιότητας με τη δημιουργία του Παγκόσμιου Ιστού (γνωστό με τα αρχικά www), τον οποίο δημιούργησε ο Τιμ Μπέρνερς Λι στις 12 Νοεμβρίου του 1990. Το έμπιστο λοιπόν Blockchain μας δίνει την δυνατότητα να κοιτάξουμε το μέλλον και να δημιουργήσουμε τις επόμενες εφαρμογές οι οποίες θα βασίζονται σε αυτό, αλλάζοντας ριζικά τον τρόπο που λειτουργεί ο κόσμος, όπως ακριβώς είχε γίνει και με την

δημιουργία του Internet.

7. ***Βιβλιογραφία***

Acheson, N., 2018. How Bitcoin Mining Works. [Ηλεκτρονικό] Available at: https://www.coindesk.com/information/how-bitcoin-mining-works

Anon., 2005. International Standards Organization 9000.

Bauerle, N., 2017. What is the Difference Between Public and Permissioned Blockchains?. [Ηλεκτρονικό] Available at: https://www.coindesk.com/information/what-is-the-difference-between-open-andpermissioned-blockchains

Buterin, V., 2013. Ethereum White Paper. [Ηλεκτρονικό] Available at: https://web.archive.org/web/20161021061647/https://www.weusecoins.com/assets/pdf/library /Ethereum white papera next generation smart contract and decentralized application platform-vitalik-buterin.pdf

Cachin, C., 2016. Architecture of the Hyperledger Blockchain Fabric. p. https://www.zurich.ibm.com/dccl/papers/cachin_dccl.pdf.

Church, Z., 2017. Blockchain, explained. [Ηλεκτρονικό] Available at: https://mitsloan.mit.edu/ideas-made-to-matter/blockchain-explained

Friebe, T., 2017. Bitcoin, Ethereum, and Hyperledger Fabric — which one wins?. [Ηλεκτρονικό] Available at: https://medium.com/blockchainspace/3-comparison-of-bitcoin-ethereum-andhyperledger-fabric-cd48810e590c

Galvin, D., 2018. IBM and Walmart: Blockchain for Food Safety.

Gutierrez, C., 2017. Blockchain at Walmart: Tracking Food from Farm to Fork. [Ηλεκτρονικό] Available at: https://www.altoros.com/blog/blockchain-at-walmart-tracking-food-from-farm-tofork/

Hyperledger Fabric Docs, 2018. Smart Contracts. [Ηλεκτρονικό] Available at: https://hyperledgerfabric.readthedocs.io/en/latest/whatis.html?highlight=smart%20contracts#smart-contracts

Hyperledger Foundation, 2019. Hyperledger Composer Intro. [Ηλεκτρονικό] Available at:

https://hyperledger.github.io/composer/latest/introduction/introduction

IBM, 2018. Topology of a blockchain network with Hyperledger Fabric, Hyperledger Composer, and IBM ODM. [Ηλεκτρονικό] Available at: https://www.ibm.com/developerworks/library/mw-1708-mery-blockchain/1708- mery.html

Kamath, R., 2018. Food Traceability on Blockchain: Walmart's Pork and Mango Pilots. The Journal of The British Blockchain Association, 1(1), pp. 1-12.

Meunier, S., 2016. Blockchain technology - a very special kind of Distributed Database. [Ηλεκτρονικό] Available at: https://medium.com/@sbmeunier/blockchain-technology-a-very-special-kind-ofdistributed-database-e63d00781118

Nakamoto, S., 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. [Ηλεκτρονικό] Available at: https://bitcoin.org/bitcoin.pdf

Rilee, K., 2018. Understanding Hyperledger Fabric — Byzantine Fault Tolerance. [Ηλεκτρονικό] Available at: https://medium.com/kokster/understanding-hyperledger-fabric-byzantine-faulttolerance-cf106146ef43

Schollmeier, R., 2002. A Definition of Peer-to-Peer Networking for the Classification of Peer-toPeer Architectures and Applications.

Stone, S., 2017. Debug your Blockchain business network using Hyperledger Composer. [Ηλεκτρονικό] Available at: https://medium.com/@mrsimonstone/debug-your-blockchain-business-networkusing-hyperledger-composer-9bea20b49a74

Szabo, N., 1996. Smart Contracts: Building Blocks for Digital Markets

Terzi, S. & Stamelos, I., 2018. Permissioned Blockchains and Smart Contracts into Agile Software Processes. Communications in Computer and Information Science, Τόμος 918.