ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ ΤΟΜΕΑΣ ΤΕΧΝΟΛΟΓΙΑΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

ΥΛΟΠΟΙΗΣΗ DECENTRALIZED APPLICATION ΣΕ ΣΥΝΕΡΓΑΣΙΑ ΜΕ ΤΗΝ ΕΤΑΙΡΕΙΑ SPIRIT INNOVATIONS

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Παναγιώτης Βέκιος

Επιβλέπων: Νεκτάριος Κοζύρης

Καθηγητής Ε.Μ.Π

Αθήνα, Σεπτέμβριος 2019

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ ΤΟΜΕΑΣ ΤΕΧΝΟΛΟΓΙΑΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

ΥΛΟΠΟΙΗΣΗ DECENTRALIZED APPLICATION ΣΕ ΣΥΝΕΡΓΑΣΙΑ ΜΕ ΤΗΝ ΕΤΑΙΡΕΙΑ SPIRIT INNOVATIONS

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Παναγιώτης Βέκιος

Επιβλέπων: Νεκτάριος Κοζύρης

Καθηγητής Ε.Μ.Π

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 9η Οκτωβρίου 2019.

(Υπογραφή)	*(Υπογραφή)*	*(Υπογραφή)*
. . . . .	. . . . .	. . . . .
Νεκτάριος Κοζύρης	Γεώργιος Γκούμας	Δημήτριος Τσουμάκος
Καθηγητής ΕΜΠ	Επ. Καθηγητής ΕΜΠ	Αναπ. Καθηγητής ΕΜΠ

Αθήνα, Σεπτέμβριος 2019

.....

Παναγιώτης Βέκιος

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

Περίληψη

Σκοπός της διπλωματικής εργασίας είναι η υλοποίηση μια αποκεντρωμένης εφαρμογής (DApp - Decentralized Application) . Οι εφαρμογές dApps ή αποκεντρωμένες εφαρμογές είναι μια νέα σειρά εφαρμογών που δεν ελέγχονται ή δεν ανήκουν σε μία μόνο αρχή και δεν μπορούν να κλείσουν ή να έχουν διακοπή λειτουργίας. Τα βασικά χαρακτηριστικά τους είναι η αυτονομία και η από κοινού συναίνεση, το γεγονός δηλαδή πως οι αλλαγές πρέπει να αποφασιστούν από το σύνολο ή την πλειοψηφία των χρηστών. Επίσης, εφαρμογές αυτές αποθηκεύουν τα πάντα σε ένα αποκεντρωμένο blockchain για να σώσουν την εφαρμογή από τους κινδύνους της κεντρικής εξουσίας. Οι DApps λειτουργούν σε αποκεντρωμένο δίκτυο P2P (P2P Network - peer-to-peer network) .Το πρώτο γνωστό dApp στον κόσμο ήταν το Bitcoin. Το blockchain, όπου αποθηκεύονται όλα τα δεδομένα των παραπάνω εφαρμογών, όπως υποδηλώνει και το όνομα του μπορεί να θεωρηθεί ως μια αλυσίδα αρχείων που αποθηκεύονται σε μορφές μπλοκ και δεν ελέγχονται από καμία αρχή. Κάθε ένα από αυτά είναι ασφαλισμένο και δεσμευμένο με το άλλο χρησιμοποιώντας κρυπτογραφικές αρχές, δημιουργώντας έτσι μια αλυσίδα (chain). Πρόκειται για ένα κατανεμημένο βιβλίο πλήρως ανοιχτό σε όλους στο δίκτυο και μόλις μια πληροφορία αποθηκευτεί σε αυτό, είναι εξαιρετικά δύσκολο να αλλαχθεί. Βασίζεται στην αρχή της ομοφωνίας (συναίνεσης) δηλαδή όλοι οι συμμετέχοντες στο δίκτυο πρέπει να καταλήξουν σε συμφωνία (ομοφωνία) ώστε να επιβεβαιωθεί μια συναλλαγή.

Η εφαρμογή που υλοποιήθηκε αφορά τη σύναψη συμφωνίας - συμβολαίου μεταξύ δύο εταιρειών για την ολοκλήρωση μιας παραγγελίας, την συνεχή αλληλεπίδραση τους μέσω αυτής με την ανταλλαγή εγγράφων που είναι απαραίτητα για να προχωρήσει η διαδικασία της παραγγελίας και την ενημέρωση τους για το στάδιο όπου βρίσκονται τα προϊόντα ανά πάσα στιγμή. Πιο συγκεκριμένα κάθε συμβόλαιο που συμφωνείται από τις εταιρείες ανεβαίνει στο Blockchain με αποτέλεσμα κανείς να μην μπορεί να αλλάξει τους όρους του, ούτε μάλιστα και η ίδια η εταιρεία (Spirit Innovations) που το ανεβάζει. Με τον τρόπο αυτό εξασφαλίζεται εμπιστοσύνη και το συμβόλαιο που συμφωνείται δεν μπορεί να μεταβληθεί, σε αντίθεση με αυτό που γινόταν προηγουμένως καθώς οποιοδήποτε εμπλεκόμενο μέρος θα μπορούσε να τροποποιήσει τους όρους του συμβολαίου προς συμφέρον του. Επίσης, κάθε έγγραφο που ανταλλάσσεται μεταξύ των εταιρειών ανεβαίνει στο blockchain με αποτέλεσμα και πάλι να μην μπορεί να μεταβληθεί από κανέναν. Όταν ανεβαίνει ή γίνεται αποδεκτό ένα έγγραφο υπάρχει real-time ενημέρωση των χρηστών ώστε να ενημερώνεται άμεσα κάθε εταιρεία και να μην υπάρχει καθυστέρηση. Επίσης, όταν κάποιο έγγραφο γίνεται αποδεκτό καταγράφεται στο blockchain η ώρα και ημερομηνία που αυτό έγινε, ώστε να μπορεί να προβληθεί ανά πάσα στιγμή. Τέλος, δίνεται η δυνατότητα στον χρήστη να δει όλα τα συμβόλαια με τα οποία εμπλέκεται και να επιλέξει εκείνο που επιθυμεί. Σε αυτό θα υπάρχουν όλα τα σχετικά έγγραφα που έχουν ανέβει καθώς και η κατάσταση στην οποία βρίσκεται.

Λέξεις Κλειδιά

Blockchain, Smart Contract, Decentralized Application, Peer-to-Peer network, Ethereum, IPFS

Summary

The purpose of the thesis is to implement a decentralized application (DApp - Decentralized Application). DApps or decentralized applications are a new set of applications that are not controlled or owned by a single authority and cannot be shut down. Their main features are autonomy and unanimous consent, which means that the changes must be decided by all or a majority of users. Also, these applications store everything in a decentralized blockchain to save the application from the dangers of centralized power. DApps operate on a P2P decentralized network (peer-to-peer network). The first known dApp in the world was the Bitcoin.

The blockchain, where all the data of the above applications are stored, as its name implies, can be considered as a chain of files stored in block formats and not controlled by any authority. Each of them is secured and bound to each other using cryptographic principles, thereby creating a chain. It is a distributed book completely open to everyone on the web and once an information is stored in it, it is extremely difficult to change. It is based on the principle of consensus, that is all participants in the network must reach an agreement (consensus) in order to confirm a transaction.

The application that materialized involves the conclusion of a contract between two companies for the completion of an order, their continuous interaction through it with the exchange of documents necessary to proceed the ordering process and informing them of the stage where the products are located anytime. In particular, any contract agreed by the companies is uploaded on the Blockchain, so that no one can change its terms, not even the company itself (Spirit Innovations) that uploaded it. This ensures trust and the contract that is agreed cannot be changed, unlike what was previously done, as any party could modify the terms of the contract in their own interest. Also, every document that is exchanged between companies is uploaded on the blockchain and again it cannot be changed by anyone. When a document is uploaded or accepted, there is a real-time user update so that every company is immediately informed and there is no delay. Also, when a document is accepted, it is recorded on the blockchain the time and date it happened, so that it can be viewed at any time. Finally, the user is given the opportunity to see all the contracts he is involved with and choose the one he wants. It will contain all the relevant documents that have been uploaded and its situation.

Keywords

Blockchain, Smart Contract, Decentralized Application, Peer-to-Peer network, Ethereum, IPFS

Ευχαριστίες

Η παρούσα διπλωματική εργασία εκπονήθηκε στο Εργαστήριο Υπολογιστικών Συστημάτων του τομέα Τεχνολογίας Πληροφορικής και Υπολογιστών της Σχολής Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών ΕΜΠ.

Με την ευκαιρία της ολοκλήρωσης της διπλωματικής μου εργασίας, θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες στον επιβλέποντα της, Καθηγητή κ. Νεκτάριο Κοζύρη για τη δυνατότητα που μου παρείχε να εργαστώ ερευνητικά στον τομέα του Blockchain, αλλά και για την επιρροή που μου άσκησε μέσα από τα μαθήματα σε όλη τη διάρκεια της φοίτησης μου στη σχολή.

Επίσης, θα ήθελα να ευχαριστήσω ιδιαίτερα την δόκτορα Κατερίνα Δόκα για την επίβλεψη και την πολύτιμη συμβολή της στην εκπόνηση αυτής της διπλωματικής εργασίας. Οι κατευθύνσεις που μου παρείχε και το διαρκές ενδιαφέρον που έδειχνε υπήρξαν κρίσιμα για την ολοκλήρωση της.

Στη συνέχεια, θα ήθελα επίσης να εκφράσω τις ειλικρινείς μου ευχαριστίες στην εταιρεία Spirit Innovations, για την οποία αναπτύχθηκε η συγκεκριμένη εφαρμογή, που μου παρείχε τη μοναδική ευκαιρία να ολοκληρώσω τη διατριβή μου σε ένα πραγματικό επιχειρηματικό περιβάλλον. Συγκεκριμένα, θα ήθελα να ευχαριστήσω τον κ. Κωνσταντίνο Βασιλάτο που με καθοδήγησε σε όλη την πορεία μου μέσω της παροχής πολύτιμων πληροφοριών και της υποστήριξης του σε ολόκληρη τη διαδικασία.

Κλείνοντας, ευχαριστώ ιδιαίτερα τα μέλη της εξεταστικής επιτροπής κ. Νεκτάριο Κοζύρη, κ. Γεώργιο Γκούμα και κ. Δημήτριο Τσουμάκο για το χρόνο που θα αφιερώσουν στη μελέτη της διπλωματικής μου εργασίας.

Τέλος, θα ήθελα να εκφράσω την ευγνωμοσύνη μου προς την οικογένεια και τους φίλους μου που μου έδειξαν άνευ όρων υποστήριξη κατά τη διάρκεια των σπουδών μου.

Περιεχόμενα

Περίληψη 5
Summary 6
Ευχαριστίες 7
Πίνακας Εικόνων 10
Πίνακας Στιγμιοτύπων 11
Πίνακας Διαγραμμάτων 12
1 Εισαγωγή 13
2 BLOCKCHAIN 15
2.1 Blockchain Ορισμός 15
2.2 Ανάλυση του Blockchain με παραδείγματα 15
2.3 Blockchain Επεξήγηση Λειτουργίας 16
2.4 Οι 3 πυλώνες της τεχνολογίας του blockchain 18
2.5 Το δίκτυο και οι κόμβοι του blockchain 24
2.5.1 Η χρησιμότητα του peer-to-peer network 24
2.5.2 Η χρήση των δικτύων και των κόμβων στα κρυπτονομίσματα 25
2.6 Λόγοι χρήσης του blockchain 26
2.7 Τύποι του blockchain 27
3 Smart Contracts 32
3.1 Επεξήγηση των Smart Contracts 32
3.1.1 Παράδειγμα Smart Contract 33
3.2 Λειτουργία του Smart Contract 34
3.3 Τα πλεονεκτήματα και η αναγκαιότητα των Smart Contracts 35
3.4 Εφαρμογές των Smart Contracts 39
3.5 Blockchains όπου μπορούν να επεξεργαστούν τα Smart Contracts 43
4 Dapps 44
4.1 Επεξήγηση των Dapps (Decentralized Applications) 44
4.2 Τα Dapps στον πραγματικό κόσμο 45
4.3 Τρόπος ανάπτυξης ενός dapp 47
4.4 Πλεονεκτήματα των dapps σε σχέση με τις συμβατικές εφαρμογές 48

5 Ethereum 49
5.1 Ανάλυση του Ethereum 49
5.2 Βασικά ιστορικά σημεία του Ethereum 49
5.3 Η εικονική μηχανή του Ethereum 51
5.4 Τρόπος χρήσης του Ethereum 51
5.5 Τα οφέλη μιας αποκεντρωμένης εφαρμογής Ethereum 53
5.6 Τρόπος πρόσβασης στο Ethereum για την ανάπτυξη εφαρμογής 53
6 InterPlanetary File System (IPFS) 55
6.1 Ορισμός 55
6.2 Επεξήγηση IPFS και οι λόγοι που το καθιστούν σημαντικό 55
7 Blockchain Events 59
7.1 Ορισμός των Events 59
7.2 Σύνδεση με User Interface 59
7.3 Συμπερασματικά 60
8 Η Dapp που υλοποιήθηκε 61
8.1 Γενικό πλαίσιο 61
8.2 Προβλήματα 62
8.3 Λύση των προβλημάτων μέσω της λειτουργίας της Dapp 62
8.4 Αρχική σελίδα της λειτουργίας του Dapp 63
8.5 Επεξήγηση της λειτουργίας του Dapp μέσα από κάθε συμβόλαιο 65
8.6 Ανάλυση των σταδίων της εφαρμογής και σχηματική απεικόνιση 71
8.7 Κόστος 94
9 Επίλογος 96
10 Βιβλιογραφία 98

Πίνακας Εικόνων

Εικόνα 1: Παραδοσιακό μοντέλο πελάτη-διακομιστή (wikipedia, n.d.) 19
Εικόνα 2: Centralized vs Decentralized Systems (Rosic, guides/blockchain, 2019) 20
Εικόνα 3: Στιγμιότυπο Συναλλαγών του Ethereum (Rosic, guides/blockchain, 2019) 21
Εικόνα 4: 1ο Παράδειγμα Λειτουργίας του SHA-256 (Rosic, guides/blockchain, 2019) 23
Εικόνα 5 : 2ο Παράδειγμα Λειτουργίας του SHA-256 (Rosic, guides/blockchain, 2019) 23
Εικόνα 6: Σύγκριση του παραδοσιακού centralized downloading με το decentralized peer-to-peer downloading (Rosic, guides/blockchain, 2019) 25
Εικόνα 7: Λειτουργία του Smart Contract (Rosic, blockgeeks, 2016)..... 35
Εικόνα 8: Διαφορές μεταξύ παραδοσιακών και έξυπνων συμβολαίων (Morrison, 2016) 39
Εικόνα 9: Προστασία περιεχομένου με πνευματικά δικαιώματα (Prapat, 2018) 42
Εικόνα 10: Apps vs dApps (Pratik, 2018) 44
Εικόνα 11: Σύγκριση ανάπτυξης συμβατικής εφαρμογής εναντίον αποκεντρωμένης (Pratik, 2018)..... 47
Εικόνα 12: Ethereum Network (Rosic, guides/ethereum, 2019)..... 53
Εικόνα 13: Συγκρίνοντας την κίνηση των δεδομένων στο IPFS και σε ένα κεντρικό σύστημα (Capital, 2018) 55
Εικόνα 14: Μερικές από τις ανερχόμενες dApps που χρησιμοποιούν IPFS σαν πλατφόρμα αποθήκευσης(Capital, 2018) 57
Εικόνα 15: Πολλές πλατφόρμες που διαμοιράζονται video, κοινωνικά μέσα δικτύωσης και άλλες αρχίζουν να χρησιμοποιούν το IPFS για να πετύχουν καλύτερη εμπειρία χρήστη και ένα καλύτερο επιχειρηματικό μοντέλο (Capital, 2018). 58
Εικόνα 16: Blockchain events (Stewart, 2018) 60
Εικόνα 17: Gas Cost σύμφωνα με το Ethereum White Paper (Wood, 2019) 95

Πίνακας Στιγμιοτύπων

Screenshot 1 63
Screenshot 2 64
Screenshot 3 64
Screenshot 4 64
Screenshot 5 65
Screenshot 6 67
Screenshot 7 68
Screenshot 8 69
Screenshot 9 70
Screenshot 10 71
Screenshot 11 71
Screenshot 12 74
Screenshot 13 75
Screenshot 14 76
Screenshot 15 77
Screenshot 16 78
Screenshot 17 79
Screenshot 18 80
Screenshot 19 81
Screenshot 20 82
Screenshot 21 83
Screenshot 22 84
Screenshot 23 85
Screenshot 24 86
Screenshot 25 87
Screenshot 26 88
Screenshot 27 89
Screenshot 28 90
Screenshot 29 91
Screenshot 30 92
Screenshot 31 93
Screenshot 32 93

Πίνακας Διαγραμμάτων

Διάγραμμα 1……..69

1 Εισαγωγή

Εκατομμύρια δολάρια έχουν δαπανηθεί στην έρευνα της τεχνολογίας blockchain κατά τα τελευταία χρόνια καθώς προσφέρει νέα εργαλεία για τον έλεγχο ταυτότητας και την εξουσιοδότηση στον ψηφιακό κόσμο, τα οποία αποκλείουν την ανάγκη για πολλούς κεντρικούς διαχειριστές. Ως αποτέλεσμα, επιτρέπει τη δημιουργία νέων ψηφιακών σχέσεων. Με την επισημοποίηση και την ασφάλιση νέων ψηφιακών σχέσεων, η επανάσταση του blockchain τίθεται για να δημιουργήσει ένα στρώμα του Διαδικτύου για συναλλαγές και αλληλεπιδράσεις αξίας (συχνά αποκαλούμενο ως «Internet of Value», σε αντίθεση με το «Internet of Information», που χρησιμοποιεί το σύστημα πελάτης-εξυπηρετητής και τις βασικές βάσεις δεδομένων που χρησιμοποιούνται τα τελευταία 20 χρόνια).

Η άνοδος των ψηφιακών τεχνολογιών κατά την τελευταία δεκαετία έχει προκαλέσει σημαντικές διαταραχές σε πολλούς τομείς της βιομηχανίας. Η εμφάνιση των κρυπτονομισμάτων και συγκεκριμένα η υποκείμενη τεχνολογία blockchain που υποστηρίζει το Bitcoin, υπόσχεται μια ριζική μεταμόρφωση του τρόπου με τον οποίο οι χρήστες ασχολούνται με τις χρηματοπιστωτικές υπηρεσίες.

Μαζί με την τεχνολογία του blockchain την παρουσία τους έκαναν και οι έξυπνες συμβάσεις . Στην πραγματικότητα, έχουν γίνει γρήγορα μια απαραίτητη καινοτομία για τις επιχειρήσεις. Αυτό το εκπληκτικό κομμάτι της τεχνολογίας επιτρέπει να πραγματοποιηθούν συναλλαγές, να γίνουν διαφανείς συμφωνίες, να αυτοματοποιηθούν οι διαδικασίες, να ανταλλαχθούν χρήματα, ακίνητα ή οτιδήποτε έχει αξία με πάρα πολύ εύκολο τρόπο. Οι έξυπνες συμβάσεις παρουσιάζουν έντονο ενδιαφέρον και για τις επιχειρήσεις. Συμβάλλουν στην επίλυση του προβλήματος της δυσπιστίας μεταξύ των εμπλεκόμενων μερών και των επιχειρηματικών εταίρων. Επίσης, έχουν πολλά οφέλη για ένα ευρύ φάσμα βιομηχανιών, μειώνοντας τις περιττές δαπάνες και τις δαπάνες χρόνου, ενισχύοντας παράλληλα τη διαφάνεια και την εμπιστοσύνη.

Σκοπός της παρούσας εργασίας είναι η ανάλυση της τεχνολογίας που κρύβεται πίσω από το blockchain και με βάση αυτή η ανάπτυξη μιας αποκεντρωμένης εφαρμογής. Υπάρχει ο στόχος της συνεισφοράς στην κοινότητα των blockchains προσφέροντας νέες ιδέες και καινοτομίες στο χώρο αυτό για την ανάπτυξη αποκεντρωμένων εφαρμογών. Έκτος όμως της κοινότητας αυτής στοχεύει και στην παρακίνηση των απλών χρηστών που δεν γνωρίζουν για τέτοιου είδους εφαρμογές να ενημερωθούν και να τις χρησιμοποιήσουν. Κάτι τέτοιο μπορεί να γίνει αν μόνο καταλάβουν τα πλεονεκτήματα, τις δυνατότητες και την ευχρηστία που προσφέρει μια τέτοια εφαρμογή σε σχέση με τις συμβατικές τόσο θεωρητικά όσο και μέσα από την χρήση της.

Αρχικά, γίνεται εκτενής αναφορά στο blockchain στο κεφάλαιο 1, ώστε να αναλυθεί πλήρως το τι ακριβώς είναι και ο τρόπος που λειτουργεί. Αναλύονται οι τρεις

βασικοί πυλώνες στους οποίους στηρίζει τη λειτουργία του καθώς και το δίκτυο στο οποίο λειτουργεί. Επίσης παρουσιάζονται οι λόγοι για τους οποίους η τεχνολογία αυτή παρουσιάζει ραγδαία ανάπτυξη και χρησιμοποιείται ολοένα και περισσότερο.

Στο κεφάλαιο 3 εξετάζονται τα smart contracts (έξυπνα συμβόλαια) , που πρόκειται ουσιαστικά για κώδικα υπολογιστών που αφορά δύο ή περισσότερα μέρη και λειτουργεί στην βάση ενός blockchain. Επεξηγείται το τι ακριβώς είναι και πως αυτά λειτουργούν. Ακόμη, παρουσιάζεται η αναγκαιότητά τους στο σύγχρονο κόσμο, οι εφαρμογές τους καθώς και από ποια blockchain μπορούν να επεξεργαστούν.

Στη συνέχεια στο κεφάλαιο 4 αναλύονται τα Dapps (Decentralized Applications), τα οποία στηρίζουν την λειτουργία τους στο blockchain και αλληλεπιδρούν με τα smart contracts μέσω του User Interface. Εξηγείται η λειτουργία τους, η χρήση τους στον πραγματικό κόσμο, οι τρόποι με τους οποίους μπορεί να αναπτυχθεί ένα dapp και τέλος τα πλεονεκτήματα τους σε σχέση με τις συμβατικές εφαρμογές.

Το περιεχόμενο του κεφαλαίου 5 έχει να κάνει με το Ethereum, ένα κατανεμημένο δημόσιο δίκτυο blockchain. Πρόκειται για μια ανοιχτή πλατφόρμα λογισμικού που βασίζεται στην τεχνολογία blockchain και επιτρέπει στους προγραμματιστές να δημιουργήσουν και να αναπτύξουν αποκεντρωμένες εφαρμογές. Γίνεται ανάλυση της λειτουργίας του και αναφορά στους τρόπους χρήσης του. Ακόμη, αναφέρονται τα οφέλη μιας αποκεντρωμένης εφαρμογής που αναπτύσσεται στο Ethereum, καθώς και οι τρόποι πρόσβασης σε αυτό για την ανάπτυξη της.

Τα επόμενα κεφάλαια 6,7 αναφέρονται στο InterPlanetary File System (IPFS) και στα blockchain events αντίστοιχα. Το πρώτο είναι ένα δίκτυο peer-to-peer για την αποθήκευση και κοινή χρήση δεδομένων σε ένα κατανεμημένο σύστημα αρχείων, ενώ τα δεύτερα χρησιμεύουν στο να ενημερωθεί άμεσα ο χρήστης μέσω του user-interface για μία ενέργεια (συναλλαγή του smart contract) που πραγματοποιήθηκε.

Τέλος, στο κεφάλαιο 8 παρουσιάζεται η Dapp που υλοποιήθηκε σε συνεργασία με την εταιρεία Spirit Innovations. Γίνεται αναφορά στο πλαίσιο ενασχόλησης της εταιρείας, στα προβλήματα που υπάρχουν και το πως αυτά μπορούν να αντιμετωπιστούν μέσα από την ανάπτυξη αυτής της εφαρμογής. Στη συνέχεια, εξηγείται αναλυτικά το πως λειτουργεί η εφαρμογή και το τι ακριβώς υλοποιεί προσφέροντας το ανάλογο σχεδιάγραμμα και τα κατάλληλα screenshots. Κλείνοντας, δηλώνεται το κόστος υλοποίησης της.

2 BLOCKCHAIN

2.1 Blockchain Ορισμός

Το blockchain με απλούς όρους είναι μια δομή δεδομένων που περιέχει αρχεία συναλλαγών και παράλληλα διασφαλίζει την ασφάλεια, την διαφάνεια και την αποκέντρωση. Μπορεί να θεωρηθεί ως μια αλυσίδα αρχείων που αποθηκεύονται σε μορφές μπλοκ που δεν ελέγχονται από καμία αρχή. Είναι ένα κατανεμημένο βιβλίο πλήρως ανοιχτό σε όλους στο δίκτυο και μόλις μια πληροφορία αποθηκευτεί σε αυτό, είναι εξαιρετικά δύσκολο να αλλαχθεί(Pratap,2018,July).

Το blockchain περιέχει μια χρονικά-σφραγισμένη σειρά αναλλοίωτων δεδομένων (data) που διαχειρίζεται από ένα σύμπλεγμα υπολογιστών που δεν ανήκουν σε καμία ενιαία οντότητα. Κάθε ένα από αυτά τα μπλοκ δεδομένων (block) είναι ασφαλισμένο και δεσμευμένο το ένα με το άλλο χρησιμοποιώντας κρυπτογραφικές αρχές, δημιουργώντας έτσι μια αλυσίδα (chain) (Rosic, guides/blockchain, 2019).

Η τεχνολογία Blockchain επιτρέπει σε όλους τους συμμετέχοντες στο δίκτυο να καταλήξουν σε συμφωνία, κοινώς γνωστή ως ομοφωνία (συναίνεση). Όλα τα δεδομένα που είναι αποθηκευμένα στο blockchain καταγράφονται ψηφιακά και έχουν ένα κοινό ιστορικό το οποίο είναι διαθέσιμο σε όλους τους συμμετέχοντες στο δίκτυο. Με αυτόν τον τρόπο εξαλείφονται οι πιθανότητες οποιασδήποτε απατηλής δραστηριότητας ή διπλής συναλλαγής χωρίς την ανάγκη ενός τρίτου (Pratap,2018,July).

Το χαρακτηριστικό που το ξεχωρίζει είναι ότι δεν έχει κεντρική εξουσία. Είναι ο ίδιος ο ορισμός ενός δημοκρατικού συστήματος. Δεδομένου ότι είναι σαν ένα κοινό και αμετάβλητο βιβλίο(ledger), οι πληροφορίες σε αυτό είναι ανοικτές για οποιονδήποτε να τις δει. Ως εκ τούτου, οτιδήποτε είναι χτισμένο στο blockchain είναι από τη φύση του διαφανές και όλοι οι συμμετέχοντες είναι υπεύθυνοι για τις ενέργειές τους (Rosic, guides/blockchain, 2019).

2.2 Ανάλυση του Blockchain με παραδείγματα

Για να κατανοηθεί καλύτερα το blockchain, θα εξεταστεί ένα παράδειγμα όπου αναζητείται μια επιλογή για να σταλούν χρήματα σε κάποιο χρήστη που ζει σε διαφορετική τοποθεσία. Μια γενική επιλογή που μπορεί να χρησιμοποιηθεί είναι μια τράπεζα ή μια εφαρμογή μεταφοράς πληρωμής όπως η PayPal ή Paytm. Αυτή η επιλογή αφορά τρίτους προκειμένου να διεκπεραιωθεί η συναλλαγή, λόγω της οποίας αφαιρείται επιπλέον ποσό από τα χρήματα ως μεταβιβαστική αμοιβή. Επιπλέον, σε περιπτώσεις όπως αυτές, δεν μπορεί να διασφαλιστεί η ασφάλεια των χρημάτων σας, καθώς είναι πολύ πιθανό ένας χάκερ να διαταράξει το δίκτυο και να

κλέψει τα χρήματα. Και στις δύο περιπτώσεις, ο πελάτης δεινοπαθεί. Εδώ μπαίνει το Blockchain (Pratap,2018,July).

Αντί να χρησιμοποιηθεί μια τράπεζα για τη μεταφορά χρημάτων, εάν χρησιμοποιηθεί blockchain σε τέτοιες περιπτώσεις, η διαδικασία γίνεται πολύ πιο εύκολη και ασφαλής. Δεν υπάρχει πρόσθετη αμοιβή δεδομένου ότι τα κεφάλαια είναι άμεσα επεξεργασμένα από τον χρήστη και έτσι εξαλείφεται η ανάγκη για ένα τρίτο μέρος. Επιπλέον, η βάση δεδομένων blockchain είναι αποκεντρωμένη και δεν περιορίζεται σε καμία συγκεκριμένη τοποθεσία που σημαίνει ότι όλες οι πληροφορίες και τα αρχεία που διατηρούνται στο blockchain είναι δημόσια και αποκεντρωμένα. Δεδομένου ότι οι πληροφορίες δεν αποθηκεύονται σε ένα μόνο μέρος, δεν υπάρχει καμία πιθανότητα διαφθοράς των πληροφοριών από οποιονδήποτε χάκερ (Pratap,2018,July).

Στο blockchain δεν έχουμε κανένα κόστος συναλλαγής (κόστος υποδομής υπάρχει μεν, αλλά δεν υπάρχει κόστος συναλλαγής.) Είναι ένας απλός αλλά έξυπνος τρόπος για να μεταφερθούν πληροφορίες από τον Α στον Β με έναν πλήρως αυτοματοποιημένο και ασφαλή τρόπο. Το ένα εμπλεκόμενο μέρος της συναλλαγής ξεκινά τη διαδικασία δημιουργώντας ένα μπλοκ. Αυτό το μπλοκ επαληθεύεται από χιλιάδες, ίσως εκατομμύρια υπολογιστές που διανέμονται γύρω από το δίκτυο. Το επαληθευμένο μπλοκ προστίθεται στην αλυσίδα, η οποία αποθηκεύεται σε ολόκληρο τον ιστό, δημιουργώντας όχι μόνο ένα μοναδικό αρχείο, αλλά ένα μοναδικό αρχείο με μοναδικό ιστορικό. Η παραποίηση ενός αρχείου θα σήμαινε την παραποίηση ολόκληρης της αλυσίδας σε εκατομμύρια περιπτώσεις. Αυτό είναι πρακτικά αδύνατο. Το Bitcoin χρησιμοποιεί αυτό το μοντέλο για χρηματικές συναλλαγές, αλλά μπορεί να αναπτυχθεί με πολλούς άλλους τρόπους. (Rosic, guides/blockchain, 2019).

2.3 Blockchain Επεξήγηση Λειτουργίας

Ένα blockchain είναι μια αλυσίδα από μπλοκς που περιέχει δεδομένα ή πληροφορίες. Παρόλο που ανακαλύφθηκε νωρίτερα, η πρώτη επιτυχημένη και δημοφιλής εφαρμογή της τεχνολογίας Blockchain δημιουργήθηκε το 2009 από τον Satoshi Nakamoto. Δημιούργησε το πρώτο ψηφιακό κρυπτονόμισμα με την ονομασία Bitcoin μέσω της χρήσης της τεχνολογίας Blockchain. Θα μελετηθεί πώς πραγματικά λειτουργεί το blockchain (Pratap,2018,July).

Κάθε μπλοκ σε ένα blockchain δίκτυο αποθηκεύει κάποιες πληροφορίες μαζί με το hash του προηγούμενου μπλοκ. Ένα hash είναι ένας μοναδικός μαθηματικός κώδικας που ανήκει σε ένα συγκεκριμένο μπλοκ. Αν οι πληροφορίες εντός του μπλοκ έχουν τροποποιηθεί, το hash του μπλοκ θα υπόκειται επίσης σε

τροποποίηση. Η σύνδεση των μπλοκ μέσω των μοναδικών κλειδιών κατακερματισμού είναι αυτό που καθιστά ασφαλές το blockchain.

Ενώ οι συναλλαγές πραγματοποιούνται σε ένα blockchain, υπάρχουν κόμβοι στο δίκτυο που επικυρώνουν αυτές τις συναλλαγές. Στο blockchain του Bitcoin, αυτοί οι κόμβοι καλούνται ως ανθρακωρύχοι και χρησιμοποιούν την έννοια της απόδειξης εργασίας(proof of work) για να επεξεργαστούν και να επικυρώσουν τις συναλλαγές στο δίκτυο. Για να είναι έγκυρη μια συναλλαγή, κάθε μπλοκ πρέπει να αναφέρεται στο hash του προηγούμενου μπλοκ. Η συναλλαγή θα πραγματοποιηθεί μόνο και μόνο εάν ο κατακερματισμός (hash) είναι σωστός. Εάν ένας χάκερ προσπαθήσει να επιτεθεί στο δίκτυο και να αλλάξει πληροφορίες από οποιοδήποτε συγκεκριμένο μπλοκ, το hash που επισυνάπτεται στο μπλοκ θα τροποποιηθεί επίσης.

Η παραβίαση θα εντοπιστεί καθώς το τροποποιημένο hash δεν θα ταιριάζει με το αρχικό. Αυτό εξασφαλίζει ότι το blockchain είναι αναλλοίωτο, αφού οποιαδήποτε αλλαγή που γίνεται στην αλυσίδα των μπλοκ αντικατοπτρίζεται σε ολόκληρο το δίκτυο και ανιχνεύεται εύκολα.

Συνοπτικά, μια συναλλαγή στο blockchain συμβαίνει με τα παρακάτω βήματα:

1. Ένα δίκτυο blockchain χρησιμοποιεί δημόσια και ιδιωτικά κλειδιά για να σχηματίσει μια ψηφιακή υπογραφή εξασφαλίζοντας ασφάλεια και συναίνεση.
2. Μόλις εξασφαλιστεί ο έλεγχος ταυτότητας μέσω αυτών των κλειδιών, προκύπτει η ανάγκη εξουσιοδότησης.
3. Το Blockchain επιτρέπει στους συμμετέχοντες του δικτύου να εκτελούν μαθηματική επαλήθευση και να φτάνουν σε ομοφωνία (συναίνεση) για να συμφωνήσουν σε οποιαδήποτε συγκεκριμένη τιμή.
4. Κατά τη μεταφορά, ο αποστολέας χρησιμοποιεί το ιδιωτικό κλειδί του και ανακοινώνει τις πληροφορίες συναλλαγής μέσω του δικτύου. Δημιουργείται ένα μπλοκ που περιέχει πληροφορίες όπως η ψηφιακή υπογραφή, η χρονική σήμανση και το δημόσιο κλειδί του δέκτη.
5. Αυτό το μπλοκ πληροφοριών μεταδίδεται μέσω του δικτύου και αρχίζει η διαδικασία επικύρωσης.
6. Οι miners (ανθρακωρύχοι) σε όλο το δίκτυο ξεκινούν την επίλυση του μαθηματικού παζλ που σχετίζεται με τη συναλλαγή για να το επεξεργαστούν. Η επίλυση αυτού του παζλ απαιτεί από τους ανθρακωρύχους να επενδύσουν την υπολογιστική τους δύναμη.
7. Με την πρώτη επίλυση του παζλ, ο ανθρακωρύχος λαμβάνει ανταμοιβές με τη μορφή bitcoins. Αυτά τα προβλήματα αναφέρονται ως μαθηματικά προβλήματα απόδειξης εργασίας (proof of work).
8. Μόλις η πλειονότητα των κόμβων στο δίκτυο έρθει σε ομοφωνία και συμφωνήσει σε μια κοινή λύση, το μπλοκ σφραγίζεται χρονικά (προστίθεται χρονική σήμανση) και προστίθεται στο υπάρχον blockchain. Αυτό το μπλοκ μπορεί να περιέχει οτιδήποτε, όπως χρήματα, δεδομένα ή μηνύματα.

9. Μετά την προσθήκη του νέου μπλοκ στην αλυσίδα, τα υπάρχοντα αντίγραφα του blockchain ενημερώνονται για όλους τους κόμβους του δικτύου (Pratap,2018,July).

Ουσιαστικά για την καλύτερη κατανόηση του μπορεί να θεωρηθεί σαν ένα λογιστικό φύλλο που αντιγράφεται χιλιάδες φορές σε ένα δίκτυο υπολογιστών όπου το δίκτυο αυτό σχεδιάστηκε για να ενημερώνει τακτικά αυτό το λογιστικό φύλλο. Έτσι δουλεύει και το blockchain (Rosic, guides/blockchain, 2019).

Οι πληροφορίες που διατηρούνται σε ένα blockchain υπάρχουν σαν μια κοινόχρηστη και συνεχώς συνδιαλασσόμενη βάση δεδομένων. Αυτός είναι ένας τρόπος χρήσης του δικτύου που έχει προφανή οφέλη. Η βάση δεδομένων του blockchain δεν αποθηκεύεται σε μια ενιαία τοποθεσία , πράγμα που σημαίνει ότι τα αρχεία που διατηρεί είναι πραγματικά δημόσια και εύκολα επαληθεύσιμα. Δεν υπάρχει κεντρική έκδοση αυτών των πληροφοριών για έναν χάκερ ώστε να μπορεί να τα διαφθείρει. Φιλοξενείται από εκατομμύρια υπολογιστές ταυτόχρονα και τα δεδομένα του είναι προσβάσιμα σε οποιονδήποτε στο διαδίκτυο.

Ο λόγος για τον οποίο το blockchain έχει κερδίσει τόσο πολύ θαυμασμό είναι ότι:

- Δεν ανήκει σε μία ενιαία οντότητα, επομένως είναι αποκεντρωμένο.
- Τα δεδομένα αποθηκεύονται κρυπτογραφικά μέσα στην αλυσίδα.
- Το blockchain είναι αμετάβλητο, οπότε κανείς δεν μπορεί να παραβιάσει τα δεδομένα που βρίσκονται μέσα σε αυτό.
- Το blockchain είναι διαφανές, ώστε ο οποιοσδήποτε να μπορεί να παρακολουθεί τα δεδομένα αν το θέλει (Rosic, guides/blockchain, 2019).

2.4 Οι 3 πυλώνες της τεχνολογίας του blockchain

Οι τρεις κύριες ιδιότητες της τεχνολογίας Blockchain, που την βοήθησαν να κερδίσει ευρεία αναγνώριση, είναι οι εξής:

- Αποκέντρωση
- Διαφάνεια
- Αμεταβλητότητα

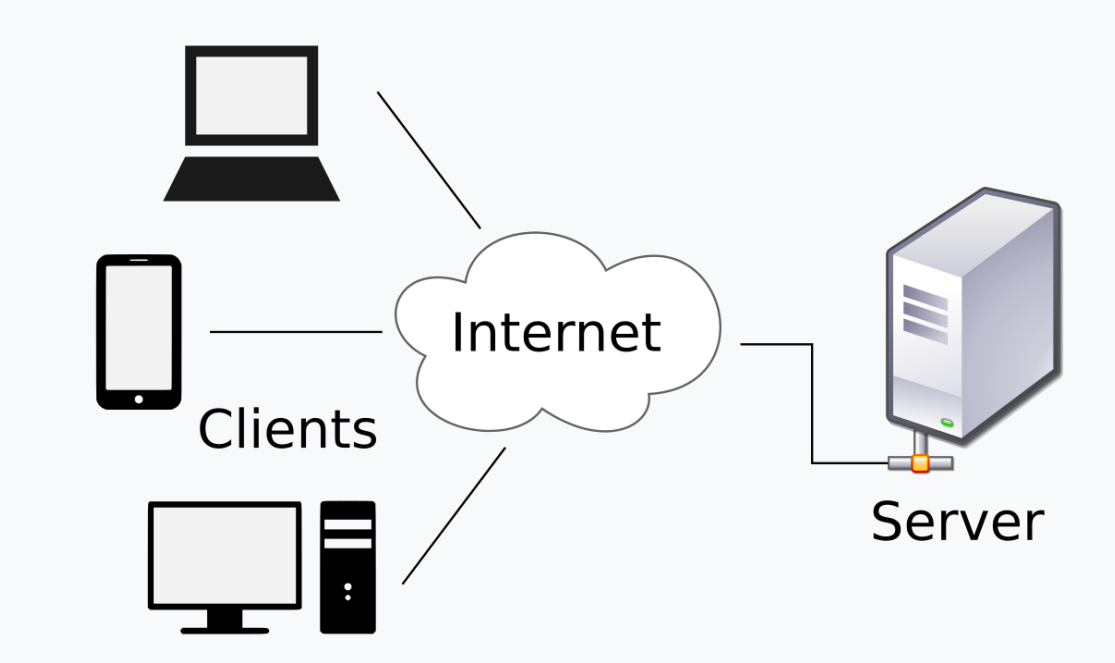
Πυλώνας # 1: Αποκέντρωση

Τα blockchain είναι αποκεντρωμένα στη φύση, που σημαίνει ότι κανένα άτομο ή ομάδα δεν κατέχει την εξουσία του συνολικού δικτύου. Ενώ όλοι στο δίκτυο έχουν το αντίγραφο του κατανεμημένου βιβλίου (distributed ledger) , κανείς δεν μπορεί να το τροποποιήσει μόνος του. Αυτό το μοναδικό χαρακτηριστικό του blockchain επιτρέπει τη διαφάνεια και την ασφάλεια δίνοντας παράλληλα τη δύναμη στους χρήστες (Pratap,2018,July).

Πριν εμφανιστούν το Bitcoin και το BitTorrent, οι χρήστες ήταν πιο συνηθισμένοι στις κεντρικές υπηρεσίες. Η ιδέα είναι πολύ απλή. Υπάρχει μια κεντρική οντότητα που αποθηκεύει όλα τα δεδομένα και θα πρέπει ο χρήστης να αλληλεπιδρά αποκλειστικά με αυτήν την οντότητα για να λάβει τις πληροφορίες που χρειάζεται.

Ένα άλλο παράδειγμα κεντρικού συστήματος είναι οι τράπεζες. Αποθηκεύουν όλα τα χρήματά του χρήστη και ο μόνος τρόπος με τον οποίο μπορεί να πληρώσει κάποιον είναι να περάσει από την τράπεζα.

Το παραδοσιακό μοντέλο πελάτη-διακομιστή είναι ένα τέλειο παράδειγμα για αυτό:



Εικόνα 1: Παραδοσιακό μοντέλο πελάτη-διακομιστή (wikipedia, n.d.)

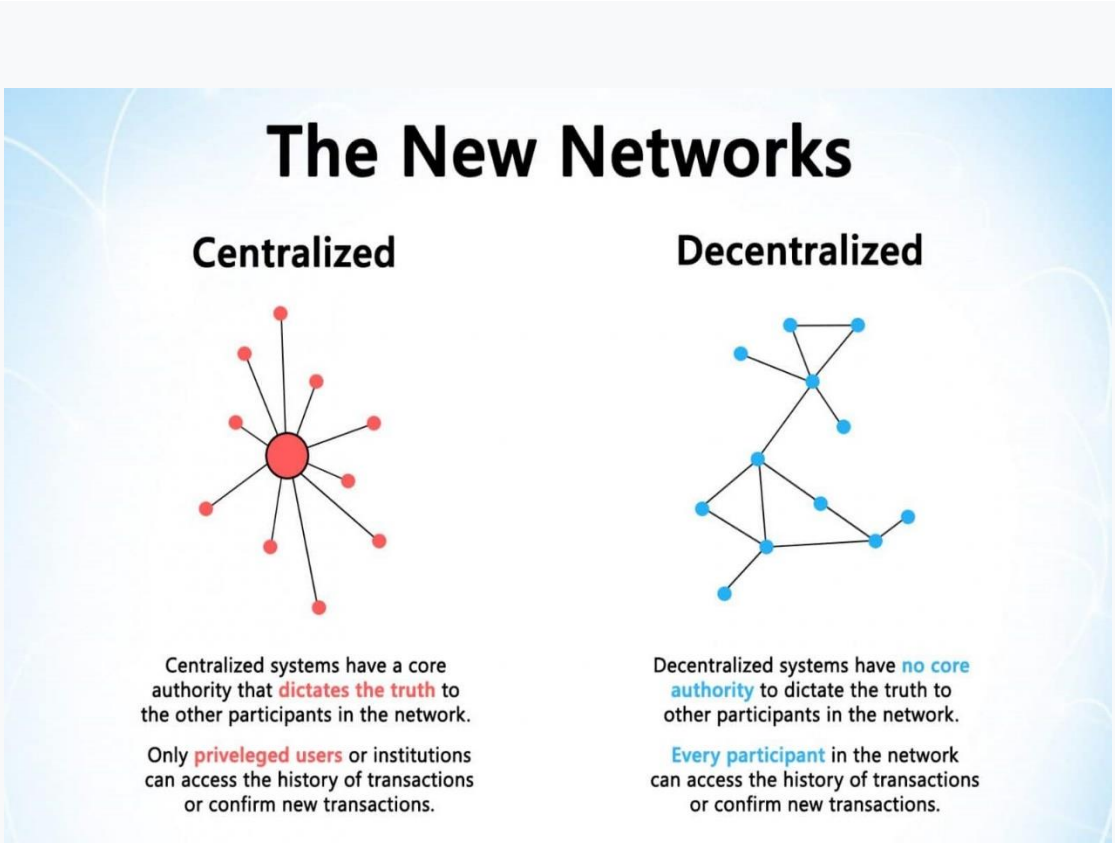
Όταν κάποιος χρήστης κάνει google αναζήτηση για κάτι, γίνεται ένα ερώτημα στο διακομιστή, ο οποίος στη συνέχεια θα απαντήσει με τις σχετικές πληροφορίες. Αυτό είναι ένα παράδειγμα απλού πελάτη-διακομιστή.

Τα κεντρικά συστήματα αν και έχουν συμπεριφερθεί καλά στους χρήστες εδώ και πολλά χρόνια έχουν ωστόσο πολλές ευπάθειες.

- Πρώτον, στα κεντρικά συστήματα, όλα τα δεδομένα αποθηκεύονται σε ένα σημείο. Αυτό τα καθιστά εύκολους στόχους για πιθανούς χάκερς.
- Εάν το κεντρικό σύστημα επρόκειτο να περάσει από αναβάθμιση λογισμικού, θα σταματούσε ολόκληρο το σύστημα.
- Αν η κεντρική οντότητα τερματιστεί για τον οποιοδήποτε λόγο τότε κανείς δεν θα έχει πρόσβαση στις πληροφορίες που διαθέτει.
- Το σενάριο της χειρότερης περίπτωσης είναι αν αυτή η οντότητα γίνει διεφθαρμένη και κακόβουλη. Εάν συμβεί αυτό, όλα τα δεδομένα που βρίσκονται μέσα στο blockchain θα παραβιαστούν.

Σε ένα αποκεντρωμένο σύστημα, οι πληροφορίες δεν αποθηκεύονται από μία μόνο οντότητα. Στην πραγματικότητα, όλοι στο δίκτυο κατέχουν τις πληροφορίες.

Σε ένα αποκεντρωμένο δίκτυο, αν ο χρήστης θέλει να αλληλεπιδράσει με τον φίλο του, τότε μπορεί να το κάνει άμεσα χωρίς να περάσει από τρίτο μέρος. Αυτή ήταν η κύρια ιδεολογία πίσω από το Bitcoin. Μόνο ο χρήστης είναι υπεύθυνος για τα χρήματά του. Μπορεί να στείλει τα χρήματά του σε όποιον θέλει χωρίς να χρειάζεται να περάσει από μια τράπεζα.



Εικόνα 2: Centralized vs Decentralized Systems (Rosic, guides/blockchain, 2019)

Πυλώνας #2: Διαφάνεια

Μία από τις πιο ενδιαφέρουσες και παρεξηγημένες έννοιες στην τεχνολογία blockchain είναι η "διαφάνεια". Μερικοί λένε ότι το blockchain σου προσφέρει ιδιωτικότητα, ενώ κάποιοι άλλοι ότι προσφέρει διαφάνεια . Θα μελετηθεί γιατί συμβαίνει αυτό.

Η ταυτότητα ενός ατόμου κρύβεται μέσω σύνθετης κρυπτογραφίας και εκπροσωπείται(παρουσιάζεται) μόνο από τη δημόσια διεύθυνση του. Έτσι, εάν αναζητηθεί το ιστορικό συναλλαγών ενός ατόμου, δεν θα φανεί "ο Bob έστειλε 1 BTC" αλλά θα φανεί "1MF1bhsFLkBzzz9vpFYEmvwT2TbyCt7NZJ έστειλε 1 BTC".

Αυτό φαίνεται καλύτερα στο ακόλουθο στιγμιότυπο των συναλλαγών του Ethereum:

TxHash	Block	Age	From		To	Value	[TxFee]
0x2d055e4585ae2a...	5629306	16 secs ago	0x003e3655090890...		0x2bdc9191de5c1b...	0,004741591554641 Ether	0.000294
0xb4d37c791ff4cde...	5629306	16 secs ago	0x6c3b4faf413e0e4...		0xf14cb3acac7b230...	0,744767225 Ether	0.000294
0x9979410dcb5f4c...	5629306	16 secs ago	0x99bcd75abbac05...		0x2d42ee86390c59...	0,016294 Ether	0.000294
0x189c4d4aae09be...	5629306	16 secs ago	0x175cd602b2a1e7...		0xd39681bb0586fb...	0,01 Ether	0.000294
0xda0e9bbb11fb77...	5629306	16 secs ago	0x73a065367d111c...		0x01995786f14357...	0 Ether	0.00150007
0x6be498fafad9acb...	5629306	16 secs ago	0xa3eb206871124a...		0x8a91cac422e55e...	0,029594 Ether	0.000294

Εικόνα 3: Στιγμιότυπο Συναλλαγών του Ethereum (Rosic, guides/blockchain, 2019)

Έτσι, ενώ η πραγματική ταυτότητα του ατόμου είναι ασφαλής, φαίνονται όλες οι συναλλαγές που έγιναν με την δημόσια διεύθυνση τους. Αυτό το επίπεδο διαφάνειας δεν υπήρξε ποτέ στο πλαίσιο ενός χρηματοπιστωτικού συστήματος. Προσθέτει αυτό το επιπλέον και πολύ αναγκαίο επίπεδο υπευθυνότητας που απαιτείται από ορισμένα από τα μεγαλύτερα ιδρύματα.

Εάν είναι γνωστή η δημόσια διεύθυνση μίας από τις μεγάλες εταιρείες, ο χρήστης μπορεί απλά να την ανοίξει σε έναν εξερευνητή και να εξετάσει όλες τις συναλλαγές με τις οποίες έχει εμπλακεί. Αυτό τις αναγκάζει να είναι ειλικρινείς, κάτι που δεν είχαν ποτέ αντιμετωπίσει στο παρελθόν.

Ωστόσο, αυτή δεν είναι η καλύτερη περίπτωση χρήσης. Οι περισσότερες από αυτές τις εταιρείες δεν θα πραγματοποιήσουν συναλλαγές χρησιμοποιώντας κρυπτονομίσματα, και ακόμη και αν το κάνουν, δεν θα κάνουν όλες τις συναλλαγές τους χρησιμοποιώντας κρυπτονομίσματα.

Πυλώνας # 3: Αμεταβλητότητα(Immutability)

Η ιδιότητα της αμεταβλητότητας ενός blockchain αναφέρεται στο γεγονός ότι δεν μπορούν να μεταβληθούν τα δεδομένα που γράφονται στο blockchain. Για να κατανοηθεί η αμεταβλητότητα, ας θεωρηθεί πως ο χρήστης στέλνει ένα μήνυμα ηλεκτρονικού ταχυδρομείου. Αφού στείλει το μήνυμα ηλεκτρονικού ταχυδρομείου σε ένα σωρό άτομα, δεν μπορεί να το πάρει πίσω. Για να βρει έναν τρόπο να το κάνει, θα πρέπει να ζητήσει από όλους τους παραλήπτες να διαγράψουν το email του, το οποίο είναι αρκετά κουραστικό. Έτσι λειτουργεί και το χαρακτηριστικό της αμεταβλητότητας.

Μόλις γίνει η επεξεργασία των δεδομένων στο blockchain , αυτά δεν μπορούν να τροποποιηθούν. Στην περίπτωση του blockchain, αν κάποιος προσπαθήσει να αλλάξει τα δεδομένα ενός μπλοκ, θα πρέπει να αλλάξει ολόκληρο το blockchain που ακολουθεί, καθώς κάθε μπλοκ αποθηκεύει το hash του προηγούμενου μπλοκ. Η αλλαγή σε ένα hash θα οδηγήσει σε αλλαγή όλα τα επόμενα hashes. Είναι πολύ περίπλοκο για κάποιον να αλλάξει όλα τα hashes, καθώς απαιτεί πολλή υπολογιστική ισχύ για να το κάνει. Ως εκ τούτου, τα δεδομένα που αποθηκεύονται στο blockchain δεν είναι ευαίσθητα σε αλλοιώσεις ή επιθέσεις από χάκερ λόγω της αμεταβλητότητας.

Η αμεταβλητότητα, στο πλαίσιο του blockchain, σημαίνει ότι μόλις εισέλθει κάτι στο blockchain, δεν μπορεί να παραβιαστεί. Κάτι τέτοιο θα ήταν ιδιαίτερα πολύτιμο για τα χρηματοπιστωτικά ιδρύματα.

Ο λόγος για τον οποίο το blockchain αποκτά αυτή την ιδιότητα είναι αυτός της κρυπτογραφικής συνάρτησης κατακερματισμού.

Με απλά λόγια, το hashing παίρνει μια συμβολοσειρά εισόδου οποιουδήποτε μήκους και δίνει μια έξοδο σταθερού μήκους. Στο πλαίσιο των cryptocurrencies όπως το bitcoin, οι συναλλαγές λαμβάνονται ως είσοδος και τρέχουν μέσω ενός αλγόριθμου κατακερματισμού (το bitcoin χρησιμοποιεί SHA-256) το οποίο δίνει μια έξοδο σταθερού μήκους.

Θα δειχθεί πώς λειτουργεί η διαδικασία κατακερματισμού, θέτοντας συγκεκριμένες εισόδους. Για αυτή την άσκηση, πρόκειται να χρησιμοποιήθεί ο SHA-256 (Secure Hashing Algorithm 256).

INPUT	HASH
Hi	3639EFCD08ABB273B1619E82E78C29A7DF02C1051B1820E99FC395DCAA3326B8
Welcome to blockgeeks. Glad to have you here.	53A53FC9E2A03F9B6E66D84BA701574CD9CF5F01FB498C41731881BCDC68A7C8

Εικόνα 4: 1ο Παράδειγμα Λειτουργίας του SHA-256 (Rosic, guides/blockchain, 2019)

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

Μια κρυπτογραφική συνάρτηση κατακερματισμού είναι μια ειδική κατηγορία συναρτήσεων κατακερματισμού η οποία έχει διάφορες ιδιότητες καθιστώντας την ιδανική για κρυπτογραφία. Υπάρχουν ορισμένες ιδιότητες που χρειάζεται μια κρυπτογραφική λειτουργία κατακερματισμού προκειμένου να θεωρηθεί ασφαλής.

Υπάρχει μία ιδιότητα που θα μελετηθεί εκτενέστερα και ονομάζεται " Avalanche Effect".

Ακόμα κι αν γίνει μια μικρή αλλαγή στην είσοδο, οι αλλαγές που θα αντικατοπτριστούν στο hash θα είναι τεράστιες. Ας δοκιμαστεί χρησιμοποιώντας το SHA-256:

INPUT	HASH
This is a test	C7BE1ED902FB8DD4D48997C6452F5D7E509FBCDBE2808B16BCF4EDCE4C07D14E
this is a test	2E99758548972A8E8822AD47FA1017FF72F06F3FF6A016851F45C398732BC50C

Εικόνα 5 : 2ο Παράδειγμα Λειτουργίας του SHA-256 (Rosic, guides/blockchain, 2019)

Είναι προφανές πως παρόλο που αλλάχθηκε μόνο το πρώτο γράμμα της εισόδου, επηρεάστηκε και άλλαξε όλο το hash εξόδου.

Τώρα, όπως αναφέρθηκε και σε προηγούμενο σημείο το blockchain είναι μια συνδεδεμένη λίστα που περιέχει δεδομένα και ένα δείκτη κατακερματισμού που δείχνει το προηγούμενο μπλοκ, δημιουργώντας έτσι την αλυσίδα. Ένας δείκτης κατακερματισμού είναι παρόμοιος με έναν δείκτη, αλλά αντί να περιέχει μόνο τη διεύθυνση του προηγούμενου μπλοκ περιέχει επίσης το hash των δεδομένων μέσα στο προηγούμενο μπλοκ.

Αυτή η μικρή τροποποίηση είναι που κάνει τα blockchains τόσο εκπληκτικά και αξιόπιστα.

Ως αποτέλεσμα , αν ένας χάκερ επιτεθεί στο μπλοκ 3 και προσπαθήσει να αλλάξει τα δεδομένα του, τότε λόγω των ιδιοτήτων των συναρτήσεων κατακερματισμού, μια μικρή αλλαγή στα δεδομένα θα αλλάξει δραματικά το hash. Αυτό σημαίνει ότι όλες οι μικρές αλλαγές που έγιναν στο μπλοκ 3, θα αλλάξουν το hash που αποθηκεύεται στο μπλοκ 2, που με τη σειρά του θα αλλάξει τα δεδομένα και το hash του μπλοκ 2 που θα έχει ως αποτέλεσμα αλλαγές στο μπλοκ 1 και ούτω καθεξής . Αυτό θα αλλάξει εντελώς την αλυσίδα, κάτι που είναι αδύνατο. Αυτός ακριβώς είναι ο τρόπος με τον οποίο το blockchain επιτυγχάνει αμεταβλητότητα (Pratap,2018,July).

2.5 Το δίκτυο και οι κόμβοι του blockchain

Το blockchain διατηρείται από ένα δίκτυο peer-to-peer. Το δίκτυο είναι μια συλλογή κόμβων που αλληλοσυνδέονται μεταξύ τους. Οι κόμβοι είναι μεμονωμένοι υπολογιστές που λαμβάνουν εισροή και εκτελούν μια λειτουργία σε αυτούς και δίνουν μια έξοδο. Το blockchain χρησιμοποιεί ένα ειδικό είδος δικτύου που ονομάζεται "δίκτυο peer-to-peer" το οποίο χωρίζει ολόκληρο το φόρτο εργασίας του μεταξύ των συμμετεχόντων, οι οποίοι είναι εξίσου προνομιούχοι και ονομάζονται "peers". Δεν υπάρχει πλέον ένας κεντρικός διακομιστής, τώρα υπάρχουν αρκετοί διανεμημένοι και αποκεντρωμένοι peers (Rosic, guides/blockchain, 2019).

2.5.1 Η χρησιμότητα του peer-to-peer network

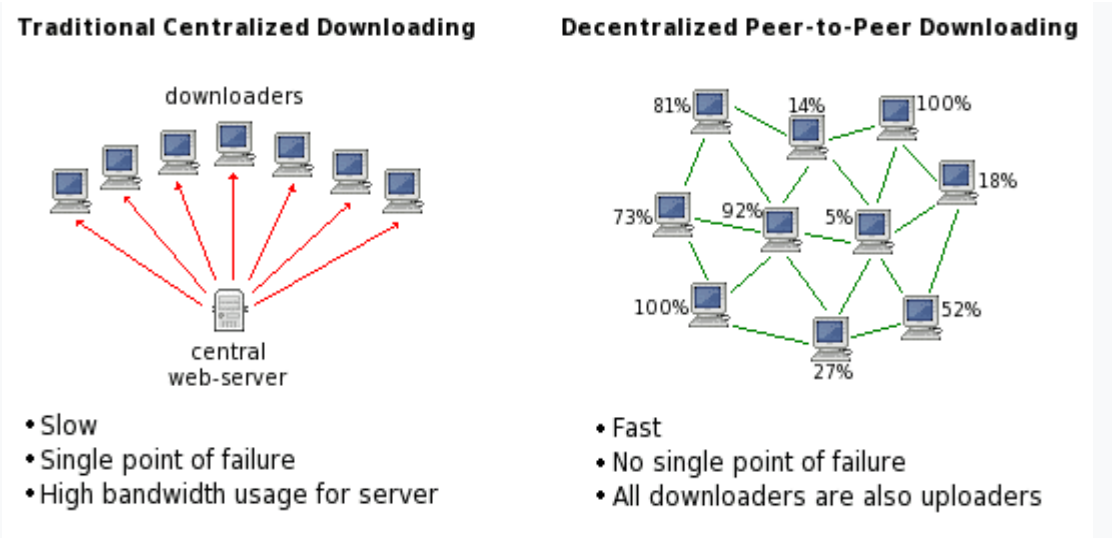
Με τη χρήση του Blockchain, η αλληλεπίδραση μεταξύ δύο μελών ενός peer-to-peer δικτύου επιτυγχάνεται εύκολα χωρίς την απαίτηση τρίτου μέρους. Το Blockchain χρησιμοποιεί πρωτόκολλο P2P το οποίο επιτρέπει σε όλους τους συμμετέχοντες στο δίκτυο να κατέχουν ένα πανομοιότυπο αντίγραφο των συναλλαγών, επιτρέποντας την έγκριση μέσω ενός μηχανισμού ομοφωνίας. Για παράδειγμα, αν ο χρήστης θέλει να πραγματοποιήσει οποιαδήποτε συναλλαγή από ένα μέρος του κόσμου σε άλλο, μπορεί να το κάνει με blockchain μόνος του μέσα σε λίγα δευτερόλεπτα. Επιπλέον, οι τυχόν διακοπές ή επιπλέον χρεώσεις δεν θα αφαιρεθούν κατά τη μεταφορά.

Μία από τις κύριες χρήσεις του δικτύου peer-to-peer είναι η κοινή χρήση αρχείων, που ονομάζεται torrenting. Εάν πρόκειται να χρησιμοποιηθεί ένα μοντέλο πελάτη-διακομιστή για λήψη, τότε είναι συνήθως εξαιρετικά αργό και εξαρτάται εξ ολοκλήρου από την κατάσταση του διακομιστή. Επιπλέον είναι επιρρεπές στη λογοκρισία.

Ωστόσο, σε ένα σύστημα peer-to-peer, δεν υπάρχει κεντρική αρχή και, επομένως, αν κάποιος από τους peers του δικτύου βγει από το δίκτυο, υπάρχουν ακόμα

περισσότεροι χρήστες από τους οποίους μπορεί να γίνει το download. Επιπλέον, δεν υπόκειται στα ιδεαλιστικά πρότυπα ενός κεντρικού συστήματος και άρα δεν είναι επιρρεπές στη λογοκρισία.

Μια σύντομη σύγκριση του παραδοσιακού centralized downloading με το decentralized peer-to-peer downloading δίνεται στην παρακάτω εικόνα:



Εικόνα 6: Σύγκριση του παραδοσιακού centralized downloading με το decentralized peer-to-peer downloading (Rosic, guides/blockchain, 2019)

Η αποκεντρωμένη φύση ενός συστήματος peer-to-peer καθίσταται κρίσιμη. Η απλή (τουλάχιστον σε χαρτί) ιδέα του συνδυασμού αυτού του δικτύου peer-to-peer με ένα σύστημα πληρωμών έχει φέρει επανάσταση στη χρηματοπιστωτική βιομηχανία γεννώντας τα κρυπτονομίσματα (Rosic, guides/blockchain, 2019).

2.5.2 Η χρήση των δικτύων και των κόμβων στα κρυπτονομίσματα

Η δομή του peer-to-peer δικτύου στα κρυπτονομίσματα είναι δομημένη σύμφωνα με τον μηχανισμό ομοφωνίας (consensus mechanism) που χρησιμοποιούν. Για κρυπτονομίσματα όπως το Bitcoin και το Ethereum που χρησιμοποιούν έναν κανονικό proof of work μηχανισμό ομοφωνίας (το Ethereum θα προχωρήσει τελικά στο proof of stake), όλοι οι κόμβοι έχουν το ίδιο προνόμιο. Η ιδέα είναι να δημιουργηθεί ένα δίκτυο ισότητας. Οι κόμβοι δεν έχουν ειδικά προνόμια, ωστόσο οι λειτουργίες και ο βαθμός συμμετοχής τους μπορεί να διαφέρουν. Δεν υπάρχει κεντρικός διακομιστής / οντότητα, ούτε υπάρχει ιεραρχία. Είναι μια επίπεδη τοπολογία.

Αυτά τα αποκεντρωμένα κρυπτονομίσματα είναι δομημένα με αυτόν τον τρόπο για έναν απλό λόγο, να παραμείνουν πιστά στη φιλοσοφία τους. Η ιδέα είναι να

υπάρχει ένα νομισματικό σύστημα, όπου όλοι αντιμετωπίζονται ως ίσοι και δεν υπάρχει κυβερνητικό όργανο, το οποίο να μπορεί να καθορίσει την αξία του νομίσματος με βάση κάποιο συμφέρον. Αυτό ισχύει τόσο για το Bitcoin όσο και για το Ethereum.

Εάν, όμως δεν υπάρχει κεντρικό σύστημα, πώς θα μάθουν όλοι στο σύστημα ότι έχει συμβεί κάποια συναλλαγή; Το δίκτυο ακολουθεί το πρωτόκολλο κουτσομπολιού. Αν η Αλίκη στείλει 3 ETH στον Bob, τότε οι κόμβοι που βρίσκονται πλησιέστερα σε αυτήν θα μάθουν για αυτήν την συναλλαγή και έπειτα θα το πουν στους κόμβους που βρίσκονται πιο κοντά σε αυτούς και έπειτα θα το πουν στους γείτονές τους και αυτό θα συνεχίσει να εξαπλώνεται μέχρι όλοι οι κόμβοι να το μάθουν. Οι κόμβοι είναι βασικά εκείνοι που διαδίδουν το μήνυμα.

Τι είναι τελικά ένας κόμβος στο πλαίσιο του Ethereum; Ένας κόμβος είναι απλά ένας υπολογιστής που συμμετέχει στο δίκτυο Ethereum. Η συμμετοχή αυτή μπορεί να γίνει με τρεις τρόπους:

- Διατηρώντας ένα ρηχό αντίγραφο του blockchain γνωστού ως Light Client.
- Διατηρώντας ένα πλήρες αντίγραφο του blockchain γνωστού ως Full Node.
- Με την επαλήθευση των συναλλαγών γνωστή ως Mining.

Ωστόσο, το πρόβλημα με αυτό το σχέδιο είναι ότι δεν είναι πραγματικά τόσο κλιμακούμενο. Αυτός είναι ο λόγος για τον οποίο πολλά κρυπτονομίσματα νέας γενιάς υιοθετούν έναν μηχανισμό ομοφωνίας με βάση τον ηγέτη (leader-based consensus mechanism). Στην EOS, Cardano, Neo κλπ., οι κόμβοι επιλέγουν κόμβους ηγέτες ή "σούπερ κόμβους" που είναι υπεύθυνοι για την ομοφωνία και τη γενική υγεία του δικτύου. Αυτά τα κρυπτονομίσματα είναι πολύ πιο γρήγορα, αλλά δεν θεωρούνται από τα πιο αποκεντρωμένο συστημάτα.

Έτσι, κατά κάποιο τρόπο, τα κρυπτονομίσματα πρέπει να κάνουν τον συμβιβασμό μεταξύ ταχύτητας και αποκέντρωσης (Rosic, guides/blockchain, 2019) .

2.6 Λόγοι χρήσης του blockchain

Σαν δικτυακή υποδομή, δεν χρειάζεται ο χρήστης να ξέρει για το blockchain για να είναι χρήσιμο στη ζωή του.

Επί του παρόντος, χρηματοοικονομικά προσφέρει τις ισχυρότερες περιπτώσεις χρήσης της τεχνολογίας, όπως για παράδειγμα τα διεθνή εμβάσματα. Η Παγκόσμια Τράπεζα εκτιμά ότι περισσότερα από 430 δισεκατομμύρια δολάρια των ΗΠΑ στάλθηκαν σε μεταφορές χρημάτων το 2015. Και αυτή τη στιγμή υπάρχει μεγάλη ζήτηση για προγραμματιστές blockchain.

Το blockchain ενδεχομένως κόβει τον μεσάζοντα για αυτούς τους τύπους συναλλαγών. Ο προσωπικός υπολογιστής έγινε προσβάσιμος στο ευρύ κοινό με την εφεύρεση του Graphical User Interface (GUI), το οποίο έλαβε τη μορφή "desktop". Ομοίως, το πιο συνηθισμένο GUI που σχεδιάστηκε για το blockchain είναι οι λεγόμενες εφαρμογές "πορτοφόλι" (wallet applications) , τις οποίες οι χρήστες χρησιμοποιούν για να αγοράσουν πράγματα με το Bitcoin και να το αποθηκεύσουν μαζί με τα άλλα κρυπτονομίσματα.

Οι συναλλαγές στο διαδίκτυο συνδέονται στενά με τις διαδικασίες επαλήθευσης ταυτότητας. Είναι εύκολο να φανταστεί κανείς ότι οι εφαρμογές πορτοφολιού (wallet aps) θα μετασχηματιστούν τα επόμενα χρόνια για να συμπεριλάβουν άλλους τύπους διαχείρισης ταυτότητας (Rosic, guides/blockchain, 2019).

2.7 Τύποι του blockchain

Αν και το Blockchain έχει εξελιχθεί σε πολλά επίπεδα από την έναρξή του, υπάρχουν δύο ευρείες κατηγορίες στις οποίες τα blockchains μπορούν να ταξινομηθούν κατά κύριο λόγο, τα Public and Private blockchains. (Aziz, n.d.)

Θα μελετηθεί η διαφορά μεταξύ αυτών των δύο, αλλά πρώτα θα παρουσιαστούν οι ομοιότητες που έχουν το δημόσιο και το ιδιωτικό blockchain:

- Τόσο το δημόσιο όσο και το ιδιωτικό blockchain έχουν peer-to-peer αποκεντρωμένα δίκτυα μεταξύ τους.
- Όλοι οι συμμετέχοντες στο δίκτυο διατηρούν μαζί τους το αντίγραφο του κοινόχρηστου βιβλίου.
- Το δίκτυο διατηρεί αντίγραφα του κοινόχρηστου βιβλίου(ledger) και συγχρονίζει την τελευταία ενημέρωση με τη βοήθεια της ομοφωνίας.
- Οι κανόνες για την αμεταβλητότητα και την ασφάλεια του κοινόχρηστου βιβλίου αποφασίζονται και εφαρμόζονται στο δίκτυο, ώστε να αποφεύγονται οι κακόβουλες επιθέσεις.

Τώρα θα εξεταστεί κάθε τύπος του blockchain ατομικά μαζί με τα πλεονεκτήματα και τα μειονεκτήματά του:

Public blockchain:

Όπως υποδηλώνει και το όνομα, ένα δημόσιο blockchain είναι ένα κοινόχρηστο βιβλίο που δεν απαιτεί άδεια για είσοδο σε αυτό και είναι προσβάσιμο από τον οποιονδήποτε. Οποιοσδήποτε με πρόσβαση στο διαδίκτυο έχει δικαίωμα λήψης και πρόσβασης σε αυτό. Επιπλέον, μπορεί επίσης να ελεγχθεί το συνολικό ιστορικό του blockchain αυτού μαζί με την πραγματοποίηση οποιωνδήποτε συναλλαγών μέσω αυτού. Τα public blockchains συνήθως επιβραβεύουν τους συμμετέχοντες στο δίκτυο για την εκτέλεση της διαδικασίας εξόρυξης(mining process) και τη διατήρηση της αμεταβλητότητας του βιβλίου. Ένα παράδειγμα δημόσιου blockchain είναι το Bitcoin Blockchain.

Τα public blockchains επιτρέπουν στις κοινότητες σε όλο τον κόσμο να ανταλλάσσουν πληροφορίες ανοιχτά και με ασφάλεια. Ωστόσο, ένα προφανές μειονέκτημα αυτού του τύπου blockchain είναι ότι μπορεί να διακυβευτεί εάν οι κανόνες γύρω από αυτόν δεν εκτελούνται αυστηρά. Επιπλέον, οι κανόνες που αποφασίστηκαν και εφαρμόστηκαν αρχικά έχουν πολύ λίγα περιθώρια τροποποίησης στα μεταγενέστερα στάδια.

Πλεονεκτήματα:

- Εμπιστοσύνη: Οι στόχοι του δημοσίου blockchain από την αρχή ήταν να εξαλειφθούν οι μεσάζοντες οποιασδήποτε μορφής και το πιο σημαντικό, επιδιώκει να αφαιρέσει την εμπιστοσύνη που τους έχει τεθεί. Στην πραγματικότητα, οι συμμετέχοντες στο δίκτυο δεν χρειάζεται να εμπιστεύονται ο ένας τον άλλον για την επεξεργασία και την ασφάλεια των συναλλαγών. Οι public blockchains είναι έμπιστες, αφού όλοι έχουν κίνητρο να κάνουν το σωστό για την βελτίωση του δικτύου.

- Ασφαλές: Όσο μεγαλύτερη είναι η αποκέντρωση και η ενεργός συμμετοχή, τόσο πιο ασφαλές θα είναι το blockchain. Με περισσότερους κόμβους στο δίκτυο, θα είναι πολύ πιο δύσκολο για τους κακούς ηθοποιούς να επιτεθούν στο σύστημα. Σε ένα δημόσιο δίκτυο blockchain, οποιοσδήποτε μπορεί να συμμετάσχει ως ένας πλήρης κόμβος ή ανθρακωρύχος και να συμβάλλει στην ασφάλεια του συστήματος. Είναι πρακτικά αδύνατο για τους «κακούς

ηθοποιούς» να συνεννοούνται και να συνεργάζονται για να αποκτήσουν τον έλεγχο του δικτύου ομοφωνίας.

- Ανοιχτό & Διαφανές: Όλα τα δεδομένα που σχετίζονται με τις συναλλαγές είναι ανοιχτά για το κοινό για επαλήθευση. Η διαφάνεια του public blockchain είναι ίσως ένα σημαντικό χαρακτηριστικό που προσελκύει ένα ευρύ φάσμα χρηστών, από ψηφοφορία έως χρηματοοικονομικές συναλλαγές. Επιπλέον, ο καθένας μπορεί να ελέγξει την εγκυρότητα των συναλλαγών και των δεδομένων.

Μειονεκτήματα:

- Αργό: Δεν αποτελεί έκπληξη το γεγονός ότι τα public blockchain χωρίς άδεια πρόσβασης όπως το Bitcoin είναι εξαιρετικά αργά. Το Bitcoin μπορεί να επεξεργαστεί 7 TPS ενώ το Ethereum μπορεί να κάνει 15 TPS. Δεν ταιριάζει με έναν κεντρικό επεξεργαστή πληρωμής, όπως η Visa που μπορεί να κάνει 24.000 TPS. Ένα δημόσιο blockchain είναι αργό, δεδομένου ότι χρειάζεται χρόνος για το σύνολο του δικτύου να επιτευχθεί ομοφωνία σχετικά με την κατάσταση των συναλλαγών, μέσω μηχανισμών ομοφωνίας όπως Bitcoins Proof-of-Work (POW). Υπάρχουν επίσης όρια σχετικά με τον αριθμό των συναλλαγών που μπορούν να χωρέσουν σε ένα μπλοκ και τον χρόνο που απαιτείται για την επεξεργασία ενός μόνο μπλοκ.

- Ανησυχίες επεκτασιμότητας: Επί του παρόντος, τα δημόσια blockchains δεν μπορούν να ανταγωνιστούν τα παραδοσιακά συστήματα που μπορούν να επεξεργάζονται τεράστιες ποσότητες συναλλαγών. Στην πραγματικότητα, όσο περισσότεροι είναι οι συμμετέχοντες και η χρήση, τόσο βραδύτερο ένα δημόσιο blockchain γίνεται δεδομένου ότι ο τεράστιος αριθμός των συναλλαγών θα φράξει το δίκτυο. Ωστόσο, σημειώνεται σημαντική πρόοδος στον χώρο κρυπτογράφησης που στοχεύει στην αντιμετώπιση του ζητήματος της κλιμάκωσης. Διάφορες τεχνολογίες και καινοτομίες σχεδιάζονται και υλοποιούνται για να ενισχύσουν σημαντικά την επεκτασιμότητα των blockchain. Ένα παράδειγμα είναι το δίκτυο Lightcoin's Lightning Network.

- Κατανάλωση ενέργειας: Ο αλγόριθμος ομοφωνίας του Bitcoin - Απόδειξη της εργασίας (proof of work)- χρησιμοποιεί μια σημαντική ποσότητα ηλεκτρικών πόρων για να λειτουργήσει, γεγονός που δημιουργεί ανησυχίες για το περιβάλλον. Στην πραγματικότητα, το Bitcoin χρησιμοποιεί τόση ηλεκτρική ενέργεια όσο και η χώρα της Ιρλανδίας. Ωστόσο, υπάρχουν πολλοί άλλοι μηχανισμοί ομοφωνίας που προσπαθούν να επιτύχουν ομοφωνία δικτύου χωρίς να χρησιμοποιούν τεράστιους πόρους, όπως το Proof of Stake (POS).

Private Blockchain

Σε αντίθεση με τα δημόσια blockchain, τα ιδιωτικά blockchains είναι αυτά που είναι κοινόχρηστα μόνο μεταξύ των εμπιστευμένων συμμετεχόντων. Ο συνολικός έλεγχος του δικτύου βρίσκεται στα χέρια των ιδιοκτητών. Επιπλέον, οι κανόνες ενός ιδιωτικού blockchain μπορούν να τροποποιηθούν ανάλογα με τα διαφορετικά επίπεδα δικαιωμάτων, την έκθεση, τον αριθμό των μελών, την εξουσιοδότηση κ.λπ.

Τα ιδιωτικά blockchains μπορούν να λειτουργούν ανεξάρτητα ή μπορούν να ενσωματωθούν με άλλα blockchains επίσης. Αυτά χρησιμοποιούνται συνήθως από επιχειρήσεις και οργανισμούς. Ως εκ τούτου, το επίπεδο εμπιστοσύνης που απαιτείται μεταξύ των συμμετεχόντων είναι υψηλότερο στα private blockchain.

Πλεονεκτήματα:

- Ταχύτερα: Τα private blockchains μπορούν να επεξεργάζονται πολύ υψηλότερες συναλλαγές ανά δευτερόλεπτο (TPS) σε σύγκριση με τα δημοφιλή blockchains, δεδομένου ότι η ύπαρξη μερικών εξουσιοδοτημένων συμμετεχόντων οδηγεί σε σημαντικά μικρότερους χρόνους στην επίτευξη ομοφωνίας για το δίκτυο. Αυτό επιτρέπει την επεξεργασία περισσότερων συναλλαγών για κάθε μπλοκ. Τα ιδιωτικά blockchains μπορούν να επεξεργαστούν χιλιάδες ή και εκατοντάδες χιλιάδες συναλλαγές ανά δευτερόλεπτο (TPS), σε σύγκριση με τις 7 TPS της Bitcoin.

- Εύχρηστα: Δεδομένου ότι μόνο μερικοί κόμβοι είναι εξουσιοδοτημένοι και υπεύθυνοι για τη διαχείριση των δεδομένων, το δίκτυο είναι σε θέση να υποστηρίζει και να επεξεργάζεται πολύ υψηλότερες συναλλαγές. Σε αντίθεση με ένα αποκεντρωμένο σύστημα, όπου η επίτευξη ομοφωνίας μπορεί να χρειαστεί χρόνο, η διαδικασία λήψης αποφάσεων σε ένα ιδιωτικό δίκτυο είναι πιο συγκεντρωμένη και επομένως πολύ πιο γρήγορη. Μια αναλογία είναι ότι διαρκεί πολύ περισσότερο χρόνο για 100 δασκάλους να βαθμολογήσουν το test ενός μαθητή (και να συμφωνήσουν ότι είναι σωστό / λανθασμένο) σε σύγκριση με έναν μόνο δάσκαλο που το βαθμολογεί.

Μειονεκτήματα:

- Απαίτηση εμπιστοσύνης: Σε αντίθεση με το δημόσιο blockchain που δεν απαιτεί την εμπιστοσύνη κανενός, η ακεραιότητα του ιδιωτικού δικτύου blockchain βασίζεται στην αξιοπιστία των εξουσιοδοτημένων κόμβων. Πρέπει να είναι αξιόπιστοι για να επαληθεύσουν και να επικυρώσουν τις αυθεντικές συναλλαγές. Επιπλέον, η εγκυρότητα των εγγραφών δεν μπορεί να επαληθευτεί ανεξάρτητα. Οι εξωτερικοί παράγοντες πρέπει να

εμπιστεύονται ένα private blockchain χωρίς να έχουν οποιαδήποτε μορφή ελέγχου της διαδικασίας επαλήθευσης. Αυτός είναι ο λόγος για τον οποίο πρέπει να υπάρχει ένας βαθμός εμπιστοσύνης και αξιοπιστίας έναντι των εξουσιοδοτημένων φορέων.

- Ασφάλεια: Με λιγότερους κόμβους, είναι πολύ πιο εύκολο για έναν «κακό ηθοποιό» να αποκτήσει τον έλεγχο του δικτύου και να θέσει σε κίνδυνο ολόκληρο το δίκτυο. Ένα ιδιωτικό δίκτυο είναι πολύ πιο ευάλωτο στους κινδύνους ατυχιών και χειραγώγησης των δεδομένων.

- Κεντροποίηση: Το ιδιωτικό δίκτυο πρέπει να δημιουργηθεί και να συντηρηθεί από το έργο (ή την επιχείρηση) ή από μια κοινοπραξία βιομηχανικών παραγόντων, οι οποίες περιλαμβάνουν τη διατήρηση ενός πολύπλοκου συστήματος διαχείρισης ταυτότητας και πρόσβασης (IAM) για τους χρήστες. Αυτό συχνά οδηγεί σε κεντροποίηση, κάτι που προσπαθούμε ειδικά να αποφύγουμε με το blockchain (Aziz, n.d.).

3 Smart Contracts

3.1 Επεξήγηση των Smart Contracts

Οι έξυπνες συμβάσεις (smart contracts) βοηθούν τον χρήστη να ανταλλάξει χρήματα, ακίνητα, μετοχές ή οτιδήποτε έχει αξία με τρόπο διαφανή, χωρίς συγκρούσεις, αποφεύγοντας παράλληλα τις υπηρεσίες ενός μεσάζοντος.

Ο καλύτερος τρόπος για να περιγραφούν τα έξυπνα συμβόλαια είναι να συγκριθεί η τεχνολογία τους με μια μηχανή αυτόματης πώλησης. Συνήθως, ο χρήστης θα πάει σε δικηγόρο ή συμβολαιογράφο, θα τους πληρώσει και θα περιμένει μέχρι να λάβει το έγγραφο. Με τα έξυπνα συμβόλαια, απλώς ρίχνει ένα bitcoin στο μηχάνημα αυτόματης πώλησης (δηλ. το καθολικό βιβλίο), και η μεσεγγύηση, η άδεια οδήγησης ή οτιδήποτε άλλο πέφτει στο λογαριασμό του. Πιο συγκεκριμένα, οι έξυπνες συμβάσεις όχι μόνο καθορίζουν τους κανόνες και τις κυρώσεις γύρω από μια συμφωνία με τον ίδιο τρόπο που εφαρμόζεται μια παραδοσιακή σύμβαση, αλλά και αυτομάτως επιβάλλουν αυτές τις υποχρεώσεις (Rosic, blockgeeks, 2016).

Ένα smart contract (έξυπνο συμβόλαιο) είναι ένα σύνολο από κώδικα υπολογιστών μεταξύ δύο ή περισσοτέρων μερών που λειτουργούν στην βάση ενός blockchain και αποτελεί ένα σύνολο κανόνων που συμφωνούνται από τα εμπλεκόμενα μέρη. Κατά την εκτέλεση, εάν ικανοποιηθεί αυτό το σύνολο προκαθορισμένων κανόνων, το έξυπνο συμβόλαιο εκτελείται για να παράγει την έξοδο. Αυτό το κομμάτι κώδικα επιτρέπει την αποκεντρωμένη αυτοματοποίηση διευκολύνοντας, επαληθεύοντας και επιβάλλοντας τους όρους μιας υποκείμενης συμφωνίας. Τα έξυπνα συμβόλαια επιτρέπουν στο χρήστη να ανταλλάξει οτιδήποτε έχει αξία , συμπεριλαμβανομένου του χρήματος, των μετοχών, της ιδιοκτησίας κ.λπ., με διαφανή τρόπο, εξαλείφοντας την ανάγκη για έναν μεσάζοντα και διατηρώντας το σύστημα χωρίς συγκρούσεις.

Σε μια κανονική διαδικασία στον κόσμο για την απόκτηση εγγράφου καταχωρημένου στο δικαστήριο ως απόδειξη, θα πρέπει πρώτα ο χρήστης να πάει σε ένα δικηγόρο ή συμβολαιογράφο, να τους δώσει χρήματα με αντάλλαγμα τις υπηρεσίες τους και να περιμένει μέχρι να λάβει το έγγραφο που χρειάζεται. Ωστόσο, το σενάριο αλλάζει εντελώς με τα smart contracts. Όταν τρέχει αυτή τη διαδικασία με smart contracts, απλά παίρνει το έγγραφο της ανάγκης του πληρώνοντας μόνο για αυτό και η διαδικασία θα γίνει χωρίς τη συμμετοχή τρίτου όπως ο δικηγόρος σε αυτή την περίπτωση. Επιπλέον, τα smart contracts δεν περιορίζονται μόνο στον ορισμό των κανόνων για κάθε συμφωνία, αλλά είναι επίσης υπεύθυνα για την αυτόματη εκτέλεση αυτών των κανόνων και υποχρεώσεων.

Συνοπτικά τα smart contract είναι αυτομάτως εκτελέσιμες γραμμές κώδικα που είναι αποθηκευμένες σε ένα blockchain και περιέχουν προκαθορισμένους κανόνες. Όταν πληρούνται αυτοί οι κανόνες, αυτοί οι κώδικες εκτελούνται από μόνοι τους και παρέχουν την έξοδο. Στην απλούστερη μορφή, τα smart contracts είναι

προγράμματα που τρέχουν σύμφωνα με τον τρόπο που έχει ορισθεί από τον δημιουργό τους. Οι έξυπνες συμβάσεις (smart contracts) είναι πιο επωφελείς στις επιχειρηματικές συνεργασίες, στις οποίες χρησιμοποιούνται για να συμφωνήσουν τα εμπλεκόμενα μέρη με τους όρους που αποφασίστηκαν κατά τη συγκατάθεση τους. Αυτό μειώνει τον κίνδυνο απάτης και καθώς δεν υπάρχει τρίτος, το κόστος μειώνεται επίσης.

Τα smart contracts συνήθως λειτουργούν σε μηχανισμό που περιλαμβάνει ψηφιακά περιουσιακά στοιχεία μαζί με πολλαπλά μέρη, όπου οι συμμετέχοντες μπορούν αυτομάτως να διαχειρίζονται τα περιουσιακά τους στοιχεία. Αυτά τα περιουσιακά στοιχεία μπορούν να κατατεθούν και να αναδιανεμηθούν μεταξύ των συμμετεχόντων σύμφωνα με τους κανόνες της σύμβασης. Τα smart contracts έχουν τη δυνατότητα να παρακολουθούν την απόδοση σε πραγματικό χρόνο και να εξοικονομούν κόστος (Rosic, blockgeeks, 2016)

Οι ιδιότητες του smart contract είναι:

- Αυτο-επαληθεύσιμο
- Αυτο-εκτελέσιμο
- Αδύνατο να παραβιαστεί ή να αλλαχθεί

(Prapat, 2018)

3.1.1 Παράδειγμα Smart Contract

Έστω ότι ένας χρήστης νοικιάζει ένα διαμέρισμα από κάποιον άλλον. Μπορεί να το κάνει αυτό μέσω του blockchain πληρώνοντας με κρυπτονόμισμα. Παίρνει μια απόδειξη που κατέχει το εικονικό τους συμβόλαιο. Του δίνεται ακόμη το ψηφιακό κλειδί εισόδου που έρχεται σε εκείνον μέχρι την καθορισμένη ημερομηνία. Αν το κλειδί δεν έχει έρθει στην ώρα του, το blockchain κάνει αυτόματα επιστροφή χρημάτων. Αν σταλεί το κλειδί πριν από την ημερομηνία ενοικίασης, το smart contract κρατά τόσο την αμοιβή όσο και το κλειδί και τα απελευθερώνει στον κάθε χρήστη αντίστοιχα όταν έρθει η ώρα. Το σύστημα λειτουργεί με βάση τη λειτουργία του If-Then και γίνεται μάρτυρας εκατοντάδων ανθρώπων, με αποτέλεσμα μια άψογη παράδοση. Εάν δοθεί το κλειδί στο χρήστη, τότε είναι σίγουρος και ο χρήστης που το ενοικιάζει ότι θα πληρωθεί. Αν σταλεί ένα συγκεκριμένο ποσό σε bitcoins, θα ληφθεί το κλειδί. Το έγγραφο ακυρώνεται αυτόματα μετά την πάροδο του χρόνου και ο κώδικας δεν μπορεί να παρεμβληθεί από τον καθένα από εμάς , καθώς όλοι οι συμμετέχοντες ενημερώνονται ταυτόχρονα.

Μπορεί να χρησιμοποιηθούν έξυπνες συμβάσεις για κάθε είδους καταστάσεις που κυμαίνονται από χρηματοπιστωτικά παράγωγα έως ασφάλιστρα, παραβάσεις συμβάσεων, ιδιοκτησιακό δίκαιο, πιστωτική επιβολή, χρηματοπιστωτικές

υπηρεσίες, νομικές διαδικασίες και συμφωνίες πληθοπορισμού (Rosic, blockgeeks, 2016).

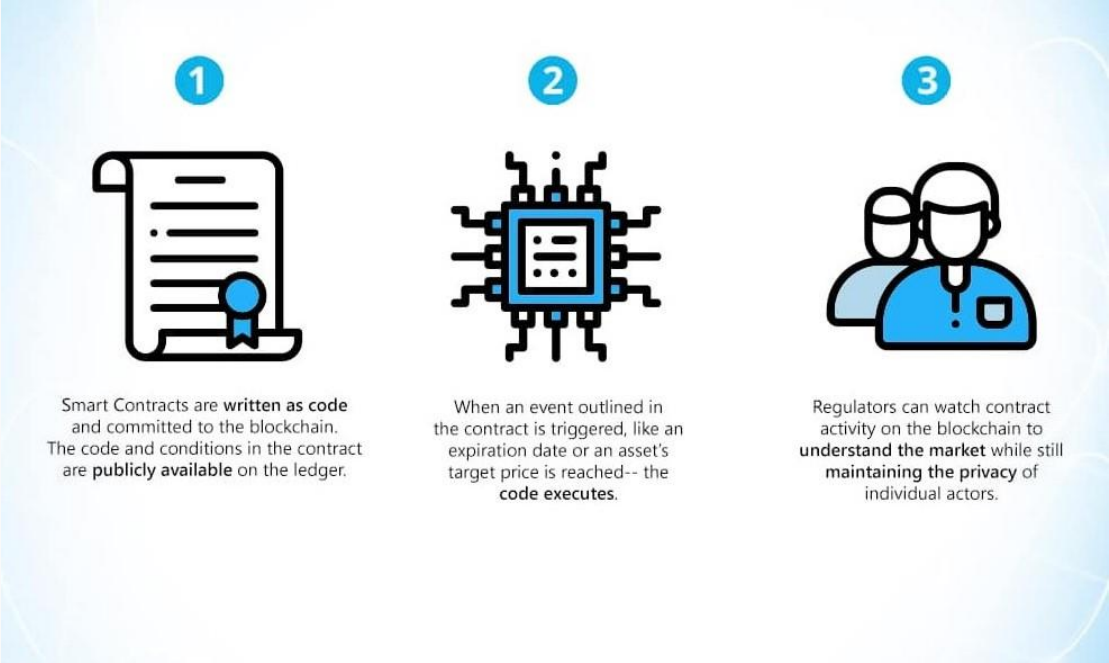
3.2 Λειτουργία του Smart Contract

Για να κατανοηθεί πώς λειτουργεί ένα smart contract, ας θεωρηθεί πως ο χρήστης επιθυμεί να πουλήσει μια δική του ιδιοκτησία. Η διαδικασία πώλησης ακινήτων απαιτεί πολλή γραφειοκρατία καθώς και επικοινωνία με πολλά μέρη. Εκτός από την πολυπλοκότητα της επικοινωνίας, συνεπάγεται επίσης τον κίνδυνο απάτης. Στην σημερινή εποχή, οι περισσότεροι από τους ανθρώπους που θέλουν να ασχοληθούν με ακίνητα το κάνουν μέσα από τους μεσίτες. Εκείνοι είναι υπεύθυνοι για την αντιμετώπιση των εγγράφων και των αγορών. Δρουν ως μεσάζοντες στη συνολική διαδικασία και εργάζονται για τις διαπραγματεύσεις καθώς και εποπτεύουν τη συμφωνία (Prapat, 2018).

Σε τέτοιες περιπτώσεις, ο χρήστης δεν μπορεί να βασίζεται κάθε φορά στο άτομο με το οποίο έρχεται σε επαφή , επομένως, οι οργανισμοί παρέχουν υπηρεσίες μεσεγγύησης που μεταφέρουν τα κεφάλαια από το ένα μέρος στο άλλο. Όταν ολοκληρωθεί η συμφωνία, ο χρήστης θα πρέπει να πληρώσει τόσο στον πράκτορα όσο και στην υπηρεσία μεσεγγύησης την προμήθειά τους με βάση τα καθορισμένα ποσοστά. Αυτό οδηγεί σε επιπλέον απώλεια χρημάτων και σπατάλη χρόνου.

Για τους λόγους αυτούς εισάγονται τα smart contracts . Η χρήση smart contracts σε τέτοιες καταστάσεις μπορεί να έχει οδηγήσει σε μεγαλύτερη αποτελεσματικότητα, μειώνοντας την καθυστέρηση και το κόστος. Τα smart contracts έχουν σχεδιαστεί για να λειτουργούν με βάση την κατάσταση στην οποία βρίσκονται, πράγμα το οποίο θα επιλύσει το ζήτημα της ιδιοκτησίας μεταβιβάζοντάς το στον αγοραστή μόνο όταν συμφωνηθούν οι νομισματικές και άλλες συνθήκες. Επιπλέον, όταν πρόκειται για υπηρεσίες μεσεγγύησης, οι έξυπνες συμβάσεις μπορούν να τις αντικαταστήσουν.

Τόσο τα χρήματα όσο και το δικαίωμα κατοχής του ακινήτου μπορούν να αποθηκευτούν σε ένα κατανεμημένο σύστημα το οποίο μπορεί να προβληθεί από τα εμπλεκόμενα μέρη σε πραγματικό χρόνο. Δεδομένου ότι η μεταφορά χρημάτων θα πιστοποιηθεί από όλους τους συμμετέχοντες στο δίκτυο, εξαλείφονται οι πιθανότητες απάτης. Επιπλέον, δεν υπάρχει καμία πιθανότητα να εμπλακεί ένας μεσάζων, καθώς η εμπιστοσύνη μεταξύ των μερών δεν αποτελεί πια πρόβλημα. Όλες οι λειτουργίες που εκτελεί ο κτηματομεσίτης μπορούν να κωδικοποιηθούν στο smart contract, εξοικονομώντας έτσι ένα σημαντικό χρηματικό ποσό τόσο στον αγοραστή όσο και στον πωλητή (Prapat, 2018).



Εικόνα 7: Λειτουργία του Smart Contract (Rosic, blockgeeks, 2016)

3.3 Τα πλεονεκτήματα και η αναγκαιότητα των Smart Contracts

Με την εφαρμογή των smart contracts στην καθημερινή ζωή, παρουσιάζονται πρωτοφανείς αλλαγές, καθώς προσφέρουν πολλαπλά πλεονεκτήματα έναντι των παραδοσιακών συμβάσεων. Οι έξυπνες συμβάσεις είναι πιο βολικές και γρηγορότερες, καθιστώντας τες αποδεκτές για τους ανθρώπους να απλοποιήσουν τις ροές εργασίας τους (Prapat, 2018).

Παρέχουν το σωστό συνδυασμό ασφάλειας και ευκολίας στην εφαρμογή όπως και πότε πρέπει να ανταλλαχθεί το οτιδήποτε αξίζει, όπως είναι ιδιοκτησία, χρήμα ή κοινή χρήση.

Η εξάλειψη της ανάγκης για μεσάζοντες καθιστά τα smart contracts ακόμη πιο ελκυστικά για να εφαρμοστούν στη ζωή. Η χρήση έξυπνων συμβάσεων είναι πιθανό να αυξηθεί με την πρόοδο της τεχνολογίας. Τα οφέλη που προσφέρουν τα smart contracts είναι:

Διαφάνεια

Ένα από τα βασικά χαρακτηριστικά της τεχνολογίας blockchain, το οποίο μοιράζονται και τα smart contract, είναι η διαφάνεια. Όπως αναφέρθηκε προηγουμένως, οι έξυπνες συμβάσεις πληρούνται με όρους και προϋποθέσεις με απόλυτη λεπτομέρεια, οι οποίες ελέγχονται επίσης από τα μέρη που συμμετέχουν στη συμφωνία.

Αυτό εξαλείφει την πιθανότητα διαφωνίας και προβλημάτων στα μεταγενέστερα στάδια, καθώς οι όροι και οι προϋποθέσεις ελέγχονται διεξοδικά και τίθενται σε εφαρμογή μόνο όταν όλοι οι συμμετέχοντες συμφωνούν με αυτούς. Αυτό το χαρακτηριστικό των έξυπνων συμβάσεων επιτρέπει στα εμπλεκόμενα μέρη να διασφαλίζουν τη διαφάνεια κατά τη διάρκεια των συναλλαγών.

Επιπλέον, η ανάγκη για ακρίβεια στη λεπτομερή περιγραφή των συμβάσεων διατηρεί όλες τις πληροφορίες ανοικτές σε όλους, οι οποίες τελικά επιλύουν οτιδήποτε σχετίζεται με το θέμα της κακής επικοινωνίας. Ως εκ τούτου, με τη βοήθεια των έξυπνων συμβάσεων, μπορεί να αποκατασταθεί η αποτελεσματικότητα σε κενά επικοινωνίας.

Αποδοτικότητα από πλευράς χρόνου

Προκειμένου να πραγματοποιηθεί οποιαδήποτε διαδικασία που περιλαμβάνει τεκμηρίωση, συνήθως διαρκεί περισσότερο από τουλάχιστον δύο ημέρες. Η καθυστέρηση στις διαδικασίες οφείλεται σε πολλούς μεσάζοντες και περιττά βήματα στην πορεία. Από την άλλη πλευρά, οι έξυπνες συμβάσεις τρέχουν μέσω της βοήθειας του διαδικτύου, καθώς δεν είναι παρά κομμάτια κώδικα λογισμικού.

Επομένως, η ταχύτητα ολοκλήρωσης των συναλλαγών μέσα από έξυπνους κώδικες είναι πολύ γρήγορη. Οι έξυπνες συμβάσεις μπορούν να εξοικονομήσουν ώρες ή ακόμα και ημέρες σε σύγκριση με οποιαδήποτε παραδοσιακή επιχειρηματική διαδικασία. Επιπλέον, εξαλείφεται η χρονική καθυστέρηση λόγω της χειρωνακτικής εμπλοκής.

Ακρίβεια

Μια έξυπνη σύμβαση είναι κωδικοποιημένη με μια ρητά λεπτομερή μορφή. Απαιτείται να τηρούνται όλοι οι όροι και προϋποθέσεις πριν τεθεί τελικά στην εργασία. Οποιοσδήποτε όρος που έχει απομείνει εκτός σύμβασης ενδέχεται να οδηγήσει σε σφάλμα κατά την εκτέλεση, συνεπώς κατά τη δημιουργία έξυπνων συμβολαίων, όλες οι προϋποθέσεις τίθενται σε λεπτομερή μορφή.

Εξαιτίας αυτού, το έξυπνο συμβόλαιο γίνεται μια ολοκληρωμένη συμφωνία, η οποία εκτελείται αυτόματα και φέρει εις πέρας όλα όσα έχουν συμφωνηθεί. Στην περίπτωση των χειρωνακτικών συμβάσεων, υπάρχουν πιθανότητες σφαλμάτων, καθώς το πρόσωπο που είναι υπεύθυνο για τη σύναψη μιας σύμβασης ενδέχεται να χάσει κάποιον όρο. Επιπλέον, δεν υπάρχει κανένας τρόπος να εντοπιστεί μέχρι να γίνει το σφάλμα. Ως εκ τούτου, οι έξυπνες συμβάσεις αποτελούν καλύτερη εναλλακτική λύση όσον αφορά την επίτευξη ακρίβειας και ορθότητας.

Ασφάλεια και αποτελεσματικότητα

Οι έξυπνες συμβάσεις με αυτοματοποιημένες λειτουργίες κωδικοποίησης είναι οι ασφαλέστερες επιλογές όταν πρόκειται για κρυπτογραφημένη τεχνολογία δεδομένων στην τρέχουσα εποχή. Δεδομένου ότι ανταποκρίνονται στα υψηλότερα πρότυπα ασφαλείας, το επίπεδο προστασίας που τις χαρακτηρίζει επιτρέπει την ασφαλή χρήση τους για κρίσιμες διαδικασίες.

Επιπλέον, δεδομένου ότι τα έξυπνα συμβόλαια είναι τόσο ακριβή και ασφαλή, το επίπεδο αποτελεσματικότητάς τους είναι υπερβολικά υψηλό και δημιουργεί μεγαλύτερη αξία στις συναλλαγές.

Αποθήκευση Δεδομένων

Οι έξυπνες συμβάσεις είναι ακριβείς ακόμη και στο μικρότερο επίπεδο της συμφωνίας. Όλες οι λεπτομέρειες οποιασδήποτε συναλλαγής αποθηκεύονται στη σύμβαση και οποιοσδήποτε από τους εμπλεκόμενους μπορεί να έχει πρόσβαση σε αυτήν ανά πάσα στιγμή. Επιπλέον, οι συναλλαγές αυτές αποθηκεύονται στο blockchain με τη μορφή μελλοντικών εγγραφών. Αυτό είναι ιδιαίτερα χρήσιμο σε σχέση με τυχόν διαφωνίες σχετικά με τους όρους της σύμβασης στο μέλλον.

Οικονομία χρημάτων

Η χρήση έξυπνων συμβάσεων αντί των παραδοσιακών συμφωνιών μπορεί να έχει ως αποτέλεσμα πολλές αποταμιεύσεις. Πρώτα απ 'όλα, καθώς οι έξυπνες συμβάσεις αφορούν μόνο τα μέρη που αποτελούν μέρος της συμφωνίας, η ανάγκη για μεσάζοντες εξαλείφεται και τα χρήματα που εμπλέκονται σε αυτούς εξοικονομούνται επίσης.

Όλοι οι δικηγόροι, οι μάρτυρες και οι μεσάζοντες δεν έχουν κανένα ρόλο όταν χρησιμοποιούνται έξυπνες συμβάσεις. Επιπλέον, όπως αναφέρθηκε προηγουμένως, οι έξυπνες συμβάσεις εξοικονομούν χρήματα, καθώς τα έγγραφα δεν εμπλέκονται σε καμία διαδικασία.

Εμπιστοσύνη

Οι ιδιότητες της διαφάνειας και της ασφάλειας καθιστούν την έξυπνη σύμβαση αξιόπιστη στις επιχειρήσεις. Καταργούν κάθε πιθανότητα χειραγώγησης καθώς και χειροκίνητα σφάλματα και δημιουργούν εμπιστοσύνη στην εκτέλεσή τους. Μετά από συμφωνία για όλες τις προϋποθέσεις, το συμβόλαιο εκτελείται αυτομάτως.

Ένα άλλο μοναδικό χαρακτηριστικό αυτών των συμβάσεων είναι η ικανότητά τους να μειώνουν σημαντικά την απαίτηση των δικών και τα δικαστήρια. Οι έξυπνες

συμβάσεις αυτοεκτελούνται και επιτρέπουν στα εμπλεκόμενα μέρη να εμπιστεύονται και να δεσμεύονται από τους όρους και τους κανόνες που γράφονται μέσα σε αυτές.

Μη έντυπη μορφή-χωρίς χαρτί

Καθώς τα έξυπνα συμβόλαια είναι κωδικοποιημένα έγγραφα με ηλεκτρονικό υπολογιστή , η χρήση χαρτιού σε όλες τις διαδικασίες εξαλείφεται. Από τη μία πλευρά, αυτό εξοικονομεί το κόστος ενώ από την άλλη, αυτό είναι χρήσιμο για τις εταιρείες παγκοσμίως, καθώς τις βοηθά να αποφύγουν το χαρτί που χρησιμοποιούν για τα συμβόλαια και να προωθήσουν τη συμβολή τους στην κοινωνία (Prapat, 2018).

Αυτονομία

Ο χρήστης είναι εκείνος που κάνει τη συμφωνία. Δεν χρειάζεται να βασιστεί σε έναν μεσίτη, δικηγόρο ή άλλους μεσάζοντες για να εγκριθεί. Παρεμπιπτόντως, αυτό εξαλείφει επίσης τον κίνδυνο χειραγώγησης από τρίτους, δεδομένου ότι η εκτέλεση γίνεται αυτόματα από το δίκτυο και όχι από ένα ή περισσότερα ενδεχομένως προκατειλημμένα άτομα που μπορεί να κάνουν λάθος (Rosic, blockgeeks, 2016).

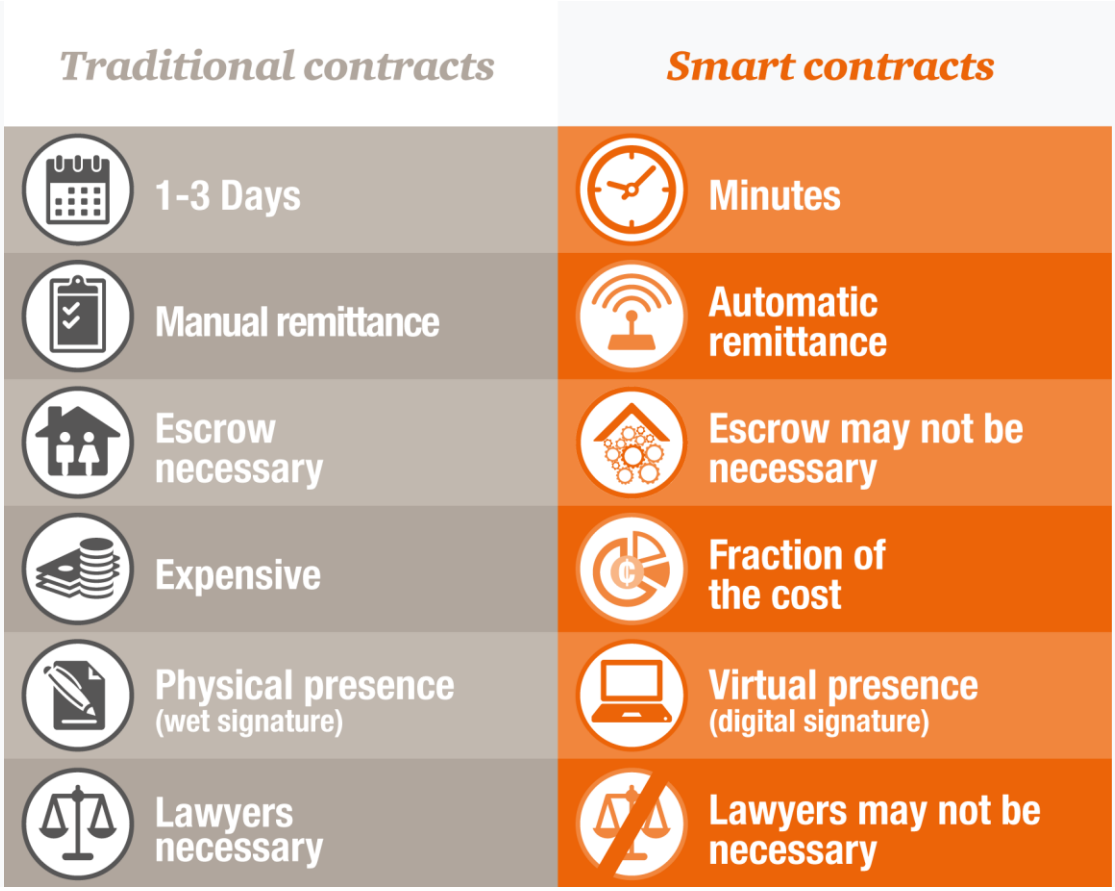
Δημιουργία αντιγράφων ασφαλείας

Υπάρχει περίπτωση η τράπεζα να χάσει τον λογαριασμό ταμιευτηρίου ενός χρήστη. Στο blockchain, κάθε χρήστης έχει πρόσβαση σε όλα τα έγγραφα του καθολικού βιβλίου. Τα έγγραφά του κάθε χρήστη αντιγράφονται πολλές φορές.

Αξιοπιστία-Πίστωση

Τα έγγραφά του χρήστη είναι κρυπτογραφημένα σε ένα καθολικό βιβλίο. Δεν υπάρχει κανένας τρόπος να πει κάποιος ότι τα έχασε (Rosic, blockgeeks, 2016).

Στην παρακάτω εικόνα παρουσιάζονται σύντομα οι διαφορές μεταξύ παραδοσιακών και έξυπνων συμβολαίων: (Morrison, 2016)



Εικόνα 8: Διαφορές μεταξύ παραδοσιακών και έξυπνων συμβολαίων (Morrison, 2016)

3.4 Εφαρμογές των Smart Contracts

Είτε πρόκειται για νέα δουλειά είτε για αγορά νέου προϊόντος, οι συμβατικές συμφωνίες λειτουργούν ως απόδειξη για τέτοια πράγματα. Ωστόσο, η πολύπλοκη διαδικασία παραδοσιακών γραφειοκρατικών εργασιών και συμβάσεων συνεπάγεται υψηλό κόστος, τρίτα μέρη και πιθανότητες χειροκίνητων σφαλμάτων σε τέτοιες διαδικασίες (Prapat, 2018).

Με την ψηφιοποίηση και την τεχνολογική εξέλιξη, μπορούν να γίνουν αυτές οι διαδικασίες πιο αξιόπιστες και οικονομικά αποδοτικές με τη βοήθεια έξυπνων συμβάσεων. Η ιδέα είναι να αποφεύγονται οι μεσάζοντες και τα συστήματα τρίτων και να καταστούν τα συστήματα πιο αποτελεσματικά και αποδοτικά. Οι έξυπνες

συμβάσεις μπορούν να εφαρμοστούν σε διαφορετικές βιομηχανίες και τομείς, όπως αυτοί παρακάτω:

Ασφάλιση

Η έλλειψη αυτοματοποίησης στην ασφαλιστική διοίκηση και η επεξεργασία απαιτήσεων μπορεί να διαρκέσει από εβδομάδες έως μήνες. Αυτό είναι πρόβλημα τόσο για τους πελάτες, όσο και για τις ασφαλιστικές εταιρείες, καθώς οι πελάτες είναι παγιδευμένοι σε χρονικούς περιορισμούς για τα χρήματά τους. Από την άλλη πλευρά, οι εταιρείες πρέπει να αντιμετωπίσουν ζητήματα όπως το ανεπιθύμητο διοικητικό κόστος, τους δυσαρεστημένους πελάτες και την αναποτελεσματικότητα.

Χρησιμοποιώντας Smart Contracts σε τέτοιες διαδικασίες μπορεί να οδηγήσει στην απλούστευση και τον εξορθολογισμό των διαδικασιών με την αυτόματη ενεργοποίηση της πληρωμής για μια απαίτηση, όταν πληρούνται ορισμένες προϋποθέσεις σύμφωνα με τον πελάτη και τη συμφωνία της εταιρείας. Για παράδειγμα, σε περίπτωση απώλειας λόγω φυσικής καταστροφής, οι έξυπνες συμβάσεις μπορούν να εκτελεστούν έγκαιρα και οι άνθρωποι μπορούν να διεκδικήσουν τα χρήματά τους και να τα χρησιμοποιήσουν σε χρόνο ανάγκης. Οποιεσδήποτε συγκεκριμένες λεπτομέρειες, όπως η έκταση της απώλειας λόγω ζημιάς, μπορούν να διατηρηθούν σε ένα blockchain και το ποσό της αποζημίωσης μπορεί να αποφασιστεί αναλόγως.

Internet of Things (IoT)

Η τεχνολογία IoT χρησιμοποιείται για τη σύνδεση καθημερινών συσκευών στο Διαδίκτυο, προκειμένου να βελτιωθεί η διασύνδεση των συστημάτων με τη βοήθεια αισθητήρων. Αυτές οι συσκευές μπορούν να συνδεθούν στο σύστημα του blockchain για να ακολουθήσουν τα ίχνη όλων των προϊόντων και διαδικασιών στον βρόχο. Για παράδειγμα, σε ένα γενικό σενάριο, ενδεχομένως να ληφθεί μια λανθασμένη παραγγελία, ενώ γίνονται αγορές online, αλλά με το συνδυασμό Blockchain και IoT, το προϊόν και η θέση του μπορούν να παρακολουθούνται σε κάθε βήμα της διαδρομής, συμπεριλαμβανομένης της αποθήκευσης, μεταφοράς, και της αποστολής στον ζητούμενο προορισμό. Ένα πλήρως αυτοματοποιημένο σύστημα θα διασφαλίσει ότι το σωστό προϊόν θα παραδοθεί στο σωστό άτομο.

Οι αισθητήρες που συμμετέχουν στο σύστημα δημιουργούν τους δικούς τους κόμβους στο blockchain και με τη βοήθεια έξυπνων συμβολαίων, εντοπίζεται η θέση και η κατοχή του αντίστοιχου προϊόντος. Ένα έξυπνο συμβόλαιο διατηρεί την κατάσταση της τοποθεσίας ενημερωμένη καθ 'όλη τη διαδρομή μέχρι να παραδοθεί το προϊόν. Αυτό βοηθά στη διασφάλιση της ορθότητας του προϊόντος από την αρχική αποστολή έως την παράδοση.

Στεγαστικά Δάνεια

Οι συμφωνίες υποθηκών είναι περίπλοκες, καθώς πολλές λεπτομέρειες περιλαμβάνονται σε αυτές, όπως το εισόδημα του ενυπόθηκου δανειστή, η πιστοληπτική του ικανότητα καθώς και τα έξοδα. Προκειμένου να πάρει ο χρήστης στεγαστικό δάνειο, είναι απαραίτητο να διεξαχθούν οι έλεγχοι αυτών των λεπτομερειών. Αυτή η διαδικασία πηγαίνει συχνά στα χέρια διαμεσολαβητών και τρίτων, γεγονός που την καθιστά μακρά και ενοχλητική για τον δανειστή καθώς και για τον δανειολήπτη.

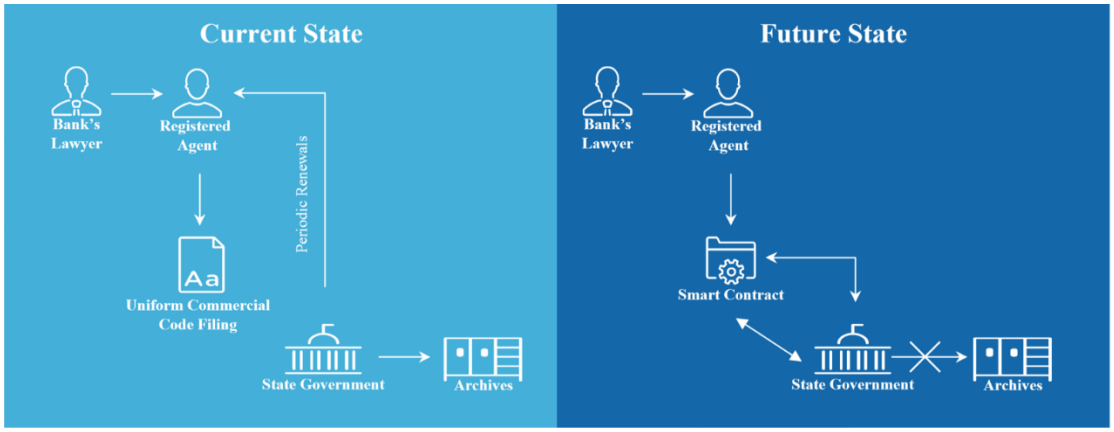
Η χρήση έξυπνων συμβολαίων σε αυτή την περίπτωση είναι ευεργετική λόγω πολλών λόγων. Ο σημαντικότερος είναι η εξάλειψη των μεσαζόντων για να αποφευχθεί οποιαδήποτε μακροχρόνια διαδικασία και σύγχυση. Επιπλέον, όλες οι λεπτομέρειες μπορούν να αποθηκευτούν σε μια θέση που είναι προσβάσιμη από αμφότερα τα μέρη ανά πάσα στιγμή.

Συμβάσεις Εργασίας

Οι συμβάσεις εργασίας είναι ένας άλλος τομέας στον οποίο απαιτούνται smart contracts. Εάν κάποιος από τους συμβαλλομένους, δηλαδή ο εργοδότης ή ο υπάλληλος, δεν ανταποκρίνεται στις απαιτήσεις που έχουν τεθεί, οι όροι της συμφωνίας μπορούν να τεθούν σε κίνδυνο . Αυτό οδηγεί σε έλλειψη εμπιστοσύνης που επιλύεται με έξυπνες συμβάσεις. Χρησιμοποιώντας ένα ενιαίο έξυπνο συμβόλαιο και για τα δύο μέρη, μπορούν να καταστούν σαφείς οι όροι και οι προϋποθέσεις που θα συμβάλουν στη βελτίωση της δικαιοσύνης. Αυτά τα αρχεία θα μπορούσαν να είναι οτιδήποτε όπως το ποσό μισθού, οι εργασιακές ευθύνες κλπ. Μόλις οι συναλλαγές αυτές καταγραφούν σε έξυπνες συμβάσεις, μπορούν να εξεταστούν σε περίπτωση οποιασδήποτε σύγκρουσης. Αυτό θα βελτιώσει τη σχέση των εργαζομένων με τον εργοδότη.

Επιπλέον, οι έξυπνες συμβάσεις μπορούν να χρησιμοποιηθούν για να διευκολύνουν την επεξεργασία των μισθών έτσι ώστε ο ενδιαφερόμενος εργαζόμενος να λάβει το συμφωνηθέν ποσό σε μια συγκεκριμένη χρονική περίοδο. Επίσης, στην περίπτωση προσωρινής εργασίας, όπου εμπλέκεται ο εργοδότης, ο εργαζόμενος και ένας οργανισμός, μπορούν να χρησιμοποιηθούν έξυπνες συμβάσεις για την εισαγωγή διαφάνειας. Αυτό θα εμποδίσει τους οργανισμούς να παρεμβαίνουν στους όρους εργασίας του μισθωτού όταν αυτός μισθωθεί από την εταιρεία. Οποιεσδήποτε αλλαγές στους όρους μπορούν να εντοπιστούν με τη βοήθεια έξυπνων συμβάσεων.

Προστασία περιεχομένου με πνευματικά δικαιώματα



Εικόνα 9: Προστασία περιεχομένου με πνευματικά δικαιώματα (Prapat, 2018)

Στον ψηφιακό κόσμο του σήμερα, το περιεχόμενο δεν περιορίζεται μόνο σε λέξεις. Θα μπορούσε να είναι από ένα γραπτό έγγραφο έως ένα βίντεο ή ένα κλιπ ήχου. Όταν ένα κομμάτι περιεχομένου κυκλοφορεί εμπορικώς, ο κάτοχος του περιεχομένου λαμβάνει μια θεωρητική αμοιβή. Ωστόσο, η διαδικασία της δημιουργίας εμπλέκει πολλαπλά μέρη και, ως εκ τούτου, όλοι είναι υπεύθυνοι για πληρωμές ή πνευματικά δικαιώματα. Στην πράξη, αυτό δεν διασφαλίζεται, καθώς δεν υπάρχει κανένας καθορισμένος τρόπος για την εκκαθάριση της σύγχυσης ως προς το δικαίωμα. Οι έξυπνες συμβάσεις μπορούν να επιλύσουν κάτι τέτοιο, εξασφαλίζοντας τα πνευματικά δικαιώματα στον επιθυμητό συνεισφέροντα, καταγράφοντας την ιδιοκτησία του στο blockchain.

Εφοδιαστική Αλυσίδα (Supply Chain)

Η διαχείριση της αλυσίδας εφοδιασμού περιλαμβάνει τη ροή αγαθών και προϊόντων από το αρχικό στάδιο μέχρι το τελικό στάδιο. Ως σημαντικό μέρος πολλών βιομηχανιών, η εύρυθμη λειτουργία μιας αλυσίδας εφοδιασμού είναι ζωτικής σημασίας για τις επιχειρήσεις. Η διαχείριση της αλυσίδας εφοδιασμού δεν είναι δουλειά ενός ατόμου και έτσι υπάρχουν διάφορες οντότητες που εμπλέκονται σε αυτήν. Οι έξυπνες συμβάσεις στην αλυσίδα εφοδιασμού μπορούν να καταγράφουν δικαιώματα ιδιοκτησίας ενώ τα προϊόντα μεταφέρονται μέσω της αλυσίδας εφοδιασμού. Όλοι στο δίκτυο μπορούν να παρακολουθήσουν τη θέση του προϊόντος ανά πάσα στιγμή.

Το τελικό προϊόν μπορεί να ελεγχθεί σε κάθε στάδιο σε όλη τη διαδικασία παράδοσης μέχρι να φτάσει στον τελικό πελάτη. Εάν ένα στοιχείο χαθεί στην πορεία μπορούν να χρησιμοποιηθούν έξυπνες συμβάσεις για την ανίχνευση της θέσης του. Επίσης, αν κάποιος εταίρος δεν εκπληρώσει τους όρους της σύμβασης, θα είναι διαφανές για το σύνολο του συστήματος να το δει. Οι έξυπνες συμβάσεις φέρνουν τη διαφάνεια στο συνολικό σύστημα αλυσίδας εφοδιασμού.

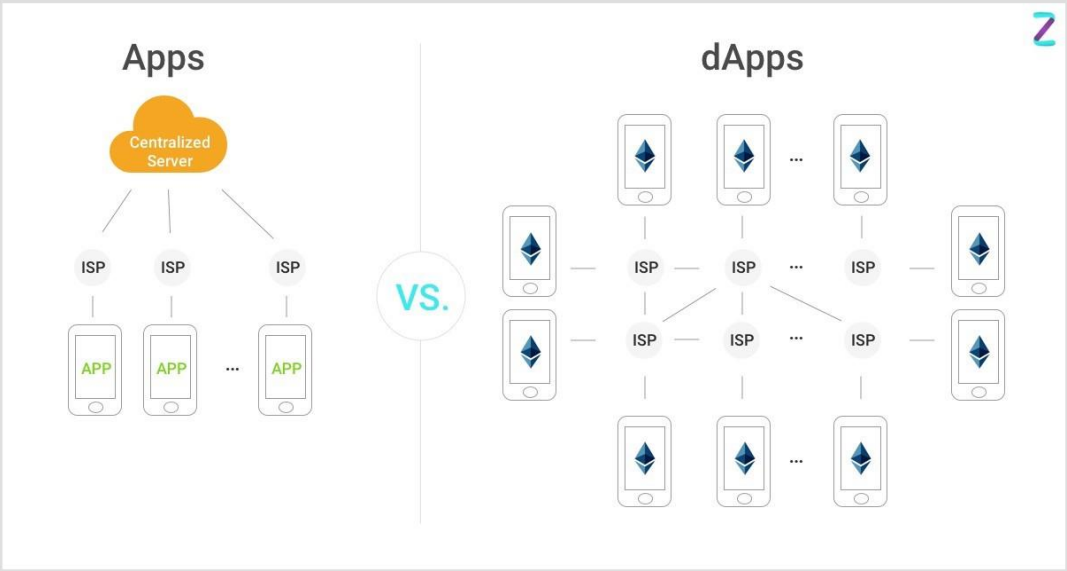
Οι έξυπνες συμβάσεις έχουν ορισμένα πλεονεκτήματα σε πολλούς τομείς της βιομηχανίας, όπως η μείωση των γενικών εξόδων, η διαφάνεια και η εξοικονόμηση χρόνου. Ενώ είναι πιο έμπιστες, ασφαλείς, αποτελεσματικές και αξιόπιστες σε σύγκριση με τα συμβόλαια χαρτιού, πρέπει να ληφθεί μέριμνα για την αποφυγή των κινδύνων διαφθοράς του κώδικα. Καθώς οι επιχειρήσεις προχωρούν προς τα εμπρός και αποδέχονται τις ψηφιακές διαδικασίες, η επίγνωση του κινδύνου είναι αναπόσπαστη (Prapat, 2018).

3.5 Blockchains όπου μπορούν να επεξεργαστούν τα Smart Contracts

- Bitcoin: Το Bitcoin είναι ιδανικό για την επεξεργασία συναλλαγών Bitcoin, αλλά έχει περιορισμένη δυνατότητα επεξεργασίας εγγράφων.
- Side Chains: Αυτό είναι ένα άλλο όνομα για blockchains που τρέχουν δίπλα στο Bitcoin και προσφέρουν περισσότερα περιθώρια επεξεργασίας συμβολαίων.
- NXT: NXT είναι μια δημόσια πλατφόρμα blockchain που περιέχει μια περιορισμένη επιλογή των προτύπων για έξυπνες συμβάσεις. Ο χρήστης πρέπει να χρησιμοποιήσει την πλατφόρμα που του δίνεται και δεν μπορεί να κωδικοποιήσει τη δική του.
- Ethereum: Το Ethereum είναι μια δημόσια πλατφόρμα και η πιο προηγμένη για την κωδικοποίηση και την επεξεργασία έξυπνων συμβάσεων. Ο χρήστης μπορεί να κωδικοποιήσει ό, τι επιθυμεί αλλά θα πρέπει να πληρώσει για υπολογιστική ισχύ με μάρκες "ETH" (Rosic, blockgeeks, 2016).

4 Dapps

4.1 Επεξήγηση των Dapps (Decentralized Applications)



Εικόνα 10: Apps vs dApps (Pratik, 2018)

Ο τεχνολογικός κόσμος είναι ένα από τα πιο δυναμικά τμήματα σε ολόκληρο το σύμπαν. Πολλοί τεχνολογικοί πυλώνες, πλαίσια και γλώσσες είναι διαθέσιμα για την ανάπτυξη μιας εφαρμογής, αλλά ακόμα, οι προγραμματιστές δεν είναι σίγουροι για ένα ενιαίο πλαίσιο που μπορεί να προσφέρει τα καλύτερα αποτελέσματα.

Καθώς ο κόσμος προσαρμόζεται σε συμβατικές εφαρμογές, όλο το οικοσύστημα εξελίσσεται επίσης. Οι εφαρμογές dApps ή αποκεντρωμένες εφαρμογές είναι μια νέα σειρά εφαρμογών που δεν ελέγχονται ή ανήκουν σε μία μόνο αρχή, δεν μπορούν να κλείσουν ή δεν μπορούν να έχουν διακοπή λειτουργίας.

Η ιδέα του dApp βρίσκεται ακόμα στο στάδιο της εκμάθησης. Η εξήγηση του σε μία γραμμή είναι δύσκολη επειδή δεν υπάρχει συγκεκριμένος ορισμός που να ταιριάζει με όλα τα χαρακτηριστικά που κάνουν μια εφαρμογή μια αποκεντρωμένη εφαρμογή. Σαν dApp απαιτείται μια εφαρμογή να παρουσιάζει τα ακόλουθα τέσσερα χαρακτηριστικά:

- Ανοικτή πηγή: Το πρώτο και κύριο χαρακτηριστικό είναι ότι τέτοιες εφαρμογές θα πρέπει να διαθέτουν τον πυρήνα του πηγαίου κώδικα για όλους. Δεδομένου ότι τα βασικα χαρακτηριστικα των dApps είναι η αυτονομία και η ομόφωνη συναίνεση, ουσιαστικά οι αλλαγές πρέπει να αποφασιστούν από το σύνολο ή την πλειοψηφία των χρηστών. Επίσης, ο κώδικας θα πρέπει να είναι διαθέσιμος σε όλους για έλεγχο.

- Αποκεντρωμένη φύση: Όπως υποδηλώνει το όνομα, οι αποκεντρωμένες εφαρμογές αποθηκεύουν τα πάντα σε ένα αποκεντρωμένο blockchain ή οποιαδήποτε κρυπτογραφική τεχνολογία για να σώσουν την εφαρμογή από τους κινδύνους της κεντρικής εξουσίας και να τονίσουν την αυτόνομη φύση.

- Ενθάρρυνση/ Κίνητρο: Καθώς η εφαρμογή βασίζεται στο αποκεντρωμένο blockchain, οι επικυρωτές των συναλλαγών στο δίκτυο πρέπει να επιβραβεύονται με κρυπτογραφικά νομίσματα ή οποιαδήποτε μορφή ψηφιακού στοιχείου που έχει αξία.

- Αλγόριθμος: Η αποκεντρωμένη εφαρμογή πρέπει να έχει έναν μηχανισμό συναίνεσης που απεικονίζει την απόδειξη αξίας (proof of value) στο κρυπτογραφικό σύστημα. Ουσιαστικά, αυτό προσδίδει αξία στο κρυπτογραφικό νόμισμα και δημιουργεί ένα πρωτόκολλο συναίνεσης σύμφωνα με το οποίο οι χρήστες συμφωνούν να παράγουν πολύτιμες κρυπτογραφικά μάρκες.

Τώρα που αναφέρθηκαν τα χαρακτηριστικά, θα δοθεί ένας ορισμός που θα βοηθήσει να εντοπιστούν παραδείγματα πραγματικής ζωής. Ουσιαστικά, το dApp είναι μια εφαρμογή που λειτουργεί σε αποκεντρωμένο δίκτυο P2P που διέπεται από όλα τα μέλη και όχι από μία κεντρική αρχή (Pratik, 2018).

4.2 Τα Dapps στον πραγματικό κόσμο

Σύμφωνα με τα παραπάνω, προκύπτει ότι το πρώτο γνωστό dApp στον κόσμο ήταν το Bitcoin. Δημοφιλές ως το αποκορύφωμα του κρυπτονομίσματος , το bitcoin λύνει το ζήτημα της συγκέντρωσης και δίνει στους χρήστες τη δυνατότητα να εκτελούν συναλλαγές χωρίς κανένα μεσάζοντα ή κεντρική αρχή μέσω ενός αυτοσυντηρούμενου δημόσιου βιβλίου. Προχωρώντας στην περίπτωση χρήσης αποκεντρωμένων εφαρμογών, μπορούμε να ταξινομήσουμε αυτές τις εφαρμογές με βάση το σενάριο στο οποίο μπορούν να καταταχθούν. Αυτή η ταξινόμηση κατατάσσει τα dApps σε τρία τμήματα που είναι επίσης πιθανές περιπτώσεις χρήσης:

- **Διαχείριση χρημάτων & μεταφορά**

  Οι αποκεντρωμένες εφαρμογές μπορούν να χρησιμοποιηθούν για την εξομάλυνση της μεταφοράς χρημάτων στον κόσμο. Έχουμε ήδη δει τα οφέλη με τη μορφή επιτυχίας bitcoin και άλλων cryptocurrencies. Χρησιμοποιώντας το δίκτυο blockchain και το δικό του κρυπτογραφικό σήμα, το dApp μπορεί να επιταχύνει τη διαχείριση χρημάτων, τη μεταφορά και το δανεισμό εξαλείφοντας τους μεσάζοντες και ενισχύοντας την ασφάλεια λόγω του μηχανισμού συναίνεσης που είναι αδύνατον να αλλάξει χωρίς πλειοψηφία.

- **Διαχείριση Επιχειρησιακών Διαδικασιών**

  Οι εταιρείες μπορούν να ενσωματώσουν αποκεντρωμένες εφαρμογές για να διευκολύνουν τις διαδικασίες χωρίς ανθρώπινη παρέμβαση. Με τη βοήθεια έξυπνων συμβολαίων, ενός ουσιαστικού γραναζιού στο δίκτυο blockchain, μπορούν να επιλυθούν κρίσιμα ζητήματα και να βελτιωθεί η αποτελεσματικότητα της διαδικασίας. Για παράδειγμα, οι λογιστικές εταιρείες μπορούν να ενσωματώσουν τσιπ RFID στην αποστολή τους, τα οποία μπορούν να σαρωθούν στους λιμένες προορισμού, από τους οποίους η πληρωμή μπορεί να διευθετηθεί αυτόματα μέσω μιας έξυπνης σύμβασης μεταξύ αγοραστή και πωλητή.

- **DAO (Αποκεντρωμένος Αυτόνομος Οργανισμός)**
  (Decentralized Autonomous Organization)

  Το DAO είναι ένα εντελώς νέο φαινόμενο της έναρξης απρόσωπων οργανώσεων χωρίς ηγέτες. Οι οργανώσεις αυτές μπορούν να λειτουργούν ως εταιρικές και να εκτελούνται μέσω κανόνων που ορίζονται από γλώσσες προγραμματισμού στο blockchain. Πώς τα μέλη θα ψηφίσουν, σε ποιο επιχειρηματικό τμήμα θα λειτουργήσει ο οργανισμός, ποιοι μπορούν να είναι μέλη, πώς θα ανταλλάσσεται το κρυπτονόμισμα, όλα μπορούν να προγραμματιστούν στο blockchain που θα λειτουργήσει ο οργανισμός. Οι οργανισμοί αυτοί δεν μπορούν να σταματήσουν μόλις αναπτυχθούν και μπορούν να δουλέψουν παγκοσμίως. (Pratik, 2018).

4.3 Τρόπος ανάπτυξης ενός dapp

Όπως σε κάθε νέα τεχνολογία προγραμματισμού, υπάρχει ένα ευρύ φάσμα επιλογών κωδικοποίησης και πλατφόρμες που οι προγραμματιστές μπορούν να αξιοποιήσουν ενώ σκέφτονται να αναπτύξουν αποκεντρωμένες εφαρμογές. Εάν ο χρήστης πρέπει να αναπτύξει ένα dApp για τον ίδιο, πρέπει να έχει τα κατάλληλα εργαλεία, συστατικά και πλαίσια για την επιτυχία. Στον παρακάτω πίνακα συγκρίνεται η ανάπτυξη του dApp με την συμβατική ανάπτυξη εφαρμογής και παρουσιάζεται ό, τι χρειάζεται για να δημιουργηθεί μια αποκεντρωμένη εφαρμογή:

	Web 2.0	Web 3.0 (dApps)
Scalable Computation	Amazon EC2	Ethereum, Truebit
File Storage	Amazon S3	IPFS/Filecoin, Storj
External Data	3rd Party APIs	Oracles (Augur)
Monetization	Ads, Selling Products	Token Model
Payments	Credit Cards, Paypal	Ethereum, Bitcoin, state channels, 0x

Source : www.intuz.com

Εικόνα 11: Σύγκριση ανάπτυξης συμβατικής εφαρμογής εναντίον αποκεντρωμένης (Pratik, 2018)

Τα dApps βασίζονται σε κώδικα backend που λειτουργεί σε δίκτυο P2P. Σε σύγκριση με τις συμβατικές εφαρμογές, αυτή είναι μια σημαντική διαφορά, καθώς το backend κανονικής εφαρμογής τρέχει σε έναν κεντρικό διακομιστή. Όταν πρόκειται για το frontend, ο κώδικας μπορεί να γραφτεί σε οποιαδήποτε γλώσσα προγραμματισμού. Χρησιμοποιώντας ένα API, το frontend καλεί το backend σε περίπτωση αποκεντρωμένων εφαρμογών. Επίσης, το frontend μπορεί να φιλοξενείται σε ένα αποκεντρωμένο σύστημα αποθήκευσης όπως το IPFS.

Τώρα που παρατηρήθηκε πόσο διαφορετική είναι η ανάπτυξη μιας αποκεντρωμένης εφαρμογής σε σχέση με μια κανονική εφαρμογή, ας παρουσιαστούν τα πλεονεκτήματα της επιλογής των dApps έναντι εφαρμογών που είναι διαχειρίσιμες μέσω κεντρικών διακομιστών (Pratik, 2018).

4.4 Πλεονεκτήματα των dapps σε σχέση με τις συμβατικές εφαρμογές

Τα dApps προάγουν την αποκέντρωση, καθιστώντας τα απαραβίαστα και τα αρχεία αναλλοίωτα. Καθώς τα dApps βασίζονται σε ένα ασφαλές δίκτυο blockchain, τέτοιες εφαρμογές προωθούν ένα υψηλό επίπεδο ασφάλειας και είναι αμετάβλητες από τα hacks και τις εισβολές. Μερικά από τα πλεονεκτήματά τους είναι:

- Ταχύτερη και πιο επεξεργασμένη πληρωμή χωρίς να χρειάζεται να ενσωματωθεί η πύλη πληρωμών για την αποδοχή χρημάτων.

- Υψηλά επίπεδα ασφάλειας δεδομένων λόγω των έξυπνων συμβολαίων που διέπονται από ιδιωτικά κλειδιά.

- Μεγαλύτερη ανωνυμία χωρίς να χρειάζεται οι χρήστες να ακολουθήσουν τη μακρά διαδικασία εγγραφής.

- Αξιόπιστες καταγραφές δεδομένων, καθώς οι χρήστες μπορούν να έχουν πρόσβαση στο δημόσιο blockchain για να επαληθεύσουν τις πληροφορίες συναλλαγών (Pratik, 2018).

5 Ethereum

5.1 Ανάλυση του Ethereum

Το Ethereum είναι μια παγκόσμια, αποκεντρωμένη πλατφόρμα για χρήματα και νέες εφαρμογές. Στο Ethereum, ο χρήστης μπορεί να γράψει κώδικα που ελέγχει τα χρήματα και να δημιουργήσει εφαρμογές που είναι προσβάσιμες οπουδήποτε στον κόσμο.

Παρόλο που συνήθως συνδέεται με το Bitcoin, η τεχνολογία blockchain έχει πολλές άλλες εφαρμογές που ξεπερνούν τα ψηφιακά νομίσματα. Στην πραγματικότητα, το Bitcoin είναι μόνο μία από τις εκατοντάδες εφαρμογές που χρησιμοποιούν τεχνολογία blockchain σήμερα.

Μέχρι πρόσφατα, οι εφαρμογές blockchain απαιτούσαν πολύπλοκο υπόβαθρο στην κωδικοποίηση, την κρυπτογραφία, τα μαθηματικά καθώς και σημαντικούς πόρους. Αλλά οι εποχές έχουν αλλάξει. Παλαιότερα εφαρμογές, όπως ηλεκτρονικές ψηφοφορίες και ψηφιακά καταγεγραμμένα περιουσιακά στοιχεία μέχρι κανονιστική συμμόρφωση και διαπραγμάτευση, τώρα αναπτύσσονται και εξελίσσονται πιο γρήγορα από ποτέ. Παρέχοντας στους προγραμματιστές τα εργαλεία για την ανάπτυξη αποκεντρωμένων εφαρμογών, το Ethereum τα κάνει όλα αυτά δυνατά (Rosic, guides/ethereum, 2019)

5.2 Βασικά ιστορικά σημεία του Ethereum

- Νοέμβριος 2013: Ο Vitalik Buterin δημοσιεύει το whitepaper του Ethereum.
- Ιανουάριος 2014: Η ανάπτυξη της πλατφόρμας Ethereum ανακοινώνεται δημοσίως. Η αρχική ομάδα ανάπτυξης του Ethereum αποτελούντο από τον Vitalik Buterin, τον Mihai Alisie, τον Anthony Di Iorio και τον Charles Hoskinson.
- Αύγουστος 2014: Το Ethereum τερματίζει το ICO και φτάνει τα 18,4 εκατομμύρια δολάρια.
- Μάιος 2015: "Ολυμπιακή" η δοκιμαστική έκδοση του Ethereum.
- 30 Ιουλίου 2015: Το πρώτο στάδιο της ανάπτυξης του Ethereum, "Frontier" κυκλοφόρησε.

- 14 Μαρτίου 2016: Η Homestead, η πρώτη "σταθερή" έκδοση Ethereum, βγήκε στο μπλοκ 1,150,000.

- Ιούνιος 2016: Η επίθεση DAO από hackers συμβαίνει και η αξία 50 εκατομμυρίων δολαρίων χάνεται, η οποία ήταν το 15% της συνολικής αξίας που κυκλοφόρησε την εποχή εκείνη.

- 25 Οκτωβρίου 2016: Το Ethereum Classic διακλαδίζεται μακριά από το αρχικό πρωτόκολλο Ethereum.

- 16 Οκτωβρίου 2017: Η ενήμερωση του Metropolis Bizantum hardfork συμβαίνει.

- 28 Φεβρουαρίου 2019: Η ενημέρωση του Metropolis Constantinople hardfork πραγματοποιείται.

Στην απλούστερη, το Ethereum είναι μια ανοιχτή πλατφόρμα λογισμικού που βασίζεται στην τεχνολογία blockchain και επιτρέπει στους προγραμματιστές να δημιουργήσουν και να αναπτύξουν αποκεντρωμένες εφαρμογές.

Όπως και το Bitcoin, το Ethereum είναι ένα κατανεμημένο δημόσιο δίκτυο blockchain . Αν και υπάρχουν κάποιες σημαντικές τεχνικές διαφορές μεταξύ των δύο, η σημαντικότερη διάκριση που πρέπει να σημειωθεί είναι ότι το Bitcoin και το Ethereum διαφέρουν ουσιαστικά ως προς το σκοπό και την ικανότητά τους. Το Bitcoin προσφέρει μία συγκεκριμένη εφαρμογή της τεχνολογίας blockchain, ενός ηλεκτρονικού συστήματος μετρητών από ομότιμους χρήστες (peer to peer) που επιτρέπει online πληρωμές Bitcoin. Ενώ το blockchain του Bitcoin χρησιμοποιείται για την παρακολούθηση της ιδιοκτησίας ψηφιακού νομίσματος (bitcoins), το Ethereum blockchain επικεντρώνεται στην εκτέλεση του κώδικα προγραμματισμού οποιασδήποτε αποκεντρωμένης εφαρμογής.

Στο blockchain Ethereum, αντί για εξόρυξη για bitcoin, οι ανθρακωρύχοι εργάζονται για να κερδίσουν Ether, ένα είδος κρυπτογραφικού νομίσματος που προμηθεύεται το δίκτυο. Πέρα από ένα εμπορεύσιμο κρυπτονόμισμα, το ether χρησιμοποιείται επίσης από τους προγραμματιστές εφαρμογών για να πληρώνουν τους φόρους συναλλαγών και τις υπηρεσίες στο δίκτυο Ethereum.

Υπάρχει ένας δεύτερος τύπος νομίσματος που χρησιμοποιείται για την καταβολή αμοιβών των ανθρακωρύχων για τις συναλλαγές στο μπλοκ τους, το οποίο ονομάζεται gas και κάθε εκτέλεση ενός smart contract απαιτεί την αποστολή κάποιας ποσότητας gas μαζί με αυτό για να προσελκύσουν τους ανθρακωρύχους να το βάλουν στο blockchain (Rosic, guides/ethereum, 2019).

5.3 Η εικονική μηχανή του Ethereum

Πριν από τη δημιουργία του Ethereum, οι εφαρμογές blockchain σχεδιάστηκαν για να κάνουν ένα πολύ περιορισμένο σύνολο λειτουργιών. Το Bitcoin και άλλα κρυπτονομίσματα , για παράδειγμα, αναπτύχθηκαν αποκλειστικά για να λειτουργήσουν ως ψηφιακά νομίσματα peer-to-peer.

Οι προγραμματιστές αντιμετώπισαν πρόβλημα που βρισκόταν στο είτε να επεκτείνουν το σύνολο των λειτουργιών που προσφέρονται από το Bitcoin και άλλους τύπους εφαρμογών, το οποίο είναι πολύ περίπλοκο και χρονοβόρο, είτε να αναπτύξουν μια νέα εφαρμογή blockchain και μια εντελώς νέα πλατφόρμα. Αναγνωρίζοντας αυτή τη δυσκολία, ο δημιουργός του Ethereum, ο Vitalik Buterin ανέπτυξε μια νέα προσέγγιση.

Η βασική καινοτομία του Ethereum, η εικονική μηχανή Ethereum (EVM) είναι ένα πλήρες λογισμικό της Turing που λειτουργεί στο δίκτυο Ethereum. Επιτρέπει σε οποιονδήποτε να εκτελέσει οποιοδήποτε πρόγραμμα, ανεξάρτητα από τη γλώσσα προγραμματισμού και δίνει αρκετό χρόνο και μνήμη. Η εικονική μηχανή Ethereum καθιστά τη διαδικασία δημιουργίας εφαρμογών blockchain πολύ πιο εύκολη και αποτελεσματική από ποτέ. Αντί να χρειαστεί να χτίσει ένα εντελώς πρωτότυπο blockchain για κάθε νέα εφαρμογή, το Ethereum επιτρέπει την ανάπτυξη ενδεχομένως χιλιάδων διαφορετικών εφαρμογών σε μία πλατφόρμα (Rosic, guides/ethereum, 2019).

5.4 Τρόπος χρήσης του Ethereum

Το Ethereum επιτρέπει στους προγραμματιστές να δημιουργούν και να αναπτύσσουν αποκεντρωμένες εφαρμογές. Μια αποκεντρωμένη εφαρμογή ή Dapp εξυπηρετεί κάποιο συγκεκριμένο σκοπό για τους χρήστες της. Το Bitcoin, για παράδειγμα, είναι ένα Dapp που παρέχει στους χρήστες του ένα σύστημα ηλεκτρονικών μετρητών (peer to peer) από ομότιμους χρήστες που επιτρέπει online πληρωμές Bitcoin. Επειδή οι αποκεντρωμένες εφαρμογές αποτελούνται από κώδικα που λειτουργεί σε δίκτυο blockchain, δεν ελέγχονται από κανένα άτομο ή κεντρική οντότητα.

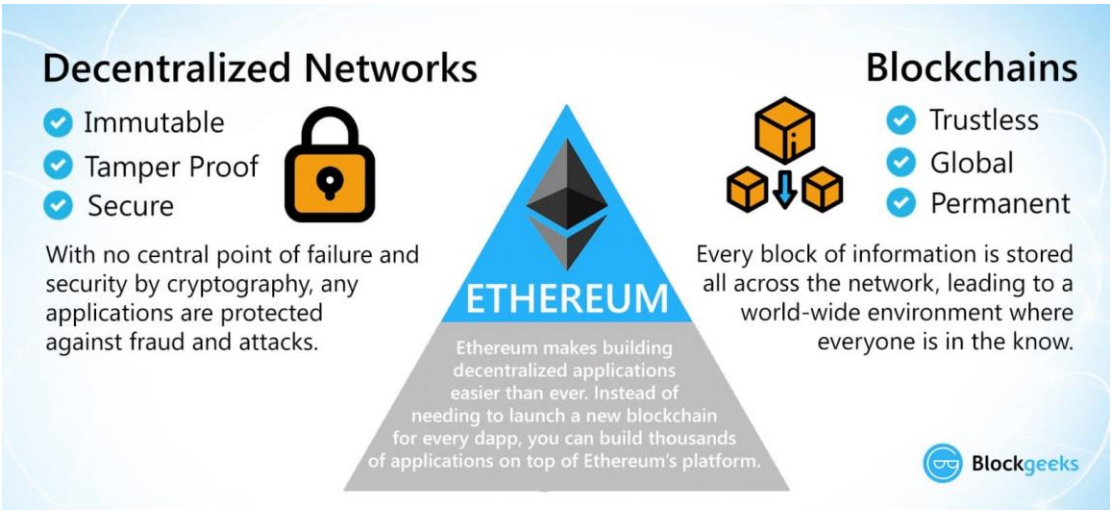
Οποιεσδήποτε κεντρικές (centralized) υπηρεσίες μπορούν να αποκεντρωθούν (decentralized) χρησιμοποιώντας το Ethereum. Για παράδειγμα όλες οι υπηρεσίες διαμεσολάβησης που υπάρχουν σε εκατοντάδες διαφορετικές βιομηχανίες. Από προφανείς υπηρεσίες όπως τα δάνεια που παρέχουν οι τράπεζες έως ενδιάμεσες

υπηρεσίες που σπάνια θα σκεφτούν οι περισσότεροι άνθρωποι όπως τα μητρώα τίτλων, τα συστήματα ψηφοφορίας, η κανονιστική συμμόρφωση και πολλά άλλα.

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

Το Ethereum χρησιμοποιείται επίσης ως πλατφόρμα για την εκτόξευση άλλων κρυπτονομισμάτων. Λόγω του προτύπου νομίσματος ERC20 που ορίζεται από το Ίδρυμα Ethereum, οι προγραμματιστές μπορούν να εκδώσουν τις δικές τους εκδοχές αυτού του νομίσματος και να συγκεντρώσουν χρήματα με μια αρχική προσφορά νομισμάτων (ICO). Σε αυτή τη στρατηγική συγκέντρωσης κεφαλαίων, οι εκδότες του συμβολαίου καθορίζουν ένα ποσό που θέλουν να αυξήσουν, το προσφέρουν σε ένα πλήθος και λαμβάνουν Ether σαν αντάλλαγμα. Δισεκατομμύρια δολάρια έχουν εγερθεί από τους ICO στην πλατφόρμα Ethereum τα τελευταία δύο χρόνια και ένα από τα πιο πολύτιμα κρυπτονομίσματα στον κόσμο, το EOS, είναι ERC20 νόμισμα.

Η εταιρεία Ethereum δημιούργησε πρόσφατα ένα νέο πρότυπο που ονομάζεται νόμισμα ERC721 για την παρακολούθηση μοναδικών ψηφιακών στοιχείων. Μία από τις μεγαλύτερες περιπτώσεις χρήσης για τέτοιες μάρκες είναι τα ψηφιακά συλλεκτικά αντικείμενα, καθώς η υποδομή επιτρέπει στους ανθρώπους να αποδείξουν την ιδιοκτησία των σπάνιων ψηφιακών προϊόντων. Πολλά παιχνίδια κατασκευάζονται αυτή τη στιγμή χρησιμοποιώντας αυτή την τεχνολογία, όπως το CryptoKitties, ένα παιχνίδι όπου οι χρήστες μπορούν να συλλέγουν και να αναπαράγουν ψηφιακές γάτες (Rosic, guides/ethereum, 2019).



Εικόνα 12: Ethereum Network (Rosic, guides/ethereum, 2019)

5.5 Τα οφέλη μιας αποκεντρωμένης εφαρμογής Ethereum

- Αμεταβλητότητα - Ένα τρίτο μέρος δεν μπορεί να κάνει αλλαγές στα δεδομένα.
- Είναι απαραβίαστη και δεν μπορεί να υπάρξει διαφθορά - Οι εφαρμογές βασίζονται σε ένα δίκτυο που διαμορφώνεται γύρω από την αρχή της συναίνεσης, καθιστώντας αδύνατη τη λογοκρισία.
- Secure - Με κανένα κεντρικό σημείο αποτυχίας και ασφαλισμένες με κρυπτογραφία, οι εφαρμογές προστατεύονται καλά από επιθέσεις hackers και από δόλιες δραστηριότητες.
- Μηδενική διακοπή λειτουργίας - Οι εφαρμογές δεν πέφτουν ποτέ και δεν μπορούν ποτέ να απενεργοποιηθούν (Rosic, guides/ethereum, 2019).

5.6 Τρόπος πρόσβασης στο Ethereum για την ανάπτυξη εφαρμογής

Υπάρχουν πολλοί τρόποι με τους οποίους μπορεί ο χρήστης να συνδεθεί στο δίκτυο Ethereum, ένας από τους ευκολότερους τρόπους είναι να χρησιμοποιηθεί το πρόγραμμα περιήγησης Mist native. Το Mist παρέχει ένα φιλικό προς το χρήστη περιβάλλον και ψηφιακό πορτοφόλι για τους χρήστες να εμπορεύονται και να αποθηκεύουν Ether, καθώς και να γράφουν, να διαχειρίζονται, να αναπτύσσουν και να χρησιμοποιούν έξυπνες συμβάσεις. Όπως τα προγράμματα περιήγησης στο διαδίκτυο δίνουν πρόσβαση και βοηθούν τους ανθρώπους να περιηγούνται στο διαδίκτυο, η Mist παρέχει μια πύλη στον κόσμο των αποκεντρωμένων εφαρμογών blockchain.

Υπάρχει επίσης η επέκταση του προγράμματος περιήγησης MetaMask, η οποία μετατρέπει το Google Chrome σε πρόγραμμα περιήγησης Ethereum. Το MetaMask επιτρέπει σε οποιονδήποτε να τρέχει εύκολα ή να αναπτύσσει αποκεντρωμένες εφαρμογές από το πρόγραμμα περιήγησης. Αν και αρχικά δημιουργήθηκε ως πρόσθετο στο Chrome, το MetaMask υποστηρίζει τον Firefox και το Brave Browser επίσης.

Ενώ είναι ακόμα πρώτες μέρες, η Mist, το MetaMask και μια ποικιλία άλλων προγραμμάτων περιήγησης έχουν την τάση να κάνουν εφαρμογές που βασίζονται σε blockchain, προσβάσιμες σε περισσότερους ανθρώπους από ποτέ. Ακόμη και τα άτομα χωρίς τεχνικό υπόβαθρο μπορούν τώρα να δημιουργήσουν εφαρμογές blockchain. Αυτό είναι ένα επαναστατικό άλμα για την τεχνολογία blockchain που θα μπορούσε να φέρει τις αποκεντρωμένες εφαρμογές στο επίκεντρο (Rosic, guides/ethereum, 2019).

6 InterPlanetary File System (IPFS)

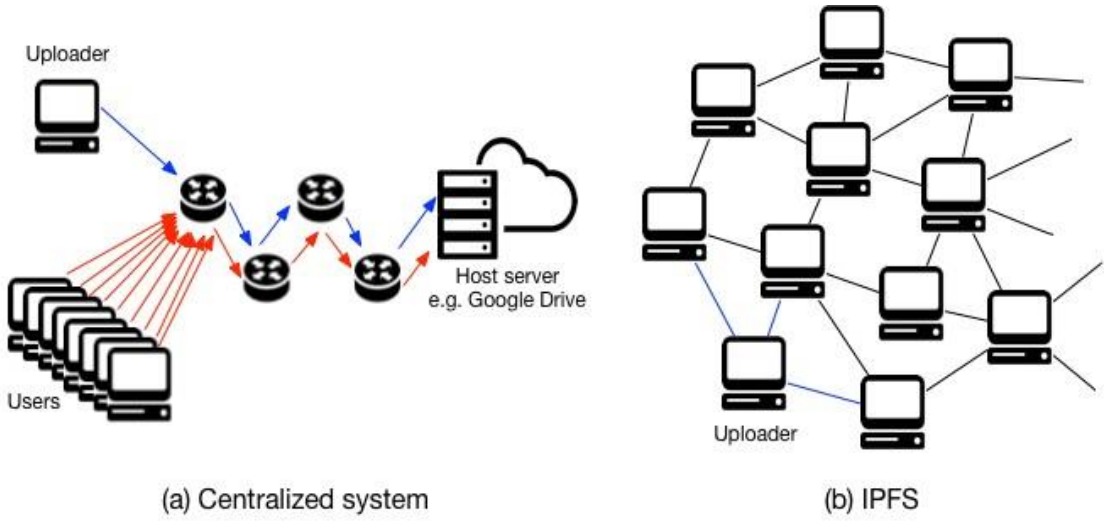
6.1 Ορισμός

Το Διατραπεζικό σύστημα αρχείων (IPFS) είναι ένα πρωτόκολλο και ένα δίκτυο peer-to-peer για την αποθήκευση και κοινή χρήση δεδομένων σε ένα κατανεμημένο σύστημα αρχείων. Το IPFS χρησιμοποιεί τη διευθυνσιοδότηση περιεχομένου για να αναγνωρίσει με μοναδικό τρόπο κάθε αρχείο σε ένα παγκόσμιο χώρο ονομάτων που συνδέει όλες τις υπολογιστικές συσκευές (wikipedia, n.d.) .

6.2 Επεξήγηση IPFS και οι λόγοι που το καθιστούν σημαντικό

Το IPFS είναι μία σημαντική εξέλιξη των προηγούμενων τεχνολογιών

Το IPFS έχει επωφεληθεί σημαντικά από πολλαπλές προηγμένες τεχνολογίες όπως οι κατανεμημένοι πίνακες hash (DHT), το BitTorrent, το git και το SFS. Έχει εμπνευστεί από αυτές τις τεχνολογίες για να προσφέρει μια βελτιωμένη λύση για την ανταλλαγή δεδομένων. Το IPFS είναι ένα project ανοιχτού κώδικα, στο οποίο συνεισφέρουν παγκοσμίως για την έρευνα, την ανάπτυξη και την ενίσχυση αυτού του συστήματος.



Εικόνα 13: Συγκρίνοντας την κίνηση των δεδομένων στο IPFS και σε ένα κεντρικό σύστημα (Capital, 2018)

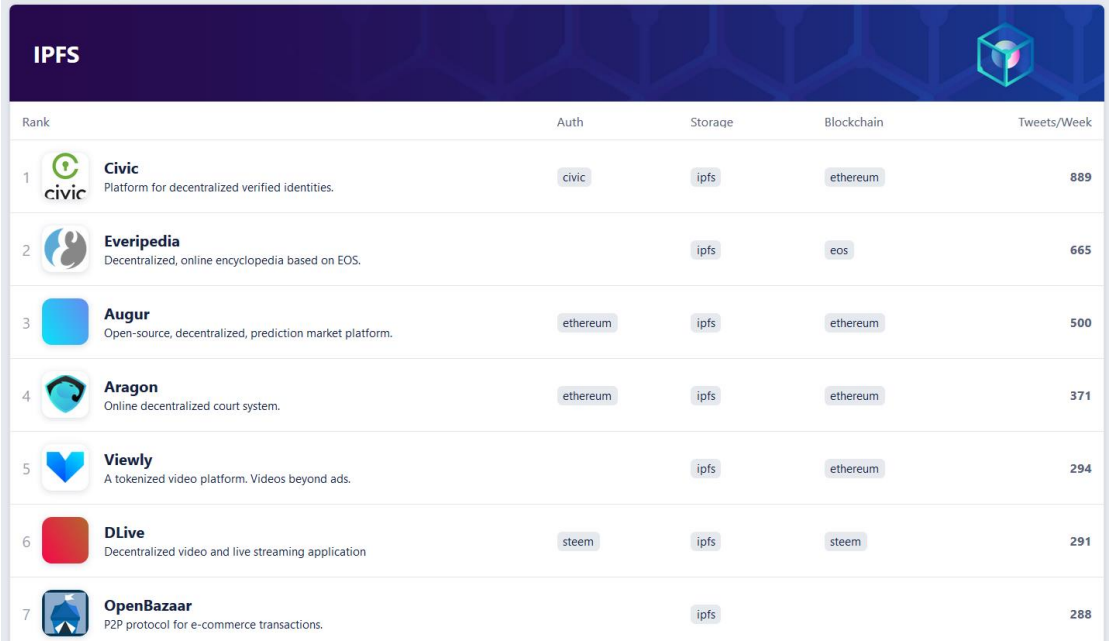
Το IPFS αποτελεί σημαντικό στοιχείο της υποδομής Web 3.0

Το Web 3.0 είναι ένας μακροπρόθεσμος στόχος που αποσκοπεί στην αντικατάσταση της τρέχουσας υποδομής διαδικτύου. Καθώς η αποκέντρωση είναι η όλη η ουσία του Web 3.0. πολλοί θεωρούν την τεχνολογία κατανεμημένου βιβλίου (DLT-Distributed Ledger Technology), όπως για παράδειγμα τα blockchains, ως το βασικό δομικό στοιχείο του Web 3.0. Όπως αναφέρθηκε ένα blockchain είναι σαν ένα αμετάβλητο καθολικό βιβλίο που αποθηκεύει την κατάσταση του δικτύου. Είναι απαραίτητη η κατανεμημένη συναίνεση μεταξύ όλων των κόμβων του δικτύου προκειμένου να επεκταθεί το blockchain και να αποθηκευτούν τα κρίσιμα δεδομένα του δικτύου μεταξύ των κόμβων του δικτύου. Ως εκ τούτου, θα μπορούσε να είναι απαγορευτικά δαπανηρή η αποθήκευση οποιουδήποτε άλλου είδους δεδομένων στην μπλοκ αλυσίδα. Για περιπτώσεις πολλαπλών χρήσεων, μπορεί να είναι πιο αποτελεσματική η αποθήκευση άλλων μη κρίσιμων δεδομένων με ασφαλή τρόπο κοντά στο επίπεδο ασφάλειας που προσφέρει και το blockchain.

Το IPFS είναι το καταλληλότερο μέσο αποθήκευσης για αυτήν την κατηγορία δεδομένων. Το IPFS επιτρέπει κατανεμημένη αποθήκευση δεδομένων που είναι αδύνατον να αλλοιωθούν ή να πλαστογραφηθούν. Τα δεδομένα που είναι αποθηκευμένα στο δίκτυο IPFS δεν μπορούν να τροποποιηθούν χωρίς αλλαγή του αναγνωριστικού δεδομένων. Στο IPFS, το αναγνωριστικό είναι ένα κρυπτογραφικό hash των δεδομένων. Αυτό σημαίνει ότι μη κρίσιμα δεδομένα μπορούν να αποθηκευτούν στο IPFS κατά την αποθήκευση αυτού του αναγνωριστικού σε ένα θεμελιώδες κατανεμημένο βιβλίο (π.χ. blockchain). Αυτό θα είχε ως αποτέλεσμα λιγότερες εξαντλητικές πράξεις πάνω από το κατανεμημένο βιβλίο.

Το IPFS είναι μια βέλτιστη πλατφόρμα αποθήκευσης για αποκεντρωμένες εφαρμογές

Οι αποκεντρωμένες εφαρμογές (dApps) αποτελούν μια κατηγορία εφαρμογών που αξιοποιούν την αποκέντρωση για να επιτύχουν πρωτοφανή οφέλη. Μεταξύ αυτών είναι οι αποκεντρωμένες ανταλλαγές και οι αγορές όπου αποσύρονται οι κεντρικοί διαμεσολαβητές, εξαλείφοντας / μειώνοντας τα τέλη διαπραγμάτευσης. Ένα άλλο παράδειγμα είναι τα αποκεντρωμένα μέσα κοινωνικής δικτύωσης και οι πλατφόρμες βίντεο, όπου το περιεχόμενο δεν μπορεί να λογοκρίνεται από τη βούληση της εταιρείας που λειτουργεί. Τέτοια dApps απαιτούν την αποθήκευση ενός σημαντικού αριθμού δεδομένων. Το IPFS επιτρέπει την αποθήκευση αυτών των δεδομένων με κατανεμημένο τρόπο που είναι ανθεκτικό στη λογοκρισία. Για τους λόγους αυτούς, το IPFS μετατρέπεται σε μια προτιμώμενη πλατφόρμα αποθήκευσης για τα dApps. Στην παρακάτω εικόνα προβάλλονται κάποιες γνωστές αποκεντρωμένες εφαρμογές που χρησιμοποιούν το IPFS ως την πλατφόρμα αποθήκευσης τους:



Εικόνα 14: Μερικές από τις ανερχόμενες dApps που χρησιμοποιούν IPFS σαν πλατφόρμα αποθήκευσης (Capital, 2018)

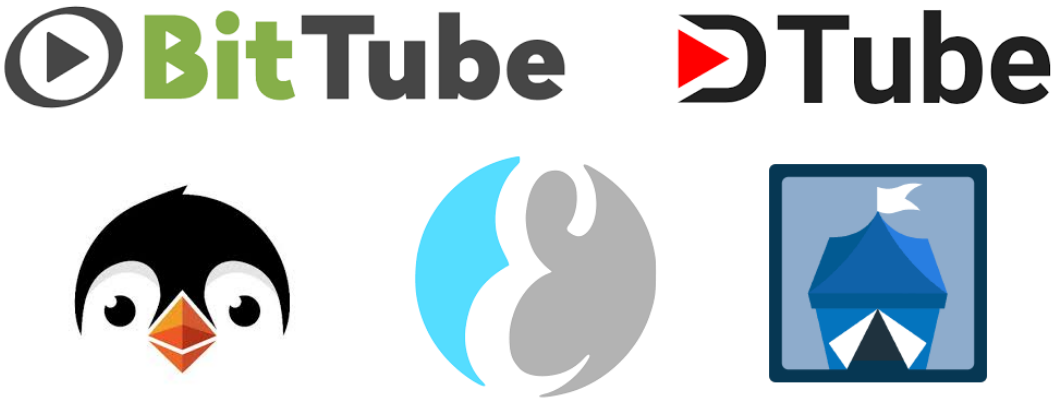
Το IPFS μπορεί να προσφέρει καλύτερη εμπειρία χρήστη

Το IPFS θα μπορούσε να οδηγήσει σε βελτιωμένη εμπειρία χρήστη σε πολλές περιπτώσεις. Για παράδειγμα, η προσπάθεια περιήγησης ή λήψης κάποιου δημοφιλούς περιεχομένου χρησιμοποιώντας το τυπικό μοντέλο πελάτη-διακομιστή μπορεί να εξαντλήσει το εύρος ζώνης του δικτύου και να οδηγήσει σε συμφόρηση δικτύου. Αυτό μπορεί να έχει ως αποτέλεσμα μια ενοχλητική εμπειρία χρήστη λόγω των μεγαλύτερων χρόνων καθυστέρησης. Στο IPFS, το περιεχόμενο παραδίδεται από τους πλησιέστερους κόμβους του δικτύου (peers) που διαθέτουν ένα αντίγραφο του περιεχομένου αφαιρώντας την πίεση που δέχεται ένας και μόνος κόμβος, βελτιώνοντας έτσι την εμπειρία του χρήστη. Επιπλέον, το IPFS επιτρέπει συνεχή και ομαλή περιήγηση στο περιεχόμενο, ακόμη και αν ο κάτοχος του περιεχομένου δεν είναι πλέον διαθέσιμος.

Το IPFS δέχεται νέα επιχειρηματικά μοντέλα (online)

Στο σημερινό διαδίκτυο, κάθε διαδικτυακό περιεχόμενο πρέπει να φιλοξενείται σε ειδικούς διακομιστές. Είναι σημαντικό για τον εκδότη περιεχομένου να διασφαλίσει τη διαθεσιμότητα του περιεχομένου και επαρκές εύρος ζώνης για να ικανοποιήσει την απαιτούμενη ζήτηση. Το IPFS αλλάζει ριζικά αυτό το μοντέλο. Στο IPFS, αντί να υπάρχει ένας κεντρικός εξυπηρετητής που εξυπηρετεί όλους τους χρήστες, τα δεδομένα μοιράζονται με κατανεμημένο τρόπο και μπορούν να προσφερθούν από οποιονδήποτε κόμβο που τα κατέχει. Ως αποτέλεσμα, οι απαιτήσεις σχετικά με το εύρος ζώνης μειώνονται σημαντικά και βελτιώνεται η αξιοπιστία. Συνεπώς, νέα επιχειρηματικά μοντέλα θα αρχίσουν να εξελίσσονται. Για παράδειγμα, με τη χρήση

ορισμένων projects, όπως το Filecoin, θα ήταν δυνατό οι εκδότες περιεχομένου να πληρώνουν στους χρήστες μια μικρή ανταμοιβή για την αποθήκευση του περιεχομένου. Αυτό θα βελτίωνε τη διανομή περιεχομένου και θα εξασφάλιζε τη διαθεσιμότητα του.



Εικόνα 15: Πολλές πλατφόρμες που διαμοιράζονται video, κοινωνικά μέσα δικτύωσης και άλλες αρχίζουν να χρησιμοποιούν το IPFS για να πετύχουν καλύτερη εμπειρία χρήστη και ένα καλύτερο επιχειρηματικό μοντέλο (Capital, 2018).

Το IPFS λαμβάνει αυξημένη γενική υιοθέτηση

Λόγω των πολλαπλών ελκυστικών χαρακτηριστικών του IPFS, αυξάνεται η γενική υιοθέτηση του. Υπάρχουν περιπτώσεις όπου το IPFS βοήθησε τους χρήστες να καταπολεμήσουν τη λογοκρισία στην Τουρκία και την Ισπανία. Επιπλέον σύμφωνα με την ανακοίνωση του Cloudflare, είναι πλέον δυνατή η φιλοξενία ιστοσελίδων στο IPFS και η αναφορά σε αυτές χρησιμοποιώντας ένα εύκολο τυποποιημένο όνομα τομέα (domain name). Οι φιλοξενούμενοι ιστότοποι IPFS είναι ιστοτόποι ανθεκτικοί στη λογοκρισία και τώρα μπορούν εύκολα να αναγνωριστούν και να περιηγηθούν από τους χρήστες με ασφάλεια χρησιμοποιώντας HTTP και HTTPS καθώς και την πύλη IPFS του Cloudfare. Επίσης, το Cloudflare έχει εφαρμόσει τεχνικές που εγγυώνται ότι οι χρήστες δεν χρειάζεται να έχουν εμπιστοσύνη στο Cloudflare για να τους παρέχει το σωστό περιεχόμενο που ζήτησαν (Capital, 2018).

7 Blockchain Events

7.1 Ορισμός των Events

Τα events στα smart contracts δίνουν μια αφηρημένη έννοια πάνω στη λειτουργία καταγραφής συμβάντων του Ethereum Virtual Machine. Οι εφαρμογές μπορούν να εγγραφούν και να ακούν σε αυτά τα συμβάντα μέσω της διεπαφής RPC ενός πελάτη του Ethereum.

Τα γεγονότα είναι κληρονομικά μέλη των έξυπνων συμβολαίων. Όταν καλούνται, προκαλούν την αποθήκευση δεδομένων στο αρχείο καταγραφής συναλλαγών (transaction's log) - μια ειδική δομή δεδομένων στο blockchain. Αυτά τα αρχεία καταγραφής συνδέονται με τη διεύθυνση του συμβολαίου, ενσωματώνονται στο blockchain και παραμένουν εκεί όσο υπάρχει πρόσβαση σε ένα μπλοκ . Το αρχείο καταγραφής (log) και τα δεδομένα συμβάντων του (event data) δεν είναι προσβάσιμα από τα smart contracts (ούτε καν από εκείνο που τα δημιούργησε).

Είναι δυνατόν να ζητηθεί μια απλή επαλήθευση πληρωμής για τα αρχεία καταγραφής, οπότε αν μια εξωτερική οντότητα προμηθεύσει μια σύμβαση με μια τέτοια επαλήθευση, μπορεί να ελέγξει ότι η καταγραφή υπάρχει πραγματικά μέσα στο blockchain (solidity.readthedocs, n.d.).

7.2 Σύνδεση με User Interface

Τα events και τα (logs) αρχεία καταγραφής είναι σημαντικά στο Ethereum επειδή διευκολύνουν την επικοινωνία μεταξύ έξυπνων συμβάσεων (smart contracts) και των διεπαφών χρήστη (user interface). Στο παραδοσιακό web development, παρέχεται μια απάντηση διακομιστή σε μια επιστροφή κλήσης στο frontend. Στο Ethereum, όταν εξορύσσεται (επιβεβαιώνεται) μια συναλλαγή, τα έξυπνα συμβόλαια μπορούν να εκπέμπουν events και να γράψουν αρχεία καταγραφής στο blockchain που μπορεί στη συνέχεια να επεξεργαστεί το frontend. Υπάρχουν διάφοροι τρόποι με τους οποίους μπορεί ο χρήστης να αναφερθεί στα συμβάντα και τα αρχεία καταγραφής.

Όταν ένα smart contract θέλει να πυροδοτήσει το frontend , το smart contract εκπέμπει ένα event. Καθώς το frontend παρακολουθεί συνεχώς για γεγονότα, μόλις καταλάβει ένα τέτοιο (που πηγάζει από το smart contract) μπορεί να λάβει μέτρα, να εμφανίσει ένα μήνυμα , να προβεί σε μια ενέργεια κλπ.

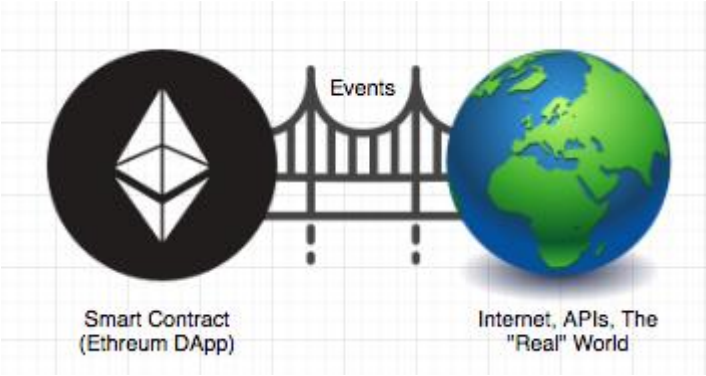
Με αυτόν τον τρόπο επιτυγχάνεται real-time επικοινωνία μεταξύ smart contract και user-interface (Consensys, 2016).

7.3 Συμπερασματικά

Συμπερασματικά, τα events επιτρέπουν στις συναλλαγές on-chain να επικοινωνούν με υπηρεσίες off-chain στον "πραγματικό" κόσμο.

Τα smart contracts έχουν τη δυνατότητα να εκπέμπουν events κατά την επεξεργασία μιας συναλλαγής. Όπως σημειώθηκε, μια συναλλαγή πρέπει πρώτα να εξορυχθεί πριν γίνει διαθέσιμη η πληροφορία συμβάντος.

Σε ένα βαθύτερο επίπεδο, τα συμβάντα (events) επωφελούνται από τις εγκαταστάσεις καταγραφής του Ethereum Virtual Machine και μπορούν να χρησιμοποιηθούν για να ενεργοποιήσουν JavaScript callbacks (Stewart, 2018).



Εικόνα 16: Blockchain events (Stewart, 2018)

8 Η Dapp που υλοποιήθηκε

8.1 Γενικό πλαίσιο

Η εταιρεία Spirit Innovations προσφέρει ολοκληρωμένες λύσεις στους επιχειρηματικούς τομείς. Ειδικότερα η εταιρεία διευκολύνει τις εισαγωγές και τη χονδρική διανομή ειδών στα καταστήματα λιανικής πώλησης αλλά και σε άλλους χονδρεμπόρους.

Αν ένας χρήστης επιθυμεί να προμηθευτεί ένα μεγάλο πλήθος προϊόντων, τότε η εταιρεία φροντίζει για την οικονομικότερη αγορά και παραλαβή αυτών των προϊόντων. Αυτό σημαίνει πως επιλέγει:

1. Το κατάλληλο εργοστάσιο για την παραγωγή αυτών των προϊόντων.

2. Την κατάλληλη μεταφορική για την διανομή των προϊόντων από το εργοστάσιο στο λιμάνι φόρτωσης τους.

3. Την κατάλληλη ναυτιλιακή για την μεταφορά αυτών των προϊόντων από το λιμάνι φόρτωσης στο λιμάνι εκφόρτωσης.

4. Τέλος, την κατάλληλη μεταφορική για την διανομή των προϊόντων από το λιμάνι εκφόρτωσης στο σημείο διανομής.

Φυσικά, η εταιρεία λειτουργεί σύμφωνα με τις απαιτήσεις του πελάτη. Αν για παράδειγμα, ο πελάτης επιθυμεί να αγοράσει τα προϊόντα του από κάποιο συγκεκριμένο εργοστάσιο με το οποίο συνεργάζεται, τότε η εταιρεία λαμβάνει ως δεδομένο το βήμα 1 και φροντίζει για τα υπόλοιπα 3 βήματα.

Έτσι, δηλώνει στον πελάτη τις εταιρείες εκείνες που τον συμφέρουν να συνεργαστεί και τους φέρνει όλους σε επαφή προκειμένου να συνεργαστούν. Η κάθε εταιρεία υπογράφει με εκείνες που συνεργάζεται ένα συμβόλαιο και ανταλλάσσει τα κατάλληλα έγγραφα, ώστε να επιβεβαιώνεται κάθε φορά η ασφαλής προώθηση των προϊόντων.

Για παράδειγμα, το εργοστάσιο υπογράφει συμβόλαιο με την μεταφορική που θα παραλάβει τα προϊόντα και τον αγοραστή , η μεταφορική με το εργοστάσιο και την ναυτιλιακή κλπ.

Όλες οι εταιρείες που κλείνουν συμβόλαια αλληλεπιδρούν μεταξύ τους στέλνοντας σε κάθε στάδιο της παραγγελίας το απαιτούμενο έγγραφο η μία στην άλλη (όπως για παράδειγμα την απόδειξη προκαταβολής ή το έγγραφο που δηλώνει ότι τα προϊόντα φορτώθηκαν στο πλοίο) και αναμένουν την αποδοχή του, ώστε να προχωρήσει η διαδικασία της παραγγελίας.

Αυτό όμως κρύβει προβλήματα, τα οποία αναλύονται στην συνέχεια.

8.2 Προβλήματα

Αρχικά, θα εξεταστεί η περίπτωση όπου ο χρήστης (π.χ. μια εταιρεία) υπογράφει ένα συμβόλαιο παραγγελίας με ένα εργοστάσιο. Στο συμβόλαιο αυτό υπάρχουν πληροφορίες που έχουν να κάνουν με τον τύπο του προϊόντος, την ποσότητα, την τιμή του, το ποσό προκαταβολής κλπ. Το συμβόλαιο αυτό το συμφωνούν μεν στην αρχή και οι δύο χρήστες, αλλά αυτό δεν σημαίνει ότι στην πορεία δεν μπορεί κάποιος από τους δύο να το τροποποιήσει προς δικό του συμφέρον. Παρόμοια προβλήματα προκύπτουν για κάθε συμβόλαιο που υπογράφεται μεταξύ όλων των παραπάνω χρηστών.

Επίσης, μέχρι στιγμής η αποστολή του κάθε εγγράφου και η επιβεβαίωση του από τον χρήστη που αυτό στέλνεται γίνεται με mail, γεγονός που σημαίνει τεράστια καθυστέρηση και δυσχρηστία.

Επιπλέον, δεν υπάρχει κάποια ιστοσελίδα που να δηλώνει ανά πάσα στιγμή την τρέχουσα κατάσταση του συμβολαίου , που να περιέχει όλα τα έγγραφα που εμπλέκονται με την συγκεκριμένη συμφωνία και να ενημερώνεται σε real-time όταν κάποιο εμπλεκόμενο μέρος ανεβάζει ένα έγγραφο η αποδέχεται κάποιο.

Τέλος, δεν υπάρχει κάποια πλατφόρμα όπου ο χρήστης να μπορεί άμεσα να ενημερωθεί για το κάθε συμβόλαιο που έχει συνάψει με ένα κλικ, καθώς μπορεί να εμπλέκεται σε παραπάνω από ένα. Θα πρέπει να κάνει αναζήτηση στα mail του κάθε φορά για αυτό που επιθυμεί να βρει.

8.3 Λύση των προβλημάτων μέσω της λειτουργίας της Dapp

Για να δοθεί λύση στα παραπάνω προβλήματα υλοποιήθηκε η συγκεκριμένη Dapp. Ειδικότερα κάθε συμβόλαιο που συμφωνείται από τις εταιρείες ανεβαίνει στο Ethereum Blockchain με αποτέλεσμα κανείς να μην μπορεί να αλλάξει τους όρους του συμβολαίου, ούτε μάλιστα και η ίδια η εταιρεία (Spirit Innovations) που το ανεβάζει. Έτσι παρέχεται εμπιστοσύνη και οι εταιρείες είναι σίγουρες πως το συμβόλαιο που συμφωνούν δεν υπάρχει καμία περίπτωση να μεταβληθεί.

Επίσης, κάθε έγγραφο που ανταλλάσσεται μεταξύ των εταιρειών ανεβαίνει και αυτό (το hash του) στο blockchain με αποτέλεσμα και πάλι να μην μπορεί να μεταβληθεί από κανέναν εάν αυτό γίνει αποδεκτό από την εταιρεία που το δέχεται.

Επιπλέον, κάθε φορά παρέχονται οι απαραίτητες πληροφορίες σχετικά με την τρέχουσα κατάσταση του εκάστοτε συμβολαίου και υπάρχει real-time ενημέρωση

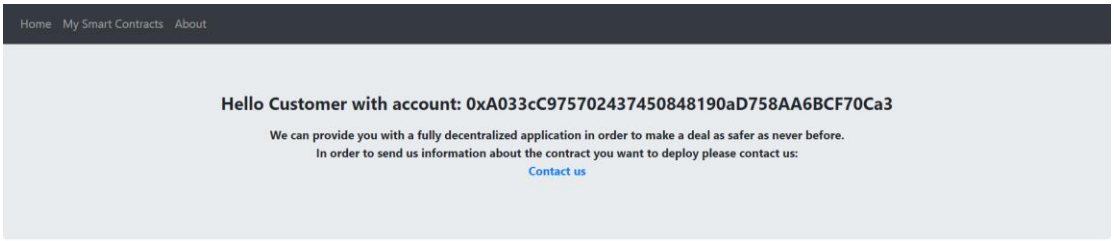
της εφαρμογής μέσω των blockchain events όταν ανεβαίνει ή γίνεται αποδεκτό κάποιο έγγραφο για να ενημερώνεται άμεσα κάθε εταιρεία και να μην υπάρχει καθυστέρηση.

Επίσης, κάθε εμπλεκόμενο μέρος του συμβολαίου μπορεί ανά πάσα στιγμή να δει τα έγγραφα που έχουν να κάνουν με το τρέχον συμβόλαιο (τα οποία έχουν ανέβει και στο blockchain).

Τέλος, μέσα από το Dapp προβάλλονται όλα τα συμβόλαια που έχει συνάψει ο χρήστης ώστε να μπορεί ανά πάσα στιγμή να ενημερωθεί για εκείνο που επιθυμεί με ένα κλικ.

8.4 Αρχική σελίδα της λειτουργίας του Dapp

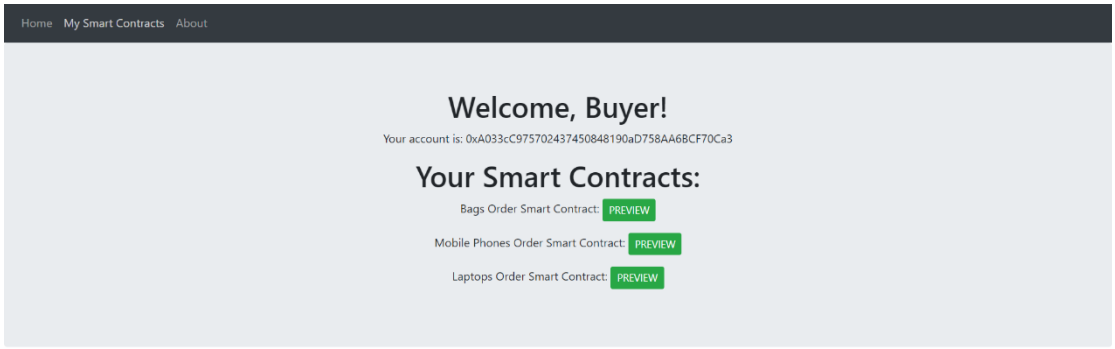
Αρχικά ο κάθε χρήστης μόλις εισέλθει με το account του στην εφαρμογή πληροφορείται σύντομα για αυτή και μπορεί αμέσως να ξεκινήσει ένα νέο συμβόλαιο επικοινωνώντας άμεσα με την εταιρεία μέσα από το Home Page στέλνοντας mail σχετικά με τις απαιτούμενες πληροφορίες:



Screenshot 1

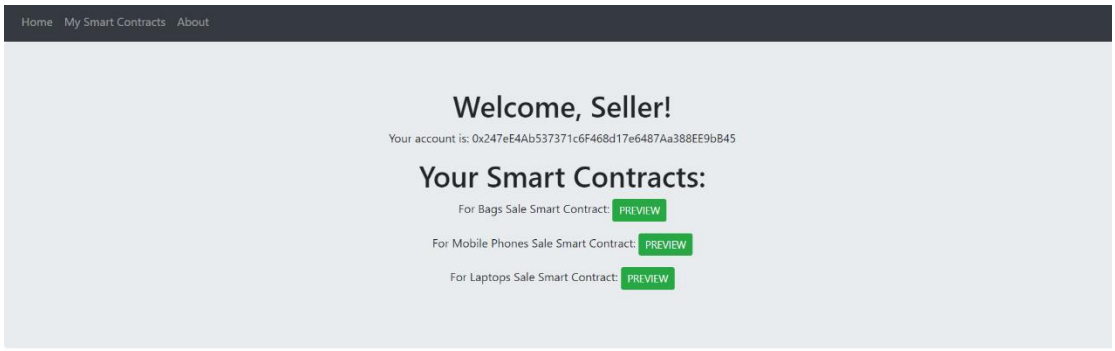
Στη συνέχεια, εάν πατήσει στο My Smart Contracts, εμφανίζονται όλα τα συμβόλαια τα οποία έχει συνάψει ο συγκεκριμένος χρήστης με αυτό το account, καθώς και με τι προϊόν σχετίζεται το καθένα ώστε να μπορεί να επιλέξει αυτό που επιθυμεί άμεσα.

Για παράδειγμα σε έναν αγοραστή τριών προϊόντων φαίνεται:



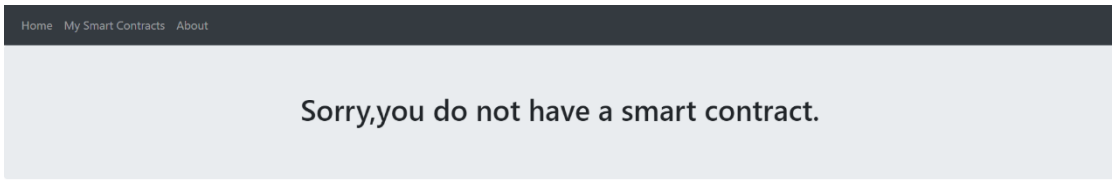
Screenshot 2

Ενώ σε έναν πωλητή τριών προϊόντων φαίνεται:



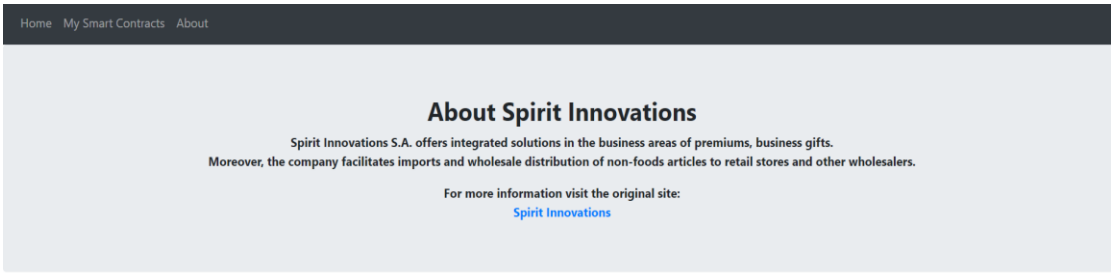
Screenshot 3

Αν κάποιος χρήστης δεν έχει συνάψει κάποιο συμβόλαιο, τότε στο My Smart Contracts του εμφανίζεται:



Screenshot 4

Τέλος, αν πατήσει το πεδίο About πληροφορείται σύντομα για το γενικό έργο που επιτελεί η εταιρεία Spirit Innovations, ενώ πατώντας στον αντίστοιχο σύνδεσμο που παρέχεται κατευθύνεται στο επίσημο site της εταιρείας:



Screenshot 5

Μόλις ο χρήστης στο πεδίο My Smart Contracts επιλέξει το συμβόλαιο που επιθυμεί τότε βλέπει την τρέχουσα κατάσταση του και προβαίνει σε ενέργειες που αναλύονται στη συνέχεια.

8.5 Επεξήγηση της λειτουργίας του Dapp μέσα από κάθε συμβόλαιο

Αφού ο χρήστης επιλέξει το συμβόλαιο που επιθυμεί, η εφαρμογή έχει να κάνει με τη σύναψη της συμφωνίας μεταξύ ενός αγοραστή και ενός πωλητή, την συνεχή αλληλεπίδραση τους μέσα από αυτή και την ενημέρωση τους για το στάδιο όπου βρίσκονται τα προϊόντα ανά πάσα στιγμή.

Στη συγκεκριμένη περίπτωση, το εργοστάσιο (ο πωλητής) αναλαμβάνει και την μεταφορά των προϊόντων από το εργοστάσιο του στο λιμάνι φόρτωσης.

Ο αγοραστής και ο πωλητής συμφωνούν μεταξύ τους ένα συμβόλαιο το οποίο περιέχει τις παρακάτω πληροφορίες:

- Τύπος προϊόντος (π.χ. bag)
- Ποσότητα (π.χ. 1000)
- Τιμή ανά μονάδα προϊόντος (π.χ. 1.810 /ea)
- Λιμάνι Φόρτωσης (π.χ. FOB Ningbo)
- Το ποσό της προκαταβολής (π.χ. 20%)
- Πληροφορίες(π.χ. balance against copy of landing)
- Χρόνος φόρτωσης (π.χ. 40 min after deployment)

Το συμβόλαιο αυτό στέλνεται στην εταιρεία και φροντίζει να δημιουργήσει ένα smart contract που περιέχει όλες τις παραπάνω πληροφορίες καθώς και όλα τα στάδια αλληλεπίδρασης αγοραστή-πωλητή που συνοδεύουν την ολοκλήρωση της συμφωνίας τους.

Τα στάδια ολοκλήρωσης του smart contract που η εταιρεία ανεβάζει στο blockchain είναι 6:

0. Upload Sales Confirmation (by buyer) and Upload Sales Confirmation Approval, Approve Contract (by seller)

1. Upload Downpayment Receipt (by buyer) and Confirm Downpayment Receipt (by seller)

2. Commence Production (by seller)

3. Goods Loaded on Ship (by seller)

4. Upload Shipping Documents (by seller) and Confirm Shipping Documents (by buyer)

5. Upload Settlement Receipt (by buyer) and Confirm Settlement Receipt (by seller)

6. Upload Telex Release (by seller) and Confirm Telex Release (by buyer)

Εννοείται πως πάντα ο αγοραστής και ο πωλητής βρίσκονται στο ίδιο στάδιο, αφού αλληλεπιδρούν με το ίδιο smart contract.

Στη συνέχεια η εταιρεία φροντίζει να ανεβάσει το smart contract στο public blockchain του Ethereum ώστε κανείς από τους δύο χρήστες, που εμπλέκονται να μην μπορεί να αλλάξει τους όρους τους συμβολαίου. Ακόμη, παρέχει στον καθένα την δικιά του ιστοσελίδα αλληλεπίδρασης με τον άλλον χρήστη και το blockchain, κάνοντας αμεσότερη και ευκολότερη την όλη διαδικασία.

Ο κάθε χρήστης ανεβάζει σε κάθε στάδιο στο ipfs network μια εικόνα το hash της οποίας αποθηκεύεται στο blockchain, ώστε να μην μπορεί να μεταβληθεί από κανέναν. Ο άλλος χρήστης βλέπει την εικόνα-έγγραφο και την αποδέχεται ή την απορρίπτει ανάλογα με το αν συμφωνεί ή όχι. Αν την αποδεχτεί τότε το smart contract προχωρά στο επόμενο στάδιο και για τους δύο χρήστες.

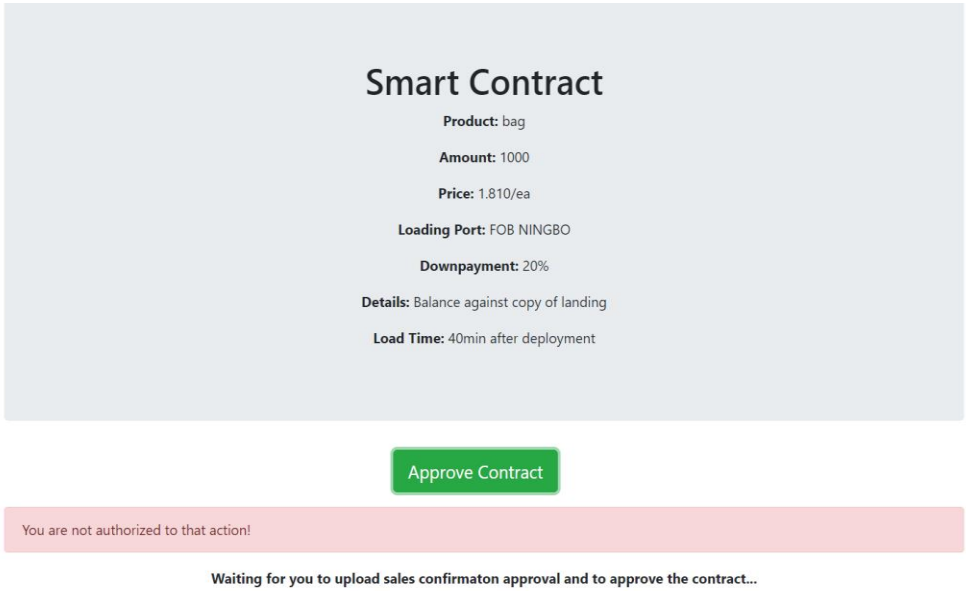
Ουσιαστικά ο κάθε χρήστης (αγοραστής-πωλητής) μέσα από την σελίδα που του παρέχεται αλληλεπιδρά με το blockchain και η διαδικασία αγοράς του προϊόντος

προχωρά βήμα βήμα με απόλυτη ασφάλεια όσον αφορά τα έγγραφα που ανεβαίνουν και όλα όσα έχουν συμφωνηθεί.

Υπάρχει real-time ενημέρωση σε κάθε σελίδα και ο κάθε χρήστης ειδοποιείται όταν ένα έγγραφο ανεβαίνει ή γίνεται αποδεκτό μέσω των blockchain events, με αποτέλεσμα να μειώνονται σημαντικά οι καθυστερήσεις.

Ο αγοραστής και ο πωλητής έχουν συγκεκριμένα accounts (σαν public address) τα οποία δίνονται στην εταιρεία. Έτσι κατά την δημιουργία του smart contract η εταιρεία ορίζει το account του αγοραστή και του πωλητή και μόνο ο καθένας από αυτούς μπορεί να αλληλεπιδράσει με το site που του έχει δοθεί. Κανείς άλλος δεν μπορεί δηλαδή να αλληλεπιδράσει με το site που προσφέρεται στον αγοραστή και στον πωλητή παρά μόνο οι ίδιοι.

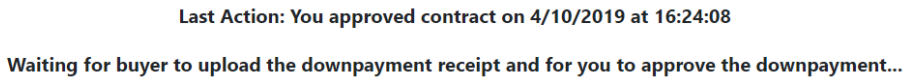
Αν για παράδειγμα κάποιος χρήστης με διαφορετικό account από εκείνο του αγοραστή προσπαθήσει να κάνει approve το smart contract πού έχει ανέβει στο blockchain, εμφανίζεται το παρακάτω μήνυμα σφάλματος:



Screenshot 6

Σε κάθε φάση όπου η εφαρμογή προχωρά σε ένα επόμενο στάδιο και υπάρχει αποδοχή κάποιου εγγράφου ή ακόμα και κατά την δήλωση παραγωγής και φόρτωσης των προϊόντων καταγράφεται η ακριβής ώρα και ημερομηνία που το έκανε αυτό ο εκάστοτε χρήστης μέσα από το smart contract που έχει ανέβει στο blockchain.

Για παράδειγμα:



Screenshot 7

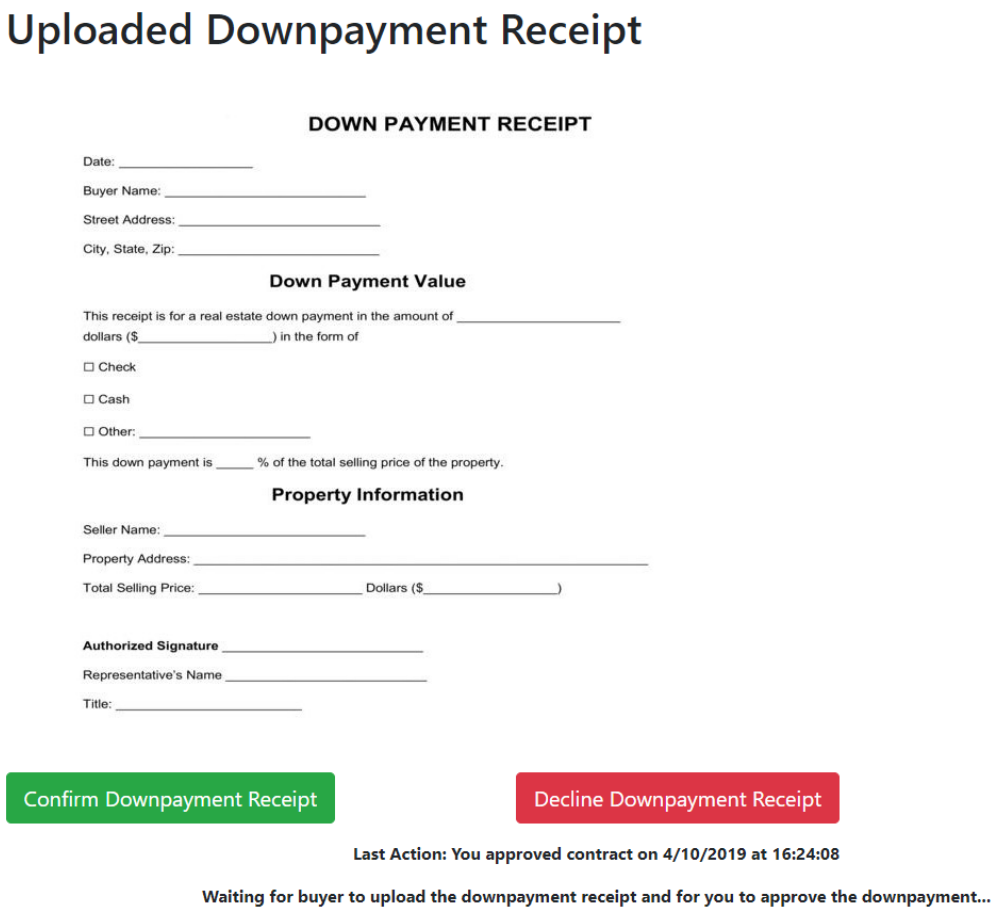
Επίσης, δίπλα από κάθε Confirmation Button υπάρχει και ένα Decline Button, όπου ο κάθε χρήστης μπορεί να πατήσει εάν δεν συμφωνεί με κάποιο έγγραφο και αμέσως να κατευθυνθεί ώστε να στείλει mail στον άλλον σχετικά με το που βρίσκεται το συγκεκριμένο πρόβλημα για την άμεση επίλυση του.

Επίσης σε κάθε button της εφαρμογής που έχει να κάνει με Submit και Confirmation ο κάθε χρήστης αλληλεπιδρά με το blockchain, αλλά μόνο στα Confirmation Buttons και στα Commence Production, Goods Loaded on Ship αλλάζει η κατάσταση (το στάδιο) του συμβολαίου (smart contract).

Όταν ο χρήστης κάνει upload μια εικόνα, ουσιαστικά κρατιέται το hash της και με το submit αυτό το hash αποθηκεύεται στο smart contract ώστε να μπορεί να τραβηχτεί ανά πάσα στιγμή και σαν αποτέλεσμα να προβληθεί η ζητούμενη εικόνα και στους δύο χρήστες.

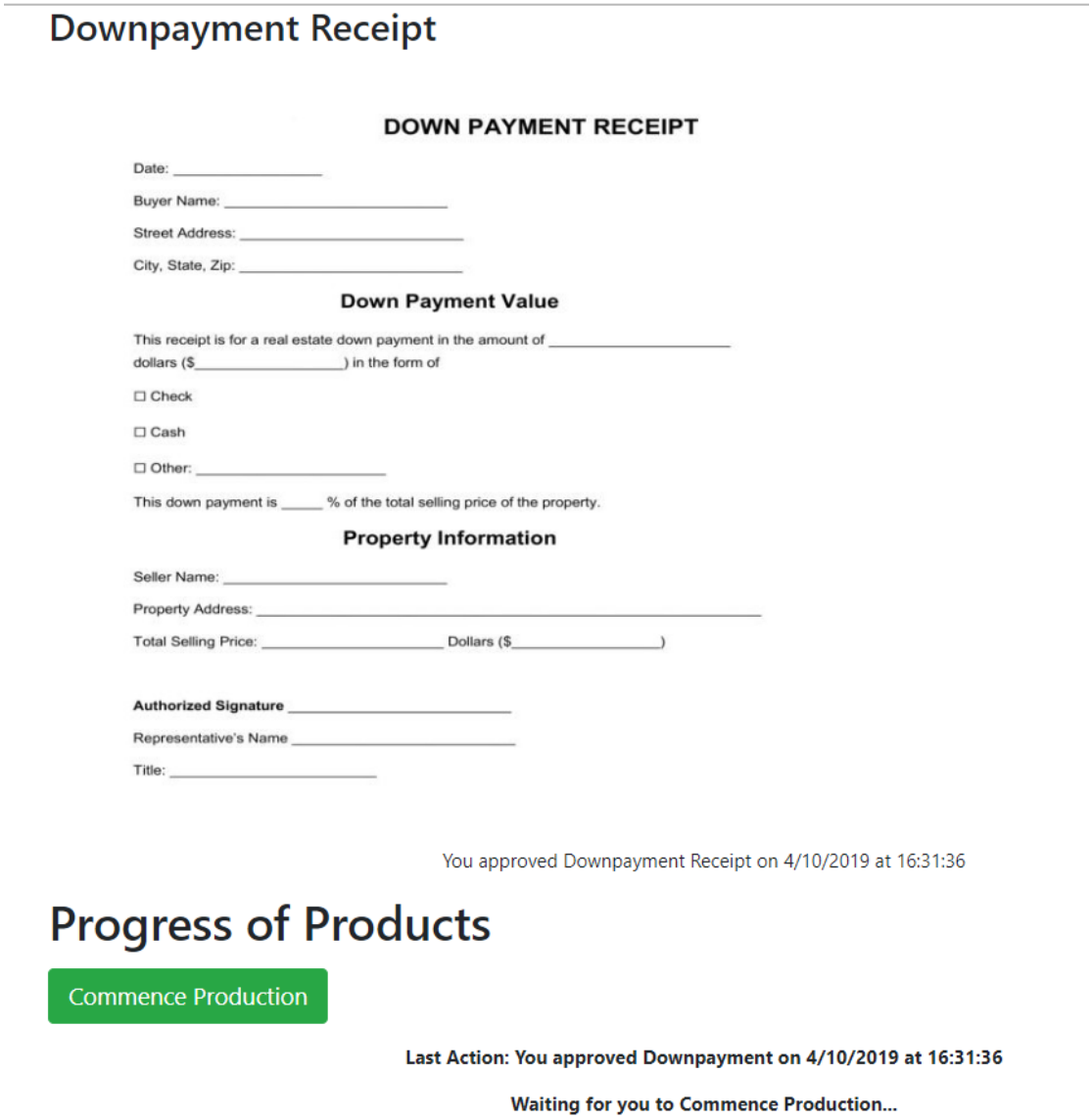
Επίσης, όταν ένα έγγραφο γίνεται approved, το smart contract προχωράει σε επόμενο στάδιο και αυτόματα εξαφανίζονται τα πεδία upload/submit του συγκεκριμένου εγγράφου καθώς αυτό ανέβηκε στο blockchain, έγινε αποδεκτό από τον άλλο χρήστη και δεν μπορεί να μεταβληθεί πλέον.

Για παράδειγμα, έτσι είναι η εφαρμογή πριν:



Screenshot 8

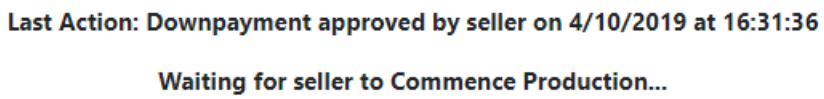
και μετά την αποδοχή της προκαταβολής (Downpayment) από τον πωλητή:



Screenshot 9

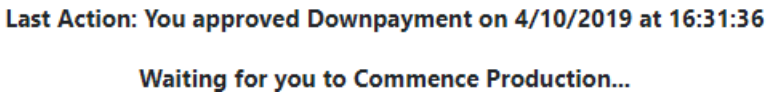
Επίσης, επειδή κάθε στάδιο εμφανίζεται με την σειρά του σε κάθε site και αφού ολοκληρωθεί το προηγούμενό του, κάθε φορά ο αγοραστής και ο πωλητής πληροφορούνται για το τι πρέπει να γίνει προκειμένου να προχωρήσει το συμβόλαιο στο επόμενο στάδιο.

Για παράδειγμα στο στάδιο 2 έχω για τον αγοραστή:



Screenshot 10

Και για τον πωλητή:

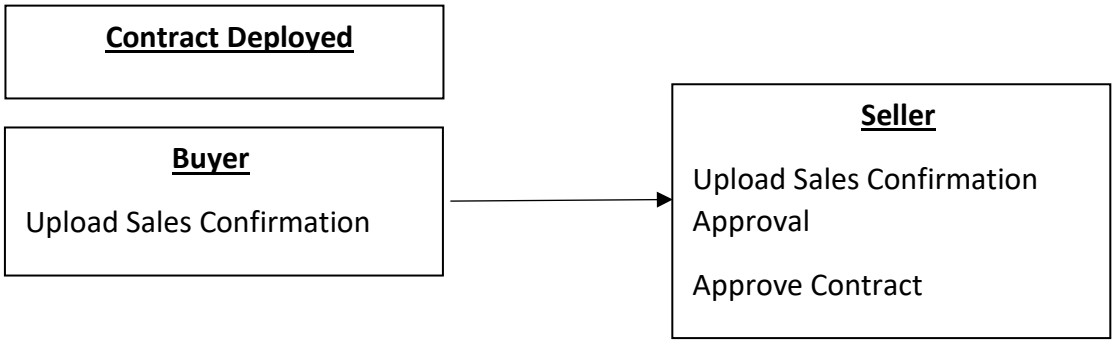


Screenshot 11

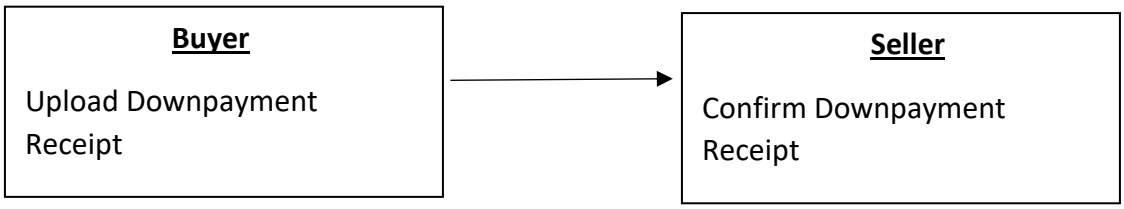
8.6 Ανάλυση των σταδίων της εφαρμογής και σχηματική απεικόνιση

Στο παρακάτω διάγραμμα δίνονται σχηματικά τα στάδια αλληλεπίδρασης μεταξύ αγοραστή και πωλητή για μια πιο άμεση επαφή με τη λειτουργία της εφαρμογής:

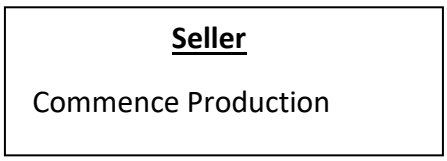
Stage 0



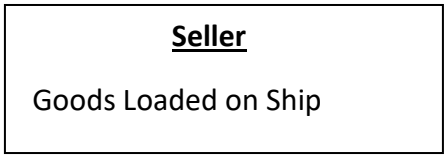
Stage 1



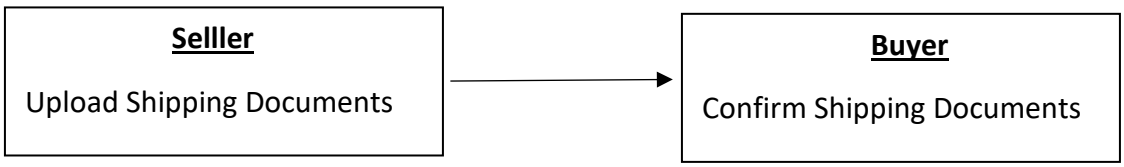
Stage 2



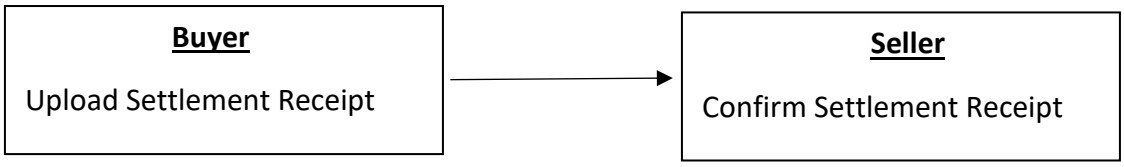
Stage 3



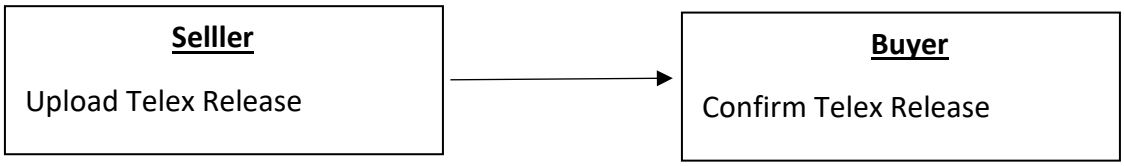
Stage 4



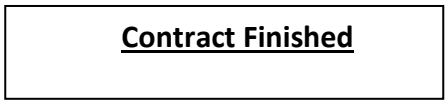
Stage 5



Stage 6

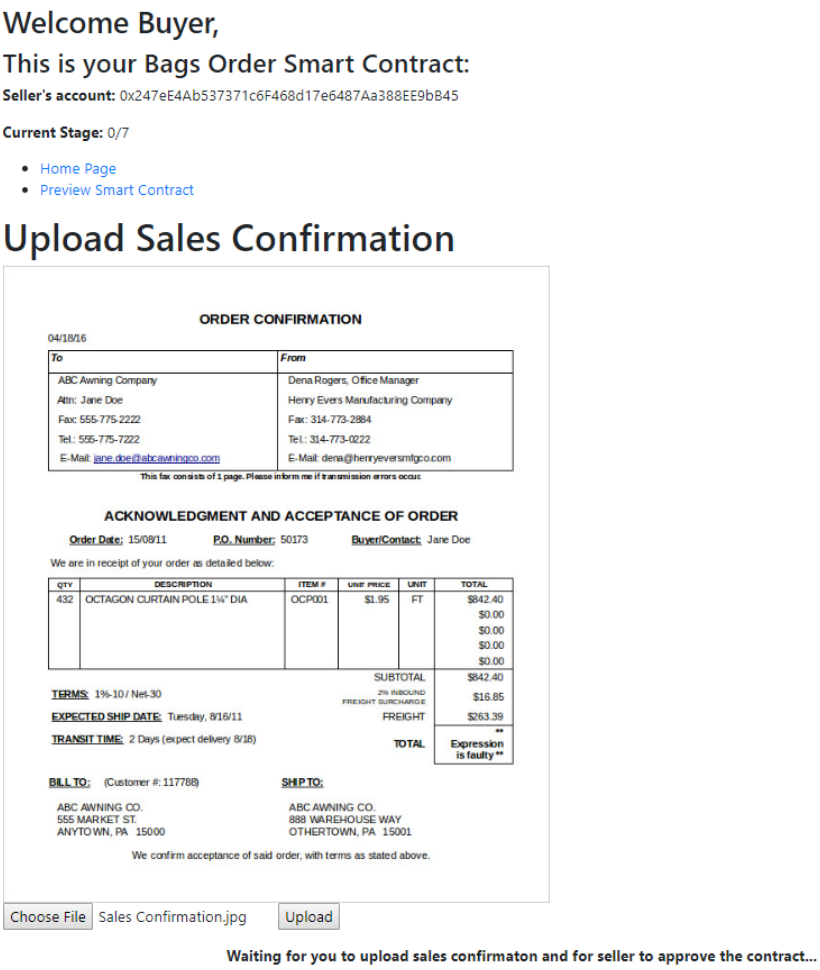


Stage 7



Διάγραμμα 1: *Σχηματική αναπαράσταση των σταδίων αλληλεπίδρασης αγοραστή-πωλητή για την ολοκλήρωση του smart contract.*

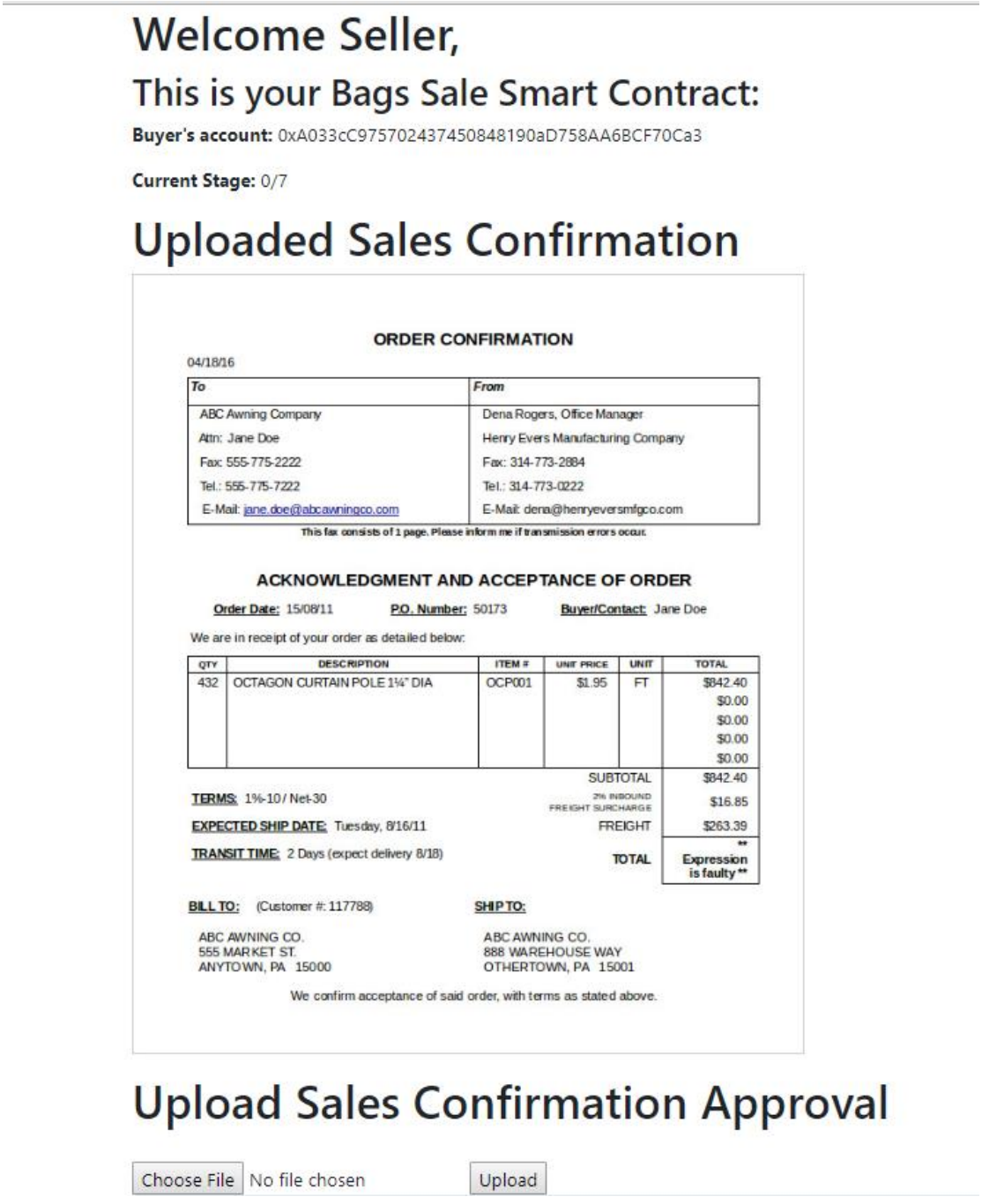
Αρχικά, στο στάδιο 0, ο αγοραστής (buyer) μέσα από την ιστοσελίδα του κάνει Upload το Sales Confirmation:



Screenshot 12

Αυτό είναι ένα αρχείο με ένα συγκεκριμένο hash το οποίο και αποθηκεύεται στο blockchain με αποτέλεσμα να μην μπορεί να αλλαχτεί από κανέναν. Έτσι γίνεται και με όλα τα αρχεία της πλατφόρμας.

Στη συνέχεια, ο πωλητής (seller) βλέπει το sales confirmation από την δική του ιστοσελίδα:

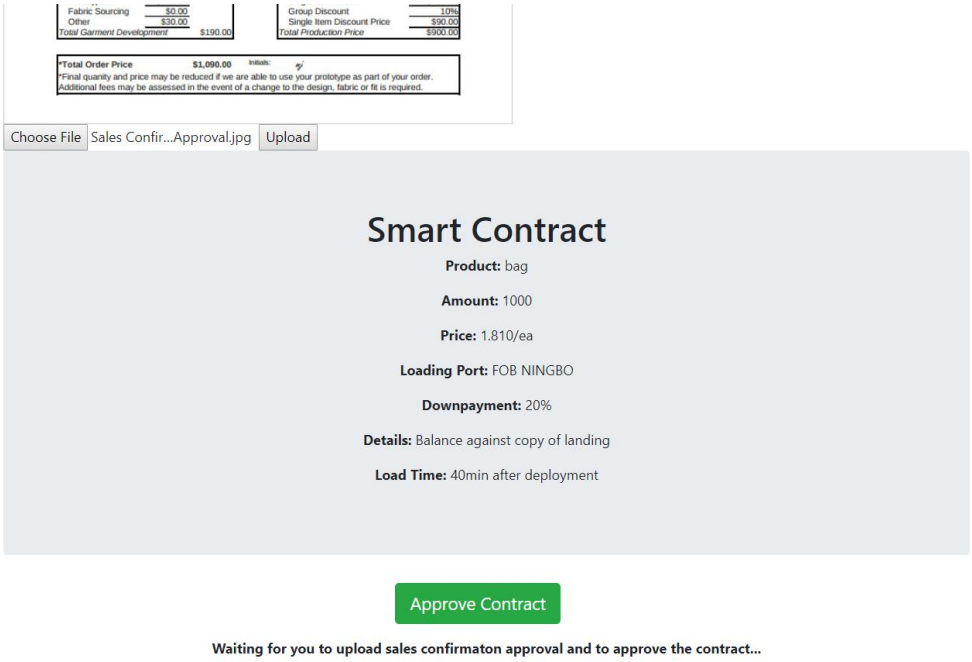


Screenshot 13

Και κάνει με τη σειρά του upload το Sales Confirmation Approval:

Screenshot 14

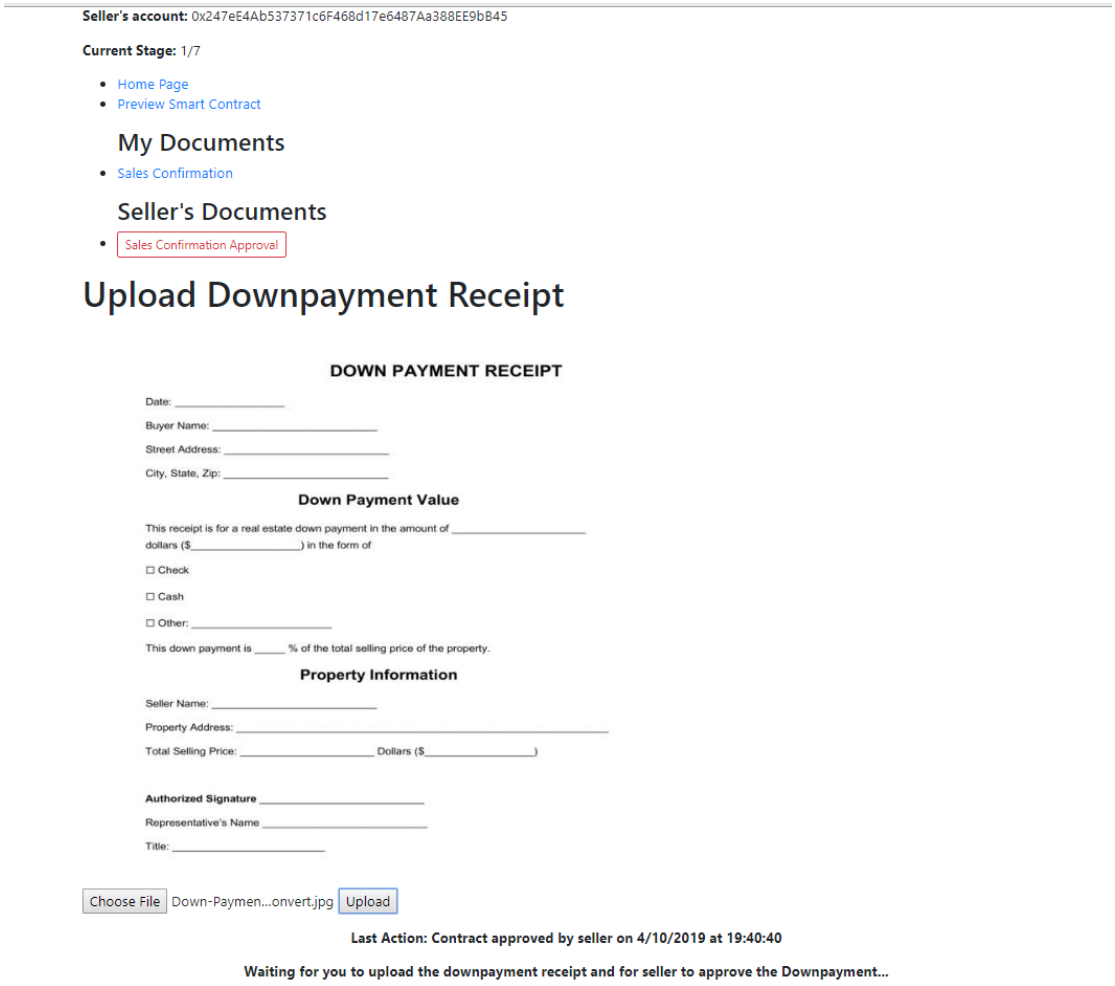
Επίσης βλέπει τις πληροφορίες του συμβολαίου που έχει ανέβει στο blockchain και εφόσον συμφωνεί αποδέχεται το συμβόλαιο (Approve Contract):



Screenshot 15

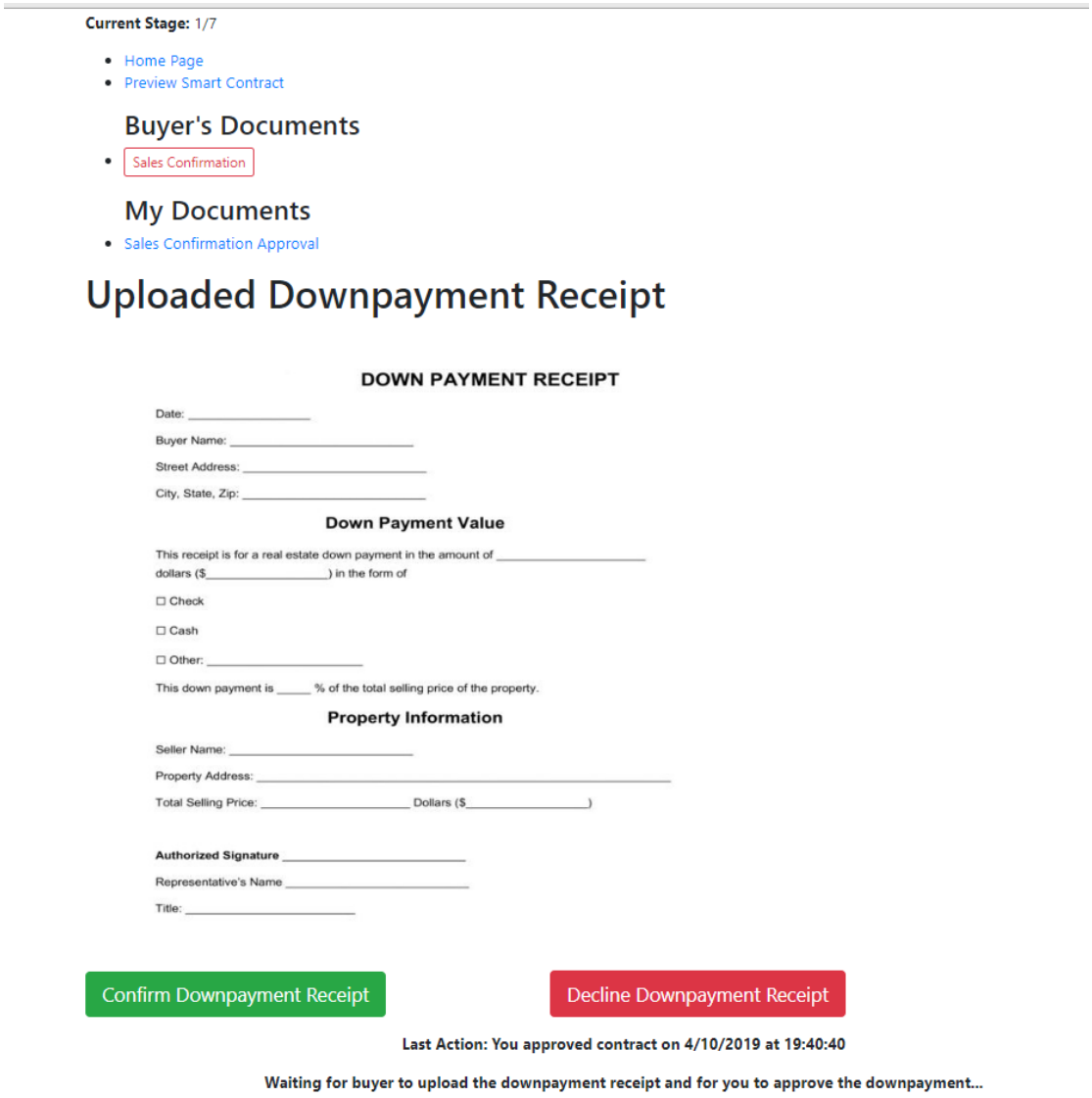
Τότε ολοκληρώνεται και το στάδιο 0 της εφαρμογής και προχωρά στο επόμενο εμφανίζοντας τα κατάλληλα πεδία στους δύο χρήστες, τα οποία προηγουμένως δεν εμφανίζονταν.

Στο στάδιο 1 ο αγοραστής ανεβάζει την απόδειξη της προκαταβολής (Upload Downpayment Receipt) που έχει συμφωνηθεί:



Screenshot 16

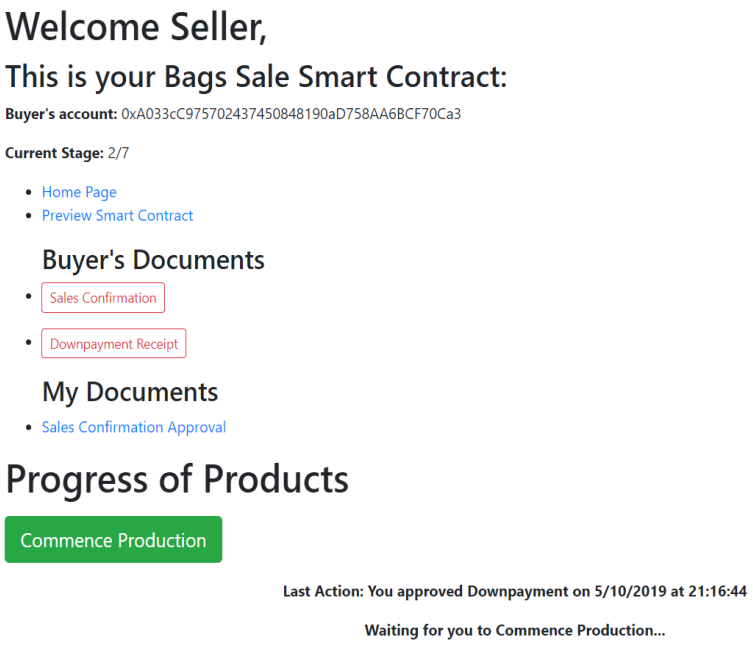
Ο πωλητής την βλέπει και ελέγχει εάν είναι αυτή που συμφωνήθηκε:



Screenshot 17

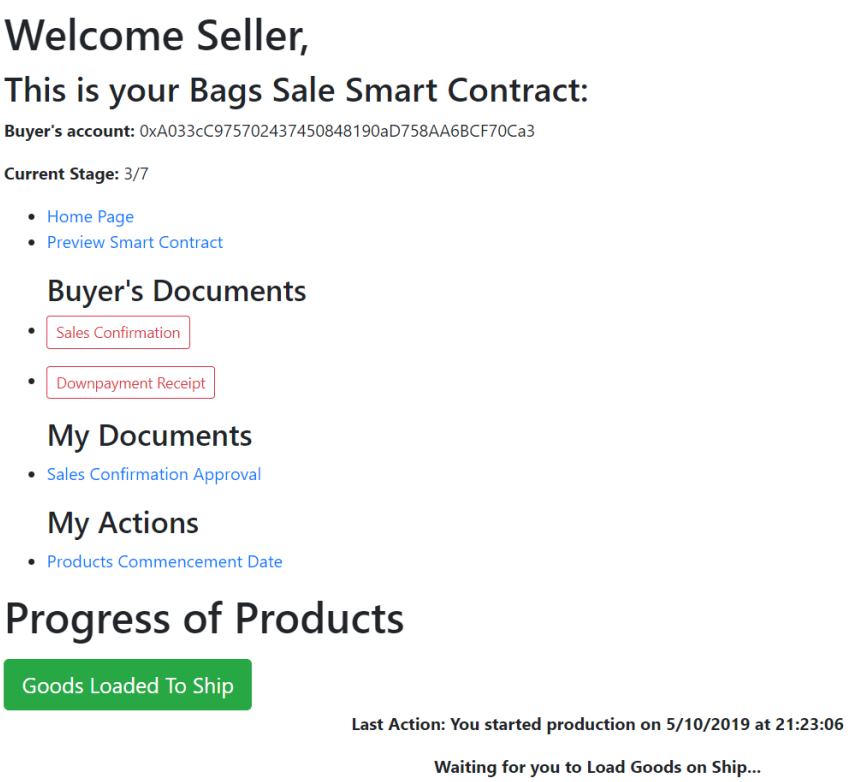
Εάν είναι αυτή που συμφωνήθηκε κάνει αποδοχή της προκαταβολής (Confirm Downpayment Receipt), ενημερώνεται το blockchain και η πλατφόρμα προχωρά στο επόμενο στάδιο ανοίγοντας πάλι τα κατάλληλα πεδία στους χρήστες, όπου πριν δεν εμφανίζονταν.

Προχωρώντας, τα επόμενα 2 στάδια είναι καθαρά του πωλητή καθώς έχουν να κάνουν με την διαδικασία παραγωγής και φόρτωσης των προϊόντων. Ειδικότερα, ο πωλητής δηλώνει το πότε ξεκινάει τη διαδικασία παραγωγής των ζητούμενων προϊόντων (Commence Production):



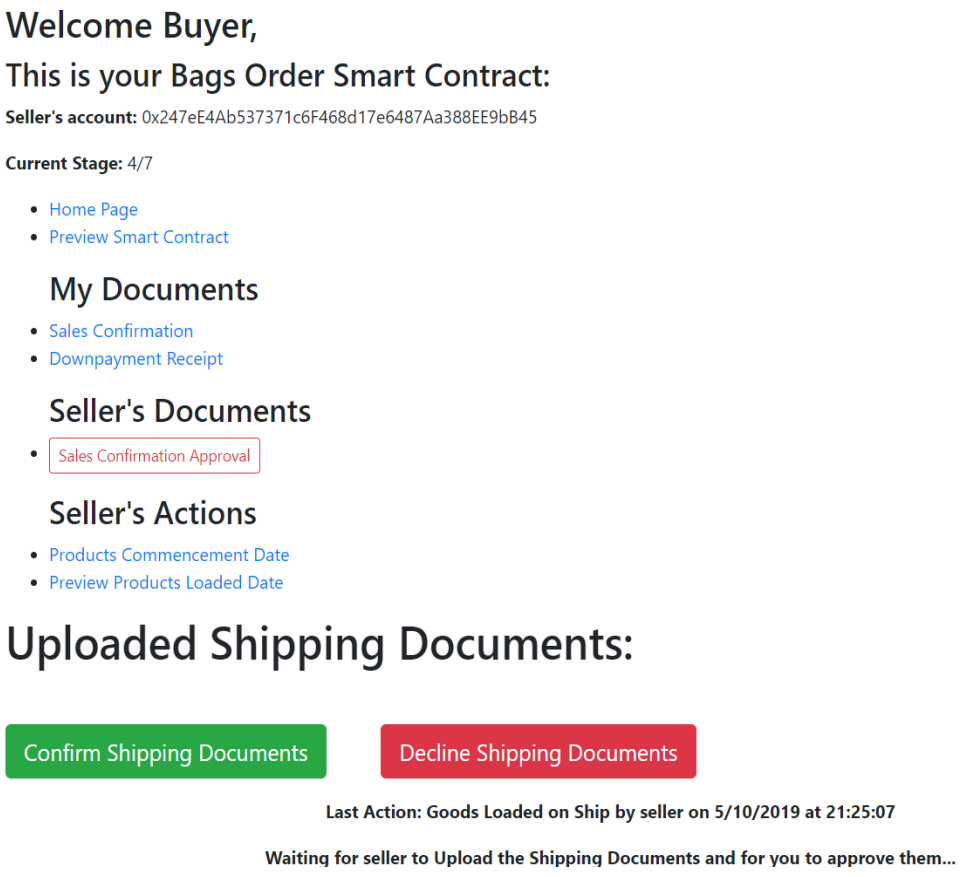
Screenshot 18

καθώς και το πότε φορτώνει τα προϊόντα στο πλοίο (Goods Loaded on Ship):



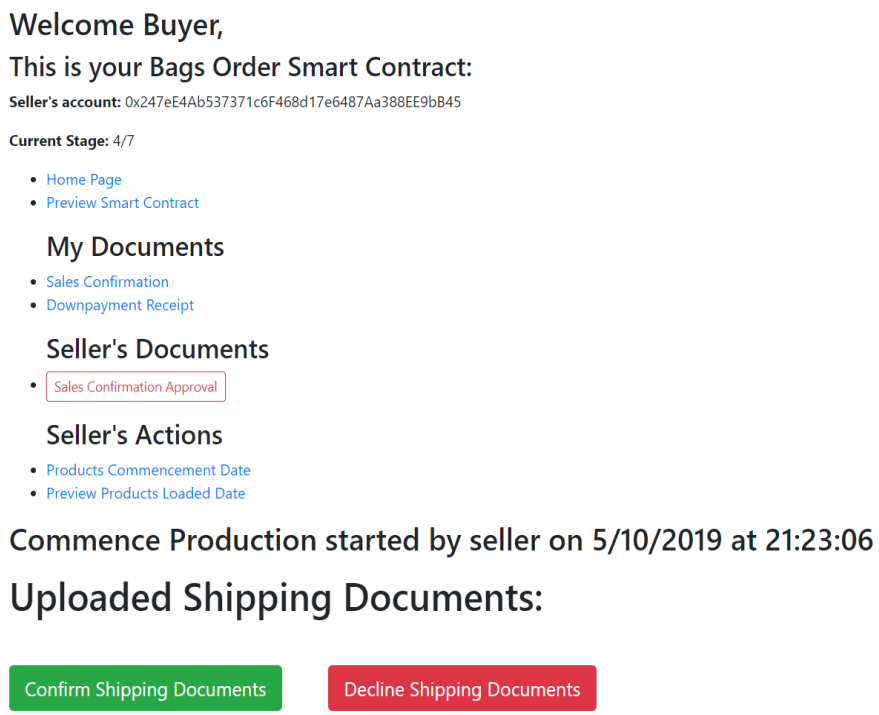
Screenshot 19

Ώστε να μένει ενήμερος και ο αγοραστής μέσα από την δικιά του ιστοσελίδα:



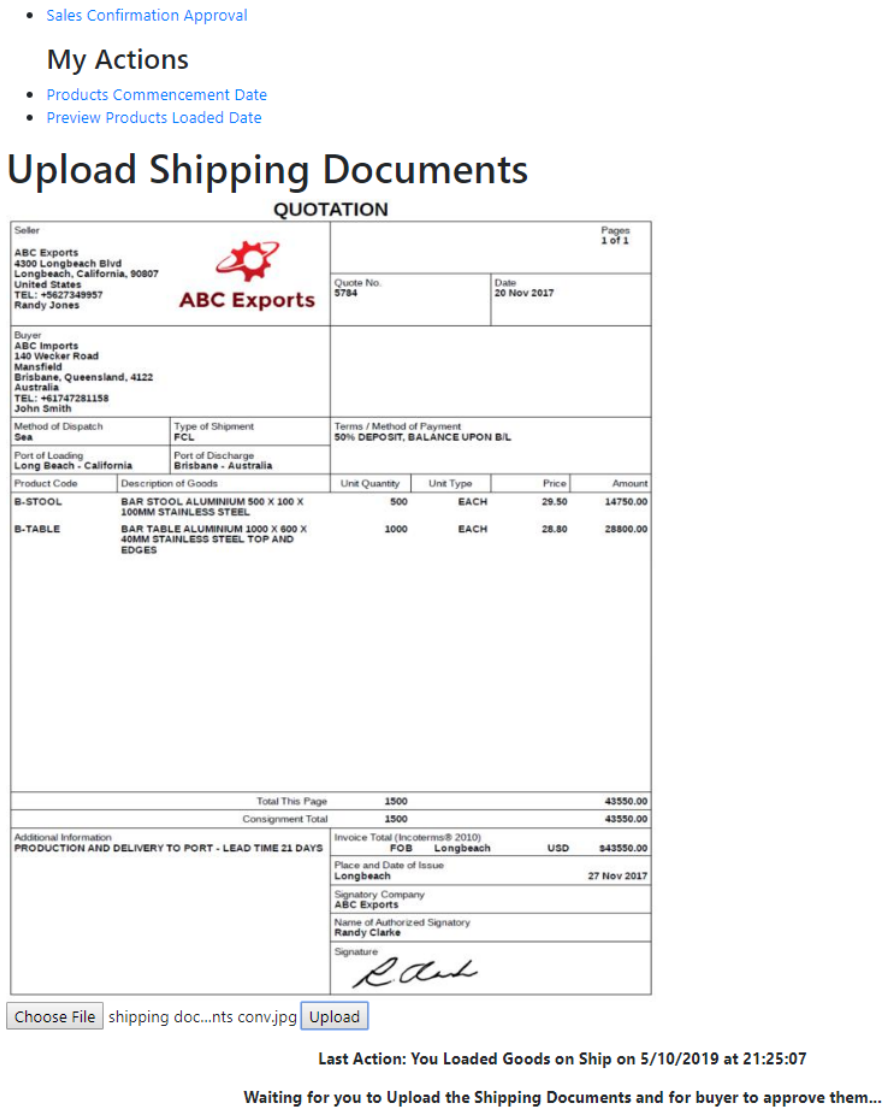
Screenshot 20

Πατώντας, όταν επιθυμεί στο αντίστοιχο link κάτω από το seller’s action (παραδείγματος χάρη στο Products Commencement Date για να δει πότε ξεκίνησε η διαδικασία παραγωγής των προϊόντων):



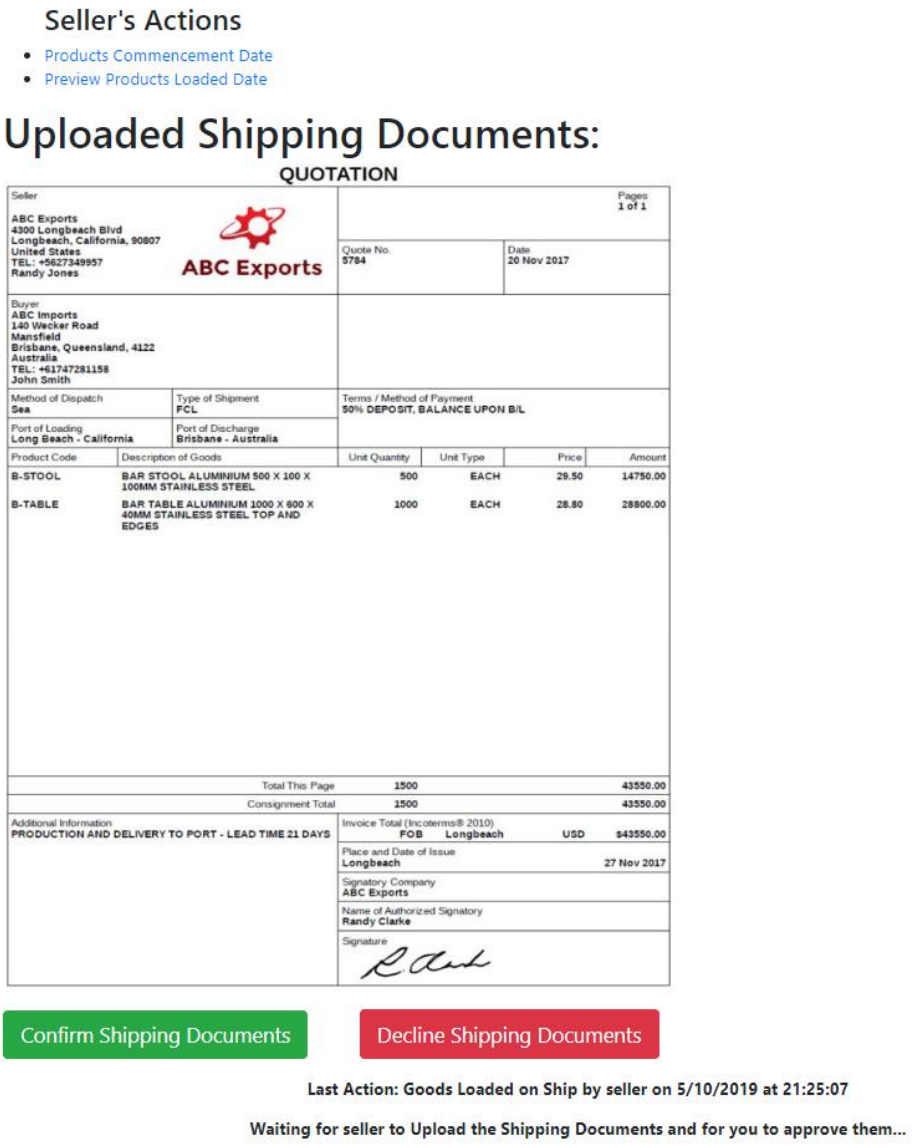
Screenshot 21

Στο στάδιο 4 ο πωλητής πάλι ανεβάζει τα ναυτιλιακά έγγραφα (Shipping Documents):



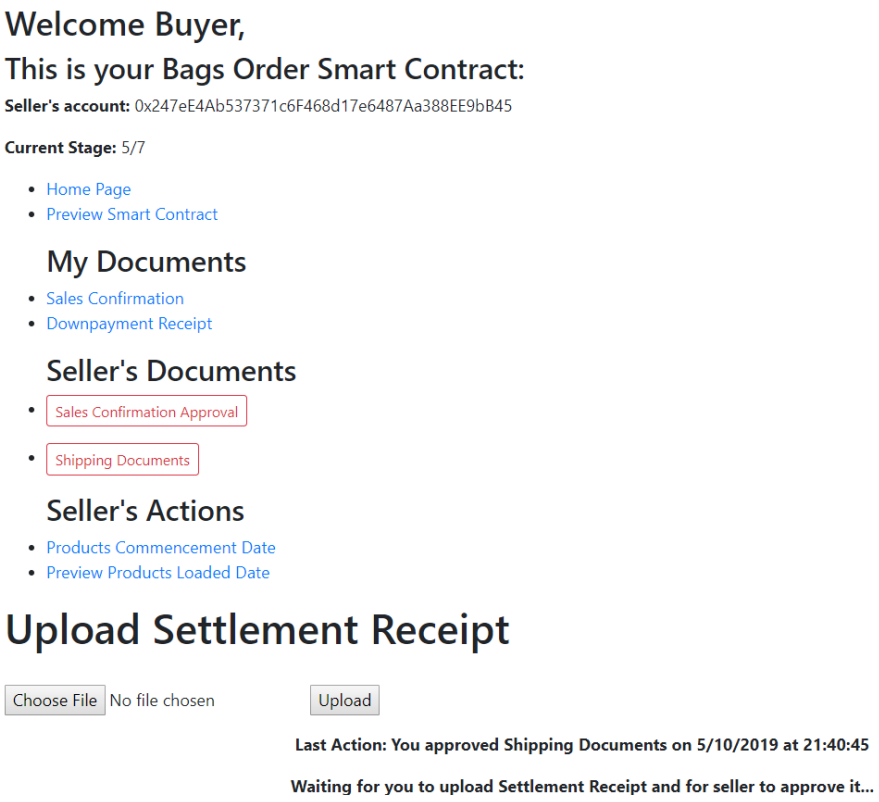
Screenshot 22

τα οποία βλέπει ο αγοραστής:



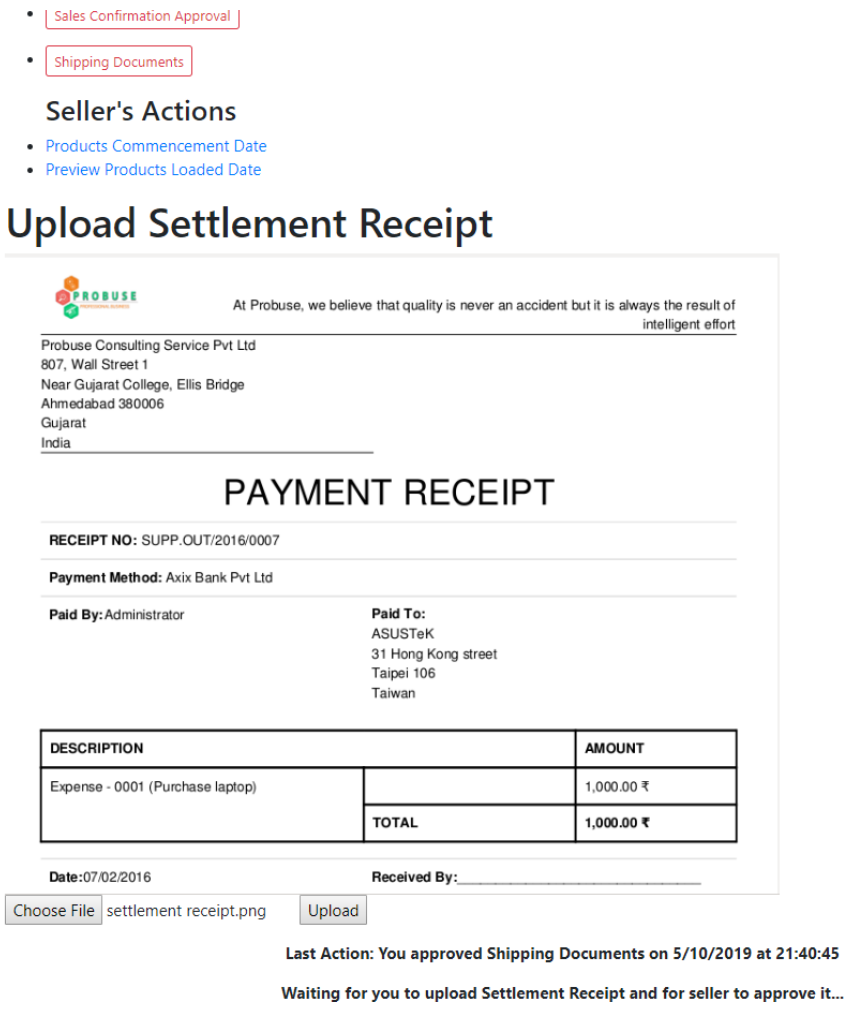
Screenshot 23

και τα αποδέχεται εάν συμφωνεί (Confirm Shipping Documents):



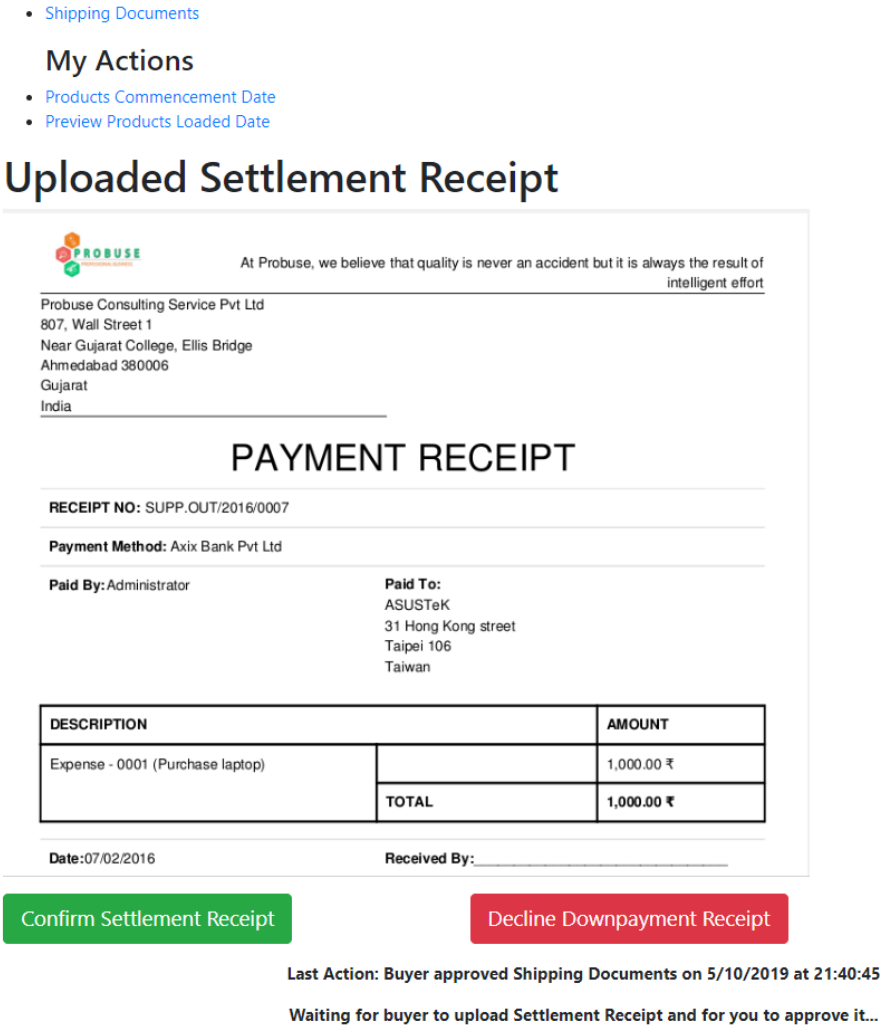
Screenshot 24

Στο στάδιο 5, ο αγοραστής ανεβάζει την απόδειξη της τελικής πληρωμής (Upload Settlement Receipt):



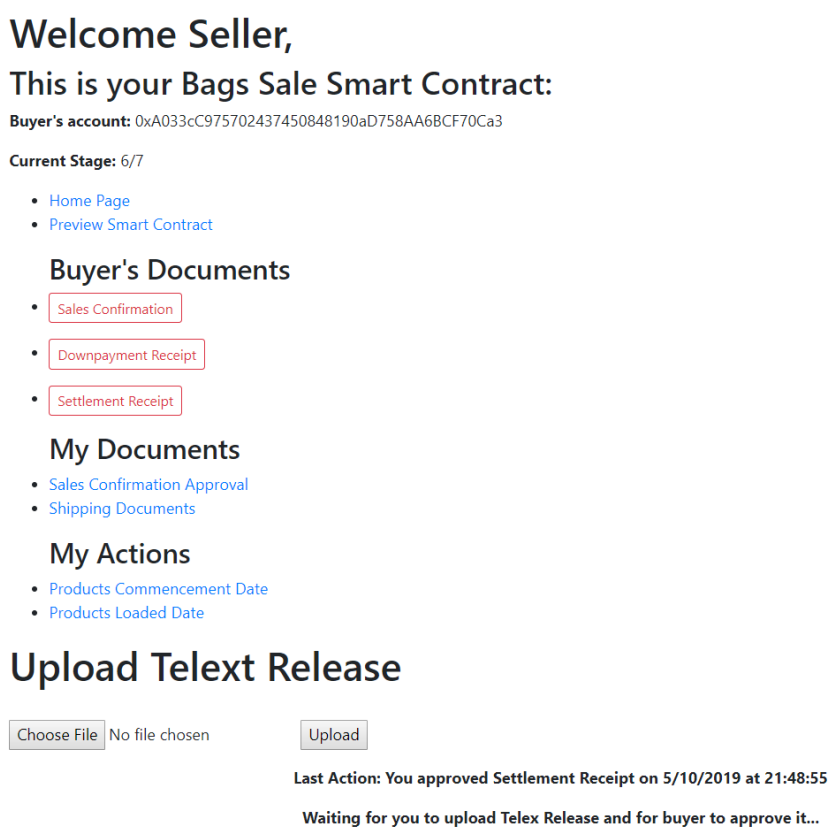
Screenshot 25

και ο πωλητής την εξετάζει:



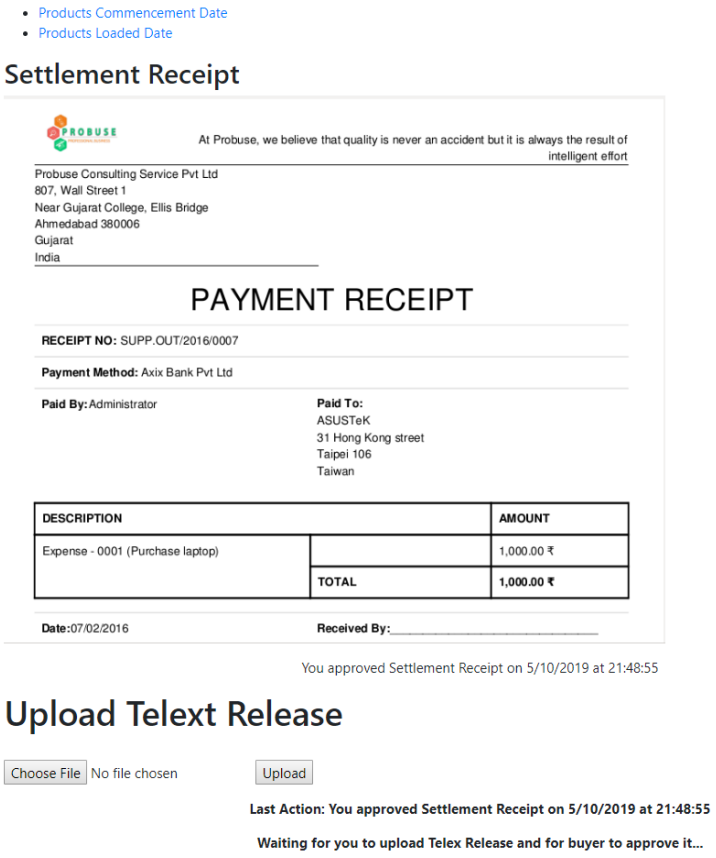
Screenshot 26

και την αποδέχεται εάν είναι αυτή που συμφωνήθηκε (Confirm Settlement Receipt):



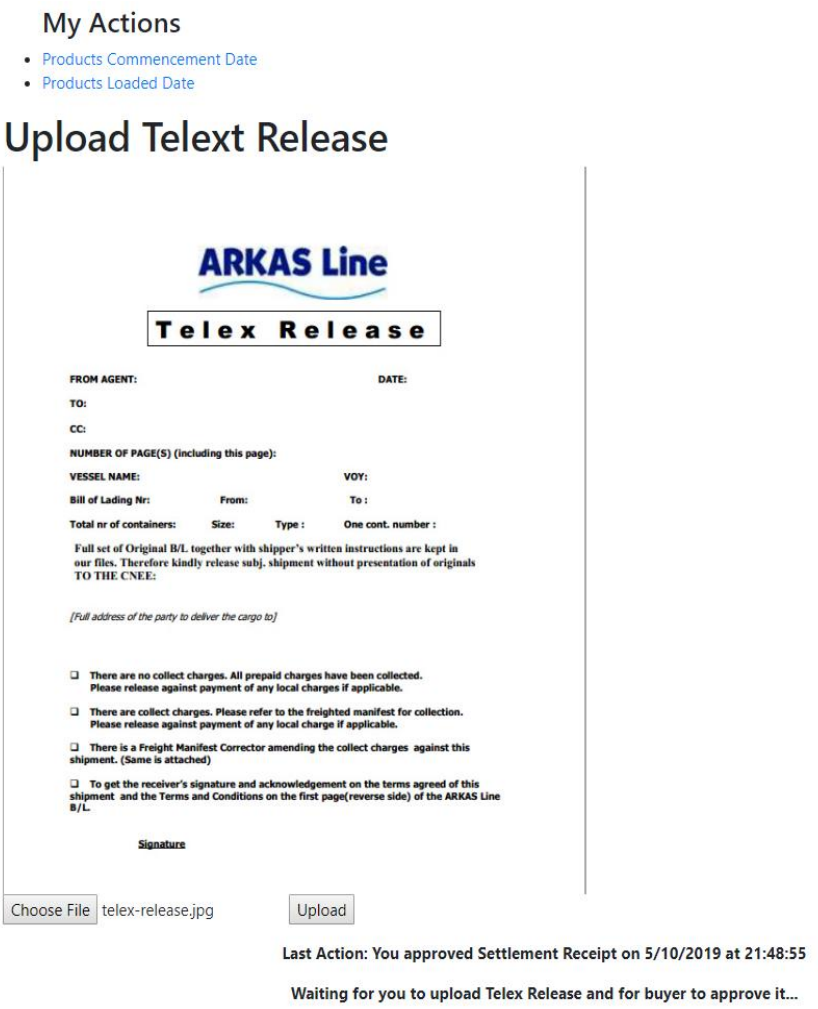
Screenshot 27

Ανά πάσα στιγμή, ο αγοραστής ή ο πωλητής μπορούν να δουν κάθε έγγραφο που έχει ανέβει και έχει γίνει αποδεχτό. Για παράδειγμα, ο πωλητής μπορεί να πατήσει για να δει το Settlement Receipt που μόλις αποδέχθηκε πατώντας στο αντίστοιχο link και μαζί προβάλλονται και η ώρα και ημερομηνία που αυτό έγινε αποδεχτό:



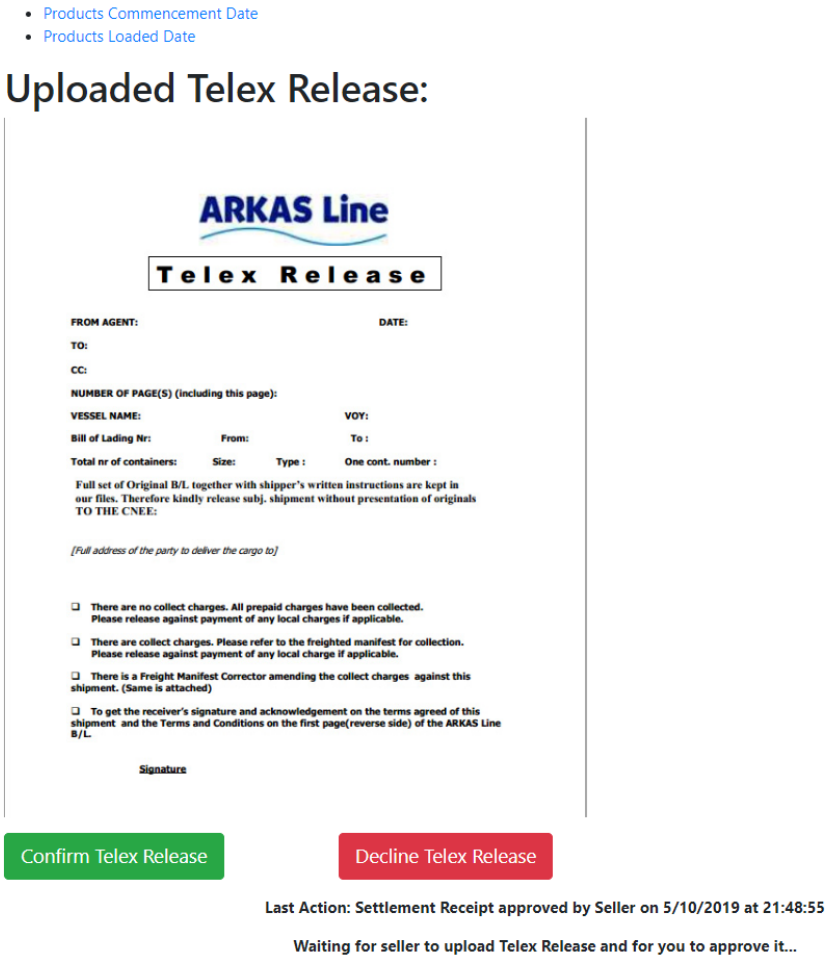
Screenshot 28

Τέλος, στο στάδιο 6, ο πωλητής ανεβάζει το Telex Release (Upload Telex Release):



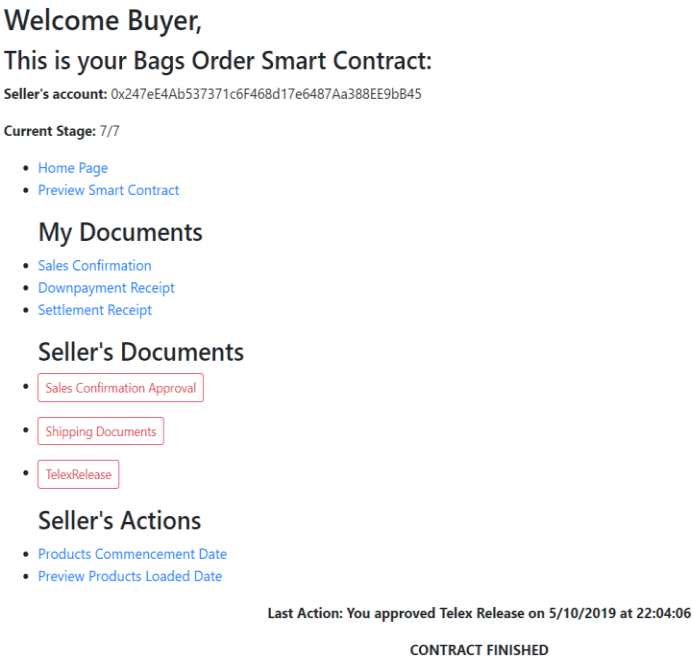
Screenshot 29

και ο αγοραστής το βλέπει και συμφωνεί ή διαφωνεί με αυτό (Confirm Telex Release):



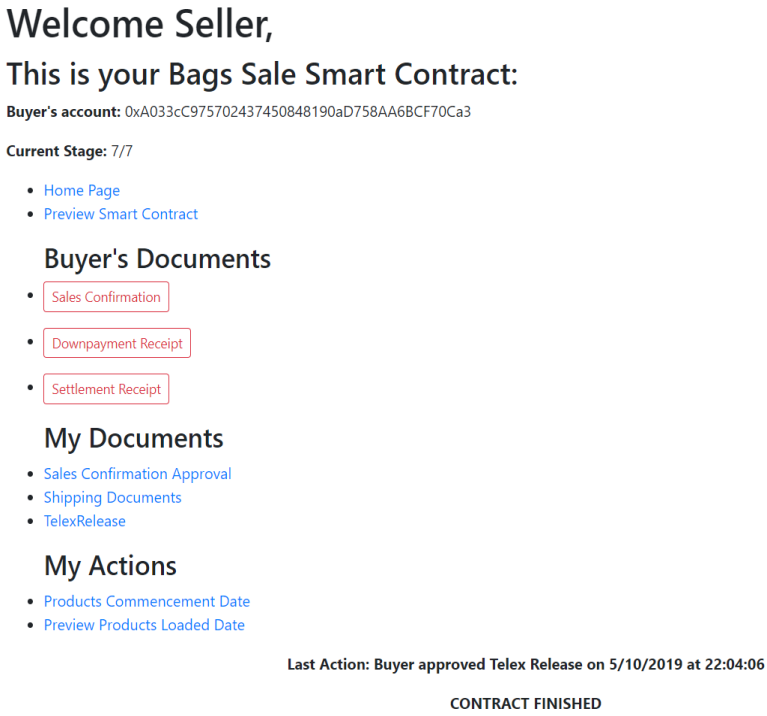
Screenshot 30

Εάν το αποδεχθεί ολοκληρώνεται και το τελευταίο στάδιο της εφαρμογής και ολοκληρώνεται η διαδικασία αγοράς-πώλησης:



Screenshot 31

Φυσικά και ο πωλητής ενημερώνεται με το κατάλληλο μήνυμα για την ολοκλήρωση της διαδικασίας:



Screenshot 32

8.7 Κόστος

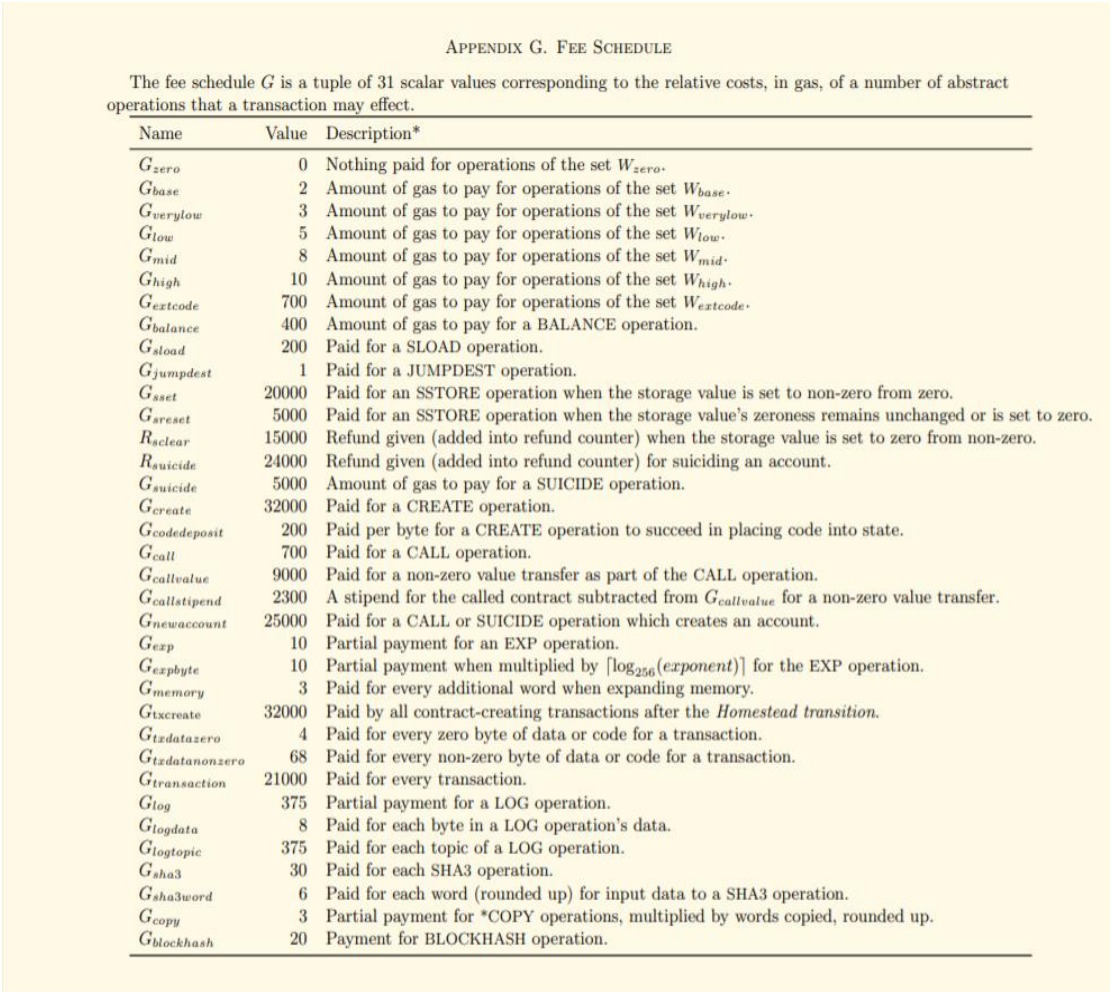
Αρχικά, το κόστος του κάθε upload είναι μηδαμινό καθώς ουσιαστικά πρόκειται για 1 μόνο transaction στο smart contract το οποίο και αποθηκεύει στο συμβόλαιο το hash της εικόνας που ανέβασε ο χρήστης ώστε να μπορεί να το χρησιμοποιήσει στο μέλλον και να μη χαθεί (ουσιαστικά μια απλή συνάρτηση set(x)). Συνεπώς, σύμφωνα με το white paper του Ethereum (Wood, 2019) , φαίνεται πως το κόστος της πράξης SSTORE είναι:

Gas Required	Cost (ETH)	Cost (USD)
20000	0.0006	0.177

Η εικόνα αποθηκεύεται στο ipfs και κάθε φορά που πρέπει να προβληθεί απλά καλείται ένα ipfs link που στο τέλος περιέχει το hash της εικόνας(https://ipfs.io/ipfs/${this.state.ipfsHash5) το οποίο βρίσκεται από το smart contract , όπου αποθηκεύτηκε προηγουμένως. Όμως αυτό το hash είναι στο smart contract δηλωμένο σαν public μεταβλητή και όταν καλείται η τιμή μιας public μεταβλητής στο συμβόλαιο δεν υπάρχει κάποιο κόστος. Συνεπώς και για να προβληθεί η εικόνα δεν υπάρχει κάποιο κόστος.

Επίσης τα confirmation buttons είναι απλές συναρτήσεις που στην ουσία μόνο αλλάζουν το στάδιο του συμβολαίου, όταν πληρούνται οι ζητούμενες συνθήκες και άρα το κόστος είναι πολύ χαμηλό.

Παρακάτω παρατίθεται ένα αρχείο από το white paper του Ethereum, όπου φαίνεται πόσο μπορεί να κοστίζει μια διαδικασία.



APPENDIX G. FEE SCHEDULE

The fee schedule G is a tuple of 31 scalar values corresponding to the relative costs, in gas, of a number of abstract operations that a transaction may effect.

Name	Value	Description*
G_{zero}	0	Nothing paid for operations of the set W_{zero}.
G_{base}	2	Amount of gas to pay for operations of the set W_{base}.
$G_{verylow}$	3	Amount of gas to pay for operations of the set $W_{verylow}$.
G_{low}	5	Amount of gas to pay for operations of the set W_{low}.
G_{mid}	8	Amount of gas to pay for operations of the set W_{mid}.
G_{high}	10	Amount of gas to pay for operations of the set W_{high}.
$G_{extcode}$	700	Amount of gas to pay for operations of the set $W_{extcode}$.
$G_{balance}$	400	Amount of gas to pay for a BALANCE operation.
G_{sload}	200	Paid for a SLOAD operation.
$G_{jumpdest}$	1	Paid for a JUMPDEST operation.
G_{sset}	20000	Paid for an SSTORE operation when the storage value is set to non-zero from zero.
G_{sreset}	5000	Paid for an SSTORE operation when the storage value's zeroness remains unchanged or is set to zero.
R_{sclear}	15000	Refund given (added into refund counter) when the storage value is set to zero from non-zero.
$R_{suicide}$	24000	Refund given (added into refund counter) for suiciding an account.
$G_{suicide}$	5000	Amount of gas to pay for a SUICIDE operation.
G_{create}	32000	Paid for a CREATE operation.
$G_{codedeposit}$	200	Paid per byte for a CREATE operation to succeed in placing code into state.
G_{call}	700	Paid for a CALL operation.
$G_{callvalue}$	9000	Paid for a non-zero value transfer as part of the CALL operation.
$G_{callstipend}$	2300	A stipend for the called contract subtracted from $G_{callvalue}$ for a non-zero value transfer.
$G_{newaccount}$	25000	Paid for a CALL or SUICIDE operation which creates an account.
G_{exp}	10	Partial payment for an EXP operation.
$G_{expbyte}$	10	Partial payment when multiplied by $\lceil \log_{256}(exponent) \rceil$ for the EXP operation.
G_{memory}	3	Paid for every additional word when expanding memory.
$G_{txcreate}$	32000	Paid by all contract-creating transactions after the *Homestead transition*.
$G_{txdatazero}$	4	Paid for every zero byte of data or code for a transaction.
$G_{txdatanonzero}$	68	Paid for every non-zero byte of data or code for a transaction.
$G_{transaction}$	21000	Paid for every transaction.
G_{log}	375	Partial payment for a LOG operation.
$G_{logdata}$	8	Paid for each byte in a LOG operation's data.
$G_{logtopic}$	375	Paid for each topic of a LOG operation.
G_{sha3}	30	Paid for each SHA3 operation.
$G_{sha3word}$	6	Paid for each word (rounded up) for input data to a SHA3 operation.
G_{copy}	3	Partial payment for *COPY operations, multiplied by words copied, rounded up.
$G_{blockhash}$	20	Payment for BLOCKHASH operation.

Εικόνα 17: Gas Cost σύμφωνα με το Ethereum White Paper (Wood, 2019)

Τώρα, όσον αφορά το κόστος αρχικοποίησης (migration cost) αυτό εξαρτάται κυρίως από τους παρακάτω παράγοντες:

Από ένα σταθερό κόστος για τη δημιουργία του smart contract, που όπως φαίνεται από το white paper του ethereum είναι (πράξη CREATE):

Gas Required	Cost (ETH)	Cost (USD)
32000	0.00096	0.2832

και από το μέγεθος του bytecode όταν γίνεται compile το smart contract , δηλαδή από το πόσο μεγάλο είναι το συμβόλαιο.

Στο συγκεκριμένο συμβόλαιο το migration cost είναι περίπου 15 ευρώ.

9 Επίλογος

Σε αυτήν την διπλωματική εργασία πραγματοποιήθηκε η υλοποίηση μια αποκεντρωμένης εφαρμογής (DApp) σε συνεργασία με την Spirit Innovations που αφορά την σύναψη ενός συμβολαίου-συμφωνίας. Έγινε εκτενής ανάλυση της τεχνολογίας του blockchain, των έξυπνων συμβολαίων και των αποκεντρωμένων εφαρμογών με σκοπό να προβληθεί όλη η τεχνολογία στην οποία βασίζεται η εφαρμογή. Επίσης, πραγματοποιήθηκε αναφορά σε όλα τα εργαλεία που χρησιμοποιήθηκαν για την ανάπτυξη της, όπως η πλατφόρμα του Ethereum και το IPFS (InterPlanetary File System). Στη συνέχεια μέσα από την αναφορά των υπαρχόντων προβλημάτων στον χώρο δραστηριοποίησης της εταιρείας , εξηγήθηκε πως η συγκεκριμένη εφαρμογή προσφέρει τις ανάλογες λύσεις. Προβλήθηκε, αναλυτικά ο τρόπος λειτουργίας της και αναλύθηκαν όλα τα στάδια και οι δυνατότητες της. Ως αποτέλεσμα, ο χρήστης μπορεί να κατανοήσει τις απεριόριστες δυνατότητες που οι αποκεντρωμένες εφαρμογές προσφέρουν και να εξοικειωθεί με τον κόσμο του blockchain.

Συμπερασματικά, πριν την υλοποίηση της υπήρχαν τεράστιοι χρόνοι αναμονής αφού η επικοινωνία μεταξύ των εταιρειών γινόταν με mail, κάθε εμπλεκόμενο μέρος μπορούσε να μεταβάλλει τους όρους του κάθε συμβολαίου ή εγγράφου που ανταλλασσόταν προς συμφέρον του και δεν υπήρχαν πουθενά όλα μαζί τα έγγραφα που αφορούσαν μια συμφωνία ή το παρόν στάδιο στο οποίο βρίσκεται. Όλα αυτά αντιμετωπίστηκαν μέσω της υλοποίησης της συγκεκριμένης εφαρμογής εξασφαλίζοντας ασφάλεια, χρόνο και ευχρηστία. Επίσης, σε αντίθεση με τις συμβατικές εφαρμογές δεν υπάρχει ποτέ περίπτωση η αποκεντρωμένη εφαρμογή να κλείσει ή να διακοπεί η λειτουργία της και δεν ανήκει σε καμία αρχή, ώστε να χειραγωγηθεί.

Ως περαιτέρω έρευνα, θα μπορούσε να γραφεί κώδικας για να αποφεύγεται το confirmation button που εμφανίζεται στο metamask κάθε φορά που ο χρήστης πραγματοποιεί μια συναλλαγή και αλληλεπιδρά με το blockchain. Κάτι τέτοιο θα κάνει την εφαρμογή ακόμα πιο εύχρηστη και ξεκούραστη.

Επίσης, σαν ένα ακόμη πεδίο έρευνας θα μπορούσε να είναι η εγγραφή του χρήστη στην εφαρμογή απλά με ένα username - password και από εκεί και πέρα:

- Εάν, έχει κάποιο account στο blockchain να το δηλώνει και στη συνέχεια να αλληλεπιδρά με αυτό.
- Εάν δεν έχει account στο blockchain, να του δημιουργεί η εφαρμογή ένα κατά την ώρα της εγγραφής και να το ταυτίζει με το username – password που δίνει ο χρήστης.

Έπειτα, κάθε φορά που συνδέεται θα κάνει την είσοδο του απλά με το username-password και η εφαρμογή μέσα από ένα hash table ή mapping που θα έχει

δημιουργήσει θα τον συνδέει με το blockchain account του και θα είναι έτοιμος να αλληλεπιδράσει με αυτήν.

Κάτι, τέτοιο θα ήταν ιδιαίτερα χρήσιμο για τους χρήστες που δεν είναι πολύ ή και καθόλου εξοικειωμένοι με το blockchain, ώστε να τους βοηθήσει σε μια πρώτη επαφή με αυτό.

10 Βιβλιογραφία

(χ.χ.). Ανάκτηση από wikipedia: https://en.wikipedia.org/wiki/InterPlanetary_File_System

(χ.χ.). Ανάκτηση από solidity.readthedocs: https://solidity.readthedocs.io/en/latest/contracts.html#events

(χ.χ.). Ανάκτηση από wikipedia: https://en.wikipedia.org/wiki/Client%E2%80%93server_model

Aziz. (χ.χ.). *mastercrypto*. Ανάκτηση από https://masterthecrypto.com/public-vs-private-blockchain-whats-the-difference/

Capital, Z. (2018, 9 30). Ανάκτηση από hackernoon: hackernoon.com/ipfs-a-complete-analysis-of-the-distributed-web-6465ff029b9b

Consensys. (2016, 6 6). *media*. Ανάκτηση από medium: https://media.consensys.net/technical-introduction-to-events-and-logs-in-ethereum-a074d65dd61e

Morrison, A. (2016, 3 22). Ανάκτηση από pwc: https://usblogs.pwc.com/emerging-technology/how-smart-contracts-automate-digital-business/

Prapat, M. (2018, 8 27). *smartcontract*. Ανάκτηση από hackernoon: https://hackernoon.com/everything-you-need-to-know-about-smart-contracts-a-beginners-guide-c13cc138378a

Pratap, M. (2018, July). *blockchain*. Ανάκτηση από Hackernoon: https://hackernoon.com/blockchain-technology-explained-introduction-meaning-and-applications-edbd6759a2b2

Pratik, R. (2018, 11 5). Ανάκτηση από hackernoon: https://hackernoon.com/what-are-decentralized-applications-dapps-explained-with-examples-7ff8f2c4a460

Rosic, A. (2016). Ανάκτηση από blockgeeks: https://blockgeeks.com/guides/smart-contracts/

Rosic, A. (2019, March 01). *guides/blockchain*. Ανάκτηση από Blockgeeks: https://blockgeeks.com/guides/what-is-blockchain-technology/

Rosic, A. (2019). *guides/ethereum*. Ανάκτηση από blockgeeks: https://blockgeeks.com/guides/ethereum/

Stewart, B. (2018, 7 3). Ανάκτηση από medium: https://medium.com/@BIGbenStew/future-of-work-connecting-the-real-and-digital-worlds-via-smart-contract-events-7d924a21d22d

Wood, D. G. (2019, 8 16). *yellowpaper.* Ανάκτηση από ethereum: https://ethereum.github.io/yellowpaper/paper.pdf