Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών *Ασφάλεια Υπολογιστών και Δικτύων*

Μεταπτυχιακή Διατριβή

Εφαρμογή Έξυπνων Συμβολαίων στις Τραπεζικές Συναλλαγές

Φωτεινή Έλληνα

Επιβλέπων Καθηγητής
Νικόλαος Σκλάβος

Μάϊος 2020

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών *Ασφάλεια Υπολογιστών και Δικτύων*

Μεταπτυχιακή Διατριβή

Εφαρμογή Έξυπνων Συμβολαίων στις Τραπεζικές Συναλλαγές

Φωτεινή Έλληνα

Επιβλέπων Καθηγητής
Νικόλαος Σκλάβος

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών στην Ασφάλεια Υπολογιστών και δικτύων από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών του Ανοικτού Πανεπιστημίου Κύπρου.

Μάϊος 2020

Περίληψη

Η τεχνολογία της αλυσίδας που παρουσιάζεται στη παρούσα μεταπτυχιακή διατριβή αποτελεί μια υπηρεσία διαχείρισης πληροφορίας η οποία διατηρείται σε διαφορετικούς σταθμούς που αποτελούν μέλη ενός ενιαίου δικτύου. Για την είσοδο στο δίκτυο το κάθε μέλος ταυτοποιείται, αποκτά τα απαιτούμενα δικαιώματα διαχείρισης της πληροφορίας και κατόπιν αμείβεται για τις υπηρεσίες που παρέχει εντός του δικτύου. Οι πληροφορίες ομαδοποιούνται σε συστοιχίες (blocks), συνδέονται μεταξύ τους με χρονολογική σειρά δημιουργώντας με τον τρόπο αυτό μια αλυσίδα (chain) από την οποία προέρχεται και η ονομασία της τεχνολογίας BlockChain. Η διατήρηση της πληροφορίας σε διαφορετικούς σταθμούς εξασφαλίζει την ακεραιότητα της αφού οποιαδήποτε προσπάθεια τροποποίησης της προϋποθέτει την έγκριση του συνόλου των μελών του δικτύου.

Η τεχνολογία αυτή αποτελεί τη βάση των ψηφιακών νομισμάτων που με βασικότερο το bitcoin γνωρίζουν μεγάλη αποδοχή στις μέρες μας. Βασικό ρόλο στη τάση αυτή επιτέλεσε η κρίση του τραπεζικού τομέα που οδήγησε στη παγκόσμια οικονομική κρίση που βίωσε ο πλανήτης στις ημέρες μας και παρέπεμψε τους καταναλωτές να αναζητήσουν νέες μεθόδους συναλλαγής. Η τεχνολογία της αλυσίδας παρέχει ενδιαφέρουσες προτάσεις στο τομέα αυτό όπως ταχύτητα στις συναλλαγές, εξάλειψη του ρόλου των μεσαζόντων και άρα σημαντική μείωση του κόστους, ασφάλεια και απαγκίστρωση από κρατικές κατευθύνσεις.

Στη παρούσα μεταπτυχιακή διατριβή παρουσιάζουμε τη λειτουργία της τεχνολογίας, τις επιμέρους τεχνολογίες στις οποίες στηρίζεται καθώς και μια νέα προσθήκη που αποτελεί το έξυπνο συμβόλαιο. Ακολούθως, παρουσιάζουμε την θέση που κατέχει στη διεθνή αγορά σήμερα. Στη συνέχεια συγκρίνουμε τέσσερεις από τις πλέον σημαντικότερες πλατφόρμες που κυριαρχούν στην αγορά επικεντρώνοντας την ανάλυση στη γενική περιγραφή τους, στις τεχνολογικές ιδιότητες τους καθώς και στα χρηματοοικονομικά τους στοιχεία. Ακολούθως θα εστιάσουμε στο τραπεζικό κλάδο και θα διερευνήσουμε την εφαρμογή της τεχνολογίας αλλά και των έξυπνων συμβολαίων στους διάφορους κλάδους της τραπεζικής. Τέλος θα παρουσιάσουμε τη διαδικασία υλοποίησης ενός έξυπνου συμβολαίου σε περιβάλλον λιανικής τραπεζικής.

Λέξεις κλειδιά: Τεχνολογία Κατανεμημένου Καθολικού, Τεχνολογία αλυσίδας, Έξυπνα συμβόλαια, Μηχανισμοί Ομοφωνίας, Αξιολόγηση Πλατφορμών Τεχνολογιών Αλυσίδας Συστοιχιών, Εφαρμογές Έξυπνων Συμβολαίων στις Τραπεζικές Συναλλαγές

Summary

BlockChain technology which is presented in this thesis is an application that handles information and maintains it at different locations called nodes that exist in a network. In order to become member of the network every node must register first and then it gains certain rights to access the information. In the network the node provides services handling that information and receives payment for those services. The information is organized in blocks and connected in a chronological order thus creating a chain. From those two words, block and chain, became the name of the technology, Blockchain. The fact that the information is stored in different nodes ensures that it will remain intact as any attempt to alter it has to be approved from every node in the network.

That is the technology behind crypto currencies or crypto coins like bitcoin which is the leader among the platforms. Those platforms are very popular in our days and the main reason for that is the crisis of the banking sector that led to the worldwide economic crisis which we all experienced in the last 10 years. That crisis forced people to look for new ways of transacting and the technology of blockchain has the tools to accomplish that. For example, blockchain can execute transactions faster and safer than the traditional ways, eliminating the need of mediators which leads to a smaller cost per transaction and away from government intervention.

In this thesis we present how BlockChain works, the technologies it uses and a new addition, the smart contracts. We examine its position in the world market and then we study four wide accepted BlockChain platforms. Next, we focus at the banking sector and how the technology of blockchain and smart contracts can be used. Lastly, we present the process of creating and using a smart contract for the retail banking sector.

Keywords: Distributed Ledger Technology, BlockChain Technology, Smart Contracts, Bitcoin, Ethereum, Hyperledger, R3 Corda, Blockchain Platform Evaluation, Use of Smart Contracts in Bank Sector

Ευχαριστίες

θα ήθελα να ευχαριστήσω την οικογένεια μου, Παύλο, Βασίλη και Ελένη, για όλη την στήριξη και υπομονή που έδειξαν καθ' όλη την διάρκεια των μεταπτυχιακών μου σπουδών και ειδικά το διάστημα εκπόνησης αυτής της μεταπτυχιακής διατριβής.

Επίσης, θα ήθελα να ευχαριστήσω τον επιβλέπων καθηγητή μου, Νικόλαο Σκλάβο, για την εμπιστοσύνη που μου έδειξε και την βοήθεια του.

Περιεχόμενα

Κεφάλαιο 1
Εισαγωγή

Ένα από τα βασικά χαρακτηριστικά της εποχής μας είναι ο ρυθμός με τον οποίο επέρχονται οι αλλαγές στη καθημερινότητα της ζωής των ανθρώπων. Ο ρυθμός αυτός έχει ενταθεί τα τελευταία χρόνια και συνεχώς επεκτείνεται και σε νέους τομείς. Ρίχνοντας μια ματιά στο κοντινό παρελθόν αρκεί για να καταλάβει ο αναγνώστης το πόσο έχει αλλάξει η καθημερινότητα μας, από τον τρόπο που μετακινούμαστε, που συναναστρεφόμαστε μεταξύ μας, το πώς διασκεδάζουμε και γενικότερα το πώς λειτουργούμε σήμερα σε σχέση με το κοντινό παρελθόν μας.

Σε αυτή την εποχή των γρήγορων αλλαγών ελάχιστα είναι τα πράγματα που έχουν μείνει σταθερά και δεν έχουν επηρεαστεί από αυτή την τάση. Ένα από αυτά είναι και ο τρόπος με τον οποίο συναλλασσόμαστε και πιο συγκεκριμένα το τραπεζικό σύστημα, από τα ελάχιστα πράγματα που δεν έχουν αποκλείσει ιδιαίτερα από τον αρχικό τους σχεδιασμό. Ειδικότερα, για το σύστημα αυτό όπου ο σχεδιασμός του τοποθετείτε χρονικά στις πρώτες μέρες των αρχαίων πολιτισμών. Στο μακροχρόνιο διάστημα της ύπαρξης του έχει εξελιχθεί σε μεγάλο βαθμό αλλά ο βασικός άξονας λειτουργίας του παραμένει σταθερός.

Τα τελευταία χρόνια γίνετε όλο και περισσότερο αντιληπτό ότι και αυτό το σύστημα θα πρέπει να αλλάξει ουσιαστικά μιας και στη μορφή αυτή δεν είναι σε θέση να ικανοποιήσει πλέον ουσιαστικά το σκοπό για τον οποίο δημιουργήθηκε. Παρόλες τις επεμβάσεις που έχει υιοθετήσει, τις νέες τεχνολογίες που χρησιμοποιεί και γενικότερα την εξέλιξη που έχει ακολουθήσει τα τελευταία χρόνια δεν μπορεί να ακολουθήσει τους ρυθμούς της σημερινής εποχής. Μέχρι και το πρόσφατο παρελθόν για να γίνει μία απλή συναλλαγή απαιτούνταν η φυσική παρουσία του ατόμου σε κάποιο υποκατάστημα τραπέζης, τις ώρες γραφείου αποκλειστικά, διαδικασία ιδιαίτερα χρονοβόρα και κοστοβόρα. Στις μέρες μας όμως οι διαδικασίες αυτές γίνονται μέσω κινητού τηλεφώνου, οποιαδήποτε στιγμή και από οπουδήποτε. Ακόμα όμως και οι βελτιώσεις αυτής της τάξης δεν είναι αρκετές για να ανταποκριθεί ο χρηματοοικονομικός τομέας στις προκλήσεις της σημερινής εποχής. Σήμερα οι συναλλαγές θα πρέπει να γίνονται άμεσα, ασφαλή και με όσο το δυνατόν χαμηλό κόστος. Με το υπάρχον τραπεζικό σύστημα σήμερα μια απλή

μεταφορά χρημάτων από μία τράπεζα μιας χώρας σε μία άλλη άλλης χώρας έχει υπολογίσιμο κόστος, απαιτεί χρόνο για να υλοποιηθεί και δεν είναι πάντα ασφαλή. Γίνεται εύκολα αντιληπτό ότι η μέθοδος αυτή δεν μπορεί να συμβαδίσει με τους ρυθμούς και τις απαιτήσεις της εποχής μας.

Λύση σε αυτά τα ζητήματα υπόσχεται να φέρει η τεχνολογία του μπλοκ αλυσίδας η Blockchain όπως ονομάζεται στα διεθνή μέσα. Με τα νέα μέσα που εισάγει στοχεύει στο να αλλάξει ριζικά τους τρόπους με τους οποίους συναλλασσόμαστε και γενικότερα το τραπεζικό σύστημα. Εμπνευστής του, ένας άνθρωπος με το ψευδώνυμο Σατόσι Νακαμότο, πρότεινε μια λύση για το διάσημο πρόβλημα των Βυζαντινών Στρατηγών με εφαρμογή στο χρηματοοικονομικό τομέα. Ο Νακαμότο έχοντας σαν αφετηρία το Μαθηματικό πρόβλημα της ανάγκης δημιουργίας ενός δικτύου εμπιστοσύνης μεταξύ των Βυζαντινών Στρατηγών εμπνεύστηκε ένα δίκτυο υπολογιστών μέσω του οποίου οι άνθρωποι θα εκτελούν τις μεταξύ τους χρηματοοικονομικές συναλλαγές με ασφάλεια και επίσης θα είναι απαλλαγμένο από κάθε κεντρική εξουσία που θα μπορούσε να παρέμβει και να επιβάλλει τους δικούς της κανόνες. Καρπός αυτής της έμπνευσης το διάσημο Bitcoin, ένα ψηφιακό νόμισμα το οποίο μπορούν οι άνθρωποι να χρησιμοποιούν για τις συναλλαγές τους το οποίο όμως είναι δημόσιο και κανείς δεν μπορεί να το ελέγξει.

Η τεχνολογία όμως αυτή δεν σταματάει μόνο στη δημιουργία ενός νέου νομίσματος αλλά με τη συνδρομή των έξυπνων συμβολαίων μπορεί να επεκταθεί και σε άλλους τομείς της καθημερινότητας των ανθρώπων. Προκειμένου τα έξυπνα αυτά συμβόλαια να γίνουν κατανοητά από τον αναγνώστη, στο σημείο αυτό κρίνεται σκόπιμο να αναφέρουμε το απλό παράδειγμα της πιτσαρίας. Η επιχείρηση υπόσχεται να παραδώσει το προϊόν της στο καταναλωτή σε χρόνο 30 λεπτών και συνάπτει με αυτόν ένα έξυπνο συμβόλαιο. Εκείνος καταθέτει τα χρήματα σε τρίτο ουδέτερο φορέα και αυτά μεταφέρονται στην επιχείρηση αυτόματα εάν το χρονοδιάγραμμα της παράδοσης τηρηθεί. Σε διαφορετική περίπτωση επιστρέφονται στο καταναλωτή. Η όλη διαδικασία γίνεται αυτόματα μέσω υπολογιστή, χωρίς το κόστος μεσαζόντων και χωρίς καθυστερήσεις.

1.1. Στόχος

Στόχος της παρούσας μεταπτυχιακής διατριβής είναι η παρουσίαση της λειτουργίας της τεχνολογίας αλυσίδας και του έξυπνου συμβολαίου καθώς και η διερεύνηση των εφαρμογών τους στον τραπεζικό κλάδο. Η ανάλυση τεσσάρων από τις πλέον σημαντικότερες πλατφόρμες που υποστηρίζουν έξυπνα συμβόλαια και κυριαρχούν στην αγορά, και τέλος, η υλοποίηση ενός έξυπνου συμβολαίου λιανικής τραπεζικής στο περιβάλλον του HyperLedger Fabric, ώστε να σχηματίσει ο αναγνώστης μια εικόνα για το τι είναι τα έξυπνα συμβόλαια και πώς γίνεται η υλοποίηση αυτών.

1.2. Ερευνητικά Ερωτήματα

Στη παρούσα μεταπτυχιακή διατριβή θα κάνουμε μια προσέγγιση, προκειμένου να απαντήσουμε στα ακόλουθα ερευνητικά ερωτήματα (RQs):

- **RQ1** - Ποια είναι η τρέχουσα κατάσταση και οι προβλέψεις σχετικά με τη τεχνολογία blockchain και τα έξυπνα συμβόλαια σε σχέση με το τραπεζικό σύστημα;
- **RQ2** – Είναι η πλατφόρμα Hyperledger fabric μια αρκετά ανταγωνιστική επιλογή με βασικά χαρακτηριστικά την απλότητα, την τεκμηρίωση και την μικρή απαίτηση σε πόρους;

1.3. Μεθοδολογία και Περίγραμμα

Η ερευνητική μεθοδολογία της παρούσας μεταπτυχιακής διατριβής βασίζεται στην τρέχουσα βιβλιογραφία ώστε να παρουσιαστούν προτεινόμενες εφαρμογές αλλά κυρίως η τρέχουσα κατάσταση και οι προβλέψεις σχετικά με τη τεχνολογία blockchain και τα έξυπνα συμβόλαια σε σχέση με το τραπεζικό σύστημα και τις τραπεζικές συναλλαγές. Εκτός από τη μελέτη της βιβλιογραφίας, θα αναπτύξουμε ένα έξυπνο συμβόλαιο λιανικής τραπεζικής χρησιμοποιώντας τη πλατφόρμα Hyperledger Fabric περιγράφοντας τα βήματα της υλοποίησης. Για την πραγματοποίησή του θα εγκατασταθεί ένα blockchain δίκτυο σε ένα virtual machine της Oracle με λειτουργικό Ubuntu, ενώ για την σύνταξη του έξυπνου συμβολαίου θα χρησιμοποιήσουμε τη γλώσσα προγραμματισμού JavaScript. Το περίγραμμα της μεταπτυχιακής διατριβής δίνεται παρακάτω:

Στο κεφάλαιο 2 παρουσιάζονται σχετικές ερευνητικές εργασίες που χρησιμοποιούν την τεχνολογία blockchain και τα έξυπνα συμβόλαια.

Στο κεφάλαιο 3 γίνεται περιγραφή της τεχνολογίας αλυσίδας και μια σύντομη ιστορική αναδρομή με στόχο να κατανοήσει ο αναγνώστης τα τεχνολογικά ορόσημα που οδήγησαν στην δημιουργία της αλυσίδας. Τέλος παρουσιάζονται τα βασικά της είδη καθώς και οι τεχνολογίες πάνω στις οποίες στηρίζεται η αλυσίδα.

Στο κεφάλαιο 4 παρουσιάζονται η λειτουργία, τα πεδία εφαρμογής, οι προκλήσεις οι περιορισμοί, το κόστος καθώς και τα οφέλη χρήσης, μιας ιδιαίτερα σημαντικής λειτουργίας της αλυσίδας συστοιχιών, τα έξυπνα συμβολαίων.

Στο κεφάλαιο 5 αναφέρεται η εξάπλωση που έχουν πετύχει οι τεχνολογίες τόσο του BlockChain όσο και των έξυπνων συμβολαίων στην αγορά διεθνώς έως σήμερα. Επίσης, τι αναμένετε να επακολουθήσει αναφορικά με την οικονομική πλευρά των τεχνολογιών αυτών.

Στο κεφάλαιο 6 μελετώνται και συγκρίνονται οι πλέον διαδεδομένες πλατφόρμες τεχνολογίας αλυσίδας που υποστηρίζουν έξυπνα συμβόλαια. Θα αναφερθούμε στα ιδιαίτερα χαρακτηριστικά τους, το μερίδιο αγοράς που κατέχουν καθώς και τις τεχνολογίες που υποστηρίζουν. Μέσω αυτής της σύγκρισης θα γίνει η επιλογή της πλατφόρμας που θα χρησιμοποιήσουμε στην πρότασή μας για έξυπνο συμβολαίο λιανικής τραπεζικής.

Στο κεφάλαιο 7 παρουσιάζεται η εικόνα του τραπεζικού συστήματος και αναφέρονται οι βελτιώσεις που μπορεί να επιφέρει η εφαρμογή της τεχνολογίας αλυσίδας σε συνδυασμό με την χρήση των έξυπνων συμβολαίων.

Στο κεφάλαιο 8 παρουσιάζεται η διαδικασία υλοποίησης ενός έξυπνου συμβολαίου λιανικής τραπεζικής με χρήση της πλατφόρμας HyperLedger Fabric.

Στο κεφάλαιο 9 δίνονται απαντήσεις στα ερευνητικά ερωτήματα και συνοψίζονται τα ευρήματα και τα συμπεράσματα της παρούσας μεταπτυχιακής διατριβής.

1.4. Τρέχουσα Κατάσταση

Δεδομένου ότι η τεχνολογία blockchain θα μπορούσε να προσφέρει ευκαιρίες για μείωση του κόστους και βελτίωση της ταχύτητας διακανονισμού συναλλαγών, οι τράπεζες και ολόκληρη η βιομηχανία κινητών αξιών ενδιαφέρεται όλο και περισσότερο για την τεχνολογία. Επιπλέον, διεθνείς οργανισμοί, όπως το Διεθνές Νομισματικό Ταμείο, και έθνη, όπως οι ΗΠΑ, το Ηνωμένο Βασίλειο, η Ιαπωνία, η Κίνα, η Ρωσία, η Ινδία και η Νότια Αφρική έχουν ξεκινήσει έρευνα για εφαρμογές τεχνολογίας blockchain (Guo, Liang 2016:24). Πρόσφατα, διεθνείς οργανισμοί, συμπεριλαμβανομένου και του Διεθνούς Νομισματικού Ταμείου (Guo, Liang, 2016:24), καθώς και κεντρικές τράπεζες στο Ηνωμένο Βασίλειο, την Κίνα, τις ΗΠΑ, την Κορέα, τη Σιγκαπούρη, την Ιαπωνία, τη Ρωσία, την Ινδία, την Ολλανδία και τη Νότια Αφρική ανακοίνωσαν τα σχέδια τους για την τεχνολογία blockchain (Mori 2016:208, Tsai, Blower, Zhu, Yu 2016:450). Εθνικά χρηματιστήρια όπως ο Nasdaq, τραπεζικοί τιτάνες όπως η J.P. Morgan; και χρηματοοικονομικοί φορείς όπως ο USA Depository Trust and Clearing Corporation αλλά και η Λαϊκή Τράπεζα της Κίνας έχουν ξεκινήσει ερευνητικά εργαστήρια της τεχνολογίας blockchain (Guo, Liang, 2016:24, Mori 2016:208). Τα περισσότερα χρηματοπιστωτικά ιδρύματα διαθέτουν πιλοτικά προγράμματα για το blockchain όπως για παράδειγμα, το R3 - ιδρύθηκε το 2015 ως κοινοπραξία τεχνολογίας blockchain - συνεργάστηκε με πάνω από ογδόντα χρηματοπιστωτικά ιδρύματα και φορείς (R3 2020.). Η China Financial Blockchain Consortium (Guo, Liang, 2016:24) είναι μια άλλη συμμαχία. Εταιρείες όπως η Blockstream και η Digital Asset Holdings προσφέρουν ήδη υπηρεσίες χρηματοπιστωτικών ιδρυμάτων που διευκολύνουν τη διαχείριση ψηφιακών περιουσιακών στοιχείων (Pilkington 2016:225).

Έρευνα (Arjun, R., & Suprabha, K. R., 2020:1) έδειξε ότι λιγότερα από 5 άρθρα σχετικά με τον όρο "blockchain" και "bank" δημοσιεύθηκαν το 2015 αλλά μέχρι το 2019 αυτά αυξήθηκαν σε 35. Στις αναπτυγμένες και αναπτυσσόμενες οικονομίες το ενδιαφέρον για την τεχνολογία blockchain και τα έξυπνα συμβόλαια είναι μεγάλο παρόλα αυτά οι προτεινόμενες θεωρητικές λύσεις δεν έχουν γνωστές υλοποιήσεις αφού τα τραπεζικά συστήματα θα πρέπει να επανασχεδιαστούν ώστε να μπορέσουν να την υιοθετήσουν.

Κεφάλαιο 2
Σχετικές Ερευνητικές Εργασίες

Στο κεφάλαιο αυτό θα παρουσιάσουμε σχετικές ερευνητικές εργασίες που χρησιμοποιούν την τεχνολογία Blockchain και τα έξυπνα συμβόλαια.

2.1 Εφαρμογή του Ethereum Blockchain στο Τραπεζικό Σύστημα

Το τρέχων τραπεζικό σύστημα βασίζεται σε έναν κεντρικό διακομιστή όπου όλα τα καταστήματα είναι συνδεδεμένα σε αυτόν. Οποιαδήποτε διακοπή στον κεντρικό διακομιστή επηρεάζει όλους τους άλλους συνδεδεμένους κλάδους. Η τεχνολογία Blockchain και τα έξυπνα συμβόλαια μπορούν να δώσουν λύση σε αυτό το πρόβλημα αφού πρόκειται για ένα αποκεντρωμένο σύστημα με επιπλέον βασικά πλεονεκτήματα το αμετάβλητο, την ασφάλεια και την διαφάνεια. Μία προτεινόμενη λύση (Bakaul, Das, Moni 2020:50) είναι η χρήση της πλατφόρμας Ethereum σε συνδυασμό με έξυπνα συμβόλαια για το back-end. Τα αρχεία των συναλλαγών αποθηκεύονται σε μπλοκ και διατηρούνται σε όλους τους υπολογιστές που είναι συνδεδεμένοι σε ένα δίκτυο peer-to-peer. Τα μπλοκ συνδέονται μεταξύ τους με γραμμικό τρόπο όπου κάθε μπλοκ περιέχει μια τιμή κατακερματισμού του προηγούμενου μπλοκ. Σε σύγκριση με τα παραδοσιακά τραπεζικά συστήματα, το Blockchain διατηρεί όλα τα ιστορικά των συναλλαγών. Ασφαλίζει τις συναλλαγές ώστε οποιαδήποτε εγγραφή της συναλλαγής που συνέβη στο παρελθόν, δεν μπορεί να τροποποιηθεί καθώς η τροποποίηση αλλάζει το κατακερματισμό πολλών μπλοκ.

2.2 Σχεδιασμός Συστήματος Τράπεζας Χρόνου σε Hyperledger Fabric Blockchain

Αυτό το άρθρο (Lee, Lin, Hsu, Wu 2020) παρουσιάζει τη δημιουργία ενός συστήματος τράπεζας χρόνου με βάση το blockchain και τη πλατφόρμα Hyperledger Fabric. Οι περισσότερες από τις υπηρεσίες που πραγματοποιούνται στα υπάρχοντα συστήματα τραπεζών χρόνου καταγράφονται χειροκίνητα με αποτέλεσμα κόστος σε χρόνο και ανθρώπινους πόρους αλλά ακόμα χειρότερα, στερείται ασφάλειας. Το προτεινόμενο σύστημα επιτρέπει σε όλες τις διαδικασίες που σχετίζονται με τις υπηρεσίες να εκτελούνται και να καταγράφονται σε ένα blockchain. Η αντιστοίχιση μεταξύ των εργασιών και των υπηρεσιών μπορεί να γίνει άμεσα μέσω αυτόνομων έξυπνων συμβολαίων. Επίσης, η οικοδόμηση ενός συστήματος χρονικής τράπεζας σε blockchain ωφελεί τη συναλλαγή πίστωσης χρόνου που παίζει το ρόλο του ψηφιακού νομίσματος.

Το δίκτυο Fabric στη συγκεκριμένη πρόταση αποτελείται από τρία διαφορετικά κανάλια. Το πρώτο ασχολείται με όλα τα ζητήματα δικτύωσης που σχετίζονται με τις υπηρεσίες. Το δεύτερο είναι υπεύθυνο για τη συλλογή όλων των δεδομένων πορτοφολιού από το καθολικό (ledger). Το τρίτο επιτρέπει στα εγγεγραμμένα μέλη να βαθμολογούν το ένα το άλλο. Κάθε κανάλι είναι συνδεδεμένο με έξυπνα συμβόλαια που εκτελούνται σε peers και παρέχει μια πλατφόρμα για την εκτέλεση του προγράμματος και τη μεταφορά των συναλλαγών. Τελικά, όλες οι συναλλαγές αποστέλλονται σε μια ειδική οντότητα που ονομάζεται «εντολέας» (orderer), η οποία ενημερώνει το ledger με τις επιβεβαιωμένες συναλλαγές.

2.3 Εφαρμογές των Εξυπνων Συμβολαίων στο Κλάδο της Εφοδιαστικής Αλυσίδας

Στο σημείο αυτό αξίζει να αναφερθεί και το έργο του Gunnar Prause (Prause 2019:2501) ο οποίος μελέτησε τις εφαρμογές των έξυπνων συμβολαίων στο κλάδο της εφοδιαστικής αλυσίδας. Η μεγάλη προσφορά των έξυπνων συμβολαίων στο χώρο αυτό είναι ότι προσφέρουν σημεία διασύνδεσης των διαφορετικών εταιριών κατά μήκος της αλυσίδας με αποτέλεσμα οι διαδικασίες να πραγματοποιούνται αυτόματα και σε ελάχιστο χρόνο. Πιο συγκεκριμένα, η κάθε εταιρία κατά μήκος της αλυσίδας μπορεί να είναι εντελώς διαφορετική από τις υπόλοιπες, με διαφορετικούς τρόπου λειτουργίας, διαφορετική γλώσσα επικοινωνίας, να βρίσκεται σε άλλο κράτος και να διέπετε από άλλους νόμους, ζώνη ώρας κλπ. Η διαφορετικότητα αυτή καθιστά δύσκολες τις

συναλλαγές και προσφέρει πρόσφορο έδαφος σε μεγάλους κολοσσούς, που έχουν ενσωματώσει το σύνολο της αλυσίδας, να επικρατούν. Η ενσωμάτωση των έξυπνων συμβολαίων, που επιτρέπουν για παράδειγμα την πληρωμή των προϊόντων μόλις αυτά παραληφθούν, αντιμετωπίζει αυτή τη δυσκολία και επιτρέπει και σε μικρότερες εταιρίες να ανταγωνιστούν τους κολοσσούς που έως τώρα επικρατούν.

2.4 Κατανεμημένο Σύστημα Ελέγχου Βασισμένο σε Blockchain

Ο Stanciu (Stanciu 2017:667) πρότεινε μια ενδιαφέρουσα χρήση της πλατφόρμας Hyperledger Fabric σε ένα σύστημα ιεραρχικού κατανεμημένου ελέγχου πρόσβασης βάσει του προτύπου IEC61499. Το Hyperledger και το Docker χρησιμοποιούνται για την εφαρμογή μπλοκ λειτουργίας και το Kubernetes χρησιμοποιείται για την οργάνωση της εκτέλεσης σε όλους τους κόμβους. Ο στόχος είναι μια αρχιτεκτονική τριών επιπέδων όπου οι κόμβοι των άκρων μπορούν να χρησιμοποιηθούν για να κάνουν τα πρώτα βήματα επεξεργασίας ώστε να υπάρξει σημαντική μείωση των μεγεθών μεταφοράς και της εξάρτησης από το cloud.

2.5 Blockchain και Έξυπνα Συμβόλαια στο IoT

Ο σχεδιασμός αυτού του συστήματος (Shurman, M., Obeidat A., Al-Shurman, S. 2020) προτείνει ένα έξυπνο συμβόλαιο να είναι η πύλη για όλες τις συσκευές IoT στο δίκτυο. Έτσι, η επικοινωνία μεταξύ των συσκευών είναι κυρίως μέσω έξυπνων συμβολαίων που συντονίζουν και αυτοματοποιούν τις συναλλαγές μεταξύ των συσκευών IoT. Το έξυπνο συμβόλαιο χρησιμοποιεί το blockchain ως βάση δεδομένων για την αποθήκευση και την επικύρωση όλων των συναλλαγών παρέχοντας χρονική σήμανση και επικυρωμένο καθολικό πληροφοριών.

Κεφάλαιο 3
Η Τεχνολογία Αλυσίδας Συστοιχιών (Blockchain)

Στο κεφάλαιο αυτό γίνεται περιγραφή της τεχνολογίας αλυσίδας με σκοπό να σχηματίσει ο αναγνώστης μια σφαιρική εικόνα του θέματος. Η λειτουργία της χωρίζεται σε 4 βασικά βήματα ώστε να γίνει όσο το δυνατόν πιο εύκολη η κατανόηση της λειτουργίας της. Ακολούθως γίνεται μια σύντομη ιστορική αναδρομή με στόχο να κατανοήσει ο αναγνώστης τα τεχνολογικά ορόσημα που οδήγησαν στην δημιουργία της αλυσίδας. Τέλος παρουσιάζονται τα βασικά της είδη καθώς και οι τεχνολογίες πάνω στις οποίες στηρίζεται η αλυσίδα.

3.1 Περιγραφή της Τεχνολογίας

Η τεχνολογία αλυσίδας συστοιχιών αναφέρεται σε ένα σύνολο αμετάβλητων εγγραφών που διατηρούνται σε μπλοκ, με τη σειρά που δημιουργήθηκαν και στο σύνολο τους σε διαφορετικές τοποθεσίες. Οι εγγραφές αυτές δύναται να περιγράφουν οτιδήποτε έχει αξία, από μία συναλλαγή έως μια υπόσχεση. Το γεγονός ότι αποθηκεύονται με τη σειρά που δημιουργήθηκαν και ότι δεν επιτρέπεται να τροποποιηθούν εξασφαλίζει την ασφάλεια των συναλλασσόμενων μελών. Η εφαρμογή μιας τέτοιας αλυσίδας θα μπορούσε να διατηρεί τα χρηματικά υπόλοιπα μια ομάδας ανθρώπων για παράδειγμα. Ο Α έχει στη διάθεση του 100 ευρώ και από αυτά δίνει στον Β 10. Ο Β που αρχικά είχε 80 τώρα έχει 90. Ακολούθως δίνει στον Γ 20 που πλέον έχει 130. Η συναλλαγές αυτές αποθηκεύονται σε διαφορετικά σημεία με τη σειρά που δημιουργήθηκαν. Οπότε, όλοι οι συμμετέχοντες στην αλυσίδα γνωρίζουν τα υπόλοιπα του κάθε συμμετέχοντα και μπορούν ανά πάσα στιγμή να επιβεβαιώσουν ή να απορρίψουν μια συναλλαγή. Η βασική ιδέα πίσω από τη τεχνολογία είναι η μεταφορά και επιβεβαίωση της πληροφορίας χωρίς την χρήση μεσαζόντων (Swan 2015).

Οι συναλλαγές είναι κρυπτογραφημένες οπότε κανείς μη εξουσιοδοτημένος δεν μπορεί να έχει πρόσβαση σε πληροφορίες που δεν έχει δικαίωμα. Επιπλέον, από την αλυσίδα απουσιάζει η

κεντρική αρχή. Όλα τα μέλη είναι ισότιμα και κανείς δεν έχει το δικαίωμα να παρεμβαίνει στη λειτουργία της ή να αποκομίζει κέρδος από την λειτουργία της. Τέλος, κάθε μέλος είναι υπεύθυνο να διατηρεί ένα αντίγραφο του συνόλου των εγγραφών ώστε να μπορεί να επιβεβαιώνει τις νέες συναλλαγές, να το ανανεώνει όποτε αυτό κρίνεται απαραίτητο και να αμείβεται για τις υπηρεσίες του αυτές.

3.2 Τρόπος Λειτουργίας

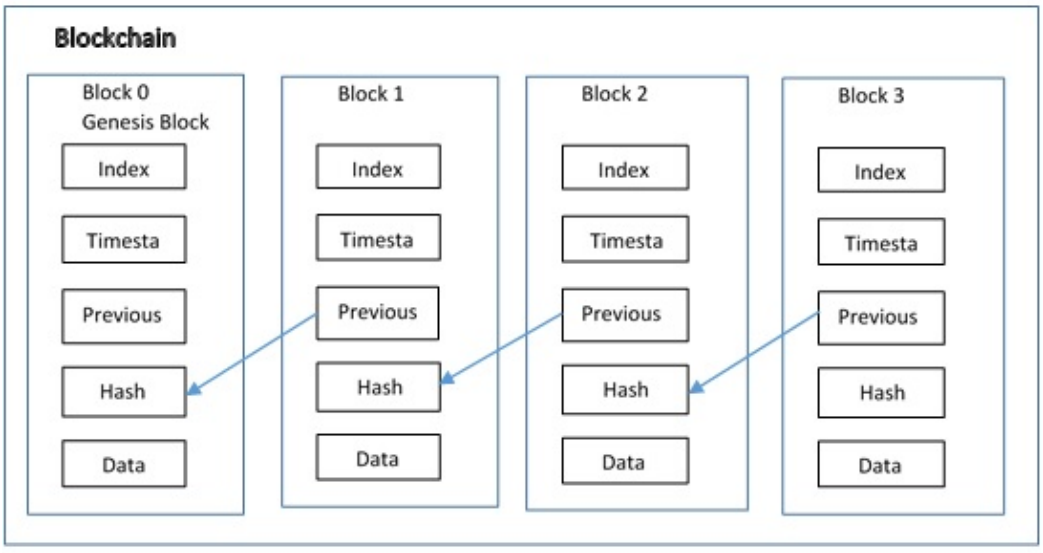
Η λειτουργία της αλυσίδας βασίζεται σε τέσσερα βήματα, την εκτέλεση μιας συναλλαγής, την επιβεβαίωση της από τους συμμετέχοντες, την αποθήκευση της και τέλος την επεξεργασία της από μια συνάρτηση κατακερματισμού.

1. Εκτέλεση της συναλλαγής. Όπως προαναφέρθηκε η συναλλαγή μπορεί να περιλαμβάνει οτιδήποτε έχει αξία, όπως μια αγοροπωλησία, μια μεταφορά χρημάτων κ.α. Στο παράδειγμα μας έχουμε τη μεταφορά χρημάτων μεταξύ των μελών της αλυσίδας.

2. Επιβεβαίωση της συναλλαγής. Για να είναι έγκυρη και αποδεκτή μια συναλλαγή θα πρέπει να επιβεβαιωθεί. Το ρόλο αυτό τον εκτελεί μια ομάδα υπολογιστών που βρίσκονται σε διαφορετικά γεωγραφικά σημεία και όλοι διαθέτουν το σύνολο των συναλλαγών που έχουν γίνει έως τη δεδομένη χρονική στιγμή. Οι υπολογιστές αυτοί ελέγχουν για παράδειγμα εάν το χρηματικό υπόλοιπο του αγοραστή είναι αρκετό και αν ο πωλητής διαθέτει πραγματικά το προς πώληση προϊόν. Η συναλλαγή θεωρείτε έγκυρη μόνο όταν επιβεβαιωθεί από ένα ορισμένο σύνολο υπολογιστών.

3. Αποθήκευση της συναλλαγής. Αφού η συναλλαγή επιβεβαιωθεί και κριθεί ως έγκυρη αποθηκεύεται σε μια μορφή μπλοκ όπου περιέχει διαφορές πληροφορίες ανάλογα με τον τύπο της αλυσίδας που εφαρμόζεται. Μεταξύ των πληροφοριών αυτών είναι η ημερομηνία της εκτέλεσης της, αναγνωριστικά των συμβαλλόμενων, το ύψος του χρηματικού ποσού κ.α. Το μπλοκ αυτό πληροφορίας θα αποσταλεί στη συνέχεια σε όλους τους υπολογιστές της αλυσίδας προκειμένου να αποθηκευτεί. Έτσι ο κάθε υπολογιστής θα μπορεί να ελέγξει την εγκυρότητα μια συναλλαγής κοιτάζοντας το ιστορικό της. Με τον τρόπο αυτό θα μπορεί, στο παράδειγμα μας, να βεβαιώσει ότι όντως ο Β έχει 90 ευρώ αφού πριν είχε 80 και έλαβε από τον Α 10 ευρώ.

4. Εφαρμογή συνάρτησης κατακερματισμού (Hash). Προκειμένου να διασφαλισθεί η ασφάλεια των συναλλαγών θα πρέπει τα μπλοκ της πληροφορίας να μην είναι εφικτό να τροποποιηθούν σε καμία περίπτωση. Γίνεται αντιληπτό στον αναγνώστη ότι αν υπήρχε δυνατότητα σε τρίτο άτομο να τροποποιήσει είτε τα χρηματικά υπόλοιπα αλλά ακόμα και την ημερομηνία μιας συναλλαγής αυτό θα καθιστούσε το όλο σύστημα μη λειτουργικό. Για το λόγο αυτό κάθε φορά που ένα νέο μπλοκ εισάγεται στη λίστα, αυτή εισάγεται σε μια συνάρτηση κατακερματισμού. Οι συναρτήσεις αυτές δέχονται σαν είσοδο ένα σύνολο χαρακτήρων και παράγουν ως αποτέλεσμα μια συμβολοσειρά σταθερού μήκους. Το αποτέλεσμα αυτό παραμένει ίδιο για δεδομένη είσοδο ενώ η παραμικρή αλλαγή στα δεδομένα εισόδου παράγει εντελώς διαφορετικό αποτέλεσμα. Επιπλέον δεν είναι δυνατόν από το αποτέλεσμα να προβλέψει κανείς την αρχική είσοδο. Πριν εισαχθεί λοιπόν ένα μπλοκ στην αλυσίδα, όλη η αλυσίδα δίδεται σε μια συνάρτηση κατακερματισμού και το αποτέλεσμα αυτής εισάγεται στο νέο μπλοκ αφού πρώτα συγκριθεί και ταυτιστεί με αυτά των υπολοίπων υπολογιστών. Έτσι, εάν κάποιος έχει τροποποιήσει κάποιο μπλοκ το αποτέλεσμα της συνάρτησης κατακερματισμού θα είναι διαφορετικό από αυτό των άλλων υπολογιστών και άρα η αλυσίδα αυτή του συγκεκριμένου υπολογιστή θα έχει τροποποιηθεί.



Εικόνα 1: Παράδειγμα αλυσίδας συστοιχιών.

Η παραπάνω εικόνα 1 παρουσιάζει ένα απλοποιημένο αντίγραφο μιας αλυσίδας. Όπως προαναφέρθηκε αποτελείται από ομαδοποιημένες συναλλαγές που αποθηκεύονται με τη σειρά που δημιουργήθηκαν. Όπως μπορούμε να δούμε, το κάθε μπλοκ περιέχει ένα πεδίο Index που είναι ένας μοναδικός αριθμός που ξεχωρίζει το κάθε μπλοκ, ακολούθως ένα πεδίο χρονοσφραγίδας που

δηλώνει την χρονική στιγμή που αποθηκεύτηκε το μπλοκ, το πεδίο Previous Hash που συνδέει το μπλοκ με το προηγούμενο και περιέχει τη τιμή Hash της αλυσίδας έως τώρα, το νέο Hash που θα συνδεθεί με το επόμενο μπλοκ και τέλος το πεδίο Data που περιέχει μια σειρά από συναλλαγές. Το μέγιστο πλήθος των συναλλαγών που μπορούν να συμπεριληφθούν σε ένα μπλοκ εξαρτάται από το μέγεθος του μπλοκ και το μέγεθος της κάθε συναλλαγής.

3.3 Ιστορική Αναδρομή

Η πρώτη αναφορά σε ασφαλή μπλοκ αλυσίδας εντοπίζεται στην επίσημη βιβλιογραφία το 1991 στη εργασία των Stuart Haber και W. Scott Stornetta (Haber, Storneta 1991:99) Με στόχο την βελτίωση της απόδοσης οι Bayer, Haber και Stornetta το 1992 υιοθέτησαν τα δέντρα κατακερματισμού ή αλλιώς Merkle tree στη λειτουργία τις αλυσίδας επιτυγχάνοντας με τον τρόπο αυτό την αύξηση του αριθμού των εγγράφων σε ένα μπλοκ. Στη συνέχεια το 2008 ο Satoshi Nakamoto (Nakamoto 2008) σύστησε στον κόσμο το πρώτο ψηφιακό νόμισμα, το bitcoin λύνοντας με τον τρόπο αυτό το διάσημο μαθηματικό πρόβλημα των Βυζαντινών Στρατηγών. Ένα χρόνο μετά, το 2009, το ψηφιακό νόμισμα υιοθέτησε την τεχνολογία της αλυσίδας. Ο Nakamoto στο έργο του το 2008 χρησιμοποιούσε ξεχωριστά τους όρους μπλοκ και αλυσίδα οι οποίοι τελικά ενοποιήθηκαν το 2016 σε μια λέξη ,Blockchain (Brito, Castillo 2013).

3.4 Το πρόβλημα των Βυζαντινών Στρατηγών

Το πρόβλημα εντοπίζεται για πρώτη φορά στη βιβλιογραφία το 1982 στο έργο των M. Pease, R. Shotstack και L. Lamport (Lamport, Shostak, Pease 1982:382) και αναφέρετε στον τρόπο που μια ομάδα Βυζαντινών Στρατηγών θα οργανώσει την επίθεση της. Οι στρατηγοί βρίσκονται σε διαφορετικές γεωγραφικές τοποθεσίες και ο μόνος τρόπος επικοινωνίας μεταξύ τους είναι η αποστολή μηνυμάτων μέσω αγγελιοφόρων. Οι αγγελιοφόροι όμως αυτοί μπορεί να αιχμαλωτιστούν από τον εχθρό και το μήνυμα που μεταφέρουν να τροποποιηθεί. Επιπλέον δεν είναι όλοι οι στρατηγοί στην ίδια παράταξη. Είναι πιθανόν κάποιος (ή κάποιοι) να έχουν προσεγγισθεί από τον εχθρό και να έχουν αλλάξει πλευρά χωρίς φυσικά οι υπόλοιποι που βασίζονται πάνω τους να το γνωρίζουν. Με αυτά τα δεδομένα όταν ένα στρατηγός στείλει μήνυμα με περιεχόμενο ‘ επίθεση αύριο την αυγή’ ο στρατηγός που θα το λάβει δεν είναι σε θέση να γνωρίζει εάν το μήνυμα αυτό είναι αληθές. Στη περίπτωση που δεν είναι αληθές, είναι πολύ πιθανόν να οδεύει σε παγίδα μιας και η μεμονωμένη επίθεση θα οδηγήσει σε καταστροφή του

στρατού του. Ομοίως όμως και ο στρατηγός που έστειλε το μήνυμα δεν είναι σε θέση να γνωρίζει εάν ο έτερος το έλαβε και θα επιτεθεί ή θα τον εγκαταλείψει.

Με τον ίδιο τρόπο που οι Βυζαντινοί Στρατηγοί δεν ήταν σε θέση να επιβεβαιώσουν την γνησιότητα ενός μηνύματος έτσι και σήμερα οι χρήστες δεν μπορούν να είναι σίγουροι για τη γνησιότητα των μηνυμάτων που λαμβάνουν από τους διάφορους χρήστες του δικτύου. Ο Satoshi Nakamoto πρότεινε να κρυπτογραφείται η πληροφορία, ώστε κανείς μη εξουσιοδοτημένος να μην μπορεί να τη διαβάσει και τα στοιχεία της, που μπορούν να χρησιμοποιηθούν για να βεβαιώσουν την εγκυρότητα της, να είναι διαθέσιμα στον οποιοδήποτε.

3.5 Τα Είδη της Αλυσίδας

Σήμερα, μπορούμε να εντοπίσουμε τρία είδη Αλυσίδας, την δημόσια, την ιδιωτική, και την υβριδική (Buterin 2015).

3.5.1 Η Δημόσια Αλυσίδα

Το είδος του δικτύου αυτού ανήκει στη κατηγορία των προγραμμάτων ανοιχτού κώδικα. Ο οποιοσδήποτε μπορεί να κατεβάσει τον κώδικα στον υπολογιστή του και να μελετήσει τον τρόπο λειτουργίας του. Πέρα όμως από αυτό, ο οποιοσδήποτε μπορεί να συμμετάσχει σε όλες τις διαδικασίες του δικτύου χωρίς κανένα περιορισμό. Δεν υπάρχει κάποια κεντρική αρχή που θα πρέπει να εγκρίνει το νέο μέλος. Ο οποιοσδήποτε μπορεί τη κάθε στιγμή να εγκαταστήσει την αλυσίδα στον υπολογιστή του και με τον τρόπο αυτό να εισαχθεί στο δίκτυο και να επιβεβαιώσει συναλλαγές ή να προσθέσει νέα μπλοκ. Προκειμένου να εξασφαλισθεί η ασφάλεια των συναλλαγών μεταξύ των συμμετεχόντων εφαρμόζονται πρωτόκολλα κοινής συναίνεσης τα οποία εξασφαλίζουν ότι πληρούνται συγκεκριμένες προϋποθέσεις.

3.5.2 Η Ιδιωτική Αλυσίδα

Όπως μαρτυρά και το όνομα της στη περίπτωση αυτή υπάρχει ένα κεντρικός οργανισμός που αποτελείται από μια ομάδα συμμετεχόντων οι οποίοι αποφασίζουν για τα δικαιώματα των υπολοίπων. Με τον τρόπο αυτό κάθε νέο μέλος θα πρέπει να εξασφαλίσει άδεια προκειμένου να ενταχθεί στο δίκτυο και να εκτελέσει συγκεκριμένες λειτουργίες. Πρωτόκολλα κοινής συναίνεσης δεν εφαρμόζονται μιας και υπάρχει εμπιστοσύνη μεταξύ των συμμετασχόντων. Επιπλέον οι

πληροφορίες δεν είναι ορατές από μη εξουσιοδοτημένα άτομα πράγμα που καθιστά το είδος αυτό κατάλληλο για ενδοεταιρική χρήση.

3.5.3 Το Υβριδικό Μοντέλο

Το μοντέλο αυτό συνδυάζει τα πλεονεκτήματα του εποπτευόμενου ιδιωτικού δικτύου με την ασφάλεια και την διαφάνεια του δημοσίου. Έτσι ο οργανισμός μπορεί να επιλέξει ποια δεδομένα θα είναι διαθέσιμα στο κοινό και ποια θα είναι προσβάσιμα μόνο από εξουσιοδοτημένα μέλη. Η λειτουργικότητα της αλυσίδας βελτιώνεται μιας και είναι ευκολότερη η διασύνδεση με έτερα πρωτόκολλα αλυσίδας. Επιπλέον καθίσταται γρηγορότερη η επιβεβαίωση συναλλαγών αφού οι δημόσιες είναι ευκολότερο να επιβεβαιωθούν. Τέλος η διαδικασία της κοινής συναίνεσης εποπτεύεται από μια ομάδα διαπιστευμένων μελών (Buterin 2015). Το μοντέλο αυτό βρίσκει εφαρμογή ιδιαίτερα στον τραπεζικό τομέα όπου διάφορα τμήματα της αλυσίδας χρήζουν διαφορετικό επίπεδο προσβασιμότητας.

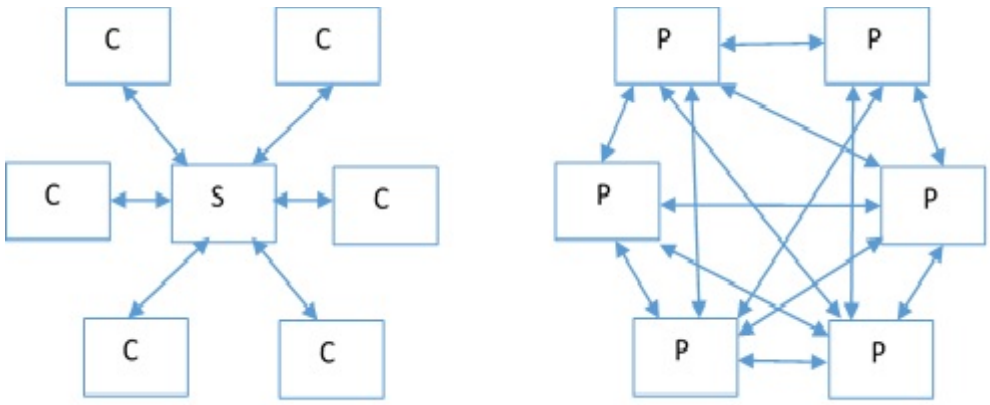
3.6 Τεχνολογίες που Υποστηρίζουν την Αλυσίδα

Η υλοποίηση της αλυσίδας συστοιχιών δεν θα ήταν εφικτή χωρίς την ενσωμάτωση διαφόρων διαφορετικών τεχνολογιών που υποστηρίζουν την λειτουργίας της. Οι υπολογιστές που απαρτίζουν τα μέλη της αλυσίδας θα πρέπει να επικοινωνήσουν μέσω ενός αποκεντρικοποιημένου δικτύου. Επιπλέον τα δεδομένα που διακινούνται μέσω του δικτύου αυτού θα πρέπει να μην μπορούν να αξιοποιηθούν από μη εξουσιοδοτημένα άτομα, δεδομένου ότι δεν αποτελούν όλοι οι κόμβοι του δικτύου των υπολογιστών μέλη του δικτύου της αλυσίδας. Ακολούθως θα πρέπει να διασφαλισθεί ότι τα μπλοκ της αλυσίδας δεν έχουν τροποποιηθεί υποθάλποντας έτσι την αξιοπιστία των συναλλαγών. Τέλος θα πρέπει να εφαρμοστεί μια μέθοδος δόμησης εμπιστοσύνης μεταξύ των συναλλασσόμενων μελών.

3.6.1 Δίκτυο Διασύνδεσης

Για να μπορέσουν να επικοινωνήσουν μια ομάδα από υπολογιστές μεταξύ τους θα πρέπει να είναι συνδεμένοι σε ένα δίκτυο. Τα βασικά μοντέλα που χρησιμοποιούνται είναι αυτό του πελάτη – διακομιστή και το μοντέλο ομότιμων (Peer to Peer). Στη πρώτη περίπτωση υπάρχει ένας υπολογιστής ο οποίος διαθέτει ένα πόρο (πληροφορία ή υπηρεσία) και εκτελεί τον ρόλο του διακομιστή δίνοντας τη δυνατότητα στους υπολογιστές πελάτες να συνδεθούν με αυτόν και να

έχουν πρόσβαση στο πόρο. Ο υπολογιστής διακομιστής θα πρέπει να είναι αρκετά ισχυρός ώστε να μπορεί να εξυπηρετήσει το σύνολο των χρηστών που θα απαιτήσουν την διαθέσιμη υπηρεσία καθώς επίσης και να εξασφαλιστεί ότι θα είναι διαθέσιμος ανά πάσα στιγμή αυτό κριθεί απαραίτητο. Το μοντέλο αυτό δεν εξυπηρετεί το δίκτυο αλυσίδας μιας και από αυτό απουσιάζει η κεντρική διαχείριση, ρόλο τον οποίο εκτελεί ο διακομιστής. Αντί αυτού εφαρμόζετε το μοντέλο Peer to Peer όπου κάθε κόμβος στο δίκτυο διαθέτει το πόρο άλλα έχει εξίσου πρόσβαση στους πόρους των άλλων κόμβων. Στη περίπτωση της αλυσίδας ο πόρος είναι η αλυσίδα των μπλοκ. Κάθε κόμβος διαθέτει το δικό του αντίγραφο και δεν απαιτείται να συνδεθεί σε κάποιο εξυπηρετητή προκειμένου να έχει πρόσβαση στα μπλοκ της αλυσίδας. Επιπλέον, η μέθοδος αυτή εξασφαλίζει ότι το δίκτυο θα είναι πιο αξιόπιστο μιας και η λειτουργία του δεν βασίζεται σε ένα κεντρικό εξυπηρετητή ο οποίος μπορεί να τεθεί έκτος λειτουργίας χωρίς προειδοποίηση. Τέλος είναι αποδοτικότερο μιας και το σύνολο της εργασίας δεν διεκπεραιώνεται από ένα εξυπηρετητή αλλά από κάθε κόμβο εξίσου.



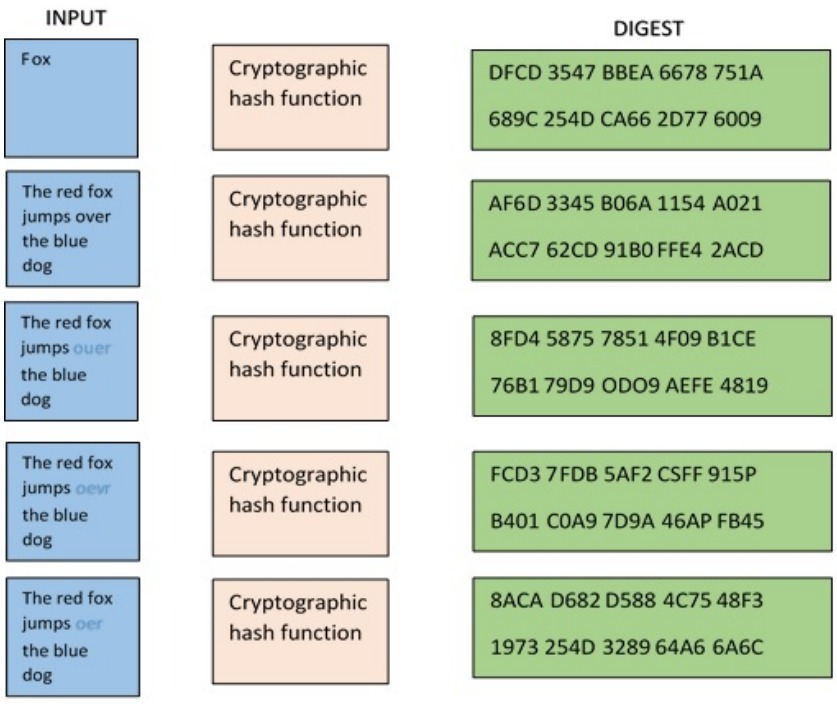
Εικόνα 2: Αρχιτεκτονική server – client στα αριστερά ενώ αρχιτεκτονική Peer to Peer στα δεξιά. **.**

3.6.2 Συνάρτηση Κατατεμαχισμού

Η αλυσίδα συστοιχιών, όπως προαναφέρθηκε, αποτελείται από σειρές ομαδοποιημένων συναλλαγών. Για το είδος της σύνδεσης των συναλλαγών αυτών επιλέχτηκε αυτό της αλυσίδας, εξου και ο όρος αλυσίδα συστοιχιών. Αυτό είναι λογικό διότι εάν η αλυσίδα ‘σπάσει’, αν τροποποιηθεί δηλαδή η σειρά των συναλλαγών ή οποιοδήποτε άλλο στοιχείο της συναλλαγής, αυτομάτως το σύστημα καταρρέει. Πιο συγκεκριμένα, η όλη ιδέα βασίζεται στο γεγονός ότι από τη στιγμή που μια συναλλαγή εισαχθεί στην αλυσίδα είναι αδύνατον να τροποποιηθεί κατά

κανένα τρόπο. Η μέθοδος για να εξασφαλιστεί η μη μεταβλητότητα είναι η συνάρτηση κατατεμαχισμού ή αλλιώς συνάρτηση κατακερματισμού.

Η συνάρτηση αυτή είναι μια μαθηματική συνάρτηση που δέχεται σαν είσοδο δεδομένα οποιουδήποτε μεγέθους και παράγει μια σειρά από δεδομένα σταθερού μήκους ανάλογα με το είδος συνάρτησης που χρησιμοποιείται, από 32bit έως 256bit ή και περισσότερα. Η συνάρτηση για ίδια είσοδο θα παράγει πάντα τα ίδια δεδομένα στην έξοδο ενώ μια μικρή αλλαγή στην είσοδο θα παράξει μια εντελώς διαφορετική έξοδο. Επίσης είναι πρακτικά αδύνατον να μαντέψει κανείς τα δεδομένα της εισόδου από τα δεδομένα της εξόδου.



Εικόνα 3: Παράδειγμα λειτουργίας συνάρτησης κατακερματισμού. Ίδια είσοδος παράγει ίδια έξοδο ενώ η παραμικρή αλλαγή στην είσοδο παράγει εντελώς διαφορετικό αποτέλεσμα.

Στην αλυσίδα συστοιχιών κάθε φορά που εισάγεται ένα νέο μπλοκ η όλη αλυσίδα εισάγεται σε μια συνάρτηση κατακερματισμού και κατόπιν όλοι οι κόμβοι ελέγχουν το αποτέλεσμα. Εάν κάποιος κόμβος έχει διαφορετικό αποτέλεσμα αυτό αυτομάτως σημαίνει ότι η αλυσίδα του κόμβου αυτού έχει παραβιαστεί σε κάποιο σημείο της και άρα δεν θεωρείτε πλέον αξιόπιστος. Με τον τρόπο αυτό εξασφαλίζεται ότι οι συναλλαγές που έχουν αποθηκευτεί δεν μπορούν να τροποποιηθούν αφού η παραμικρή τροποποίηση θα γίνεται άμεσα αντιληπτή από τους υπόλοιπους κόμβους της ομάδας.

3.6.3 Κρυπτογράφηση Πληροφορίας

Τα δεδομένα που διακινούνται μέσω ενός δικτύου υπολογιστών αρχικά είναι ανοικτά, οποιοσδήποτε στο δίκτυο μπορεί να τα διαβάσει. Για το λόγο αυτό θα πρέπει να μετασχηματισθούν πριν εισέρθουν στο δίκτυο σε μια μορφή που να μην επιτρέπουν σε μη εξουσιοδοτημένα άτομα να καταλάβουν τι περιέχουν. Αυτό επιτυγχάνεται με την κρυπτογράφηση του μηνύματος μέσω της οποίας το αρχικό μήνυμα μετασχηματίζεται σε μια ακολουθία συμβόλων από τα οποία δεν είναι εφικτό να παραχθεί το αρχικό μήνυμα από μη εξουσιοδοτημένα άτομα. Πιο αναλυτικά με την κρυπτογραφία μπορούμε να επιτύχουμε τέσσερις αντικειμενικούς σκοπούς:

1. Εμπιστευτικότητα: Όπως προαναφέρθηκε, μέσω της εμπιστευτικότητας εξασφαλίζεται ότι μόνο εξουσιοδοτημένα μέλη θα έχουν πρόσβαση στη πληροφορία. Στο ευρύ κοινό δεν θα βγάζει κάποιο νόημα.

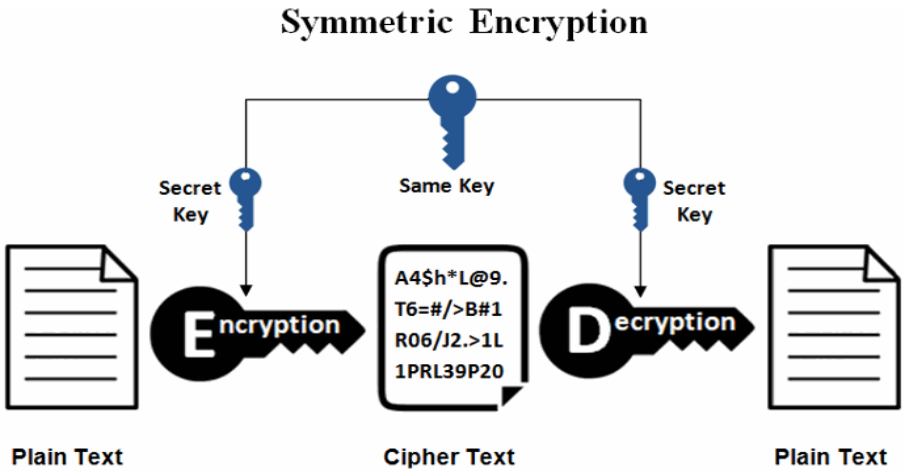
2. Ακεραιότητα: Η πληροφορία δεν μπορεί να τροποποιηθεί παρά μόνο από εξουσιοδοτημένα άτομα και επιπλέον η τροποποίηση αυτή είναι ανιχνεύσιμη.

3. Μη απάρνηση: Ο αποστολέας ή ο παραλήπτης της πληροφορίας δεν μπορεί να αρνηθεί την δημιουργία ή τη μετάδοση της πληροφορίας.

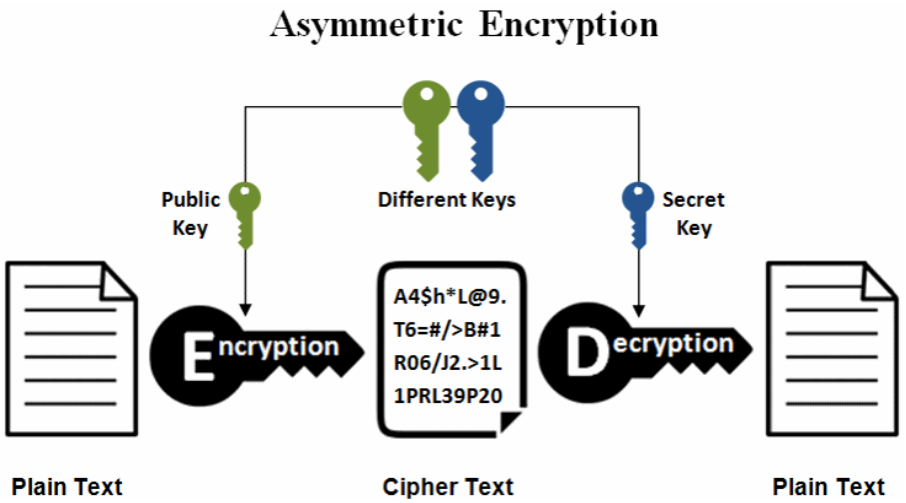
4. Πιστοποίηση: Τόσο ο αποστολέας όσο και ο παραλήπτης μπορούν να εξακριβώσουν τις ταυτότητές τους.

Για να κρυπτογραφηθεί ένα κείμενο απαιτείται ένας ‘κωδικός’, βάσει του οποίου θα γίνει η κρυπτογράφηση και η αποκρυπτογράφηση του κειμένου. Ο κωδικός αυτός ονομάζεται κλειδί κρυπτογράφησης και ουσιαστικά περιγράφει τον τρόπο με τον οποίο θα γίνει ο μετασχηματισμός του κειμένου. Οπότε, ο αποστολέας του μηνύματος κρυπτογραφεί το μήνυμα με το κλειδί και το αποστέλλει στον αποδέκτη. Οι ενδιάμεσοι κόμβοι μη γνωρίζοντας τον τρόπο με τον οποίο έχει γίνει ο μετασχηματισμός του μηνύματος, μην έχοντας το κλειδί δηλαδή, δεν είναι σε θέση να επαναφέρουν το μήνυμα στην αρχική του μορφή και να το διαβάσουν. Αντίθετα το αποδέκτης διαθέτει το κλειδί και μπορεί να αποκρυπτογραφήσει το μήνυμα. Η μέθοδος αυτή, που ονομάζεται συμμετρική κρυπτογραφία, παρουσιάζει σαν δυσκολία το πώς θα μεταφερθεί το κλειδί. Είναι προφανές ότι δεν μπορεί να σταλεί μέσω δικτύου διότι οποιοσδήποτε κόμβος θα μπορεί να το λάβει και στη συνέχεια να αποκρυπτογραφεί τα μηνύματα.

Το πρόβλημα αυτό της συμμετρικής κρυπτογράφησης έρχεται να λύσει η άλλη μορφή κρυπτογράφησης που ονομάζεται ασύμμετρη κρυπτογράφηση. Στην ασύμμετρη υπάρχουν δύο κλειδιά, ένα δημόσιο και ένα ιδιωτικό. Κάθε μέλος της επικοινωνίας παράγει το δικό του ιδιωτικό κλειδί το οποίο θα πρέπει να παραμένει κρυφό καθώς και ένα δεύτερο κλειδί το οποίο ονομάζεται δημόσιο και δεν χρειάζεται να μένει κρυφό. Τώρα, όταν ένας χρήστης θέλει να στείλει ένα μήνυμα το κρυπτογραφεί με το δημόσιο κλειδί του αποδέκτη. Το μήνυμα αυτό μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό κλειδί του αποδέκτη. Με τον τρόπο αυτό λύνεται το πρόβλημα της συμμετρικής κρυπτογραφίας μιας και τα δημόσια κλειδιά μπορούν να κυκλοφορούν ελευθέρα στο δίκτυο ενώ τα ιδιωτικά παραμένουν κρυφά. Επιπλέον ο αποδέκτης του μηνύματος, με τον τρόπο αυτό, μπορεί να είναι σίγουρος για την ταυτότητα του αποστολέα. Όπως είναι αναμενόμενο η τεχνολογία αλυσίδας χρησιμοποιεί ασύμμετρη κρυπτογράφηση για να κρυπτογραφεί τα διάφορα μηνύματα που αποστέλλονται στο δίκτυο.



Εικόνα 4: Συμμετρική κρυπτογράφηση. Για την κρυπτογράφηση αλλά και την αποκρυπτογράφηση απαιτείται το ίδιο κλειδί. Πηγή:https://wizardforcel.gitbooks.io/practical-cryptography-for-developers-book/encryption-symmetric-and-asymmetric.html



Εικόνα 5: Ασύμμετρη κρυπτογράφηση. Η κρυπτογράφηση πραγματοποιείται με το δημόσιο κλειδί του αποδέκτη ενώ η αποκρυπτογράφηση με το ιδιωτικό του. Πηγή:https://wizardforcel.gitbooks.io/practical-cryptography-for-developers-book/encryption-symmetric-and-asymmetric.html

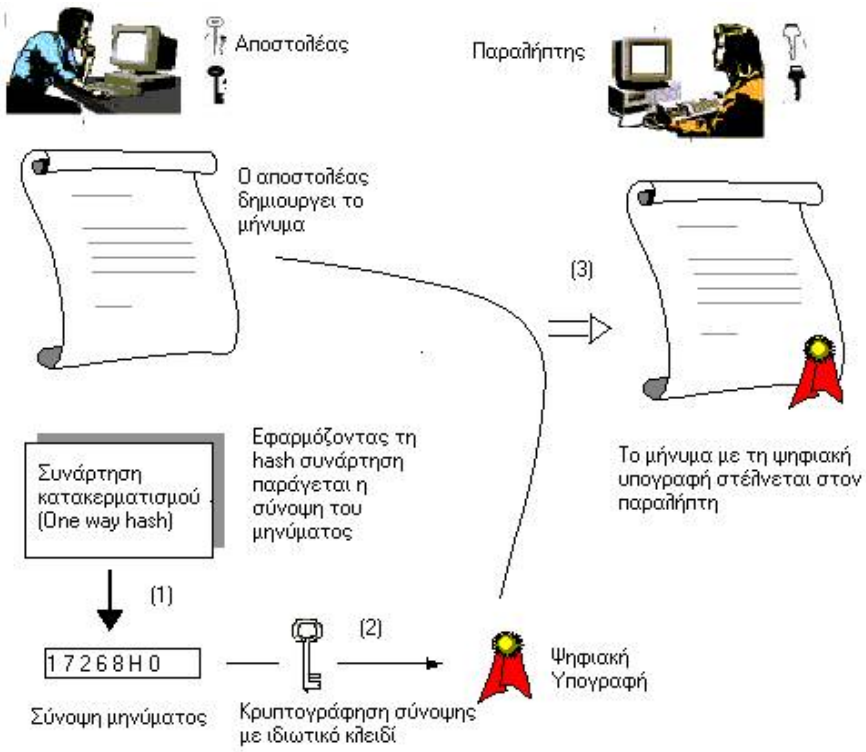
3.6.4 Ψηφιακές Υπογραφές

Πέρα όμως από την κρυπτογράφηση των μηνυμάτων εξίσου απαραίτητη λειτουργία είναι και η ταυτοποίηση των μελών του δικτύου της αλυσίδας. Τα πραγματικά στοιχεία της ταυτότητας των ατόμων πιθανόν να μην είναι απαραίτητα, όπως άλλωστε δεν είναι γνωστά και τα πραγματικά στοιχεία του Satoshi Nakamoto, θα πρέπει όμως με κάποιο τρόπο κάθε μέλος της ομάδας να αποκτά ένα είδος ταυτότητας που θα το ξεχωρίζει από τα υπόλοιπα μέλη και η ταυτότητα αυτή να μην μπορεί να κλαπεί ώστε να χρησιμοποιηθεί από άλλο μέλος. Είναι απαραίτητη η λειτουργία αυτή γιατί τα μέλη της αλυσίδας είτε διαθέτουν περιουσιακά στοιχεία εντός της αλυσίδας είτε αμείβονται για τις υπηρεσίες τους. Οπότε κρίνεται απαραίτητο να ταυτοποιηθούν ώστε τα χρήματα να μεταφέρονται στα σωστά άτομα και να μην μπορεί κάποιος κακόβουλος να υιοθετήσει την ταυτότητα άλλου μέλους και να αποκομίσει με τον τρόπο αυτό τα χρήματα που του αναλογούν.

Στην αλυσίδα συστοιχιών το πρόβλημα αυτό αντιμετωπίζεται με τη χρήση των ψηφιακών υπογραφών. Μέσω της ψηφιακής υπογραφής ο χρήστης χρησιμοποιεί το ιδιωτικό του κλειδί και υπογράφει βεβαιώνοντας με τον τρόπο αυτό την ταυτότητα του αφού το κλειδί αυτό ανήκει μόνο σε αυτόν. Ποιο συγκεκριμένα, ο χρήστης εισάγει το κείμενο σε μια συνάρτηση κατακερματισμού και ακολούθως το αποτέλεσμα μαζί με το ιδιωτικό κλειδί του τα εισάγει στον αλγόριθμο της ψηφιακής υπογραφής. Το αποτέλεσμα της διαδικασίας είναι ένα ψηφιακά υπογεγραμμένο

κείμενο. Ο παραλήπτης του κειμένου για να βεβαιώσει τη γνησιότητα του εγγράφου εισάγει το κείμενο στη συνάρτηση κατακερματισμού και λαμβάνει το αποτέλεσμα. Ακολούθως εισάγει το δημόσιο κλειδί και την υπογραφή στον αλγόριθμο κρυπτογράφησης και λαμβάνει το αποτέλεσμα. Εάν αυτό ταυτίζετε με αυτό της συνάρτησης κατακερματισμού τότε μπορεί να είναι βέβαιος ότι το κείμενο έχει υπογραφεί από το άτομο που υποστηρίζει ότι το υπόγραψε.

Μια αδυναμία του συστήματος είναι ότι ο αποδέκτης δεν μπορεί να είναι σίγουρος για το δημόσιο κλειδί μιας και αυτό είναι δημόσιο και δεν μπορεί να είναι σίγουρος ότι ανήκει στο άτομο που υποστηρίζει ότι του ανήκει. Για το λόγο αυτό έχουν συσταθεί οργανισμοί οι οποίοι καλούνται πάροχοι υπηρεσιών πιστοποίησης, οι οποίοι πιστοποιούν τη σχέση ενός ανθρώπου με το δημόσιο κλειδί του.



Εικόνα 6: Διαδικασία χρήσης ψηφιακής υπογραφής. Πηγή:https://www.eett.gr/opencms/opencms/EETT/Electronic Communications/DigitalSignatures/IntroEsign.html

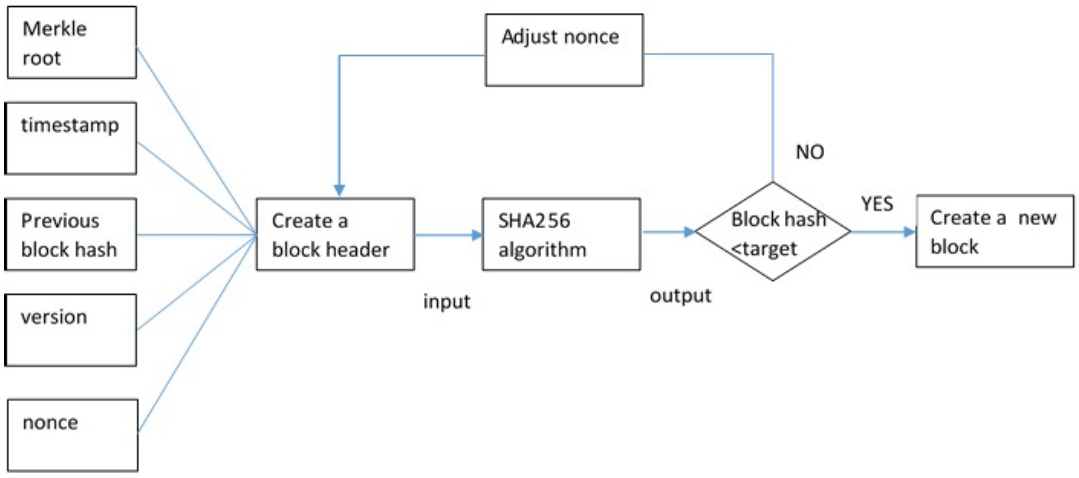
3.6.5 Πρωτόκολλα Συναίνεσης

Μία από τις σημαντικότερες προκλήσεις της αλυσίδας συστοιχιών ήταν ότι τόσο οι χρήστες της θα συμπεριφέρονται σύμφωνα με τους κανόνες της αλυσίδας όσο και η αλυσίδα θα τους αντιμετωπίζει όπως πρέπει. Ποιο συγκεκριμένα λόγω του ότι στην αλυσίδα μπορεί να συμμετάσχει όποιος επιθυμεί θα πρέπει να εφαρμοστούν κανόνες ώστε τα μέλη να προστατεύονται από κακόβουλα ή απρόσεκτα μέλη. Επιπλέον η αλυσίδα από την πλευρά της θα πρέπει να αμείβει δίκαια τα μέλη για τις υπηρεσίες τους φροντίζοντας φυσικά για την αποδοτικότερη διαχείριση τους. Τίθεται λοιπόν το πρόβλημα της εμπιστοσύνης τόσο μεταξύ των μελών όσο και μεταξύ των μελών και της αλυσίδας.

Σε ένα δίκτυο τύπου πελάτη – εξυπηρετητή το πρόβλημα αυτό αντιμετωπίζεται εύκολα λόγω του ότι ο πόρος που οι πελάτες χρειάζονται βρίσκεται αποκλειστικά στον εξυπηρετητή. Όσο ο πόρος είναι αυτός που πρέπει να είναι, οι πελάτες εμπιστεύονται τον εξυπηρετητή και χρησιμοποιούν τον πόρο. Αν αυτό διαρραγεί με κάποιο τρόπο και ο πόρος πάψει να είναι αυτός που οι πελάτες χρειάζονται τότε αυτοί απλά θα στραφούν σε άλλον εξυπηρετητή έχοντας τη δυνατότητα ακόμη και να αποζημιωθούν από τον ιδιοκτήτη του εξυπηρετητή για τη ζημιά που πιθανών προκλήθηκε. Από την άλλη πλευρά οι πελάτες έχουν περιορισμένα δικαιώματα στο εξυπηρετητή και δεν μπορούν να τον βλάψουν. Στη περίπτωση της αλυσίδας όμως ο πόρος, τα μπλοκ, είναι εξίσου κατανεμημένα στους χρήστες και δεν υπάρχει κάποια αρχή που εποπτεύει την όλη διαδικασία. Καθίσταται λοιπόν προφανές ότι θα πρέπει να εφαρμοστεί κάποιος μηχανισμός που να ελέγχει όλους τους κόμβους ώστε να μπορεί να υπάρξει εμπιστοσύνη μεταξύ τους (Kraft 2016:397). Επιπλέον κάθε φορά που προκύπτει μια συναλλαγή θα πρέπει οι κόμβοι να την επεξεργαστούν και να την αποθηκεύσουν. Η αλυσίδα από την πλευρά της θα πρέπει να ξεχωρίσει τους κόμβους που έκαναν σωστά τη διαδικασία και να τους ανταμείψει.

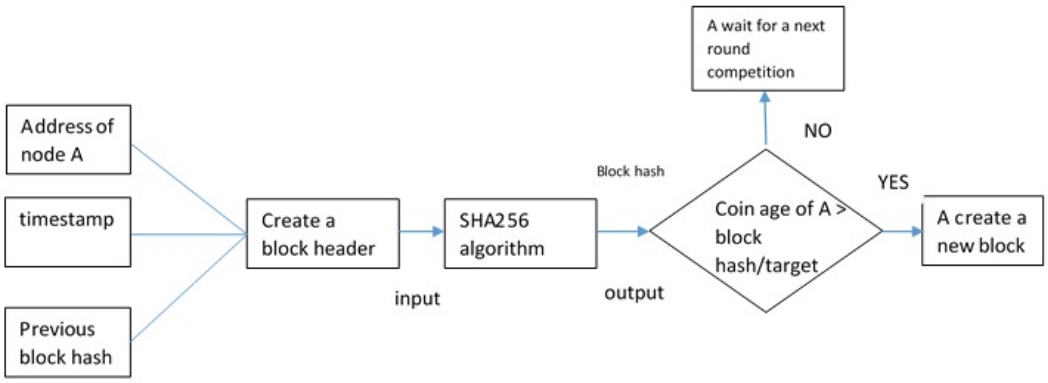
Το πρόβλημα αυτό έρχονται να το αντιμετωπίσουν τα πρωτόκολλα συναίνεσης. Μέσω των μηχανισμών αυτών μπορούμε να ελέγξουμε την εργασία των κόμβων του δικτύου και να αποφασίσουμε ποια ή ποιες από αυτές έγιναν σωστά. Τα πρωτόκολλα αυτά έχουν τη δυνατότητα να πράξουν ικανοποιητικά αποτελέσματα ακόμη και αν μεταξύ των κόμβων υπάρχουν κακόβουλοι που μας παραδίδουν ενσυνείδητα λανθασμένα αποτελέσματα ή δεν έχουν τη δυνατότητα να εκτελέσουν σωστά τις διαδικασίες ή ακόμα και αν τμήμα των κόμβων έχει τεθεί εκτός λειτουργίας.

Ένα από τα πλέον χρησιμοποιούμενα πρωτόκολλα συναίνεσης είναι αυτό της απόδειξης εργασίας (Proof Of Work). Είναι ιδιαίτερα απαιτητικό σε υπολογιστικούς πόρους και ενέργεια, έχει αποδειχθεί όμως ασφαλές και αποδοτικό (Tedeschi, Nordmo, Johansen, Johansen 2019:4223). Το πρωτόκολλο αυτό, στο οποίο βασίζονται το Bitcoin, το Ethereum κ.α. αναθέτει σε κόμβους να εκτελέσουν μια διαδικασία απαιτητική σε υπολογιστικούς πόρους, να λύσουν ένα κρυπτογραφικό πάζλ. Το πάζλ αυτό γίνεται ολοένα και δυσκολότερο όσο αυξάνεται το μέγεθος της αλυσίδας. Για να το λύσει ο κόμβος θα πρέπει να διαθέσει υπολογιστική ισχύ η οποία φυσικά μεταφράζεται σε δέσμευση υπολογιστών και κατανάλωση ηλεκτρικής ενέργειας. Ο κόμβος ο οποίος πρώτος λύνει το πάζλ επιβραβεύεται, εξουσιοδοτώντας τον να αποθηκεύσει το νέο μπλοκ της αλυσίδας. Για να μπορέσει ένας κακόβουλος χρήστης να εισάγει ένα παραποιημένο μπλοκ στην αλυσίδα θα πρέπει να λύσει ένα αρκετά δύσκολο πάζλ πράγμα που καθιστά το όλο εγχείρημα μη ανταποδοτικό.



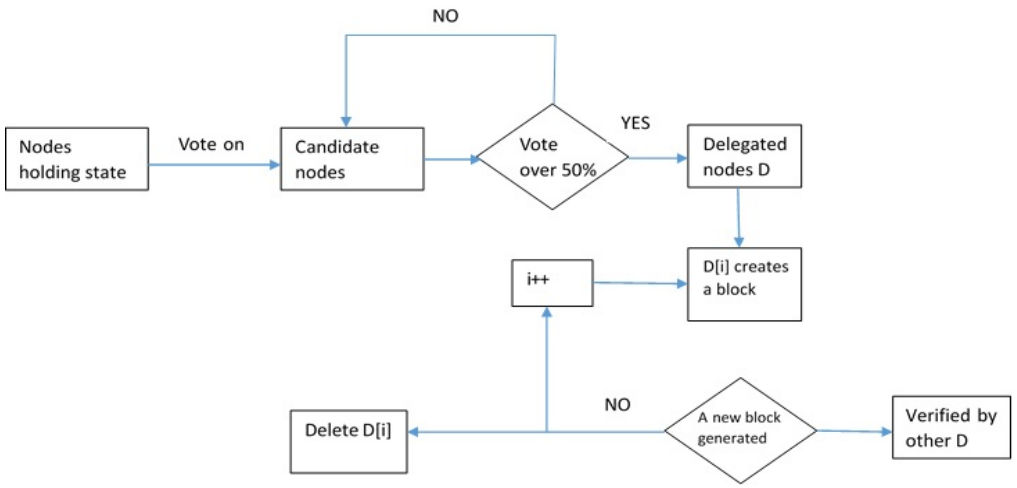
Εικόνα 7: Η λειτουργία του πρωτοκόλλου απόδειξη εργασίας. Ο πρώτος κόμβος που θα παράξει επιτυχώς το νέο μπλοκ επιβραβεύεται.

Το πρωτόκολλο απόδειξης εργασίας έχει αποδειχθεί ιδιαίτερα ενεργοβόρο λόγω των αυξημένων απαιτήσεων σε ενέργεια. Αυτός ήταν ένας από τους λόγους που οδήγησαν στο πρωτόκολλο απόδειξης κατάστασης (Proof Of Stake), στο οποίο την επιβράβευση λαμβάνει ο κόμβος που θα λύσει πρώτος το παζλ αλλά έχει και τα περισσότερα χρήματα. Ο βαθμός δυσκολίας του πάζλ στη περίπτωση του πρωτοκόλλου αυτού δεν αυξάνεται ανάλογα με το μέγεθος της αλυσίδας αλλά εξαρτάται από την ποσότητα αλλά και την ηλικία των νομισμάτων. Το πρωτόκολλο λειτουργεί τόσο καλά που το Ethereum προγραμματίζει την υιοθέτηση του ενώ άλλες αλυσίδες το χρησιμοποιούν ήδη (Nxt, Ouroboros, κ.α.)



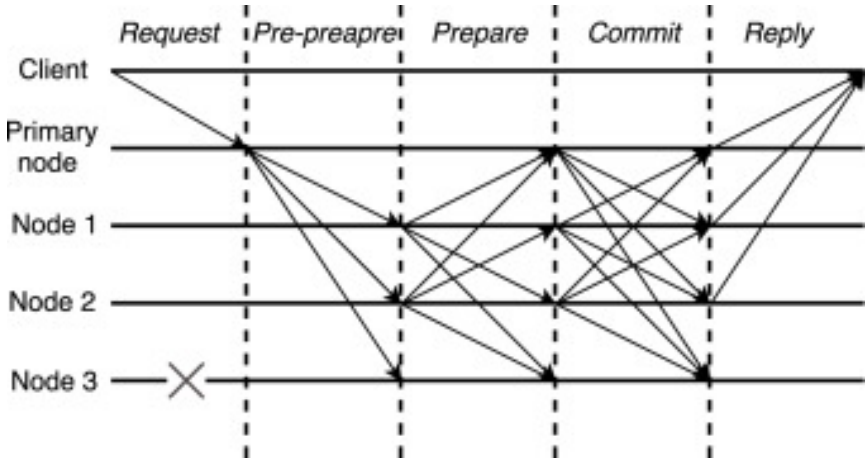
Εικόνα 8: Η λειτουργία του πρωτοκόλλου απόδειξης κατάστασής. Στην επιλογή του κόμβου λαμβάνεται υπόψη το σύνολο των νομισμάτων που διαθέτει και η ηλικία τους.

Μια διαφορετική εκδοχή του πρωτοκόλλου είναι αυτή της ανατιθεμένης απόδειξης κατάστασης (Delegated Proof of Stake). Στην εκδοχή αυτή διακεκριμένα μέλη, που διαθέτουν αρκετό αριθμό νομισμάτων, ψηφίζουν και αποφασίζουν από κοινού σε ποιους κόμβους θα αναθέσουν τη διαδικασία δημιουργίας νέου μπλοκ έτσι ώστε αυτοί να απαλλάσσονται από την υποχρέωση να καταναλώνουν υπολογιστικούς πόρους, μειώνοντας έτσι τα κόστη τους (Vasin 2014). Με τον τρόπο αυτό απαιτούνται νομίσματα για να δημιουργηθεί το νέο μπλοκ και όχι ενέργεια ((Buterin 2014). Αν ο εκλεγμένος κόμβος δεν καταφέρει να δημιουργήσει το νέο μπλοκ απαλλάσσεται και η διαδικασία επαναλαμβάνεται. Με τον τρόπο αυτό η διαδικασία διανομής της εργασίας είναι πλέον δικαιότερη, με μειωμένο το κόστος της λειτουργίας και περισσότερο αποδοτική.



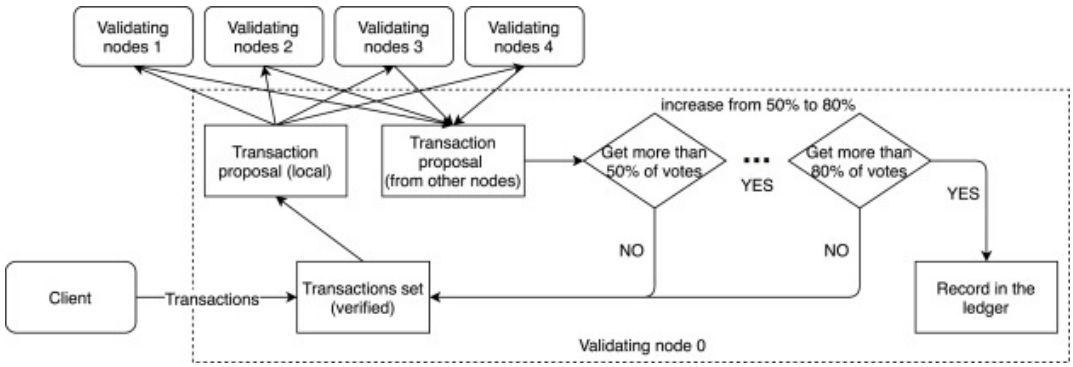
Εικόνα 9: Διάγραμμα λειτουργίας του πρωτοκόλλου ανατιθέμενης απόδειξης κατάστασης. Ο κόμβος που θα αποπειραθεί να δημιουργήσει το νέο μπλοκ προκύπτει κατόπιν ψηφοφορίας.

Το πρωτόκολλο Πρακτικής Βυζαντινής Ανεκτικότητας (Practical Byzantine Fault Tolerance) λαμβάνει ευρεία αποδοχή λόγω της χαμηλής πολυπλοκότητας και της υψηλής πρακτικότητας που διαθέτει. Διαφέρει από τις άλλες προσεγγίσεις στο ότι η όλη διαδικασία βασίζεται στην ανταλλαγή μηνυμάτων. Περιλαμβάνει πέντε φάσεις, την αίτηση, την προετοιμασία, την ετοιμασία, τη πράξη και τέλος την απάντηση. Ειδικότερα ένας κόμβος προωθεί το μήνυμα προς αποστολή σε άλλους τρείς κόμβους. Στη περίπτωση που κάποιος από τους τρεις έχει τεθεί εκτός υπηρεσίας το μήνυμα θα πρέπει να περάσει από τις πέντε προαναφερθείσες φάσεις ώστε να επιτευχθεί η συναίνεση μεταξύ των κόμβων αυτών οι οποίοι τελικά απαντούν στον αρχικό αποστολέα.



Εικόνα 10: Περιγραφή λειτουργίας του πρωτοκόλλου. Στη περίπτωση που κόμβος έχει τεθεί εκτός υπηρεσίας οι γειτονικοί του ενημερώνουν. Πηγή: https://www.sciencedirect.com/science/article/pii/S240595951930164X

Κλείνοντας, θα αναφερθούμε στο πρωτόκολλο Ripple το οποίο ανήκει στη κατηγορία των πρωτοκόλλων ανοιχτού κώδικα. Σύμφωνα με το πρωτόκολλο αυτό, οι συναλλαγές που ξεκινούν από τους πελάτες τις αλυσίδας μεταδίδονται στους κόμβους του δικτύου μέσω ειδικών σταθμών που καλούνται επικυρωτές (Validators). Οι σταθμοί αυτοί διαθέτουν μια λίστα έμπιστων άλλων σταθμών στους οποίους στέλνουν τις συναλλαγές που προτείνουν ότι είναι σωστές και θα πρέπει να αποθηκευτούν. Ακολούθως, οι σταθμοί που λαμβάνουν τις συναλλαγές ελέγχουν τις τοπικές τους αλυσίδες ώστε να αποφανθούν για την γνησιότητα τους. Ακολούθως οι σταθμοί αυτοί ψηφίζουν για να εκλέξουν ποιες από αυτές μπορούν να αποθηκευτούν. Οι συναλλαγές που αποσπούν το 50% των ψήφων αποθηκεύονται, ενώ το ποσοστό αυτό αυξάνεται σε κάθε γύρο. Τέλος, οι κόμβοι χωρίζονται σε δύο βασικές κατηγορίες, αυτούς που συμμετέχουν στην διαδικασία συναίνεσης και σε αυτούς που εκτελούν τις συναλλαγές.



Εικόνα 11:Διαδικασία επιβεβαίωσης συναλλαγών μέσω του πρωτοκόλλου Ripple.

Property	PoW	PoS	DPoS	PBFT	Ripple
Type	Probabilistic-finality	Probabilistic-finality	Probabilistic-finality	Absolute-finality	Absolute-finality
Fault tolerance	50%	50%	50%	33%	20%
Power consumption	Large	Less	Less	Negligible	Negligible
Scalability	Good	Good	Good	Bad	Good
Application	Public	Public	Public	Permissioned	Permissioned

Πίνακας 1:Σύγκριση των περιγραφόμενων πρωτοκόλλων. Πηγή: https://www.sciencedirect.com/science/article/pii/S240595951930164X

Κεφάλαιο 4
Έξυπνα συμβόλαια

Στο κεφάλαιο αυτό θα αναφερθούμε σε μια ιδιαίτερα σημαντική λειτουργία της αλυσίδας συστοιχιών, τα έξυπνα συμβόλαια. Η λειτουργία αυτή, παρόλο που σαν ιδέα είναι αρκετά παλαιά, αποτελεί μια από τις τελευταίες προσθήκες στη τεχνολογία αλυσίδας συστοιχιών. Δεν την υποστηρίζουν όλες οι πλατφόρμες, πρόκειται όμως για μια πολλά υποσχόμενη λειτουργία που εισάγει τη τεχνολογία αλυσίδας σε νέους τομείς.

4.1 Περιγραφή

Τα έξυπνα συμβόλαια είναι προγράμματα τα οποία είναι αποθηκευμένα στην αλυσίδα και εκτελούνται αυτόματα όταν οι προκαθορισμένοι όροι τηρηθούν. Οι όροι αυτοί μπορεί να είναι σχεδόν οτιδήποτε, μια ημερομηνία, μια αλλαγή σε κάποιο υπόλοιπο ενός λογαριασμού, η επιτυχημένη ολοκλήρωση μιας δραστηριότητας και άλλα. Για παράδειγμα ένα έξυπνο συμβόλαιο θα μπορούσε να μεταφέρει ένα χρηματικό ποσό σε κάποιο νεαρό την ημέρα την ενηλικίωσης του σαν δώρο από τους συγγενείς του. Οι συγγενείς απλά καταθέτουν το ποσό και ορίζουν την ημερομηνία ενηλικίωσης. Το πρόγραμμα που υλοποιεί το έξυπνο συμβόλαιο παρακολουθεί το χρόνο και μόλις φτάσει η προκαθορισμένη ημερομηνία μεταφέρει το κατατιθέμενο ποσό χωρίς να απαιτείτε ανθρώπινη παράβαση.

Ένα έξυπνο συμβόλαιο θα μπορούσε να περιγράφει σαν μια συμφωνία μεταξύ μιας ομάδας ανθρώπων όπως ακριβώς και σε ένα πραγματικό συμβόλαιο. Θα μπορούσε να αναφέρει τις υποχρεώσεις που αναλαμβάνουν να τηρήσουν τα εμπλεκόμενα μέλη, τα οφέλη που θα προκληθούν καθώς και τις ποινές που θα πρέπει να επιβληθούν σε περίπτωση που κάποιος όρος παραβιαστεί από κάποιο μέλος. Στη περίπτωση του έξυπνου συμβολαίου η επιβολή ποινής για την μη τήρηση κάποιου όρου δεν απαιτεί, όπως στα πραγματικά συμβόλαια, την προσφυγή σε κάποιο δικαστήριο αλλά επιβάλλεται αυτομάτως από το λογισμικό. Το λογισμικό αυτό που έχει γραφεί σε κάποια γλώσσα προγραμματισμού, εκτελείται με την ενεργοποίηση του συμβολαίου και περιμένει την πρόκληση ενός συμβάντος, όπως ακριβώς ένας εξυπηρετητής περιμένει ένα πελάτη

να συνδεθεί πάνω του για να του διαθέσει κάποιο πόρο. Μόλις το συμβάν λάβει χώρα τότε το συμβόλαιο εκτελεί την ενέργεια που του έχει οριστεί.

4.2 Προέλευση του όρου

Η ιδέα πρωτοπαρουσιάστηκε την δεκαετία του 90 από τον Nick Szabo ο οποίος επινόησε τον όρο σε μια προσπάθεια να μεταφέρει τις εξελιγμένες πρακτικές των νομικών συμβολαίων στον ανερχόμενο κόσμο του ηλεκτρονικού εμπορίου και του διαδικτύου. Στη πραγματικότητα δεν πρόκειται για έξυπνα προγράμματα αλλά βασικά, που απλά ορίζουν ότι αν γίνει κάτι τότε πρέπει να γίνει κάτι άλλο.

4.3 Σχέση έξυπνων συμβολαίων με την αλυσίδα

Τα έξυπνα συμβόλαια δεν μπορούν να λειτουργήσουν εκτός της αλυσίδας συστοιχιών γιατί μόνο μέσω αυτής μπορούν τα συναλλασσόμενα μέλη να είναι σίγουρα ότι αυτά θα τηρηθούν. Η τεχνολογία της αλυσίδας μπορεί να εγγυηθεί ότι κανείς δεν θα τροποποιήσει κάποιο συμβόλαιο και πολλά μέλη της αλυσίδας θα πρέπει να πιστοποιήσουν ότι οι αναφερόμενοι όροι έχουν τηρηθεί προτού το πρόγραμμα προχωρήσει στην εκτέλεση του.

4.4 Βασικά χαρακτηριστικά

Βασικά χαρακτηριστικά των έξυπνων συμβολαίων είναι η ντετερμινιστικότητα, η εξασφάλιση ότι δεν μπορούν να τροποποιηθούν και τέλος η δυνατότητα να επαληθεύονται. Τα προγράμματα επιβάλλεται να είναι ντετερμινιστικά και να παράγουν ακριβώς το ίδιο αποτέλεσμα από όλους τους κόμβους ανεξαρτήτως ώστε να έχει νόημα η εκτέλεση τους. Επιπλέον, όπως έχει προαναφερθεί θα πρέπει να είναι ασφαλισμένα από οποιοδήποτε είδος τροποποίησης ώστε οι συμβαλλόμενοι να είναι ασφαλείς. Τέλος, θα πρέπει όσο το δυνατόν ευκολότερα ο οποιοσδήποτε κόμβος να μπορεί να ελέγξει το αποτέλεσμα.

4.5 Περιγραφή λειτουργίας

Η λειτουργία του έξυπνου συμβολαίου μπορεί να περιγραφεί μέσα από τρία βήματα. Αρχικά γίνεται ο προσδιορισμός των όρων και η οργάνωση αυτών μέσα σε ένα πρόγραμμα. Το πρόγραμμα θα πρέπει να εκτελεί αυτό που τα μέλη έχουν ορίσει σωστά και με ακρίβεια εφόσον οι όροι πληρούνται. Ακολούθως, το πρόγραμμα κρυπτογραφείται και αποστέλλεται στους προκαθορισμένους κόμβους του δικτύου οι οποίοι το εντάσσουν στην αλυσίδα τους. Τέλος, όταν συμβεί κάποιο συμβάν, που περιλαμβάνεται στο συμβόλαιο, οι κόμβοι αποφασίζουν από κοινού να εκτελέσουν τις οριζόμενες διαδικασίες και να ενημερώσουν περεταίρω τις αλυσίδες τους.

4.6 Πλεονεκτήματα

Καθίσταται γρήγορα αντιληπτό στον αναγνώστη ότι τα έξυπνα συμβόλαια παρουσιάζουν πληθώρα πλεονεκτημάτων σε σχέση με τα παραδοσιακά συμβόλαια. Από τα πρώτα χαρακτηριστικά που θα διέκρινε κανείς είναι ο κατά πολύ μειωμένος χρόνος που απαιτεί ένα έξυπνο συμβόλαιο. Η σύνταξη του δεν απαιτεί ραντεβού με κάποιο συμβολαιογράφο την χρονική στιγμή που εξυπηρετεί όλα τα μέλη, αλλά το κάθε μέλος ξεχωριστά, την οποιαδήποτε στιγμή μπορεί να χρησιμοποιήσει τον υπολογιστή του και να συντάξει το συμβόλαιο το οποίο τα υπόλοιπα μέλη θα 'υπογράψουν', επίσης οποιαδήποτε στιγμή μπορούν, από τους δικούς τους υπολογιστές. Επίσης η ικανοποίηση των όρων ή των ποινών λαμβάνει χώρα αυτόματα και ακαριαία καταργώντας τις μακροχρόνιες διαδικασίες των δικαστηρίων.

Εξίσου σημαντικό κρίνεται και το γεγονός ότι τα έξυπνα συμβόλαια δεν απαιτούν τα χρηματικά ποσά που χρειάζονται τα παραδοσιακά συμβόλαια. Το μόνο που χρειάζονται είναι να δανειστούν λίγες γραμμές κώδικά και ελάχιστο χώρο να αποθηκευτούν στο προϋπάρχον δίκτυο πράγμα που καθιστά το λειτουργικό τους κόστος ιδιαίτερα χαμηλό. Αυτό τους δίνει τη δυνατότητα να μπορούν να εφαρμοστούν ακόμα και σε συναλλαγές ιδιαίτερα μικρής αξίας πράγμα που στη περίπτωση των παραδοσιακών συμβολαίων θα ήταν ασύμφορο. Μάλιστα, από πλευράς κόστους χρήσης, τα έξυπνα συμβόλαια μπορούν, στις μέρες μας, να συγκριθούν με τη διευκόλυνση που έχει προσφέρει η χρήση του πλαστικού χρήματος μέσω μηχανημάτων POS. Τα POS σήμερα, λόγω της υπάρχουσας υποδομής, μπορούν να χρησιμοποιηθούν εύκολα και με ιδιαίτερα χαμηλό κόστος ακόμη και για συναλλαγές μικροποσών. Αντίστοιχα θα μπορούν να χρησιμοποιηθούν και τα έξυπνα συμβόλαια διευκολύνοντας τη ζωή των ανθρώπων.

Το επόμενο πλεονέκτημα που θα αναφερθούμε είναι η εξασφάλιση των μελών. Στη περίπτωση των παραδοσιακών συμβολαίων, όταν κάποιο μέλος αθετήσει τα συμφωνημένα, τα υπόλοιπα μέλη για να αποζημιωθούν θα πρέπει να απευθυνθούν σε κάποια δικαστική αρχή προκειμένου αυτή να επιβάλει τις ποινές που έχουν συμφωνηθεί χωρίς όμως η διαδικασία αυτή να εγγυάται το αποτέλεσμα. Τα δικαστήρια συχνά μπορούν να οδηγηθούν σε λανθασμένα συμπεράσματα και να μην επιβάλλουν τις ποινές του συμβολαίου. Επίσης, το κόστος της διαδικασίας είναι πολύ πιθανόν να λειτουργήσει αποτρεπτικά σε κάποια μέλη που δεν διαθέτουν τα απαραίτητα χρηματικά ποσά, ειδικά όταν γνωρίζουν ότι το αποτέλεσμα της διαδικασίας δεν είναι εγγυημένο. Τέλος, δεν θα πρέπει να παραληφθεί και το γεγονός ότι ακόμα και εάν το δικαστήριο αναγνωρίσει το δίκαιο και επιβάλει τις ποινές , το άτομο θα τις εκτίσει. Ο νόμος του δίνει το δικαίωμα, για παράδειγμα, να αποφύγει την καταβολή μιας αποζημίωσης δηλώνοντας πτώχευση ή αδυναμία πληρωμής. Όλες αυτές οι αδυναμίες αντιμετωπίζονται απλά με τα έξυπνα συμβόλαια αφού η οποιαδήποτε αποζημίωση δύναται να κατατεθεί σε κάποιο ασφαλή φορέα και κατόπιν το έξυπνο συμβόλαιο να την μεταφέρει αυτόματα στα μέλη που τη δικαιούνται μόλις αποφανθεί ότι οι όροι δεν τηρήθηκαν.

Οι Zhao και Coffie (Zhao, Coffie 2018) στην εργασία τους το 2018 περιέλαβαν μια μελέτη της βιβλιογραφίας σχετικά με τα πλεονεκτήματα των έξυπνων συμβολαίων. Από αυτά ξεχωρίσαμε τη δυνατότητα των έξυπνων συμβολαίων να εκτελέσουν εργασίες που δεν θα μπορούσαν να γίνουν από τα παραδοσιακά συμβόλαια όπως τη συνεχή παρακολούθηση τιμών, την αυτονομία των συμβολαίων που άπαξ και ενεργοποιηθούν δεν μπορούν να επηρεαστούν από κανέναν καθώς και τη διαφάνεια αλλά και την απλότητα που τα χαρακτηρίζει. Επίσης, άξια αναφοράς είναι και η αυξημένη ασφάλεια που παρέχουν μέσω της κρυπτογράφησης, την προστασία του περιβάλλοντος με την αποφυγή χρήσης χαρτιού και τέλος της ασφάλειας των εγγραφών μέσω της απουσίας κεντρικής βάσης δεδομένων.

4.7 Περιορισμοί

Όπως κάθε τεχνολογία έτσι και τα έξυπνα συμβόλαια έχουν τους περιορισμούς τους. Ο Zaheer Allam (Allam 2018:137) υποστήριξε ότι το γεγονός ότι τα συμβόλαια είναι 'σταθερά' δημιουργεί περιορισμό στη χρήση τους. Αυτό γιατί στα παραδοσιακά συμβόλαια υπάρχει η δυνατότητα να συμπεριληφθούν όροι που να τα καθορίσουν πιο ευέλικτα, επιτρέποντας την παραβίαση των όρων χωρίς αυτό να καθιστά το συμβόλαιο μη εκτελέσιμο, όπως για παράδειγμα μια καθυστέρηση στη παράδοση ενός έργου με την καταβολή κάποιου αντιτίμου ή και χωρίς αυτό. Η

ενσωμάτωση τέτοιο είδους λειτουργιών σε ένα έξυπνο συμβόλαιο όμως μπορεί να οδηγήσει σε μείωση του επιπέδου της ασφάλειας που παρέχει το συμβόλαιο μιας και είναι δύσκολο να εξασφαλισθεί ότι η δικλείδα αυτή δε θα χρησιμοποιηθεί από κακόβουλα μέλη. Επίσης, το γεγονός ότι το περιεχόμενο των συναλλαγών είναι γνωστό δημιουργεί ερωτηματικά ως προς τα προσωπικά δικαιώματα των συμβαλλομένων. Ναι μεν η ταυτότητα τους παραμένει απόρρητη, το περιεχόμενο όμως της συναλλαγής θα πρέπει να είναι ορατό ώστε τα μέλη να μπορούν να επιβεβαιώσουν την τήρηση ή όχι των όρων του συμβολαίου. Τέλος, δεν είναι μικρής σημασίας το γεγονός ότι τα έξυπνα συμβόλαια δεν έχουν νομική κάλυψη πράγμα ιδιαίτερα δύσκολο να υλοποιηθεί μιας και οι νόμοι διαφέρουν ανάμεσα στα κράτη ενώ τα έξυπνα συμβόλαια δεν περιορίζονται σε ένα κράτος.

4.8 Πεδία εφαρμογής Έξυπνων Συμβολαίων

Είναι φανερό ότι τα έξυπνα συμβόλαια μπορούν να έχουν εφαρμογή σε πολλούς τομείς της καθημερινότητας των ανθρώπων και μπορούν να βελτιώσουν σημαντικά τις απαρχαιωμένες διαδικασίες των παραδοσιακών συμβολαίων.

Από τα πρώτα πεδία εφαρμογής που θα αναφερθούμε είναι ο οικονομικός τομέας. Η βασική χρησιμότητα ενός συμβολαίου είναι η περιγραφή ενός αντικειμένου αξίας και πιο συγκεκριμένα ποιος θα είναι ο ιδιοκτήτης του ή πώς θα μεταβληθεί στο χρόνο κ.α. Αντικείμενο αξίας όμως μπορεί να είναι και ένα έργο η ολοκλήρωση του οποίου θα κινητοποιήσει το έξυπνο συμβόλαιο να μεταφέρει το προσυμφωνημένο ποσό στον εργοδηγό ή την αποζημίωση σε περίπτωση μη ολοκλήρωσης του έργου στο προσυμφωνημένο χρονικό διάστημα. Τέλος, μπορούμε να αναφέρουμε και άλλες χρήσεις όπως η συγκέντρωση χρημάτων για διάφορους σκοπούς, συμβόλαια διαφήμισης κ.α.

Τα έξυπνα συμβόλαια λόγω της ιδιαιτερότητας τους να παραμένουν αμετάβλητα στο χρόνο μπορούν να χρησιμοποιηθούν για τη κατοχύρωση πνευματικών δικαιωμάτων. Για παράδειγμα οι ενδιαφερόμενοι μπορούν να εισάγουν το κείμενο της εργασίας τους σε μια συνάρτηση κατακερματισμού και να χρησιμοποιήσουν το αποτέλεσμα της για μελλοντική απόδειξη της ιδιοκτησίας της εργασίας. Αντίστοιχα η διαδικασία μπορεί να εφαρμοστεί σε οποιοδήποτε αρχείο είτε αυτό είναι ένα μουσικό κομμάτι ή μια εικόνα.

Μια χρήση που έχει εμφανιστεί τα τελευταία χρόνια είναι η χρήση τους στα παιχνίδια των ηλεκτρονικών υπολογιστών. Τα παιχνίδια θα πρέπει συνεχώς να αναβαθμίζονται προκειμένου να συμβαδίζουν με τις ανάγκες των παιχτών πράγμα που έχει οδηγήσει σε μια εκτόξευση του κόστους μέσω των προγραμματιστών. Με την εφαρμογή όμως των έξυπνων συμβολαίων ανεξάρτητοι προγραμματιστές μπορούν να αναπτύσσουν τις νέες προσθήκες και οι παίκτες να τις αγοράζουν μόνο όταν τα έξυπνα συμβόλαια τούς βεβαιώνουν ότι πληρούν τις προϋποθέσεις.

4.9 Προκλήσεις

Όπως κάθε αναπτυσσόμενη τεχνολογία έτσι και τα έξυπνα συμβόλαια έχουν να αντιμετωπίσουν διάφορες προκλήσεις προτού το καταναλωτικό κοινό αρχίσει να τα εμπιστεύεται και να τα χρησιμοποιεί. Οι προκλήσεις που καλούνται να αντιμετωπίσουν οι σχεδιαστές και οι προγραμματιστές βρίσκονται τόσο στο τεχνολογικό όσο και στο επιχειρηματικό πεδίο σύμφωνα και με τη μελέτη του Kehrli (Kehrli 2016):

1. Επεκτασιμότητα: Η δυνατότητα επέκτασης των πλατφορμών που φιλοξενούν τα έξυπνα συμβόλαια δεν έχει ακόμα αποδειχθεί, με αποτέλεσμα οι σχεδιαστές να λαμβάνουν μέτρα προς την αντιμετώπιση του φαινομένου πλην όμως παραμένει ένα δύσκολο εγχείρημα.

2. Πρόσβαση σε πραγματικά δεδομένα: Τα έξυπνα συμβόλαια θα πρέπει με κάποιο τρόπο να λαμβάνουν πληροφορία από τον εξωτερικό πραγματικό κόσμο ώστε να γνωρίζουν κατά πόσον οι όροι τηρούνται ή όχι.

3. Ιδιωτικότητα: Είναι προφανές ότι θα πρέπει να ληφθεί μέριμνα ώστε τα τμήματα των συμβολαίων που θα πρέπει να παραμένουν ιδιωτικά να μην δύναται να διαρρεύσουν χωρίς όμως αυτό να παρεμποδίζει άλλα που θα πρέπει να παραμένουν δημόσια.

4. Αποδοτικότητα: Στη περίπτωση του Ethereum απαιτούνται δεκαεπτά δευτερόλεπτα ώστε μια πιστοποιημένη συναλλαγή να αποθηκευτεί επιτυχώς. Λαμβάνοντας υπόψη ότι σε ένα παραδοσιακό σύστημα διαχείρισης μιας βάσης δεδομένων η αντίστοιχη λειτουργία απαιτεί χρονικό διάστημα χιλιοστών του δευτερολέπτου καθίσταται προφανές στον αναγνώστη ότι στο συγκεκριμένο τομέα απαιτείτε ιδιαίτερη προσπάθεια.

5. Επιτήρηση: Τα έξυπνα συμβόλαια εφαρμόζονται τόσο σε δημόσιες όσο και σε ιδιωτικές αλυσίδες. Στην περίπτωση όμως των ιδιωτικών αλυσίδων αναμένεται εντονότερη

εφαρμογή λόγω της εμπιστοσύνης, της ιδιωτικότητας καθώς και άλλων χαρακτηριστικών που διέπουν τα μέλη μιας επιτηρούμενης ομάδας. Τα χαρακτηριστικά αυτά απουσιάζουν από τα μέλη της δημόσιας αλυσίδας πράγμα που δυσχεραίνει την εφαρμογή των έξυπνων συμβολαίων.

6. Περιορισμοί στις εφαρμογές: Παρόλο που το πεδίο εφαρμογής των έξυπνων συμβολαίων είναι ιδιαίτερα ευρύ υπάρχουν περιπτώσεις που δεν μπορούν να εφαρμοστούν. Επιπλέον υπάρχουν οργανισμοί που είναι μοντελοποιημένοι με τέτοιο τρόπο που δεν μπορούν να επωφεληθούν από τη χρήση των έξυπνων συμβολαίων άλλα και γενικότερα από τις τεχνολογίες αλυσίδας.

7. Εξασφάλιση: Από τη στιγμή που τα έξυπνα συμβόλαια, όπως και όλη η τεχνολογία αλυσίδας, διαχειρίζονται περιουσιακά στοιχεία για μεγάλο χρονικό διάστημα είναι προφανές ότι θα αποτελέσουν στόχο από ανθρώπους που θα προσπαθήσουν να τα εκμεταλλευθούν. Οι χρήστες τους θα πρέπει να εξασφαλισθούν από τους κινδύνους αυτούς μακροπρόθεσμα.

4.10 Μελέτη Σκοπιμότητας

Κατά τη μελέτη σκοπιμότητας θα ξεκινήσουμε από τη μελέτη του κόστους των έξυπνων συμβολαίων μιας και το κόστος αποτελεί ένα από τα βασικότερα θέματα της μελέτης. Φυσικά τα έξυπνα συμβόλαια δεν μπορούμε να τα εξετάσουμε ξεχωριστά από μια τεχνολογία αλυσίδας αφού είναι αλληλένδετα.

4.10.1 Κόστος Έξυπνων Συμβολαίων

Το κόστος των έξυπνων συμβολαίων μπορεί να μελετηθεί από τρείς διαφορετικές οπτικές πλευρές:

1. Το κόστος δημιουργίας: Τα ποσά που θα δαπανηθούν στις εταιρίες ανάπτυξης λογισμικού οι οποίες θα αναλάβουν τη συγγραφή του κώδικα που θα δημιουργήσει τα έξυπνα συμβόλαια. Το κόστος αυτό εξαρτάται από παράγοντες όπως η πολυπλοκότητα, οι κανόνες ασφάλειας που θα πρέπει να πληροί καθώς και ενδεχομένως άλλες εξωτερικές πηγές από τις οποίες θα αντλεί δεδομένα.

2. Το κόστος μεταπώλησης, το οποίο εξαρτάται από την πολιτική του εκάστοτε μεταπωλητή.

3. Το κόστος της συναλλαγής όπως ανέλυσε ο G. Wood (Wood 2017) για την περίπτωση του Ethereum.

4.10.2 Κόστος Τεχνολογίας Αλυσίδας

Προκειμένου να υιοθετήσει μια εταιρία την οποιαδήποτε τεχνολογία αλυσίδας θα πρέπει να επωμιστεί ένα αξιοσημείωτο κόστος. Οι τομείς στους οποίους θα πρέπει να επενδύσει είναι:

1. Υλικό: Σε αυτό περιλαμβάνεται ο εξοπλισμός που θα φιλοξενήσει τις νέες υπηρεσίες. Είναι πολύ πιθανό η εταιρία να μην μπορεί να εγκαταστήσει τις νέες υπηρεσίες στον ήδη υπάρχον εξοπλισμό και να αναγκαστεί να προβεί στην αγορά νέου.

2. Λογισμικό: Όπως και στη περίπτωση του υλικού είναι πολύ πιθανόν η εταιρία να προβεί σε αγορά νέου λογισμικού για την υποστήριξη των νέων τεχνολογιών.

3. Κόστος Υλοποίησης: Στη κατηγορία αυτή θα συμπεριφερθεί το κόστος που θα απαιτηθεί προκειμένου η ήδη εγκατεστημένη αλυσίδα να φιλοξενήσει το έξυπνο συμβόλαιο. Είναι πιθανόν να απαιτηθεί η αγορά νέου πρόσθετου λογισμικού η υλικού το οποίο θα προστεθεί στον ήδη υπάρχοντα εξοπλισμό της αλυσίδας.

4. Κόστος Χρήσης: Όπως όλα τα τμήματα της εταιρίας έχουν κάποιο κόστος χρήσης έτσι και το τμήμα της αλυσίδας έχει το δικό του αντίστοιχο κόστος που απαιτείται προκειμένου να λειτουργεί.

5. Το κόστος συντήρησης: Όμοια με το κόστος χρήσης αποτελεί και αυτό ένα σημαντικό κριτήριο που θα πρέπει να ληφθεί υπόψη.

4.10.3 Οφέλη Χρήσης Έξυπνων Συμβολαίων

Τα οφέλη από τη χρήση των έξυπνων συμβολαίων εξαρτώνται από τον κλάδο στον οποίο δραστηριοποιούνται. Για το λόγο αυτό θα ξεκινήσουμε την αναφορά μας από μια γενική προσέγγιση και κατόπιν θα εξειδικεύσουμε στον οικονομικό κλάδο.

1. Κόστος Μεσαζόντων: Από τα πρώτα οφέλη που μπορούμε να εντοπίσουμε είναι η εξάλειψη του κόστους των μεσαζόντων (συμβολαιογράφων, κλπ.) το οποίο είναι ιδιαίτερα αυξημένο. Βέβαια και στη περίπτωση της τεχνολογίας αλυσίδας γενικά υπάρχει ένα κόστος μεσαζόντων το οποίο όμως είναι αρκετά μειωμένο και σχεδόν αμελητέο.

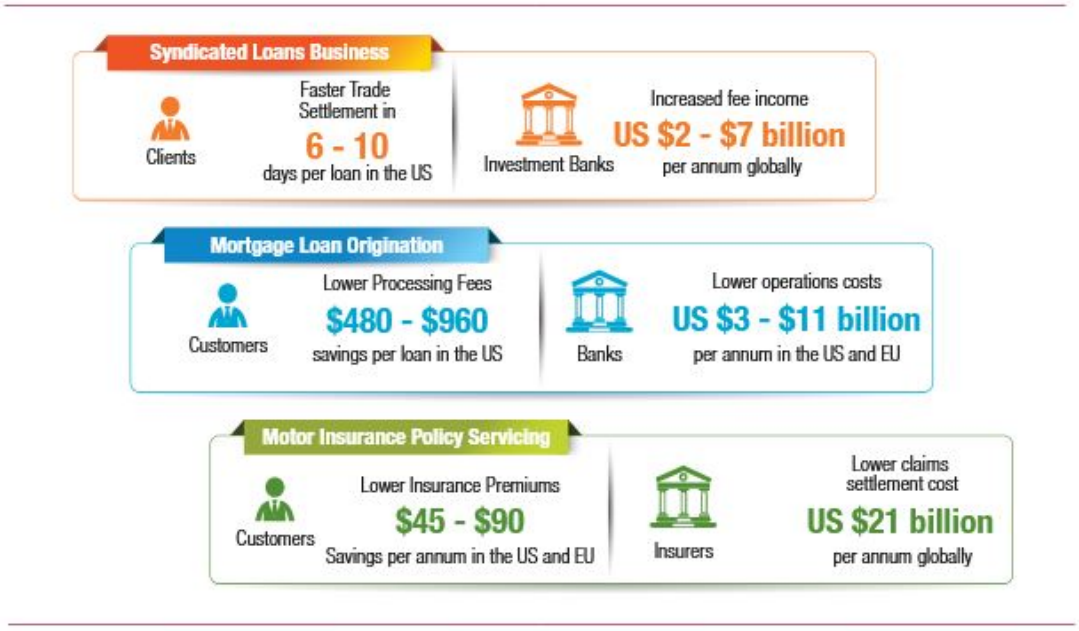
2. Αποδοτικότερη Διαδικασία: Στη περίπτωση των έξυπνων συμβολαίων οι διαδικασίες γίνονται πολύ πιο γρήγορα, πολύ πιο απλά και μειώνονται και οι πιθανότητες λάθους.

Στον οικονομικό τομέα μπορούμε να ξεχωρίσουμε τις ακόλουθες κατηγορίες, σύμφωνα και με την ανάλυση της CapGemini (Cant, Khadikar, Ruiter, Broneback, Coumaros, Buvat, Cupta 2017:1):

1. Επενδυτική Τραπεζική: Όπου οι πελάτες μπορούν να επωφεληθούν από τους σημαντικά μειωμένους χρόνους των διαδικασιών πράγμα που θα οδηγήσει σε μια αύξηση της ζήτησης.

2. Λιανική Τραπεζική: Στο τομέα αυτό αναμένονται σημαντικά κέρδη προερχόμενα κυρίως από τη μείωση του κόστους των διαδικασιών. Ενδεικτικά αναφέρουμε ότι αναμένεται μια μείωση του κόστους δανείου του καταναλωτή από 480 έως 960 δολάρια ενώ οι τράπεζες αναμένουν μια μείωση του κόστους μεταξύ των τριών και ένδεκα δισεκατομμυρίων δολαρίων ετησίως.

3. Ασφάλειες: Εξίσου σημαντικά κρίνονται τα οφέλη και για τον τομέα των ασφαλειών όπου η υιοθέτηση των έξυπνων συμβολαίων μπορεί να οδηγήσει σε μείωση του κόστους λειτουργίας της τάξης των εικοσιένα δισεκατομμύρια δολάρια ετησίως. Τμήμα του κέρδους αυτού αναμένεται να περαστεί και στους τελικούς καταναλωτές.



Source: Capgemini Consulting Analysis

Εικόνα12: Οφέλη από τη υιοθέτηση των έξυπνων συμβολαίων. Πηγή:https://www.capgemini.com/consulting-de/wp-content/uploads/sites/32/2017 /08/smart_contracts_paper_long_0.pdf

4.10.4 Συμπεράσματα

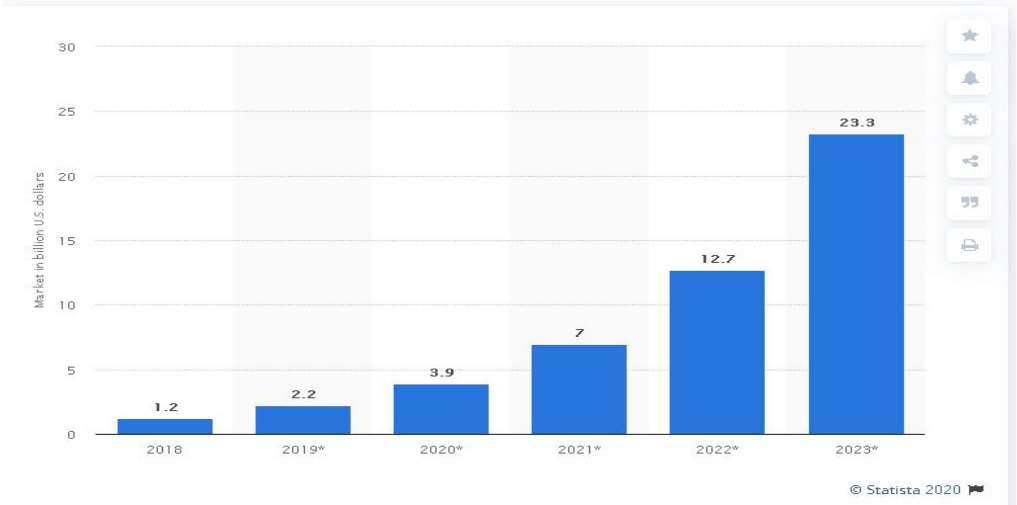
Κλείνοντας το κεφάλαιο αυτό, θα πρέπει να συνοψίσουμε ότι η υιοθέτηση των έξυπνων συμβολαίων από ένα οργανισμό απαιτεί προσεκτική μελέτη του κόστους του συστήματος. Αν αυτή διεξαχθεί σωστά τότε το όλο εγχείρημα μπορεί να οδηγήσει σε σημαντική μείωση του κόστους λειτουργίας του οργανισμού καθώς και σε εξίσου σημαντική αύξηση της απόδοσής του. Θα πρέπει όμως να ληφθεί υπόψη ότι τα έξυπνα συμβόλαια δεν είναι κατάλληλα για όλων των ειδών τις επιχειρήσεις.

Κεφάλαιο 5
Μερίδιο αγοράς

Στο κεφάλαιο αυτό θα αναφερθούμε στην εξάπλωση που έχουν πετύχει οι τεχνολογίες τόσο του BlockChain όσο και των έξυπνων συμβολαίων στην αγορά διεθνώς έως σήμερα. Επιπλέον, λόγω της ταχύτητας με την οποία επέρχονται οι αλλαγές στην εποχή μας, κρίνεται απαραίτητο να μελετήσουμε και τις προοπτικές και τις προβλέψεις ώστε να σχηματίσει ο αναγνώστης μια πιο πλήρη εικόνα του τι αναμένετε να επακολουθήσει αναφορικά με την οικονομική πλευρά των τεχνολογιών αυτών.

5.1 Μερίδιο Αγοράς

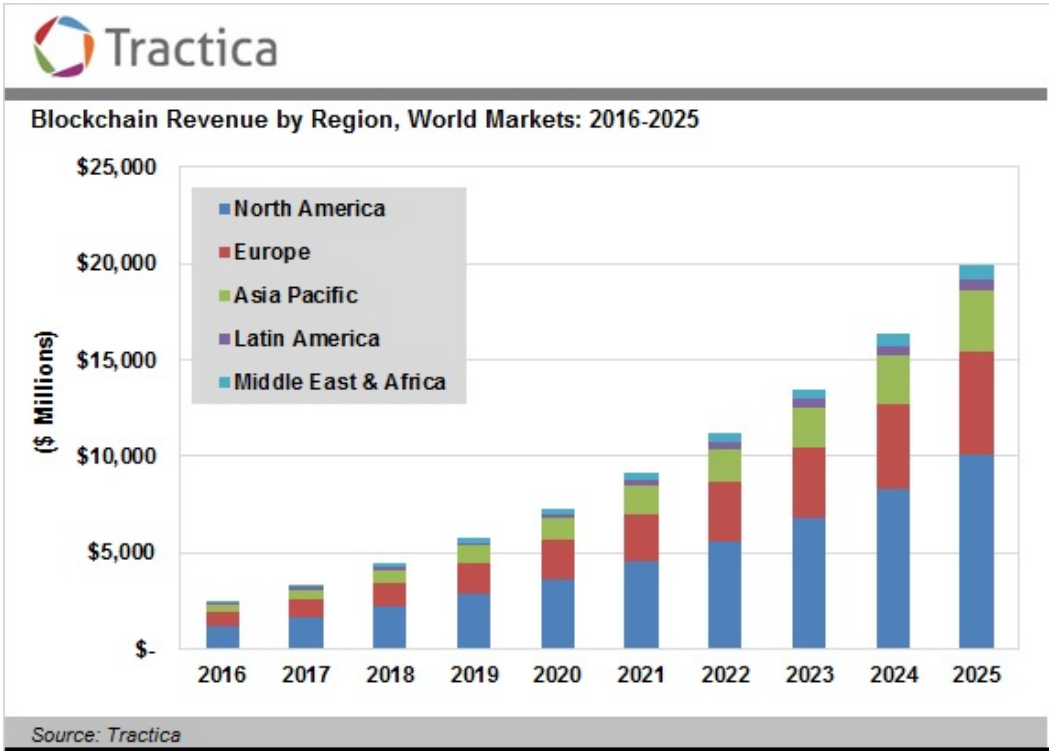
Σύμφωνα με πρόσφατες μελέτες (Hacioglu 2019), καταδεικνύεται ότι η αγορά της Blockchain τεχνολογίας θα βιώσει μια ανάπτυξη της τάξης του 80.02% και από τα 1.2 δισεκατομμύρια δολάρια που άξιζε το 2018 θα αγγίξει τα 23.3 δισεκατομμύρια δολάρια το 2023. Επιπλέον, αναμένεται μια επέκταση της χρήσης της τεχνολογίας και σε νέους τομείς όπως σε εταιρίες τύπου Start-Up οι οποίες θα συνδέουν τις τεχνολογίες BlockChain με οικονομικούς οργανισμούς.



Εικόνα 13: Ρυθμός ανάπτυξης BlockChain. Πηγή: www.statista.com/statistics/647231/worldwide-blockchain-technology-market-size/

5.2 Διεθνής Θέση

Η διεθνή αγορά κατανέμεται σε διάφορες χώρες συμπεριλαμβανομένων της Αμερικής της Ευρώπης, Ανατολικής και Δυτικής Ασίας και τέλος Αφρικής. Η Αμερική κατέχει επιφανή θέση στη πρόθεση για χρήση των τεχνολογιών έξυπνων συμβολαίων ειδικότερα από εταιρίες που δραστηριοποιούνται στο τραπεζικό κλάδο, στα οικονομικά αλλά και σε παροχές υγείας λόγω των διαφανών και ασφαλών διαδικασιών που παρέχουν τα έξυπνα συμβόλαια. Και η Ευρώπη έχει σημαντικό μερίδιο αγοράς στη τεχνολογία αλυσίδας και αναμένετε να ακολουθήσει στους ίδιους ρυθμούς ανάπτυξης. Η Ανατολική Ασία από την άλλη πλευρά κατέχει την πιο επικερδή θέση λόγω της μεγάλης ζήτησης για τη τεχνολογία από εταιρίες που δραστηριοποιούνται τόσο στον οικονομικό τομέα όσο και στο μεσιτικό αλλά και σε αυτόν της διασκέδασης. Στην αντίπερα όχθη η Λατινική Αμερική, η Αφρική και η Μέση Ανατολή βρίσκονται σε πρωταρχικό στάδιο λόγω έλλειψης ενημέρωσης αλλά και μειωμένης δυνατότητας προσαρμογής στη νέα αυτή τεχνολογία. Έρευνα της Tractica (Kokina, Mancha, Pachamanova 2017:91), προβλέπει ότι αξία των εφαρμογών Blockchain θα αγγίξει τα 19.9 δισεκατομμύρια δολάρια το 2025 από τα 2.5 δισεκατομμύρια το 2016. Ηγετική θέση στην πορεία αυτή θα κατέχει η Αμερική την οποία θα ακολουθήσει η Ευρώπη.



Εικόνα 14: Διεθνές μερίδιο αγοράς της τεχνολογίας. Πηγή:https://tractica.omdia.com/newsroom/press-releases/blockchain-for-enterprise-applications-market-to-reach-19-9-billion-by-2025/

5.3 Πεδία Εφαρμογής Τεχνολογίας Αλυσίδας

Είναι φανερό ότι η τεχνολογία αυτή βρίσκει εφαρμογή σε ένα ευρύ φάσμα εταιρικών δραστηριοτήτων. Ενδεικτικά μπορούμε να αναφέρουμε εταιρίες μεταφορών, μεσιτικές, διασκέδασης, τεχνολογίας καθώς και πολλές άλλες. Ειδικά στον οικονομικό τομέα οι εναλλακτικές είναι πολλές και για το λόγο αυτό, ειδικά στις χώρες του APAC επενδύονται μεγάλα πόσα σε επιτηρούμενα δίκτυα αλυσίδας με στόχο τη βελτίωση των εσωτερικών διαδικασιών και τη μείωση του κόστους. Η ενσωμάτωση των νέων αυτών τεχνολογιών ουσιαστικά επαναπροσδιορίζει τις διαδικασίες των εργασιών. Βασικός παράγοντας που οδήγησε στην υιοθέτηση των τεχνολογιών αυτών αποτέλεσε η διαφάνεια των διαδικασιών που προσφέρει η τεχνολογία σε συνδυασμό με την αμεταβλητότητα των συναλλαγών. Τα χαρακτηριστικά αυτά είχαν σαν αποτέλεσμα να εξασφαλιστεί η εμπιστοσύνη του καταναλωτικού κοινού και να επενδύσει στην υιοθέτηση τους.

5.3.1 Εταιρίες Παροχής Εφαρμογών

Οι εταιρίες αυτές μειώνουν τα κόστη λειτουργίας των πελατών, διευκολύνοντας τις συναλλαγές τους μέσω της εφαρμογής της τεχνολογίας αλυσίδας. Μέσω της αλυσίδας πραγματοποιούνται οι μεταφορές χρημάτων σε διεθνές επίπεδο, μειώνονται τα δεδομένα των συναλλαγών, πραγματοποιούνται περιοδικές επαληθεύσεις καθώς και οι διάφορες πιστοποιήσεις. Με τον τρόπο αυτό οι εταιρίες αυτές βελτιώνουν τη διαδικασία των συναλλαγών.

5.3.2 Εταιρίες Παροχής Διαπιστευτηρίων

Λόγω της έλλειψης κάποιας κεντρικής αρχής που θα εποπτεύει τα μέλη της αλυσίδας δημιουργείται η ανάγκη να χτίζεται ένα είδος εμπιστοσύνης μεταξύ των άγνωστων μελών. Την αποστολή αυτή αναλαμβάνουν οι εταιρίες που δραστηριοποιούνται στο χώρο αυτό. Οι εταιρίες αυτές πιστοποιούν τα μέλη και διαχειρίζονται τα δεδομένα τους. Για το λόγο αυτό προσανατολίζονται στην κατασκευή του απαιτούμενου λογισμικού προσαρμοσμένο στις απαιτήσεις της εκάστοτε εφαρμογής.

5.3.4 Οικονομικός Τομέας

Οι εταιρίες που δραστηριοποιούνται στον οικονομικό τομέα όπως τράπεζες, οικονομικοί σύμβουλοι, ασφαλιστικές και μεσιτικές εταιρίες έχουν συνειδητοποιήσει τα οφέλη της υιοθέτησης της τεχνολογίας και για αυτό επενδύουν σε αυτή (Guo, Liang 2016:24).

Πέρα όμως από τις εταιρίες αυτές, η απουσία των μεσαζόντων στις συναλλαγές και γενικότερα ο επαναπροσδιορισμός των διαδικασιών οδηγεί στην εμφάνιση νέων εταιρικών μοντέλων τόσο στο τομέα των πληρωμών, του internet banking αλλά και των συναλλαγών γενικότερα.

5.3.5 Οργάνωση του Κράτους

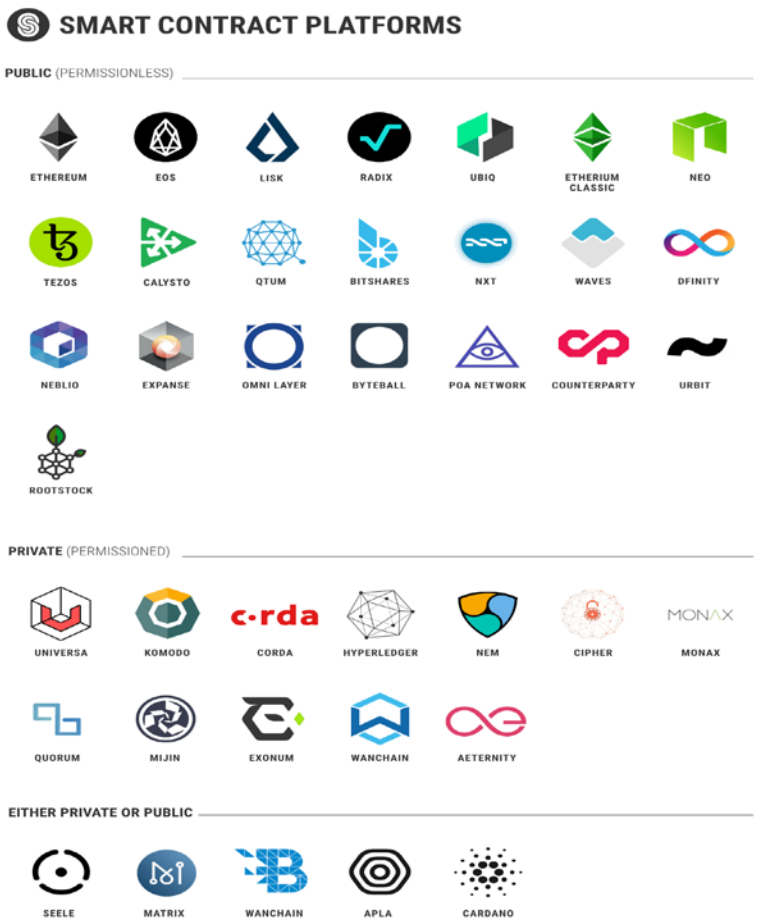
Πέρα όμως από τον τομέα των επιχειρήσεών η τεχνολογία έχει εφαρμογές και στο τομέα της οργάνωσης σημαντικών δομών ενός κράτους. Για να γίνει αυτό αντιληπτό από τον αναγνώστη θα αναφερθούμε στο πρόσφατο παράδειγμα της Κυπριακής Δημοκρατίας όπου με απόφαση του Υπουργικού Συμβουλίου, στις 30 Αυγούστου του 2018 αποφασίστηκε η σύσταση Ad Hoc Ομάδας Εργασίας για την ανάπτυξη της τεχνολογίας Blockchain και την εφαρμογή πιλοτικών έργων σε υπηρεσίας του κράτους (Κυπριακή Δημοκρατία, 2019). Οι υπηρεσίες αυτές περιλαμβάνουν μεταξύ άλλων το Τμήμα Κτηματολογίου και Χωρομετρίας, το Τελωνείο και τη Φορολογία, την Εθνική Αρχή Στοιχημάτων, στον Ακαδημαϊκό κλάδο με τη διαπίστευσή των τίτλων σπουδών, καθώς και σε άλλες υπηρεσίες.

5.3.6 Εκπαίδευση

Ο τομέας της εκπαίδευσης μπορεί επίσης να επωφεληθεί από την χρήση της τεχνολογίας blockchain. Ψηφιακά πτυχία, πιστοποιήσεις καθώς και η ανάπτυξη νέων, πιο ευέλικτων τρόπων διδασκαλίας είναι κάποια από τα πεδία που τα εκπαιδευτικά ιδρύματα έχουν την δυνατότητα να βελτιώσουν την λειτουργία τους και τις παροχές τους (Mendez, Bayyou 2019:68).

Κεφάλαιο 6
Διαθέσιμες Πλατφόρμες

Στο κεφάλαιο αυτό θα μελετήσουμε τις πλέον διαδεδομένες και επικρατέστερες πλατφόρμες τεχνολογίας αλυσίδας. Θα αναφερθούμε στα ιδιαίτερα χαρακτηριστικά τους, το μερίδιο αγοράς που κατέχουν καθώς και τις τεχνολογίες που υποστηρίζουν. Η μελέτη μας θα περιοριστεί σε αυτές που υποστηρίζουν έξυπνα συμβόλαια μιας και αυτό είναι και το αντικείμενο της παρούσας μεταπτυχιακής διατριβής.



Εικόνα 15: Πλατφόρμες που υποστηρίζουν έξυπνα συμβόλαια. Πηγή:https://blog.apla.io/smart-contract-blockchain-dlt-platforms-how-do-they-measure-up-7ac2dccb67e8

6.1 Bitcoin

Από την αναφορά μας δεν θα μπορούσε να απουσιάζει η πρώτη πλατφόρμα στο χώρο καθώς και αυτή με το μεγαλύτερο μερίδιο αγοράς, το bitcoin. Πρωτοεμφανίστηκε το 2008 όταν άτομο (ή ομάδα ατόμων) με το ψευδώνυμο Satoshi Nakamoto δημοσίευσε τη μελέτη του (Nakamoto 2008). Ακολούθως, το 2009 ο κώδικας έγινε ευρέως διαθέσιμος μέσω του διαδικτύου και το πρώτο ψηφιακό νόμισμα έγινε γεγονός.

Το bitcoin εμφανίστηκε αμέσως μετά την παγκόσμια κρίση που βίωσε ο πλανήτης στον τραπεζικό τομέα και αυτός ήταν και ένας από τους λόγους που οδήγησαν στην ταχεία εξάπλωση του. Ο κόσμος πλέον είχε αρχίσει να χάνει την εμπιστοσύνη του στις τράπεζες και στο τραπεζικό σύστημα γενικότερα και αναζητούσε νέους μηχανισμούς συναλλαγών από τους οποίους θα απουσιάζει μια κεντρική αρχή που θα τους κατευθύνει και θα επηρεάζει τη λειτουργία τους. Και αυτό ακριβώς ήρθε να προτείνει το bitcoin. Ένα νόμισμα την αξία του όποιου θα ορίζουν οι κανόνες της προσφοράς και της ζήτησης και δεν θα ανήκει σε κάποιο κράτος ώστε να εποπτεύεται από αυτό και να παρεμβαίνει στη λειτουργία του.

Το bitcoin, σαν πρώτη υλοποίηση ψηφιακού νομίσματος δεν υποστηρίζει την ιδέα των έξυπνων συμβολαίων στο βαθμό που την υποστηρίζουν μεταγενέστερες πλατφόρμες. Αυτό συνέβη πιθανόν διότι ο εμπνευστής του ψηφιακού νομίσματος είχε σαν στόχο τα ψηφιακά νομίσματα και όχι την ενσωμάτωση στη τεχνολογία και των έξυπνων συμβολαίων, πράγμα που έκαναν οι σχεδιαστές των μεταγενέστερων πλατφορμών, οι οποίοι προέβλεψαν την επιτυχία που θα έφερνε η υιοθέτηση των έξυπνων συμβολαίων. Με τις συνεχόμενες βελτιώσεις και τις προσθήκες όμως που δέχεται η πλατφόρμα μπορεί πλέον και αυτή να υποστηρίξει έξυπνα συμβόλαια που επιτρέπουν τη πραγματοποίηση συναλλαγών αυτόματα σε δεδομένη χρονική στιγμή, ή όταν συγκεκριμένα μέλη υπογράψουν, κ.α.

Όπως αναφέρθηκε ήδη, το Bitcoin είναι η τεχνολογία με το μεγαλύτερο μερίδιο αγοράς, τις περισσότερες συναλλαγές παγκοσμίως, μέχρι που εξάντλησε το μέγιστο όριο ημερήσιων συναλλαγών το 2018 και κατόπιν ξεπεράστηκε από το Ethereum,. Ενδεικτικά να αναφέρουμε ότι την περίοδο συγγραφής της μεταπτυχιακής αυτής διατριβής η αξία ενός bitcoin ήταν στα 8.732.22 δολάρια Αμερικής ενώ της αμέσως επόμενης πλατφόρμας, του Ethereum ήταν μόλις στα 223.18 δολάρια Αμερικής.

Από τα χαρακτηριστικά της θα αναφερθούμε στο ότι πρόκειται για μια τεχνολογία που ανήκει στο είδος της δημόσιας αλυσίδας, υπό την έννοια ότι δεν απαιτείται κάποια έγκριση από κάποια κεντρική αρχή για να γίνει κάποιος μέλος. Με τον τρόπο αυτό ο οποιοσδήποτε μπορεί να εγκαταστήσει το λογισμικό στον υπολογιστή του και να συμμετάσχει στη διαδικασία επικύρωσης συναλλαγών διεκδικώντας και αυτός μερίδιο. Μάλιστα η έννοια της κεντρικής αρχής απουσιάζει παντελώς από το όλο εγχείρημα και, όπως αναφέρθηκε και προηγουμένως αυτός ήταν και ένας από τους λόγους που οδήγησαν στην τόσο μεγάλη αποδοχή και επιτυχία του ψηφιακού νομίσματος.

Το bitcoin βασίζεται σε συναρτήσεις κρυπτογράφησης για την αποθήκευση και προστασία των δεδομένων καθώς και κατακερματισμού προκειμένου να εξασφαλίζεται η ακεραιότητα τους. Επιπλέον χρησιμοποιεί ψηφιακές υπογραφές, κρυπτογράφηση ιδιωτικού αλλά και δημοσίου κλειδιού για την επικοινωνία των μελών η οποία πραγματοποιείται μέσω ενός Peer to Peer δικτύου. Τέλος, για την εξασφάλιση των μελών χρησιμοποιεί σαν πρωτόκολλο συναίνεσης το Απόδειξης Εργασίας (Proof of Work), μέσω του οποίου τα μέλη μπορούν να πραγματοποιούν συναλλαγές χωρίς να απαιτείται εμπιστοσύνη μεταξύ τους.

Μία συναλλαγή περιέχει ένα μοναδικό κωδικό ID που την χαρακτηρίζει μοναδικά από τις υπόλοιπες του δικτύου, τα δεδομένα εξόδου του προηγούμενου μπλοκ σαν δεδομένα εισόδου, τον αριθμό των bitcoins καθώς και τα δεδομένα εξόδου. Προκειμένου να ολοκληρωθεί μία συναλλαγή απαιτούνται δύο οντότητες, ο συναλλασσόμενος που θα ξεκινήσει την συναλλαγή και ένας εργάτης (miner) ο οποίος είναι ένα άτομο που διαθέτει το λογισμικό και την απαραίτητη υπολογιστική ισχύ. Ο συναλλασσόμενος θα καταβάλει στον εργάτη μια προμήθεια ως αμοιβή προκειμένου εκείνος να εισάγει την συναλλαγή σε ένα μπλοκ. Η επεξεργασία του κάθε μπλοκ διαρκεί 10 λεπτά και κατόπιν οι συναλλαγές που περιέχει αποθηκεύονται στην αλυσίδα. Για να το πετύχει αυτό ο εργάτης θα πρέπει πέρα από τις πληροφορίες της συναλλαγής να έχει και δεδομένα των προηγούμενων μπλοκ. Αυτά τα αποκτά λύνοντας ένα κρυπτογραφικό παζλ, η δυσκολία του οποίου αυξάνεται με το πλήθος των συναλλαγών. Η εύρεση της λύσης απαιτεί υπολογιστικούς πόρους καθώς και κατανάλωση ηλεκτρικής ενέργειας και με τον τρόπο αυτό επιτυγχάνετε η απόδειξη εργασίας. Επιπλέον, δεν υπάρχει μόνο ένας εργάτης στο δίκτυο άλλα πολλοί οι οποίοι ανταγωνίζονται μεταξύ τους για το ποιος θα βρει πρώτος τη λύση του παζλ. Ο εργάτης που θα κερδίσει τον διαγωνισμό θα αμειφθεί με την προμήθεια που καταβάλει ο συναλλασσόμενος. Φυσικά η νέα αυτή λύση θα πρέπει να επιβεβαιωθεί από τη πλειοψηφία των υπολοίπων μελών εξασφαλίζοντας έτσι την ασφάλεια των συναλλαγών. Ακόμα και αν κάποιος κακόβουλος χρήστης

παρουσιάσει μια λύση που δεν είναι σωστή, με σκοπό να αποκομίσει παρανόμως την προμήθεια, δεν θα το καταφέρει αφού δεν θα έχει την επιβεβαίωση της πλειοψηφίας.

Με τη διαδικασία αυτή επιτυγχάνετε η εξασφάλιση των μελών, δημιουργούνται όμως προβλήματα καθώς το μέγεθος των συναλλαγών αυξάνει. Αυτό συμβαίνει διότι ο κάθε κόμβος θα πρέπει να έχει το σύνολο του ιστορικού της κάθε συναλλαγής προκειμένου να επιβεβαιώσει την νέα συναλλαγή, πράγμα που καθιστά ιδιαίτερα δαπανηρή τη διαδικασία επίλυσης του κρυπτογραφικού παζλ. Το πρόβλημα μάλιστα έχει λάβει τόσο μεγάλες διαστάσεις που το bitcoin κατηγορείται από τη διεθνή κοινότητα ότι συμβάλει σημαντικά στο φαινόμενο του θερμοκηπίου με τους ρύπους που εκλύονται στην ατμόσφαιρα από την μεγάλη κατανάλωση ενέργειας που απαιτεί για την επαλήθευση των συναλλαγών.

Σε μια προσπάθεια να αντιμετωπιστούν τα προβλήματα αυτά έχουν προταθεί διάφορες λύσεις όπως η Segregated Witness μέσω της οποία διαχωρίζονται οι πληροφορίες της υπογραφής από αυτές της συναλλαγής βελτιώνοντας έτσι τις δυνατότητες επέκτασης του δικτύου αλλά και τον περιορισμό που επιβάλλει το μέγεθος του μπλοκ, ο οποίος οδήγησε και στο περιορισμό των αριθμού των ημερήσιων συναλλαγών και επέτρεψε το Ethereum να ξεπεράσει το bitcoin στο τομέα αυτό.

6.2 Ethereum

Το Ethereum ήρθε να συμπληρώσει τα κενά που άφησε το Bitcoin. Πιο συγκεκριμένα, ενώ το bitcoin δημιουργήθηκε για να υποστηρίζει συναλλαγές μέσω ενός ψηφιακού νομίσματος εντός ενός αποκεντρικοποιημένου δικτύου, το Ethereum παρέχει μια πλατφόρμα μέσω της οποίας οι χρήστες μπορούν να δημιουργήσουν τις δικές τους αλυσίδες καθώς και τα δικά τους νομίσματα. Αναλυτικότερα η πλατφόρμα Ethereum ανήκει στη κατηγορία των Turing – Complete συστημάτων με την έννοια ότι μπορεί να υποστηρίξει το πλήρες σετ εντολών ενός υπολογιστή σε αντίθεση με το bitcoin που υποστηρίζει περιορισμένο πλήθος εντολών. Ο εμπνευστής του οραματίστηκε μια τεχνολογία αλυσίδας πάνω στην οποία οι προγραμματιστές θα μπορούσαν να δημιουργήσουν εφαρμογές real world μέσω της δημιουργίας και εκτέλεσης έξυπνων συμβολαίων.

Η πλατφόρμα παρουσιάστηκε το 2013 από τον Βίταλικ Μπούτεριν, έναν Ρώσσο ερευνητή και προγραμματιστή κρυπτονομισμάτων. Για την ανάπτυξη της δαπανήθηκαν κονδύλια τα οποία συγκεντρώθηκαν μέσω μιας διαδικτυακής χρηματοδότησης που έλαβε χώρα μεταξύ του Ιουλίου

και Αυγούστου του 2014. Το σύστημα ολοκληρώθηκε και τέθηκε σε κυκλοφορία στις 30 Ιουλίου του 2015 και διέθετε 11.9 εκατομμύρια προεξορυγμένα κέρματα, τα οποία ονομάζονται Ether, για την χρηματοδότηση του που αντιπροσώπευαν το 13% της συνολικής κυκλοφορίας. Ακολούθως το 2016, όπου η ανακάλυψη μιας ευπάθειας ενός έξυπνου συμβολαίου (του DAO) οδήγησε στην απώλεια 50 εκατομμυρίων δολαρίων (Mehar, Shier, Giambattista, Gong, Fletser, Sanayhie, Kim, Laskowski 2017) το Ethereum διασπάστηκε σε δύο πλατφόρμες, την παραδοσιακή ETC και μια νέα, την ETH.

Όπως και το bitcoin έτσι και το Ethereum ανήκει στη κατηγορία των δημόσιων αλυσίδων από την οποία απουσιάζει ο κεντρικός έλεγχος. Βασίζεται στις τεχνολογίες που χρησιμοποιεί και το bitcoin όπως τις συναρτήσεις κρυπτογράφησης και κατακερματισμού, κρυπτογράφηση δημοσίου καθώς και ιδιωτικού κλειδιού, πρωτόκολλο επικοινωνίας Peer to Peer, ένα δικό του πρωτόκολλο απόδειξης εργασίας Proff Of Work που ονομάζετε Ethash, καθώς και άλλα.

Το Ethereum, πέρα από τη δυνατότητα να δημιουργούν οι χρήστες τα δικά τους νομίσματα χρησιμοποιεί και το δικό του νόμισμα, όπως προαναφέρθηκε, που ονομάζετε Ether το οποίο είναι το δεύτερο σε αξία στην αγορά. Η εξόρυξη των νέων νομισμάτων γίνεται σε σταθερό ρυθμό ο οποίος δεν αλλάζει συχνά σε αντίθεση με το bitcoin που αλλάζει κάθε τέσσερα χρόνια. Επιπλέον, για την ολοκλήρωση ενός μπλοκ συναλλαγών απαιτείται χρονικό διάστημα περίπου 15 δευτερολέπτων σε αντίθεση με το bitcoin που απαιτεί 10 λεπτά, βελτιώνοντας έτσι σημαντικά το χρόνο λειτουργίας της πλατφόρμας. Για τη λειτουργία του διαθέτει μια εικονική μηχανή, η οποία ονομάζεται Ethereum Virtual Machine, την οποία χρησιμοποιούν οι προγραμματιστές για να ξεκινήσουν τις δικές τους ξεχωριστές αλυσίδες αλλά και τα δικά τους κρυπτονομίσματα. Το διάστημα που συντάσσονταν η παρούσα μεταπτυχιακή διατριβή η μηχανή αυτή είχε χρησιμοποιηθεί για την λειτουργία περισσότερων από 1000 εφαρμογών μεταξύ των οποίων και οι πολύ γνωστές VeChain και OmiseGo.

Η βασικότερη όμως διαφορά από το Bitcoin είναι το πλήθος των εντολών που υποστηρίζει η εικονική μηχανή με αποτέλεσμα να μπορεί να υιοθετήσει πολύπλοκα έξυπνα συμβόλαια σε αντίθεση με τον προκάτοχό του ο οποίος μπορεί να υποστηρίξει περιορισμένες λειτουργείες έξυπνων συμβολαίων. Τα έξυπνα συμβόλαια ουσιαστικά γίνονται πακέτα σε εφαρμογές οι οποίες ονομάζονται αποκεντρικοποιημένες εφαρμογές (DAps) και εκτελούνται μέσα στην εικονική μηχανή του Ethereum .

Η εφαρμογές αυτές ανήκουν στην κατηγορία των Full Stack εφαρμογών με την έννοια ότι αποτελούνται από το BackEnd τμήμα το οποίο χρησιμοποιούν οι προγραμματιστές για την ανάπτυξη και διαχείριση τους και το FrontEnd που χρησιμοποιούν οι τελικοί χρήστες. Για την ανάπτυξη του BackEnd χρησιμοποιείται η γλώσσα προγραμματισμού Solidity η οποία ανήκει στη κατηγορία των γλωσσών υψηλού επιπέδου όπως η C++, η Java, η Python και άλλες. Αντίθετα για το FrontEnd μπορεί να χρησιμοποιηθεί οποιαδήποτε γλώσσα.

Για να γίνει δεκτή μια τέτοια εφαρμογή στο Ethereum θα πρέπει να πληροί ορισμένα κριτήρια. Το βασικότερο είναι να είναι ανοιχτού κώδικα ώστε όλα τα μέλη να μπορούν να δουν το κώδικα της και να έχουν πλήρη εικόνα του τι κάνει. Επιπλέον η εφαρμογή θα πρέπει να μπορεί να λειτουργήσει αυτόνομα σε ένα αποκετρικοποιημένο περιβάλλον όπως αυτό που παρέχει η πλατφόρμα. Μέριμνα έχει δοθεί και στις μελλοντικές αλλαγές και προσθήκες που μπορεί να λάβει η εφαρμογή. Προκειμένου να μπορέσουν αυτές να εισαχθούν θα πρέπει πρωτίστως να εγκριθούν από τους χρήστες εξασφαλίζοντας έτσι ότι δεν θα θίγονται οι όροι του συμβολαίου. Όμοια, θα πρέπει τα δεδομένα του συμβολαίου να διαμοιράζονται στα μέλη της αλυσίδας κατάλληλα κρυπτογραφημένα έτσι ώστε να διασφαλίζεται η ασφαλή πρόσβαση σε αυτά από τα μέλη που έχουν την απαιτούμενη διαπίστευση. Τέλος το πρωτόκολλο συναίνεσης παράγει ειδικά κρυπτογραφημένα τόκενς που χαρακτηρίζουν τους χρήστες τα οποία χρησιμοποιεί η εφαρμογή, χωρίς κανείς να μπορεί να τα τροποποιήσει.

Το Ethereum λειτουργεί αποδοτικότερα σε σχέση με το Bitcoin με την έννοια ότι παρέχει μια μέθοδο που επιτρέπει στους χρήστες να καθορίσουν το σύνολο της υπολογιστικής ισχύς που θα διαθέσουν προκειμένου να διεκπεραιώσουν μια συναλλαγή. Για να το πετύχουν αυτό χρησιμοποιούν μια μονάδα μέτρησης της υπολογιστικής ισχύος που ονομάζετε GAS. Με τον τρόπο αυτό ο χρήστης ορίζει το μέγεθος που προτίθεται να δαπανήσει για να ολοκληρώσει τη συναλλαγή με την προσυμφωνημένη προμήθεια. Αν η συναλλαγή ολοκληρωθεί εντός των προσυμφωνημένων ορίων η διαδικασία ολοκληρώνετε και η προμήθεια εισπράττεται. Διαφορετικά, η συναλλαγή δεν επιβεβαιώνεται και το ύψος της προμήθειας επαναδιαπραγματεύεται. Κατά τον τρόπο αυτό υπάρχει ένας διαχωρισμός στη κατανάλωση ενέργειας μεταξύ των απλών συναλλαγών που απαιτούν μικρότερες ποσότητες σε σχέση με τις πολυπλοκότερες που απαιτούν μεγαλύτερες, κάνοντας έτσι τη λειτουργία της πλατφόρμας αποδοτικότερη (Wood 2018).

6.3 Hyperledger

Το Hyperledger κινείται σε μια διαφορετική κατεύθυνση από τις προηγούμενες πλατφόρμες και εστιάζει στη διευκόλυνση των εταιρικών συναλλαγών και όχι τόσο σε συναλλαγές μεταξύ ατόμων. Δεν διαθέτει δικό του νόμισμα και σύμφωνα με τον υπεύθυνο Brian Behlendorf δεν προτίθεται να αποκτήσει ούτε στο μέλλον. Δεν αποτελεί μία εφαρμογή αλλά μια ομάδα εφαρμογών πολλές από τις οποίες προέρχονται από διαφορετικές εταιρίες και έχουν ενσωματωθεί στην ομάδα επιτελώντας η κάθε μια ξεχωριστά το δικό της διαφορετικό ρόλο.

Πρωτοεμφανίστηκε το 2015 από το Linux Foundation μέσω της ανακοίνωσης για τη δημιουργία του Hyperledger Project. Ακολούθως το 2016 άρχισε να ενσωματώνει εφαρμογές άλλων εταιριών όπως η IBM, η Digital Asset και η Blockstream πράγμα που οδήγησε στην πρώτη έκδοση της αλυσίδας συστοιχιών του Hyperledger που ονομάστηκε Fabric. Λίγους μήνες αργότερα υιοθέτησε και την αλυσίδα της εταιρίας Intel με την ονομασία Sawtooth. Αργότερα ακολούθησαν πολλές εταιρίες από διάφορους κλάδους όπως οι Fujitsu, Hitachi, Nec, Red Hat, VMware εταιρίες που ανήκουν στον τομέα της τεχνολογίας, ABN AMRO, ANZ Bank, J.P. Morgan καθώς και άλλες που ανήκουν στον οικονομικό τομέα, ακαδημαϊκά ιδρύματα όπως το Cambridge Centre for Alternative Finance, UCLA Blockchain Lab καθώς και άλλες από διάφορους τομείς.

Οι εταιρικές συναλλαγές διαφέρουν από τις ατομικές και αυτές τις ανάγκες έρχεται να καλύψει η πλατφόρμα αυτή. Πιο συγκεκριμένα στις εταιρικές συναλλαγές δεν μπορεί να συμμετάσχει ο οποιοσδήποτε παρά μόνο έμπιστα και πιστοποιημένα μέλη. Αλλά και τα μέλη δεν μπορούν όλα να έχουν την ίδια πρόσβαση στο σύνολο των δεδομένων. Γίνεται εύκολα αντιληπτό στον αναγνώστη ότι ούτε όλοι οι υπάλληλοι μια εταιρίας μπορούν να έχουν πρόσβαση στα δεδομένα όλων των τμημάτων της ίδιας εταιρίας αλλά ούτε μια εταιρία μπορεί να έχει πρόσβαση στα δεδομένα μιας άλλης, τη στιγμή που μεγάλα χρηματικά πόσα δαπανούνται για να διασφαλιστούν τα διάφορα εταιρικά μυστικά. Επιπλέον, μεγάλο ρόλο παίζει και η ταχύτητα που διεκπεραιώνονται οι συναλλαγές. Η χρονική καθυστέρηση που απαιτεί το bitcoin, για παράδειγμα, για να πραγματοποιήσει μια συναλλαγή δεν είναι ανεκτή σε ένα δίκτυο εταιρικών συναλλαγών όπου οι διαδικασίες θα πρέπει να διεκπεραιώνονται άμεσα. Και φυσικά το σύστημα θα πρέπει να έχει τη δυνατότητα να επεκτείνεται επ' αόριστο, θεωρητικά, ώστε να μπορεί να συμπεριλάβει οποιαδήποτε νέα εταιρία θα θελήσει να κάνει μια συναλλαγή με τις υπάρχουσες. Στις πλατφόρμες όπως το Bitcoin και το Ethereum το δίκτυο είναι ελεύθερο για τον οποιονδήποτε θελήσει να ενταχθεί, οι συναλλαγές επιβεβαιώνονται μέσω διαδικασιών Proof Of Work οι όποιες είναι απαιτητικές σε πόρους με αποτέλεσμα και οι συναλλαγές να καθυστερούν άλλα και τα περιθώρια

κλιμάκωσης του δικτύου να είναι περιορισμένα. Πειραματικά έχει αποδειχτεί ότι το Hyperleadger έχει καλύτερη απόδοση στις συναλλαγές ανά δευτερόλεπτο σε σύγκριση με το ιδιωτικό Ethereum (Pongnumkul, Siripanpornchana, Thajchayapong 2017:1). Τέλος, το σύνολο των πληροφοριών είναι διαθέσιμες σε όλα τα μέλη ανεξαιρέτως. Είναι προφανές ότι οι λύσεις αυτές δεν μπορούν να εφαρμοστούν στις εταιρικές συναλλαγές αλλά απαιτούνται διαφορετικές προσεγγίσεις όπως αυτή που προτείνει το Hyperledger.

Οι σχεδιαστές του Hyperledger, λαμβάνοντας τα παραπάνω υπόψη, σχεδίασαν και υλοποίησαν μια τεχνολογία αλυσίδας επιτηρούμενη, στην οποία μόνο μέλη τα οποία είναι έμπιστα από τα ήδη μέλη της αλυσίδας μπορούν να εισέλθουν. Τα μέλη δεν είναι ισότιμα, αλλά διακρίνονται σε τρείς βασικές κατηγορίες (Manevich, Barger, Tock 2018):

1. Client: Ο πελάτης είναι η οντότητα που υποβάλλει την συναλλαγή προς έλεγχο. Είναι αυτός που την ξεκινά και κατόπιν τα άλλα μέλη του δικτύου θα πρέπει να την διεκπεραιώσουν.

2. Peer. Τα μέλη που ανήκουν στη κατηγορία αυτή διατηρούν τα αντίγραφα των εγγραφών του δικτύου στους σταθμούς εργασίας τους. Οι σταθμοί αυτοί αναλαμβάνουν να επιβεβαιώσουν τις συναλλαγές αλλά και να τις αποθηκεύσουν εφόσον λάβουν την απαραίτητη έγκριση.

3. Endorsers: Οι κόμβοι αυτοί εποπτεύουν και συντονίζουν τη λειτουργία των Peers. Ειδικότερα αναθέτουν στα Peers να ελέγξουν την εγκυρότητα ή όχι των συναλλαγών και στη συνέχεια εξετάζουν τις απαντήσεις τους. Στη περίπτωση που αρκετός αριθμός Peers επιβεβαιώσει μια συναλλαγή τότε ενημερώνουν το σύνολο των Peer να αποθηκεύσει τη συναλλαγή.

Η πλατφόρμα Hyperledger αποτελείται από διάφορα λογισμικά τα οποία συνεργάζονται για να δημιουργήσουν την αλυσίδα. Τα λογισμικά μπορούν να κατηγοριοποιηθούν σε τέσσερις κατηγορίες ανάλογα με τις αρμοδιότητες τους. Με τον τρόπο αυτό έχουμε τα λογισμικά που διαχειρίζονται τις βάσεις δεδομένων, τις βιβλιοθήκες όπως ονομάζονται στο Hyperledger, τα διάφορα εργαλεία, τις εφαρμογές για την εξατομίκευση των οργανισμών και τέλος τις εφαρμογές που διαχειρίζονται τις συναλλαγές.

6.3.1 Hyperledger Fabric

Θα αρχίσουμε την αναφορά μας στις εφαρμογές που αποτελούν την πλατφόρμα από το Fabric το οποίο είναι ένα ιδιωτικό blockchain του οποίου τα μέλη εποπτεύονται από μια ομάδα μελών που ονομάζεται Membership Service Providers η οποία εκδίδει πιστοποιητικά αυθεντικοποίησης των υπολοίπων μελών και κατανέμει τους διάφορους ρόλους. Για την δημιουργία εμπιστοσύνης μεταξύ των μελών η πλατφόρμα προσφέρει διάφορες επιλογές στους διαχειριστές όπως κάνει και σε πολλές άλλες λειτουργίες της καθιστώντας την με τον τρόπο αυτό την καταλληλότερη για την εκάστοτε διαφορετική περίσταση.

Για τη διασφάλιση της πληροφορίας μεταξύ των διαφορετικών μελών η πλατφόρμα δημιουργεί κανάλια οι συμμετέχοντες των οποίων διαμοιράζονται τα δεδομένα. Έτσι τα μέλη που ανήκουν στο ίδιο κανάλι μπορούν να έχουν πρόσβαση στις ίδιες πληροφορίες. Τα κανάλια αυτά δεν περιορίζονται από την εταιρία ή το τμήμα που ανήκουν αλλά από το είδος της πληροφορίας που διαθέτουν. Θα μπορούσαν, για παράδειγμα, διαφορετικές εταιρίες να ανήκουν στο ίδιο κανάλι και να έχουν πρόσβαση στη διαθέσιμη πληροφορία αποκρύπτοντας την με τον τρόπο αυτό από άλλες εταιρίες ή από τμήματα των ίδιων των εταιριών που συμμετέχουν στο κανάλι αλλά δεν έχουν πρόσβαση στη πληροφορία.

Για την αποθήκευση των συναλλαγών χρησιμοποιεί δύο είδη διαφορετικών βάσεων δεδομένων, μία για τις συναλλαγές που καλείται World State και μία για την ιστορικότητα που καλείται Transaction Log. Κάθε Peer ελέγχει την ιστορικότητα της συναλλαγής και εφόσον θεωρεί ότι είναι έγκυρη ενημερώνει το συντονιστή. Ακολούθως όταν λάβει την έγκριση ενημερώνει το World State της συναλλαγής.

Λόγω του ότι το Fabric σχεδιάστηκε για να ενσωματωθεί σε άλλες πλατφόρμες που απαιτούν μια τεχνολογία αλυσίδας, προσφέρει απλά ένα κίτ ανάπτυξης λογισμικού (SDK) για τις γλώσσες προγραμματισμού Node.js, Java και Go. Για την σύνταξή των έξυπνων συμβολαίων προσφέρει σαν επιλογές την JavaScript, TypeScript και τη Go. Μπορεί όμως να δεχθεί και τη Java μέσω την εγκατάστασης ενός πρόσθετου λογισμικού.

6.3.2 Hyperledger Sawtooth

Η πλατφόρμα αυτή αρχικά ξεκίνησε από την Intel προτού ενσωματωθεί στο Hyperledger και το βασικό χαρακτηριστικό της είναι ότι διαχωρίζει τον πυρήνα του συστήματος από το χώρο των

εφαρμογών δίνοντας έτσι περισσότερη ευελιξία στις εταιρίες αφού τους επιτρέπει να σχεδιάσουν τα έξυπνα συμβόλαια τους χωρίς να απασχολούνται με τον τρόπο που λειτουργεί ο πυρήνας της αλυσίδας. Στο τομέα των πρωτοκόλλων συναίνεσης η πλατφόρμα επιτρέπει την εναλλαγή μεταξύ των διαφόρων επιλογών χωρίς να απαιτείται να τεθεί εκτός λειτουργίας το δίκτυο επιτυγχάνοντας έτσι την αύξηση της απόδοσης και της ευελιξίας. Ειδικά όταν λάβουμε υπόψη ότι η διαδικασία αυτή είναι η πλέον απαιτητικότερη σε πόρους και σε χρόνο με αποτέλεσμα να καθορίζει την κλιμάκωση και την απόδοση του δικτύου, γίνεται εύκολα αντιληπτό στον αναγνώστη πόσο σημαντική είναι η δυνατότητα να χρησιμοποιηθεί ένα γρηγορότερο πρωτόκολλο σε περιόδους συμφόρησης και η εναλλαγή αυτή να γίνεται χωρίς να επηρεάζεται η λειτουργία του δικτύου.

Για την υποστήριξη των έξυπνων συμβολαίων η πλατφόρμα παρέχει στους προγραμματιστές πληθώρα επιλογών όπως Python, Java, C++, GO, JavaScript, και Rust. Τέλος μπορεί να δεχθεί και έξυπνα συμβόλαια από το Ethereum αφού υποστηρίζει και τη Solidity.

6.3.3 Hyperledger Burrow

Η πλατφόρμα έχει σχεδιαστεί για να παρέχει ταχύτητα και ευελιξία στην ανάπτυξη και να είναι όσο το δυνατόν πιο εύκολη στη χρήση. Υποστηρίζει έξυπνα συμβόλαια τόσο του Ethereum αλλά και της Wasm ενώ για πρωτόκολλο εμπιστοσύνης χρησιμοποιεί το Byzantine Fault Tolerance μέσω του Tendermimt αλγόριθμου. Αρχικά ξεκίνησε από την Monax σαν μια πλατφόρμα ανοιχτού κώδικα με στόχο την δημιουργία και εκτέλεση εφαρμογών που βασίζονται σε τεχνολογία αλυσίδας προσαρμοσμένες σε εταιρικά συστήματα.

Όταν προκύπτει μια συναλλαγή στο δίκτυο ενεργοποιεί την εκτέλεση του κώδικα ενός έξυπνου συμβολαίου την οποία αναλαμβάνει να διεκπεραιώσει μία πρόσθετη εφαρμογή που ονομάζετε Smart Contract Application. Αυτή, εκτελεί τον κώδικα μέσα σε ένα ασφαλές και εποπτευόμενο περιβάλλον εικονικής μηχανής του Ethereum (Ethereum Virtual Machine). Η εικονική μηχανή πέρα από την εκτέλεση του κώδικα ελέγχει αν πληρούνται οι προδιαγραφές του κώδικα που έχει ορίσει το Ethereum καθώς και αν τηρούνται τα απαραίτητα δικαιώματα του.

6.3.4 Hyperledger Explorer

Η εφαρμογή αυτή παρέχει ένα φιλικό προς το χρήστη περιβάλλον μέσω του οποίου μπορούν οι χρήστες να βλέπουν τις υπάρχουσες συναλλαγές, να ξεκινούν νέες, καθώς και να αντλούν διάφορες πληροφορίες που συνοδεύουν τις συναλλαγές όπως όνομα, κατάσταση, λίστα των κόμβων που τις χειρίζονται καθώς και άλλα. Πρόκειται για ένα ιδιαίτερα σημαντικό εργαλείο αφού όπως προαναφέρθηκε οι περισσότερες πλατφόρμες παρέχουν απλά ένα SDK το οποίο δεν διευκολύνει την πρόσβαση στις διάφορες πληροφορίες της αλυσίδας. Το έργο αρχικά είχε ξεκινήσει από συνεισφορές μεγάλων εταιριών όπως η IBM, η Intel και η DTCC.

6.3.5 Hyperledger Cello

Η εφαρμογή αυτή έχει σαν στόχο να διευκολύνει την διαδικασία δημιουργίας, διαχείρισης και χρήσης της αλυσίδας. Έχει τη δυνατότητα να λειτουργήσει αυτόνομη, χωρίς την υποστήριξη λειτουργικού συστήματος και κατά συνέπεια να εγκατασταθεί σε Baremetal, ή σε εικονικό μηχάνημα απαλλάσσοντας τους χρήστες από το κόστος αγοράς και χρήσης λειτουργικού συστήματος. Μέσω της εφαρμογής αυτής η υπηρεσία της αλυσίδας μπορεί να προσφερθεί με την μορφή του ‘as-a-service’ προσφέροντας έτσι ακόμα μεγαλύτερη ευελιξία στους χρήστες.

6.3.6 Hyperledger Caliper

Λόγω των διαφορετικών προτάσεων που προσφέρει η πλατφόρμα κρίνεται σκόπιμο να υπάρξει μια εφαρμογή που θα μετρά την απόδοση των διαφόρων προτάσεων ώστε οι υλοποιητές να μπορούν να ελέγξουν την απόδοση της επιλογής τους και να αποφασίσουν αν πληροί τις προδιαγραφές τους ή θα πρέπει να επιλέξουν μια διαφορετική πρόταση. Αυτή την εργασία επιτελεί η εφαρμογή αυτή. Χρησιμοποιείται για να μετρηθεί η απόδοση της εφαρμογής κατά τη διάρκεια εκτέλεσης καθορισμένων σεναρίων, δίνοντας πληροφορίες για τον αριθμό συναλλαγών ανά δευτερόλεπτο, τη καθυστέρηση, τη απορρόφηση των πόρων και άλλα. Τα αποτελέσματα αυτά εκτιμώνται και συγκρίνονται με αυτά των άλλων λύσεων όπως του Fabric, του Sawtooth, του Burrow καθώς και των υπολοίπων που προσφέρει η πλατφόρμα. Κατόπιν οι χρήστες μπορούν να επιλέξουν την πρόταση που παρουσιάζει τα καλύτερα αποτελέσματα.

6.3.7 Hyperledger Grid

Η πλατφόρμα αυτή προσφέρεται για την δημιουργία εφαρμογών που σχετίζονται με την αλυσίδα τροφοδοσίας, Data models και έξυπνων συμβολαίων, εστιασμένα στη εταιρική λογική, βάση υπαρχόντων επιχειρηματικών μοντέλων καθώς και τις εκάστοτε βέλτιστες επιχειρηματικές πρακτικές. Με τον τρόπο αυτό παρουσιάζει πρακτικούς τρόπους εφαρμογής των μεθόδων του Hyperlegder σε μία αποδοτική επιχειρηματική λύση.

6.4 R3's Corda

Η πλατφόρμα της εταιρίας διαφέρει ουσιαστικά από ότι έχουμε δει έως τώρα με βασικότερο χαρακτηριστικό ότι είναι εστιασμένη στον οικονομικό τομέα με αποτέλεσμα να μην είναι κατάλληλη για άλλους τομείς. Ένας από τους βασικότερους λογούς που συμβαίνει αυτό είναι ότι δεν επιτρέπει σε όλα τα μέλη να διατηρούν αντίγραφα του συνόλου των συναλλαγών, μόνο τα μέλη που συμμετάσχουν ενεργά σε μια συναλλαγή διαθέτουν αντίγραφά της. Με τον τρόπο αυτό διασφαλίζεται ότι μόνο τα μέλη που έχουν δικαίωμα στη πληροφορία έχουν πρόσβαση σε αυτή και επιπλέον βελτιώνεται η απόδοση αλλά και η επεκτασιμότητα του συστήματος. Στη κατεύθυνση αυτή συμβάλει και το γεγονός ότι χρησιμοποιεί σχεσιακή βάση δεδομένων προσφέροντας διάφορες επιλογές μεταξύ αυτών της Microsoft τον SQL Server, της Oracle αλλά και μια δική της, την h2.

Τα έξυπνα συμβόλαια που χρησιμοποιούνται στη πλατφόρμα, πέρα από το κώδικα, περιέχουν και νομικές εκφράσεις προκειμένου να ενισχύσουν την αξιοπιστία τους. Για την επιβεβαίωση των συναλλαγών ελέγχεται το σύνολο της ιστορικότητας μιας συναλλαγής και η εμπιστοσύνη δεν προκύπτει από μεθόδους εξόρυξης, ή Proof Of Work, αλλά μέσω της απόδειξης της εγκυρότητας αλλά και της μοναδικότητας της κάθε συναλλαγής. Αυτά επιτυγχάνονται μέσω των έξυπνων συμβολαίων που ελέγχουν ότι καμιά άλλη συναλλαγή δεν χρησιμοποιεί τις τιμές μιας άλλης συναλλαγής και επομένως η συναλλαγή είναι μοναδική και έγκυρη.

Επιπλέον, μέριμνα έχει δοθεί και σε θέματα όπως το τοίχος προστασίας του δικτύου (Firewall) όπου επιτρέπει την είσοδο μόνο σε κόμβους που είναι μέλη του δικτύου , καθώς και σε θέματα υποστήριξης όπου σύμφωνα με την εταιρία παρέχετε υποστήριξη τύπου 24/7. Κάτι τέτοιο καθιστά τη πλατφόρμα ιδιαίτερος δημοφιλή ειδικά για μια εταιρία που έχει στενά περιθώρια down time. Επιπλέον, αν συνδυάσει κανείς την υποστήριξή αυτή με το γεγονός ότι η πλατφόρμα

είναι ανοιχτού κώδικα, πράγμα που σημαίνει ότι δεν απαιτείτε η καταβολή κάποιου αντίτιμου για την απόκτηση και χρήση της, γίνεται άμεσα αντιληπτό το πόσο δελεαστική καθίσταται η πλατφόρμα αυτή έναντι των άλλων.

Τέλος, είναι σημαντικό να αναφέρουμε και άλλες εξίσου ενδιαφέρουσες παροχές της πλατφόρμας όπως εφαρμογή για παρακολούθηση της απόδοσης αλλά και της διαθεσιμότητας της πλατφόρμας, ενισχυμένη ασφάλεια, υψηλή διαθεσιμότητα, υπηρεσίες ανάκαμψης .

6.5 Συμπεράσματα

Για τη υλοποίηση του δικού μας έξυπνου συμβολαίου, αποφασίσαμε να χρησιμοποιήσουμε το Hyperledger Fabric λόγω των ακόλουθων εκτιμήσεων:

- Το Fabric έχει υψηλό ποσοστό συναλλαγών ανά δευτερόλεπτο (TPS) αφού η επίτευξη συναίνεσης δεν απαιτεί συμφωνία από όλα τα μέλη της αλυσίδας. Έτσι, η οριστικότητα μιας συναλλαγής είναι άμεση.

- Η πληρωμή αμοιβής συναλλαγής στο Fabric δεν είναι υποχρεωτική.

- Δεν υπάρχει όριο υπολογιστικής ισχύος σε αντίθεση με το όριο GAS του Ethereum.

- Η αναγνώριση μέλους μπορεί να επαληθευτεί μέσω του Membership Service Provider (**MSP**).

- Για τη διασφάλιση της πληροφορίας μεταξύ των διαφορετικών μελών η πλατφόρμα δημιουργεί κανάλια οι συμμετέχοντες των οποίων διαμοιράζονται τα δεδομένα. Έτσι τα μέλη που ανήκουν στο ίδιο κανάλι μπορούν να έχουν πρόσβαση στις ίδιες πληροφορίες

- Το δίκτυο Fabric είναι εξαιρετικά επεκτάσιμο. Μόλις ένας νέος οργανισμός θελήσει να ενταχθεί αρκεί να δημιουργηθεί ένα νέο κανάλι που θα περιλαμβάνει τους νεοεισερχόμενους.

- Παρέχει στους προγραμματιστές πληθώρα επιλογών όπως Python, Java, C++, GO, JavaScript, και Rust. Τέλος μπορεί να δεχθεί και έξυπνα συμβόλαια από το Ethereum αφού υποστηρίζει και τη Solidity.

Κεφάλαιο 7
Το Τραπεζικό Σύστημα

Στο κεφάλαιο αυτό θα παρουσιάσουμε μια εικόνα του τραπεζικού συστήματος και θα αναφερθούμε στις βελτιώσεις που μπορεί να επιφέρει η εφαρμογή της τεχνολογίας αλυσίδας σε συνδυασμό με την χρήση των έξυπνων συμβολαίων όπως και ποια προβλήματα πρέπει να αντιμετωπίσουν.

7.1 Ο Τραπεζικός Τομέας

Ο τραπεζικός τομέας περιλαμβάνει όλους εκείνους τους οργανισμούς που εκτελούν τον ρόλο του διαμεσολαβητή ανάμεσα σε εκείνους που αποταμιεύουν και στους πιστούχους. Πρόκειται για ένα από τα σημαντικότερα όργανα που συμβάλλουν στην ανάπτυξη μιας εθνικής οικονομίας μέσω της τόνωσης της εγχώριας ζήτησης, της χρηματοδότησης των δυναμικών κλάδων της αλλά και των καινοτόμων επενδυτικών πρωτοβουλιών.

Από τους οργανισμούς που τον απαρτίζουν ο πλέον γνωστότερος είναι οι Τράπεζές οι οποίες παίζουν και το μεγαλύτερο ρόλο στην οικονομία μιας χώρας, μιας και η υγεία της οικονομίας είναι στενά συνδεδεμένη με την κατάσταση της υγείας των τραπεζών της. Αυτό συμβαίνει διότι όταν οι τράπεζες διαθέτουν τα απαραίτητα αποθέματα μπορούν να δανειοδοτήσουν τους καταναλωτές και κατά συνέπεια να οδηγήσουν την οικονομία σε ανάπτυξη. Η κρίση που βίωσε ο πλανήτης την τελευταία δεκαετία ξεκίνησε από τον τραπεζικό κλάδο με την κατάρρευση των στεγαστικών δανείων στις ΗΠΑ. Τον τομέα συμπληρώνουν επενδυτικοί οργανισμοί, ασφαλιστικές εταιρίες, εταιρίες χρηματοδότησης, διαχειριστές επενδύσεων αλλά και άλλες που δραστηριοποιούνται στο τομέα της δημιουργίας αλλά και ροής χρημάτων.

Η ιδέα του δανεισμού χρημάτων, που αποτελεί τη βασικότερη λειτουργία των τραπεζών χρονολογείται από τα χρόνια της αρχαίας Βαβυλωνίας όπου οι έμποροι παρείχαν δάνεια σε μορφή σιτηρών ως εγγύηση για τις συναλλαγές τους. Αναφορές εντοπίζονται και στην αρχαία Ελλάδα όπου οι δανειστές δεχόντουσαν καταθέσεις και εκτελούσαν και μετατροπές νομισμάτων. Αλλά

και στην αρχαία Κίνα και στην Ινδία έχουν εντοπιστεί ευρήματα που αποδεικνύουν την ύπαρξη δανειστών. Η πρώτες αναφορές τραπεζικού ιδρύματος προέρχονται όμως από την Ιταλία το 14ο αιώνα όπου οι πρωτοεμφανιζόμενες τράπεζες διαδραμάτισαν σημαντικό ρόλο στην άνοδο των ιταλικών πόλεων – κρατών σε παγκόσμιες οικονομικές δυνάμεις.

Η λειτουργία των τραπεζών καθορίζεται από το θεσμικό πλαίσιο που έχει ορίσει το κάθε κράτος το οποίο είναι εναρμονισμένο με την διεθνή νομοθεσία καθώς και τους κανονισμούς των επιμέρους κρατών. Επιπλέον κάθε κράτος διαθέτει δύο είδη τραπεζών, την Κεντρική Τράπεζα και τις Εμπορικές Τράπεζες.

Η Κεντρική Τράπεζα αποτελεί μία ανεξάρτητη αρχή που υπόκειται στον έλεγχο του Κράτους και μεριμνά για την σταθερότητα των τιμών αλλά και την εύρυθμη λειτουργία του χρηματοπιστωτικού συστήματος. Διαφέρει από τις εμπορικές τράπεζες με την έννοια ότι δεν δίνει δάνεια σε πολίτες ούτε δέχεται καταθέσεις από αυτούς. Μπορεί όμως να δώσει δάνεια στις τράπεζες της ίδιας χώρας και να λάβει καταθέσεις από αυτές.

Στα πλαίσια των αρμοδιοτήτων της μπορούμε να ξεχωρίσουμε τα ακόλουθα:

- Εποπτεύει τα πιστωτικά ιδρύματα διεξάγοντας επιτόπιους ελέγχους είτε σε περιοδική είτε σε έκτακτη βάση. Είναι αυτή που ορίζει τα επιτόκια του δανεισμού δεν εποπτεύει όμως τις σχέσεις τους με τους πολίτες με εξαίρεση περιπτώσεις που αφορούν την διαφάνεια των διαδικασιών αλλά και των όρων των τραπεζικών συναλλαγών.

- Εκδίδει τα τραπεζογραμμάτια και τους προσδίδει την καθορισμένη αξία και στη συνέχεια προμηθεύει με αυτά τις εμπορικές τράπεζες. Με τον τρόπο αυτό ελέγχει και μεταβάλει τη προσφορά του εγχώριου χρήματος. Παράλληλα διαχειρίζεται την απόσυρση και την αντικατάσταση των φθαρμένων τραπεζογραμματίων.

- Συμβάλλει στη διατήρηση της σταθερότητας των τιμών μέσω τις άσκησης νομισματικής πολιτικής. Ενδεικτικά να αναφέρουμε ότι στη ζώνη του Ευρώ οι αποφάσεις για την νομισματική πολιτική λαμβάνονται από το Διοικητικό Συμβούλιο της Ευρωπαϊκής Κεντρικής Τράπεζας και ο στόχος της νομισματικής πολιτικής είναι οι τιμές να αυξάνονται με ρυθμό κάτω από το 2% σε ετήσια βάση.

- Ενημερώνει για ζητήματα της οικονομίας μέσω διεξαγωγής ερευνών και τα γνωστοποιεί μέσω των διαφόρων δημοσιεύσεων. Ποιο συγκεκριμένα εστιάζει σε θέματα νομισματικής πολιτικής, οικονομικής και περιφερικής ανάπτυξης, οικονομίας των αγορών του χρήματος αλλά και του κεφαλαίου, εποπτικής πολιτικής καθώς και συνεπειών της κλιματικής αλλαγής. Τα ευρήματα αυτά δημοσιεύονται είτε ως επιστημονικά δοκίμια εργασίας, είτε στο Οικονομικό Δελτίο της Τράπεζας, είτε ως μέρος των Εκθέσεων του Διοικητή της Κεντρικής Τράπεζας.

Οι εμπορικές τράπεζες από την άλλη πλευρά έχουν σαν στόχο την ικανοποίηση των συναλλαγματικών αναγκών τόσο των πολιτών όσο και των επιχειρήσεων. Δέχονται καταθέσεις καταβάλλοντας ένα επιτόκιο στους καταθέτες και ακολούθως διαθέτουν τα χρήματα αυτά με τη μορφή του δανεισμού εισπράττοντας το αντίστοιχο επιτόκιο. Ειδικότερα για τις εμπορικές τράπεζες μπορούμε να ξεχωρίσουμε ότι:

- Λειτουργούν ως διαμεσολαβητές μεταξύ αυτών που αποταμιεύουν και αυτών που λαμβάνουν χρήματα με τη μορφή δανείου.

- Επηρεάζουν την προσφορά του χρήματος σε μία οικονομία μέσω της ποσότητας των χρημάτων που διαθέτουν με τη μορφή του δανεισμού.

- Από τα χρήματα που διαθέτουν ως αποθεματικά είναι υποχρεωμένες ένα ποσοστό να το διατηρούν και να μην το διαθέτουν προς δανεισμό. Το ποσοστό αυτό ορίζετε από την Κεντρική Τράπεζα και προορίζετε για την κάλυψη έκτακτων αναγκών που μπορεί να προκύψουν και να οδηγήσουν τους καταθέτες να ζητήσουν μέρος των καταθέσεών τους.

Τέλος οι εμπορικές τράπεζες δραστηριοποιούνται σε διάφορους κλάδους από τους όποιους θα αναφερθούμε στον λιανικό, στον εμπορικό, στην κεφαλαιαγορά και τέλος στον επενδυτικό κλάδο. Οι κλάδοι αυτοί αρχικά λειτουργούσαν ανεξάρτητοι και σε ξεχωριστούς οργανισμούς, τα τελευταία όμως χρόνια τείνουν να ενσωματώνονται καθώς όλο και περισσότερες τράπεζες, προκειμένου να γίνουν πιο ανταγωνιστικές επεκτείνονται και στους άλλους κλάδους προσφέροντας αντίστοιχα προϊόντα.

7.1.1 Λιανική Τραπεζική

Ο κλάδος αυτός περιέχει τα προϊόντα και τις υπηρεσίες που στοχεύουν στην εξυπηρέτηση του ευρύ καταναλωτικού κοινού που αποτελείτε από τους ιδιώτες, τα νοικοκυριά, τις μικρές και μεσαίες επιχειρήσεις. Μια λιανική τράπεζα θα μπορούσε να δεχθεί καταθέσεις και από μεγάλες εταιρίες ή να τις δανειοδοτήσει με τον όρο ότι το ύψος του δανείου ή των καταθέσεων θα παραμένουν σε χαμηλά επίπεδα, η περίοδος αποπληρωμής θα έχει σχετικά μικρό ορίζοντα και δεν θα περιλαμβάνονται περίπλοκες διαδικασίες αποπληρωμής. Μεταξύ των δανειακών αυτών προϊόντων μπορούμε να ξεχωρίσουμε τις πιστωτικές κάρτες, τα καταναλωτικά και προσωπικά δάνεια, τα στεγαστικά καθώς και τα δάνεια σε μικρές και μεσαίες επιχειρήσεις. Οι καταθέσεις από την άλλη πλευρά διακρίνονται σε βραχυπρόθεσμες και σε μακροπρόθεσμες με βασικό διαχωρισμό το ύψος του επιτοκίου.

7.1.2 Εμπορική Τραπεζική

Για την κάλυψη των αναγκών των πολύ μεγάλων επιχειρήσεων αρμόδιες είναι οι εμπορικές τράπεζες οι όποιες δύνανται να δανειοδοτήσουν με μεγάλους χρηματικούς όγκους καθώς και με πιο πολύπλοκες διαδικασίας αποπληρωμής. Συχνά οι τράπεζες αυτές σχηματίζουν κοινοπραξίες με σκοπό να χρηματοδοτήσουν στη περίπτωση που το ύψος του δανείου είναι τόσο υψηλό που δεν μπορεί να καλυφθεί από μεμονωμένες τράπεζες. Οι εμπορικές τράπεζες συχνά αλλάζουν και ρόλους αφού από δανειστές γίνονται μέτοχοι μετατρέποντας το αρχικό δάνειο που διέθεσαν σε μια εταιρία σε μετοχικό κεφάλαιο. Τέλος αξίζει να αναφερθεί ότι οι εμπορικές τράπεζες δεν μπορούν να εφαρμόσουν τις ίδιες πρακτικές μάρκετινγκ της λιανικής τραπεζικής μιας και η δανειοδότηση των μεγάλων αυτών εταιριών θα πρέπει να είναι προσαρμοσμένη στις ανάγκες της εκάστοτε περίπτωσης και άρα προκύπτει μέσω ξεχωριστών κάθε φορά συμφωνιών.

7.1.3 Επενδυτική Τραπεζική

Οι επενδυτικές τράπεζες αναλαμβάνουν να βοηθήσουν τις δημόσιες αλλά και τις ιδιωτικές εταιρίες στη συλλογή κεφαλαίων από τις κεφαλαιαγορές και γενικότερα μέσω στρατηγικών γνωμοδοτικών υπηρεσιών που αφορούν συγχωνεύσεις, κτήσεις αλλά και άλλους τύπους οικονομικών συναλλαγών. Στην αρχική τους μορφή διέφεραν από τις εμπορικές τράπεζες αλλά τα τελευταία χρόνια τείνουν να ενσωματωθούν σε αυτές μιας και οι εμπορικές τράπεζες έχουν αρχίσει να διευρύνουν τις υπηρεσίες που παρέχουν. Ο διαχωρισμός αυτός υπαγορεύτηκε δια νόμου στις ΗΠΑ μετά το κραχ του 1929 με στόχο να αποτρέψει μελλοντική επανάληψη του αλλά

καταργήθηκε το 1999. Άλλες χώρες, συμπεριλαμβανομένων και των υπολοίπων του G7 δεν προέβλεπαν τέτοιο διαχωρισμό.

7.1.4 Κλάδος Κεφαλαιαγοράς

Στο τομέα αυτό περιλαμβάνονται οι τράπεζες που η αποστολή τους είναι η διεκπεραίωση των αγοροπωλησιών των μετοχών, χρεογράφων και αμοιβαίων κεφαλαίων. Οι τράπεζες αυτές τείνουν να ενταχθούν στις επενδυτικές τράπεζες με πιο γνωστά παραδείγματα αυτό της Goldman Sachs, της UBS και τη Houlihan Lokey.

7.2 Λειτουργίες των Τραπεζών

Ο πρωταρχικός ρόλος μιας Τράπεζας είναι η αποδοχή για φύλαξη των καταθέσεων των καταναλωτών. Οι καταθέσεις αυτές χωρίζονται σε δύο κατηγορίες, τις καταθέσεις των πολιτών που καλούνται και καταθέσεις πυρήνα και τις καταθέσεις χονδρικής.

Οι καταθέσεις πολιτών έχουν συνήθως πολύ σύντομες προθεσμίες και αυτό διότι οι άνθρωποι έχουν την τάση να τοποθετούν τα χρήματα τους στη τράπεζα όταν τα εισπράττουν και στη συνέχεια να τα αποσύρουν σταδιακά για να καλύψουν τις τρέχουσες ανάγκες τους. Με τον τρόπο αυτό ενώ οι καταναλωτές διατηρούν λογαριασμούς για μεγάλα χρονικά διαστήματα έχουν το δικαίωμα να αποσύρουν πλήρως τα ποσά ανά πάσα χρονική στιγμή. Η διαδικασία προβλέπει την υποβολή μιας αίτησης από τον ενδιαφερόμενο και συνήθως απαιτεί χρονικό διάστημα μερικών ημερών ανάλογα με τη τράπεζα και το ύψος του ποσού. Καθίσταται προφανές στον αναγνώστη ότι το σύστημα έχει όρια με την έννοια ότι αν όλοι οι καταθέτες ζητήσουν τις καταθέσεις τους οι τράπεζες δεν θα μπορούν να ανταπεξέλθουν μιας και το μεγαλύτερο μέρος αυτών δεν είναι διαθέσιμο αφού έχει προσφερθεί σε άλλους πελάτες μέσω του δανεισμού.

Οι καταθέσεις χονδρικής χαρακτηρίζουν κατά βάση τα διατραπεζικά δάνεια τα όποια συνάπτονται προκειμένου μια τράπεζα να ενισχύσει τη διαθέσιμη της ρευστότητα. Η επιλογή αυτή είναι πιο δαπανηρή από την άντληση κεφαλαίων από τις καταθέσεις πολιτών μιας και τα επιτόκια είναι κατά πολύ υψηλότερα. Κατά συνέπεια η πρακτική αυτή θα πρέπει να αποφεύγετε καθώς αποτελεί δείγμα ότι η συγκεκριμένη τράπεζα δεν είναι πλέον τόσο ανταγωνιστική όσο οι υπόλοιπες. Μέτρα για την μείωση της έκθεσης στον διατραπεζικό δανεισμό αποτελούν μεταξύ άλλων η μείωση κερδών, η μείωση του λειτουργικού κόστους καθώς και η αύξηση των

επενδυτικών αποδόσεων πράγμα όμως που πιθανόν να επιφέρει μεγαλύτερο κίνδυνο στις επενδύσεις αυτές.

Παράλληλα με τις καταθέσεις, σημαντικό μέρος του κεφαλαίου μια τράπεζας αποτελεί και το μετοχικό κεφάλαιο που διαθέτει. Το κεφάλαιο αυτό προκύπτει είτε από αγορά μετοχών άλλων εταιριών είτε από την έκδοση μετοχών της ίδιας της τράπεζας. Η απόκτηση του κεφαλαίου αυτού είναι δαπανηρή και για το λόγο αυτό οι τράπεζες προβαίνουν στην τακτική αυτή όταν θα πρέπει να αντλήσουν κεφάλαια, για να πραγματοποιήσουν κάποια αγορά ή για να αποκαταστήσουν την κεφαλαιακή τους θέση μετά από μία περίοδο αυξημένων επισφαλών δανείων.

Τα κεφάλαια που συγκεντρώνουν οι τράπεζες, τα διοχετεύουν στην αγορά με τη μορφή δανείων για τα οποία εισπράττουν το εκάστοτε επιτόκιο το οποίο αποτελεί άλλο ένα μέρος των εσόδων τους. Τα δάνεια προσφέρονται κατόπιν σύνταξης των απαραίτητων συμφωνητικών με σταθερά ή με κυμαινόμενα επιτόκια. Σε αρκετές περιπτώσεις, για την έκδοση του δανείου απαιτείται κάποιο είδος εγγύησης, που μπορεί να δοθεί είτε μέσω προσώπου είτε μέσω κάποιου περιουσιακού στοιχείου αντίστοιχου του ύψους του δανείου. Οι δανειολήπτες δε, έχουν την δυνατότητα να αποπληρώσουν το δάνειο είτε στη προσυμφωνημένη χρονική περίοδο είτε νωρίτερα καταβάλλοντας συνήθως κάποια ρήτρα για τη μη τήρηση των συμφωνημένων.

Σαν τελευταία πηγή εσόδων θα αναφέρουμε τα κεφάλαια που αντλούνται μέσω της διαδικασίας έκδοσης χρεογράφων. Το χρεόγραφο ουσιαστικά είναι ένα επενδυτικό διαπραγματεύσιμο προϊόν που εκδίδεται από κάποιο οργανισμό και αποτελεί αποδεικτικό χρέους ή δικαίωμα σε διανεμόμενα κέρδη. Οι τράπεζες αγοράζουν τα χρεόγραφα και κατόπιν τα εισπράττουν οι ίδιες ή τα μεταπουλούν. Σαν ποσοστό το χρέος είναι συνήθως πολύ χαμηλότερο από το συνολικό πόσο των καταθέσεων ή δανείων και ως εκ τούτου δεν αποτελεί ζωτική πηγή δανειοληπτικών κεφαλαίων.

7.3 Η Τεχνολογία Αλυσίδας στο Τραπεζικό Τομέα

Έχοντας ολοκληρώσει την παρουσίαση της τεχνολογίας αλυσίδας και του τραπεζικού τομέα μπορούμε πλέον να διερευνήσουμε τα σημεία στα οποία οι δύο τομείς θα μπορούσαν να συνδυαστούν. Καθίσταται γρήγορα αντιληπτό στον αναγνώστη ότι η τεχνολογία έχει πολλά να προσφέρει στον τραπεζικό τομέα. Μάλιστα η επιστημονική κοινότητα στο Παγκόσμιο Οικονομικό Φόρουμ (WEF) του 2016 πρόβλεψε ότι η τεχνολογία θα φέρει επανάσταση στον οικονομικό

τομέα ενώ το UN Future την ενέταξε μεταξύ των 10 μελλοντικών τεχνολογιών. Ο Διοικητής της Τράπεζας της Ελλάδας Γιάννης Στουρνάρας , σε ομιλία του σε ημερίδα που διοργάνωσε η Εθνικής Αρχής Διαφάνειας με αφορμή τη Παγκόσμια Ημέρα κατά της Διαφθοράς επισήμανε ότι η τεχνολογία του BlockChain μπορεί να επιφέρει σημαντική μείωση του κόστους των συναλλαγών.

Ποιο συγκεκριμένα οι Shah και Jani (Shah, Jani 2018) διαχώρισαν τις περιπτώσεις όπου η τεχνολογία αλυσίδας δύναται να επιφέρει σημαντικά οφέλη στο τραπεζικό τομέα.

- Μεσολαβητές. Η ύπαρξη διαμεσολαβητών προκαλεί αύξηση του κόστους των συναλλαγών με την υποχρέωση καταβολής προμήθειας, προκαλεί σημαντική καθυστέρηση στις συναλλαγές και συχνά επιβάλλεται λόγω της έλλειψης εμπιστοσύνης μεταξύ των συναλλασσόμενων μελών. Η τεχνολογία μέσω του διαμερισμού της πληροφορίας στα συναλλασσόμενα μέλη λύνει το πρόβλημα της εμπιστοσύνης, ταχύτητας αλλά και μειώνει το κόστος της συναλλαγής.

- Διαφάνεια. Λόγω του μεγάλου αριθμού των συμμετεχόντων, η διαφάνεια στις συναλλαγές είναι απαραίτητη προκειμένου αυτοί να διευκολυνθούν. Η τεχνολογία αλυσίδας, χάρη στις συναρτήσεις κατακερματισμού που χρησιμοποιεί καθιστά τις εγγραφές αμετάβλητες και μη αναστρέψιμες μειώνοντας έτσι σημαντικά το κίνδυνο της απάτης.

- Αποθήκευση της πληροφορίας. Η ύπαρξη πολλαπλών αντιγράφων της ίδιας πληροφορίας σε πολλά και διαφορετικά σημεία εγείρει ερωτήματα του τύπου κατά πόσον η πληροφορία είναι ενημερωμένη και συνεπής. Η κατανομή της πληροφορίας διασφαλίζει την ενημέρωση της στα διάφορα σημεία ενώ τα πρωτοκολλά συναίνεσης επιτυγχάνουν την συνέπεια.

- Χειρωνακτική Επεξεργασία. Οι υπάρχουσες διαδικασίες περιλαμβάνουν πολλές λειτουργίες που απαιτούν την ανθρώπινη παρέμβαση με αποτέλεσμα να είναι απαιτητικές σε χρόνο αλλά και σε εργατοώρες. Η τεχνολογία παρέχει προτάσεις για αυτοματοποίηση των διαδικασιών μειώνοντας έτσι την ανθρώπινη εργασία.

- Εμπιστοσύνη. Όπως προαναφέρθηκε, η εμπιστοσύνη μεταξύ των χρηστών αποτελεί σημαντικό ζήτημα. Θα πρέπει να διερευνηθούν ζητήματα όπως ποιοι από τα μέλη έχουν δικαίωμα να τροποποιούν συναλλαγές καθώς και τρόποι να προστατευθεί το σύστημα από κακόβουλες συναλλαγές. Η τεχνολογία διαθέτει και τους μηχανισμούς συναίνεσης

αλλά και τα έξυπνα συμβόλαια που επιβεβαιώνουν τις συναλλαγές ώστε να μειώνετε σημαντικά ο κίνδυνος εξαπάτησης.

- Τεκμηρίωση. Μέρος της τεκμηρίωσης των διαδικασιών αλλά και των διαφόρων αναφορών είναι σε έντυπο μέσο, ο όγκος του οποίου θα μπορούσε να μειωθεί σημαντικά με τη χρήση των έξυπνων συμβολαίων που αναλαμβάνουν να τηρούν τις εταιρικές συμφωνίες.

- Χρονικά περιθώρια. Ο χρόνος των συναλλαγών θα βελτιωθεί σημαντικά αφού η τεχνολογία μπορεί να τις διεκπεραιώνει σε πραγματικό χρόνο ακόμα και αν γίνονται σε διαφορετικά κράτη.

Άξια αναφοράς είναι και μελέτη που πραγματοποιήθηκε (Peter , Moser 2017:142) σχετικά με τις ευκαιρίες υλοποίησης της τεχνολογίας αλυσίδας στον τραπεζικό τομέα γερμανόφωνων περιοχών της Ευρώπης. Ειδικότερα σε ένα κοινό αποτελούμενο από 110 άτομα από το τραπεζικό κλάδο, 10 από το Χρηματιστηριακό, 7 παρόχους πιστωτικών καρτών, 23 από το κλάδο της τεχνολογίας, 17 από εταιρίες που δραστηριοποιούνταν στο συμβουλευτικό χώρο και τέλος 15 από Κρατικά και Ευρωπαϊκά ιδρύματα, απεύθυναν τις ακόλουθες ερωτήσεις:

- Η εταιρία σας μελετά την υιοθέτηση της τεχνολογίας για την διενέργεια συναλλαγών;

- Ποια τα πλεονεκτήματα της σε σύγκριση με το προηγούμενο σύστημα σας;

- Ποια τα θέματα που καλείστε να αντιμετωπίσετε κατά την ενσωμάτωση της τεχνολογίας;

- Ποιες οι προβλέψεις σας για το μέλλον των ψηφιακών συναλλαγών;

- Έχει περιέλθει στην αντίληψη σας άλλος οργανισμούς που επίσης δραστηριοποιείτε στον οικονομικό τομέα να σχεδιάζει την εφαρμογή της τεχνολογίας;

- Έχετε υπόψη σας εφαρμογές βασισμένες στη τεχνολογία;

Τα αποτελέσματα έδειξαν ότι καμία από τις τράπεζες που ανταποκρίθηκαν στο ερωτηματολόγιο δεν σκόπευε να υλοποιήσει την τεχνολογία με μοναδική εξαίρεση μία τράπεζα η οποία διερευνούσε ένα σύστημα, το Ripple. Βασική αιτία αυτού αποτελεί το γεγονός ότι οι τράπεζες είναι ιδιαίτερα συντηρητικές όσο αφορά τις νέες τεχνολογίες. Αναγνωρίζονται φυσικά οι προοπτικές

όπως η διευκόλυνση των διεθνών συναλλαγών αλλά το ενδιαφέρον παραμένει σε χαμηλά επίπεδα καθώς η οποιαδήποτε προσπάθεια υιοθέτησης της τεχνολογίας προϋποθέτει την συμμετοχή μεγάλου αριθμού διαφορετικών οργανισμών. Όλοι όμως συμφωνούν ότι η κατάσταση αυτή θα αλλάξει στο κοντινό μέλλον.

Εκτός Ευρώπης η κατάσταση παρουσιάζει διαφοροποίηση σύμφωνα με μελέτη (Yoo 2017:312). Σύμφωνα με τα ευρήματα της, πολλές start-up εταιρίες αναπτύσσουν εφαρμογές βασισμένες στη τεχνολογία blockchain με στόχο την πραγματοποίηση πληρωμών. Η εταιρία TenX, με έδρα στη Σιγκαπούρη προετοιμάζει ένα σύστημα σε συνεργασία με τη MasterCard άλλα και τη Visa για την αγορά συναλλάγματος. Τέλος, αναφορά γίνεται και στις χρηματιστηριακές αγορές όπου ο Nasdaq OMX σχεδιάζει την υιοθέτηση της τεχνολογίας.

Παρόμοια εικόνα παρουσιάζει και η υλοποίηση της τεχνολογίας των έξυπνων συμβολαίων. Συμπερασματικά μπορούμε να αναφέρουμε ότι η επιστημονική κοινότητα στη πλειοψηφία της συμφωνεί για τα πλεονεκτήματα της τεχνολογίας αλλά αρκετοί παράγοντες συνδράμουν ώστε ο τραπεζικό τομέας να την αντιμετωπίζει με σκεπτικισμό. Μεταξύ αυτών το γεγονός ότι είναι μια νέα τεχνολογία, ειδικά τα έξυπνα συμβόλαια είναι νεότερη πράγμα που σημαίνει ότι ακόμα αποτελεί αντικείμενο μελέτης. Σημαντικό επίσης είναι και το γεγονός της έλλειψης του απαιτούμενου νομικού πλαισίου που θα καθορίζει τις διάφορες λειτουργίες. Τέλος, δεν λείπουν και οι φωνές της αμφισβήτησης τροφοδοτούμενες κυρίως από τον υπαρκτό κίνδυνο εξαπάτησης.

Κεφάλαιο 8
Υλοποίηση Τεχνολογίας

Στο κεφάλαιο αυτό θα παρουσιάσουμε τη διαδικασία υλοποίησης ενός έξυπνου συμβολαίου στο περιβάλλον της λιανικής τραπεζικής. Πιο συγκεκριμένα θα δείξουμε τα βήματα που απαιτούνται για την δημιουργία του περιβάλλοντος τεχνολογίας αλυσίδας καθώς και της ανάπτυξης, της εγκατάστασης αλλά και της χρήσης ενός έξυπνου συμβολαίου που θα υλοποιεί την υπηρεσία 'Λεφτά στο Λεπτό' της Τράπεζας Πειραιώς.

8.1 Υπηρεσία Λεφτά Στο Λεπτό

Η υπηρεσία αυτή παρέχεται από την Τράπεζα Πειραιώς. Πρόκειται για μια υπηρεσία που αποσκοπεί στην απλούστευση της διαδικασίας μεταφοράς χρημάτων μεταξύ ατόμων, μέσω του δικτύου των συστημάτων Αυτόματων Συναλλαγών της τράπεζας.

Η υπηρεσία επιτρέπει τη μεταφορά ποσού έως 600 ευρώ την ημέρα η 3.000 ευρώ το μήνα. Είναι διαθέσιμη στους πελάτες της τράπεζας, στα άτομα δηλαδή που διαθέτουν λογαριασμό στη τράπεζα. Ο πελάτης της τράπεζας είτε μέσω του ATM της τράπεζας, είτε μέσω διαδικτύου από το κινητό του η από τον υπολογιστή του, είτε ακόμα και τηλεφωνικά, ορίζει το ποσό που επιθυμεί να στείλει, τον λογαριασμό από τον οποίο θα χρεωθεί το ποσό, τη χρονική διάρκεια της εντολής και τέλος πώς θα λάβει τον κωδικό παραλαβής των μετρητών. Ο κωδικός αυτός μπορεί είτε να εκτυπωθεί στην απόδειξη στη περίπτωση που η διαδικασία πραγματοποιηθεί σε ATM είτε να σταλεί με SMS σε κινητό τηλέφωνο. Ακολούθως ο οποιοσδήποτε γνωρίζει τον κωδικό αυτό και το ακριβές ποσό των χρημάτων μπορεί να επισκεφθεί ένα ATM της τράπεζας και να εισπράξει το

ποσόν μέσα στο προκαθορισμένο χρονικό διάστημα που δόθηκε από τον εντολέα. Για την είσπραξη αυτή δεν απαιτείτε κάποια κάρτα και άρα το άτομο που θα εισπράξει δεν απαιτείτε να είναι πελάτης της τράπεζας. Με τον τρόπο αυτό ο εντολέας ενημερώνει το άτομο που θέλει να του στείλει τα χρήματα για το κωδικό, το ποσό αλλά και το χρονικό διάστημα που μπορεί να τα εισπράξει και η όλη διαδικασία ολοκληρώνετε με την ανάληψη του ποσού από το ATM. Είναι προφανές ότι η υπηρεσία μπορεί να χρησιμοποιηθεί και από κάποιον που έχασε τη κάρτα του ή το πορτοφόλι του για να λάβει χρήματα χωρίς την κάρτα ανάληψης. Ο κωδικός μπορεί να χρησιμοποιηθεί μόνο μια φορά και εντός του χρονικού ορίου. Εάν το χρονικό όριο παρέλθει ο κωδικός δεν ισχύει πλέον και τα χρήματα παραμένουν στον λογαριασμό. Τέλος, η συναλλαγή δεν μπορεί να ολοκληρωθεί εάν δεν υπάρχει το απαιτούμενο υπόλοιπο.

8.2 Περιβάλλον υλοποίησης

Για την ανάπτυξη της εφαρμογής επιλέχτηκε η πλατφόρμα του Hyperledger. Αρκετοί ήταν οι λόγοι που οδήγησαν στην επιλογή αυτή με βασικότερους, όπως προαναφέρθηκε, ότι αποτελεί μια λύση ανοιχτού κώδικα και άρα είναι δωρεάν, στην ανάπτυξή της οποίας λαμβάνουν μέρος ηχηρά ονόματα όπως αυτά της IBM, της Intel και όλα γίνονται υπό την αιγίδα του Linux Foundation. Τέλος, από τις διαθέσιμες επιλογές του Hyprledger επιλέχτηκε αυτή του Fabric καθώς αυτή αποτελεί την πλέον αρμόζουσα πλατφόρμα για το έξυπνο συμβόλαιο λιανικής τραπεζικής που θα υλοποιήσουμε.

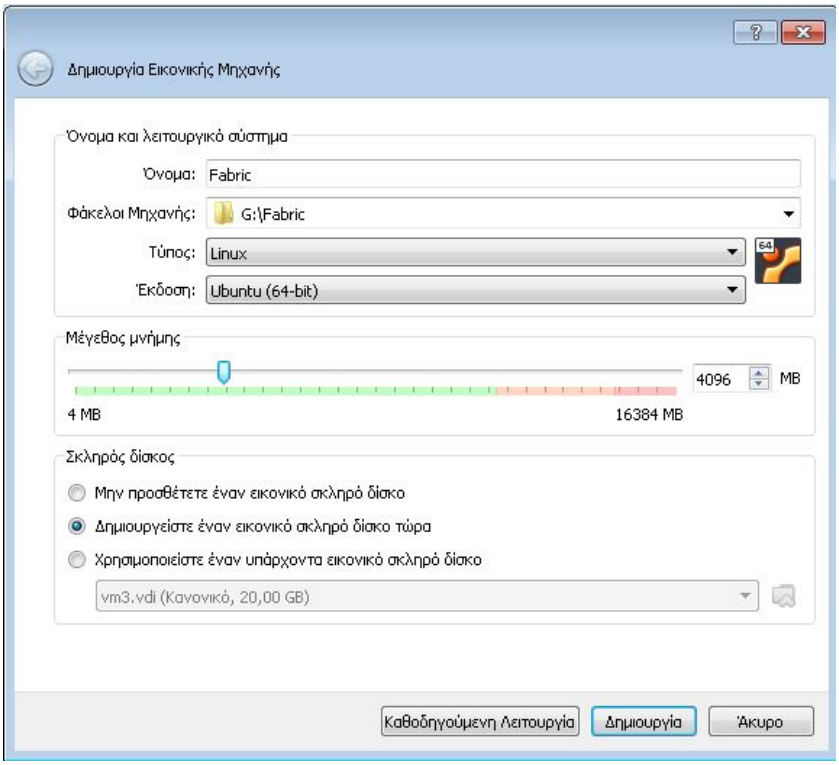
Ακολουθώντας την επίσημη βιβλιογραφία, από τις διαθέσιμες επιλογές εγκατάστασης επιλέγουμε αυτή του λειτουργικού συστήματος Ubuntu έκδοσης 16.04 μιας και δεν απαιτείτε άδεια, σε αντίθεση με τα Windows και επιπλέον και τα δύο (Hyperledger και Ubuntu) ανήκουν στη ομάδα του Linux. Τον υπολογιστή που θα φιλοξενήσει την όλη υποδομή θα τον αποτελεί ένα Εικονικό Μηχάνημα (Virtual Machine) της εταιρίας Oracle. Ομοίως η εφαρμογή της εταιρίας παρέχετε δωρεάν προσφέροντας κάποιες περιορισμένες λειτουργίες που δεν επηρεάζουν την υλοποίηση μας.

8.2.1 Δημιουργία Υποδομής

Το πρώτο βήμα για την δημιουργία της απαιτούμενης υποδομής είναι η εγκατάσταση της εφαρμογής Oracle VIrual Box έκδοσης 6 το οποία διατίθεται δωρεάν από τον ιστότοπο: https://www.virtualbox.org/wiki/Downloads. Μετά την λήψη του λογισμικού ακολουθεί η

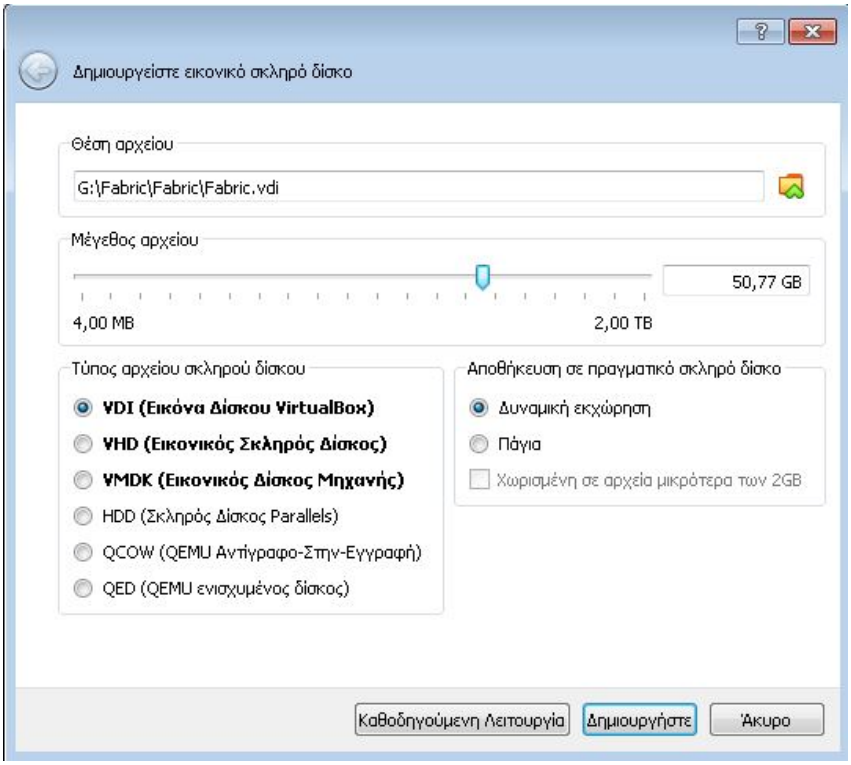
εγκατάσταση του η οποία δεν παρουσιάζει κάποια δυσκολία και ολοκληρώνεται ακολουθώντας τις προεπιλεγμένες τιμές. Επόμενο βήμα η λήψη του λειτουργικού συστήματος Ubuntu το οποίο είναι διαθέσιμο από τον ιστότοπο: http://releases.ubuntu.com/16.04/ από τον οποίο θα επιλέξουμε την έκδοση 64-bit server install image. Παράλληλα με τη λήψη του λειτουργικού μπορούμε να δημιουργήσουμε και τον φιλοξενητή στον οποίο θα εκτελείτε η μηχανή.

Εκκινούμε την εφαρμογή Virtual Box της Oracle και επιλέγουμε από το μενού Νέα εικονική μηχανή.



Εικόνα 16:Δημιουργία της εικονικής μηχανής

Στο παράθυρο διαλόγου αυτό ορίζουμε το όνομα της εικονικής μηχανής, τη θέση όπου θα αποθηκευτεί καθώς την ποσότητα της μνήμης που θα της ανατεθεί και τέλος επιλέγουμε Δημιουργία. Η διαδικασία ολοκληρώνεται με τον ορισμό του μεγέθους του σκληρού δίσκου. Προτείνεται το μέγεθος να είναι τουλάχιστον 50Gb.



Εικόνα 17:Παραμετροποίηση σκληρού δίσκου

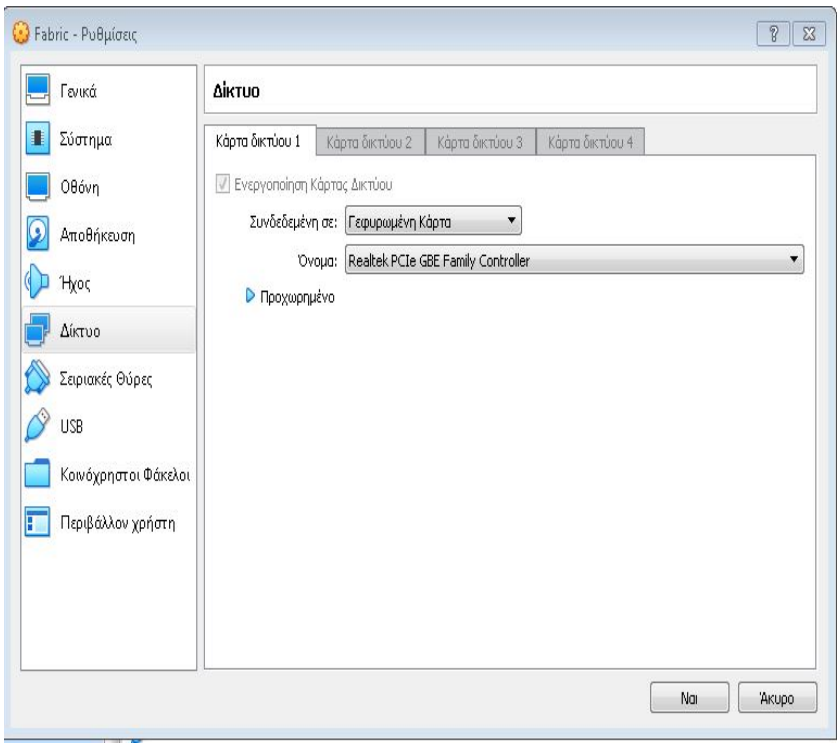
Η μηχανή πλέον είναι έτοιμη να ξεκινήσει. Κατά την εκκίνηση θα πρέπει να οριστεί το μέσο από το οποίο θα φορτώσει το λειτουργικό σύστημα Ubuntu 16 Server.

8.2.2 Εγκατάσταση Λειτουργικού Συστήματος

Η εγκατάσταση του λειτουργικού δεν απαιτεί κάποια ιδιαίτερη παραμετροποίηση και οι προκαθορισμένες επιλογές είναι αρκετές. Μοναδικό σημείο προσοχής συναντάται κατά την εγκατάσταση εφαρμογών όπου η εγκατάσταση του SSH Server κρίνεται αναγκαία μιας και μέσω αυτού θα επικοινωνούμε με τη μηχανή.

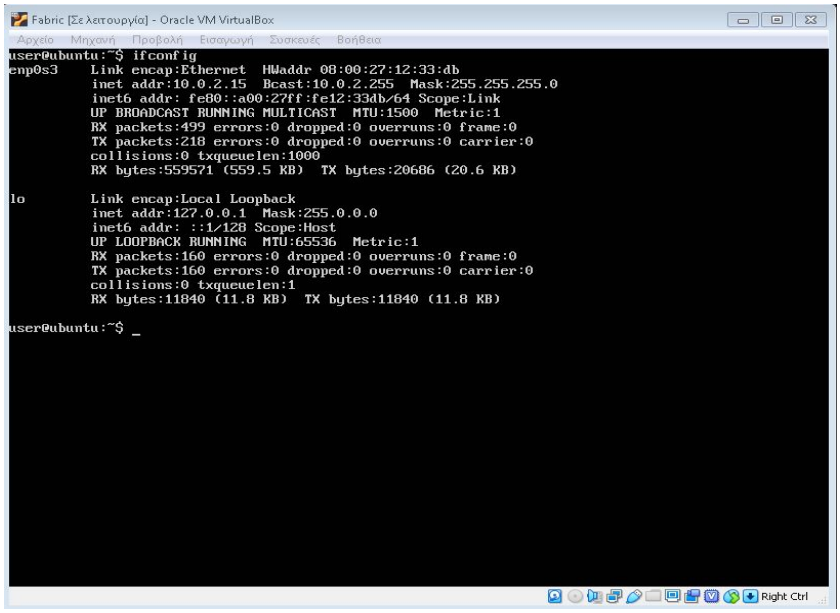
8.2.3 Σύνδεση με την Εικονική Μηχανή

Μετά την ολοκλήρωση της εγκατάστασης και την εκκίνηση της μηχανής θα πρέπει να παραμετροποιηθεί το δίκτυο ώστε να μπορεί η μηχανή να επικοινωνήσει με τον εξωτερικό κόσμο. Προτείνεται η κάρτα δικτύου να οριστεί σε κατάσταση 'Γεφυρωμένη κάρτα' ώστε η μηχανή να πάρει διεύθυνση από τον ίδιο DHCP Server που παίρνουν και οι υπόλοιποι υπολογιστές του δικτύου. Η επιλογή αυτή ορίζετε επιλέγοντας την εικονική μηχανή, ακολούθως επιλέγουμε τις ρυθμίσεις της και στη συνέχεια Δίκτυο.



Εικόνα 18:Παραμετροποίηση κάρτας δικτύου

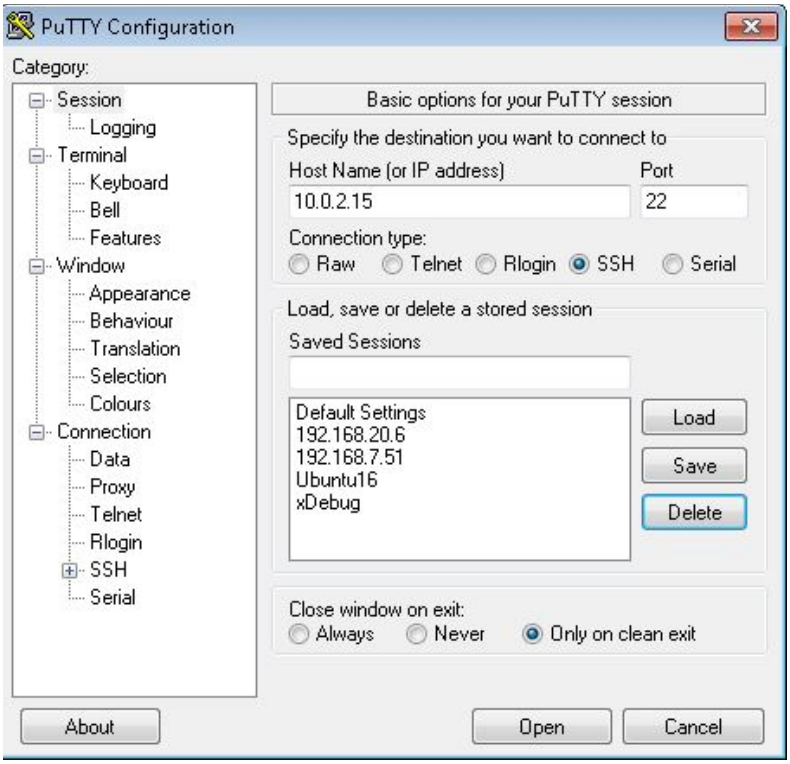
Επόμενο βήμα είναι η εξακρίβωση της IP διεύθυνσης της εικονικής μηχανής. Επιτυγχάνετε μετά την επιτυχή σύνδεση στη μηχανή, χρησιμοποιώντας τους κωδικούς που δοθήκαν κατά την εγκατάσταση και την πληκτρολόγηση της εντολής ifconfig.



Εικόνα 19: Το αποτέλεσμα της εντολής ifconfig

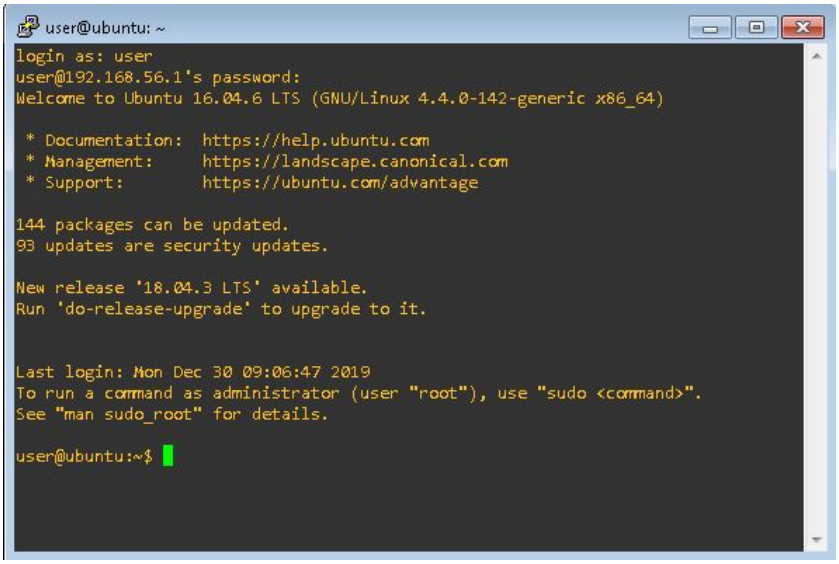
Στην οθόνη αναζητούμε τη τιμή inet addr: της κάρτας δικτύου που στο παράδειγμα μας ονομάζετε enp0s3 και η διεύθυνση της είναι η 10.0.2.15.

Προκειμένου να συνδεθούμε μέσω SSH με τη μηχανή θα κατεβάσουμε στον υπολογιστή μας την εφαρμογή putty από την διεύθυνση : https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html . Από τον ιστότοπο αυτό θα επιλέξουμε την έκδοση που είναι συμβατή με τον υπολογιστή μας και αφού ολοκληρωθεί η λήψη θα εκτελέσουμε την εφαρμογή.



Εικόνα 20: Παραμετροποίηση του SSH Client

Στο πεδίο Host Name πληκτρολογούμε τη διεύθυνση που πήραμε από το προηγούμενο βήμα, το πρωτόκολλο SSH και πατάμε Open. Απαντάμε καταφατικά σε ερώτηση για το αν εμπιστευόμαστε το πιστοποιητικό και ακολούθως πληκτρολογούμε τα διαπιστευτήρια μας για να εισέλθουμε στο σύστημα. Η διαδικασία έχει ολοκληρωθεί επιτυχώς.



Εικόνα 21: Επιτυχής SSH σύνδεση

8.2.4 Εγκατάσταση Προαπαιτούμενων Πακέτων

Προτού ξεκινήσουμε τη δημιουργία του δικτύου Blokchain θα πρέπει να διαμορφώσουμε κατάλληλα τον υπολογιστή εγκαθιστώντας τα απαραίτητα πακέτα. Στη περίπτωση που η εγκατάσταση κάποιου πακέτου δεν ξεκινά λόγω του ότι ο χρήστης δεν έχει τα απαραίτητα δικαιώματα θα πρέπει πριν την πληκτρολόγηση την εντολής να δοθεί η οδηγία sudo η οποία αλλάζει το επίπεδο διαπίστευσης. Ακολούθως, ο χρήστης θα πληκτρολογήσει τους κωδικούς του και κατόπιν η εντολή θα εκτελεστεί. Θα ξεκινήσουμε με την εγκατάσταση του Git το οποίο εγκαθιστάτε πληκτρολογώντας την εντολή apt-get install git ενώ εάν πρέπει να δοθεί η οδηγία sudo η εντολή γίνεται sudo apt-get install git. Ακολουθεί η εγκατάσταση του εργαλείου Curl πληκτρολογώντας sudo apt-get install curl. Επόμενο βήμα η εγκατάσταση του Docker.

Το Docker είναι απαραίτητο μιας και το δίκτυο του Blokchain θα εκτελείτε μέσα σε εικονικά περιβάλλοντα τύπου Docker. Για την εγκατάσταση του πληκτρολογούμε τις εντολές:

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

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

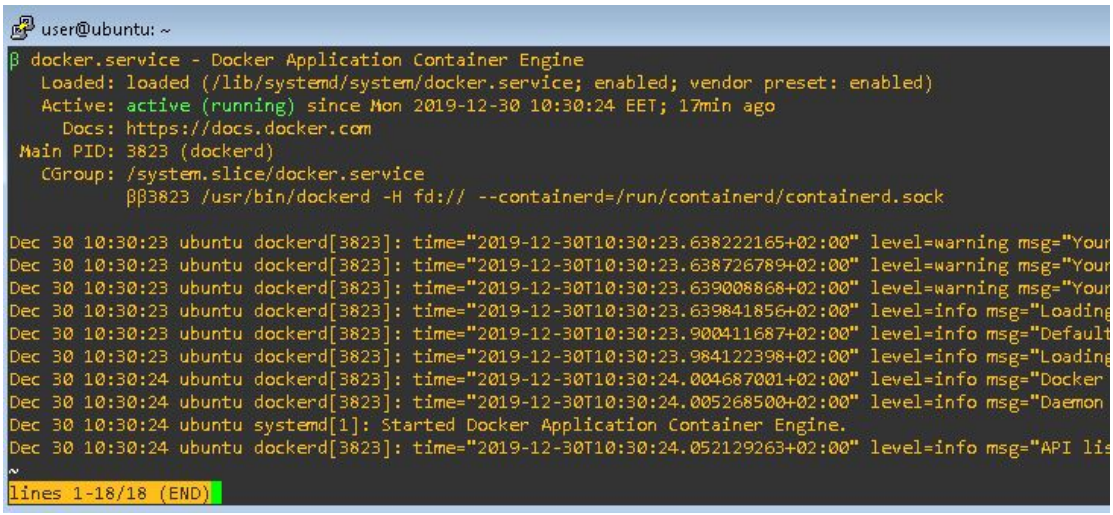
3. sudo apt-get update

4. `sudo apt-get install -y docker-ce`

Για να βεβαιωθούμε ότι η εγκατάσταση ολοκληρώθηκε επιτυχώς πληκτρολογούμε

`sudo systemctl status docker`

Το σύστημα θα πρέπει να μας απαντήσει ότι η υπηρεσία εκτελείται. Για το τερματισμό της προβολής πληκτρολογούμε Ctrl + C . Τέλος, ο χρήστης θα πρέπει να προστεθεί στη λίστα με τους έμπιστους χρήστες Docker πληκτρολογώντας την εντολή sudo usermod -a -G docker ακολουθούμενη από το όνομα του χρήστη. Ακολούθως, ο χρήστης θα πρέπει να αποσυνδεθεί και να συνδεθεί εκ νέου.



Εικόνα 22: Η κατάσταση της υπηρεσίας Docker

Η εγκατάσταση ολοκληρώνετε με το Docker compose με τη χρήση της εντολής `sudo apt install docker-compose`

Η παραμετροποίηση του περιβάλλοντος συνεχίζεται με την εγκατάσταση της γλώσσας προγραμματισμού GO έκδοση 1.13.

wget https://dl.google.com/go/go1.13.3.linux-amd64.tar.gz

sudo tar -xvf go1.13.3.linux-amd64.tar.gz

sudo mv go /usr/local

export GOPATH=/usr/local/go

export PATH=$PATH:$GOPATH/bin

Ακολούθως εισάγουμε Node.js και NPM:

curl -sL https://deb.nodesource.com/setup_8.x | sudo -E bash -

sudo apt-get install -y nodejs

sudo npm install npm@5.6.0 –g

8.2.5 Εγκατάσταση και Χρήση του Hypelredger Fabric

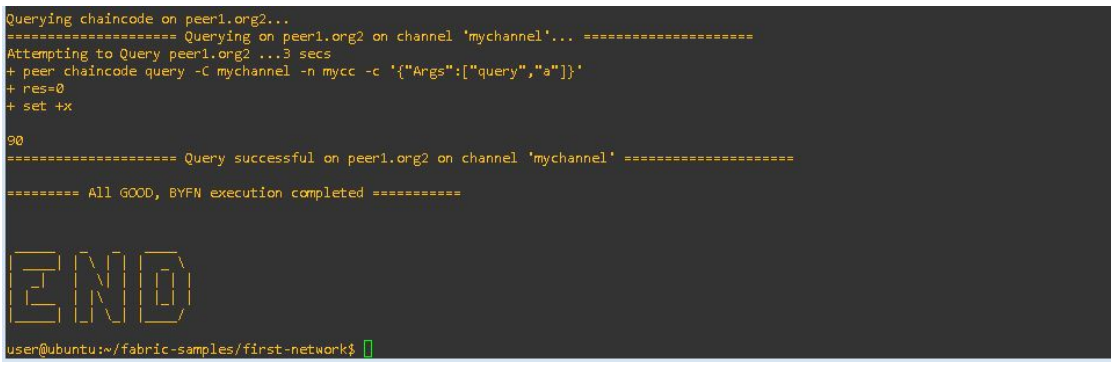
Η εγκατάσταση του δικτύου γίνεται μέσω ενός script αρχείου το οποίο λαμβάνεται και εκτελείται με την εντολή curl -sSL https://bit.ly/2ysbOFE | bash -s

Η εντολή απαιτεί ορισμένο χρόνο για να ολοκληρωθεί μιας και θα πρέπει να κατεβάσει τα αρχεία εικόνας που απαιτούνται. Ακολούθως, θα πρέπει να προστεθεί στη μεταβλητή PATH η διαδρομή του φακέλου bin ο οποίος βρίσκεται στο φάκελο εγκατάστασης.

export PATH=/home/user/fabric-samples/bin:$PATH

Για την έναρξη του δικτύου ο χρήστης θα πρέπει να μπει στο φάκελο που περιέχει τα απαραίτητα αρχεία με την εντολή cd fabric-samples/first-network, ακολούθως να προετοιμάσει το δίκτυο με την εντολή ./byfn.sh generate και τέλος να το ξεκινήσει με την εντολή ./byfn.sh up

Εφόσον όλα εγκατασταθούν σωστά, το σύστημα μας ενημερώνει για το επιτυχημένο αποτέλεσμα. Κατόπιν, ο χρήσης θα πρέπει να εισάγει ./byfn.sh down προκειμένου το δίκτυο να ‘κατέβει’.



Εικόνα 23: Επιτυχημένη εγκατάσταση του δικτύου

8.3 Υλοποίηση του Έξυπνου Συμβολαίου

Για την σύνταξη του έξυπνου συμβολαίου έχουμε να επιλέξουμε τις γλώσσες προγραμματισμού JavaScript, Java, Go και TypeScript. Θα επιλέξουμε την JavaScript μιας και είναι μια υψηλού επιπέδου, δυναμική γλώσσα προγραμματισμού και μία από τις πιο διαδεδομένες. Η εφαρμογή μας αποτελείται από δύο αρχεία, ένα που αποτελεί τον πυρήνα της εφαρμογής και ένα που αποτελεί την πύλη εισόδου στην εφαρμογή μας.

Το αρχείο του πυρήνα αποθηκεύεται στη διαδρομή /home/user/fabric-samples/chaincode/moneyatonce/javascript/lib και ουσιαστικά περιέχει την κλάση του έξυπνου συμβολαίου. Κατά την έναρξη του δικτύου το αρχείο αυτό μοιράζεται στους κόμβους του δικτύου σύμφωνα με την πολιτική που έχει οριστεί στο αρχείο που αρχικοποιεί το δίκτυο και είναι το configtx.yaml.

Ο κώδικας του έξυπνου συμβολαίου ξεκινά με την εισαγωγή του αντικειμένου Contract. Το αντικείμενο αυτό παρέχει τις συναρτήσεις που θα χρησιμοποιήσουμε και αναλαμβάνει να διεκπεραιώσει τις απαιτούμενες διαδικασίες προκειμένου να ολοκληρωθεί η συναλλαγή.

```
const { Contract } = require('fabric-contract-api');
```

Ακολούθως, ορίζουμε το δικό μας αντικείμενο το οποίο κληρονομεί από το Contract και ονομάζουμε moneyAtOnce:

```
class MoneyAtOnce extends Contract {
```

Η πρώτη συνάρτηση του αντικειμένου είναι η initLedger η οποία θα αρχικοποιήσει το αντικείμενο καθώς παίζει το ρόλο του constructor. Σαν όρισμα δέχεται ένα αντικείμενο τύπου Transaction

Contex το οποίο μας βοηθά να μεταφέρουμε δεδομένα μεταξύ των κλάσεων και μας δίνει πρόσβαση στο API του Fabric. Αργότερα θα δούμε τις συναρτήσεις που θα χρησιμοποιήσουμε.

```
async initLedger(ctx) {

        const counter = 0;

    console.info('============= START : Initialize Ledger ===========');

}
```

Η κλάση μας περιέχει ένα μετρητή για να γνωρίζουμε πόσα αντικείμενα έχουμε δημιουργήσει πράγμα που θα μας βοηθήσει στην αναζήτηση και στο να είναι όλα τα αντικείμενα διαφορετικά. Επίσης, εκτυπώνει στην οθόνη ένα διαγνωστικό μήνυμα για να γνωρίζουμε ότι το αντικείμενο δημιουργήθηκε.

Κατόπιν, δημιουργούμε τις υπόλοιπες συναρτήσεις που θα χρειαστούμε. Θα ξεκινήσουμε από τη συνάρτηση που δημιουργεί νέους λογαριασμούς. Η συνάρτηση δέχεται τον αριθμό λογαριασμού και το διαθέσιμο ποσό:

```
async createAccount(ctx, accountNum, balance) {

    console.info('============= START : Create Account ===========');



      const client = {

        accountNum,

      docType: 'client',

      balance,

    };
```

```
    await ctx.stub.putState(accountNum, Buffer.from(JSON.stringify(client)));

                console.info('============= END : Create Client ===========');

  }
```

Την όλη διαδικασία αναλαμβάνει η συνάρτηση putState του αντικειμένου Transaction Context που ονομάζετε ctx. Η συνάρτηση αυτή ενημερώνει όλους τους αρμόδιους κόμβους να αποθηκεύσουν την πληροφορία.

Η μορφή που θα αποθηκευτεί η πληροφορία είναι για παράδειγμα :

```
{"Key":"accountNum", "Record":{"balance":1254.66,}}
```

Ακολούθως η συνάρτηση που θα ξεκινήσει την μεταφορά:

```
async createPay(ctx, accountNum, amount, etime) {

    console.info('============= START : Create Pay ===========');



                const iterator = await ctx.stub.getState(accountNum);

                var data = JSON.parse(iterator);

                const results = [];



                            if ((data.balance-amount)>0){



                                const client = {

                                accountNum,
```

```
                docType: 'clientData',
                amount,
                pin = this.counter++,
                etime,
            };

            await ctx.stub.putState(pin, Buffer.from(JSON.stringify(client)));
            results.push({ 'Status', 'Ok' });
            return JSON.stringify(results);
            }
            else {
                results.push({ 'Status', 'Not enough money.' });
                return JSON.stringify(results);
            }
        }
    }
```

Η συνάρτηση δέχεται ως όρισμα τον αριθμό λογαριασμού του δικαιούχου, το πόσο που θέλει να μεταφέρει και τέλος σε πόσο χρόνο θα λήξει η συναλλαγή. Μέσω της getState ζητάει από τους κόμβους τα δεδομένα του συγκεκριμένου λογαριασμού. Ακολούθως παίρνουμε τα δεδομένα και αφού ελέγξουμε ότι το διαθέσιμο υπόλοιπο είναι αρκετό και ότι δεν έχει παρέλθει το

προκαθορισμένο χρονικό διάστημα ολοκληρώνουμε τη συναλλαγή τέλος, ενημερώνουμε το υπόλοιπο του πελάτη.

Βλέπουμε λοιπόν ότι με ελάχιστες γραμμές κώδικα μπορούμε να υλοποιήσουμε ένα υποτυπώδες έξυπνο συμβόλαιο. Αυτό είναι το βασικό χαρακτηριστικό της πλατφόρμα Hyperledger Fabric όπου μας παρέχει τα αντικείμενα που θα χρησιμοποιήσουμε απλοποιώντας έτσι τις διαδικασίες, αφού ο προγραμματιστής εστιάζει στις διαδικασίες που τον αφορούν χωρίς να απασχολείτε με το τι γίνεται μέσα στη πλατφόρμα, όπως για παράδειγμα τι πρέπει να γίνει προκειμένου να επιτευχθεί η συμφωνία μεταξύ των κόμβων.

Για να είναι προσβάσιμο το έξυπνο συμβόλαιο και ειδικότερα το αντικείμενο αυτό, έχουμε δημιουργήσει άλλα τρία προγράμματα. Το πρώτο δημιουργεί τον λογαριασμό, το δεύτερο δημιουργεί την διαταγή πληρωμής και το τρίτο την εκτελεί.

Το αρχείο που αναλαμβάνει την δημιουργία του λογαριασμού είναι το create.js και είναι αποθηκευμένο στη διαδρομή /home/user/fabric-samples/moneyatonce/javascript :

```
'use strict';



const { FileSystemWallet, Gateway } = require('fabric-network');

const path = require('path');



const ccpPath = path.resolve(__dirname, '..', '..', 'first-network', 'connection-org1.json');



async function main() {

  try {
```

```
    // Create a new file system based wallet for managing identities.
    const walletPath = path.join(process.cwd(), 'wallet');
    const wallet = new FileSystemWallet(walletPath);
    console.log(`Wallet path: ${walletPath}`);

    // Check to see if we've already enrolled the user.
    const userExists = await wallet.exists('user1');
    if (!userExists) {
        console.log('An identity for the user "user1" does not exist in the wallet');
        console.log('Run the registerUser.js application before retrying');
        return;
    }

    // Create a new gateway for connecting to our peer node.
    const gateway = new Gateway();
    await gateway.connect(ccpPath, { wallet, identity: 'user1', discovery: { enabled: true, asLocalhost: true } });

    // Get the network (channel) our contract is deployed to.
```

```
        const network = await gateway.getNetwork('mychannel');


        // Get the contract from the network.
        const contract = network.getContract('moneyatonce');


        // Create the account.
        // createClient transaction - requires 2 argument, ex: ('createAccount', 123456789, 1254.56);


        await contract.submitTransaction(' createAccount ', 123456789, 1254.56);
        console.log('Client created Successfully');


        // Disconnect from the gateway.
        await gateway.disconnect();


    } catch (error) {
        console.error(`Failed to submit transaction: ${error}`);
        process.exit(1);
    }
}
```

main();

Το πρόγραμμα, αφού εισάγει το αντικείμενο FileSystemWallet που χρησιμοποιείται για την αποθήκευση των χρηστών και το αντικείμενο Gateway που αποτελεί την πύλη εισόδου στο δίκτυο, ελέγχει εάν ο χρήστης έχει τα απαραίτητα δικαιώματα για να ενεργοποιήσει το έξυπνο συμβόλαιο. Ο χρήστης αυτός δημιουργείται από τον διαχειριστή του συστήματος. Ακολούθως, η εφαρμογή συνδέεται στο δίκτυο mychannel και αποκτά πρόσβαση στο συμβόλαιο moneyatonce. Στη συνέχεια, καλεί την συνάρτηση createClient του συμβολαίου παρέχοντας της τις απαραίτητες παραμέτρους.

Η συνάρτηση createClient δίδεται ως παράμετρος στη συνάρτηση submitTransaction του αντικειμένου contract. Η συνάρτηση αυτή θα στείλει την πληροφορία σε όλους του κόμβους του δικτύου που έχουν οριστεί από την πολιτική να χειρίζονται την πληροφορία αυτή. Κάθε κόμβος θα εκτελέσει το συμβόλαιο και θα επιστρέψει το αποτέλεσμα στο διαχειριστή του. Εκείνος από την πλευρά του τα συγκεντρώνει και αφού βεβαιωθεί ότι συμφωνούν τότε μόνο τα επαναπροωθεί στους κόμβους για μόνιμη αποθήκευση. Τέλος, ενημερώνει την εφαρμογή για το αποτέλεσμα αυτό. Στη περίπτωση που η απόκριση ενός μόνο κόμβου είναι αρκετή θα έπρεπε να κληθεί η evaluateTransaction.

Στη συνέχεια, η εφαρμογή εκτυπώνει τα μηνύματα της επιτυχούς αποθήκευσης στην οθόνη, αποσυνδέεται από το δίκτυο και ολοκληρώνει της λειτουργία της. Αντίστοιχα, τα άλλα δύο αρχεία καλούν τις createPay και commitPay ολοκληρώνοντας έτσι τη διαδικασία.

8.4 Εκτέλεση του Κώδικα

Για να λειτουργήσει το δίκτυο αλυσίδας και να εγκατασταθεί το συμβόλαιο σε αυτό, η πλατφόρμα μας παρέχει προγράμματα που εκτελούν τις εντολές που θα πρέπει να εκτελεστούν. Μάλιστα η πλατφόρμα παρέχει τέτοια προγράμματα για διάφορες χρήσεις όπως για την δημιουργία δοκιμαστικών δικτύων καθώς και δοκιμαστικών έξυπνων συμβολαίων και όλα αυτά σε διάφορες γλώσσες προγραμματισμού όπως Java, JavaScript,Go και Typescript. Τα προγράμματα αυτά χρησιμοποιήσαμε και εμείς για τις δοκιμές μας.

Για να εκτελεστεί το συμβόλαιο θα πρέπει αρχικά να ‘σηκωθεί’ το δίκτυο. Αυτό επιτυγχάνετε εκτελώντας την εφαρμογή ./startFabric.sh javascript από το φάκελο που περιέχει τα αρχεία μας. Αυτό δέχεται σαν όρισμα την γλώσσα που θα χρησιμοποιηθεί και ακολούθως ‘σηκώνει’ το δίκτυο αποτελούμενο από δύο οργανισμούς που ονομάζονται org1 και org2 κάθε ένας από τους όποιους αποτελείται από δύο κόμβους peer0 και peer1. Ακολούθως εισάγει τα απαραίτητα διαπιστευτήρια στους κόμβους αλλά και το συμβόλαιο που δημιουργήσαμε στους κόμβους peer0 του org1 και peer0 του org2. Στη συνέχεια, ο χρήστης θα εισάγει τα απαραίτητα πακέτα μέσω της npm με την εντολή npm install. Αυτή θα κατεβάσει τα υπόλοιπα απαιτούμενα προγράμματα.

Στη συνέχει ο χρήστης θα εκτελέσει το enrollAdmin.js μέσω του node το οποίο θα ενεργοποιήσει το χρήστη admin στο δίκτυο. Ο χρήστης αυτός είναι απαραίτητος για τη δημιουργία των υπολοίπων χρηστών του δικτύου. Τέλος, θα πρέπει να δημιουργηθεί ο χρήστης που θα εισάγει το συμβόλαιο και αυτό ολοκληρώνεται με το πρόγραμμα regirsterUser.js. Το δίκτυο είναι έτοιμο να εκτελέσει τις συναρτήσεις του συμβολαίου καλώντας μέσω του node τα αρχεία create.js, createPay.js και commitPay.js. Τα προγράμματα εκτελούν τις συναρτήσεις του συμβολαίου και εκτυπώνουν στην οθόνη τα αποτελέσματα.

Κεφάλαιο 9
Επίλογος

Στη παρούσα μεταπτυχιακή διατριβή μελετήθηκε η εφαρμογή των έξυπνων συμβολαίων στις τραπεζικές συναλλαγές προτεινόμενες εφαρμογές αλλά κυρίως η τρέχουσα κατάσταση και οι προβλέψεις σχετικά με τη τεχνολογία blockchain και τα έξυπνα συμβόλαια σε σχέση με το τραπεζικό σύστημα. Επίσης, παρουσιάστηκαν σχετικές ερευνητικές μελέτες

Παρουσιάστηκε λεπτομερώς η τεχνολογία της αλυσίδας συστοιχιών και τα διάφορα είδη της, η οποία αποτελεί το περιβάλλον μέσα στο οποίο δημιουργούνται και λειτουργούν τα έξυπνα συμβόλαια . Ακολούθως, μελετήθηκαν οι τεχνολογίες που κατέστησαν δυνατή την υλοποίηση των υπηρεσιών αυτών όπως τα δίκτυα διασύνδεσης των ηλεκτρονικών υπολογιστών, οι συναρτήσεις κατακερματισμού, οι μέθοδοι κρυπτογράφησης της πληροφορίας, οι ψηφιακές υπογραφές καθώς και τα πρωτόκολλα συναίνεσης.

Παρουσιάστηκαν τα έξυπνα συμβόλαια, ο τρόπος λειτουργίας τους, η σχέση τους με την αλυσίδα συστοιχιών και τα βασικά χαρακτηριστικά τους. Τα σημαντικά πλεονεκτήματα που παρουσιάζουν σε σχέση με τα παραδοσιακά όπως η εξοικονόμηση χρόνου, το μειωμένο κόστος, η έλλειψη μεσαζόντων, η άμεση επιβολή ποινών σε περίπτωση αθέτησής τους, η αυξημένη ασφάλεια που παρέχουν μέσω της κρυπτογράφησης και της απουσίας μίας κεντρικής βάσης δεδομένων και τέλος η προστασία του περιβάλλοντος με την αποφυγή χρήσης χαρτιού. Αναφέρθηκαν οι τομείς στους οποίους μπορούν να εφαρμοστούν όπως ο οικονομικός, η κατοχύρωση πνευματικών δικαιωμάτων αλλά και ο κλάδος της εφοδιαστικής αλυσίδας. Οι προκλήσεις που οι προγραμματιστές και η κοινότητα του blockchain καλούνται να αντιμετωπίσουν όπως η επεκτασιμότητα, η ανάγκη πρόσβαση σε πραγματικά δεδομένα, η ιδιωτικότητα, η αποδοτικότητα, η εξασφάλιση και οι περιορισμοί στις εφαρμογές .

Στη συνέχεια, παρουσιάστηκε η θέση της τεχνολογίας αλυσίδας στη παγκόσμια αγορά καθώς και τα διάφορα πεδία στα οποία βρίσκει εφαρμογή, όπως ο οικονομικός τομέας, η εκπαίδευση και η οργάνωση του κράτους.

Κατόπιν, έγινε εκτενής αναφορά στις πλατφόρμες Bitcoin, Ethereum, Hyperledger και R3 Cobra που υποστηρίζουν έξυπνα συμβόλαια μιας και αυτό είναι το αντικείμενο της παρούσας διατριβής. Αναφερθήκαμε στα ιδιαίτερα χαρακτηριστικά τους, στο τρόπο λειτουργίας τους, στο μερίδιο αγοράς που κατέχουν και στις τεχνολογίες που υποστηρίζουν.

Ακολούθως, παρουσιάστηκε μία εικόνα του τραπεζικού συστήματος. Αναφερθήκαμε στις οφέλη που μπορεί να επιφέρει η τεχνολογία blockchain σε συνδυασμό με τα έξυπνα συμβόλαια όπως η διαφάνεια, η έλλειψη μεσολαβητών, η αποθήκευση της πληροφορίας, η μείωση της χειρωνακτικής επεξεργασίας, η τεκμηρίωση και η μείωση του χρόνου των συναλλαγών.

Τέλος, δημιουργήθηκε ένα έξυπνο συμβόλαιο που υλοποιεί την υπηρεσία "Λεφτά στο Λεπτό" της Τράπεζας Πειραιώς. Για την πραγματοποίησή του αναπτύχθηκε ένα blockchain δίκτυο σε ένα virtual machine της Oracle με λειτουργικό Ubuntu, ενώ μετά από την ανάλυση των προαναφερόμενων πλατφορμών επιλέχτηκε η πλατφόρμα Hyperledger Fabric , ως η καταλληλότερη.

Στην εισαγωγή παρουσιάσαμε τα ερευνητικά μας ερωτήματα, παρέχουμε μια σύνοψη των απαντήσεων που δόθηκαν μέσω της ανάλυσης της παρούσας μεταπτυχιακής διατριβής:

- **RQ1 - Ποια είναι η τρέχουσα κατάσταση και οι προβλέψεις σχετικά με τη τεχνολογία blockchain και τα έξυπνα συμβόλαια σε σχέση με το τραπεζικό σύστημα;** Διερευνήσαμε την ιστορία του blockchain και το κύριο ζήτημα που προσπαθεί να λύσει. Παρουσιάσαμε τις τεχνολογίες που υποστηρίζουν το blockchain και τον τρόπο λειτουργίας του. Όσον αφορά τα έξυπνα συμβόλαια, παρείχαμε μια επισκόπηση των πλεονεκτημάτων, των προκλήσεων και των περιορισμών τους, συμπεριλαμβανομένης μιας ανάλυσης κόστους για την ανάπτυξη ενός έξυπνου συμβολαίου. Παρουσιάσαμε πληροφορίες από έρευνες αγοράς που επισημαίνουν ότι τα επόμενα χρόνια θα υπάρξει αύξηση στο διεθνές μερίδιο αγοράς καθώς και στο ρυθμό ανάπτυξης της τεχνολογίας. Επιπλέον, βασιζόμενοι στην τρέχουσα βιβλιογραφία καταγράψαμε ότι κεντρικές τράπεζες σε διάφορα έθνη, διεθνείς οργανισμοί, εθνικά χρηματιστήρια, τραπεζικοί τιτάνες αλλά και χρηματοοικονομικοί φορείς έχουν ανακοινώσει τα σχέδιά τους ή έχουν ξεκινήσει ερευνητικά εργαστήρια και πιλοτικά προγράμματα σχετικά με την τεχνολογία blockchain. Αυτό σημαίνει ότι η τεχνολογία Blockchain και τα έξυπνα συμβόλαια θα μπορούσαν δυνητικά να διεισδύσουν σε όλους τους τομείς του χρηματοπιστωτικού

κλάδου, αυτό όμως από μόνο του δεν αρκεί. Για να είναι αποτελεσματικές τέτοιες προσπάθειες πρέπει να συνδυάζονται με θεμελιώδεις αλλαγές των καθιερωμένων διαδικασιών και των επιχειρηματικών μοντέλων.

- **RQ2 – Είναι η πλατφόρμα Hyperledger fabric μια αρκετά ανταγωνιστική επιλογή με βασικά χαρακτηριστικά την απλότητα, την τεκμηρίωση και την μικρή απαίτηση σε πόρους;** Συμπερασματικά μπορούμε να πούμε ότι η πλατφόρμα προσφέρει μια αρκετά αξιόλογη επιλογή με βασικό χαρακτηριστικό την απλότητα. Δείξαμε ότι με ελάχιστες εντολές ο χρήστης έχει τη δυνατότητα να εγκαταστήσει εύκολα το δίκτυο και κατόπιν με λίγες γραμμές κώδικα να δημιουργήσει τα δικά του έξυπνα συμβόλαια. Ειδικότερα για τα έξυπνα συμβόλαια θα πρέπει να γνωρίζει τη χρήση ουσιαστικά των δύο συναρτήσεων που χρησιμοποιούνται για να τεθούν τα διάφορα ερωτήματα στο δίκτυο. Άξιο αναφοράς επίσης είναι και το γεγονός ότι η πλατφόρμα δεν είναι καθόλου απαιτητική σε πόρους και μπορεί να εγκατασταθεί σχεδόν οπουδήποτε ώστε ο χρήστης να εξοικειωθεί με την χρήση της.

Στην αντίπερα όχθη, στο τομέα των μειονεκτημάτων θα αναφερθούμε στη τεκμηρίωση. Η εταιρία έχει κάνει μια αξιόλογη προσπάθεια να καθοδηγήσει τους χρήστες προσφέροντας οδηγίες για την εγκατάσταση του δικτύου, την ενεργοποίηση καθώς και την εκτέλεση έξυπνου συμβολαίου. Η όλη τεκμηρίωση της πλατφόρμας είναι χαοτική και δεν διευκολύνει ιδιαίτερα το χρήστη. Ναι μεν η πλατφόρμα διαθέτει μεγάλο αριθμό λεπτομερειών που θα πρέπει να λάβει υπόψη του ο χρήστης κατά τη χρήση της άλλα από την άλλη εκτιμούμε ότι η όλη τεκμηρίωση έχει πολλά περιθώρια βελτίωσης. Για παράδειγμα θα αναφέρουμε ότι παρέχει οδηγίες για την εκτέλεση του συμβολαίου, αλλά δεν παρέχει οδηγίες για τα βήματα που θα πρέπει να κάνει ο χρήστης προκειμένου να δημιουργήσει και να εγκαταστήσει το δικό του. Και αυτός ήταν και ο λόγος που δεν καταφέραμε να δοκιμάσουμε το δικό μας συμβόλαιο μέσα στο περιβάλλον του δικτύου.

Δεν πρέπει να παραλείψουμε να αναφέρουμε ότι η μέτριας ποιότητας τεκμηρίωση δεν είναι χαρακτηριστικό μόνο του Hyperledger αλλά συνοδεύει την πλειονότητα των λογισμικών ανοιχτού κώδικα. Το γεγονός αυτό οφείλετε σε πολλούς παράγοντες ο βασικότερος των οποίων εκτιμούμε ότι είναι οι περιορισμένοι πόροι που διαθέτουν οι δημιουργοί τους. Τρίτες εταιρίες έρχονται να καλύψουν το κενό αυτό πλαισιώνοντας την εφαρμογή ανοιχτού κώδικα με τις δικές τους προσθήκες που διευκολύνουν το χρήστη παρέχοντας του παράλληλα μια βελτιωμένη τεκμηρίωση και όλα αυτά με ένα κόστος αγοράς. Παράδειγμά αυτού αποτελεί τη πρόταση της IBM (IBM 2019).

9.1 Συμπεράσματα

Παρακολουθώντας την εξέλιξη της συγκεκριμένης τεχνολογίας τα τελευταία χρόνια και μην παραβλέποντας το γεγονός ότι έχει αρχίσει να διεκδικεί σημαντικό μέρος της δημοσιότητας, είναι σίγουρο ότι θα μας απασχολήσει ακόμα περισσότερο στο εγγύς μέλλον.

Φυσικά, όπως καθετί πρωτοποριακό που απειλεί να αλλάξει παγιωμένες πρακτικές ετών έχει υποστηρικτές αλλά και πολέμιους. Πολλοί είναι αυτοί που πιστεύουν ότι πρόκειται να επιφέρει σημαντικές αλλαγές, όχι μόνο στις συναλλαγές των ανθρώπων αλλά γενικότερα στην κοινωνία, έντασης αντίστοιχης με αυτές που προκάλεσε η είσοδος του διαδικτύου στη ζωή των ανθρώπων. Φυσικά δεν απουσιάζουν και οι φωνές που παρουσιάζουν ένα σκεπτικισμό σχετικά με το εάν πρόκειται για κάποια ‘μόδα’ και κατά πόσο αναμένεται να την στηρίξουν και να την εμπιστευτούν τομείς ιδιαίτερα επιφυλακτικοί στις νέες τεχνολογίες όπως ο τραπεζικός τομέας.

Εκτιμούμε ότι τα επόμενα χρόνια η τεχνολογία της αλυσίδας και τα έξυπνα συμβόλαια θα ενσωματωθούν στην καθημερινότητα μας όπως ακριβώς και η τεχνολογία του διαδικτύου. Θα απαιτηθεί όμως αρκετή εργασία προκείμενου να ωριμάσουν ώστε να μην επαναληφθούν φαινόμενα απάτης, να διευθετηθούν τα ανοιχτά θέματα της νομοθεσίας αλλά και να υπάρξει η απαιτούμενη αποδοχή τόσο από τους τραπεζικούς κλάδους αλλά και από τους πολίτες γενικότερα.

Βιβλιογραφία

Κυπριακή Δημοκρατία, (2019) Αποκεντρωμένες Τεχνολογίες (Blockchain) Εθνική Στρατηγική για την Κύπρο. http://mof.gov.cy/assets/modules/wnp/articles/201907/480/docs/blockchain_ypoyrgoy.pdf [Πρόσβαση: 26.12.2019].

Allam, Z., (2018) On Smart Contracts and Organisational Performance: A Review of Smart Contracts through the Blockchain Technology. Review of Economic and Business Studies, *11*(2), 137–156.

Arjun, R., & Suprabha, K. R. (2020). Innovation and Challenges of Blockchain in Banking: A Scientometric View. International Journal of Interactive Multimedia and Artificial Intelligence,1.

Bakaul, M., Das, N., Moni, M., (2020) The Implementation of Blockchain in Banking System using Ethereum. International Journal of Computer Applications 177(38),50.

Brito, J., Castillo, A., (2013) Bitcoin - A Primer For Policymakers. George Mason University, USA: Mercatus Center.

Buterin, V., (2014) Slasher: A Punitive Proof-Of-Stake Algorithm. https://blog.ethereum.org. [Πρόσβαση: 26.10.2019]

Buterin, V., (2015) On Public And Private Blockchains. https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains. [Πρόσβαση:01.12.2019].

Cant, B., khadikar A., Ruiter A., Broneback j., Coumaros j., Buvat J., Cupta A., (2017) Getting From Hype To Reality. CapGemini, 1-24.

Guo, Y., Liang, C. (2016) Blockchain application and outlook in the banking industry. *Financial Innovation*, *2*(1), 24.

Haber, S., Stornetta, W., S., (1991) How To Time-stamp A Digital Document. Journal of Cryptology, vol.3, 99-111.

Hacioglu, U. (2019) Blockchain Economics and Financial Market Innovation: Financial Innovations in the Digital Age. Switzerland. Springer Nature.

IBM (2019) Deploy a Smart Contract on the Network. https://cloud.ibm.com/docs/blockchain?topic=blockchain-ibp-console-smart-contracts [Πρόσβαση: 15.12.2019].

Kehrli, J., (2016) Blockchain 2.0 - From Bitcoin Transactions To Smart Contract Applications. https://www.niceideas.ch/blockchain_2.0.pdf. [Πρόσβαση: 10.01.2020]

Kokina J., Mancha, R., & Pachamanova, D. (2017) Blockchain: Emergent Industry Adoption and Implications for Accounting. Journal of Emerging Technologies in Accounting, 14(2), 91–100.

Kraft, D., (2016) Difficulty Control For Blockchain-Based Consensus Systems. Springer Peer-to-Peer Networking and Applications, 9, 397–413.

Lamport, L., Shostak, R., & Pease, M. (1982) The Byzantine Generals Problem. ACM Transactions on Programming Languages and Systems, 4(3), 382–401.

Lee, Y., Lin, J., Hsu, J., Wu, J. (2020) A Time Bank System Design on the Basis of Hyperledger Fabric Blockchain. https://www.researchgate.net/publication/341260200_A_Time_Bank_System_Design_on_the_Basis_of_Hyperledger_Fabric_Blockchain [Πρόσβαση:02.05.2020].

Manevich, Y., Barger A., & Tock Y. (2018) Service Discovery for Hyperledger Fabric.https://www.researchgate.net/publication/325009023_Service_Discovery_for_Hyperledger_Fabric [Πρόσβαση:25.02.2020].

Mehar, M., Shier, C., Giambattista, A., Gong, E., Fletcher, G., Sanayhie, R., Kim, H. M., & Laskowski, M. (2017) *Understanding a Revolutionary and Flawed Grand Experiment in Blockchain: The DAO Attack*. Social Science Research Network.

Mendez C., Bayyou D. (2019) Blockchain Technology Applications in Education. International Journal of Computing and Technology, 6, 68-73.

Mori, T. (2016) Financial technology: Blockchain and securities settlement. Journal of Securities Operations & Custody, 8(3), 208-217.

Nakamoto, S., (2008) Bitcoin: A Peer-To-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf. [Πρόσβαση: 25.10.2019]

Peter, H., Moser, A., (2017) Blockchain Applications in Banking & Payment Transactions: Results Of A Survay. International Scientific Conference, 142.

Pilkington, M. (2016) Blockchain technology: Principles and applications. Research handbook on digital transformations, 225.

Pongnumkul, S.; Siripanpornchana, C.; Thajchayapong, S., (2017) Performance Analysis of Private Blockchain Platforms in Varying Workloads. In Proceedings of the 2017 26th International Conference on Computer Communication and Networks (ICCCN), Vancouver, BC, Canada, IEEE: Piscataway, NJ, USA, 1–6.

Prause, G. (2019) Smart Contracts for Smart Supply Chains. *IFAC-PapersOnLine*, *52*(13), 2501–2506.

R3 | DLT & Blockchain Software Development Company, (2020). https://www.r3.com/ [Πρόσβαση:30.05.2020]

Shah, T., Jani, S., (2018) Applications Of Blockchain Technology In Banking & Finance. https://www.researchgate.net/publication/327230927 [Πρόσβαση:20.02.2020]

Shurman, M., Obeidat A., Al-Shurman, S. (2020) Blockchain and Smart Contract for IoT. (2020.) https://www.researchgate.net/publication/340974628_Blockchain_and_Smart_Contract_for_IoT [Πρόσβαση:31.05.2020]

Stanciu, A., (2017) Blockchain based distributed control system for edge computing. 21st International Conference on Control Systems and Computer Science (CSCS), 667–671.

Swan, M., (2015) Blockchain: Blueprint For A New Economy. Beijing: O'Reilly Media, Inc.

Tedeschi, E., Nordmo, T.-A. S., Johansen, D., & Johansen, H. D. (2019) Predicting Transaction Latency with Deep Learning in Proof-of-Work Blockchains. IEEE International Conference on Big Data 4223-4231.

Tsai, W.-T., Blower, R., Zhu, Y., & Yu, L. (2016) A System View of Financial Blockchains. 2016 IEEE Symposium on Service-Oriented System Engineering (SOSE), 450.

Vasin, P., (2014) Blackcoins Proof-Of-Stake Protocol v2. https://blackcoin.org/blackcoin-pos-protocol-v2-whitepaper.pdf. [Πρόσβαση:11.11.2019].

Wood, G., (2017) Ethereum:A Secure Decentralised Generalised Transaction Ledger. https://ethereum.github.io/yellowpaper/paper.pdf [Πρόσβαση: 15.02.2020]

Wood, G., (2018) Ethereum Yellow Paper: a formal specification of Ethereum, a programmable blockchain. https://ethereum.github.io/yellowpaper/paper.pdf. [Πρόσβαση 7 2 2020].

Yoo, S. (2017). Blockchain based financial case analysis and its implications. *Asia Pacific Journal of Innovation and Entrepreneurship*, *11*(3), 312–321.

Zhao, H., & Coffie, C. P. K. (2018) *Economic Force of Smart Contracts*. https://papers.ssrn.com/abstract=3138063 [Πρόσβαση: 02.12.2019].