ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΝΑΥΠΗΓΩΝ ΜΗΧΑΝΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΤΟΜΕΑΣ ΜΕΛΕΤΗΣ ΠΛΟΙΟΥ ΚΑΙ ΘΑΛΑΣΣΙΩΝ ΜΕΤΑΦΟΡΩΝ

Διπλωματική Εργασία

ΜΕΙΩΣΗ ΑΕΡΙΩΝ ΡΥΠΩΝ ΜΕ ΧΡΗΣΗ ΣΥΣΤΗΜΑΤΟΣ ΕΜΠΟΡΙΑΣ ΣΤΗΡΙΖΟΜΕΝΕΣ ΣΕ ΚΑΙΝΟΤΟΜΕΣ ΛΥΣΕΙΣ (BLOCKCHAIN)

Επιβλέπων: Νικόλαος Βεντίκος Αναπληρωτής Καθηγητής Ε.Μ.Π.

Ημερομηνία 21/06/2020
Σπουδαστής: Γεννηματάς Χρήστος (nm13039)

Ευχαριστίες

Ξεκινώντας, θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου κ. Ν.Βεντίκο, αναπληρωτή καθηγητή στο Εθνικό Μετσόβιο Πολυτεχνείο, καθώς μέσω εκείνου μου δόθηκε η ευκαιρία να εργαστώ πάνω σε ένα τρέχον ζήτημα της ναυτιλίας με καινοτόμα μέσα. Οι γνώσεις και η εμπειρία που απέκτησα κατά την εκπόνηση αυτής της εργασίας είναι εξαιρετικά διδακτικές και χρήσιμες.

Επιπρόσθετα θα ήθελα να ευχαριστήσω θερμότατα και την κα Ε.Σταματοπούλου, υποψήφια διδάκτωρ του ομώνυμου ιδρύματος. Η υποστήριξη και καθοδήγηση που μου παρείχε ήταν διαθέσιμη και καθοριστική καθ' όλη τη διαδικασία.

Τέλος, ευχαριστώ όλα τα οικεία μου πρόσωπα, που στάθηκαν στο πλευρό μου καθ' όλη τη διάρκεια των σπουδών μου και την εκπόνηση της Διπλωματικής Εργασίας.

Περιεχόμενα

Περίληψη

Στο πλαίσιο των περιβαλλοντικών μεταρρυθμίσεων που λαμβάνουν χώρα στη ναυτιλία, στην ευρωπαϊκή ένωση μελετάται η μείωση των αέριων ρύπων, όπως για παράδειγμα του διοξειδίου του άνθρακα. Ωστόσο ο χώρος της ναυτιλίας χαρακτηρίζεται από μεγάλη αδράνεια σε θέματα προσαρμοστικότητας σε ότι αφορά τις πλοιοκτήτριες εταιρίες, με αποτέλεσμα να καθίσταται δύσκολη η επίτευξη των απαιτητικών στόχων που έχουν τεθεί. Η ανάγκη για ένα οικονομικό σύστημα που θα λειτουργήσει σαν κίνητρο ανάπτυξης νέων πράσινων τεχνολογιών είναι εμφανής και στην Ε.Ε. ερευνώνται ήδη οικονομικά συστήματα ως προέκταση του MRV, με τη μορφή φορολογίας ή συμπερίληψης της ναυτιλίας στο EU ETS (Emissions Trading Scheming).

Ως απάντηση στο παραπάνω πρόβλημα προτείνεται η ανάπτυξη ενός συστήματος εμπορίας αέριων ρύπων, το οποίο θα δημιουργήσει περιβάλλον εύνοιας προς τη δραστική μείωση των ρύπων, προσφέροντας επιβράβευση στην προσαρμογή, ωστόσο αποφεύγοντας μη βιώσιμες πιέσεις προς τις εταιρίες. Στην παρούσα εργασία μελετώνται τα περιβαλλοντικά προβλήματα που αντιμετωπίζονται στη ναυτιλία, την αναμενόμενη εξέλιξή τους, καθώς πραγματοποιείται και η ανάπτυξη και αξιολόγηση ενός συστήματος καταγραφής και εμπορίας αέριων ρύπων, στη βάση του οποίου θα γίνει χρήση της τεχνολογίας μπλοκ αλυσίδας (Blockchain).

Abstract

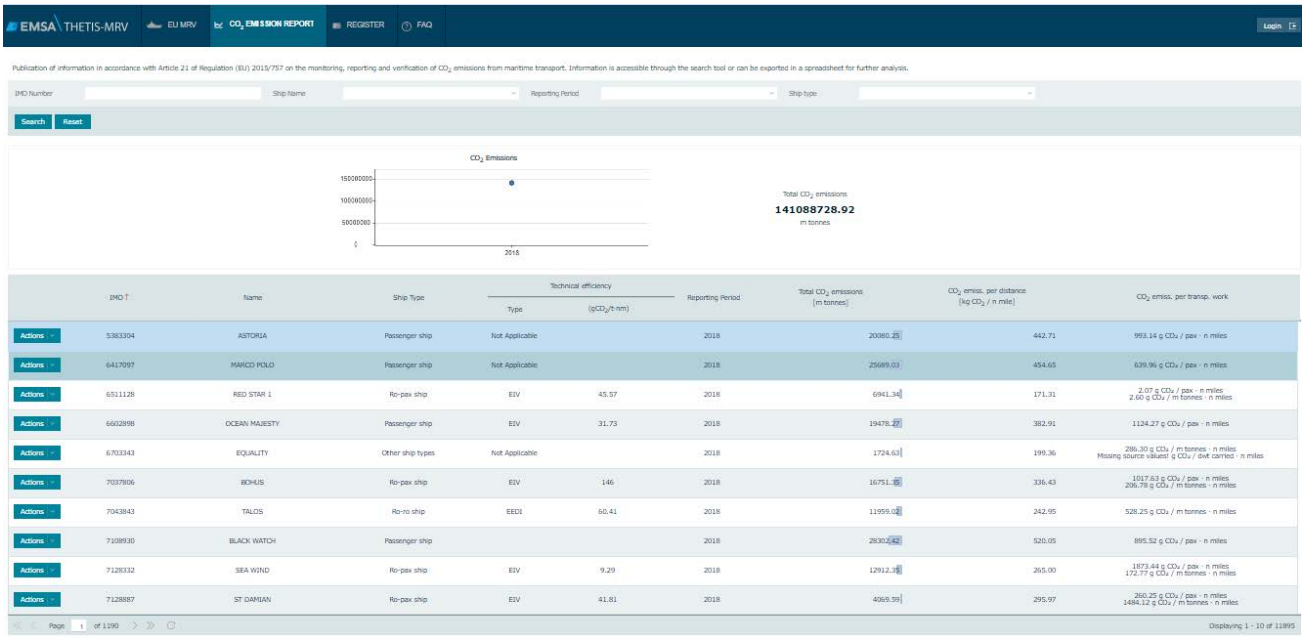
In the context of environmental reforms taking place in maritime, discussion in Europe has been focused upon reduction of gas emissions, such as carbon dioxide. On the contrary, however, the field of maritime and especially large shipping companies are characterized by great inaction as far as adaptability is concerned, making goals set by the EU difficult to achieve. The need for an economic model, one that will serve as stimulus for investments in green technologies, is evident in the EU and already under process as an extension of MRV with the form of taxation or inclusion of field to EU ETS (Emissions Trading Scheming).

In response to above, it is proposed for an emission trading model to be created, one that will create the necessary environment for drastic emissions reduction, offering reward for adapting, however also avoiding great economic pressure towards shipping companies. The present study examines the current environmental concern in maritime, forthcoming measures and, in the meantime, proceeds in developing and evaluating an emission reporting and trading scheme, which is based on blockchain technology.

Κεφάλαιο 1: Νομοθεσία εκπομπών ρύπων

1.1 Νομοθεσία MRV

Χαρακτηριστικό είναι πως από το 2018 έχει λάβει χώρα η εφαρμογή εποπτείας σχετικά με τις εκπομπές, μέσα στο πλαίσιο των νομοθετικών μέτρων ως απάντηση στις συνεχώς εντεινόμενες ενδείξεις της κλιματικής αλλαγής. Η μελέτη αυτή, ωστόσο, εκφράζεται με αντιπαραθέσεις ανάμεσα στην Ευρωπαϊκή ένωση, τον IMO και τα συμφέροντα των εταιριών. Συγκεκριμένα στην Ευρωπαϊκή Ένωση έχουν ήδη τεθεί σε ισχύ οι κανονισμοί MRV, οι οποίοι υποχρεώνουν τα πλοία να αναφέρουν αναλυτικά δεδομένα που αφορούν τις εκπομπές ρύπων τους, ήδη από το 2018. Με βάση τους κανονισμούς τα πλοία έχουν την υποχρέωση να αναφέρουν τα απαιτούμενα δεδομένα έως τις 31 Δεκεμβρίου του εκάστου έτους, τα οποία ελέγχονται από επίσημους επιβεβαιωτές έως τις 30 Απριλίου του επόμενου έτους. Τέλος τα δεδομένα αυτά δημοσιεύονται, με την πρώτη δημοσίευση να έχει πραγματοποιηθεί στις 30 Ιουνίου 2019 (*THETIS-MRV*, 2019).



Εικόνα 1. Δημοσιευμένα στοιχεία MRV 30 Ιουνίου 2019

Οι εταιρείες είναι υποχρεωμένες να αναφέρουν αναλυτικά στοιχεία, όπως

- Καταναλώσεις κάθε είδους καυσίμου με ποσότητες
- Συνολική ποσότητα CO_2 που παράχθηκε, καθώς και συγκεκριμένες μετρήσεις σε κάθε μία από τις εξής περιπτώσεις:
    α) Κατά τη διάρκεια ταξιδιού από και προς λιμάνι της ΕΕ
    β) Κατά τη διάρκεια ταξιδιού μεταξύ λιμανιών της ΕΕ
    γ) Κατά τη διάρκεια παραμονής σε λιμάνι
- Χρόνος παραμονής σε λιμάνι και χρόνος ταξιδιού
- Συνολική ποσότητα φορτίου που μεταφέρθηκε
- Μέση ενεργειακή αποδοτικότητα, με την έννοια του μεταφορικού έργου σχετικά με τις εκπομπές

Αντίστοιχα ο ΙΜΟ έχει εφαρμόσει από 1η Μαρτίου 2018 το πρόγραμμα IMO DCS (IMO Data Collection System) (Miura *et al.*, IMO, 2003). Το πρόγραμμα λειτουργεί με ανάλογο τρόπο, ωστόσο τα στοιχεία δε γίνονται γνωστά δημοσίως. Οι διαφορές είναι πως σε αντίθεση με την αναφορά βάρους φορτίου, αναφορά γίνεται στο νεκρό βάρος πλοίου, ως ένδειξη της μεταφορικής ικανότητας.

Σε κάθε περίπτωση και τα δύο αυτά συστήματα δεν αποτελούν, καθαυτά, μέτρα αντιμετώπισης της κρίσης. Αποτελούν εργαλεία περισυλλογής πληροφοριών για την καλύτερη δυνατή υλοποίηση ενός συστήματος, το οποίο να είναι η βάση για αποθάρρυνση των υψηλών εκπομπών και όδευση προς ένα πράσινο μέλλον. Στην συνέχεια αναφέροντα τα υπάρχοντα μέτρα, αλλά και αυτά που μελετώνται για εφαρμογή.

1.2 Νομοθεσία EEDI

Αυτήν την στιγμή ισχύουσα νομοθεσία για τη ρύθμιση της εκπομπής διοξειδίου του άνθρακα είναι ο κανονισμός ANNEX 19 RESOLUTION MEPC.203(62), ο οποίος περιγράφει τον αριθμό «Energy Efficiency Design Index» ή αλλιώς **EEDI** (THE MARINE ENVIRONMENT PROTECTION COMMITTEE, 2011). Στόχος του συγκεκριμένου μέτρου είναι προαγωγή πιο αποδοτικού περιβαλλοντικά εξοπλισμού σε ότι αφορά την παραγωγή και εγκατάσταση σε πλοία, ο οποίος να είναι ανάλογος της τεχνολογικής προόδου.

Πιο συγκεκριμένα περιγράφονται ο επιτευχθέντας και ο απαιτούμενος αριθμός EEDI, οι οποίοι εκφράζονται σε:

$$\frac{grams\ of\ CO_2\ produced}{Tonne - mile}$$

Σχέση 1. Δείκτης EEDI

Προαπαίτηση είναι για κάθε α) νεόχτιστο πλοίο, β) νέο πλοίο, το οποίο έχει υποστεί σημαντικές κατασκευαστικές αλλαγές και γ) νέο ή παλαιό πλοίο που έχει υποστεί κατασκευαστικές αλλαγές σε τέτοιο βαθμό, έτσι ώστε να θεωρείται καινούριο πλοίο από τη σημαία, να υπολογιστεί ο αριθμός του επιτευχθέντος EEDI ως μικρότερος από τον απαιτούμενο. Η μέθοδος υπολογισμού του επιτευχθέντος EEDI περιγράφεται από το άρθρο «Mepc.245(66) - 2014 Guidelines on the Method of Calculation of the Attained Energy Efficiency Design Index (Eedi) for New Ships» (IMO, 2014) και είναι συνάρτηση των τεχνικών χαρακτηριστικών της μηχανολογικής εγκατάστασης του πλοίου, αλλά και της χωρητικότητας του πλοίου σε φορτίο.

Ο απαιτούμενος αριθμός EEDI αποτελεί το όριο της νομοθεσίας για την περιβαλλοντική απόδοση. Η μέθοδος υπολογισμού του, όπως περιγράφεται στο άρθρο «Mepc.203(62)»[34], είναι η χρήση των συντελεστών a και c από τον πίνακα 1. σε συνάρτηση με τη χωρητικότητα εκτοπίσματος («Reference line value» = $a \times b^{-c}$, όπου b το εκτόπισμα). Οι τιμές των a και c έχουν προκύψει από τη μελέτη της αποδοτικότητας όλων των κατασκευασμένων πλοίων κατά την περίοδο 2000 – 2010 και εκπροσωπούν τη μέση αποδοτικότητα ενός πλοίου της περιόδου αυτής, ανάλογα με τον τύπο του πλοίου και το εκτόπισμα. Τέλος στην παραπάνω τιμή πολλαπλασιάζεται ο δυντελεστής (100 – x)/100, όπου x το ποσοστό μείωσης του ορίου.

Μέχρι στιγμής το όριο έχει οριστεί σύμφωνα με τον παρακάτω πίνακα 1:

Από 01/01/2015	Από 01/01/2020	Από 01/01/2025	Κάθε 5 χρόνια έως το 2050
10	20	30	+10

Πίνακας 1. Ποσοστιαία τιμή της μείωσης του EEDI

Η τιμή έχει οριστεί ως 10% από τη 1η Ιανουαρίου του 2015 με στόχο να αυξάνεται κατά 10 μονάδες κάθε χρόνο. Έως τώρα έχει νομοθετηθεί η τιμή έως και το 2025 (30%) και η νομοθεσία θα αναθεωρηθεί με στόχο τη ρύθμιση του ποσοστού αναλογικά στο 80% το 2050.

1.3 Κριτική πάνω στη νομοθεσία του EEDI

Η νομοθεσία του EEDI πρόκειται για μία ρύθμιση, η οποία επικεντρώνεται στο ζήτημα των ρύπων και το ρυθμίζει με γνώμονα το περιβάλλον. Παρ' όλα αυτά η ρύθμιση αυτή αποτυγχάνει να καλύψει κάποιες βασικές συνιστώσες του προβλήματος:

- Η νομοθεσία του EEDI αποτυγχάνει στη ρύθμιση των ήδη υπαρχόντων πλοίων. Τα παλαιότερα πλοία παράγουν σημαντικά μεγαλύτερες ποσότητες ρύπων συγκριτικά με τα νέα, τα οποία είναι εξοπλισμένα με πιο καινοτόμες και αποδοτικές μηχανολογικές εγκαταστάσεις. Αντίθετα με το στόχο της νομοθεσίας, αποθαρρύνεται η κατασκευή νέων πλοίων, καθώς απαιτείται μεγαλύτερο κόστος κατασκευής, χωρίς να υπάρχουν επιπτώσεις για χρήση παλαιότερων πλοίων.
- Η νομοθεσία του EEDI αποτυγχάνει να ελέγξει το ακριβές ποσό ρύπων που παράγεται από τον κλάδο, αλλά ελέγχει μία μόνο συνιστώσα του ζητήματος. Σύμφωνα με την πρώτη πρόταση, είναι εύκολο να κατανοηθεί γιατί αυτή η συνιστώσα από μόνη της δε συνεπάγεται τα επιθυμητά θετικά αποτελέσματα.
- Δεν παρέχεται κανένας βαθμός ελαστικότητας σχετικά με την πραγματική τεχνολογική πρόοδο. Οι κατασκευαστές καταλήγουν πως δεν υπάρχει καμία δυνατότητα να επιτευχθούν τα επίπεδα μείωσης που ορίζονται στους κανονισμούς, ειδικά του ποσοστού 80% μέχρι το 2050, χρησιμοποιώντας συμβατικά μέσα.

- Ο κανονισμός δεν προσφέρει καμία επιβράβευση για την κατασκευή ενός φιλικού προς το περιβάλλον πλοίου. Αντίθετα προτρέπει τους κατασκευαστές, προκειμένου να μειωθούν τα κατασκευαστικά έξοδα, στην ελάχιστη δυνατή κάλυψη του ορίου.

Οι παραπάνω δύο τελευταίες προτάσεις προκαλούν άξιο απόρροιας το κατά πόσο οι κατασκευαστές θα είναι ικανοί να συμμορφωθούν με τον κανονισμό. Από τη μία πλευρά είναι απαραίτητη η τεχνολογική έρευνα πάνω στο ζήτημα, έτσι ώστε να μπορούν να είναι προετοιμασμένοι να ανταποκριθούν στα μελλοντικά χαμηλά όρια. Από την άλλη η ζήτηση για τεχνολογικά προηγμένο και πιο αποδοτικό εξοπλισμό από αυτόν του ορίου είναι μηδενική, εφόσον αυτός ο εξοπλισμός συνεπάγεται και μεγαλύτερο κόστος.

Μία νομοθεσία η οποία θα περιελάμβανε ένα σύστημα ανταμοιβής για αποδοτικότερο εξοπλισμό θα μπορούσε να βοηθήσει στο παραπάνω πρόβλημα. Μία εταιρεία, η οποία θα έπρεπε να επενδύσει μεγαλύτερο κεφάλαιο για την εγκατάσταση πιο αποδοτικού εξοπλισμού, θα μπορούσε να αποσβέσει αυτό το κόστος μέσω κάποιας ανταμοιβής. Ως αποτέλεσμα οι κατασκευαστές θα μπορούσαν να προσφέρουν πολύ πιο αποδοτικές προτάσεις και να εκλάβουν σημαντικά μεγαλύτερη ζήτηση. Σε μεγάλη κλίμακα το παραπάνω εγχείρημα θα μπορούσε να αποσκοπήσει σε μεγαλύτερη μείωση των παγκόσμιων ρύπων με σημαντική μείωση του κόστους για την κατασκευή των πλοίων.

Για να γίνει κατανοητή η παραπάνω πρόταση ας υποθέσουμε το εξής σενάριο:
Έστω 3 υποθετικά συστήματα πρόωσης #1, #2, #3 με αντίστοιχα κόστη εγκατάστασης 10’000$, 20’000$ και 30’000$ και αντίστοιχες εκπομπές ρύπων ανά μίλι 450 [kg CO_2 / n mile], 300 [kg CO_2 / n mile] και 100 [kg CO_2 / n mile]. Ας υποθέσουμε επίσης ότι αναφερόμαστε σε μία εταιρεία η οποία σκοπεύει να κατασκευάσει 10 νέα πλοία. Τέλος ας μελετήσουμε 2 περιπτώσεις κανονισμών για τους οποίους ισχύει:

Α) Κάθε νεόχτιστο πλοίο πρέπει να έχει μέγιστο αριθμό εκπομπών ρύπων ανά μίλι: 300 [kg CO_2 / n mile] και

Β) Κάθε 10 νεόχτιστα πλοία ο αθροιστικός αριθμός εκπομπών ρύπων σε ίση απόσταση πρέπει να ισούται με 300 [kg CO_2 / n mile]

Έτσι λοιπόν, κατά τη βελτιστοποίηση των παραπάνω περιπτώσεων, καταλήγουμε:

Υποθετικό σενάριο	Σύστημα #1	Σύστημα #2	Σύστημα #3	**Συνολικά Έξοδα $**	αθροιστικός αριθμός εκπομπών ρύπων ανά μίλι
Περίπτωση Α	0	10	0	200’000	300
Περίπτωση Β	5	1	4	180’000	300

Πίνακας 2. Παράδειγμα οικονομικής και περιβαλλοντικής βελτιστοποίησης προβλήματος εγκατάστασης συστήματος πρόωσης

Είναι, λοιπόν, προφανές, πως η περίπτωση Α σίγουρα δεν είναι ιδανική.

Λαμβάνοντας υπόψη τα παραπάνω, γίνεται σαφές ότι υπάρχει ανάγκη από τις εταιρείες να μειώσουν τις εκπομπές στον μέγιστο κατά το δυνατόν βαθμό με τα λιγότερα δυνατά έξοδα. Φαίνεται, λοιπόν σε ότι αφορά τα παραπάνω, από το παράδειγμά μας ότι η μέθοδος του EEDI αποτυγχάνει.

1.4 Φορολογία ρύπων

Μία ακόμη μέθοδος διασύνδεσης των εκπομπών CO_2 με κόστος είναι η επιβολή φορολογίας (Parry, Heine, Kizzier, Smith *et al.*, 2018). Η μέθοδος αυτή χρησιμοποιείται για τη ρύθμιση ρύπων σε πολλές χερσαίες βιομηχανίες χωρών:

- Γερμανία 10€/ ton CO_2 (25€ από 1/1/2021. Αναθεώρηση για 55€ μέχρι το 2025) (Traufetter, 2019)
- Γαλλία 65.40€/ton CO_2 από το 2020 και €86.20/ton από το 2022 (Transition, 2020)

Παρόλα αυτά στο επίπεδο της ευρωπαϊκής ένωσης η νομοθεσία για φορολόγηση των ρύπων απορρίφθηκε. Σύμφωνα με τη συζήτηση της εποχής αποφάνθηκε ότι η επιβολή φόρων για αποθάρρυνση για εκπομπές ρύπων δε θα μπορούσε να φέρει τα επιθυμητά αποτελέσματα. Οι φόροι που θα έπρεπε να επιβληθούν θα ήταν ιδιαίτερα μεγάλοι και θα επιβάρυναν τους υπόλογους τομείς (OECD, 2005). Ήταν φανερό πως μία άλλη λύση έπρεπε να βρεθεί με κριτήριο τη καλύτερη δυνατή αποδοχή από τη βιομηχανία.

1.5 Emission trade scheming – EU ETS

Ως αντικείμενο το “emission trade scheme” αφορά την ανταλλαγή του περιθωρίου εκπομπών ρυπογόνων στοιχείων έναντι χρηματικού ποσού, μεταξύ επιχειρήσεων, με σκοπό τη συμμόρφωσή τους στους κανονισμούς. Αυτή η πρακτική μπορεί να οδηγήσει σε φιλικότερο προς το περιβάλλον αποτέλεσμα, καθώς παρέχει ένα βαθμό ελευθερίας ως προς τις πρακτικές που ακολουθεί η κάθε επιχείρηση, η οποία μπορεί να εκμεταλλευτεί για την επιβολή πιο αυστηρών περιβαλλοντικών μέτρων.

Ένα από τα καλύτερα παραδείγματα ενός συστήματος ανταλλαγής εκπομπών είναι το EU ETS (EU Emissions Trading System), το οποίο λειτουργεί από το 2005 και περιλαμβάνει 31 χώρες μέλη (τα μέλη της ευρωπαϊκής ένωσης, την Ισλανδία, το Λιχτενστάιν και την Νορβηγία). Μέσω του συστήματος αυτού δίνεται η δυνατότητα χρήσης του περιθωρίου ρύπων σε μεταγενέστερη χρονική περίοδο ή πώλησης του σε άλλη επιχείρηση, παρέχονται συγκεκριμένες ελαφρύνσεις εκπομπών, οι οποίες μπορούν να μεταπωληθούν, καθώς επίσης διαμοιράζονται και περιορισμένα κονδύλια για περιβαλλοντικές ενέργειες παγκοσμίως. Το πρόγραμμα αυτό δημιουργήθηκε με πολύ συγκεκριμένους στόχους, οι οποίοι είναι μείωση κατά 21% των εκπομπών στην περίοδο 2005-2020 και 43% μέχρι το 2030. Οι στόχοι αυτοί αφορούν τους τομείς εκείνους, στους οποίους απευθύνεται το πρόγραμμα και αυτοί αποτελούν το 45% όλων των εκπομπών αερίων του θερμοκηπίου της ευρωπαϊκής ένωσης, ενώ αναμένεται να προστεθούν κι άλλων ειδών ρύποι κατά τη διάρκεια του προγράμματος με προγραμματισμένες αναθεωρήσεις.

1.6 Το πρόβλημα των ρύπων στη ναυτιλία

Η σημερινή χρονική περίοδος είναι κρίσιμη για το μέλλον της ναυτιλίας σε ότι αφορά τον περιβαλλοντικό τομέα. Η εφαρμογή ενός κατάλληλου οικονομικού μέτρου, το οποίο θα ρυθμίσει τις εκπομπές διοξειδίου του άνθρακα απαιτείται άμεσα. Οι βάσεις ενός τέτοιου μέτρου έχουν ήδη τεθεί με το σύστημα MRV της ΕΕ και το DCS του IMO. Σε αντίθεση με

το EEDI το μέτρο που θα οριστεί θα πρέπει να είναι οικονομικού χαρακτήρα θέτοντας με σαφήνεια τη διασύνδεση ρυπογόνους ποσότητας και κόστους.

Πολύ χαρακτηριστική είναι η μελέτη του νηογνώμονα ABS σχετικά με τις μελλοντικές τεχνολογίες καύσης που θα πρέπει να εφαρμοστούν για την επίτευξη των περιβαλλοντικών στόχων έως το 2050 (G. Plevrakis, S. Mamalis, L. Karaminas, E.Li, D.Carlucci, G. Burton, M. Lezama, N. Lamprinidis, D. Sofiadi, A. Vourdachas. and R. Barling in collaboration with Maritime Strategies International and Herbert Engineering, 2020). Πόρισμα της μελέτης είναι η επιτακτική ανάγκη για στροφή των χρησιμοποιούμενων καυσίμων από τα πετρελαϊκά καύσιμα και το φυσικό αέριο, σε μεγάλο ποσοστό, προς τη μεθανόλη, τα βιοκαύσιμα, το υδρογόνο και την αμμωνία, καθώς και την εγκατάσταση μηχανισμών κατακράτησης του διοξειδίου του άνθρακα. Οι τεχνολογίες αυτές, ωστόσο, χαρακτηρίζονται από μεγάλο κόστος, τόσο εγκατάστασης, όσο και έρευνας στους αντίστοιχους τομείς. Τίθεται, λοιπόν η ανάγκη ενός οικονομικού μοντέλου προώθησης τέτοιων τεχνολογιών.

Στην συνέχιση των κανονισμών του MRV και DCS, έχουμε ήδη αναφέρει προτεινόμενες λύσεις που σχετίζονται με την φορολόγηση των ρύπων είτε την ένταξη της ναυτιλίας στο ευρωπαϊκό σύστημα αγοροπωλησίας ελαφρύνσεων. Ενώ τα δύο συστήματα πετυχαίνουν σε ένα βαθμό να διασυνδέσουν το κόστος με τη ποσότητα εκπομπής ρύπων, αδυνατούν και τα δύο να δημιουργήσουν ένα περιβάλλον άνθισης νέων πράσινων τεχνολογιών.

Στα παρακάτω κεφάλαια γίνεται η περιγραφή ενός συστήματος ανταλλαγής ρύπων βασισμένο σε blockckhain. Το μοντέλο που αναπτύχθηκε δίνει τη δυνατότητα ανταμοιβής πράσινων πλοίων και επιβολής προστίμου σε περιβαλλοντικά επιβλαβή πλοία. Σαν αποτέλεσμα, δημιουργείται ένα πλαίσιο, μέσα στο οποίο παρέχεται αξιοσημείωτο κίνητρο σε κάποια εταιρεία να επενδύσει σε περιβαλλοντικά συμφέρουσες λύσεις, κερδίζοντας σε βάθος χρόνου από την ανταμοιβή που παρέχει το σύστημα ανταλλαγής αέριων ρύπων. Τέλος, το σύστημα λειτουργεί χωρίς κάποια κεντρική αρχή, μειώνοντας σημαντικά οποιοδήποτε κόστος λειτουργίας και δεν συνεπάγεται κανένα επιπλέον κόστος προς εξωτερικούς φορείς. Κάθε πρόστιμο που θα επιβληθεί σε πλοίο μη συμμορφωμένο με τα όρια που έχουν τεθεί, θα λειτουργήσει, άμεσα, ως ανταμοιβή των πλοίων εκείνων, τα οποία παρήχθησαν το μέγιστο μεταφορικό έργο, με το λιγότερο περιβαλλοντικό κόστος.

Κεφάλαιο 2: Ιστορία των Blockchain και Εφαρμογές

2.1 Ιστορία του blockchain.

Πριν περιγραφεί αναλυτικά η εφαρμογή που αναπτύχθηκε στα πλαίσια της διπλωματικής εργασίας, θα πρέπει να μελετηθεί η λειτουργία και η χρησιμότητα των blockchain, ξεκινώντας με μία ιστορική αναδρομή.

Ο αγγλικός όρος blockchain έχει αποδοθεί με διάφορες εκφράσεις, όπως «Τεχνολογία Αλυσίδας Κοινοποιήσεων» («ΦΕΚ. Τεύχος Β’ 3488/21.08.2018. 44103 κ.ε.. .». Εφημερίδα της Κυβερνήσεως. 21 Αυγούστου 2018, 2019) είτε «Τεχνολογίες Μπλοκ Αλυσίδας» («ΦΕΚ. Τεύχος Β’ 1756/22.05.2017». Εφημερίδα της Κυβερνήσεως: 17803, 17805, 17807 κ.ε.. 22 Μαΐου 2017., 2017) στην εφημερίδα της Κυβερνήσεως, είτε «αλυσίδα συστοιχιών» στην ιστοσελίδα της Ευρωπαϊκής Κεντρικής Τράπεζας (ecb.europa.eu, 2017). Εφόσον, λοιπόν, ο όρος δεν είναι αυστηρά καθορισμένος στην ελληνική γλώσσα και η κοινότυπη αναφορά γίνεται με τη χρήση του αγγλικού όρου, στο πλαίσιο της εργασίας θα χρησιμοποιείται ο όρος «blockchain». Ένας ορισμός της λέξης blockchain θα μπορούσε να είναι μία αναπτύξιμη λίστα καταγραφής δεδομένων σε μορφή μπλοκ, τα οποία είναι χρονικώς διατεταγμένα και συνδέονται με τη χρήση κρυπτογραφίας.

2.1.1 Το πρώτο blockchain

Η πρώτη περιγραφή ενός τέτοιου μοντέλου έγινε το 1991 από τους Haber, Stuart και Stornetta, W Scott (Haber and Stornetta, 1991). Ο στόχος τους ήταν η δημιουργία ενός συστήματος χρονικής ταυτοποίησης όλων των αρχείων των χρηστών μέσα σε ένα περιβάλλον, το οποίο θα μπορούσε, για παράδειγμα, να είναι μία εταιρεία, ένα σύνολο εταιρειών, είτε ένα οποιοδήποτε άλλο σύνολο. Το ζήτημα που είχαν να αντιμετωπίσουν ήταν πως η αποστολή ενός ολόκληρου αρχείου προς επικύρωση ήταν ιδιαίτερα προβληματική, καθώς

a) το αρχείο θα μπορούσε να είναι μεγάλο σε μέγεθος, δημιουργώντας ζητήματα ότι αφορά τον αποθηκευτικό χώρο και τους περιορισμούς του εύρους ζώνης, την δηλαδή ικανότητα για μεταφορά ογκωδών δεδομένων
b) η υπηρεσία ταυτοποίησης θα είχε πρόσβαση στο αρχείο, θέτοντας ζητήματα ιδιωτικότητας

c) η μεταφορά ενός ολόκληρου αρχείο είναι επιρρεπής σε αλλοίωση δεδομένων

Η λύση που προτείνουν είναι η χρήση μιας συνάρτησης κατακερματισμού (hash function), δηλαδή μια κωδικοποιημένη συμπύκνωση των δεδομένων σε πεπερασμένο μέγεθος. Η μέθοδος αυτή είναι μη αναστρέψιμη και σε συνδυασμό την πρόταση τους για ηλεκτρονική υπογραφή των εγγράφων από το χρήστη, επιτρέπει την μη αποθήκευση των εγγράφων στην υπηρεσία ταυτοποίησης.

Το μοντέλο, λοιπόν, διαμορφώνεται σε στοιχεία μπλοκ, τα οποία περιέχουν μια κωδικοποίηση των δεδομένων και την ημερομηνία. Οι τελευταίες δύο ιδιότητες ης εφαρμογής τους είναι η διασύνδεση των διαφορετικών μπλοκ μεταξύ τους σε μια αλληλουχία που το κάθε μπλοκ περιέχει κάποια κωδικοποιημένα στοιχεία του προηγούμενου, μέσω μιας συνάρτησης hash, καθώς και η διαδικασία κατά την οποία το αρχείο που περιέχει όλα τα παραπάνω στοιχεία διαμοιράζεται ανάμεσα σε όλους τους χρήστες, χωρίς την ανάγκη μιας κεντρικής αρχής.

Σχήμα 1. Δομή Μοντέλου Χρονικής Ταυτοποίησης Haber & Stornetta

Η παραπάνω περιγραφή αποτελεί και την αρχή λειτουργίας ενός σύγχρονου ολοκληρωμένου blockchain, ωστόσο η πρώτη πρακτική εφαρμογή ενός τέτοιου μοντέλου θα γίνει αρκετά χρόνια αργότερα, το 2009 με την κυκλοφορία του πρώτου κρυπτονομίσματος, του μπίτκοϊν (Bitcoin ₿)

2.1.2 Bitcoin

Στις 31 Οκτωβρίου του 2008 ο «Satoshi Nakamoto» δημοσιεύει το άρθρο «Bitcoin: A peer-to-Peer Electronic Cash System» (Satoshi Nakamoto, 2008) στην ιστοσελίδα bitcoin.org, η οποία είχε ιδρυθεί τον Αύγουστο του ίδιου έτους. Το όνομα Satoshi Nakamoto δεν έχει ταυτοποιηθεί έχει σήμερα και είναι αποδεκτό πως πρόκειται για ένα ψευδώνυμο(WIRED, 2011). Στο άρθρο αυτό γίνεται η περιγραφή του "Bitcoin", μιας μορφής ηλεκτρονικού χρήματος, το οποίο επιτρέπει πληρωμές μεταξύ χρηστών, χωρίς τον έλεγχο από κάποια κεντρική αρχή, όπως αναφέρει, κοινώς του πρώτου κρυπτονομίσματος. Η εφαρμογή που περιγράφεται έχει τη βάση σε ένα μοντέλο, όπως αυτό που περιέγραψαν οι Haber και Stornetta, όμως αυτή τη φορά τα δεδομένα που πρόκειται να αποθηκεύονται στα μπλοκ είναι χρηματικές συναλλαγές. Ο κάθε χρήστης έχοντας ένα μοναδικό κλειδί μπορεί να υπογράφει συναλλαγές προς άλλους χρήστες και το συνολικό ποσό που αντιστοιχεί στο πορτοφόλι κάθε χρήστη προσδιορίζεται από το άθροισμα όλων των προηγούμενων συναλλαγών προς και από το λογαριασμό του. Κάθε φορά δηλαδή που κάποιος θέλει να ελέγξει πόσα bitcoins κατέχει, θα πρέπει να διαβάσει ξανά όλη τη λίστα των συναλλαγών, προσθαφαιρώντας εκείνες που τον περιέχουν είτε ως αποστολέα, είτε ως παραλήπτη.

Για την επίτευξη του παραπάνω στόχου είναι απαραίτητη η χρήση ενός συστήματος επιβράδυνσης της διαδικασίας, το οποίο ο Nakamoto ονομάζει «απόδειξη της εργασίας» (proof of work) και βασίζεται στο άρθρο του Adam Back «Hashcash - A Denial of Service Counter-Measure» (Back, 2002). Επί της ουσίας αναγκάζεται οποιοσδήποτε θελήσει να δημιουργήσει ένα καινούριο μπλοκ, κατά τον υπολογισμό του hash να συνυπολογίσει έναν ακόμα αριθμό «nonce», τέτοιο ώστε το αποτέλεσμα να είναι μια ακολουθία από χαρακτήρες (hash), η οποία ξεκινάει από μια σειρά από «0», τόσα, όσα ορίζει η δυσκολία. Για παράδειγμα ένα μπλοκ με δυσκολία 3 θα πρέπει το hash του να ξεκινάει με τουλάχιστον 3 «0». Έτσι, λοιπόν, ένας χρήστης που θέλει να δημιουργήσει ένα καινούριο μπλοκ θα πρέπει να βρει ένα κατάλληλο hash μέσα από μια χρονοβόρα επαναληπτική διαδικασία, κατά την οποία θα ελέγξει χιλιάδες ή και περισσότερους αριθμούς nonce. Παράδειγμα για δυσκολία 3:

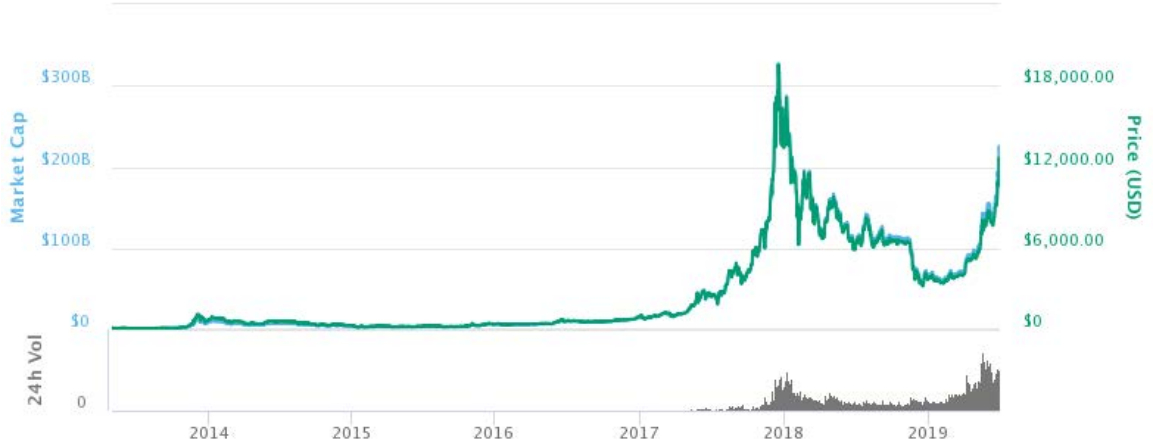
Data	Nonce	Αποτέλεσμα Hash	Έλεγχος
¯Ø¯'…†©ÇM¼□€…‡©ÇM¼,€†,Á□ƒp=b‰¸/ŠÔA'	79	à-'âFàßvLØLqâJ]ÚÚ□öæñ□ûª ¦=R#	Επανάληψη
MË[3óØôÎm¦¸ÿAF□5{,)□°J(¶Ð"	12840	-O□Ã½úkðK□Ñ□Óçë·&ïFÿlÐ×C¼]□	Επανάληψη
{ëÚ+!0[íÉt}1Àg"þy5³ò€ÝÇ4t.˜€wü„-t0%ö,'=JÂ:ß¼'Ús	90341	000È»7□4K□¥b□x-"ÖéI¬úÜ□HKÊ	Δεκτό

Πίνακας 3. Αναπαράσταση Υπολογισμού Κατάλληλου Hash

Αποτέλεσμα αυτής της επιβράδυνσης της διαδικασίας είναι η αποτροπή του ελέγχου της αλυσίδας από κάποιο κακόβουλο άτομο. Η απόδειξη της εργασίας είναι ένας «αλγόριθμος συναίνεσης» (consensus algorithm), το χαρακτηριστικό, δηλαδή, αξιοπιστίας ενός blockchain. Στη συγκεκριμένη περίπτωση το proof of work απαιτεί υπολογιστική ισχύ για τη δημιουργία ενός καινούριου μπλοκ. Μεγαλύτερη υπολογιστική ισχύ έχει σαν αποτέλεσμα μεγαλύτερη πιθανότητα το επόμενο μπλοκ της αλυσίδας να δημιουργηθεί από τον συγκεκριμένο χρήστη. Ως αποτέλεσμα ένας κακόβουλος χρήστης θα έπρεπε να διαθέτει τουλάχιστον την ίδια επεξεργαστική ισχύ με αυτή των ανταγωνιστών του για να δημιουργήσει πιο γρήγορα ένα καινούριο μπλοκ. Σε διαφορετική περίπτωση, η αλυσίδα έχει μεγαλώσει και οι υπόλοιποι χρήστες δουλεύουν ήδη στο επόμενο μπλοκ. Για να αλλοιώσει λοιπόν τα δεδομένα ενός μπλοκ ένας χρήστης, εφόσον, όπως έχει ήδη αναφερθεί, τα μπλοκ είναι συνδεδεμένα μεταξύ τους, θα πρέπει να υπολογίσει εκ νέου το hash όλων των επόμενων μπλοκς, πιο γρήγορα απ' ότι οι ανταγωνιστές του υπολογίσουν ένα μπλοκ. Όπως καταλήγει και το άρθρο η πιθανότητα να συμβεί αυτό μειώνεται εκθετικά με τη προσθήκη κάθε ενός μπλοκ.

Τέλος, για να έχουν οι χρήστες ένα κίνητρο συμμετοχής στην παραπάνω διαδικασία, αποδίδεται αμοιβή στον χρήστη εκείνο που θα καταφέρει να προσθέσει ένα καινούριο μπλοκ στην αλυσίδα. Η αμοιβή ήταν 50 BTC για κάθε μπλοκ που δημιουργείται κατά την εκκίνηση της εφαρμογής, ωστόσο είναι προκαθορισμένο να υποδιαιρείται κάθε 4 χρόνια, έτσι ώστε να μην ξεπεραστεί ποτέ το ποσό των 21,000,000 coins[8]. Η τελευταία αμοιβή θα δοθεί το 2140 και στη συνέχει το σύστημα θα συντηρείται είτε από εθελοντές, είτε θα δίνεται αμοιβή από την ύπαρξη κάποιου φόρου σε κάθε συναλλαγή.

Η πρώτη εκδοχή του blockchain σε μορφή ανοιχτού κώδικα δημοσιεύεται στις 11 Ιανουαρίου 2009 (Nakamoto, 2009) με το πρώτο μπλοκ να είναι δημιουργημένο στις 3 και τη πρώτη συναλλαγή να πραγματοποιείται στις 12 του ίδιου μήνα. Στις 5 Οκτωβρίου ανακοινώνεται η πρώτη ισοτιμία του νομίσματος σε σχέση με το δολάριο US$1 = 1,309.03 BTC από τη «New Liberty Standard» (New Liberty Standard, 2009), υπολογισμένη σε ισοδύναμη αξία ρεύματος που χρειάζεται για τον υπολογισμό ενός μπλοκ. Η ισοτιμία έφτασε το 1$ το 2011 και τη μέγιστη τιμή των $19,783.06 στις 17 Δεκεμβρίου 2017 (Godbole, 2017). Η τιμή του νομίσματος γνώρισε πολλές και ραγδαίες αυξομειώσεις.

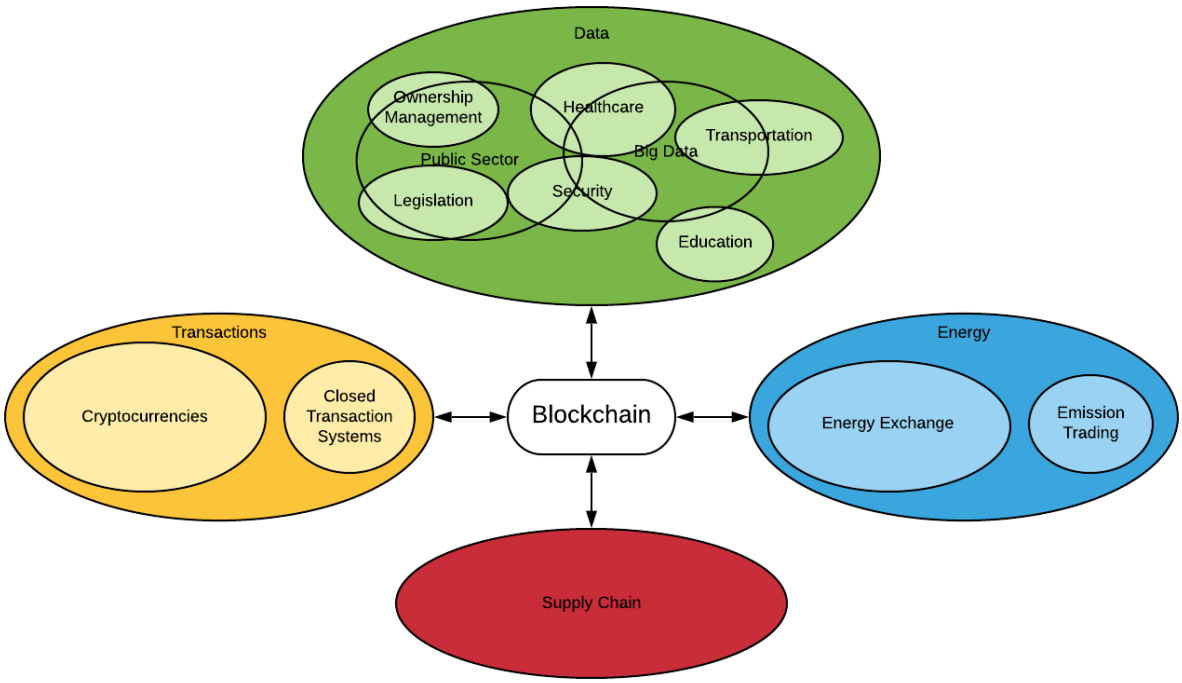


Σχήμα 2. Ιστορικό κεφαλαιοποίησης ₿ σε $, πηγή: https://coinmarketcap.com/charts/

Τέλος, αξίζει να αναφερθεί, ότι το Bitcoin αναγνωρίζεται πλήρως από τις περισσότερες χώρες παγκοσμίως με μερικές εξαιρέσεις, οι οποίες νομοθετικά το περιορίζουν ή και το απαγορεύουν πλήρως, με τη Ρωσία, την Κίνα, το Βιετνάμ, τη Βολιβία, την Κολομβία και το Εκουαδόρ να αποτελούν τις κυριότερες.

2.2 Εφαρμογή των Blockchain:

Τα Blockchain παρουσιάζουν κάποια αδιαμφισβήτητα πλεονεκτήματα, με αποτέλεσμα να μελετάται η χρήση τους σε ευρύ φάσμα εφαρμογών, οι οποίες μπορούν να κατηγοριοποιηθούν στους τομείς της πραγματοποίησης συναλλαγών, της αποθήκευσης και επεξεργασίας δεδομένων, της ενέργειας και της εφοδιαστικής αλυσίδας.



Σχήμα 3. Εφαρμογές των Blockchain

2.2.1 Συναλλαγές

2.2.1α Κρυπτονομίσματα:

Αυτήν την στιγμή η χρήση Blockchain είναι δημοφιλής τεχνολογία ως βάση για τα κρυπτονομίσματα, με κυρίαρχο το Bitcoin. Η πραγματοποίηση συναλλαγών σε ένα περιβάλλον κρυπτονομίσματος γίνεται με την καταγραφή τους σε μία ολοένα αυξανόμενη λίστα blockchain. Το Bitcoin, όντας το πρώτο, δημιουργήθηκε με σκοπό να ξεπεράσει τα προβλήματα που φέρει το παραστατικό χρήμα (BARTOS, 2015). Η αξία του νομίσματος προκύπτει από τους νόμους της αγοράς και της ζήτησης σε συνδυασμό με το γεγονός ότι η συνολική ποσότητα συναλλάγματος Bitcoin συνεχώς αυξάνεται, αλλά με αυστηρά προκαθορισμένο αλγοριθμικό τρόπο και μειωμένο ρυθμό, έως έναν πεπερασμένο αριθμό. Η αξία δε προκύπτει από την αυθαιρεσία μιας κεντρικής τράπεζας ή μιας κυβέρνησης, αλλά μόνο από τους νόμους της ίδιας της αγοράς.

Επίσης οι συναλλαγές πραγματοποιούνται μέσα σε ένα σύστημα διαμοιρασμού, το οποίο, όπως και η αξία του νομίσματος, δεν ελέγχεται από κανέναν οργανισμό, ωστόσο χαρακτηρίζεται από μεγάλη αξιοπιστία. Ο έλεγχος και πραγματοποίηση των συναλλαγών μέσω οργανισμών, όπως είναι οι τράπεζες, απαιτούν κόστος, το οποίο εκφράζεται σε φόρους και χρόνο, δηλαδή καθυστέρηση των συναλλαγών, προβλήματα τα οποία ένα κρυπτονόμισμα καλείται να αντιμετωπίσει.

2.2.1β Γενικότερη αγορά:

Παρά το γεγονός ότι η τεχνολογία Blockchain είναι συνδεδεμένη με τα κρυπτονομίσματα, δεν είναι και η αποκλειστική εφαρμογή της τεχνολογίας αυτής. Το τελευταίο διάστημα παρατηρούμε ότι αντίστοιχα συστήματα συναλλαγών συνεργαζόμενα με πληθώρα τραπεζών, τα οποία κερδίζουν έδαφος. Με δεδομένο ότι η τεχνολογία είναι πολλά υποσχόμενη, καθώς επιτρέπει τη μείωση του χρόνου εκτέλεσης και επαλήθευσης μιας συναλλαγής από ημέρες σε λίγα μόλις λεπτά, η εφαρμογή της στον τραπεζικό κλάδο προσφέρει εξαιρετικά σημαντικά οφέλη. Ένα τέτοιο σύστημα μπορεί να είναι ένα δίκτυο Blockchain, το οποίο περιλαμβάνει τράπεζες αλλά και οποιουδήποτε άλλου τύπου φορέα συναλλαγών (ιδιωτικές, δημόσιες εταιρίες και ιδιώτες)(Ikeda and Hamid, 2018). Στη συνέχεια οι φορείς αυτοί μπορούν να χρησιμοποιηθούν σαν διαμεσολαβητές για

χρήστες εκτός του δικτύου, οι οποίοι με τη σειρά τους μπορούν να επωφεληθούν από τα πλεονεκτήματα για τις συναλλαγές τους με φορείς μέσα στο δίκτυο. Αυτή η καινοτομία, λοιπόν, παρουσιάζεται εφαρμόσιμη και σε μεγάλη κλίμακα, με τη σύμπραξη διαφόρων οργανισμών, αλλά και σε πιο εξειδικευμένα ζητήματα, όπως η εσωτερική λειτουργία ενός μόνο οργανισμού.

2.2.2 Ανάλυση δεδομένων

Ένα από τα μεγαλύτερα ζητήματα σύγχρονων εταιριών είναι η συλλογή και επεξεργασία δεδομένων για στατιστική ανάλυση (Big data). Η πλέον δημοφιλής μορφή συλλογής δεδομένων είναι μέσω της καταγραφής τους σε μεγάλες βάσεις δεδομένων. Οι βάσεις αυτές είναι συνήθως διαμοιρασμένες σε ένα βαθμό έτσι ώστε να αποφεύγεται η απώλεια δεδομένων σε περιπτώσεις σφαλμάτων και συγκριτικά με τα Blockchains παρουσιάζουν σημαντικά αυξημένη ταχύτητα λειτουργίας του συστήματος. Ωστόσο ελέγχονται πάντα από μία αρχή, κάτι που έχει σοβαρά μειονεκτήματα:

a) είναι εύκολο να αλλοιωθούν από κακόβουλους χρήστες και δύσκολο να ελεγχθούν
b) δίνεται η δυνατότητα αλλοίωσης της ταυτότητας των προσωπικών στοιχείων από τον διαχειριστή και έτσι πολλοί χρήστες αποθαρρύνονται να κοινοποιήσουν πληροφορίες λόγω έλλειψης εμπιστοσύνης
c) η αδυναμία να υλοποιηθούν διεργασίες χωρίς την επέμβαση/έγκριση του διαχειριστή
d) οι λίστες αυτές συνήθως χαρακτηρίζονται από περιορισμένη προσβασιμότητα για τρίτους
e) το ακριβές αντικείμενο που αποθηκεύεται είναι πολλές φορές, επειδή ακριβώς είναι περιορισμένης προσβασιμότητας, δύσκολο να ελεγχθεί, κάτι που θέτει το ζήτημα της ιδιωτικότητας

Δύο χαρακτηριστικά παραδείγματα έρευνας πάνω σε τέτοιου είδους χρήση της τεχνολογίας Blockchain, κατά την συγκεκριμένη χρονική περίοδο, αφορούν τους χώρους της υγείας και της αυτοκινητοβιομηχανίας. Σε ό,τι αφορά τον χώρο της υγείας πρόκειται για δημιουργία μεγάλης κλίμακας λίστας Blockchain, η οποία θα χρησιμοποιείται για

καταγραφή ιατρικών περιπτώσεων με σκοπό την μεταγενέστερη αξιοποίηση του υλικού για ερευνητικούς σκοπούς. Το εγχείρημα αυτό υπόσχεται συντριπτική αύξηση των δεδομένων προς ανάλυση, αλλά και εξασφάλιση των προσωπικών δεδομένων των ασθενών.

Στον χώρο της αυτοκινητοβιομηχανίας τα Blockchain εκφράζονται συνήθως σε μικρότερης κλίμακας συστήματα που αναπτύσσουν διαφορετικές εταιρίες. Αυτήν την στιγμή διαφορετικές εταιρίες, όπως η Tesla η Toyota(Kim, 2018) και η Porsche έχουν εκφράσει ενδιαφέρον στην έρευνα πάνω στην ανάπτυξη τέτοιων συστημάτων, ενώ πολλά αντίστοιχα ανεξάρτητα εγχειρήματα πραγματοποιούνται. Ο στόχος είναι η καταγραφή κυκλοφοριακών δεδομένων μεταξύ των οχημάτων για την χρήση τους τόσο στα αυτοκινούμενα οχήματα, όσο και στη βελτιστοποίηση των αυτοκινήτων μέσω της καταγραφής καταστάσεων λειτουργίας. Τόσο η αποτελεσματικότητα, όσο και η προστασία της ιδιωτικότητας καθιστούν τα Blockchain τουλάχιστον άξια προς διερεύνηση επιλογή για την επίτευξη των παραπάνω στόχων(Zhang *et al.*, 2019).

Ακόμη ένα παράδειγμα μεγάλης κλίμακας αξιοποίησης της τεχνολογίας Blockchain αποτελεί η Σιγκαπούρη. Η Σιγκαπούρη είναι μια χώρα που χαρακτηρίζεται από έντονη τεχνολογική καινοτομία, κάτι που δίνει πάτημα στα αδιαμφισβήτητα οφέλη της τεχνολογίας Blockchain. Εκτός από το γεγονός ότι ένα Blockchain στον τομέα της υγείας είναι υπό συζήτηση, πολλοί τομείς διαθέτουν και αξιοποιούν ήδη αντίστοιχα συστήματα. Τα συστήματα που εφαρμόζονται στους χώρους της αεροπλοΐας, της εκπαίδευσης και της ιδιοκτησίας ακινήτων έχουν όλα έναν κοινό στόχο: την καταγραφή των προσωπικών δεδομένων, με σκοπό την γρήγορη, έγκυρη διασταύρωση των στοιχείων, χωρίς κινδύνους υποκλοπής πατάσσοντας οποιαδήποτε μορφής γραφειοκρατίας (Lago, 2018). Συγκεκριμένα στους χώρους των αερομεταφορών και της εκπαίδευσης οι πολίτες προμηθεύονται κάρτες ταυτότητας, οι οποίες συνδέονται με τον προσωπικό τους λογαριασμό με στοιχεία που αφορούν το ιστορικό τους και τα εισιτήριά τους, είτε το βιογραφικό τους αντίστοιχα. Επιπρόσθετα το Blockchain για την ιδιοκτησία ακινήτων έχει ως στόχο την αποφυγή γραφειοκρατίας και καθυστερήσεων κατά την αγοροπωλησία ακινήτων, εκμεταλλευόμενο την ευκολία και αξιοπιστία της εφαρμογής. Άλλες χώρες που έχουν υιοθετήσει συστήματα Blockchain για την καταγραφή δεδομένων είναι η Εσθονία, στους χώρους της υγείας, του δικαίου, της νομοθεσίας, της ασφάλειας και εμπορικών κανονισμών (με κύριο πρόσχημα

την προστασία απέναντι σε αλλοίωση και κακομεταχείριση) και η Γεωργία στο χώρο της καταγραφής και αγοροπωλησίας ακινήτων.

Παρά την ευρεία ανάπτυξη και υιοθέτηση του Blockchain στο χώρο των δεδομένων, σημαντικό είναι να αναφερθούν και τα μειονεκτήματα που εμφανίζουν οι εφαρμογές αυτές, τα οποία αφορούν τόσο τη μειωμένη ταχύτητα καταγραφής και αποθήκευσης των δεδομένων, όσο και την επιβάρυνση σε αποθηκευτικό χώρο και κόστος λειτουργίας. Το πρόβλημα πηγάζει από το γεγονός ότι η αποθήκευση όλων των δεδομένων πρέπει να γίνεται σε κάθε ένα χρήστη του λογισμικού ξεχωριστά. Όταν, λοιπόν, το αντικείμενο τέτοιων εφαρμογών είναι η αποθήκευση και διαμοιρασμός δεδομένων μεγέθους εκατοντάδων GB ή και περισσότερο, η λειτουργία γίνεται δύσκολη. Ωστόσο καινοτόμες λύσεις πάνω στην υπερκέραση τέτοιων ζητημάτων φαίνεται να είναι δυνατόν να βρεθούν, όπως η διαμοιρασμένη αποθήκευση των δεδομένων της αλυσίδας σε 3 ή περισσότερα αντίγραφα, ανά τους χρήστες(Mcconaghy *et al.*, 2016). Ένα τέτοιο blockchain θα συνδύαζε τα θετικά των τυπικών βάσεων δεδομένων, αποφεύγοντας προβλήματα κεντρικού ελέγχου και ιδιωτικότητας. Ακόμη αξίζει να σημειωθεί πως οι δυνατότητες για αποθηκευτικό χώρο και ταχύτητα μετάδοσης δεδομένων αυξάνονται συνεχώς με την ανάπτυξη της τεχνολογίας και μάλιστα εξετάζονται συνεχώς νέες μέθοδοι, πολλά υποσχόμενες για δραστικές αλλαγές(Bhat, 2018). Επομένως, πέρα από τις καινοτόμες λύσεις, η ίδια η ανάπτυξη της τεχνολογίας ενδέχεται να δώσει απάντηση στο συγκεκριμένο πρόβλημα.

2.2.3 Αλυσίδα προμηθειών

Τα Blockchain εμφανίζουν σημαντικά πλεονεκτήματα στη λειτουργία ενός συστήματος διαχείρισης πόρων και προϊόντων μεταξύ διαφόρων φορέων. Σήμερα απαιτείται η χρήση τέτοιων συστημάτων, τα οποία μπορούν να είναι υπηρεσίες εντοπισμού προϊόντων, λίστες καταγραφής εφοδίων και προμηθευτών, λίστες καταγραφής πελατών κτλ. Τα συστήματα όμως που χρησιμοποιούνται παρουσιάζουν σαφή προβλήματα απόδοσης, καθώς χαρακτηρίζονται από δυσκολία ενοποίησης μεταξύ τους, καθυστέρηση στο χρόνο εποπτείας, ενημέρωσης και έγκρισης ενεργειών, καθώς και ανάγκη από τον

ανθρώπινο παράγοντα σε μεγάλο βαθμό. Η χρήση, ωστόσο, συστημάτων Blockchain για την διεκπεραίωση τέτοιων λειτουργιών λύνουν αυτά τα προβλήματα.

Επί της ουσίας ένα ERP σύστημα ή σύστημα ενδοεπιχειρησιακού σχεδιασμού αποτελεί έναν χώρο καταγραφής και διαχείρισης των πόρων ενός οργανισμού. Δημοφιλή τέτοια συστήματα είναι αποτελούν το SAP ERP ή το ORACLE DATABASE. Αντίστοιχα συστήματα είναι ιδιαίτερα αποτελεσματικά στην εύκολη και γρήγορη εποπτεία των πόρων για την καλύτερη δυνατή διαχείρισή τους. Παρόλα αυτά, τα συγκεκριμένα λογισμικά παρουσιάζουν μία πολύ χαρακτηριστική έλλειψη συμβατότητας μεταξύ τους. Αυτό έχει σαν αποτέλεσμα να καθίσταται αδύνατη η διαχείριση πόρων σε διεπιχειρησιακό επίπεδο είτε ακόμα, πολλές φορές, σε διατμηματικό στα πλαίσια μίας εταιρείας.

Είναι σαφές πως κάθε εταιρεία, η οποία επιθυμεί να έχει ένα τέτοιο σύστημα διαχείρισης, απαιτεί και τον πλήρη έλεγχό του. Το ανώτερο ζήτημα θα μπορούσε λυθεί πλήρως από τη χρήση ενός συστήματος ERP βασισμένο σε Blockchain, με τη χρήση του οποίου ο έλεγχος πάνω στις πληροφορίες και τη διαχείρισή τους θα μπορούσε να είναι τόσο καθολικός, σε ότι αφορά την εποπτεία και την πρόσβαση, όσο και ασφαλής σε ότι αφορά την διαχείριση. Ένα Blockchain αρχικά δίνει τη δυνατότητα δημιουργίας ενός δικτύου μεταξύ όλων των φορέων που επιθυμούν να ενοποιηθούν και αυτοί μπορεί να είναι επιχειρήσεις, προμηθευτές, πελάτες και εταιρίες υπηρεσιών(Banerjee, 2018). Όλα τα διαφορετικά στοιχεία μπορούν να εντάσσονται σε μια ενιαία λίστα, όπου και να υπάρχει πιο γρήγορη και διασταυρωμένη εποπτεία, καθώς και ένα προσβάσιμο αναλλοίωτο ιστορικό της διακίνησης οποιουδήποτε προϊόντος. Οι πόροι και τα προϊόντα μπορούν να εντοπιστούν και να αναλυθούν σε οποιοδήποτε στάδιο βρίσκονται πολύ πιο εύκολα από ότι χρησιμοποιώντας κάθε φορά αυτόνομα συμβατικά ERP (Enterprise Resource Planning) συστήματα, τα οποία δεν είναι προσβάσιμα σε τρίτους.

Επιπρόσθετα τα Blockchain μπορούν να προσδώσουν το στοιχείο της αυτοματοποίησης σε ένα σύστημα, όπως αυτό που αναπτύχθηκε παραπάνω. Η χρήση των smart contracts μπορεί να συμβάλει στην αυτόματη επικύρωση συναλλαγών μεταξύ των χρηστών, χωρίς την ανάγκη για πολύωρους ελέγχους. Η ποιότητα και η φύση των προϊόντων και των πόρων, όπως και των συμφωνιών είναι εξακριβωμένη σε κάθε στάδιο του συστήματος μην αφήνοντας περιθώριο για διαφωνίες και αθέτηση όρων μεταξύ των

διαφορετικών φορέων.

2.2.4 Ενέργεια

Ο τομέας της ενέργειας αποτελεί ένα ακόμη πεδίο όπου το blockchain έχει πολλές δυνατότητες. Η παραγωγή ενέργειας χαρακτηρίζεται από συγκεντρωτικά καθεστώτα και πολλούς μεσάζοντες, γεγονός που ιδιωτικοποιεί τον έλεγχο της παραγωγής και αυξάνει την τιμή. Η χρήση Blockchain στο εμπόριο ενέργειας είναι μία λύση που συζητιέται όλο και περισσότερο τα τελευταία χρόνια και το ζήτημα της ανανεώσιμης ενέργειας, ευνοείται ιδιαίτερα σε αυτό το περιβάλλον. Χαρακτηριστικά είναι τα παραδείγματα δημιουργίας ηλεκτρικών δικτύων μεταξύ ανεξάρτητων παραγωγών ηλεκτρικής ενέργειας, όπως ιδιωτικοί ηλιακοί συσσωρευτές στις οροφές κτιρίων, καθώς και εμπορίου ηλεκτρικής ενέργειας μεταξύ ηλεκτρικών οχημάτων(Brilliantova and Thurner, 2019). Αντίστοιχες εφαρμογές μελετώνται ολοένα και περισσότερο με τα μεγαλύτερα εγχειρήματα να είναι τα παραδείγματα της Ρωσίας και της Νότιας Αφρικής.

Στην Ρωσία, ενώ το δίκτυο παραγωγής ήταν το μεγαλύτερο παγκοσμίως, ωστόσο από τη δεκαετία του 90 ξεκίνησε μια διαδικασία ιδιωτικοποίησής του. Αυτό είχε σαν αποτέλεσμα να αυξηθούν τα κόστη και πολλές εταιρίες να στραφούν σε ανεξάρτητη παραγωγή ενέργειας, η οποία πλέον αγγίζει το 10% της εγχώριας παραγωγής. Παρά όλα αυτά η πλειοψηφία της Ρωσίας συνεχίζει να καταναλώνει ηλεκτρικό ρεύμα από το κεντρικό δίκτυο. Η δημιουργία ενός ενοποιημένου δικτύου blockchain για εμπόριο ηλεκτρικού ρεύματος στη συγκεκριμένη περίπτωση θα μπορούσε να δώσει δικαίωμα σε περισσότερες πηγές τροφοδοσίας ηλεκτρικού ρεύματος να εμφανιστούν και να ανταγωνιστούν το καθεστώς, κάτι που θα έδινε τη δυνατότητα στους πολίτες να επωφεληθούν από τις χαμηλότερες χρεώσεις, αλλά θα προσέδιδε και αποδοτικότερη αξιοποίηση της παραγωγής στο εγχώριο σύστημα.

Η περίπτωση της Νότιας Αφρικής ωστόσο αποτελεί ένα διαφορετικό παράδειγμα. Το 2013 η εθνική υπηρεσία ηλεκτρικής ενέργειας (NERSA, National Energy Regulator of South Africa) αποφάσισε την στροφή της παραγωγής προς την ηλιακή ενέργεια. Τα στοιχεία του 2018 αναφέρουν 80% παραγωγή από εργοστάσια άνθρακα, ενώ οι στόχοι για

το 2030 είναι 26% παραγωγή από ανανεώσιμες πηγές ενέργειας. Συνολικά 12’000 MW θα πρέπει να μετατεθούν από την πρώτη βιομηχανία (Swan, 2018). Αυτό το κλίμα έδωσε το έναυσμα σε εταιρίες όπως την Sun Exchange να εμφανιστούν. Πρόκειται για μια start up εταιρία ηλιοροφών, η οποία έχει δημιουργήσει ένα δίκτυο blockchain ανταλλαγής ηλιακής ενέργειας έναντι του SolarCoin, ενός κρυπτονομίσματος. Η εταιρία συνεργάζεται ήδη με πάνω από 6’500 μέλη, ιδιώτες ή οργανισμούς, οι οποίοι αφού εγκαταστήσουν ηλιοροφές σε κάποιο κτίριο, έχουν τη δυνατότητα να πουλήσουν οποιαδήποτε περίσσεια ηλεκτρικής ενέργειας απευθείας στο δίκτυο, έναντι αμοιβής (Sun Exchange, 2019).

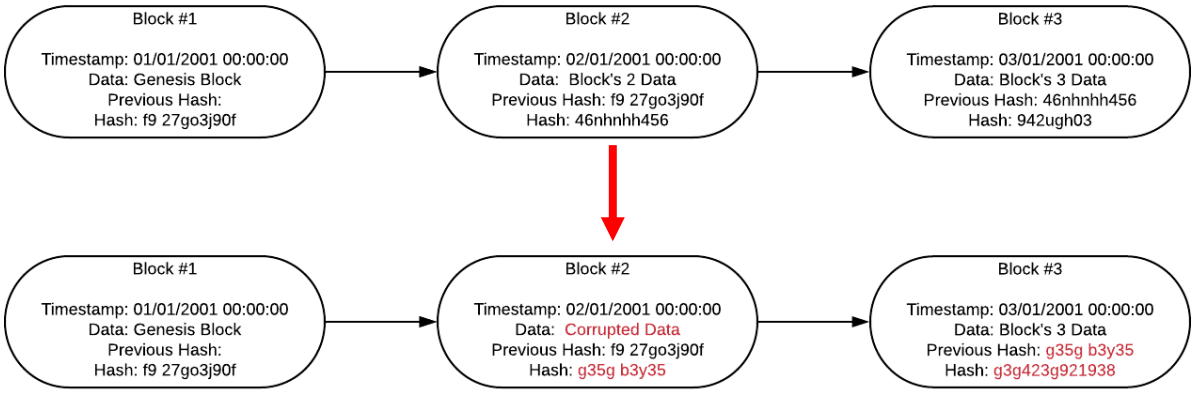
Κεφάλαιο 3: Τι είναι Blockchain

3.1 Τι είναι Blockchain;

Με βάση όλα τα προαναφερθέντα μπορούμε να καταλήξουμε σε μια πιο ολοκληρωμένη εικόνα του τι είναι ένα Blockchain. Το Blockchain, λοιπόν, είναι μία εκτενής λίστα καταγραφής δεδομένων, η οποία διαμοιράζεται ανάμεσα σε χρήστες. Ο λόγος, όμως, για τον οποίο παρουσιάζει ιδιαίτερη σημασία και χρησιμότητα είναι η αρχή λειτουργίας του. Με τον τρόπο που λειτουργεί ένα Blockchain μπορεί να εξασφαλίσει ακεραιότητα, ιδιωτικότητα και διαφάνεια των δεδομένων που διακινούνται, καθώς αυτά δεν ελέγχονται από μία κεντρική αρχή, αλλά διαμοιράζονται ανάμεσα σε χρήστες που έχουν μεταξύ τους τα ίδια δικαιώματα (Ikeda, 2018).

Η βασική αρχή λειτουργίας ενός Blockchain είναι η ακολουθία κάποιων προκαθορισμένων κανόνων, σύμφωνα με τους οποίους μπορεί να γίνει διακίνηση πληροφοριών. Οι κανόνες έχουν ανακοινωθεί ουσιαστικά από τον δημιουργό του εκάστοτε blockchain, κατά την δημοσίευση του ανοιχτού κώδικα και έκτοτε τηρούνται χάρη στη συμφωνία της πλειοψηφίας.

Καταρχάς η δομή ενός Blockchain αποτελείται από πολλά κομμάτια πληροφοριών (blocks) τα οποία είναι τοποθετημένα με συγκεκριμένη σειρά μέσα στη λίστα - Blockchain. Πέραν όλων των άλλων πληροφοριών ένα μπλοκ περιέχει μια ακολουθία χαρακτήρων γνωστής ως hash, ο οποίος προκύπτει ως συνάρτηση όλων των υπόλοιπων πληροφοριών, καθώς και της τιμής hash του προηγούμενου μπλοκ. Η ακολουθία αυτή είναι αποτέλεσμα μιας μονοσήμαντης και μη αντιστρέψιμης συνάρτησης, η οποία αποδομεί και συναθροίζει όλα τα υπόλοιπα δεδομένα του μπλοκ. Αυτό το χαρακτηριστικό δίνει την εξής ιδιότητα στο Blockchain: αν οποιαδήποτε πληροφορία, μέσα σε οποιοδήποτε μπλοκ αλλάξει, τότε το συγκεκριμένο μπλοκ δε μπορεί να επικυρωθεί, χωρίς να υπολογιστεί ένας καινούριος αριθμός hash, κατάλληλος για το καινούριο σύνολο πληροφοριών. Αυτό έχει σαν αποτέλεσμα, επίσης, το επόμενο μπλοκ να είναι εσφαλμένο, καθώς ένα από τα στοιχεία του είναι και ο αριθμός hash του προηγούμενου. Επομένως αν μια πληροφορία αλλάξει μέσα σε ένα μπλοκ, τότε εκείνο και όλα τα επόμενα είναι αυτομάτως εσφαλμένα και πρέπει να υπολογιστούν εκ νέου.

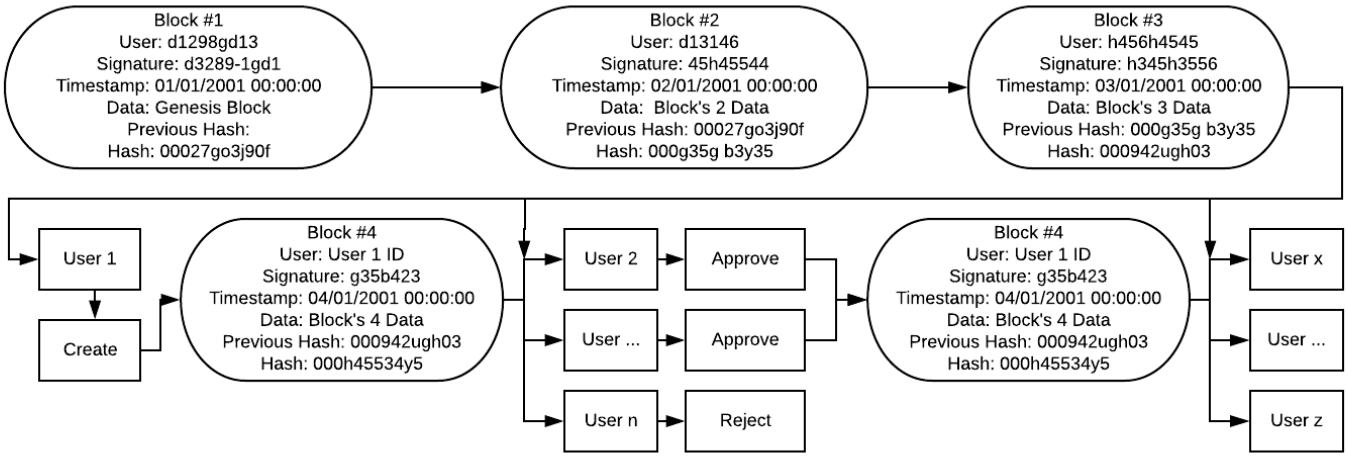


Σχήμα 4. Συνάρτηση Hash σε ένα Blockchain

Ο υπολογισμός ενός αριθμού hash καθαυτός δεν είναι μία δύσκολη διαδικασία. Ωστόσο τα blockchains έχουν συγκεκριμένους, προκαθορισμένους κανόνες που πρέπει να ακολουθηθούν για να προστεθεί ένα μπλοκ μέσα στη λίστα ενός blockchain. Αυτοί οι κανόνες αποτελούν τον "αλγόριθμο συναίνεσης" (consesus algorithm) ενός blockchain. Η πιο δημοφιλής κατηγορία κανόνων συναίνεσης είναι η τεχνητή δυσκολία υπολογισμού του αριθμού hash (mining), συνήθως με τη προαπαίτηση ο αριθμός να ξεκινάει με προκαθορισμένο τρόπο, παραδείγματος χάρη 3 χαρακτήρες "0". Ο αριθμός hash, όπως προαναφέρθηκε είναι αποτέλεσμα συγκεκριμένης συνάρτησης όλων των υπολοίπων πληροφοριών και ο τρόπος διαμόρφωσής του, από ένα χρήστη είναι η προσθήκη ενός επιπλέον στοιχείου - αριθμού, μεγάλου εύρους, το οποίο καλείται ο χρήστης, που θέλει να προσθέσει ένα καινούριο μπλοκ στο Blockchain, να υπολογίσει. Ωστόσο η συνάρτηση υπολογισμού ενός αριθμού hash δεν λειτουργεί και αντίστροφα, με αποτέλεσμα ο μόνος τρόπος εύρεσης του να είναι η δοκιμή πολλών εκατομμυρίων στοιχείων - αριθμών ή και πολύ περισσότερων, ανάλογα με τη δυσκολία που είναι προκαθορισμένη, κάτι που αποτελεί μια χρονοβόρα επαναληπτική διαδικασία (βλ. πίνακας 3, κεφάλαιο 2.1.2). Η παραπάνω διαδικασία ονομάζεται Blockchain mining και είναι ο πλέον χρησιμοποιούμενος αλγόριθμος συναίνεσης στα πιο δημοφιλή Blockchain, όπως το Bitcoin, το Etherium κ.α. Υπάρχουν και άλλοι αλγόριθμοι συναίνεσης που συνήθως δίνουν το δικαίωμα μόνο σε συγκεκριμένους χρήστες να προσθέσουν μπλοκ με πιθανότητες βασισμένες στη

χρήση που κάνουν ή εντελώς στην τύχη. Σε κάθε περίπτωση οι αλγόριθμοι αυτοί έχουν έναν κοινό τόπο: εξασφαλίζουν ότι η δημιουργία ενός μπλοκ είναι μία διαδικασία που βασίζεται στην πλειοψηφία και κανένας χρήστης δε μπορεί να καταχραστεί για προσωπικό συμφέρον.

Μόλις ένας χρήστης καταφέρει να κατασκευάσει ένα μπλοκ τότε έχει ως στόχο την κοινοποίηση του. Τα Blockchain κατά κύριο λόγο χρησιμοποιούν διαμοιρασμό μέσω ενός δικτύου χρήστη προς χρήστη (peer to peer network ή p2p). Αυτό σημαίνει πως κάθε χρήστης μπορεί να επικοινωνήσει άμεσα με τους υπόλοιπος χρήστες του δικτύου, είτε ως πομπός, διαμοιράζοντας ένα καινούριο μπλοκ, είτε ως δέκτης. Οι δέκτες ενός δικτύου Blockchain, έχουν ως στόχο την επικύρωση του νέου μπλοκ και εκ νέου διαμοίρασή του, είτε τη απόρριψή του, ενώ παράλληλα, εφόσον προσπαθούν να δημιουργήσουν και οι ίδιοι καινούριο μπλοκ (miners), αποδέχονται την καινούρια αλυσίδα και ξεκινούν να δουλεύουν πάνω στο επόμενο μπλοκ. Με αυτόν τον τρόπο ένα μπλοκ που ακολουθεί τους κανόνες του Blockchain θα επικυρωθεί και θα προωθηθεί και στους υπόλοιπους χρήστες, ενώ ένα μπλοκ που δεν τους ακολουθεί θα περιοριστεί. Επίσης ένας χρήστης θα προσθέσει τα καινούρια μπλοκ στο Blockchain που έχει ήδη αποθηκευμένο ή και θα διαμορφώσει τα τελευταία μπλοκ, ώστε να ταυτίζονται, μόνο αν πρόκειται για αλυσίδα επικυρωμένη και μεγαλύτερη από αυτή που διαθέτει ήδη. Έναν χρήστη τον συμφέρει να υιοθετήσει την καινούρια αλυσίδα που διαμοιράζεται άμεσα και όχι να συνεχίσει να προσπαθεί να δημιουργήσει ένα καινούριο μπλοκ στην παλιά, καθώς όλοι οι υπόλοιποι χρήστες θα κάνουν το ίδιο και θα δουλεύουν πάνω σε μια πιο εκτενή αλυσίδα από ότι ο ίδιος. Είναι, λοιπόν, ξεκάθαρο, ότι η διαδικασία που παρουσιάζεται παραπάνω έχει ως αποτέλεσμα το διαμοιρασμό μιας επικυρωμένης αλυσίδας με εγγυητή την πλειοψηφία.



Σχήμα 5. Διαμοιρασμός μιας λίστας Blockchain

Στα κρυπτονομίσματα, εκτός από όλα τα στοιχεία που έχουν αναφερθεί προηγουμένως, αναγράφεται επίσης ο αριθμός λογαριασμού του χρήστη, ο οποίος δημιούργησε το μπλοκ, καθώς και η υπογραφή του (βλ. κεφ. 5.8 Δημιουργία Ψηφιακών Υπογραφών). Ο αριθμός λογαριασμού του χρησιμοποιείται για την ανταμοιβή του σε κρυπτονομίσματα. Κατά τον διαμοιρασμό του μπλοκ αυτά τα στοιχεία δεν μπορούν να αλλοιωθούν προφανώς, καθώς συμπεριλαμβάνονται στην τιμή του hash, η οποία θα αλλοιωνόταν επίσης. Τα δεδομένα, όπως συναλλαγές, τα οποία οι χρήστες ανακοινώνουν με τη προθυμία να εισαχθούν στην λίστα, διαμοιράζονται και αυτά σε μία λίστα μέσα στο p2p δίκτυο, μέχρις ότου κάποιος χρήστης τα εντάξει κατά τη δημιουργία ενός μπλοκ στο δεδομένα του μπλοκ. Τα δεδομένα αυτά είναι συνήθως με τη σειρά τους υπογεγραμμένα με ασφαλή πρωτόκολλα, έτσι ώστε να μην γίνεται να υποστούν αλλοίωση.

Ο σκοπός, λοιπόν, ενός αλγόριθμου συναίνεσης είναι η εξασφάλιση της ακεραιότητας των δεδομένων που διακινούνται μέσα σε ένα Blockchain. Στην περίπτωση του Blockchain mining ένας χρήστης που θα ήθελε για προσωπικό όφελος να αλλάξει μια πληροφορία θα έπρεπε, όπως ήδη αναφέρθηκε να υπολογίσει εκ νέου τον αριθμό hash. Ωστόσο αυτή η διαδικασία είναι χρονοβόρα και εφόσον θέλει να αλλάξει μια πληροφορία σε ένα μπλοκ, το μπλοκ αυτό ήδη υπάρχει και οι υπόλοιποι χρήστες του Blockchain ήδη υπολογίζουν τον αριθμό hash του επόμενου. Ως αποτέλεσμα, ο κακόβουλος χρήστης θα

πρέπει σε λιγότερο χρόνο από όλους τους άλλους χρήστες να υπολογίσει τον καινούριο αριθμό hash του ήδη υπάρχοντος μπλοκ και τον αριθμό του επόμενου, ενώ οι υπόλοιποι χρήστες ασχολούνται μόνο με τον επόμενο αριθμό. Το σενάριο αυτό συνεπάγεται πως ο κακόβουλος χρήστης κατέχει αρκετά μεγαλύτερη υπολογιστική ισχύ από όλους τους άλλους χρήστες μαζί, κάτι που είναι πρακτικά αδύνατο.

3.2 Χαρακτηριστικά των Blockchain

Το κύριο χαρακτηριστικό ενός Blockchain είναι η έλλειψη μιας κεντρικής αρχής. Οι εφαρμογές εκείνες που χρησιμοποιούν Blockchain, επιτυχημένα, είναι απαντήσεις σε ζητήματα που θέτουν την ανάγκη για έλλειψη μιας κεντρικής αρχής ως επιτακτική, πχ το Bitcoin και η ανάγκη για ανεξαρτητοποίηση από τις τράπεζες. Οι λόγοι για τους οποίους μία κεντρική αρχή είναι αρνητική έχει να κάνει με την εκάστοτε εφαρμογή, ωστόσο μπορούν να συνοψισθούν στις ανάγκες για a) διαφάνεια, b) εμπιστευτικότητα και c) ιδιωτικότητα.

Η πλήρης **διαφάνεια** εξασφαλίζεται από τη στιγμή που μια εφαρμογή χρησιμοποιεί διαμοιρασμό ανάμεσα σε χρήστες για την αποθήκευση παλαιών και καινούριων πληροφοριών, όπως περιγράφηκε στο προηγούμενο κεφάλαιο, αντί ενός κεντρικού Server με κάποιον διαχειριστή και ως αποτέλεσμα περιορισμένα δικαιώματα στους χρήστες του. Οποιοσδήποτε χρήστης ενός Blockchain μπορεί να εξάγει από αυτό οποιαδήποτε πληροφορία έχει εισαχθεί από τη στιγμή της δημιουργίας του και έπειτα, ενώ αντίθετα στην περίπτωση ενός server, θα ήταν στην ευχέρεια του διαχειριστή να επιβάλει περιορισμένη προσβασιμότητα στους χρήστες. Αντίθετα σε ένα Blockchain, δεν υπάρχει τίποτα κρυφό, αφού και ο κώδικα είναι ανοιχτού τύπου και τα δεδομένα προσβάσιμα σε όλους.

Εμπιστευτικότητα μέσα σε ένα Blockchain προκύπτει, καθώς όλοι οι κανόνες, σύμφωνα με τους οποίους λειτουργεί ένα Blockchain είναι προκαθορισμένοι. Ένας χρήστης δεν χρειάζεται να εμπιστεύεται τους υπόλοιπους χρήστες για την πραγμάτωση κάποιου στόχου του μέσα στην εφαρμογή, αλλά μπορεί να εμπιστευτεί τους κανόνες λειτουργίας του Blockchain και σύμφωνα με τους οποίους αναγκάζονται να λειτουργούν

όλοι οι υπόλοιποι χρήστες. Χαρακτηριστικό παράδειγμα εμπιστευτικότητας, όπως αυτή προκύπτει από τη χρήση Blockchain είναι τα “smart contracts”, που χρησιμοποιούνται ευρέως σε αρκετά Blockchain (βλ. επόμενη ενότητα).

Τέλος, στη σύγχρονη εποχή γίνεται ολοένα και πιο επιτακτική η ανάγκη για **ιδιωτικότητα**, λαμβάνοντας τον όγκο πληροφοριών που διακινούνται στο διαδίκτυο, κάτι που ελέγχεται απόλυτα από τον διαχειριστή κάθε εφαρμογής. Με τη χρήση Blockchain, όμως, οι πληροφορίες που διακινούνται είναι εξ ολοκλήρου διαφανείς, εξαλείφοντας τη πιθανότητα κάποια πληροφορία να διακινηθεί χωρίς τη γνώση του χρήστη, με δεδομένο ότι ο ίδιος ο χρήστης έχει ήδη διαμοιραστεί την πληροφορία αυτή που έχει αποθηκευτεί στο αντίστοιχο μπλοκ. Εφαρμογές που χρησιμοποιούν μία κεντρική αρχή για τη λειτουργία τους τείνουν να απαιτούν τη χρήση “cookies”, δεδομένων δηλαδή που κοινοποιεί ο χρήστης στον διαχειριστή, προκειμένου ο τελευταίος να πραγματοποιήσει όλες τις απαιτούμενες διεργασίες εκ μέρους του. Τα δεδομένα αυτά αποθηκεύονται συνήθως κρυπτογραφημένα, με σχετική ασφάλεια, ωστόσο οι περιπτώσεις διαρροής δεδομένων σε κακόβουλα άτομα δεν είναι λίγες. Σε ένα Blockchain τις απαιτούμενες διεργασίες τις κάνει ο ίδιος ο χρήστης, ο οποίος είναι και υπεύθυνος για την αποθήκευση και διασφάλιση των προσωπικών του δεδομένων, παραδείγματος χάρη σε ένα κρυπτονόμισμα των κλειδιών κρυπτογράφησης του λογαριασμού του.

Τα παραπάνω χαρακτηριστικά καλύπτονται από την κατάργηση της κεντρικής αρχής. Το Blockchain είναι μια μέθοδος που μπορεί να προσδώσει, επιπλέον, ασφάλεια σε μια εφαρμογή, σύμφωνα με την αποτελεσματικότητα ενός κατάλληλου αλγορίθμου συναίνεσης, ουσιαστικά καταργώντας οποιαδήποτε ανάγκη για κεντρική διαχείριση. Παρόλα αυτά η χρήση Blockchain παρουσιάζει και κάποια αρνητικά, κάνοντάς τα δύσχρηστα ή μη συμφέρουσα επιλογή για κάποιες εφαρμογές.

Ένα σημαντικό μειονέκτημα της χρήσης Blockchain είναι η ταχύτητα και ο αποθηκευτικός χώρος, όπως αυτά περιγράφηκαν και στην ενότητα 2.2.2 Ανάλυση δεδομένων. Ένα ακόμη σημαντικό μειονέκτημα παρουσιάζει ο πλέον διαδεδομένος αλγόριθμος συναίνεσης proof of work (PoW), ο οποίος έχει ως βάση το “mining”. Πρόκειται για το γεγονός ότι η ανάγκη για επεξεργαστική ισχύ επιφέρει μεγάλο κόστος στην κατανάλωση ηλεκτρικής ενέργειας, κάτι που αυξάνεται όσο ένα Blockchain κερδίζει

έδαφος και περισσότεροι χρήστες εργάζονται στην εύρεση ενός κατάλληλου hash για ένα καινούριο μπλοκ.

Παρά τη ευρεία χρήση του συγκεκριμένου πρωτοκόλλου, δεν είναι λίγες οι εφαρμογές Blockchain, που κάνουν χρήση διαφορετικών αλγορίθμων συναίνεσης (Zhang and Lee, 2019). Τα πιο χαρακτηριστικά είναι:

- Το «τεκμήριο μεριδίου» (Proof of Stake - PoS), σύμφωνα με το οποίο η επιλογή του υπεύθυνου χρήστη για τη δημιουργία του επόμενου μπλοκ δε γίνεται μέσω ενός διαγωνισμού ταχύτητας υπολογισμού, όπως στον PoW, αλλά μέσω της σύγκρισης των κεφαλαιωρών των λογαριασμών (κεφάλαιο επί ώρες). Το πρωτόκολλο αυτό το χρησιμοποιούν εφαρμογές όπως το PPcoin (Kiayias *et al.*, 2017) και το Ouroburos (Katz and Shacham, 2017)
- Η «Εξουσιοδότηση μέσω τεκμηρίου μεριδίου» (Delegated Proof of Stake - DPoS), κατά την οποία οι λογαριασμοί με το μεγαλύτερο αριθμό κεφαλαιωρών ορίζουν τον υπεύθυνο χρήστη για τη δημιουργία του επόμενου μπλοκ (BitShares (Daniel Larimer, 2018), EOS (G. Lee 2018) - BFTDPoS
- Το πρωτόκολλο BFT (Byzantine Fault Tolerance) (Pathak and Iftode, 2006), μέσω του οποίου όλοι οι χρήστες ελέγχουν κατά πόσον οι υπόλοιποι χρήστες είναι κακόβουλοι και τελικά δημιουργείται ένα περιβάλλον χρηστών που εμπιστεύονται ο ένας τον άλλον.
- Το πρωτόκολλο Ripple Protocol consensus algorithm (RPCA) (Chase and MacBrough, 2018), σύμφωνα με το οποίο, οι φορείς του blockchain επικοινωνούν συνεχώς μεταξύ τους για την επικύρωση κάθε συναλλαγής, οι οποίοι «ψηφίζουν» και με 80% συμφωνία αποδέχονται την καινούρια συναλλαγή.

Οι παραπάνω αλγόριθμοι έχουν το πλεονέκτημα ότι δεν απαιτούν την μεγάλη υπολογιστική δύναμη του PoW. Ωστόσο στην εφαρμογή που αναπτύχθηκε στο πλαίσιο της εργασίας χρησιμοποιήθηκε ως πρωτόκολλο συναίνεσης το PoW. Αυτό συνέβη, καθώς ο αλγόριθμος του πρωτοκόλλου αποτελεί το πιο διαδεδομένο και δοκιμασμένο μέσο συναίνεσης, καθώς επίσης χαρακτηρίζεται από καλή λειτουργικότητα σε μικρή κλίμακα. Προκειμένου η εφαρμογή να δοκιμαστεί και να είναι λειτουργική προτιμήθηκε αυτός ο

αλγόριθμος, ωστόσο η δημιουργία μιας αντίστοιχης εφαρμογής, βασισμένη στην παρούσα, με διαφορετικό πρωτόκολλο θα μπορούσε να αποτελέσει μία εξίσου αξιόπιστη επιλογή.

3.3 Χρήση των smart contracts στα blockchains

Με τον όρο smart contracts δε γίνεται αναφορά άμεσα στο νομικό όρο του συμβολαίου. Ως smart contract μπορεί να χαρακτηριστεί οποιαδήποτε αυτοματοποιημένη διαδικασία προκαθορισμένου περιεχομένου εκτελείται με έναυσμα ένα προκαθορισμένο και ψηφιακά αποδεδειγμένο γεγονός. Ουσιαστικά πρόκειται για μια ψηφιακή συμφωνία με συγκεκριμένα κριτήρια και συγκεκριμένο περιεχόμενο. Τέτοιου είδους λογισμικό δε συναντάται για πρώτη φορά στα Blockchain, ωστόσο η ασφάλεια και η εμπιστοσύνη, που προσφέρονται στο περιβάλλον ενός Blockchain, έθεσαν τη βάση για την αύξηση της αξιοποίησής τους με την επέκταση της χρήσης της αντίστοιχης τεχνολογίας (Geiregat, 2018).

Από τις πρώτες αναφορές στον όρο ήταν η δημοσίευση του Nick Szabo το 1997 «Smart Contracts: Formalizing and Securing Relationships on Public Networks» (Szabo, 1997). Ο Szabo εισήγαγε την έννοια των smart contracts χρησιμοποιώντας ως παράδειγμα μηχανήματα - αυτόματους πωλητές, στις οποίες ένας οποιοσδήποτε πελάτης μπορεί να κάνει μια ανταλλαγή νομίσματος με ένα προϊόν, χωρίς τη συμμετοχή κάποιου τρίτου.

Τα οφέλη μιας τέτοιας αυτοματοποιημένης διαδικασίας γίνονται εύκολα αντιληπτά. Η αξιοπιστία των Blockchain με τη χρήση των smart contracts είναι δυνατόν να αντικαταστήσει την ανάγκη από τρίτους εγγυητές για τη διεκπεραίωση συμφωνιών μεταξύ των μελών του Blockchain. Τέτοιες συμφωνίες θα μπορούσαν να έχουν να κάνουν με τη ανταλλαγή αντικειμένων έως και ιδιοκτησίας, χωρίς κάποιο ρίσκο για τη συναλλαγή και μειώνοντας το κόστος της συμβουλής ενός συμβολαιογράφο, για παράδειγμα. Ο περιορισμός είναι οι δυνατότητες του κώδικα να μπορούν να περιλαμβάνει τους διαφορετικούς τομείς στους οποίους θα μπορούσαν να χρησιμοποιηθούν τα smart contracts, τομείς οι οποίοι, με τη διάδοση της τεχνολογίας και ενσωμάτωση ολοένα και περισσότερων χώρων στην τεχνολογία και τη διασύνδεση του διαδικτύου, συνεχώς διευρύνονται (Woebbeking, 2019).

Το Ethereum είναι το πλέον διαδεδομένο Blockchain για τη χρήση smart contracts. Πρόκειται για το δεύτερο σε αξία κρυπτονόμισμα (Ether) μετά το Bitcoin. Οι λογαριασμοί του Ethereum χωρίζονται σε δύο κατηγορίες: Τους ιδιωτικούς (Externally owned accounts EOA) και τους λογαριασμούς – συμβόλαια (contract accounts). Οι ιδιωτικοί λογαριασμοί είναι συνήθεις λογαριασμοί ενός κρυπτονομίσματος. Περιέχουν ιδιωτικό και δημόσιο κλειδί, με χρήση των οποίων μπορούν να πραγματοποιηθούν συναλλαγές.

Ενδιαφέρον παρουσιάζουν, ωστόσο, τα συμβόλαια. Πρόκειται ουσιαστικά για κώδικα, ο οποίος αποθηκεύεται στο Blockchain και εκτελείται αυτόματα από τους χρήστες του. Τα δεδομένα του αποθηκεύονται με τη μορφή hash, από την οποία προκύπτει η διεύθυνση url στην οποία είναι αποθηκευμένος ο κώδικας. Στην ίδια διεύθυνση είναι αποθηκευμένα και τα δεδομένα του συμβολαίου, όπως το ιστορικό ή άλλα χρήσιμα στοιχεία που αξιοποιούνται από τον κώδικα. Η γλώσσα πάνω στην οποία βασίζονται, κατά κύριο λόγο, τα smart contracts είναι η Solidus, η οποία είναι αρκετά όμοια με την Javascript, ωστόσο χρησιμοποιούνται και άλλες. Ο κώδικας εκτελείται είτε εκτελώντας μία συναλλαγή με αποδέκτη το συμβόλαιο είτε καλώντας το μέσα σε κώδικα και το περιεχόμενό του μπορεί να περιλαμβάνει συναλλαγές ή οτιδήποτε μπορεί να παραχθεί μία σύγχρονη γλώσσα με πολλές δυνατότητες όπως η Javascript.

Κεφάλαιο 4: Τα Blockchain στην Ναυτιλία

Η ναυτιλία αποτελεί το κύριο μεταφορικό μέσο τόσο για τελικά προϊόντα όσο και για πρώτες ύλες, ενώ συνολικά περίπου το 90% του παγκόσμιου όγκου(Jickells, Carpenter and Liss, 1990) μεταφέρεται με πλοία. Παρόλα αυτά η ναυτιλία είναι η λιγότερο αυτοματοποιημένη βιομηχανία μεταφοράς συγκριτικά με τις χερσαίες και τις εναέριες μεταφορές, όπου τα συστήματα ελέγχου και διαχείρισης από τη μεριά των διαφόρων φορέων είναι πολύ πιο σύγχρονα και ενοποιημένα. Ενώ η χρήση blockchain έχει ήδη ξεκινήσει σε πιλοτικό επίπεδο στην αυτοκινητοβιομηχανία, όπως αναφέρεται στο κεφάλαιο «2.2.2 Ανάλυση δεδομένων», στη ναυτιλία ακόμη δεν έχουμε κάποια εμπορική εφαρμογή που να στηρίζεται στην τεχνολογία Blockchain

Λαμβάνοντας υπόψιν, λοιπόν, τα παραδείγματα που αναφέρθηκαν στα προηγούμενα κεφάλαια και αφού αναλύθηκαν τα πλεονεκτήματα της τεχνολογίας Blockchain μπορούμε να καταλήξουμε σε κάποιους πολύ συγκεκριμένους παράγοντες, οι οποίοι καθιστούν ένα ζήτημα άξιο χρήσης της τεχνολογίας Blockchain, ιδιαίτερα σε ότι αφορά το περιβάλλον της ναυτιλίας:

- Ένα blockchain παρέχει τη δυνατότητα ανάπτυξης εμπιστοσύνης σε ένα περιβάλλον αγνώστων ή ακόμα και ανταγωνιστικών φορέων, σύμφωνα με τις προκαθορισμένες και αμετάβλητες αρχές λειτουργίας της εφαρμογής
- Ένα blockchain χαρακτηρίζεται από έλλειψη κεντρικής αρχής με λειτουργικό ωστόσο τρόπο, κάτι που προσφέρει νέες δυνατότητες για διευθέτηση ζητημάτων στον τομέα
- Τέλος ένα blockchain χαρακτηρίζεται από απόλυτη διαφάνεια, η οποία σε συνδυασμό με τα παραπάνω μπορεί να λύσει τα ζητήματα συμβατότητας μεταξύ διαφορετικών περιβαλλόντων, στον βαθμό που αυτό είναι επιθυμητό

Στη ναυτιλία εντοπίζεται ποικιλία ζητημάτων τα οποία παρουσιάζουν σημαντικά προβλήματα, στα οποία η χρήση τεχνολογίας blockchain θα μπορούσε να αποτελέσει αποτελεσματική λύση.

4.1 Αλυσίδα διακίνησης προϊόντων

Δημιουργία ενός δικτύου καταγραφής διακινούμενων προϊόντων ως μέρος ενός ευρύτερου συστήματος καταγραφής πόρων και προϊόντων. Αυτήν την στιγμή χρησιμοποιούνται υπηρεσίες εντοπισμού (tracking services), οι οποίες όμως είναι ανεξάρτητες και επιβαρύνουν τη διακίνηση πληροφοριών. Ένα σύστημα βασισμένο θα μπορούσε να μειώσει στο ελάχιστο το χρόνο επικύρωσης συναλλαγών και διακινήσεων προϊόντων μέσω λειτουργιών smart contracts, να καταστήσει δυνατό το ζωντανό έλεγχο και την ανάλυση του ιστορικού της εκάστοτε διακίνησης, καθώς και να βοηθήσει τον προγραμματισμό και την οργάνωση της λειτουργίας του στόλου. Τα smart contracts θα μπορούσαν να αντικαταστήσουν πλήρως τον ανθρώπινο παράγοντα από ενέργειες όπως την επικύρωση διακινήσεων και τον προγραμματισμό τους, ενέργειες που κοστίζουν ένα πολύ σημαντικό ποσοστό του συνολικού χρόνου μεταφοράς.

Ένα σύστημα blockchain, χάρη στους αυτοματοποιημένους και διεξοδικούς ελέγχους που γίνονται κατά τη λειτουργεία του μπορεί να προσφέρει ασφάλεια σε ένα δίκτυο μεταξύ αγνώστων φορέων, εταιρειών και προμηθευτών. Μέσω αυτού του δικτύου και χάρη στην ασφαλή αυτοματοποίηση, είναι δυνατή η διασταύρωση εγκυρότητας και συνέπειας των προμηθευτών και των εταιρειών για την λήψη απόφασης σχετικά με την επικύρωση συναλλαγών.

Τέλος ένα τέτοιο σύστημα είναι δυνατό να επεκταθεί σε όλα τα στάδια της αλυσίδας προμηθειών, φτάνοντας ακόμα και στο σημείο της πρώτης ύλης ενός εξαρτήματος. Χάρη στη διαφάνεια, αλλά και τη δυνατότητα ιδιωτικότητας μέσω κρυπτογράφησης είναι εύκολη η ενοποίηση όλων των φορέων μέσα σε ένα τέτοιο σύστημα, ενώ, παράλληλα, η διαχείριση και ο έλεγχος να μην υπάγεται σε μία μόνο κεντρική αρχή. Ως αποτέλεσμα μπορεί να είναι η χρήση ενός κοινού περιβάλλοντος πληροφοριών, σχετικά με τη γραμμή προμηθειών, από όλους τους φορείς, για τους οποίους, τα θετικά της καλύτερης εποπτεία, δεν συνεπάγονται την υποβάθμιση του ελέγχου πάνω στην διαχείριση των δικών του πόρων και πληροφοριών.

4.2 Συμβατότητα εταιρικών διαχειριστικών συστημάτων

Δημιουργία ενός ολοκληρωμένου συστήματος ERP, το οποίο να περιλαμβάνει όλα τα διαφορετικά συστήματα, δεδομένα των οποίων είναι απαραίτητα για τη διαχείριση και προγραμματισμό των πλοίων μίας εταιρείας. Τέτοια συστήματα μπορούν να αποτελούν: α) συστήματα καταγραφής θέσης, β) καταναλώσεων και λοιπόν στοιχείων πλοήγησης, γ) δεδομένων λειτουργίας των διαφόρων συστημάτων του πλοίου, δ) σύστημα καταγραφής ιστορικού συντήρησης πλοίου από ναυλωτές ή χρηματοπιστωτικά ιδρύματα, ε) καταγραφή ιστορικού ανταλλακτικών και προμηθειών, στ) καταγραφή ιστορικού συναλλαγών με προμηθευτές, ζ) διαχείριση γραφειοκρατικών ζητημάτων μιας εταιρείας.

Τα παραδείγματα που αναφέρθηκαν δεν αποτελούν από μόνα τους κάποια σημαντική καινοτομία. Ωστόσο η τεχνολογία blockchain, ιδιαίτερα χρησιμοποιώντας τεχνολογίες διαμοιρασμένων βάσεων δεδομένων, είναι δυνατόν να ενοποιήσει συστήματα παρόμοια με αυτό που περιγράφονται παραπάνω μεταξύ διαφόρων φορέων.

Ένα τέτοιο δίκτυο θα μπορούσε να αποτελέσει πηγή δεδομένων με σκοπό τη βελτιστοποίηση κάθε διεργασίας από οποιοδήποτε φορέα του δικτύου σε ό,τι αφορά τον οικονομικό παράγοντα και το χρόνο. Άλλα πιθανά δεδομένα προς καταγραφή θα μπορούσαν να είναι δρομολογήσεις και χαρακτηριστικά των πλοίων, τιμές καυσίμων, καιρικές και περιβαλλοντικές συνθήκες ανά περιοχή.

4.3 Σύστημα ανταλλαγής περιθωρίου ρύπων

Πρόκειται για το ζήτημα που θίγεται στο παρών κείμενο. Αυτήν την στιγμή στην ΕΕ πραγματοποιείται το πρόγραμμα MRV (Κεφ. 1.1 Νομοθεσία MRV), σύμφωνα με το οποίο κάθε πλοίο πρέπει να αναφέρει συγκεκριμένα δεδομένα σχετικά με τις καταναλώσεις και τις εκπομπές που είχε μέσα στον χρόνο. Οι αναφορές αυτές αφού δοθούν σε επίσημους επικυρωτές ανακοινώνονται τον επόμενο Ιούνιο. Ωστόσο το MRV είναι ένα σύστημα μελέτης και καταγραφής ρύπων και όχι ένα σύστημα επιβολής ορίων.

Μία λύση για επιβολή ορίων, συνδυαστικά με το παραπάνω πρόγραμμα, στο ναυτιλιακό περιβάλλον είναι ένα πρόγραμμα τύπου ETS (Emissions Trading Scheming), δηλαδή ανταλλαγής περιθωρίου ρύπων. Στο πλαίσιο αυτό, ένα πλοίο, το οποίο δεν μπορεί να πληροί τα όρια που έχουν οριστεί για εκπομπές θα μπορεί να εξαγοράσει ελαφρύνσεις

από άλλα πλοία. Ένα πρόγραμμα ETS λειτουργεί ήδη στην ευρωπαϊκή βιομηχανία (Κεφ. 1.5), ωστόσο στο πλαίσιο του προγράμματος εταιρείες έχουν τη δυνατότητα εξαγοράς ελαφρύνσεων μέσω διεξαγωγής δημόσιων δημοπρασιών.

Αντιθέτως ένα σύστημα ETS βασισμένο σε τεχνολογία blockchain παρουσιάζει τη δυνατότητα διεξαγωγής ανταλλαγών ρύπων μεταξύ των ίδιων των πλοίων. Αυτή η λύση προσφέρει την δυνατότητα της ανακύκλωσης του κόστους μέσα στον τομέα, αφού τα πλοία που είναι πιο φιλικά προς το περιβάλλον ανταμείβονται.

Κεφάλαιο 5: Εφαρμογή EnChain CO_2 a Blockchain based ETS

Στο πλαίσιο της εργασίας αναπτύχθηκε ένα πρόγραμμα Blockchain σε προγραμματιστική γλώσσα Matlab με στόχο τη δημιουργία ενός αυτοματοποιημένου συστήματος εμπορίας αέριων ρύπων. Το σύστημα αυτό λειτουργεί με βάση το δικό του κρυπτονόμισμα, το οποίο λειτουργεί ως μέσο για το εμπόριο ρύπων, επιβραβεύοντας τις περιπτώσεις εκείνες, στις οποίες ένα πλοίο βρίσκεται κάτω από το προκαθορισμένο όριο και χρεώνοντας τα πλοία που βρίσκονται πάνω από το όριο. Συγκεκριμένα, το blockchain περιέχει μία αλληλουχία από blocks, τα οποία χαρακτηρίζονται από λίστες καταγραφής δεδομένων στοιχείων των πλοίων και των αντίστοιχων ποσοτήτων αέριων ρύπων και καταγραφής συναλλαγών βασισμένες στο κρυπτονόμισμα της εφαρμογής, ανάμεσα σε διευθύνσεις χρηστών.

Για τη δημιουργία καθώς και επικύρωση διευθύνσεων χρησιμοποιήθηκε ο αλγόριθμος της java για την χρήση ελλειπτικών καμπυλών με στόχο την κρυπτογράφηση “ECDSA”(Elliptic Curve Digital Signature Algorithm), ο οποίος είναι και ο αλγόριθμος που χρησιμοποιεί και το Bitcoin. Με τη χρήση του αλγορίθμου αυτού δίνεται η δυνατότητα δημιουργίας ενός μοναδικού συνδυασμού κλειδιών για κάθε χρήστη: ενός ιδιωτικού και ενός δημοσίου. Το ιδιωτικό κλειδί χρησιμοποιείται για τη δημιουργία ψηφιακών υπογραφών, οι οποίες με χρήση του αλγόριθμο μπορούν να ελεγχθούν για εγκυρότητα χρησιμοποιώντας το δημοσίου κλειδί. Αυτό σημαίνει ότι μόνο ο ίδιος ο χρήστης μπορεί να υπογράψει μια συναλλαγή, μια καταγραφή δεδομένων και τη δημιουργία ενός block της λίστας blockchain, καθώς το ιδιωτικό κλειδί που απαιτείται το έχει μόνο ο ίδιος, ενώ οι υπόλοιποι χρήστες μπορούν να το επιβεβαιώσουν γνωρίζοντας το δημόσιο κλειδί του, το οποίο είναι ουσιαστικά η διεύθυνση λογαριασμού του χρήστη στη λίστα. Ο αλγόριθμος δε μπορεί να δουλέψει αντίστροφα και δεν υπάρχει τρόπος εξαγωγής ενός ιδιωτικού κλειδιού μέσα από αυτήν την διαδικασία.

Ένας χρήστης λοιπόν μπορεί να κάνει τις εξής ενέργειες στην λίστα blockchain:

- ✓ να πραγματοποιήσει μια συναλλαγή από τον λογαριασμό του προς έναν άλλον (εφόσον έχει το ποσό στο λογαριασμό του και υπογράψει σωστά τη συναλλαγή)

- ✓ να προωθήσει δεδομένα καταγραφής αέριων ρύπων ενός πλοίου που ανήκει στον λογαριασμό αυτόν (απαιτείται τα δεδομένα να είναι υπογεγραμμένα, με χρονολογική σειρά και σε καθημερινή βάση, διαφορετικά δε λαμβάνονται υπόψη)
- ✓ να επικυρώσει τα ανώτερα δεδομένα, αν ο χρήστης είναι ενδεικνυόμενος από την ευρωπαϊκή ένωση
- ✓ να δημιουργήσει ένα καινούργιο μπλοκ στη λίστα, στο οποίο εντάσσει τις συναλλαγές και τα δεδομένα που δεν έχουν ενταχθεί ακόμα στη λίστα, αλλά είναι επικυρωμένα.

Όταν ένας χρήστης δημιουργήσει ένα καινούργιο μπλοκ λαμβάνει μια αμοιβή, καθώς ο αλγόριθμος συναίνεσης που χρησιμοποιήθηκε κατά την ανάπτυξη του blockchain είναι το blockchain mining. Στο σενάριο που μελετάται το πρόγραμμα θεωρείται πως έχει μεγάλο αριθμό χρηστών από την ημέρα λειτουργίας του, καθώς το πρόγραμμα είναι ένας επίσημος τρόπος εμπορίας των αέριων ρύπων. Με τη χρήση του blockchain mining και με την ύπαρξη αρκετών χρηστών η έλλειψη κακόβουλων στοιχείων κατά τη λειτουργία του προγράμματος είναι πρακτικά δεδομένη.

Όπως αναφέρθηκε το πρόγραμμα δίνει τη δυνατότητα εμπορίας αέριων ρύπων μεταξύ των διαφόρων πλοίων. Αυτό επιτυγχάνεται με την ύπαρξη ενός προγραμματισμένου smart-contract μέσα στη δομή του προγράμματος. Εφόσον ένα πλοίο πληροί τα κριτήρια, τα οποία είναι, μεταξύ άλλων, να έχει το απαραίτητο υπόλοιπο για την πραγματοποίηση της συναλλαγή τότε το πλοίο συμμετέχει στην προγραμματισμένη διεκπεραίωση του smart-contract. Η δομή του blockchain προκαθορίζει τη δημιουργία συγκεκριμένων blocks, τα οποία περιέχουν τις απαραίτητες συναλλαγές, καθώς και τις αντίστοιχες μεταβιβάσεις στις ποσότητες των αέριων ρύπων.

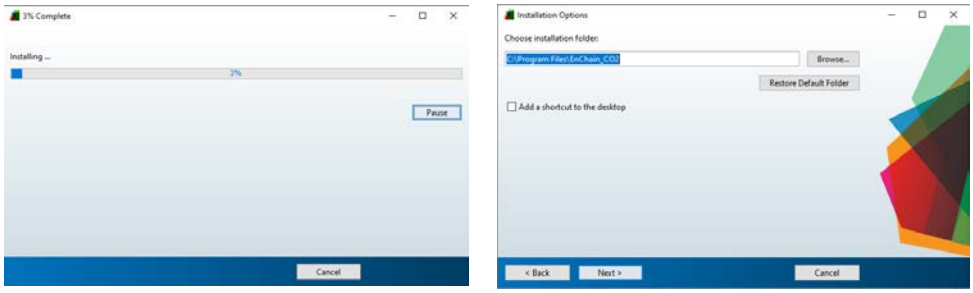
Τέλος το πρόγραμμα για να λειτουργήσει απαιτεί την ανταλλαγή της λίστας blockchain μεταξύ των χρηστών. Αυτό πραγματοποιείται μέσω της εργαλειοθήκης tcp/ip της Matlab, κατά την οποία ένας χρήστης γίνεται πομπός της λίστας του και ένας άλλος δέκτης, με τον δεύτερο να αξιολογεί την λίστα του πρώτου και αν περιέχει περισσότερα blocks, καθώς και πληροί τα κριτήρια εγκυρότητας, τότε την υιοθετεί. Με έναν μεγάλο αριθμό χρηστών αυτή η διαδικασία έχει ως αποτέλεσμα μόνο έγκυρες λίστες να

διαμοιράζονται και να επικρατεί ασφάλεια χάρη στην πλειοψηφία και τον αλγόριθμο συναίνεσης.

Για την αναλυτικότερη και πιο επεξηγηματική περιγραφή της εφαρμογής θα αναφερθούν παρακάτω οι σημαντικότερες λειτουργίες με παραπομπές από τον κώδικα:

5.1 Δημιουργία αυτόνομου προγράμματος μέσω του εργαλείου Matlab Runtime

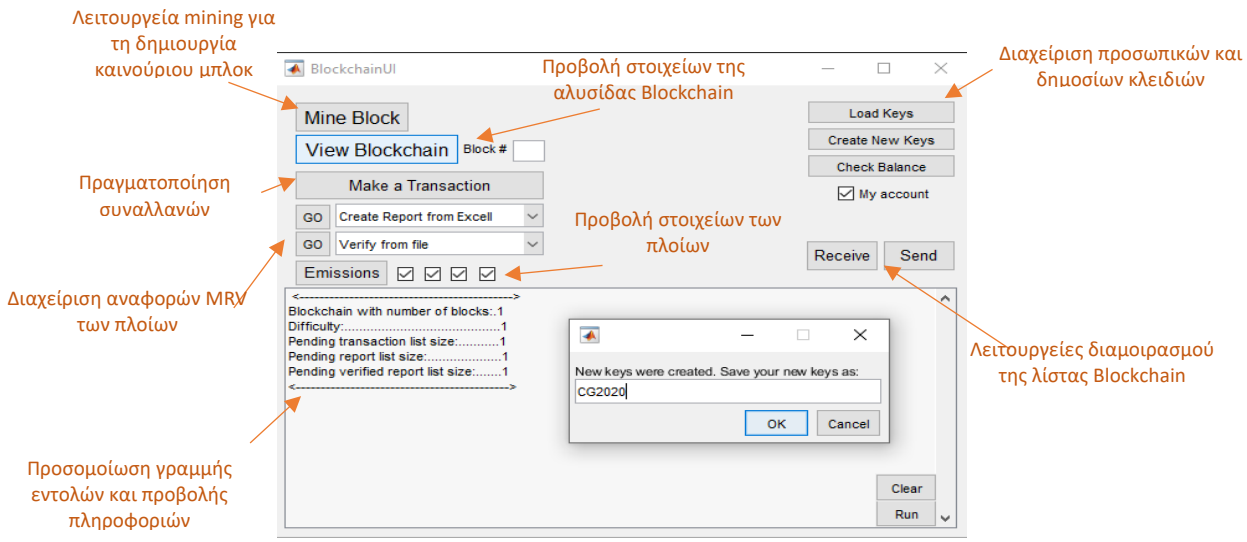
Μέσω του εργαλείου Matlab Runtime και του ενσωματωμένου στη Matlab μεταγλωττιστή ήταν δυνατή η δημιουργία ενός αρχείου εγκατάστασης της εφαρμογής. Το αρχείο εγκαθιστά τόσο την εφαρμογή, όσο και την υπηρεσία Matlab Runtime, η οποία λειτουργεί ως βάση, εφόσον δεν υπάρχει αντίγραφο της Matlab διαθέσιμο σε έναν υπολογιστή.



Εικόνα 2. Εγκατάσταση του αυτόνομου προγράμματος περιβάλλοντος Matlab Runtime – EnChain

5.2 Δημιουργία γραφικού περιβάλλοντος μέσω του εργαλείου GUIDE με τη μορφή figure

Μέσω του εργαλείου GUIDE δημιουργήθηκε γραφικό περιβάλλον, το οποίο περιλαμβάνει τις βασικές λειτουργίες της εφαρμογής. Παράλληλα προγραμματίστηκε μια προσομοίωση γραμμής εντολών, για την υλοποίηση πιο πολύπλοκων εντολών από το πρόγραμμα. Το σχετικό κουτί λειτουργεί και ως δίαυλος παροχής πληροφοριών στον χρήστη.



Εικόνα 3. Γραφικό περιβάλλον και βασικές λειτουργίες της εφαρμογής

5.3 Δημιουργία Blockchain

```
classdef Blockchain < handle

    properties
        chain
        difficulty
        pending_trx
        pending_report
        pending_vreport
        cashflow
        co2_limit
    end

    methods
        function obj = Blockchain()
            obj.chain = Block.genesisBlock(); %dhmeiourgei to prwto block
            obj.difficulty = 1;
            obj.cashflow = 0.5;
            obj.co2_limit = 1;
            obj.pending_trx = Transaction( ' ', ' ', 0, ' ');
            obj.pending_vreport = VReport(Report,' ',' ',' ',' ');
            obj.pending_report = Report;
        end
```

Για την χρήση της εφαρμογή χρησιμοποιείται η κλάση «Blockchain», για την οποία πρέπει να προσδιοριστούν:

α) η ιδιότητα «co2_limit», δηλαδή το όριο του διοξειδίου του άνθρακα ανά ώρα πλεύσης του πλοίου (με βάση το οποίο θα γίνει η ανταλλαγή ρύπων των πλοίων),

β) η ιδιότητα «cashflow», δηλαδή το ποσοστό του συναλλάγματος που θα πρέπει να αξιοποιηθεί για τις ανταλλαγές διοξειδίου του άνθρακα, το οποίο, τελικά, ρυθμίζει την τιμή του τόνου διοξειδίου του άνθρακα. Το κόστος υπολογίζεται ως:

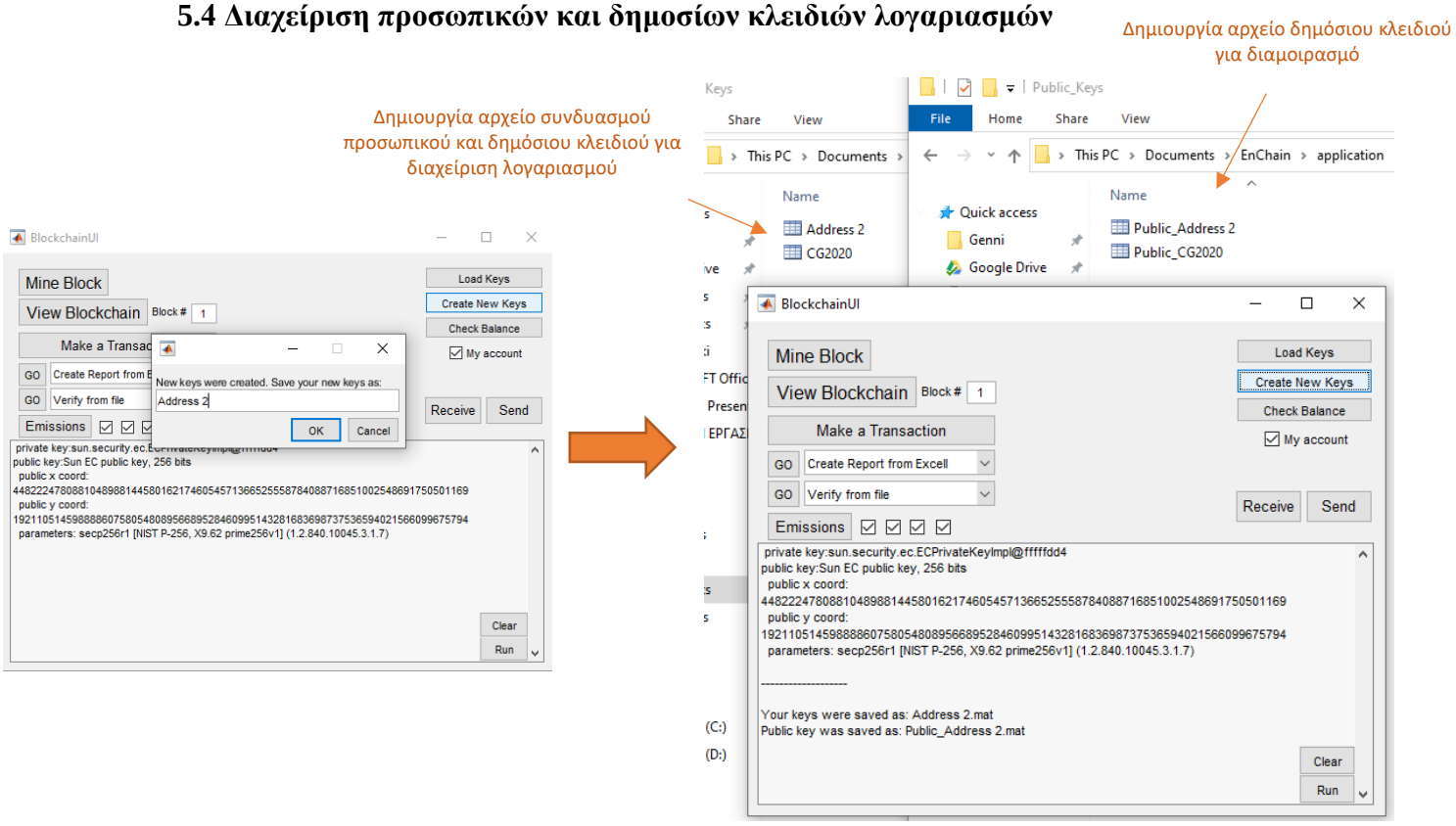
cost per CO_2 ton = cashflow * total currency produced / total exchanged tons of CO_2

Με αυτόν τον τρόπο ρυθμίζεται το κόστος και κατ' επέκταση η αξία του κρυπτονομίσματος, αφού σε καμία περίπτωση το κόστος του $1^{ος}$ τόνου διοξειδίου του άνθρακα δε θα είναι δυνατόν να ξεπεράσει την τιμή του αντίστοιχου επιβαλλόμενου προστίμου σε περίπτωση αδυναμίας εκπλήρωσης των συναλλαγών.

γ) η ιδιότητα «difficulty», η δυσκολία της αλυσίδας, δηλαδή η δυσκολία δημιουργίας ενός καινούριου μπλοκ, κατά τη διαδικασία του mining.

Επιπρόσθετα η συγκεκριμένη κλάση περιέχει τον κορμό του Blockchain (chain), και τις λίστες με τις συναλλαγές, τις αναφορές δεδομένων και τις επικυρωμένες αναφορές δεδομένων, οι οποίες δεν έχουν συμπεριληφθεί στον κορμό (pending_trx/report/vreport). Παραπάνω καλούνται οι γενέτειρες εντολές των παραπάνω λειτουργιών.

5.4 Διαχείριση προσωπικών και δημοσίων κλειδιών λογαριασμών



Εικόνα 4. Λειτουργίες δημιουργίας, αποθήκευσης και φόρτωσης κλειδιών λογαριασμού

Μέσω των λειτουργιών αυτών ένας χρήστης μπορεί να

- Δημιουργήσει καινούριο ζεύγος κλειδιών και ένα αντίγραφο του δημόσιου κλειδιού του
- Μεταφορτώσει και να διαχειριστεί ένα αποθηκευμένο ζεύγος κλειδιών
- Μεταφορτώσει ένα αντίγραφο δημοσίου κλειδιού για ενέργειες όπως αποστολή νομισμάτων

Γίνεται σαφές ότι για τη πραγματοποίηση λειτουργιών, όπως δημιουργία συναλλαγής από έναν λογαριασμό, αποστολή αναφορών πλοίου, επικύρωση συναλλαγών, δημιουργία καινούριου μπλοκ απαραίτητη είναι η υπογραφή των προαναφερθέντων. Για τη δημιουργία μιας έγκυρης υπογραφής απαιτείται η χρήση του ιδιωτικού κλειδιού, το οποίο είναι αποθηκευμένο στο αρχείο του ζεύγους κλειδιών. Η υπογραφή μπορεί να ελεγχθεί ως έγκυρη από έναν τρίτο, μόνο με τη χρήση του δημοσίου κλειδιού του λογαριασμού.

5.5 Δημιουργία Block

Όλα τα δεδομένα, για τα οποία γίνεται λόγος εισάγονται στη λίστα Blockchain, με τη μορφή ενός μπλοκ που τα περιέχει. Συγκεκριμένα ένα μπλοκ μέσα στη λίστα περιλαμβάνει τα εξής στοιχεία:
timestamp: Χρόνος δημιουργίας του μπλοκ
trxlist: Λίστα συναλλαγών
vreportlist: Λίστα επικυρωμένων αναφορών
hash: Χαρακτηριστικό hash του εν λόγω μπλοκ
prevHash: Χαρακτηριστικό hash του προηγούμενου μπλοκ
nonce: Τυχαίος αριθμός, ώστε το hash να έχει αποδεκτή τιμή
signature: Υπογραφή του χρήστη που δημιούργησε το μπλοκ
public: Λογαριασμός του χρήστη που δημιούργησε το μπλοκ

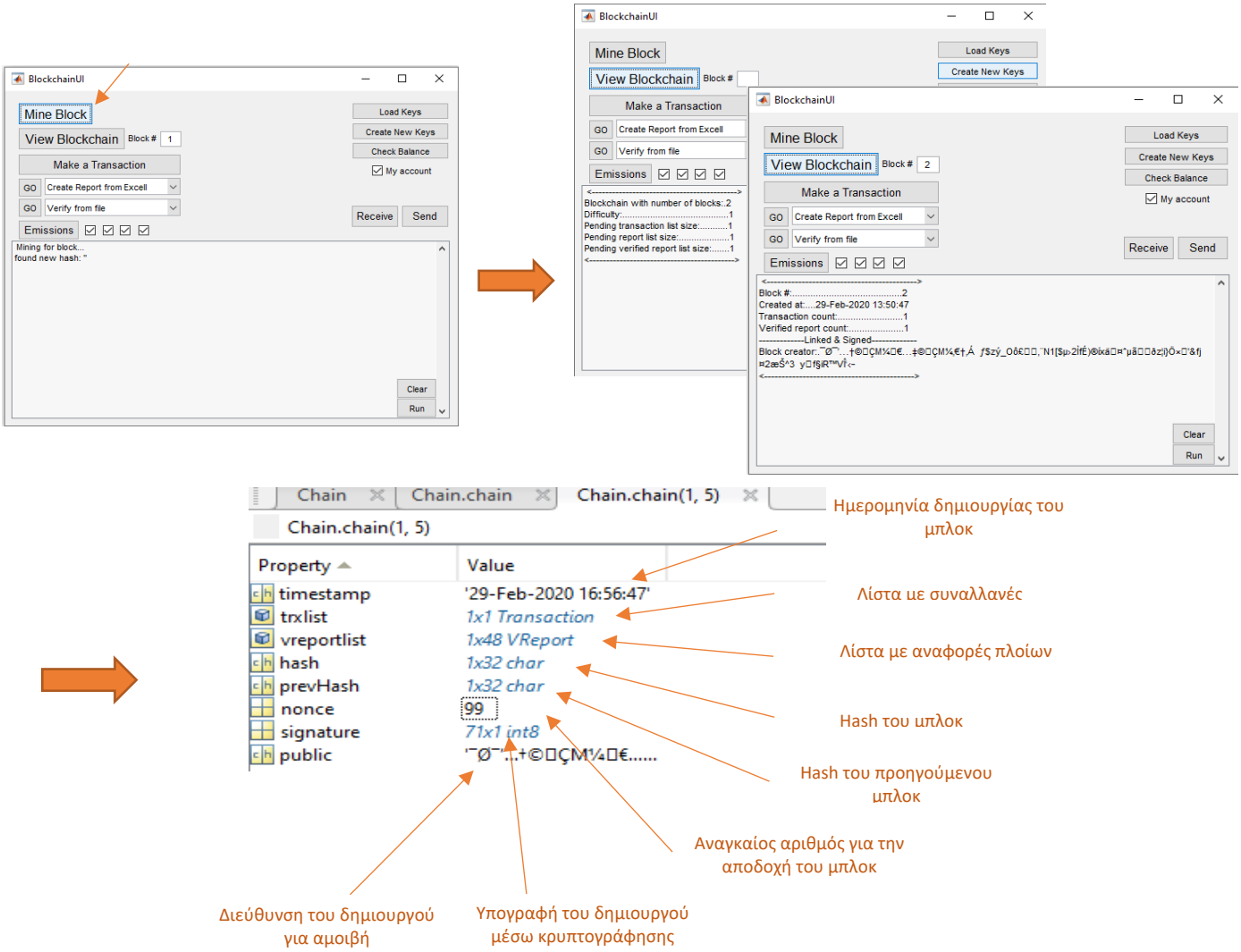
```
classdef Block < handle

   properties
      timestamp
```

```
        trxlist
        vreportlist
        hash
        prevHash
        nonce
        signature
        public
    end


        function block = Block(varargin)
            block.prevHash = varargin{1};
            block.timestamp = varargin{2};
            block.trxlist = varargin{3};
            block.vreportlist = varargin{4};
            block.nonce = 0;
            block.signature = int8(0);
            block.public = ' ';
            block.hash = Blockchain.calculateHash(block.prevHash,
block.timestamp, block.trxlist, block.vreportlist);
            if length(varargin) == 7 & varargin{5}~=0
                hash = block.hash;
                block.signature = Blockchain.Sign(hash,
varargin{6});%native2unicode(uint16(char(int16(Blockchain.Sign(hash, priv))' +
127)));
                valid = Blockchain.VerifySign(hash,varargin{7},block.signature);
                diff = varargin{5};
                block.public = varargin{7};
                block = mine(block, diff);
            end
        end
```

Η αλληλουχία χαρακτήρων «hash» είναι αποτέλεσμα της εντολής Blockchain.calculateHash. Ωστόσο εφόσον δεν έχει την επιθυμητή μορφή, προσδιορισμένη από τη δυσκολία του του blockchain, απαιτείται η χρήση της εντολής mine για τον υπολογισμό του hash. Το τελευταίο βήμα παρακάμπτεται για μπλοκ του τύπου “contract”, δηλαδή αυτοματοποιημένα μπλοκ διευθέτησης των ρύπων, τα οποία δεν έχουν διεύθυνση χρήστη ή υπογραφή.



Εικόνες 5α. και 5β. Δημιουργία ενός καινούριου μπλοκ και ιδιότητες

5.6 Block Mining

.

```
function block = mine(block, diff)
          NumZeros = diff; % Difficulty
          delay_time = 0.0003;
          found = false;
          Run.display_text('Mining for block...');
          strtrxlist = '';
          for i = 1:numel(block.trxlist)
              strtrxlist = strtrxlist + string(block.trxlist(i).fromAddress) +
string(block.trxlist(i).toAddress) + string(block.trxlist(i).amount) +
string(native2unicode(uint16(char(int16(block.trxlist(i).signature))' + 127)));
          end
          strvreportlist = '';
          for i = 1:numel(block.vreportlist)
              strvreportlist = strvreportlist +
string(block.vreportlist(i).vessel) + string(block.vreportlist(i).emission) +
```

```
string(block.vreportlist(i).SteamingTime) +
string(block.vreportlist(i).Deadweight) + string(block.vreportlist(i).time) +
string(block.vreportlist(i).public) +
string(native2unicode(uint16(char(int16(block.vreportlist(i).signature))' +
127)))  + string(block.vreportlist(i).Vpublic) +
string(block.vreportlist(i).url) + string(block.vreportlist(i).proof) +
string(native2unicode(uint16(char(int16(block.vreportlist(i).Vsignature))' +
127))) ;
          end
          for idx = 0:2^32
             block.hash = Blockchain.calculateHash(block.prevHash,
block.timestamp, strtrxlist, strvreportlist, block.nonce, block.signature,
block.public);
             if NumZeros == 0
                found = true;
                break
             end
             if block.hash(1:NumZeros) == zeros(1,NumZeros, 'uint8')
                found = true;
                break;
             end
             block.nonce = block.nonce+1;
             if block.nonce == 10000 || block.nonce == 250000 || block.nonce ==
50000
                Run.display_text(string('try no. ')+ num2str(block.nonce));
             end
          end
          if found
             Run.display_text(string('found new hash: "')+ num2str(block.hash)+
'"');
          end
          pause (delay_time)
        end
```

Η παραπάνω λειτουργία χρησιμοποιείται κατά την διαδικασία του mining για τη δημιουργία του αποδεκτού hash. Στην εφαρμογή που αναπτύχθηκε στα πλαίσια της διπλωματικής ο βαθμός δυσκολίας (Difficulty) είναι ενσωματωμένος στην αλυσίδα και ουσιαστικά αποτελεί τον αριθμό μηδενικών (0) που θα πρέπει να υπάρχουν στην αρχή της αλληλουχίας χαρακτήρων hash, ώστε αυτή να θεωρείται αποδεκτή. Το hash περιλαμβάνει όλα τα δεδομένα των επιμέρους στοιχείων κάθε μπλοκ μέσω της συνάρτησης, αποτέλεσμα της εντολής «calculateHash» σε συνδυασμό με το hash του προηγούμενου μπλοκ. Η ιδιότητα αυτή κάνει την αλυσίδα ασφαλή, όπως αυτό έχει περιγραφεί στις προηγούμενες ενότητες.

5.7 Δημιουργία Report

```
classdef Report < handle
	properties
		vessel
		emission
		SteamingTime
		Deadweight
		time
		signature
		public
	end

	methods
		function Rpt = Report(varargin)
			if numel(varargin)==0
				varargin{1}=' ';
				varargin{2}=0;
				varargin{3}=0;
				varargin{4}=0;
				varargin{5}=0;
			end
			if numel(varargin)==7
				Rpt.vessel=varargin{1};
				Rpt.emission=varargin{2};
				Rpt.SteamingTime=varargin{3};
				Rpt.Deadweight=varargin{4};
				Rpt.time=char(varargin{5});
				if ~strcmp(varargin{6},' ')
					str = string(Rpt.vessel) + string(num2str(Rpt.emission)) +
string(Rpt.SteamingTime) + string(Rpt.Deadweight) + string(Rpt.time);
					sha256hasher = System.Security.Cryptography.SHA256Managed;
					uint8_sha256 = uint8(sha256hasher.ComputeHash(uint8(char(str))));
					hash = char(uint8_sha256);
					Rpt.signature = Blockchain.Sign(hash, varargin{6});
					valid = Blockchain.VerifySign(hash,varargin{7},Rpt.signature);
				else
					Rpt.signature = 0;
				end
				Rpt.public=varargin{7};
			else
				disp('Error: could not create the report')
			end
		end
	end
```

Τα δεδομένα των πλοίων καταγράφονται μέσα στις αναφορές, οι οποίες δημιουργούνται μέσω της κλάσης «Report». Συμπληρώνονται τα εξής στοιχεία: α)

vessel - Αριθμός IMO πλοίου, Emission (Συνολικές εκπομπές μέσα στον αναφερόμενο χρόνο), Steaming Time (Ώρες λειτουργίας του πλοίου), Deadweight (Βάρος), Time (Χρονική περίοδος της αναφοράς).

5.8 Δημιουργία ψηφιακών υπογραφών

Στη συνέχεια με χρήση των προσωπικών κλειδιών του ιδιοκτήτη (Private key: varargin{6}, public key: Rpt.public) πραγματοποιείται η υπογραφή των παραπάνω στοιχείων (χρησιμοποιώντας το ιδιωτικό κλειδί) και ο έλεγχος εγκυρότητας της υπογραφής (χρησιμοποιώντας το δημόσιο κλειδί) μέσω των εντολών Blockchain.Sign και Blockchain.VerifySign αντίστοιχα. Σημειώνεται ότι στο αποτέλεσμα, δεν αναγράφεται το ιδιωτικό κλειδί που χρησιμοποιήθηκε, αλλά μόνο το δημόσιο, με αποτέλεσμα να είναι δυνατός ο έλεγχος της εγκυρότητας, αλλά όχι η αναπαραγωγή της υπογραφής από άλλο χρήστη. Ο τρόπος με τον οποίο λειτουργεί η ψηφιακή υπογραφή είναι παίρνοντας ως δεδομένα το ιδιωτικό κλειδί και τα δεδομένα τα οποία χρειάζεται να υπογραφούν με τη μορφή μιας αλληλουχίας χαρακτήρων που παράγεται από τη χρήση της εντολής System.Security.Cryptography.SHA256Managed.ComputeHash από την αντίστοιχη βιβλιοθήκη ελλειπτικών καμπυλών ECDSA. Με τη μέθοδο που περιγράφεται παραπάνω υπογράφονται και ελέγχονται όλα τα απαιτούμενα στοιχεία από χρήστες μέσα στον κώδικα.

Παρακάτω παρατίθενται οι εντολές υπογραφής, ελέγχου, αλλά και παραγωγής ζεύγους κλειδιών για χρήση ως λογαριασμός. Γίνεται χρήση των βιβλιοθηκών της JAVA security σχετικά με τη χρήση κλειδιών και υπογραφών

```
  function sign = Sign(str,privcode)
    ecKeyFac = KeyFactory.getInstance("EC");
    privcodenum = int8(int16(unicode2native(privcode)') - 127);
    pkcs8EncodedKeySpec = PKCS8EncodedKeySpec(privcodenum);
    priv = ecKeyFac.generatePrivate(pkcs8EncodedKeySpec);
    dsa = Signature.getInstance("SHA1withECDSA");
    dsa.initSign(priv);
    strByte = unicode2native(str);
    dsa.update(strByte);
    sign = dsa.sign();
end
function valid = VerifySign(str,pubcode,sign)
```

```
            dsa = Signature.getInstance("SHA1withECDSA");
            ecKeyFac = KeyFactory.getInstance("EC");
            pubcodenum = int8(int16(unicode2native(pubcode)') - 127);
            x509EncodedKeySpec = X509EncodedKeySpec(pubcodenum);
            pub = ecKeyFac.generatePublic(x509EncodedKeySpec);
            sig = Signature.getInstance("SHA1withECDSA");
            sig.initVerify(pub);
            strByte = unicode2native(str);
            sig.update(strByte);
            valid = sig.verify(sign);
            if ~valid
               fprintf('The signature is invalid\n')
            end

        end
        function [Prcode,Pkcode] = KeyGen()
            dsa = Signature.getInstance("SHA1withECDSA");
            keyGen = KeyPairGenerator.getInstance("EC");
            random = SecureRandom.getInstance("SHA1PRNG");
            keyGen.initialize(256, random);
            pair = keyGen.generateKeyPair();
            priv = pair.getPrivate();
            pub = pair.getPublic();
            Pkcode = native2unicode(uint16(char(int16(pub.getEncoded)' + 127)));
            Prcode = native2unicode(uint16(char(int16(priv.getEncoded)' + 127)));
            fprintf(['\n   private   key:',   char(priv),   '\n   public   key:',
char(pub),'\n'])
        end
```

Στις περιπτώσεις εκείνες, όποτε τα στοιχεία δεν προέρχονται από κάποιον χρήστη, αλλά από το πρόγραμμα αυτοματοποιημένα (όπως το smart contract και τις ανταμοιβές των miners βλ. παρακάτω), τα αντίστοιχα δεδομένα δεν υπογράφονται και αυτό λαμβάνεται υπόψη στην επικύρωση των μπλοκς.

5.9 Επικυρωμένες αναφορές

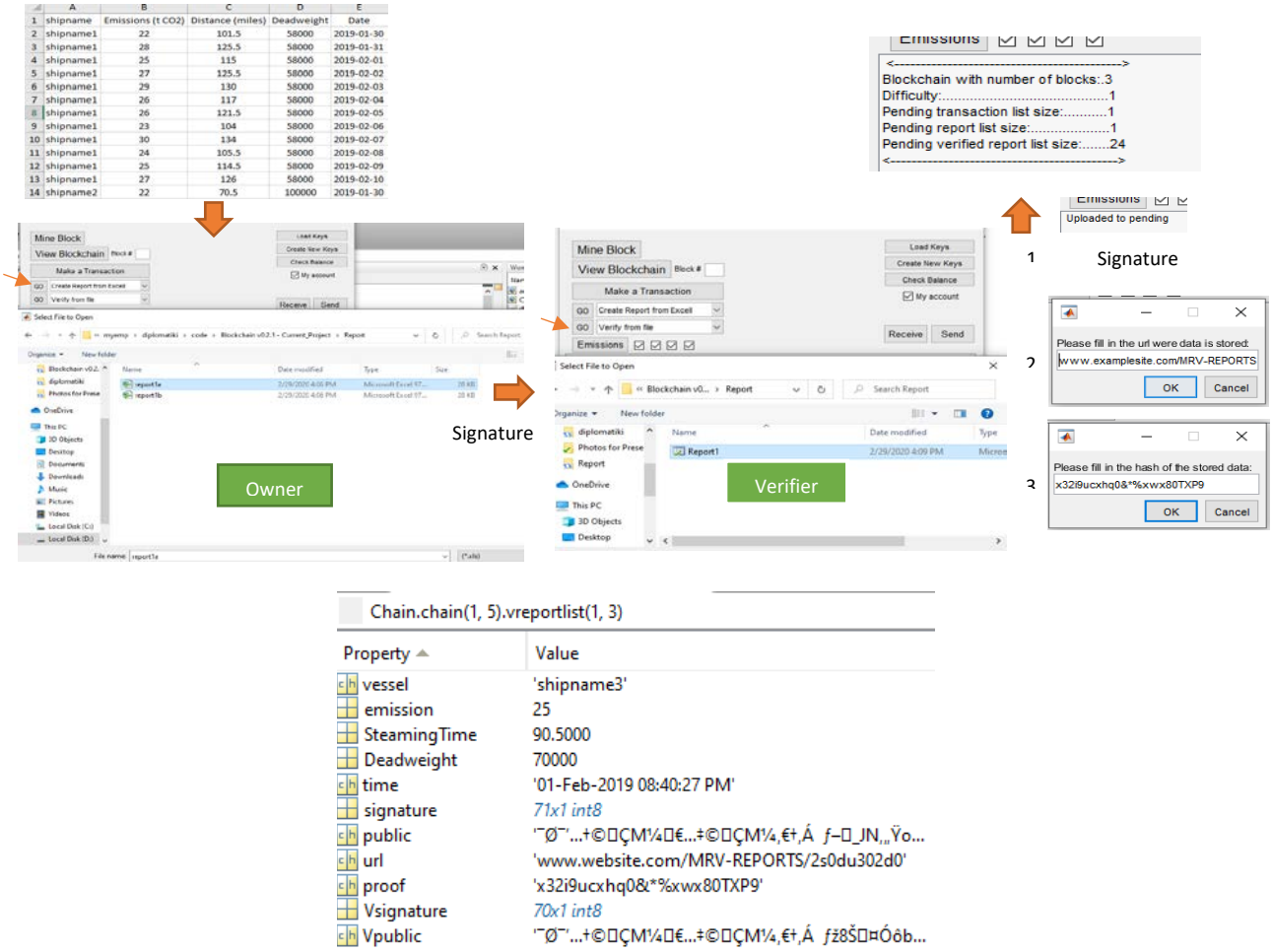
Όπως έχει ήδη αναφερθεί, οι αναφορές των πλοίων για να είναι αποδεκτές απαιτείται η υπογραφή και ενός επίσημου λογαριασμού (public key) επικυρωτή (verifier). Η ενέργεια αυτή γίνεται μέσω της παρακάτω λειτουργίας:

```
classdef VReport < handle
   properties
      vessel
      emission
      SteamingTime
      Deadweight
      time
      signature
      public
      url
      proof
      Vsignature
      Vpublic
   end

   methods
      function Rpt = VReport(Report,url,proof,private_key,public_key)
            Rpt.vessel=Report.vessel;
            Rpt.emission=Report.emission;
            Rpt.SteamingTime=Report.SteamingTime;
            Rpt.Deadweight=Report.Deadweight;
            Rpt.time=Report.time;
            Rpt.signature=Report.signature;
            Rpt.public=Report.public;
            Rpt.url=url;
            Rpt.proof=proof;

            if ~strcmp(private_key,' ')
               str  =  string(Rpt.vessel)  +  string(num2str(Rpt.emission))  +
string(Rpt.SteamingTime)   +   string(Rpt.Deadweight)   +   string(Rpt.time)   +
string(native2unicode(uint16(char(int16(Rpt.signature))'     +     127)))     +
string(Rpt.public) + string(Rpt.url) + string(Rpt.proof);
               sha256hasher = System.Security.Cryptography.SHA256Managed;
               uint8_sha256                                                    =
uint8(sha256hasher.ComputeHash(uint8(char(str))));
               hash = char(uint8_sha256);
               Rpt.Vsignature = Blockchain.Sign(hash, private_key);
               valid = Blockchain.VerifySign(hash,public_key,Rpt.Vsignature);
            else
               Rpt.Vsignature = 0;
            end
            Rpt.Vpublic=public_key;
      end
   end
endclassdef
```

Επί της ουσίας, σε μία ολοκληρωμένη αναφορά (Report), προστίθενται ο λογαριασμός του επικυρωτή (Rpt.Vpublic) και η υπογραφή (Rpt.Vsignature) μέσω του προσωπικού του κλειδιού (private_key). Επιπρόσθετα, ο επικυρωτής υποχρεούται να αναγράψει τη διαδικτυακή διεύθυνση, στην οποία αναγράφονται αναλυτικά οι αναφορές του αντίστοιχου πλοίου, οι οποίες δικαιολογούν τα στοιχεία της αναφοράς (Rpt.url). Τέλος πρέπει να αναγραφεί ένα υπολογισμένο hash, αποτέλεσμα συγκεκριμένης πράξης όλων των δεδομένων που αναγράφονται στο εν λόγω αρχείο. Η πράξη αυτή είναι και η πράξη που πραγματοποιείται σε κάθε μπλοκ για την εξαγωγή του μοναδικού hash του μπλοκ, αλλά και σε κάθε υπογραφή, για την εξαγωγή της μοναδικής «χορδής», η οποία υπογράφεται. Με αυτή τη μέθοδο πιστοποιείται η ακεραιότητα των δεδομένων που αναγράφονται στην εν λόγω διεύθυνση, ως αναλλοίωτα.



Εικόνες 6α. και 6β. Διαδικασία δημιουργίας ενός επικυρωμένου report και ιδιότητες

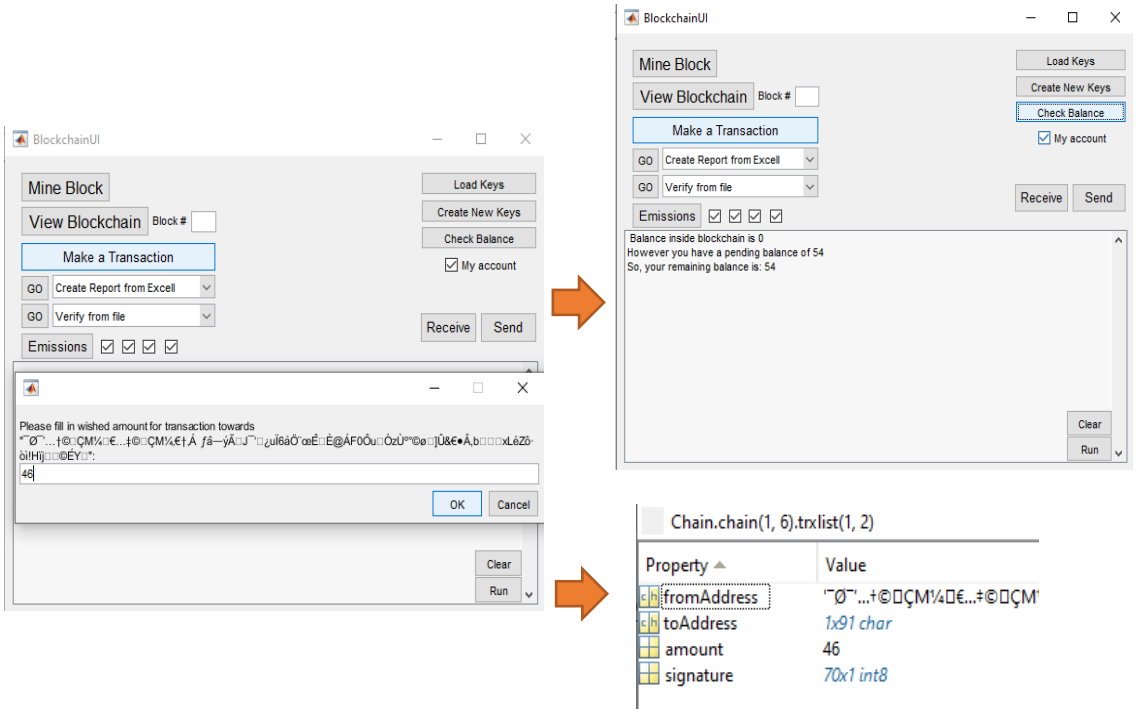
5.10 Συναλλαγές

Μέσω του στοιχείου της συναλλαγής (transaction) πραγματοποιείται η καταγραφή μιας συναλλαγής κρυπτονομίσματος μεταξύ δύο λογαριασμών. Σε μία συναλλαγή γίνεται, λοιπόν, αναγραφή των εξής χαρακτηριστικών: α) Διεύθυνση λογαριασμού (public key) πιστωτή (fromAddress), β) Παραλήπτη (toAddress), γ) Ποσού (amount) και δ) της υπογραφής του πιστωτή (signature), μέσω της ECDSA μεθόδου.

```
classdef Transaction < handle

   properties
      fromAddress
      toAddress
      amount
      signature
   end

   methods
      function trx = Transaction(from, to, amount, priv)
         trx.fromAddress = from;
         trx.toAddress = to;
         trx.amount = amount;
         if ~(priv == 0)
            str = string(from) + string(to) + string(num2str(amount));
            sha256hasher = System.Security.Cryptography.SHA256Managed;
            uint8_sha256 = uint8(sha256hasher.ComputeHash(uint8(char(str))));
            hash = char(uint8_sha256);
         end
         if from == ' '
            trx.signature = 0;
            valid = true();
         elseif ~(priv == 0)
            trx.signature = Blockchain.Sign(hash, priv);
            valid = Blockchain.VerifySign(hash,from,trx.signature);
         else
            trx.signature = 0;
            valid = true;
         end
         if ~valid
            trx.fromAddress = ' ';
            trx.toAddress = ' ';
            trx.amount = 0;
            trx.signature = 0;
         end
      end
   end
end
```



Εικόνα 7. Διαδικασία δημιουργίας συναλλαγής και ιδιότητες

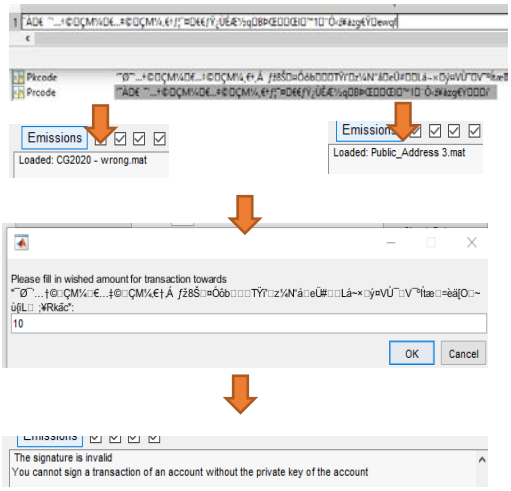
5.11 Επικύρωση Blockchain

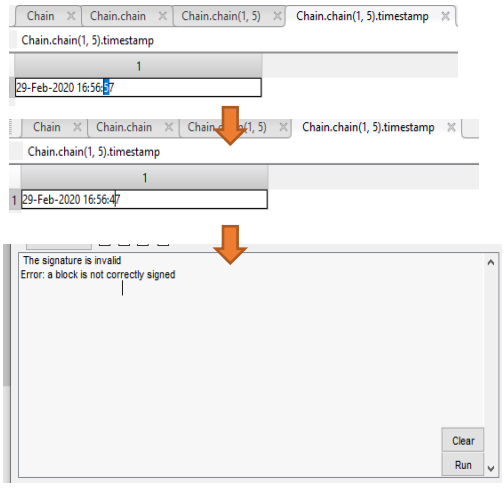
Παρακάτω παρουσιάζεται ένα από τα σημαντικότερα τμήματα της εφαρμογής. Πρόκειται για τον έλεγχο εγκυρότητας, δηλαδή ουσιαστικά τους κανόνες, σύμφωνα με τους οποίους ένα μπλοκ μπορεί να θεωρηθεί αποδεκτό. Η λειτουργία είναι καθοριστικής σημασίας, καθώς, μέσω αυτής εξασφαλίζεται η τήρηση των κανόνων λειτουργίας, καθώς και το κατά πόσον η αλυσίδα ενός χρήστη θα θεωρηθεί, αρχικά, αποδεκτή, θα υιοθετηθεί και κατ' επέκταση θα αναπαραχθεί σε τρίτους χρήστες. Πρόκειται για ελέγχους συνέχειας μεταξύ των μπλοκ και αυθεντικότητας των συναλλαγών και των αναφορών που περιέχονται στην αλυσίδα, μέσω της χρήσης των δημόσιων κλειδιών των χρηστών και των υπογραφών που αναγράφονται πάνω σε αυτή:

```
        function valid = validBlock(obj,i)
          valid = true;
          currentBlock = obj.chain(i);
          prevBlock = obj.chain(i-1);
          str = Blockchain.calculateHash(currentBlock.prevHash,
currentBlock.timestamp, currentBlock.trxlist, currentBlock.vreportlist);
          if
~Blockchain.VerifySign(str,currentBlock.public,currentBlock.signature)
             valid = false;
             Run.display_text('Error: a block is not correctly signed')
          end
```

```
          if currentBlock.hash ~=
Blockchain.calculateHash(currentBlock.prevHash, currentBlock.timestamp,
currentBlock.trxlist, currentBlock.vreportlist, currentBlock.nonce,
currentBlock.signature, currentBlock.public)
             Run.display_text('Error:1.'+ num2str(i));
             valid = false;
             Run.display_text('Error: A hash is not correctly calculated')
          elseif currentBlock.prevHash ~= prevBlock.hash
             Run.display_text(string('Error:2.')+ num2str(i));
             valid = false;
             Run.display_text('Error: A hash discontinuity has been observed')
          end
          counter1 = true;
          counter2 = true;
          if ~strcmp(prevBlock.public, ' ')
             counter1 = false;
          end
          for j = 1:numel(currentBlock.trxlist)
             if currentBlock.trxlist(j).fromAddress ~= ' '
                str = string(currentBlock.trxlist(j).fromAddress) +
string(currentBlock.trxlist(j).toAddress) +
string(num2str(currentBlock.trxlist(j).amount));
                sha256hasher = System.Security.Cryptography.SHA256Managed;
                uint8_sha256 =
uint8(sha256hasher.ComputeHash(uint8(char(str))));
                hash = char(uint8_sha256);
                if
~Blockchain.VerifySign(hash,currentBlock.trxlist(j).fromAddress,currentBlock.tr
xlist(j).signature)
                   valid = false;
                   Run.display_text('Error: a transaction is not correctly
signed')
                end
             end
             if strcmp(prevBlock.public, currentBlock.trxlist(j).toAddress) &
(currentBlock.trxlist(j).amount == 100)
                if counter1 == true
                   valid = false;
                   Run.display_text('Error: attempt of multiple mining
rewards')
                   break
                end
                counter1 = true;
             end
             if strcmp(currentBlock.trxlist(j).fromAddress, ' ') &
(~strcmp(prevBlock.public,
currentBlock.trxlist(j).toAddress)&~strcmp(currentBlock.trxlist(j).toAddress, '
'))
                k = i;
                while strcmp(obj.chain(k-1).public, ' ')
                   k = k-1;
                end
                if ~strcmp(obj.chain(k-2).public,
currentBlock.trxlist(j).toAddress)
                   counter2 = false;
                   Run.display_text('Error: attempt of illegal mining reward')
                end
             end
          end
          if ~counter1 | ~counter2
             valid = false;
             Run.display_text('Error: a transaction is not correct')
          end
```

```
            for j = 1:numel(currentBlock.vreportlist)
               if ~(j==1 & currentBlock.vreportlist(j).signature == 0);
                  str = string(currentBlock.vreportlist(j).vessel) +
string(num2str(currentBlock.vreportlist(j).emission)) +
string(num2str(currentBlock.vreportlist(j).SteamingTime))
+string(num2str(currentBlock.vreportlist(j).Deadweight)) +
string(currentBlock.vreportlist(j).time);
                  sha256hasher = System.Security.Cryptography.SHA256Managed;
                  uint8_sha256 =
uint8(sha256hasher.ComputeHash(uint8(char(str))));
                  hash = char(uint8_sha256);
                  if
~Blockchain.VerifySign(hash,currentBlock.vreportlist(j).public,currentBlock.vre
portlist(j).signature)
                     valid = false;
                     Run.display_text('Error: a vreport is not correctly signed
by owner')
                  end
                  str = string(currentBlock.vreportlist(j).vessel) +
string(num2str(currentBlock.vreportlist(j).emission)) +
string(currentBlock.vreportlist(j).SteamingTime) +
string(currentBlock.vreportlist(j).Deadweight) +
string(currentBlock.vreportlist(j).time) +
string(native2unicode(uint16(char(int16(currentBlock.vreportlist(j).signature))
' + 127))) + string(currentBlock.vreportlist(j).public) +
string(currentBlock.vreportlist(j).url) +
string(currentBlock.vreportlist(j).proof);
                  sha256hasher = System.Security.Cryptography.SHA256Managed;
                  uint8_sha256 =
uint8(sha256hasher.ComputeHash(uint8(char(str))));
                  hash = char(uint8_sha256);
                  if
~Blockchain.VerifySign(hash,currentBlock.vreportlist(j).Vpublic,currentBlock.vr
eportlist(j).Vsignature)
                     valid = false;
                     Run.display_text('Error: a vreport is not correctly signed
by verifier')
                  end
               end
            end
         end
```





Εικόνα 8. Παραδείγματα αποτυχίας συμμόρφωσης στα κριτήρια ελέγχου

5.12 Αυτόματο συμβόλαιο και οικονομική αξιολόγηση

Ακολουθεί η διαδικασία δημιουργίας του αυτόματου συμβολαίου, με βάση το ιστορικών των αναφορών που έχουν κοινοποιηθεί στη λίστα της αλυσίδας Blockchain μέχρι τη στιγμή της διεκπεραίωσής του:

```
       function c = Contract(varargin)
          obj = varargin{1};
          c = obj.Distribution;
          timestamp = char(datetime);
          if numel(varargin) == 2
             timestamp = varargin{2};
          else
             Run.display_text(c{3});
          end
          prevHash = obj.chain(end).hash;
          trxlist = c{1};
          vreportlist = VReport(Report,' ',' ',' ',' ');
          block = Block(prevHash, timestamp, trxlist, vreportlist, 0);
obj.chain(numel(obj.chain) + 1) = block;
       end

function s = Distribution(obj)
          ss1 = obj.Distribution2(obj.Distribution1);
          vessel = ss1.vessel;
          contractvalue = ss1.contractvalue;
          public = ss1.public;
          new_emission = contractvalue;
          total_emission = 0;
          for k = 1:numel(vessel)
             total_emission = contractvalue(k) + total_emission;
          end
          if total_emission < 0
             quote = ['Ships still stayed over the limit'];
             counter = 0;
             transacted_emission = 0;
             for k = 1:numel(vessel)
                if (contractvalue(k)) > 0
                   counter = counter + 1;
                   new_emission(k) = 0;
                   transacted_emission = transacted_emission +
contractvalue(k);
                end
             end
             total_transacted_emission = transacted_emission;
             while transacted_emission>0
                max = -10000000;
                for k = 1:numel(vessel)
                   if new_emission(k) < 0
                      if new_emission(k) > max
                         max = new_emission(k);
                      end
                   end
                end
                if -max < transacted_emission
                   for k = 1:numel(vessel)
                      if new_emission(k) == max
                         new_emission(k) = 0;
                      end
                   end
```

```
                    transacted_emission = transacted_emission + max;
                else
                    for k = 1:numel(vessel)
                        if new_emission(k) == max
                            new_emission(k) = max + transacted_emission;
                            transacted_emission = 0;
                        end
                    end
                end
            end
        else
            quote = ['All transactions were executed correctly'];
            counter = 0;
            transacted_emission = 0;
            for k = 1:numel(vessel)
                if contractvalue(k) < 0
                    counter = counter + 1;
                    new_emission(k) = 0;
                    transacted_emission = transacted_emission -
contractvalue(k);
                end
            end
            total_transacted_emission = transacted_emission;
            while transacted_emission>0
                mina = 0;
                minb = 0;
                min_counter = 0;
                for k = 1:numel(vessel)
                    if new_emission(k) > mina
                        minb = mina;
                        mina = new_emission(k);
                        min_counter = 1;
                    elseif new_emission(k) == mina
                        min_counter = 1 + min_counter;
                    elseif new_emission(k) > minb
                        minb = new_emission(k);
                    end
                end
                a = (minb - mina)*min_counter;
                if -a >= transacted_emission
                    for k = 1:numel(vessel)
                        if new_emission(k) > minb
                            new_emission(k) = new_emission(k) -
transacted_emission/min_counter;
                        end
                    end
                    transacted_emission = 0;
                else
                    for k = 1:numel(vessel)
                        if new_emission(k) > minb
                            new_emission(k) = minb;
                        end
                    end
                    transacted_emission = transacted_emission + a;
                end
            end
        end
        Price = obj.cashflow*(-obj.checkBalance(' ',-
1))/total_transacted_emission;
        strxs = Transaction( ' ', ' ', 0, ' ');
        j=1;
        for k = 1:numel(vessel)
            if new_emission(k) < contractvalue(k,1)
```

```
                strxs(j) =  Transaction( char(public(k)), 'Contract',
(contractvalue(k) - new_emission(k))*Price, 0);
                j=j+1;
             elseif new_emission(k) > contractvalue(k,1)
                strxs(j) =  Transaction( 'Contract', char(public(k)),
(new_emission(k) - contractvalue(k))*Price, 0);
                j=j+1;
             end
          end
          for k = 1:numel(vessel)
             strxs(j) =  Transaction( 'Contract', char(vessel(k)),
(new_emission(k) - contractvalue(k)), 0);
             j=j+1;
          end
          s = [{strxs},{table(vessel, new_emission, contractvalue,
public)},{quote}];
       end

function ss1 = Distribution1(obj)
          vessel = {' '};
          emission = [0];
          public = {' '};
          ContractBl = 1;
          for i = 2:numel(obj.chain)
             if strcmp(obj.chain(i).public,' ')
                ContractBl = i;
             end
          end
          new_obj = Blockchain;
          for j = ContractBl+1:numel(obj.chain)
             new_obj.chain(j-ContractBl) = obj.chain(j);
          end
          obj = new_obj;
          for i = 1:numel(obj.chain)
             for j = 1:numel(obj.chain(i).vreportlist)
                flag = false;
                c1 = 0;
                for k = 1:numel(vessel)
                   if ~strcmp(obj.chain(i).vreportlist(j).public,' ')
                      if (strcmp(obj.chain(i).vreportlist(j).vessel,vessel(k))
& (strcmp(public(k,1), obj.chain(i).vreportlist(j).public)))
                         flag = true;
                         c1 = k;
                      end
                   end
                end
                if ~strcmp(obj.chain(i).vreportlist(j).public,' ')
                   if flag
                      emission(c1,1) = emission(c1,1) +
obj.chain(i).vreportlist(j).emission;
                      SteamingTime(c1,1) = SteamingTime(c1,1) +
obj.chain(i).vreportlist(j).SteamingTime;
                      Deadweight(c1,1) = Deadweight(c1,1) +
obj.chain(i).vreportlist(j).Deadweight;
                      Times(c1,1) = Times(c1,1) + 1;
                   elseif strcmp(' ',vessel(1))
                      vessel(1,1) = {obj.chain(i).vreportlist(j).vessel};
                      emission(1,1) = [obj.chain(i).vreportlist(j).emission];
                      SteamingTime(1,1) =
[obj.chain(i).vreportlist(j).SteamingTime];
                      Deadweight(1,1) =
[obj.chain(i).vreportlist(j).Deadweight];
                      Times(1,1) = [1];
```

```
                        public(1,1) = {obj.chain(i).vreportlist(j).public};
                    else
                        emission(numel(vessel)+1,1) =
[obj.chain(i).vreportlist(j).emission];
                        SteamingTime(numel(vessel)+1,1) =
[obj.chain(i).vreportlist(j).SteamingTime];
                        Deadweight(numel(vessel)+1,1) =
[obj.chain(i).vreportlist(j).Deadweight];
                        Times(numel(vessel)+1,1) = [1];
                        public(numel(vessel)+1,1) =
{obj.chain(i).vreportlist(j).public};
                        vessel(numel(vessel)+1,1) =
{obj.chain(i).vreportlist(j).vessel};
                    end
                end
            end
        end
        ss1 = table(vessel, emission, SteamingTime, Deadweight, Times,
public);
    end

    function ss2 = Distribution2(obj,ss1)
        vessel = ss1.vessel;
        emission = [ss1.emission];
        SteamingTime = [ss1.SteamingTime];
        Deadweight = [ss1.Deadweight];
        Times = [ss1.Times];
        public = ss1.public;
        for k = 1:numel(vessel)
            flag = true;
            date = ' ';
            for i = 1:numel(obj.chain)
                for j = 1:numel(obj.chain(i).vreportlist)
                    if (strcmp(obj.chain(i).vreportlist(j).vessel,vessel(k,1))
& (strcmp(public(k,1), obj.chain(i).vreportlist(j).public)))
                        if date ~= ' '
                            if ((date + 32 ) >=
datetime(obj.chain(i).vreportlist(j).time))
                                date =
datetime(obj.chain(i).vreportlist(j).time);
                            else
                                flag = false;
                            end
                        else
                            date = datetime(obj.chain(i).vreportlist(j).time);
                            public(k,1) = {obj.chain(i).vreportlist(j).public};
                        end
                    end
                end
            end
            if ~flag
                vessel(k,1) = {''};
            end
        end
        ss2 = table(vessel, emission, SteamingTime, Deadweight, Times,
public);
        for i = 1:numel(vessel)
            if strcmp('',vessel(i,1))
                ss2(i,:) = [];
            end
        end
        size(ss2);
        vessel = ss2.vessel;
```

```
          emission = [ss2.emission];
          SteamingTime = [ss2.SteamingTime];
          Deadweight = [ss2.Deadweight];
          Times = [ss2.Times];
          public = ss2.public;
          tpublic = {' '};
          temission = [0];
          for i = 1:numel(vessel)
             added = 0;
             for k = 1:numel(tpublic)
                total_transacted_emission = 0;
                if strcmp(tpublic(numel(tpublic)),' ')
                   tpublic(1) = public(i,1);
                   temission(1) = emission(i,1);
                   tSteamingTime(1) = SteamingTime(i,1);
                   tDeadweight(1) = Deadweight(i,1);
                   tTimes(1) = Times(i,1);
                   added = 1;
                else
                   if (strcmp(public(i,1), tpublic(k)))
                      temission(k) = temission(k) + emission(i,1);
                      tSteamingTime(k) = tSteamingTime(k) + SteamingTime(i,1);
                      tDeadweight(k) = tDeadweight(k) + Deadweight(i,1);
                      tTimes(k) = tTimes(k) + Times(i,1);
                      added = 1;
                   end
                end
             end
             if (added == 0)
                tpublic(numel(tpublic)+1) = public(i,1);
                temission(numel(temission)+1) = emission(i,1);
                tSteamingTime(numel(tSteamingTime)+1) = SteamingTime(i,1);
                tDeadweight(numel(tDeadweight)+1) = Deadweight(i,1);
                tTimes(numel(tTimes)+1) = Times(i,1);
             end
          end
          contractvalue = [(obj.co2_limit-
emission./SteamingTime./Deadweight.*100000.*Times).*SteamingTime];
          ss2 = table(vessel, contractvalue, public);
          All_Korect = 1;
          while All_Korect == 1
             total_transacted_emission = 0;
             total_transacted_emission1 = 0;
             total_transacted_emission2 = 0;
             for i = 1:numel(contractvalue)
                if contractvalue(i) > 0
                   total_transacted_emission1 = contractvalue(i) +
total_transacted_emission1;
                else
                   total_transacted_emission2 = -contractvalue(i) +
total_transacted_emission2;
                end
             end
             total_transacted_emission =
min(total_transacted_emission1,total_transacted_emission2);
             t = table(tpublic);
             Price = obj.cashflow*(-obj.checkBalance(' ',-
1))/total_transacted_emission;
             for i = 1:numel(tpublic)
                if (contractvalue(i)*Price) <= obj.checkBalance(tpublic(i),-1)
                   t(i,:) = [];
                end
             end
```

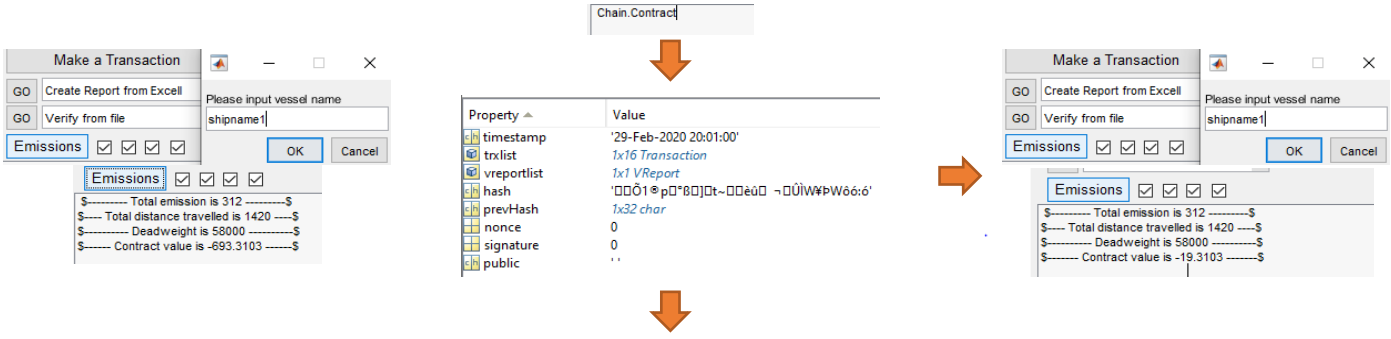
```
            size(t);
            All_Korect = 2;
            if numel(public)>0
                tpublic = t.tpublic;
                for j = 1:numel(tpublic)
                    if strcmp(tpublic(j),public(j,1))
                        ss2([j],:) = [];
                        All_Korect = 1;
                    end
                end
            end
            size(ss2);
        end
    end
```

Η λειτουργία “Distribtution1” δημιουργεί μια λίστα όλων των λογαριασμών και των αντίστοιχων στοιχείων σχετικά με τις εκπομπές ρύπων.

Η λειτουργία “Distribtution2”, αφού ελέγξει τις αναφορές διοξειδίου για μηνιαία συνέπεια, ελέγχει τη διαθεσιμότητα των λογαριασμών για κάλυψη των υποχρεώσεων, καθώς και πραγματοποιεί τον υπολογισμό της τιμής.

Η λειτουργία “Distribtution”, πραγματοποιεί τη όλες τις απαιτούμενες συναλλαγές μεταξύ των χρηστών που βρίσκονται πάνω και κάτω από το όριο.

Τέλος, η λειτουργία “Contract” είναι εκείνη που καλεί της ανώτερες και διαμορφώνει το μπλοκ στην αλυσίδα.



Vessel	ContractValue	Account	Balance
shipname1	-693.3103	Address 3	154
shipname2	151.1		
shipname3	-854.6714	CG2020	100
shipname4	1316.9		
shipname5	1076.9	Address 2	246
shipname6	-1197.53		
shipname7	-693.31		
shipname8	151.1		

=>

Vessel	ContractV	Account	Balance
shipname1	-19.3103	Address 3	115.2092
shipname2	0		
shipname3	-180.671	CG2020	147.6929
shipname4	0		
shipname5	0	Address 2	237.0979
shipname6	-523.529		
shipname7	-19.3103		
shipname8	0		

Εικόνα 9. Παράδειγμα δημιουργίας ενός αυτοματοποιημένου συμβολαίου

Στο παράδειγμα που παρουσιάζεται παραπάνω κλήθηκε η εντολή δημιουργίας ενός συμβολαίου ανταλλαγής ρύπων έναντι κρυπτονομίσματος. Η συγκεκριμένη εντολή κατά την ομαλή λειτουργία του προγράμματος θα καλείται αυτομάτως κάθε 1η Μαρτίου, λαμβάνοντας υπόψη όλες τις αναφορές που παραδόθηκαν τον προηγούμενο χρόνο.

Παράταση δύο μηνών δίνεται, έτσι ώστε οι εταιρίες να έχουν το χρόνο να προβούν σε όλες τις απαραίτητες προετοιμασίες για πληρούν τα κριτήρια συμμετοχής στο πρόγραμμα. Κύρια υποχρέωση είναι η αγορά κρυπτονομισμάτων, έτσι ώστε να καλύψουν το κόστος κατά τη διεκπεραίωση του συμβολαίου, εφόσον βρίσκονται πάνω από το όριο.

Στο παράδειγμα που πραγματοποιήθηκε στο περιβάλλον του προγράμματος τα πλοία “shipnamex”, τα οποία ανήκουν στους λογαριασμούς “Addrress 3”, “Addrress 2” και “CG2020” συμμετείχαν. Στην τελική αναφορά φαίνονται οι αλλαγές που προέκυψαν στο πορτοφόλι των λογαριασμών, αλλά και τι αντίκτυπο είχε αυτό στην τιμή συμβολαίου του κάθε πλοίου. Αρνητική τιμή υποδεικνύει υπερκέραση του ορίου και θετική αντίστροφα. Όπως φαίνεται το σύστημα δεν ήταν ικανό να καλύψει όλες τις ανάγκες για εκπομπές ρύπων των πλοίων, επομένως το υπόλοιπο αυτό μεταφέρεται προς το επόμενο συμβόλαιο.

Ο δείκτης συμβολαίου “contractvalue” προκύπτει από την παρακάτω σχέση:

$$\frac{grams\ of\ CO2\ produced}{Deadweight\ \times \text{Distance}} - limit) \times \text{Distance}$$

Σχέση 2. Δείκτης ωφέλειας συμβολαίου EnChain

σύμφωνα με τι αντίστοιχες αναφορές του πλοίου, με τον όρο «limit» να αναφέρεται στην ιδιότητα obj.co2_limit του blockchain, η οποία βρίσκεται ενσωματωμένη στη δομή της αλυσίδας.

Το ποσό που θα πρέπει ένας λογαριασμός να καταβάλει προκύπτει από τη σχέση:

$$contractvalue\ \times \text{Price}$$

όπου

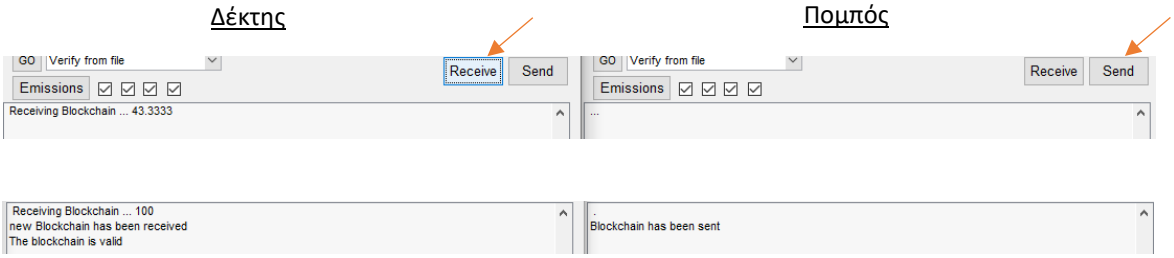
```
Price = obj.cashflow*(-obj.checkBalance(' ',-1))/total_transacted_emission;
```

Σχέση 3. Προσδιορισμός κόστους ανά μονάδα παραγόμενου ρύπου

Ο όρος obj.cashflow είναι ενσωματωμένος στην αλυσίδα και ουσιαστικά αναφέρεται στο ποσοστό του συνολικού συναλλάγματος το οποίο θα διακινηθεί για τη διεκπεραίωση όλων των ανταλλαγών ρύπων, δηλαδή του ποσού "total_transacted_emission". Τέλος η εντολή obj.checkBalance(' ',-1)) πραγματοποιεί έλεγχο όλων των ανταμοιβών που έχουν δοθεί σε miners, το άθροισμα των οποίων είναι ο συνολικός αριθμός κρυπτονομισμάτων που έχουν κοπεί.

Η παραπάνω διαδικασία είναι και αυτή που σε μεγάλο βαθμό θα καθορίσει την αξία του νομίσματος. Σε καμία περίπτωση μια εταιρεία δε θα επιθυμήσει να αγοράσει κρυπτονόμισμα έναντι μεγαλύτερης αξίας από την ποινή που θα δεχόταν, εφόσον δε συμμετάσχει στο συμβόλαιο. Από την άλλη τίθεται ένα ζήτημα εύρεσης του ποσού κρυπτονομισμάτων από λογαριασμούς που έχουν και είναι πρόθυμοι να το παρέχουν έναντι χρηματικής αξίας. Η σχέση αυτή αγορά και ζήτησης θα καθορίσει και την ανταλλακτική αξία συναλλάγματος.

5.13 Αποστολή μέσω P2P



Μέσω εντολών tcip δημιουργείται μία σχέση πομπού και δέκτη για την αποστολή και λήψη μίας αλυσίδας, εφόσον δοθούν οι εντολές από δύο διαφορετικούς χρήστες. Στόχος για την λειτουργικότητα μιας τέτοιας εφαρμογής θα ήταν η αυτόματη λειτουργία ενός δικτύου peer to peer, όπου οι χρήστες διαμοιράζουν τα αντίγραφα τις αλυσίδας τους συνεχώς.

Στην εφαρμογή που αναπτύχθηκε η αποστολή και λήψη πραγματοποιείται χειροκίνητα, ενώ η μέθοδος είναι η αποστολή κάθε ενός στοιχείου ξεχωριστά με συνεχή επικοινωνία των προγραμμάτων των δύο χρηστών για ομαλή διεξαγωγή της διαδικασίας.

Τέλος μετά την ολοκλήρωση της λήψης πραγματοποιείται καθολικός έλεγχος από τον λήπτη, ο οποίος υιοθετεί το αντίγραφο της αλυσίδας που περιέχει τα περισσότερα μπλοκ.

Κεφάλαιο 6: Τελικά συμπεράσματα

Το πρόγραμμα που παρουσιάστηκε στο παρόν κείμενο καλείται να ρυθμίσει ένα μείζον ζήτημα της εποχής σε ότι αφορά τομέα της ναυτιλίας. Ως πρόταση η θέση του συστήματος ανταλλαγής ρύπων βασισμένο σε τεχνολογία blockchain βρίσκεται στην προέκταση των συστημάτων MRV και DCS. Το πρόγραμμα όπως έχει παρουσιαστεί και αναπτυχθεί βρίσκεται σε πλήρη συμφωνία με τα δύο αυτά συστήματα, ως προς τον τρόπο λειτουργίας του.

Τα θετικά και ο λόγος για τον οποίο πραγματοποιήθηκε η παραπάνω ανάλυση είναι η δυνατότητα δημιουργίας ενός περιβάλλοντος μείωσης των εκπομπών, χωρίς ωστόσο να επιβαρυνθεί ο τομέας της ναυτιλίας. Η μηδενική επιβάρυνση του τομέα της ναυτιλίας πραγματοποιείται με την έννοια ότι κάθε κόστος από εταιρείες διαχείρισης πλοίων μη συμμορφωμένων στους κανονισμούς είναι δυνατόν να αποδοθεί ως επιβράβευση σε μία άλλη εταιρεία με πλοία χαμηλότερων εκπομπών. Σκοπός είναι η συνολική ενεργειακή αποδοτικότητα του κλάδου να αυξηθεί, το κόστος προς συμμόρφωση να μειωθεί και ταυτόχρονα να υπάρξει ένα κίνητρο επιβράβευσης προς πράσινες καινοτομίες.

Η τεχνολογία blockchain είναι ένα εξαιρετικά χρήσιμο εργαλείο για την υλοποίηση της παραπάνω λειτουργίας. Σε αντίθεση με ένα διαχειριζόμενο σύστημα ETS από κάποιον συγκεκριμένο οργανισμό, μέσω του blockchain, το κόστος λειτουργίας μπορεί να συρρικνωθεί. Τέλος ένα τέτοιο σύστημα αποτελεί μονόδρομο για τη πραγματοποίηση ανταλλαγής ρύπων μεταξύ ιδιωτικών φορέων σε μεγάλη κλίμακα, αντιμετωπίζοντας ζητήματα εμπιστευτικότητας μεταξύ των εταιρειών, αβεβαιότητας σε ότι αφορά την αξία και τήρησης όλων των κανονισμών.

Βιβλιογραφία

‘«ΦΕΚ. Τεύχος B’ 1756/22.05.2017». Εφημερίδα της Κυβερνήσεως: 17803, 17805, 17807 κ.ε.. 22 Μαΐου 2017’ (2017).

‘«ΦΕΚ. Τεύχος B’ 3488/21.08.2018. 44103 κ.ε.. .». Εφημερίδα της Κυβερνήσεως. 21 Αυγούστου 2018’ (2019).

Back, A. (2002) ‘Hashcash - A Denial of Service Counter-Measure’, *Http://Www.Hashcash.Org/Papers/Hashcash.Pdf*, (August), pp. 1–10.

Banerjee, A. (2018) *Blockchain Technology: Supply Chain Insights from ERP*. 1st edn, *Advances in Computers*. 1st edn. Elsevier Inc. doi: 10.1016/bs.adcom.2018.03.007.

BARTOS, J. (2015) ‘Does Bitcoin follow the hypothesis of efficient market?’, *International Journal of Economic Sciences*, IV(2), pp. 10–23. doi: 10.20472/es.2015.4.2.002.

Bhat, W. A. (2018) ‘Bridging data-capacity gap in big data storage’, *Future Generation Computer Systems*. Elsevier B.V., 87(2018), pp. 538–548. doi: 10.1016/j.future.2017.12.066.

Brilliantova, V. and Thurner, T. W. (2019) ‘Blockchain and the future of energy’, *Technology in Society*. Elsevier Ltd, 57(July 2018), pp. 38–45. doi: 10.1016/j.techsoc.2018.11.001.

Chase, B. and MacBrough, E. (2018) ‘Analysis of the XRP Ledger Consensus Protocol’. Available at: http://arxiv.org/abs/1802.07242.

Daniel Larimer (2018) ‘Delegated Proof-of-Stake Consensus | BitShares Blockchain’. Available at: https://bitshares.org/technology/delegated-proof-of-stake-consensus/.

Eropean Comission (2019) ‘EU Emissions Trading System (EU ETS) | Climate Action’, *Energy, climate, environment*, p. 1. Available at: https://ec.europa.eu/clima/policies/ets_en.

Geiregat, S. (2018) ‘Cryptocurrencies are (smart) contracts’, *Computer Law and Security Review*. Elsevier Ltd, 34(5), pp. 1144–1149. doi: 10.1016/j.clsr.2018.05.030.

Godbole, O. (2017) ‘Bitcoin Price Primed to Test $20k Ahead of CME Launch - CoinDesk’.

Haber, S. and Stornetta, W. S. (1991) ‘How to time-stamp a digital document’, *Journal of*

Cryptology, 3(2), pp. 99–111. doi: 10.1007/BF00196791.
Https://www.ecb.europa.eu/ (2017) ‘Πώς μπορεί η νέα τεχνολογία να μεταμορφώσει τις χρηματοπιστωτικές αγορές’;
Ikeda, K. (2018) *Security and Privacy of Blockchain and Quantum Computation*. 1st edn, *Advances in Computers*. 1st edn. Elsevier Inc. doi: 10.1016/bs.adcom.2018.03.003.
Ikeda, K. and Hamid, M. N. (2018) *Applications of Blockchain in the Financial Sector and a Peer-to-Peer Global Barter Web*. 1st edn, *Advances in Computers*. 1st edn. Elsevier Inc. doi: 10.1016/bs.adcom.2018.03.008.
IMO (2014) ‘Mepc.245(66) - 2014 Guidelines on the Method of Calculation of the Attained Energy Efficiency Design Index (Eedi) for New Ships’, *International Maritime Organization*, 245(April), pp. 1–30.
Jickells, T. D., Carpenter, R. and Liss, P. S. (1990) ‘Marine environment’, *The Earth as transformed by human action*, pp. 313–334. doi: 10.4337/9781788116275.00019.
Katz, J. and Shacham, H. (2017) *Crypto 2017, Proceedings, Part I*. Available at: https://link.springer.com/content/pdf/10.1007%2F978-3-319-63688-7.pdf.
Kiayias, A. *et al.* (2017) ‘PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake’, *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS’16*, 1919(January), pp. 1–27. doi: 10.1017/CBO9781107415324.004.
Kim, S. (2018) *Blockchain for a Trust Network Among Intelligent Vehicles*. 1st edn, *Advances in Computers*. 1st edn. Elsevier Inc. doi: 10.1016/bs.adcom.2018.03.010.
Lago, C. (2018) ‘How Singapore is using blockchain outside of cryptocurrencies’. Available at: https://www.cio-asia.com/article/3291758/blockchain/how-singapore-is-using-blockchain-outside-of-crypto-currencies.html.
Lee, G. (2018) ‘Documentation_TechnicalWhitePaper’. Available at: https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md.
Mcconaghy, Trent *et al.* (2016) ‘BigchainDB: A Scalable Blockchain Database’, *BigchainDB*, pp. 1–65.
Miura, A. *et al.* (2003) ‘Data collection system’, *Journal of the National Institute of Information and Communications Technology*, pp. 191–195. doi: 10.17660/actahortic.1968.6.20.
Nakamoto, S. (2009) ‘Bitcoin v0’.

New Liberty Standard (2009) *An Economic Revolution*.
OECD (2005) ‘The United Kingdom Climate Change Levy: A Study in Political Economy’, *Oecd Papers*, 5(5), p. 1. doi: 10.1787/oecd_papers-v5-art19-en.
Parry, I. *et al.* (2018) ‘Carbon Taxation for International Maritime Fuels: Assessing the Options’, *IMF Working Papers*, 18(203), p. 1. doi: 10.5089/9781484374559.001.
Pathak, V. and Iftode, L. (2006) ‘Byzantine fault tolerant public key authentication in peer-to-peer systems’, *Computer Networks*, 50(4), pp. 579–596. doi: 10.1016/j.comnet.2005.07.007.
Satoshi Nakamoto (2008) ‘Bitcoin: A Peer-to-Peer Electronic Cash System’, *www.bitcoin.org*, pp. 1–9. doi: 10.1007/s10838-008-9062-0.
Sun Exchange (2019) ‘SOLAR POWERED MONEY | The Sun Exchange’. Available at: https://thesunexchange.com/.
Swan, M. (2018) *Blockchain for Business: Next-Generation Enterprise Artificial Intelligence Systems*. 1st edn, *Advances in Computers*. 1st edn. Elsevier Inc. doi: 10.1016/bs.adcom.2018.03.013.
Szabo, N. (1997) ‘View of Formalizing and Securing Relationships on Public Networks | First Monday’. Available at: https://journals.uic.edu/ojs/index.php/fm/article/view/548/469.
THE MARINE ENVIRONMENT PROTECTION COMMITTEE (2011) ‘Annex 19: Resolution Mepc.203(62)’, 203(July), pp. 1–17.
THETIS-MRV (2019). EMSA. Available at: https://mrv.emsa.europa.eu/#public/emission-report.
ABS:Parry, Heine, Kizzier, Smith *et al.*(2018), ‘Low Carbon Shipping Setting the Course To Pathways To Sustainable Shipping’.
Transition, M. of the E. and I. (2020) ‘Energy taxation’.
Traufetter, G. (2019) ‘Klimapaket_ Bund und Länder erzielen Einigung - DER SPIEGEL’.
WIRED (2011) ‘The Rise and Fall of Bitcoin’. Available at: http://www.wired.com/2011/11/mf_bitcoin/all/.
Woebbeking, M. K. (2019) ‘The impact of smart contracts on traditional concepts of contract law’, *Journal of Intellectual Property, Information Technology and E-Commerce*

Law, pp. 106–113.
Zhang, L. *et al.* (2019) ‘Blockchain based secure data sharing system for Internet of vehicles: A position paper’, *Vehicular Communications*. Elsevier Inc., 16, pp. 85–93. doi: 10.1016/j.vehcom.2019.03.003.
Zhang, S. and Lee, J.-H. (2019) ‘Analysis of the main consensus protocols of blockchain’, *ICT Express*. Elsevier B.V., (xxxx), pp. 1–5. doi: 10.1016/j.icte.2019.08.001.