ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ Μ/Υ
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΣΧΟΛΗ ΝΑΥΤΙΛΙΑΣ ΚΑΙ ΒΙΟΜΗΧΑΝΙΑΣ
ΤΜΗΜΑΤΟΣ ΒΙΟΜΗΧΑΝΙΚΗΣ ΔΙΟΙΚΗΣΗΣ & ΤΕΧΝΟΛΟΓΙΑΣ
ΔΙΑΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
«ΤΕΧΝΟ-ΟΙΚΟΝΟΜΙΚΑ ΣΥΣΤΗΜΑΤΑ»

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Η ΧΡΗΣΗ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ BLOCKCHAIN ΓΙΑ ΤΗΝ ΔΙΑΣΦΑΛΙΣΗ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΤΩΝ ΨΗΦΙΑΚΩΝ ΒΙΒΛΙΟΘΗΚΩΝ ΚΑΙ ΤΩΝ ΧΡΗΣΤΩΝ ΤΟΥΣ

ΚΑΛΑΜΠΟΥΚΑΣ ΝΕΚΤΑΡΙΟΣ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ
ΠΑΠΑΒΑΣΙΛΕΙΟΥ ΣΥΜΕΩΝ

ΟΚΤΩΡΙΟΣ 2020

Περίληψη

Με την τεχνολογία Blockchain να γίνεται ένα πιο σχετικό θέμα που συζητείται τόσο στην επιχείρηση όσο και στους χρηματοοικονομικούς τομείς, το ενδιαφέρον για αυτήν την τεχνολογία έχει γίνει ένα αυξανόμενο θέμα και οι εικασίες δείχνουν ότι η αύξηση του ενδιαφέροντος θα μεγαλώνει κάθε χρόνο όπως αναφέρεται στην ανασκόπηση της βιβλιογραφίας. Επομένως η παρούσα διπλωματική ασχολείται με τα οφέλη αυτής της νέας τεχνολογίας. Οι χάκερ καταλήγουν σε μεθόδους και δυνατότητες παραβίασης των τειχών ασφαλείας του Blockchain. Το Hyperledger είναι μια τεχνολογία Blockchain ανοιχτού κώδικα που επιτρέπει σε χρήστες από όλο τον κόσμο να κάνουν συναλλαγές μεταξύ πολλών επιχειρήσεων πιο αποτελεσματικά από τις τρέχουσες τεχνολογίες. Τα έξυπνα συμβόλαια επιτρέπουν πιο ασφαλείς συναλλαγές χωρίς την ανάγκη τρίτων μερών και συναντήσεων όπου γίνονται συζητήσεις και προγραμματισμός, επιταχύνοντας τις διαδικασίες μεταξύ πολλών οντοτήτων.

Λέξεις Κλειδιά: τεχνολογία Blockchain, έξυπνα συμβόλαια, ψηφιακή βιβλιοθήκη

Abstract

With blockchain technology becoming a more relevant topic discussed in the business as well as financial fields, the interest in this technology has become a growing topic, speculations show that the growth of interest is rising each year as spoken about in the literature review therefore this project has talked about the benefits of this newly profound technology. Hackers come up with methods and possibilities to breach the security walls of the blockchain. Hyperledger being an open source blockchain technology which allows users from across the world to make transactions between multiple businesses more efficiently than current technologies. Smart contracts allow for more secure transactions without the need of extra parties and meetings where discussions and planning take place, speeding up the process of the terms between multiple entities.

Key Words: Blockchain, Smart contracts, digital libraries

Πρόλογος

Η παρούσα εργασία εκπονήθηκε από τον φοιτητή Καλαμπουκά Νεκτάριο στα πλαίσια ολοκλήρωσης των μεταπτυχιακών σπουδών στο δια τμηματικό πρόγραμμα μεταπτυχιακών σπουδών «Τεχνοοικονομικά συστήματα», που προσφέρεται σε συνεργασία από το Εθνικό Μετσόβιο Πολυτεχνείο και το Πανεπιστήμιο Πειραιά.

Αυτή η διατριβή αφορά στη δημιουργία ενός περιβάλλοντος όπου ο χρήστης μπορεί να χρησιμοποιήσει την τεχνολογία Blockchain για να αγοράσει βιβλία από μια ψηφιακή βιβλιοθήκη στο Blockchain. Η εφαρμογή ενός τέτοιου συστήματος δεν περιορίζεται σε διαχειριστές και χειριστές ψηφιακών βιβλιοθηκών, αλλά μπορεί να επεκταθεί σε εταιρικά περιβάλλοντα και εκπαιδευτικά ιδρύματα. Η ασφάλεια των συναλλαγών είναι πιο αξιόπιστη και ασφαλής λόγω των αλγορίθμων κατακερματισμού.

ΠΕΡΙΕΧΕΜΕΝΑ

Εισαγωγή 6

ΚΕΦΑΛΑΙΟ 1: ΒΙΒΛΙΟΓΡΑΦΙΚΗ ΑΝΑΣΚΟΠΗΣΗ 9

1.1 Εισαγωγή 9

1.2 Στόχοι 9

1.3 Αυθεντικοποίηση 11

1.4 Τεχνολογίες Hyperledger 11

1.5 BlockChain και Bitcoin 13

1.6 Οφέλη Τεχνολογίας Blockchain 16

1.7 Χρήση Τεχνολογίας Blockchain για διατήρηση ιδιωτικότητας 18

1.8 Έξυπνα vs Παραδοσιακά Συμβόλαια 19

1.9 Τωρινά Έξυπνα Συμβόλαια και τι είναι 22

1.10 Έξυπνα Συμβόλαιο και Επιθέσεις 25

1.11 Τρέχουσα Πρόληψη Επιθέσεων 26

1.12 Προκλήσεις να ξεπεραστούν 27

1.13 Τρέχουσες Τεχνολογίες σε Ψηφιακές Βιβλιοθήκες 28

1.14 Πρόσφατες Επιθέσεις σε Ψηφιακές Βιβλιοθήκες 31

1.15 Τεχνητή Νοημοσύνη και Ψηφιακές Βιβλιοθήκες 32

1.16 Επίλογος 32

ΚΕΦΑΛΑΙΟ 2 : Μεθοδολογία 33

2.1 Εισαγωγή 33
2.2. Σχεδιασμός Μεθοδολογίας 33
2.3 Testbed 35
2.4 Συμπεράσματα 37
ΚΕΦΑΛΑΙΟ 3 : Υλοποίηση 38
3.1 Εισαγωγή 38
3.2 Παραμετροποίηση του Hyperledger Composer 38
3.3 Δημιουργία Αρχείου Μοντέλου 41
3.4 Αρχείο Σεναρίου 44
3.5 Έλεγχος Πρόσβασης και Άδειες 46
ΚΕΦΑΛΑΙΟ 4: Αποτελέσματα 47
4.1 Hyperledger Composer Backround 47
4.2 Output 48
ΚΕΦΑΛΑΙΟ 5 : Επίλογος 50
ΒΙΒΛΙΟΓΡΑΦΙΑ 51

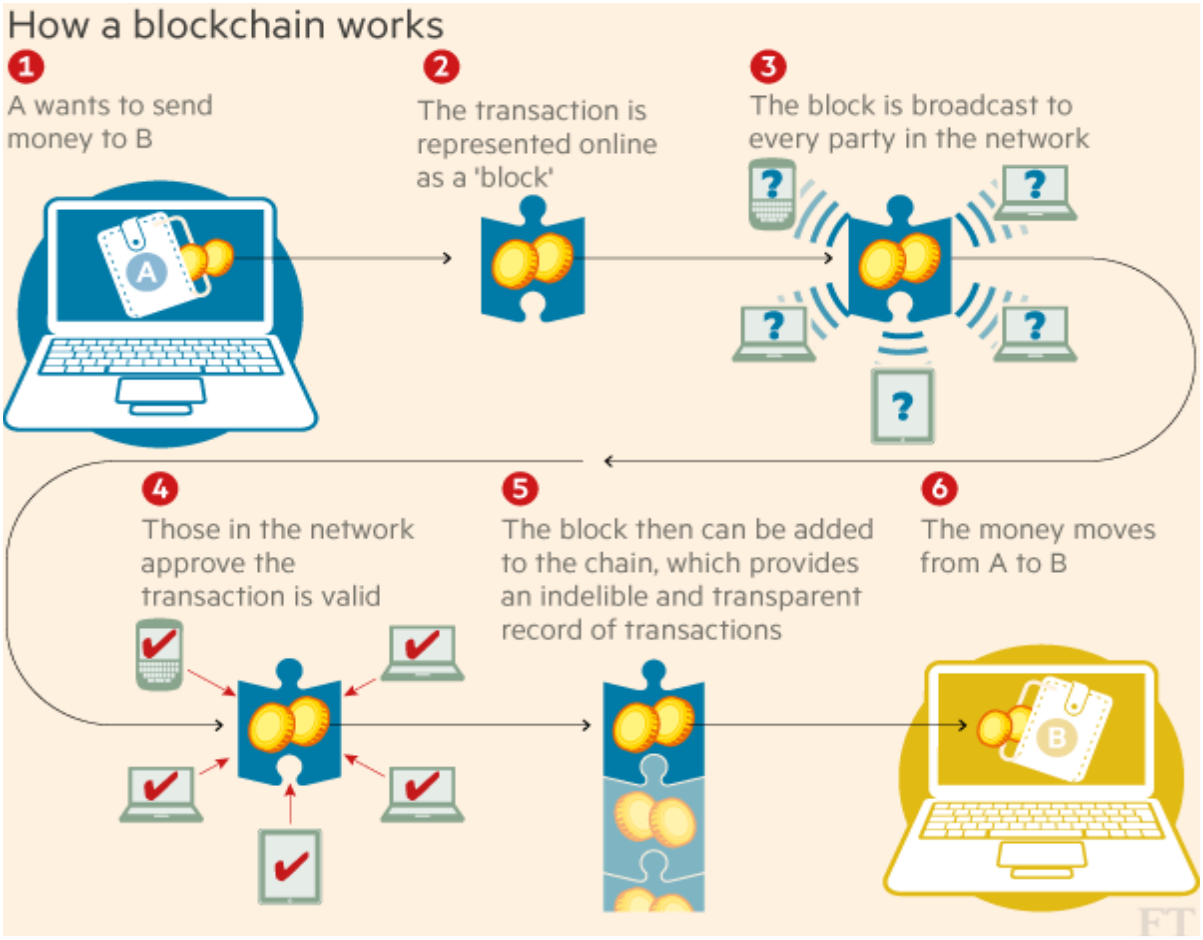
Εισαγωγή

Η ιδέα της εξασφάλισης πληροφοριών σε (ηλεκτρονικές βιβλιοθήκες) ψηφιακές βιβλιοθήκες χρησιμοποιώντας Blockchain.

Οι ψηφιακές βιβλιοθήκες διατηρούν όλες τις πληροφορίες σε έναν κεντρικό διακομιστή. Με αυτόν τον τρόπο οι πληροφορίες μπορούν να αποθηκευτούν, να ανακτηθούν και να αποθηκευτούν σχεδόν αμέσως χωρίς να χρειάζεται να φύγετε από το σπίτι. Με την πάροδο των ετών οι ψηφιακές βιβλιοθήκες έχουν βελτιωθεί σημαντικά και αυξάνουν τον βαθμό διείσδυση τους, όπως γράφει το έγγραφο: «Οι ψηφιακές βιβλιοθήκες έχουν σημειώσει σημαντική πρόοδο, τόσο στην τεχνολογία όσο και στις εφαρμογές της». (Somvir & Kaushik, 2019). Η συλλογή πληροφοριών σε ηλεκτρονική και ψηφιακή μορφή αποτελεί τη βάση των ψηφιακών βιβλιοθηκών. Ο ορισμός της ψηφιακής βιβλιοθήκης ορίζεται ως «Οι ψηφιακές βιβλιοθήκες είναι οργανισμοί που παρέχουν τους πόρους, συμπεριλαμβανομένου του εξειδικευμένου προσωπικού, για να επιλέξουν, να δομήσουν, να προσφέρουν πνευματική πρόσβαση , να ερμηνεύσουν, να διανείμουν, να διατηρήσουν την ακεραιότητα και να διασφαλίσουν ότι οι συλλογές ψηφιακών είναι εύκολα και οικονομικά διαθέσιμες για χρήση από μια καθορισμένη κοινότητα ή ένα σύνολο κοινοτήτων. " (Somvir & Kaushik, 2019), το οποίο αναφέρεται άμεσα ότι το μέλλον της βιβλιοθήκης έγκειται στην ψηφιοποίηση καθώς παρέχει καλύτερη οργάνωση καθώς και ευκολότερη πρόσβαση στις πληροφορίες, επομένως αυξάνεται η δημοτικότητά του έναντι των κανονικών βιβλιοθηκών.

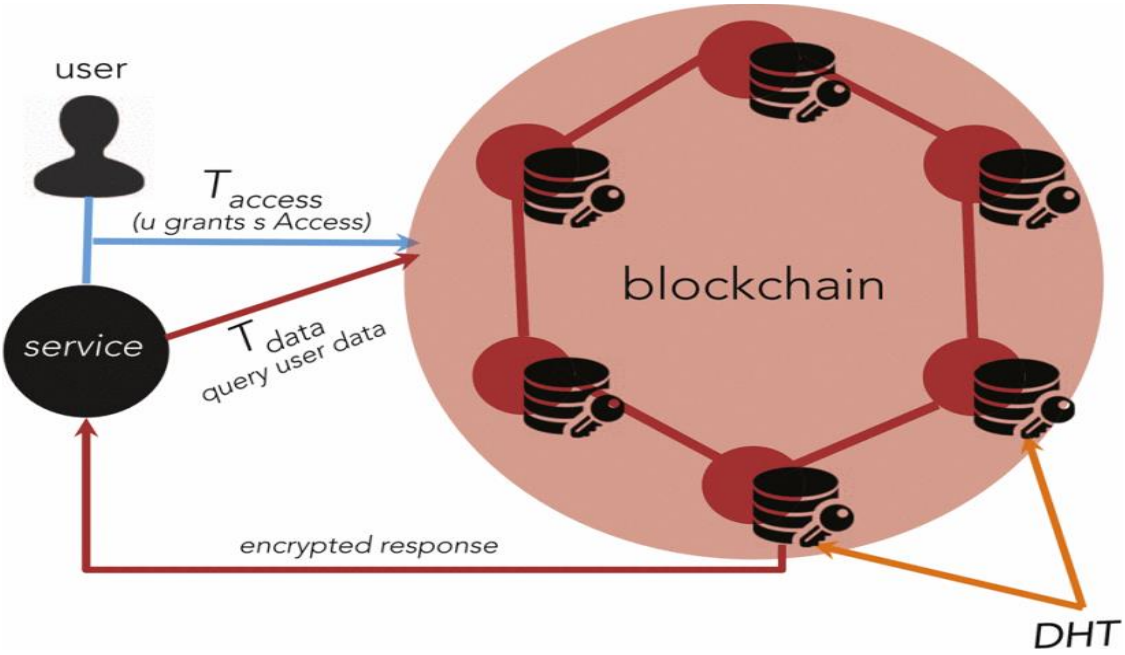
Το Blockchain θα εφαρμοστεί για να αποδείξει ότι είναι ασφαλέστερο από οποιαδήποτε τρέχουσα τεχνολογία να διατηρήσει τις πληροφορίες ασφαλείς και να αποτρέψει επιθέσεις. Το Blockchain μπορεί να εφαρμοστεί σε οποιαδήποτε συναλλαγή στον ψηφιακό κόσμο, επομένως υπάρχουν πολλά οφέλη και τομείς που μπορούν να επωφεληθούν από τη χρήση αυτής της τεχνολογίας. Ο τρόπος λειτουργίας του Blockchain είναι παρόμοιος με τις συναλλαγές Blockchain .

Ο ορισμός του Blockchain ορίζεται ως "Κάθε συναλλαγή προστατεύεται μέσω ψηφιακής υπογραφής, αποστέλλεται στο" δημόσιο κλειδί "του παραλήπτη και υπογράφεται ψηφιακά χρησιμοποιώντας το" ιδιωτικό κλειδί "του αποστολέα . Για να δαπανήσει χρήματα, ο ιδιοκτήτης του κρυπτονομίσματος πρέπει να αποδείξει την ιδιοκτησία του "ιδιωτικού κλειδιού" (Crosby, 2016). Επομένως κάθε συναλλαγή προστατεύεται από κρυπτογραφία. Τα περισσότερα δίκτυα Blockchain είναι αποκεντρωμένα, επομένως οι πληροφορίες είναι πιο δύσκολο να καταστραφούν.



Διάγραμμα 1: Συναλλαγές χρησιμοποιώντας τεχνολογία Blockchain

Το Blockchain λειτουργεί σε αποκεντρωμένη πλατφόρμα, αυτό σημαίνει ότι δεν υπάρχει κεντρικός φορέας που να ελέγχει τη μεταφορά των πληροφοριών. «Η βασική ιδέα της αποκέντρωσης είναι να διανέμεται ο έλεγχος και η εξουσία στις περιφέρειες ενός οργανισμού αντί ενός κεντρικού οργάνου να έχει τον πλήρη έλεγχο του οργανισμού. (Bashir, n.d.), επομένως δεν υπάρχει σώμα που να ελέγχει τη μεταφορά των πληροφοριών μεταξύ των χρηστών. Ο αποκεντρωμένος ορισμός συστήματος ορίζεται ως «Ένα αποκεντρωμένο σύστημα είναι ένας τύπος δικτύου όπου οι κόμβοι δεν εξαρτώνται από έναν μόνο κύριο κόμβο. Αντίθετα, ο έλεγχος κατανέμεται μεταξύ πολλών κόμβων. Αυτό είναι ανάλογο με ένα μοντέλο όπου κάθε τμήμα σε έναν οργανισμό είναι υπεύθυνο για τον δικό του διακομιστή βάσεων δεδομένων, αφαιρώντας έτσι την εξουσία από τον κεντρικό διακομιστή και διανέμοντάς το στα υποτμήματα που διαχειρίζονται τις δικές τους βάσεις δεδομένων. " (Bashir, n.d.).



Διάγραμμα 2: Επισκόπηση Αποκεντρωμένης Πλατφόρμας

ΚΕΦΑΛΑΙΟ 1: ΒΙΒΛΙΟΓΡΑΦΙΚΗ ΑΝΑΣΚΟΠΗΣΗ

1.1 Εισαγωγή

Αυτό το κεφάλαιο παρουσιάζει μια ανασκόπηση της βιβλιογραφίας που θα καταδείξει μια καλύτερη κατανόηση των βασικών πτυχών της παρούσας διπλωματικής.

Η πρώτη ενότητα παρουσιάζει βιβλιογραφική έρευνα σχετικά με το θέμα της διατήρησης του απορρήτου στις ψηφιακές βιβλιοθήκες και τις υπάρχουσες διαθέσιμες τεχνολογίες, προκειμένου να κατανοηθεί βασικά πώς μπορούν να εφαρμοστούν και να ξεπεραστούν οι προκλήσεις καθώς και να βελτιωθεί η ασφάλεια.

Στη συνέχεια πραγματοποιείται μία σύγκριση μεταξύ των τρεχόντων κεντρικών συστημάτων που χρησιμοποιούνται έναντι της τεχνολογίας Blockchain που λειτουργεί χρησιμοποιώντας αποκεντρωμένη λογική. Τα έξυπνα συμβόλαια θα επιτρέπουν την ευκολότερη πραγματοποίηση συναλλαγών με τη βιβλιοθήκη και αυτό θα επιτρέπει ευκολότερο δανεισμό βιβλίων.

1.2 Στόχοι

Οι στόχοι της παρούσας διπλωματικής είναι η διασφάλιση του απορρήτου και της ανωνυμίας των χρηστών που χρησιμοποιούν ψηφιακές βιβλιοθήκες και χρειάζονται βιβλία.

Το συμβόλαιο θα επιτρέψει στον χρήστη να συνδεθεί με τα διαπιστευτήριά του, και εάν τα διαπιστευτήρια ταιριάζουν, τότε θα επιτρέπεται στον χρήστη να εισέλθει και να αγοράσει το

βιβλίο. Έχοντας ένα σύστημα όπου ένας βιβλιοθηκονόμος δεν έχει πρόσβαση στο ιστορικό σας, αυτό θα κάνει αυτό το σύστημα καλύτερο σύστημα από το παραδοσιακό, καθώς δεν θα υπάρχει

κανένας που θα επιτρέπει να κρίνει τον χρήστη από το τι είδους βιβλία πρόκειται να αγοράσει, προστατεύοντας έτσι την ιδιωτικότητα.

Η ύπαρξη αυτού του τύπου συστήματος θα επιτρέψει μια πιο ευχάριστη εμπειρία και θα επιτρέψει σε οποιονδήποτε να περιηγηθεί στον δικό του χώρο ανά πάσα στιγμή, εφόσον ο χρήστης έχει σύνδεση στο Διαδίκτυο. Θα έχει την δυνατότητα να αναζητήσει οποιοδήποτε είδος θέλει και να αγοράσει το βιβλίο ανά πάσα στιγμή.

Η τεχνολογία Blockchain και τα έξυπνα συμβόλαια πρόκειται να δώσουν την ασφάλεια που όλοι αναζητούν και να δώσουν στους χρήστες ασφαλέστερη περιήγηση. Επίσης θα επιτρέψει καλύτερη ασφάλεια και καλύτερη πρόληψη επιθέσεων στα τρέχοντα συστήματα , επομένως αυτό το νέο σύστημα θα πρέπει να υλοποιηθεί για καθημερινά χρήση.

Έχοντας προσωπικά στοιχεία σε έναν χρήστη ψηφιακής βιβλιοθήκης μπορεί εύκολα να γίνει κακή χρήση ή κακομεταχείριση. Αυτές οι λεπτομέρειες συνήθως περιλαμβάνουν το πλήρες όνομα, τη διεύθυνση, τον αριθμό τηλεφώνου τους και ορισμένοι χρήστες αποθηκεύουν τα στοιχεία της κάρτας τους για να διευκολύνουν την επόμενη αγορά τους. Μια τέτοια επίθεση συνέβη σε British Airways και Ticketmaster όπως (K. Nichols, 2018) δήλωσε "Η βιβλιοθήκη Javascript της Feedify παραβιάστηκε με mirroring κωδικών της MegaCart, το οποίο κλέβει πιστωτικές κάρτες. Ολόκληρη η υπόθεση δημοσιεύτηκε στην εφημερίδα. (Nichols, 2018).

Η αξιολόγηση της ασφάλειας της υλοποίησης που θα παρουσιαστεί θα γίνει με την χρήση ενός cluster Kubernets που θα επιτρέψει την εγκατάσταση του Hyperledger και την εκτέλεση των έξυπνων συμβολαίων. Στη συνέχεια, για να αποδειχθεί η βελτιωμένη ασφάλεια σε σχέση με τα τρέχοντα συστήματα θα υπάρξει επίδειξη του αποκλεισμό εισερχόμενων επιθέσεων

1.3 Αυθεντικοποίηση

Ο έλεγχος ταυτότητας ενός χρήστη που μπαίνει σε μια βιβλιοθήκη είναι σημαντικός. Οι λεπτομέρειες που πιθανότατα θα διατηρηθούν σχετικά με τον χρήστη θα είναι: Όνομα, Διεύθυνση, Φύλο, Ημερομηνία γέννησης, επιλεγμένη εικόνα, καθώς και μια λίστα βιβλίων που διαβάζει ο χρήστης . Ο βιβλιοθηκονόμος δεν πρέπει να έχει πρόσβαση σε αυτές τις ευαίσθητες λεπτομέρειες σχετικά με το άτομο που επισκέπτεται τη βιβλιοθήκη. Ο βιβλιοθηκονόμος θα πρέπει να έχει πρόσβαση μόνο για να δει ότι ο χρήστης έχει δανειστεί το βιβλίο ψηφιακό ή μη. Προκειμένου να παρέχεται στους χρήστες ενισχυμένο απόρρητο και ασφάλεια, τα έξυπνα συμβόλαια θα παρέχουν αξιόπιστες συναλλαγές. Αυτές οι συναλλαγές θα είναι peer-to-peer αντί να εμπλέκονται τρίτα μέρη. Η κρυπτογραφία θα προσφέρει καλύτερη ασφάλεια καθώς οι συναλλαγές έχουν χρονική σήμανση και εφαρμόζουν τιμή κατακερματισμού για να δημιουργήσουν ένα ασφαλές δίκτυο στο Blockchain.

1.4Τεχνολογίες Hyperledger

Η τεχνολογία hyperledger επιτρέπει τη δημιουργία πλαισίου και βάσης κώδικα καθώς και την εκτέλεση κατανεμημένων εφαρμογών χρησιμοποιώντας γενικές γλώσσες προγραμματισμού με ανοιχτές πλατφόρμες στην αγορά.

Οι κύριοι στόχοι των τεχνολογιών hyperledger είναι να προωθήσουν την τεχνολογία Blockchain προσδιορίζοντας την ανοιχτή τυπική πλατφόρμα που είναι για τα κατανεμημένα μητρώα, τα οποία στη συνέχεια μπορούν να μεταμορφώσουν τον τρέχοντα τρόπο λειτουργίας των χρηματοοικονομικών και άλλων επιχειρηματικών συναλλαγών παγκοσμίως. (Cachin, 2016).

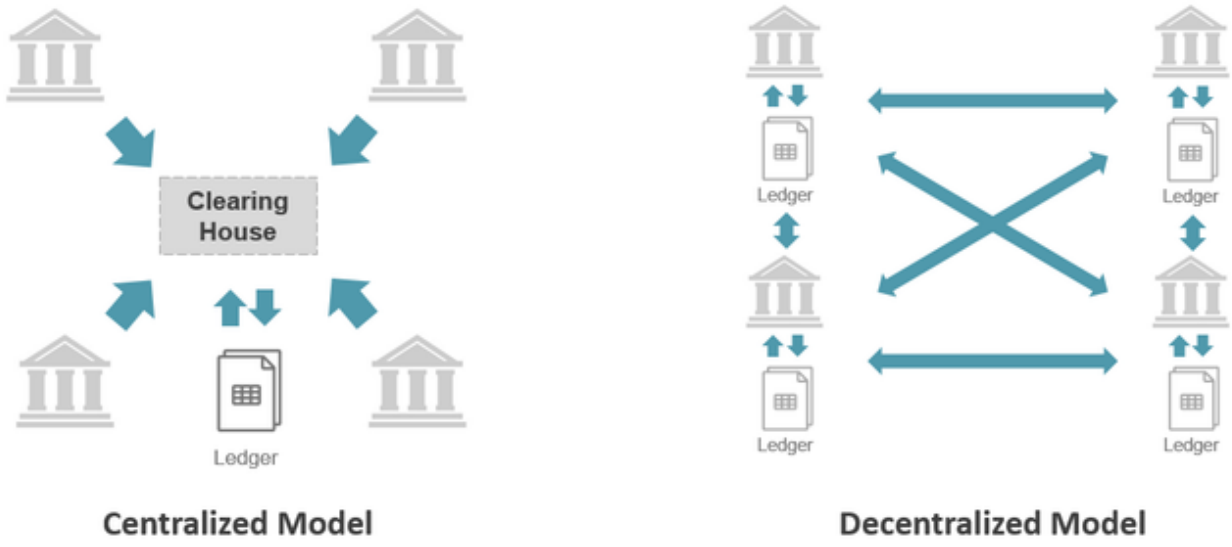
Όπως ανέφεραν οι Androulaki, Barger, Bortnikov, De Caro & Enyeart (2018): « Το Fabric είναι το πρώτο πραγματικά επεκτάσιμο σύστημα Blockchain για την εκτέλεση κατανεμημένων εφαρμογών. Υποστηρίζει αρθρωτά πρωτόκολλα συναίνεσης, τα οποία επιτρέπουν στο σύστημα να προσαρμόζεται σε συγκεκριμένες περιπτώσεις χρήσης και μοντέλα εμπιστοσύνης.

Το Fabric είναι επίσης το πρώτο σύστημα blockchain που εκτελεί κατανεμημένες εφαρμογές γραμμένες σε τυπικές γλώσσες προγραμματισμού γενικού σκοπού, χωρίς συστηματική εξάρτηση από εγγενή κρυπτογράφηση. »

Αυτό επιτρέπει την εύκολη πρόσβαση σε διάφορες εταιρείες, καθώς και σε επιχειρήσεις, για να αλλάξουν τον τρόπο επεξεργασίας των συναλλαγών στο εγγύς μέλλον, εάν οι εταιρείες θα συνειδητοποιήσουν πόσο ωφέλιμες είναι αυτές οι τεχνολογίες.

Η τρέχουσα κατάσταση των μητρώων έχει επιπτώσεις όταν εμπλέκεται με νέες τεχνολογίες μητρώων για να διασφαλίσει ότι υπάρχουν υψηλά μέτρα ασφαλείας κατά τυχόν δόλιων γεγονότων. Οι οργανισμοί χρησιμοποιούν συνήθως κεντρικά συστήματα μητρώων για την καταγραφή συναλλαγών καθ 'όλη τη διάρκεια της ημέρας. Ένα κεντρικό μητρών ελέγχεται από μια μοναδική οντότητα. Εάν το σύστημα επρόκειτο να κατέβει, αυτό θα επηρέαζε όλα τα μέλη και θα τερμάτιζε όλες τις διαδικασίες. Όπως αναφέρεται στο άρθρο από τους R Nair & Sebastian (2017) «Σε περίπτωση τραπεζικών συναλλαγών που δημοσιεύονται σε ένα κεντρικό σύστημα εάν η ελεγκτική οντότητα τερματιστεί απότομα, όλες οι συναλλαγές θα τερματιστούν και δεν είναι δυνατή η επεξεργασία τους. Αυτό μπορεί να οδηγήσει σε παράλειψη αναπαράστασης των συναλλαγών στην κατάσταση λογαριασμού. ». Αυτό θα είχε τεράστιο αντίκτυπο στο χρηματοπιστωτικό σύστημα των τραπεζών, με το κεντρικό σύστημα να απαιτείται η εσωτερική και εξωτερική κατανόηση των δεδομένων για να διασφαλιστεί η πλήρης ακεραιότητα των συναλλαγών που διέρχονται.

Για να αποφευχθούν αυτά τα ζητήματα, ένα κατανεμημένο μητρώο θα ήταν χρήσιμο. Όταν το σύστημα θα έπεφτε, θα υπήρχαν περισσότερες από μία οντότητες. Αυτό σημαίνει ότι θα επιτρέπεται στις άλλες οντότητες να μεταφέρουν αυτές τις συναλλαγές, όπως φαίνεται πώς τα δύο διαφορετικά μητρώα λειτουργούν στο παρακάτω σχήμα.



Διάγραμμα 3 : Συγκεντρωτικό vs Αποκεντρωμένο Μητρώο (M. Jeremiah, 2018)

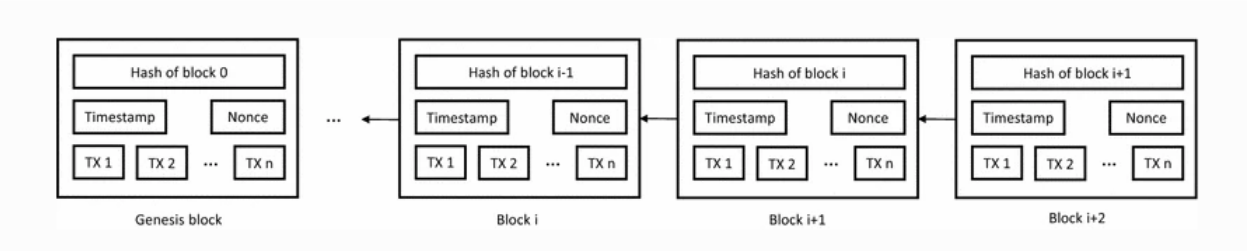
1.5 BlockChain και Bitcoin

Το Blockchain είναι ένα ρεύμα που έχει χρησιμοποιηθεί ευρέως αλλά δεν είναι κατανοητό: «Τι είναι το blockchain και ο σκοπός του;». Η τεχνολογία Blockchain και τα κατανεμημένα μητρώα έχουν αυξηθεί από το Satoshi Nakamoto και την άνοδο της οικονομικής χρήσης του Blockchain. Ο γίγαντας κρυπτονομίσματος Bitcoin ήταν το πρωταρχικό αντικείμενο στον τομέα του Blockchain. Το Bitcoin βρίσκεται σε άνοδο από το 2009 όταν δημιουργήθηκε το δίκτυο, αλλά ένα

χρόνο νωρίτερα ο Satoshi Nakamoto κυκλοφόρησε τη Λευκή Βίβλο για το Bitcoin. (Coghill, 2018).

Το Blockchain ζωντανεύει λόγω του Satoshi Nakamoto, χρησιμοποιώντας ένα ψευδώνυμο, κατάφερε να συνοψίσει τον τρόπο λειτουργίας του Bitcoin. Αυτό θα είναι το μέλλον των συναλλαγών λόγω της ασφάλειας και της ανωνυμίας του. Αυτός ο νέος τύπος νομίσματος είναι ασφαλέστερος, εύχρηστος και αξιόπιστος. Για παράδειγμα, οι συναλλαγές που εκτελούνται μεταξύ των δύο μερών, το PARTY A κατέχει το νόμισμα και το PARTY B είναι πρόθυμο να το αποκτήσει. Αυτές οι συναλλαγές χρειάζονται συμφωνία για την πραγματοποίηση της συναλλαγής για αυτά τα μέρη, προκειμένου να ικανοποιηθούν και να ενημερωθούν σωστά ότι η συναλλαγή ήταν επιτυχής. (Coghill, 2018).

Ένα Blockchain είναι ένα πολύ περίπλοκο δίκτυο που αποτελείται από δεδομένα που στη συνέχεια ορίζονται σε μια αλυσίδα μπλοκ και αυτά τα μπλοκ αντιπροσωπεύουν συναλλαγές, αυτό επεκτείνεται με επιπλέον μπλοκ και αντιπροσωπεύει ένα μητρώο ιστορικού συναλλαγών. Αυτά τα μπλοκ στη συνέχεια επικυρώνονται κρυπτογραφικά από το δίκτυο, μετά σφραγίζονταιι χρονικά και η τιμή κατακερματισμού α από το προηγούμενο μπλοκ που θα ήταν ο γονέας θα μεταβιβαστεί στο μπλοκ- παιδί . Ένα μοναδικό γονικό μπλοκ μπορεί να έχει πολλαπλά μπλοκ-παιδιά, καθένα από αυτά αναφέρεται στο ίδιο γονικό μπλοκ, γι 'αυτό περιέχει το ίδιο πεδίο κατακερματισμού στο προηγούμενο μπλοκ του πεδίου κατακερματισμού. Αυτό το είδος της ιδέας διασφαλίζει την ακεραιότητα του blockchain. (Nofer, Gomber, Hinz & Schiereck, 2017)



Διάγραμμα 4 : Σχεδιασμός Blockchain

Η συνάρτηση κρυπτογραφικού κατακερματισμού (SHA-3) χρησιμοποιείται από το Bitcoin που είναι το μεγαλύτερο κρυπτονόμισμα. Είναι απλό να προσδιοριστεί η ακεραιότητα κάποιου και να συγκρίνουμε την έξοδο των κατακερματισμών με την ήδη γνωστή και αναμενόμενη τιμή κατακερματισμού που είναι αποθηκευμένη στο Blockchain . Οι τιμές κατακερματισμού είναι μοναδικές, δεν υπάρχει ίδια τιμή και η απάτη μπορεί εύκολα να αποφευχθεί, ενώ μια αλλαγή στο μπλοκ της αλυσίδας θα άλλαζε αμέσως την τιμή κατακερματισμού. Ο αλγόριθμος κατακερματισμού μετατρέπει μεγάλο αριθμό δεδομένων σε κατακερματισμό σταθερού μήκους. Μια μικρή τροποποίηση δεδομένων θα αλλάξει εντελώς αυτό το κατακερματισμό. (Singh & Singh, 2016)

Οι τρέχουσες συναλλαγές που εκτελούνται από τις ψηφιακές βιβλιοθήκες είναι συγκρίσιμες με άλλα διαδικτυακά καταστήματα. Υπάρχουν πολλοί πιθανοί τρόποι αγοράς του προϊόντος, παλιομοδίτικος τρόπος πληρωμής καρτών και PayPal.

Οι βιβλιοθήκες θα επωφεληθούν από μια τέτοια τεχνολογία, επειδή είναι ένα πολύ πιο ασφαλές σύστημα, καθώς και ένας γρηγορότερος τρόπος αγοράς ηλεκτρονικών πόρων, όπως αναφέρεται στο περιοδικό:

«Για τις βιβλιοθήκες, αυτό θα μπορούσε να αλλάξει τον τρόπο αγοράς και πληρωμής των ηλεκτρονικών πόρων, συμπεριλαμβανομένης της διατήρησης των ετήσιων προγραμμάτων τιμολόγησης. Μια βιβλιοθήκη θα μπορούσε να αγοράσει πρόσβαση σε έναν ηλεκτρονικό πόρο από έναν προμηθευτή, να το πληρώσει με ένα ψηφιακό νόμισμα και να δημιουργήσει ή να ενημερώσει ένα συμβόλαιο για έναν πόρο μέσω Bitcoin και Blockchain. " (Coghill, 2018).

1.6 Οφέλη Τεχνολογίας Blockchain

Οι Ølnes, Ubacht & Janssen (2017) έχουν συζητήσει πολλά οφέλη που σχετίζονται με τη χρήση Blockchain, ιδίως σε σχέση με την αύξηση της διαφάνειας, τη μείωση της διαφθοράς και την αποφυγή απάτης.

Διαφάνεια - Το ιστορικό των συναλλαγών παραμένει ορατό σε κάθε κόμβο και κάθε ένας από αυτούς τους κόμβους έχει τη δυνατότητα να δει ολόκληρη την επισκόπηση.

Μείωση της διαφθοράς - Τα κατανεμημένα μητρώα επιτρέπουν την ασφαλή αποθήκευση, έχοντας έξυπνα συμβόλαια που θα αποτρέψουν τη χειραγώγηση και την αλλαγή ιδιοκτησίας, καθώς όλες οι πληροφορίες πρόκειται να αποθηκευτούν στο μπλοκ.

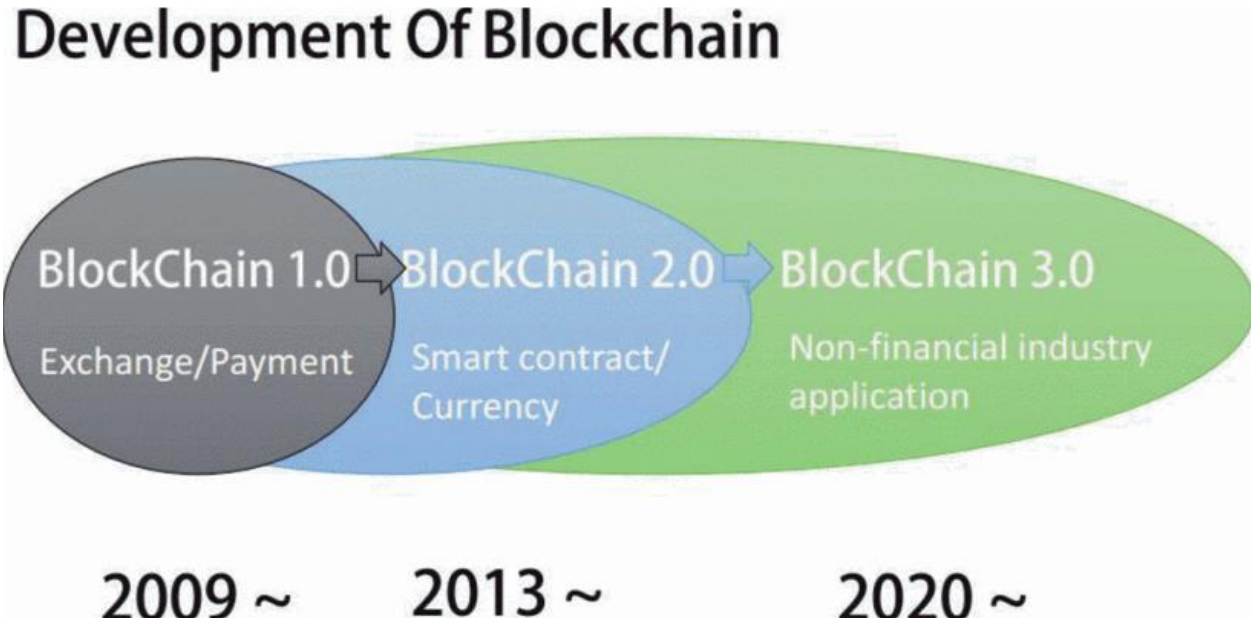
Αποφυγή απάτης - Έχοντας αποθηκευμένα δεδομένα σε πολλαπλά μητρώα, είναι πολύ δύσκολο για τους χάκερ να κάνουν οποιεσδήποτε μη εξουσιοδοτημένες αλλαγές.

Αυτά τα οφέλη εξαρτώνται σε μεγάλο βαθμό το ένα από το άλλο, αυτά τα οφέλη βελτιώνουν την ακεραιότητα των δεδομένων και τις αδιαμφισβήτητες συναλλαγές που επιτρέπουν ταχύτερη ανίχνευση εάν κάτι αλλάξει ή χαθεί. Αυτή η πρωτοβουλία μειώνει τη διαφθορά και την απάτη. (Ølnes, Ubacht & Janssen, 2017)

Αυτό δίνει μια θετική ματιά στο μέλλον όπου το Blockchain μπορεί να βελτιωθεί καθώς και να εξελιχθεί. Υπάρχει μια αύξηση εφαρμογών και δυνατοτήτων στο Blockchain, ειδικά στην περιοχή όπου ένα τρίτο μέρος θα ήταν απαραίτητο για την εξουσιοδότηση της εμπιστοσύνης. Πολλά πεδία ενδέχεται να ανακατασκευαστούν λόγω του Blockchain όπως οι βιβλιοθήκες, η πολιτική και η ψηφοφορία.

Η μετακίνηση της ψηφοφορίας στο Blockchain έχει συζητηθεί, όπως ο Yu et al. (2018) δηλώνει «Αναλύουμε την ορθότητα και την αντίσταση στον εξαναγκασμό του προτεινόμενου συστήματος ψηφοφορίας. Χρησιμοποιούμε το Hyperledger Fabric για να αναπτύξουμε το σύστημα ψηφοφορίας μας και να αναλύσουμε αριθμητικά την απόδοση του αναπτυσσόμενου σχήματος. ", Το μέλλον των ψηφοφοριών είναι η μετάβαση σε ένα πολύ πιο ασφαλές περιβάλλον όπου η ψηφοφορία χωρίς έξοδο από το σπίτι θα είναι μια επιλογή.

Η αποκέντρωση των κυβερνητικών υπηρεσιών μέσω του Blockchain είναι δυνατή καθώς θα αυξηθεί η δημοτικότητά της. Ο πλούτος μπορεί να προστατευθεί αποτελεσματικά μέσω του Blockchain, ειδικά στις χώρες του λεγόμενου τρίτου κόσμου. (Nofer, Gomber, Hinz & Schiereck, 2017)



Διάγραμμα 5 : Ανάπτυξη του Blockchain (Nofer, Gomber, Hinz & Schiereck, 2017)

1.7 Χρήση Τεχνολογίας Blockchain για διατήρηση ιδιωτικότητας

Η διατήρηση της ιδιωτικής ζωής είναι η πιο πολύτιμη ιδέα, η κατοχή των στοιχείων των χρηστών είναι κορυφαία προτεραιότητα και πρέπει να ληφθεί σοβαρά υπόψη. Το απόρρητο κάθε χρήστη αποτελεί κορυφαίο μέλημα της σύγχρονης κοινωνίας, εστιάζοντας σε υπηρεσίες που αναπτύσσονται σε κάθε χρήστη και οι οποίες συλλέγουν συνεχώς προσωπικά δεδομένα για τα οποία ο χρήστης δεν έχει τον έλεγχο. (Zyskind, Nathan & Pentland, 2019). Οι υπηρεσίες που παρέχονται από την τρέχουσα διατήρηση των δεδομένων, αποθηκεύοντάς τα σε ένα αποκεντρωμένο δίκτυο είναι ειλικρινείς και καθησυχαστικές για τους καθημερινούς ανθρώπους,

αλλά ταυτόχρονα αφήνοντας μερικούς ανθρώπους περίεργους για το τι πραγματικά προσδιορίζεται και για το τι «συμφωνούμε» κατά την επιβεβαίωση του πολιτικές.

Η προτεινόμενη λύση μέσω του Blockchain είναι να επιτρέπεται στους χρήστες να είναι σε θέση να κατέχουν και να ελέγχουν τα δεδομένα τους, καθώς και να βλέπουν την πολιτική τους. Το Blockchain θα είναι πιο αποτελεσματικό όταν διατηρεί το απόρρητο λόγω της ενεργού δομής του, έχοντας τα δεδομένα χρήστη να είναι ψευδώνυμα ανώνυμα ενώ θα μπορούν να επαληθεύουν την ταυτότητά τους. Προκειμένου να επαληθευτεί η ταυτότητα κάποιου, το Blockchain πραγματοποιεί μια συναλλαγή μεταξύ Α και Β, η συναλλαγή αντιπροσωπεύεται διαδικτυακά ως μπλοκ, το μπλοκ μεταδίδεται έπειτα σε κάθε συμβαλλόμενο μέρος σε αυτό το δίκτυο, η συναλλαγή στη συνέχεια εγκρίνεται από το μέρος σε αυτό το δίκτυο και τότε το μπλοκ προστίθεται στην αλυσίδα συναλλαγών που παρέχει εμφανή καταγραφή συναλλαγών. Επομένως, παραχωρώντας τη δυνατότητα αποθήκευσης των προφίλ των χρηστών στο Blockchain και τη δυνατότητα επαλήθευσης της ταυτότητάς τους μέσω αυτής της ασφαλούς μεθόδου, ο χρήστης θα έχει πρόσβαση όταν προσπαθεί να αγοράσει τα βιβλία του. (Zyskind, Nathan & Pentland, 2019).

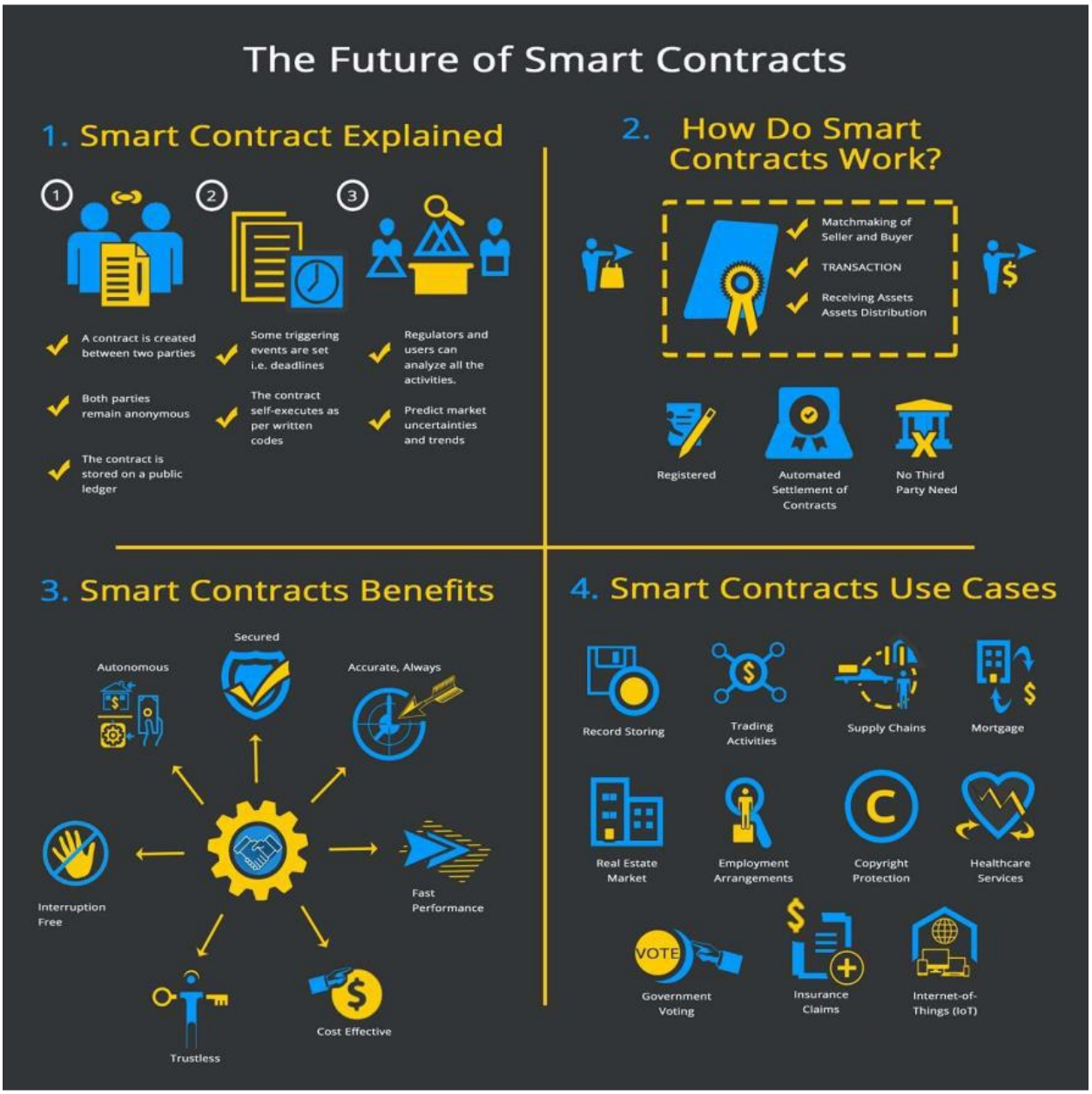
1.8 Έξυπνα vs Παραδοσιακά Συμβόλαια

Τα παραδοσιακά συμβόλαια θεωρούνται ως ένδειξη συμφωνίας μεταξύ δύο ή περισσοτέρων μερών που τους δεσμεύουν μέχρι τον καθορισμένο χρόνο όπως συμφωνήθηκε στη σύμβαση την οποία ορισμένα μέρη πιστεύουν ότι δεσμεύονται από τον νόμο. Αυτά τα συμβόλαια ωστόσο είναι γραμμένα σε χαρτί, υπογεγραμμένα από τους εκπροσώπους των μερών, ή υπάρχει ανάγκη επίσημου συνεργάτη όπως δικηγόρος ή μέλος της κυβέρνησης. Τα παραδοσιακά συμβόλαια

χρειάζονται χρόνο για να τεθούν σε ισχύ, και τα δύο μέρη πρέπει να αξιολογήσουν την κατάσταση της σύμβασης πριν την οριστικοποιήσουν και να καταλήξουν σε συμφωνία.

Τα έξυπνα συμβόλαια θα παρέχουν αξιόπιστες συναλλαγές. Ένα έξυπνο συμβόλαιο είναι μια συναλλαγή peer to peer και δεν υπάρχει ανάγκη συμμετοχής τρίτου μέρους, όπως τράπεζα. Δεν υπάρχει ανάγκη για νομικές συμφωνίες, αλλά μόνο κανονισμοί που έχουν τεθεί σε εφαρμογή από τη σύμβαση, όπως αποδεικνύεται από πολλούς ερευνητές.Ο Meitinger (2017), δήλωσε ότι οι έξυπνες συμβάσεις στα Blockchains είναι αξιόπιστες και τρίτα μέρη δεν απαιτούνται για να διασφαλιστεί ότι έχει πραγματοποιηθεί σωστή συναλλαγή. Τα πραγματικά συμβόλαια που είναι peer-to-peer είναι δυνατά χωρίς αποτυχία και στις περισσότερες περιπτώσεις η χρήση έξυπνων συμβάσεων είναι εφικτή.

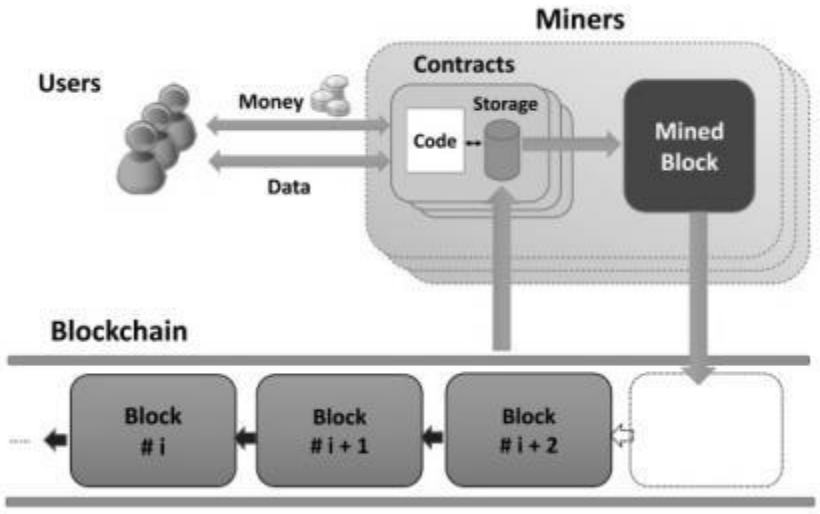
Τα έξυπνα συμβόλαια έχουν αρκετά πλεονεκτήματα σε σχέση με τα παραδοσιακά συμβόλαια, την προσέγγιση για την απόδειξη της γνησιότητας. Τα περισσότερα τρέχοντα παραδοσιακά συμβόλαια μπορούν να παραποιηθούν ή να αλλάξουν. Οι έξυπνες συμβάσεις φέρνουν ένα τεράστιο βήμα από την πλευρά της ασφάλειας των συμβάσεων. Με ένα ο έξυπνο συμβόλαιο που δεν δημιουργεί τέτοιες αλλαγές, με ψηφιακές υπογραφές κλειδιών, μόνο τα γνωστά μέρη μπορούν να το κατέχουν. Κάθε συμφωνία είναι χρονικά σφραγισμένη στο Blockchain που τα προστατεύει. Δεν υπάρχει τρόπος αλλαγής ή χειραγώγησης των συμβάσεων με οποιονδήποτε τρόπο. Όλο το δίκτυο αυτών των συμβάσεων φέρνει έναν δεσμό που δεν μπορεί να σπάσει. Είναι ο πιο ασφαλής τρόπος αντιμετώπισης και είναι καιρός αλλάξει η οπτική μας γωνία.Ζούμε σε έναν κόσμο όπου οι επιχειρησιακές δαπάνες είναι αυστηρά προϋπολογισμένες και οι έξυπνες συμβάσεις δεν απαιτούν οποιεσδήποτε δαπανηρές υπηρεσίες, δίνοντας έτσι την δυνατότητα να εξοικονομηθούν τεράστια ποσά.



Διάγραμμα 6 : Έξυπνα Συμβόλαια Επεξήγηση (Metinger, 2017))

1.9 Τωρινά Έξυπνα Συμβόλαια και τι είναι

Τα έξυπνα συμβόλαια δεν είναι αυτό που συνηθίζουν οι άνθρωποι όταν ακούνε τη λέξη «συμβόλαιο». Τα έξυπνα συμβόλαια είναι ένας εκτελέσιμος κώδικας που εκτελείται στο Blockchain και επιβάλλετε τους όρους της συμφωνίας που κωδικοποιήθηκαν. Αυτός είναι ο λόγος για τον οποίο τα έξυπνα συμβόλαια υπόσχονται χαμηλότερα τέλη συναλλαγής σε σύγκριση με τα παραδοσιακά συμβόλαια στα οποία απαιτούν ένα τρίτο μέρος για την επιβολή των όρων της σύμβασης. Ο εκτελέσιμος κώδικας αποθηκεύεται, επαληθεύεται και εκτελείται σε ένα Blockchain. Οι δυνατότητες του έξυπνου συμβολαίου εξαρτώνται από τη γλώσσα προγραμματισμού που χρησιμοποιείται για τον κωδικό της σύμβασης, το συμβόλαιο έχει το υπόλοιπο στο λογαριασμό του, τον αποθηκευτικό χώρο και όπως αναφέρθηκε προηγουμένως εκτελέσιμο κώδικα που χρησιμοποιήθηκε για τον προγραμματισμό της σύμβασης. Αποθηκεύεται στο Blockchain, κάθε φορά που χρησιμοποιείται το συμβόλαιο, το Blockchain ενημερώνεται. Μόλις χρησιμοποιηθεί το συμβόλαιο, μια μοναδική διεύθυνση εκχωρείται στο blockchain και ο κωδικός της σύμβασης δεν μπορεί να αλλάξει.



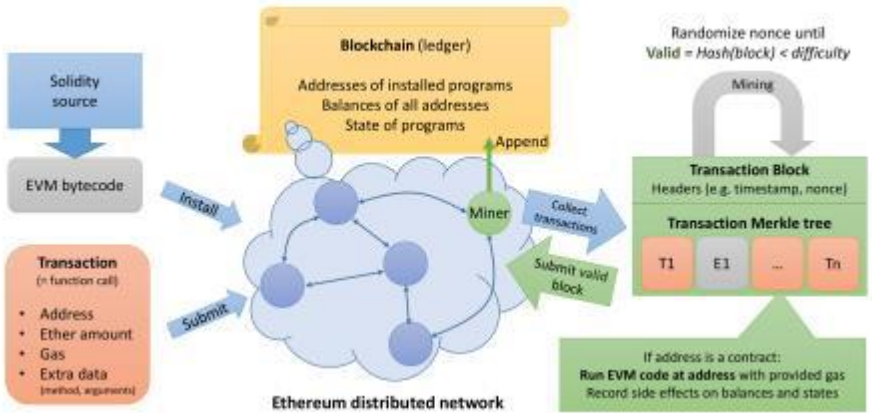
Διάγραμμα 7 : Επεξήγηση Εξόρυξης (Alharby & van Moorsel, 2020)

Οι πιο κοινές πλατφόρμες που χρησιμοποιούνται για έξυπνα συμβόλαια είναι τα Ethereum και Bitcoin, τα πιο δημοφιλή αποκεντρωμένα κρυπτονομίσματα που είναι γνωστά για την ασφάλειά τους. (Alharby & van Moorsel, 2020)

Το Ethereum χρηματοδοτεί εικονικό νόμισμα, το οποίο ονομάζεται Ether και βρίσκεται σε ένα Blockchain. Το πλαίσιο της Ethereum για την κρυπτογράφηση παρέχει μια παγκόσμια πλατφόρμα που ονομάζεται επίσης Ethereum Virtual Machine (EVM) που διαχειρίζεται το περιβάλλον για έξυπνες συμβάσεις στο Ethereum. Ο κύριος σκοπός της Εικονικής Μηχανής Ethereum είναι η εκτέλεση έξυπνων συμβολαίων που μεταφέρουν στοιχεία ενεργητικού από τον πελάτη Α στον πελάτη Β. Η συγγραφή ασφαλών συμβολαίων μπορεί να είναι εξαιρετικά δύσκολη και οφείλεται στο πόσο ανοικτό είναι το Ethereum,. Μπορεί να οδηγήσει σε πιθανές απειλές ψευδώνυμων χρηστών που μπορούν να χρησιμοποιήσουν απειλητικά προγράμματα για να επιτεθούν εάν ο

κώδικας συμβάσεων είναι ευάλωτος ή κακώς γραμμένος. Οι Bhargavan & Delignat-Lavaud (2016) δήλωσαν: Πριν από λίγα χρόνια, μια επίθεση συνέβη και αποδείχθηκε ότι επιτέθηκε στη σύμβαση DAO και έχει εκμεταλλευτεί ευαίσθητες λεπτομέρειες της Εικονικής Μηχανής Ethereum, η οποία επέτρεψε στον χρήστη να μεταφέρει περίπου $ 50 εκατομμύρια αξίας Ether.

Με την Ethereum να εκτελεί έξυπνα συμβόλαια που χειρίζονται εκατομμύρια λίρες, είναι σημαντικό να διατηρούνται οι συναλλαγές ασφαλείς. Παρόμοια με το Bitcoin, το μητρώο θα διατηρεί τα αρχεία συναλλαγών αυτού του εικονικού νομίσματος και για να δημιουργήσει αυτό το νόμισμα γίνεται μια διαδικασία που ονομάζεται «εξόρυξη». Κάθε κόμβος αυτού του δικτύου μπορεί να συνδεθεί στο επόμενο μπλοκ συναλλαγών του μητρώου εντοπίζοντας την τιμή κατακερματισμού. Αυτό διασφαλίζει ότι τα μπλοκ εξορύσσονται με σταθερό ρυθμό. Επιστρέφοντας στο Ethereum, μοιάζει πολύ με το Bitcoin, το μητρώο του Ether αποθηκεύει το συμβόλαιο με τη μορφή της Εικονικής Μηχανής Ethereum και επιτρέπει συναλλαγές ως λειτουργία καλείται στον κώδικα όπως φαίνεται στο Σχήμα 8.



Διάγραμμα 8 : Κατανεμημένο Δίκτυο Ethereum (Bhargavan & Delignat-Lavaud, 2016)

1.10 Έξυπνα Συμβόλαιο και Επιθέσεις

Όσο ασφαλή τα έξυπνα συμβόλαιο μπορεί να είναι ,πάντα θα υπάρχει κάποιο είδος ευπάθειας. Οι περισσότερες επιθέσεις στο Blockchain στοχεύουν κρυπτονομίσματα προκειμένου να κλέψουν χρήματα από κακώς γραμμένα συμβόλαια.Οι τρεις κοινές επιθέσεις σε έξυπνα συμβόλαια είναι

- Αμετάβλητα σφάλματα,
- Απώλεια Ether κατά τη μεταφορά

Με το έξυπνο συμβόλαιο δεν υπάρχει επιστροφή μετά τη δημοσίευση του έξυπνου συμβολαίου στο Blockchain. Το συμβόλαιο δεν μπορεί να αλλάξει μετά τη δημοσίευσή του. Εδώ έρχεται το παιχνίδι εμπιστοσύνης των χρηστών, καθώς δεν υπάρχει τρόπος αλλαγής των συμβάσεων, εάν υπάρχει είναι ένα σφάλμα μέσα στη σύμβαση, δεν υπάρχει τρόπος να το διορθώσουμε, τότε το συμβόλαιο πρέπει να τερματιστεί. Όταν τερματιστεί το συμβόλαιο, η συναλλαγή αποσύρεται και ένα νέο συμβόλαιο έχει ξεκινήσει. Εάν το σφάλμα έχει παραβιαστεί και εκμεταλλευτεί για να κλέψει τον Ether, τότε δεν μπορεί να εξαργυρωθεί από τον χρήστη και δεν υπάρχει δυνατότητα ανάκτησης αυτού που έχει χάσει ο χρήστης. (Atzei, Bartolett & Cimoli, 2017)

Κατά την αποστολή του Ether, ένα από τα μέλη του κόμματος πρέπει να καθορίσει τη διεύθυνση παραλήπτη και ορισμένες από τις διευθύνσεις δεν σχετίζονται με κανέναν χρήστη στην αλυσίδα ή στη σύμβαση. Εάν σύμφωνα με το Ether αποστέλλεται σε μία από τις διευθύνσεις που δεν έχουν συσχετιστεί με τη σύμβαση ή τον χρήστη, θα χαθεί για πάντα, δεν υπάρχει επίσης τρόπος ανίχνευσης της διεύθυνσης του χρήστη ή της σύμβασης. (Atzei, Bartolett & Cimoli, 2017)

1.11 Τρέχουσα Πρόληψη Επιθέσεων

Προκειμένου να αποφευχθούν ορισμένες από τις επιθέσεις που υπάρχουν πρέπει να ληφθούν βασικά ζητήματα κατά την προσπάθεια εφαρμογής των μεθόδων πρόληψης. Θα υπάρχουν πολλοί παράγοντες που θα παίξουν σημαντικό ρόλο. Έτσι κατά τη δημιουργία έξυπνων συμβολαίων οι προγραμματιστές πρέπει να είναι πολύ προσεκτικοί κατά τη δημιουργία ενός συμβολαίου. Οι χάκερ θα προσπαθήσουν να βρουν σφάλματα ή να δημιουργήσουν τα δικά τους προγράμματα που θα προσπαθήσουν να σπάσουν τη σύμβαση κάποιου. Επομένως, πρέπει να τεθούν σε εφαρμογή συστήματα πρόληψης και να ληφθούν υπόψη διάφορες επιθέσεις που ενδέχεται να εμπλέκονται κατά την απελευθέρωση νέων έξυπνων συμβάσεων, έτσι ώστε κανένα από αυτά να μην συμβεί ποτέ.

Μερικοί από τους βασικούς παράγοντες που παίζουν ρόλο έχουν τεράστια αποτελεσματικότητα ενάντια στην επίθεση. Αυτοί οι τρεις παράγοντες επιτρέπουν την ανίχνευση επίθεσης hopping και αποτρέπουν την επανάληψη της ίδιας επίθεσης. Όπως ο Singh (2019) παρέχει αυτές τις λεπτομέρειες:

Ισχύς υπολογιστή: Οι ανθρακωρύχοι(miners) χρειάζονται μεγάλη ισχύ για να μπλοκάρουν με επιτυχία ένα ορυχείο. Προκειμένου να αυξηθεί η πιθανότητα ενός επιτυχημένου ορυχείου, το μέρος με την υψηλότερη δύναμη υπολογισμού θα δημιουργήσει πρώτα περισσότερα νομίσματα ή θα λύσει κρυπτογραφικά παζλ, επομένως η απώλεια υπολογιστικής ισχύος θα απειλούσε τον στόχο της δημιουργίας περισσότερων νομισμάτων ή επίλυσης παζλ.

Κίνδυνος ανθρακωρύχων(miners): Βεβαιωθείτε ότι όταν ένας νέος ανθρακωρύχος(miners) ενταχθεί στην ομάδα, η επίθεση δεν τους επηρεάζει. Οπότε για να σταματήσει αυτό να συμβαίνει, θα υπάρξει μία εγγραφή με το πόσες φορές ένας ανθρακωρύχος((miners) εγκατέλειψε και

επέστρεψε,με τους όρους που θα τους εμποδίσουν να φύγουν. Αυτό θα εμποδίσει τους εισβολείς να ενταχθούν τυχαία για να έχουν την ευκαιρία να διακόψουν το δίκτυο εξόρυξης.

Το έξυπνο συμβόλαιο θα πρέπει να εφαρμόσει έναν τρόπο για να κάνει την είσοδο του ανθρακωρύχου((miners) στην ομάδα και στη συνέχεια να έχει κάποιον να διαχειριστεί τα αιτήματα και να συνδέσει τον ανθρακωρύχο(miners) με τη διεύθυνση αποκλεισμού, έτσι ώστε ο διαχειριστής να λάβει το πιστοποιητικό από το δίκτυο Blockchain, ώστε ο διαχειριστής να είναι είναι σε θέση να εντοπίσει τον ανθρακωρύχο(miners) και σε αυτήν την περίπτωση, εάν ο ανθρακωρύχος(miners) έχει πάει σε ομάδες, θα αναγκαστούν να υποβάλουν τα νομίσματά τους στον διαχειριστή.

1.12 Προκλήσεις να ξεπεραστούν

Υπάρχουν πολλές προκλήσεις που πρέπει να ξεπεραστούν στον τομέα του Blockchain. Είναι σημαντικό να θυμόμαστε και να δημιουργούμε το ασφαλέστερο δυνατό περιβάλλον για τους ανθρώπους και να ξεπερνάμε τα πιο κοινά λάθη. Αυτά τα λάθη θα μπορούσαν να δημιουργηθούν λανθασμένα συμβόλαια που θα αφήσουν τους χρήστες / μέλη ευάλωτους στο δίκτυο ή θα επιτρέψουν στα μέλη να έχουν πρόσβαση σε περιορισμένες περιοχές στις οποίες δεν θα έπρεπε να έχουν πρόσβαση. Θα υπάρξουν πολλά ευαίσθητα δεδομένα που υποβάλλονται σε επεξεργασία, όπως λεπτομέρειες βιβλίων, ονόματα συγγραφέων και βιβλίο ISBN (International Standard Book Number), καθώς για τους χρήστες που πρόκειται να εγγραφούν για να αγοράσουν τα βιβλία που επιθυμούν, θα μοιραστούν προσωπικά δεδομένα. Το λογισμικό πρέπει να εφαρμοστεί για δοκιμές,. Σήμερα τα δεδομένα καταλαμβάνουν όλο και περισσότερο χώρο στον οποίο θα πρέπει να ληφθεί υπόψη η αποθήκευση. Το cloud computing θα είναι ένα πρόβλημα κατά την ανάπτυξη μιας

δοκιμαστικής εφαρμογής. Μπορεί να αποτρέψει την ανάκτηση πληροφοριών όταν διακοπεί ή χαθεί η σύνδεση. Ο νόμος προστασίας δεδομένων θα ληφθεί υπόψη.

Αυτές οι προκλήσεις πρόκειται να αντιμετωπιστούν κατά τη δημιουργία ενός εργασιακού περιβάλλοντος για τις δοκιμές.

1.13 Τρέχουσες Τεχνολογίες σε Ψηφιακές Βιβλιοθήκες

Οι ψηφιακές βιβλιοθήκες άρχισαν να αυξάνονται στην Αμερική στις αρχές της δεκαετίας του '90. Η αμερικανική κυβέρνηση άρχισε να χρηματοδοτεί το πρόγραμμα καθώς επίσης να παρέχει νομοθεσία και μια σειρά από πρωτοβουλίες χρηματοδότησης ξεκίνησαν το 1993 με την ψηφιακή βιβλιοθήκη ως εξέχον θέμα και ειδικά περιοδικά άρχισαν να εμφανίζουν άρθρα. Η κυβέρνηση των ΗΠΑ άρχισε να φέρνει επανάσταση στον τρόπο λειτουργίας των τυπικών βιβλιοθηκών. Ένα χρόνο αργότερα υπήρχαν συχνές συνομιλίες, εργαστήρια και συνέδρια για αυτό το νέο σύστημα βιβλιοθηκών που ονομάζουμε τώρα «Ψηφιακές βιβλιοθήκες». Αν φέρει αυτή την τεχνολογική πρόοδο, θα επωφεληθεί από την καταστροφή των αμαζόνων με την κοπή δέντρων που χρειάζονται χαρτί, η επανάσταση έχει αρχίσει να πηγαίνει «Πέρα από το χαρτί». (Fox, Akscyn, Furuta & Leggett, 1995).

Η αμερικανική κυβέρνηση ονόμασε το πρόγραμμα DLI-1. Αυτή η έρευνα και ανάπτυξη χρηματοδοτήθηκε από κοινού το Εθνικό Ίδρυμα Επιστημών (NSF), την Υπηρεσία Προχωρημένων Έργων Άμυνας και την Εθνική Διοίκηση Αεροναυτικής και Διαστήματος (NASA). Ως αρχικός υποστηρικτής του προγράμματος, το πρόγραμμα υπολογιστών και επικοινωνιών υψηλής απόδοσης (HPCC) της κυβέρνησης των ΗΠΑ, τα έργα DLI-1 έλαβαν αρχικά ένα ποσό 24 εκατομμυρίων δολαρίων για τέσσερα χρόνια. Το 1998 η κυβέρνηση ξεκίνησε

ένα νέο πρόγραμμα που το αποκαλούσε DLI-2 με την υποστήριξη των NSF, DARPA και NASA, αλλά αυτή τη φορά η Εθνική Βιβλιοθήκη Ιατρικής (NLM), η Βιβλιοθήκη του Κογκρέσου (LC), η Εθνική Κληρονομιά για τις Ανθρωπιστικές Επιστήμες (NEH)) και το Ομοσπονδιακό Γραφείο Ερευνών (FBI) συνεργάστηκαν για να βοηθήσουν με το ανανεωμένο έργο και μέσα στα επόμενα 5 χρόνια κατάφεραν να λάβουν χρήματα 68 εκατομμυρίων δολαρίων. (Andrews & Law, 2017)

Η τεχνολογία επηρεάζει όλες τις πτυχές της ανθρώπινης φύσης, αλλάζει τον τρόπο με τον οποίο παρεμβαίνουμε και συμπεριφερόμαστε με τις πτυχές των παραδοσιακών βιβλιοθηκών.

Ορισμένες ψηφιακές βιβλιοθήκες επιτρέπουν την πρόσβαση δωρεάν περιεχομένου από το κοινό και πληρώνουν για ορισμένα προϊόντα, συλλογές και άλλες διαθέσιμες υπηρεσίες εκδοτών. Τα μακροπρόθεσμα μελλοντικά βιβλία, όπως η συλλογή εγκυκλοπαίδειας, θα εμφανίζονται δωρεάν για το κοινό, το κόστος δημιουργίας και διανομής ψηφιακών βιβλίων βαρύνει τον εκδότη.

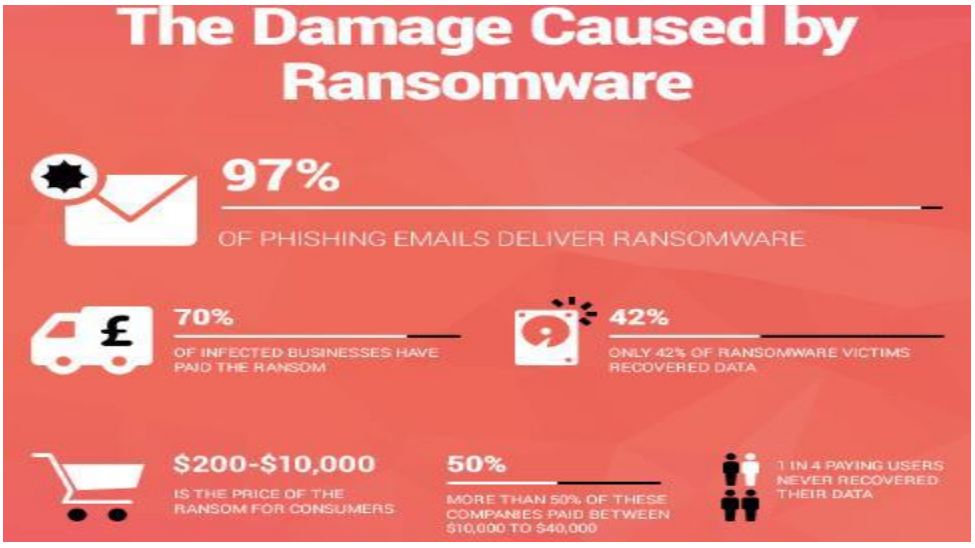
Κάποιοι θα έλεγαν «Γιατί οι ψηφιακές βιβλιοθήκες» καθώς αυτή η τεχνολογία θα καταστρέψει τις συμβατικές βιβλιοθήκες στις οποίες έχουμε συνηθίσει, και οι βασικές αρχές θα χαθούν. Το κλείσιμο των βιβλιοθηκών δεν θα γίνει καθώς θα υπάρχουν πάντα λάτρεις των συμβατικών παραδόσεων που θα κρατήσουν τις βιβλιοθήκες ανοιχτές, αλλά το κλείσιμο στις περισσότερες θα είναι αναπόφευκτο. Οι ψηφιακές βιβλιοθήκες είχαν εισαχθεί με τον κινούμενο ψηφιακό κόσμο στον οποίο οι περισσότεροι άνθρωποι έχουν ήδη συγκλίνει, καθώς οι άνθρωποι έχουν αλλάξει τον τρόπο που επικοινωνούν και ζουν. Η ζωή σε έναν ψηφιακό κόσμο επιτρέπει ταχύτερη επικοινωνία και μεταφορά πληροφοριών. Κάποιοι θα υποστήριζαν ότι το να μείνετε μακριά από μια οθόνη υπολογιστή και να διαβάσετε ένα πραγματικό βιβλίο είναι καλύτερο, καθώς θα αυξήσει τις δεξιότητές τους στην επικοινωνία και τις κοινωνικές δεξιότητες, καθώς και θα είναι έξω στο κοινό στις βιβλιοθήκες, όπως είπε ο συγγραφέας των New York Times: Khullar (2020) «Η κοινωνική απομόνωση είναι μια αυξανόμενη επιδημία - μια που αναγνωρίζεται όλο και περισσότερο ότι έχει τρομερές σωματικές, ψυχικές και συναισθηματικές συνέπειες», στην οποία είναι αλήθεια ότι το

να κάθεται μπροστά σε μια οθόνη υπολογιστή θα αποτρέψει έναν χρήστη από το να είναι κοινωνικά ικανός στον πραγματικό κόσμο όταν πρόκειται στην επικοινωνία με άλλους ανθρώπους. Η συλλογή πληροφοριών από τον προσωπικό σας υπολογιστή μέσα σε λίγα λεπτά επιτρέπει την ταχύτερη συλλογή πληροφοριών, αντί να περπατάτε στην πλησιέστερη βιβλιοθήκη ή να περπατάτε σε μια βιβλιοθήκη πανεπιστημίου και να χρειάζεται να αφιερώσετε ελεύθερο χρόνο για να αναζητήσετε ένα βιβλίο που έχει μεγάλη πιθανότητα να είναι παρωχημένο και άσχετο

Η θετικότητα που φέρνουν οι ψηφιακές βιβλιοθήκες είναι η μείωση του χαρτιού, που σημαίνει ότι υπάρχουν λιγότερα δέντρα που πρέπει να κοπούν για τη δημιουργία χαρτιού. Η εύρεση πληροφοριών σε χαρτί είναι μάλλον δύσκολη όταν η αναζήτηση πληροφοριών στο διαδίκτυο μπορεί κυριολεκτικά να διαρκέσει λεπτά, αν όχι δευτερόλεπτα, ενώ η προσπάθεια ανάκτησης πληροφοριών σε ένα βιβλίο μπορεί να διαρκέσει λεπτά, αν όχι ώρες. Υπάρχουν περισσότερες μέθοδοι για ψηφιακή αναζήτηση πληροφοριών καθώς και για ευκολότερη αναφορά κατά την προμήθεια πληροφοριών στο διαδίκτυο. Επιτρέποντας και διατηρώντας τις πληροφορίες ηλεκτρονικά, ο καθένας μπορεί να μοιράζεται αυτές τις πληροφορίες ο ένας με τον άλλο, η διαχείριση της αντιγραφής καθώς και η αντιγραφή των πληροφοριών σε ένα δίκτυο μεταξύ βιβλιοθηκών επιτρέπει την ταχύτερη ανταλλαγή πληροφοριών. Οι πληροφορίες που υπάρχουν ήδη ενδέχεται να χρειαστεί να ενημερωθούν, πρέπει να ενημερωθούν τα βιβλία που θα χρειαστεί για τους εκδότες να κυκλοφορήσουν μια νέα έκδοση, αυτό απαιτεί χρόνο για να εξαπλωθούν οι πληροφορίες και η διαδικασία δημιουργίας βιβλίων από μόνη της είναι χρονοβόρα, εδώ είναι Οι πληροφορίες που διατηρούνται ψηφιακά επιτρέπουν την ενημέρωση υλικού σχεδόν αμέσως, επιτρέποντας στις ψηφιακές βιβλιοθήκες να αφαιρούν ή να διατηρούν ένα αντίγραφο της προηγούμενης έκδοσης, δημιουργώντας ένα μικρότερο πρόβλημα για τη διάδοση των ενημερωμένων πληροφοριών σε χρήστες σε όλο τον κόσμο. Έχοντας αποθηκεύσει βιβλία σε ψηφιακή μορφή σημαίνει ότι δεν υπάρχει πιθανότητα κλοπής βιβλίων που εξοικονομεί χρήματα. Οι πληροφορίες είναι πάντα διαθέσιμες όσο ο υπολογιστής του χρήστη λειτουργεί.

1.14 Πρόσφατες Επιθέσεις σε Ψηφιακές Βιβλιοθήκες

Τα τελευταία χρόνια υπήρξαν επιθέσεις σε ψηφιακές βιβλιοθήκες. Αυτό δείχνει ότι ακόμη και σε αυτήν την εποχή είναι ευάλωτες και υπάρχει ενδιαφέρον να επιτεθούν σε αυτές τις εγκαταστάσεις, καθώς οι χάκερ μπορούν να χρησιμοποιήσουν τις πλατφόρμες τους για να κλέψουν χρήματα από τους. χρήστες. Σε μια από τις περιστάσεις σε μια επίθεση των ΗΠΑ στη βιβλιοθήκη του Σαιντ Λούις, η ψηφιακή βιβλιοθήκη σταμάτησε. Οι εισβολείς μολύνουν τη βιβλιοθήκη με έναν ιό υπολογιστή ransomware, ο συγκεκριμένος ιός που έχει χρησιμοποιηθεί για να αποσπάσει χρήματα από τα θύματα, με την ευκαιρία αυτή οι επιτιθέμενοι είχαν ζητήσει 28.000 £ για να αποκαταστήσουν τα συστήματα της βιβλιοθήκης που επηρέασαν 16 καταστήματα στο αναφέρω. Οι επιτιθέμενοι ζήτησαν χρήματα σε ηλεκτρονικό νόμισμα, «Bitcoin». Η βιβλιοθήκη αρνήθηκε να πληρώσει τους επιτιθέμενους προκειμένου να ανακτήσουν και να λειτουργήσουν τα συστήματά τους. (Kean, 2017)



Διάγραμμα 9: Προκληθείσα Ζημιά από κατηγορία ιών Ransomware (Kean, 2017)

Η βιβλιοθήκη ανέφερε ότι πρόκειται να εκκαθαρίσει ολόκληρα τα συστήματά τους και να ξαναχτίσει ολόκληρο το οικοσύστημα από το μηδέν. Αυτό το είδος λύσης κράτησε τη βιβλιοθήκη σε ακινησία για μερικές εβδομάδες. (Kean, 2017)

1.15 Τεχνητή Νοημοσύνη και Ψηφιακές Βιβλιοθήκες

Η χρήση τεχνητής νοημοσύνης σε ψηφιακές βιβλιοθήκες μπορεί να παρέχει αυτόνομες παραπομπές, επιτρέποντας ταχύτερες αναζητήσεις καθώς και ευρετηρίαση. Καθώς μια από τις εταιρείες «CiteSteerX» έχει αναπτύξει μια μηχανή αναζήτησης όπως έχουν δηλώσει: (Wu et al., 2015) «Το CiteSeerX είναι μοναδική σε σύγκριση με άλλες επιστημονικές ψηφιακές βιβλιοθήκες και μηχανές αναζήτησης. Είναι μια ψηφιακή βιβλιοθήκη ανοιχτής πρόσβασης, επειδή όλα τα έγγραφα συλλέγονται από τον δημόσιο ιστό. "

1.16 Επίλογος

Όπως φαίνεται από τη βιβλιογραφική ανασκόπηση των Hyperledger, Blockchain έξυπνων συμβολαίων υπάρχει υψηλότερο επίπεδο ασφάλειας. Υπάρχουν μειωμένοι κίνδυνοι λόγω της πολυπλοκότητας που δημιουργείται κατά τη δημιουργία έξυπνων συμβολαίων στο Blockchain και ως εκ τούτου είναι ένα καλύτερο σύστημα για ψηφιακές βιβλιοθήκες. Ο συνθέτης Hyperledger επέτρεψε τη δημιουργία της δοκιμαστικής βάσης που θα ακολουθήσει στο επόμενο κεφάλαιο όπου θα εμβαθύνουμε στην πειραματική φάση, στην οποία θα παράγουμε αποτελέσματα για να μπορέσουμε να αξιολογήσουμε το θέμα με το οποίο καταπιάνεται η παρούσα διπλωματική εργασία.

ΚΕΦΑΛΑΙΟ 2 : Μεθοδολογία

2.1 Εισαγωγή

Σε αυτό το κεφάλαιο παρουσιάζεται ο σχεδιασμός του εγχειρήματος, με στόχο την ανάδειξη των λειτουργιών των έξυπνων συμβολαίων, πώς λειτουργούν και πως αναπτύσσονται.

Τα ευρήματα από την μελέτη της βιβλιογραφίας είναι τεχνικής φύσης, χωρίς αποδείξεις και χωρίς υλοποίηση. Παρ' όλα αυτά, κατά τη διάρκεια αυτού του σταδίου θα υπάρξει μια πλήρης εξήγηση για το εγχείρημα και η υπόθεση θα προκαλέσει τα δεδομένα που χρησιμοποιούνται για να δείξουν τις ενέργειες καθώς και την συμπεριφορά του συμβολαίου.

Η επεκτασιμότητα του testbed επιτρέπει να δημιουργηθούν και να εξεταστούν περισσότερα από ένα συμβόλαια έτσι ώστε να παραχθούν τα τελικά αποτελέσματα.

΄Οσο περισσότερα συμβόλαια επιτρέπεται να δουλεύουν τόσο περισσότεροι τρόποι υπάρχουν για να εξεταστούν. Στην περίπτωση όπου μελετάται, αυτό είναι επωφελές, αφού χρειάζεται να γίνουν αρκετές δοκιμές, έτσι ώστε το εγχείρημα να είναι απολύτως λειτουργικό. Η αξιοπιστία αυτού του testbed για την μεθοδολογία θα παράσχει ουσιώδη αποτελέσματα αφού το testbed θα είναι ικανό να χειριστεί το εγχείρημα.

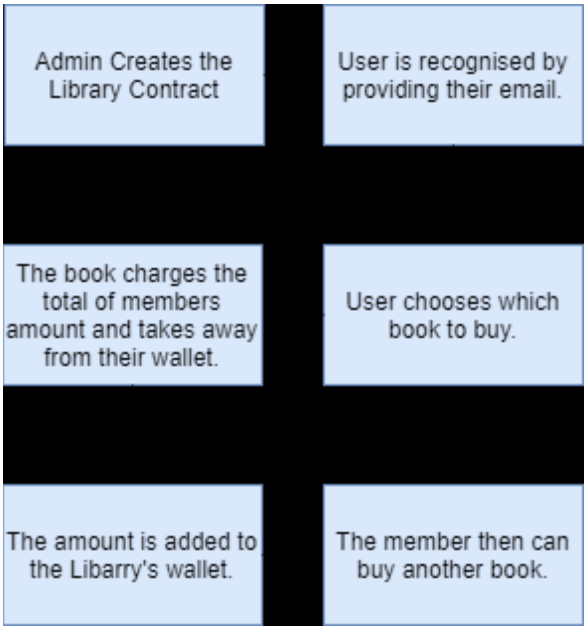
2.2. Σχεδιασμός Μεθοδολογίας

Η αρχική κατασκευή του εγχειρήματος επιτρέπει στον χρήστη να προσθέσει την διεύθυνση ηλεκτρονικού ταχυδρομείου του, αυτό επιτρέπει στον διαχειριστή να αναγνωρίζει ποιός χρήστης

αγόρασε ποιό βιβλίο. Αυτό κάνει πολύ ευκολότερη την αναγνώριση και την ιχνηλάτηση των συναλλαγών των χρηστών χρησιμοποιώντας την διεύθυνση ηλεκτρονικού ταχυδρομείου τους.

Από τον χρήστη επίσης ζητείται να επικυρώσει το μικρό του όνομα καθώς και το επώνυμο του. Στη συνέχεια το μέλος επιλέγει το ποσό των χρημάτων που επιθυμεί να μεταφέρει από το πορτοφόλι του στον λογαριασμό του. Η βιβλιοθήκη έχει ένα θεσπισμένο υπόλοιπο, το οποίο ανανεώνεται όποτε πραγματοποιείται η αγορά ενός βιβλίου, η τιμή αυτού του βιβλίου στη συνέχεια προστίθεται στηο υπόλοιπο της βιβλιοθήκης και το υπόλοιπο του μέλους ελλατώνεται.

Στη συνέχεια η συναλλαγή προστίθεται στο δίκτυο με τις υπόλοιπες συναλλαγές. Μέσα από την συναλλαγή ο διαχειριστής έχει την δυνατότητα να δει τον αριθμό συναλλαγής της του συμβολαίου, την ταυτότητα συναλλαγής καθώς και μια χρονοσήμανση (timestamp).

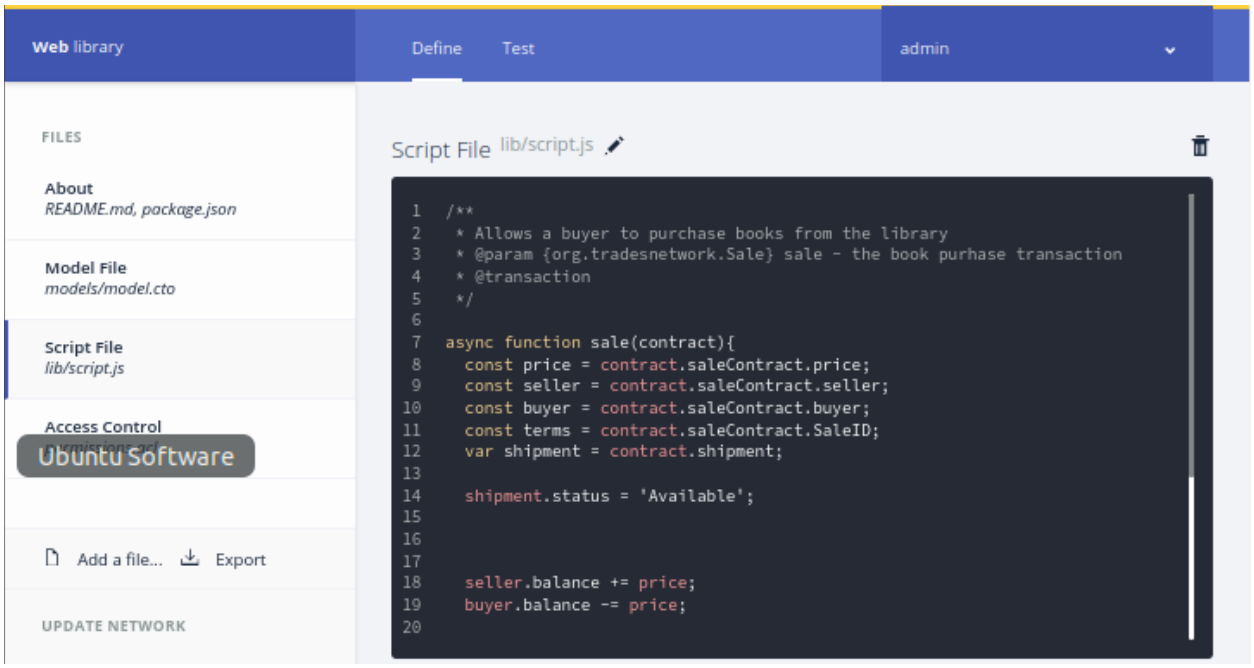


Διάγραμμα 10: Λογική Εφαρμογής

2.3 Testbed

Το testbed που χρησιμοποιήθηκε επέτρεψε να ακολουθηθούν κάποια απλά βήματα ώστε να πραγματοποιηθει η δημιουργία απαραίτητων συμβολαίων, όπως και μια Γραφική Οιεπαφή Χρήστη (GUI) για εύκολη δοκιμή μετά την παράταξη (deployment) αυτών των συμβολαίων.

Το Hyperledger Composer είναι ένα πλάισιο λογισμικού (Software Framework), και ένας πολύ καλός τρόπος για τη δημιουργία πληθώρας εφαρμογών και έξυπνων συμβολαίων. Το εργαλείο αυτό επέτρεψε τη δημιουργία του εταιρικού δικτύου χρησιμοποιώντας συναλλαγές σεναρίων (script transactions).

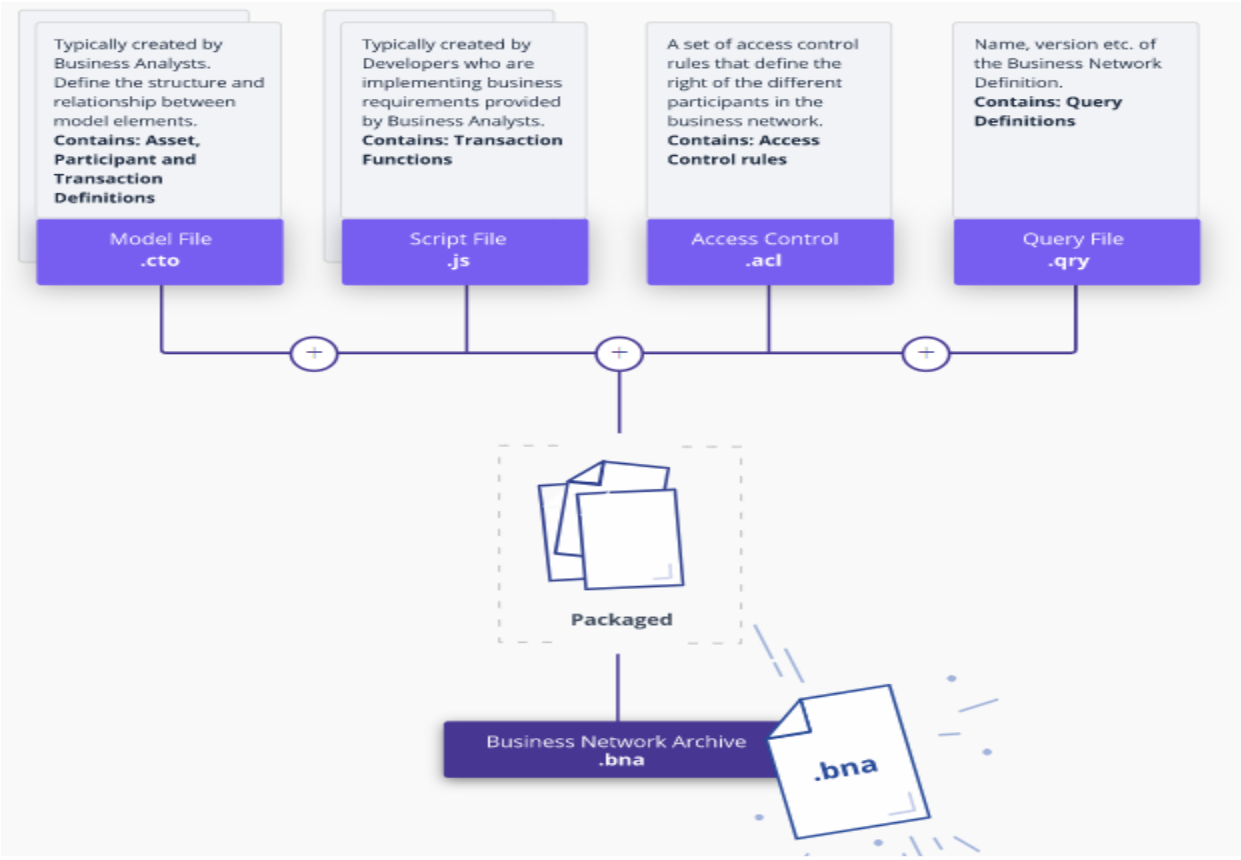


Διάγραμμα 11: Κώδικας composer Playground μητρώου

Τα συμβόλαια αυτά είναι εύκολο να ακολουθηθούν και επιτρέπουν στον διαχειριστή την προσθέση και τη διαχείρηση των μελών επεξεργάζοντας τα ή αφαιρώντας τα από το δίκτυο.

Κάθε βιβλίο έχει την δική του ταυτότητα (ID) και μπορεί να αναγνωριστεί από τον συγγραφέα ή από τον τίτλο του βιβλίου.

Στην παρακάτω εικόνα εξηγείται η λειτουργία του composer playground. Κάθε επίπεδο (layer) έχει τις δικές του τιμές μέσα σε αυτό το δίκτυο. Αυτό επιτρέπει σε αρχάριους χρήστες να αντιληφθούν ευκολότερα την συνολική λειτουργία του πρόγραμματος.



Διάγραμμα 12: Επεξήγηση composer Playground (SHARMA, 2019)

2.4 Συμπεράσματα

Η φόρτωση αυτών των συμβολαίων σε αυτό το δίκτυο και η μετατροπή αυτών σε συναλλαγές, επέτρεψε στους χρήστες να γίνουν μέλη παρέχοντας στοιχεία όπως το όνομα, το επώνυμο τους και την διεύθυνση ηλεκτρονικού ταχυδρομείου τους. Αυτή η διεύθυνση ηλεκτρονικού ταχυδρομείου στη συνέχεια χρησιμοποιείται ως η ταυτότητα τους.

Για παράδειγμα αν υπήρχε κάποιο πρόβλημα, θα ήταν ευκολότερο να αναγνωριστεί ένα μέλος από την διεύθυνση ηλεκτρονικού ταχυδρομείου του αντί για τον αριθμό συναλλαγής ο οποίος θα μπορούσε να είναι οποιοσδήποτε στο διάστημα 0000 – 9999 βραχυπρόθεσμα. Επι πλέον, επαναληπτικές μεθοδολογίες όπως αυτή του Hyperledger Composer επιτρέπουν την αλλαγή του σχεδιασμού στη φάση της υλοποίησης. Αυτό είναι αρκετά πιθανό να γίνει λόγω των αλλαγών και των δοκιμών στο συμβόλαιο όταν γίνεται παράταξη (delploying) και δοκιμή διαφορετικών μεθόδων.

Στο επόμενο κεφάλαιο παρουσιάζεται η υλοποίηση μαζί με τα αποτελέσματα στο τέλος, ενώ έπονται η αξιολόγηση και η έκβαση του παρόντος εγχειρήματος.

ΚΕΦΑΛΑΙΟ 3 : Υλοποίηση

3.1 Εισαγωγή

Σε αυτό το κεφάλαιο θα υλοποιηθεί και θα περιγραφεί η μεθοδολογία, κάνοντας χρήση εικόνων όπου περιέχονται αποσπάσματα των αρχείων σεναρίου (script), ελέγχου πρόσβασης, μοντέλων και δοκιμών. Επομένως, ο εξαγόμενος κώδικας από το σενάριο θα υλοποιηθεί στο Hyperledger Composer, και στο τέλος τα παραχθέντα αποτελέσματα του εγχειρήματος θα παρουσιαστούν και θα συνοψιστούν πριν γίνει μετάβαση στην εκτίμηση όλων των αποτελεσμάτων στο επόμενο κεφάλαιο.

Το εγχείρημα είναι σχεδιασμένο χρησιμοποιώντας το Hyperledger Composer μέσα στο οποίο θα επιτραπεί ο έλεγχος και η παράταξη (deployment) του πειράματος. Το στάδιο της υλοποίησης θα εξηγηθεί βήμα προς βήμα έτσι ώστε να είναι ευκολότερη η εξήγηση και η ανάπτυξη του. Τα συμβόλαια θα εκτελούνται από το testbed το οποίο έχει τα σενάρια (scripts) κωδικοποιημένα στο δίκτυο του

3.2 Παραμετροποίηση του Hyperledger Composer

Για να αρχίσει να εκτελείται το testbed, τα πρώτα bits πρέπει να φορτωθούν έτσι ώστε να ξεκινήσει να εκτελείται ο composer.

Αρχικά, ο composer δεν εκτελούνταν στο περιβάλλον του λειτουργικού συστήματος Windows , οπότε χρησιμοποιήθηκε το Ubuntu.

Κάνοντας χρήση του τερματικού, το πρώτο βημα ήταν να καταφορτωθεί το Docker. Το Docker είναι ένα εργαλείο το οποίο διευκολύνει τη δημιουργία, την παράταξη, καθώς και την εκτέλεση εφαρμογών χρησιμοποιώντας κιβώτια (containers). Οι βιβλιοθήκες και οι προαπαιτήσεις σε ένα μόνο πακέτο.

Στη συνέχεια έγινε εγκατάσταση του Hyperledger Composer και των πακέτων του. Για να πραγματοποιηθεί επιτυχημένα η εγκατάσταση του, υπάρχει μια διαδικασία και χρειάζονται εντολές στο τερματικό, έτσι ώστε να γίνει πλήρης εγκατάσταση των πακέτων και του composer.

Η εντολή “docker run” θα τρέξει τον composer στην πόρτα 8080, τοπικά. Ο composer επιτρέπει την τοπική εκτέλεση συμβολαίων.

Virtual Box : ˜$ docker run − name composer−playground − publ i s h 8080 hype r l e dg e r / composer−playground

Μετά την αντιστοίχιση του composer σε μια πόρτα, το επόμενο βήμα είναι η εγκατάσταση του μονοπατιού (path), όπως φαίνεται στην παρακάτω εικόνα το μονοπάτι το οποίο επιλέχτηκε για το παρόν εγχείρημα στην εικονική μηχανή με λειτουργικό σύστημα Ubuntu.

/tmp$ sudo mv go / usr / l o c a l
/tmp$ export GOROOT=/u sr / l o c a l / go
/tmp$ export GOPATH=$HOME/ go
/tmp$ export PATH=$GOPATH/ bin :$GOROOT/ bin :$PATH

Μόλις ολοκληρωθεί η εγκατάσταση της τοποθεσίας, το επόμενο βήμα είναι να γίνει επανεκίνηση του προφίλ. Αυτό θα αποδείξει ότι το προφίλ δουλεύει και ότι είναι έγκυρο.

/tmp$ sudo mv go / usr / l o c a l
/tmp$ export GOROOT=/u sr / l o c a l / go
/tmp$ export GOPATH=$HOME/ go
/tmp$ export PATH=$GOPATH/ bin :$GOROOT/ bin :$PATH
/tmp$ v i ~/. p r o f i l e
/tmp$ su – nkala

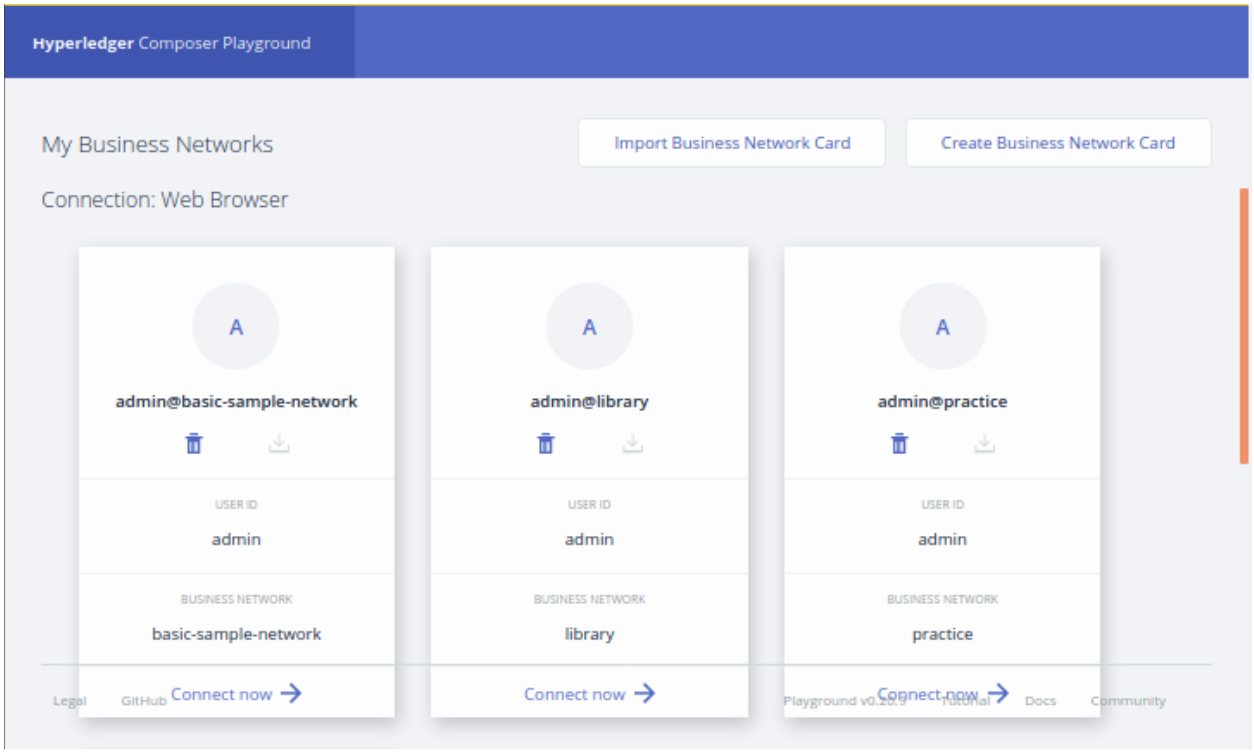
Αφού έγινε έλεγχος και βεβαιώθηκε ότι το προφίλ δουλεύει, η επόμενη διαδικασία είναι η εγκατάσταση του node.js όπως και του npm.

/tmp$ c u r l −o− https : // raw. githubusercontent. Com / c r e a t i o n i x /nvm/ v0 . 3 3 . 1 1 / i n s t a l l . sh | bash

Το Node.js είναι μια πλατφόρμα ανοιχτού κώδικα η οποία επιτρέπει στην JavaScript να εκτελείται σε έναν περιηγητή διαδικτύου.
Ο npm είναι ο προκαθορισμένος διαχειριστής πακέτων του Node.js. Αποτελείται από μια διεπαφή γραμμής εντολών (CLI) και μια online βάση δεδομένων των πακετών η οποία αποκαλείται “npm registry”.
Το τελευταίο βήμα είναι η εκτέλεση του composer μέσα από το τερματικό, εφόσον η εγκατάσταση ήταν επιτυχής, ο Mozilla Firefox θα ανοίξει τοπικά με την διεπαφή του composer.

: ~/ f ab r i c −samples / basic −network$ composer−playground

Παρακάτω απεικονίζεται η κύρια διεπαφή μετά την επιτυχή εγκατάσταση του Hyperledger composer-playground.



Διάγραμμα 13: Διεπαφή Χρήστη στο Playground

3.3 Δημιουργία Αρχείου Μοντέλου

Το αρχείο μοντέλου είναι μια γλώσσα μοντελοποίησης η οποία καθορίζει το όλο σχεδιασμό του σχεδιασμού των έξυπνων συμβολαίων, του πορτοφολιού και πως θα λειτουργεί το εγχείρημα.

```
namespace org.tradesnetwork

asset Book identified by BookId {
  o String BookId
  o String BookNumber
  o Double Quantity
  o BookAuthor bookauthor
}

enum BookAuthor {
  o Ann_Frank
  o Jacquiline_Wilson
}

abstract participant BuyerID identified by email {
  o String email
}
```

Διάγραμμα 14: Αρχείο Μοντέλο μέρος 1ο

Το asset “Book” θα ταυτοποιείται από το BookId , μέσα στον κώδικα του περιέχονται αλφαριθμητικά τα οποία επιτρέπουν την εισαγωγή του Συγγραφέα, Αριθμού βιβλίου και της ποσότητας.

Το “Enum” επιτρέπει στο μέλος να την επιλογή του βιβλίου που επιθυμεί. Στο παρόν εγχείρημα υπάρχει μια γρήγορη επιλογή δύο διαφορετικών συγγραφέων μέχρι αυτή τη στιγμή.

Το μέλος θα ταυτοποιείται μέσω της διεύθυνσης ηλεκτρονικού ταχυδρομείου του αντί του ID της συναλλαγής.

Υπάρχουν δύο συμμετέχοντες σε αυτό το μοντέλο, ο αγοραστής είναι το μέλος (μπορούν να υπάρχουν παραπάνω από ένα μέλη). Η ταυτοποίηση θα γίνεται μέσω της διεύθυνσης ηλεκτρονικού ταχυδρομείου όπως προαναφέρθηκε.

```
participant Buyer identified by BuyerID {
  o String BuyerID
  o Double balance default=100.00
  o String First_Name
  o String Last_Name
}

participant Seller identified by SellerID {
  o String SellerID
  o Double balance default=0.00
  o String name
}
```

Διάγραμμα 15: Αρχείο Μοντέλο μέρος 2ο

Ο αγοραστής έχει τη δυνατότητα εισαγωγής οποιουδήποτε ποσού για να εισαχθεί στο πορτοφόλι όπως και του ονόματος και του επιθέτου του. Ο πωλητής είναι ο βιβλιοθηκονομος ο οποίος για λόγους δοκιμών μπορεί να εισάγει οποιοδήποτε ποσό.

Το asset “SaleContract” εκτελεί το έξυπνο συμβόλαιο, θα εκτελέσει το συμβόλαιο του αγοραστή με αυτό του πωλητή. Αν ο αγοραστής δεν έχει επαρκές υπόλοιπο τότε δεν θα μπορεί να αγοράσει το βιβλίο. Αυτό αφαιρεί από το υπόλοιπο του αγοραστή και προσθέτει στου πωλητή. Το “Transaction Sale” θα εκτελέσει την πραγματική συναλλαγή του συμβολαίου.

```
asset SaleContract identified by SaleID {
  o String SaleID
  o Double price
  o BookAuthor bookauthor
  --> Buyer buyer
  --> Seller seller
}

transaction Sale {
  --> SaleContract saleContract
}
```

Διάγραμμα 16: Αρχείο Μοντέλο μέρος 3ο

3.4 Αρχείο Σεναρίου

Στην αρχή του αρχείου σεναρίου, πρέπει να συνδεθεί το αρχείο σεναρίου με το αρχείο μοντέλου.

```
/**
*       Allows a buyer to purchase books from the library
*       @ param { org . tradesnetwork . Sale} sale - the book purhase transaction
*       @ transaction
*/
```

Η σύνδεση του αρχείου σεναρίου με το αρχείο μοντέλου μέσα σε έναν χώρο ονομάτων (namespace). Χρησιμοποιείστε το όνομα συναλλαγής “Sale” από το αρχείο μοντέλου στο αρχείο σεναρίου. Το “Transaction” θα κάνει τον composer να ξέρει ότι αυτό είναι μια συναλλαγή.

Παρακάτω φαίνονται οι μεταβλητές που εξάγουν το όρισμα (argument) από την συνάρτηση, καθώς και το συμβόλαιο πωλήσεων το οποίο είναι αποτέλεσμα της συναλλαγής με το αρχείο μοντέλου. Οι όροι (terms) παίρνουν το “SaleID” από το αρχείο μοντέλου.

```
async function sale(contract){
  const price = contract.saleContract.price;
  const seller = contract.saleContract.seller;
  const buyer = contract.saleContract.buyer;
  const terms = contract.saleContract.SaleID;
```

Στο παρακάτω απόσπασμα κώδικα παρουσιάζεται η αφαίρεση του ποσού από το πορτοφόλι του αγοραστή και η πρόσθεση αυτού του στο υπόλοιπο του πωλητή.

```
  seller.balance += price;
  buyer.balance -= price;
```

Παρακάτω φαίνεται η ενημέρωση του μετέχωντος registry χρησιμοποιώντας τον χώρο ονομάτων (namespace) για την ενημέρωση των πραγματικών ποσών του registry.

```
//Update seller balance
  const sellerRegistry = await getParticipantRegistry('org.tradesnetwork.Seller');
  await sellerRegistry.update(seller);

  //Update buyer balance
  const buyerRegistry = await getParticipantRegistry('org.tradesnetwork.Buyer');
  await buyerRegistry.update(buyer);
```

Το “await buyerRegistry.update(buyer);” θα αναβαθμίσει το υπόλοιπο του μέλους και το “await buyerRegistry.seller(seller);” θα αναβαθμίσει το υπόλοιπο της βιβλιοθήκης.

3.5 Έλεγχος Πρόσβασης και Άδειες

Ο έλεγχος πρόσβασης επιτρέπει στον διαχειριστή να έχει πλήρη πρόσβαση στους πόρους των χρηστών όπως και στους πόρους συστήματος. Έτσι γίνεται ευκολότερη η υλοποίηση, η επεξεργασία και οι δοκιμές.

```
rule Network Admin User {
description : " Grant business network administrators full access to user resources"
participant: " org . hyperledger. composer. system . Network Admin " operation : ALL
resources: "**" action : ALLOW
}

rule Network Admin System {
description : " Grant business network administrators full access to system resources"
participant: " org . hyperledger. composer. system . Network Admin " operation : ALL
resources: " org . hyperledger. composer. system .** " action : ALLOW
}
```

ΚΕΦΑΛΑΙΟ 4: Αποτελέσματα

4.1 Hyperledger Composer Backround

Το playfround του Hyperledger composer επέτρεψε να γίνουν δοκιμές στο testbed. Τα αποτελέσματα που παράγονται κατηγοριοποιούνται από τρία στοιχεία, τα οποία είναι:

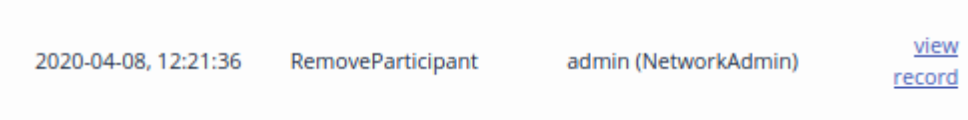
- Συμμετέχοντες
- Περιουσιακά στοιχεία
- Συναλλαγές.

Το BuyerID θα διατηρήσει το αναγνωριστικό του αγοραστή και αργότερα θα αλλάξει στο email του. Το υπόλοιπο επιλέγεται από το μέλος για να τοποθετηθεί στο πορτοφόλι του καθώς και από το όνομα και το επώνυμό τους.

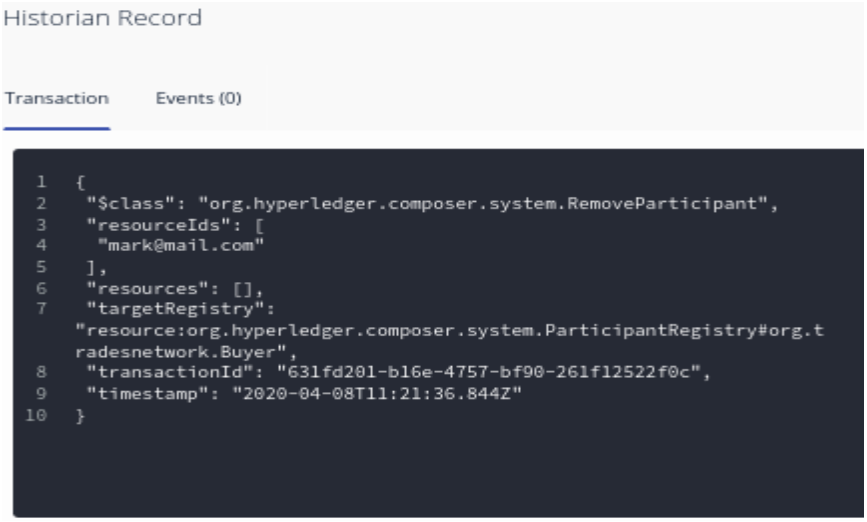
Η βιβλιοθήκη έχει το δικό της αναγνωριστικό και το υπόλοιπο ενημερώνεται κάθε φορά που αγοράζεται ένα βιβλίο.

Όταν δημιουργούνται οι δύο συμμετέχοντες, στο συμβόλαιο πωλήσεων δημιουργεί την πραγματική συναλλαγή ενημερώνοντας τις τιμές των συμμετεχόντων. Η συναλλαγή λαμβάνει τα αναγνωριστικά από το μέλος και τη βιβλιοθήκη για να ολοκληρώσει τη συναλλαγή.

Η δυνατότητα αφαίρεσης περιττών συμμετεχόντων είναι επίσης μια επιλογή που διατίθεται μόνο από τον διαχειριστή, καθώς αυτό φαίνεται στο παρακάτω σχήμα



Διάγραμμα 16: Διαγραφή Συμμετέχοντα μέρος 1ο

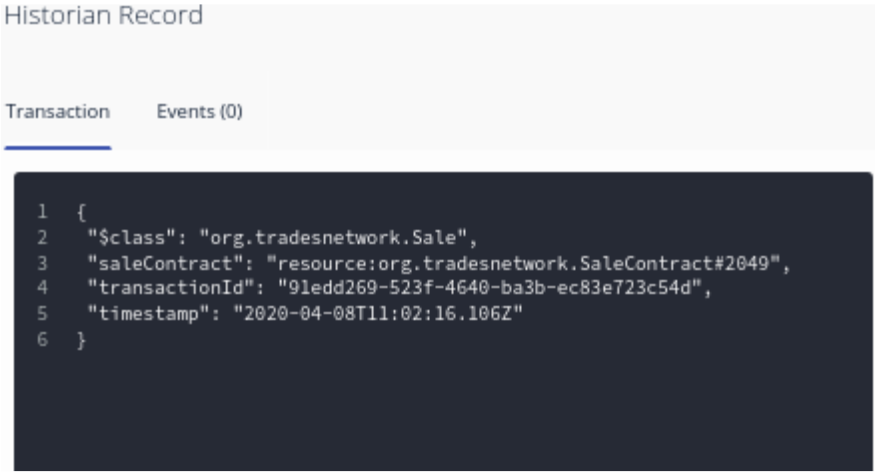


Διάγραμμα 17: Διαγραφή Συμμετέχοντα μέρος 2ο

4.2 Output

Για να περάσει η συναλλαγή, πρέπει να υποβληθεί το συμβόλαιο πώλησης. Μετά την υποβολή, η καρτέλα συναλλαγών θα ενημερωθεί και εάν η συναλλαγή ήταν επιτυχής, θα ενημερωθεί στο δίκτυο όπως θα φαίνεται στο παρακάτω σχήμα

..



Διάγραμμα 18: Αρχείο Μοντέλο μέρος 2ο

Η συναλλαγή που εμφανίζεται δείχνει μια επιτυχημένη συναλλαγή μεταξύ του αγοραστή και του πωλητή, σε αυτήν την περίπτωση μπορούμε να δούμε το αναγνωριστικό του συμβολαίου πώλησης καθώς και το αναγνωριστικό συναλλαγής με μια χρονική σήμανση για αποδεικτικά στοιχεία.

ΚΕΦΑΛΑΙΟ 5 : Επίλογος

Η παρουσία διπλωματική εργασία πραγματεύτηκε κάτι πρωτοπόρο αφού η συγκεκριμένη τεχνολογία δεν έχει ακόμα πρακτική εφαρμογή από τις ψηφιακές βιβλιοθήκες.

Αποτελεί μία πρώτη προσπάθεια υλοποίησης εφαρμογής με την τεχνολογία Blockchain που θα μπορούσε να αντικαταστήσει τα παραδοσιακά προγράμματα διαχείρισης των ψηφιακών βιβλιοθηκών.

Ο δρόμος μέχρι την παραγωγική λειτουργία είναι μακρύς , αφού ενδεικτικά κατ' ελάχιστον πρέπει να υλοποιηθούν τα εξής χαρακτηριστικά :

- Προσθήκη μεγάλου αριθμού βιβλίων
- Εύρεση βιβλίων με πολλαπλά κριτήρια
- Τα μέλη να ορίζουν τιμές ανά βιβλία
- Φιλικό περιβάλλον πλοήγησης.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Andrews, J., & Law, D. (2017). *Digital libraries*. Aldershot, Hants, England: Ashgate

Alharby, M., & van Moorsel, A. (2020). BLOCKCHAIN-BASED SMART CONTRACTS: A SYSTEMATIC MAPPING STUDY.

Atzei, N., Bartolett, M., & Cimoli, T. (2017). *A Survey of Attacks on Ethereum Smart Contracts*.

Bashir, I. *Mastering Blockchain - Second Edition*

Bhargavan, K., & Delignat-Lavaud, A. (2016). Formal Verification of Smart Contracts: Short Paper.

Coghill, J. (2018). Blockchain and its Implications for Libraries. *Journal Of Electronic Resources In Medical Libraries*, *15*(2), 66-70. doi: 10.1080/15424065.2018.148321

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). *BlockChain Technology: Beyond Bitcoin*.

Fox, E., Akscyn, R., Furuta, R., & Leggett, J. (1995). *Digital Libraries*. Communications of the ACM.

Khullar, D. (2020). How Social Isolation Is Killing Us. Retrieved from https://www.nytimes.com/2016/12/22/upshot/how-social-isolation-is-killing-us.html

Kean, D. (2017). This article is more than 3 years old Ransomware attack paralyses St Louis libraries as hackers demand bitcoins. *The Guardian*.

Lu, H., Li, Y., Chen, M., Kim, H., & Serikawa, S. (2017). Brain Intelligence:

Go beyond ArtificialIntelligence. *Mobile Networks And Applications*, *23*(2), 368-375. doi: 10.1007/s11036-017-0932-8

Meitinger, T. (2017). Smart Contracts. *Informatik-Spektrum*, *40*(4), 371-375. doi: 10.1007/s00287-017-1045-2

Nichols, S. (2018). Card-stealing code that pwned British Airways, Ticketmaster pops up on more sites via hacked JS. Retrieved 17 January 2020, from https://www.theregister.co.uk/2018/09/12/feedify_magecart_javascript_library_hacked/

Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering*, *59*(3), 183-187. doi: 10.1007/s12599-017-0467-3

Ølnes, S., Ubacht, J., & Janssen, M. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Government Information Quarterly*, *34*(3), 355-364. doi: 10.1016/j.giq.2017.09.007

SHARMA, T. (2019). Hyperledger Sawtooth Or Hyperledger Fabric : Which Is better?. Retrieved 5 February 2020, from https://www.blockchain-council.org/hyperledger/hyperledger-sawtooth-or-hyperledger-fabric-which-is-better/

Singh, S., & Singh, N. (2016). Blockchain: Future of financial and cyber security.

Somvir, & Kaushik, S. (2019). Social network services and Libraries. *IP Indian Journal Of Library Science And Information Technology*, *4*(1), 8-10. doi: 10.18231/j.ijlsit.2019.003

Wu, J., Williams, K., Chen, H., Khabsa, M., Caragea, C., & Tuarob, S. et al. (2015). CiteSeerX: AI in a Digital Library Search Engine. *AI Magazine*, *36*(3), 35. doi: 10.1609/aimag.v36i3.2601

Zyskind, G., Nathan, O., & Pentland, A. (2019). IEEE Xplore Full-Text PDF:. Retrieved 22 November 2019, from https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7163223