Πανεπιστήμιο Πειραιώς

Τμήμα Χρηματοοικονομικής & Τραπεζικής Διοικητικής

Μεταπτυχιακό Πρόγραμμα Σπουδών

«Χρηματοοικονομικής & Τραπεζικής Διοικητικής»

Master of Science (M.Sc) in Banking and Finance

ΘΕΜΑ:

«Η οικονομική ανάλυση του Blockchain»

Σόλων Α. Ανδρονής

Επιβλέπων Καθηγητής: Επίκουρος Καθηγητής Δημήτριος Βολιώτης

Τριμελής Επιτροπή: Επίκουρος Καθηγητής Δημήτριος Βολιώτης
Καθηγητής Στεφανάδης Χριστόδουλος
Αναπληρώτρια Καθηγήτρια Αναγνωστοπούλου Σεραΐνα

Πειραιάς, 2020

Περίληψη

Η τεχνολογία του Blockchain χαρακτηρίζεται από την αποκεντροποιημένη μορφή συναίνεσης μεταξύ αντισυμβαλλόμενων ατόμων, με χαμηλές σε κόστος πραγματοποίησης και ελέγχου συναλλαγές αντίθετο με τα παραδοσιακά κεντροποιημένα συστήματα. Το blockchain δεν συνδέεται μόνο με τα κρυπτονομίσματα αλλά ήδη έχει πολλά πεδία εφαρμογής και υπάρχουν πολλά σημάδια πως θα διαταράξει (disrupt) τον επιχειρηματικό και χρηματοοικονομικό κόσμο αναδύοντας νέες αγορές, τομείς αλλά και εφαρμογές όπως είναι τα Smart Contracts. Καταγράφουμε λοιπόν και αναλύουμε την τεχνολογία του blockchain πως συνδέεται με τις χαμηλές σε κόστος συναλλαγές, πως είναι η δομή της αρχιτεκτονική ενός blockchain συστήματος, αναλύσουμε τα πεδία εφαρμογής του και εξετάζοντας το βασικό αποτέλεσμα του άρθρου των Abadi J. και Brunnermeier M. (2019) που είναι το blockchain trilemma εφαρμόζουμε το μαθηματικό τους μοντέλο για να ερευνήσουμε πως μπορεί να επιτευχθεί η χειραγώγησης του blockchain δικτύου σε συγκεκριμένες περιπτώσεις αλγορίθμων συναίνεσης.

Λέξεις κλειδιά: Blockchain, Blocks, Κρυπτονομίσματα, Πρωτόκολλο λειτουργίας, Αλγόριθμος συναίνεσης, Ιδιωτικά και δημόσια blockchain, Smart Contracts, Double Spending, Επίθεση 51%, Ψηφοφορία, Blockchain Trilemma, Proof of Work (PoW), Proof of Stake (PoS), Private Blockchain, χειραγώγηση συναίνεσης

Summary

Blockchain technology is characterized by a decentralized form of consensus among counterparties, with low implementation costs and transaction control unlike traditional centralized systems. Blockchain wrongly linked only with cryptocurrencies but it already has many areas of applications and there are many signs that will disrupt the business and financial world by emerging new markets, sectors and applications such as Smart Contracts. We therefore record and analyze blockchain technology as it relates to low-cost transactions, how the architecture of a blockchain system is structured, its application areas and looking at the main result of the article by Abadi J. and Brunnermeier M. (2019) which is blockchain trilemma, appling their mathematical model to investigate how blockchain network manipulation can be achieved in specific cases of consensus algorithms.

Key Words: Blockchain, Blocks, Cryptocurrency, Protocol, Consensus algorithm, Private and Public blockchain, Smart Contracts, Double Spending, Attack 51%, Voting, Blockchain Trilemma, Proof of Work (PoW), Proof of Stake (PoS), Private Blockchain, Consensus manipulation

Ευχαριστίες

Ευχαριστώ θερμά, τον επιβλέποντα Καθηγητή μου Δημήτριο Βολιώτη για την συνεργασία του και την καθοδήγηση του κατά την διάρκεια εκπόνησης της διπλωματικής μου εργασίας.

Περιεχόμενα

Εισαγωγή

Η παρούσα διπλωματική εργασία εκπονείται με απώτερο σκοπό την απόκτηση του μεταπτυχιακού διπλώματος του τμήματος «Χρηματοοικονομικής & Τραπεζικής Διοικητικής» του Πανεπιστημίου Πειραιώς.

Στόχος της εργασίας είναι να ερευνηθεί και να αναλυθεί η οικονομική πλευρά που διέπει ένα blockchain καθολικό δίκτυο αλλά και να δοθεί έμφαση στους μηχανισμούς που μπορεί να οδηγήσουν στην χειραγώγηση των συναλλαγών σε αυτό εάν δεν υπάρχει κάποια κεντρική αρχή που εμπιστεύονται τα αντισυμβαλλόμενα άτομα, παρουσιάζοντας συγκεκριμένα παραδείγματα. Κίνητρο για την επιλογή του συγκεκριμένου θέματος διπλωματικής εργασίας αποτέλεσε το γεγονός πως επειδή το blockchain αποτελεί μια διαρκώς εξελισσόμενη τεχνολογία που γίνεται κομμάτι της καθημερινότητας μας και λανθασμένα είναι συνδεδεμένο κυρίως με την πλευρά των κρυπτονομισμάτων, καθώς έγινε γνωστό μέσα από την τεχνολογία του κρυπτονομίσματος Bitcoin, επιθυμούμε να καταγράψουμε και να αναλύσουμε τα πεδία εφαρμογής του καθώς ήδη υπάρχουν τα σημάδια πως θα διαταράξει (disrupt) τον επιχειρηματικό και χρηματοοικονομικό κόσμο.

Στην διεθνή βιβλιογραφία υπάρχουν δύο περιοχές που συνδέονται με την οικονομική έρευνα του Blockchain. Η πρώτη αφορά τον μηχανισμό του Blockchain που συνδέεται με την παραγωγή και την διατήρηση της αποκεντροποιημένης συναίνεσης, με τις μελέτες αυτές να αναλύουν και να κάνουν προβλέψεις μέσω της θεωρίας παιγνίων όπως για παράδειγμα για τα κίνητρα που υπάρχουν γύρω από τα πρωτόκολλα λειτουργίας ενός δικτύου blockchain. Αλλά και η δεύτερη που αφορά τις εφαρμογές που παρουσιάζει το Blockchain στον πραγματικό κόσμο, την λειτουργικότητα τους και την απευθείας επίδρασης τους στην πραγματική οικονομία όπως είναι οι μηχανισμοί και οι εφαρμογές των κρυπτονομισμάτων.

Για τον λόγο αυτό έχοντας ως σημείο κατεύθυνσης το πρώτο πεδίο οικονομικής μελέτης του Blockchain, βασιζόμενοι στο άρθρο των Abadi J. και Brunnermeier M. με τίτλο Blockchain Economic (2019) σε πρώτο στάδιο αναλύουμε το μαθηματικό μοντέλο που ανέπτυξαν και σε δεύτερο στάδιο αναλύουμε το βασικό συμπέρασμα τους που αναφέρεται ως Blockchain Trilemma. Το Blockchain Trilemma που εξέφρασαν αποδεικνύει πως για να επιτευχθεί η συναίνεση χωρίς την διαμεσολάβηση μιας κεντρικής έμπιστης αρχής είναι απίθανο για ένα ψηφιακό καθολικό σύστημα καταγραφής συναλλαγών blockchain

ταυτόχρονα να εξυπηρετεί τρεις σκοπούς. Να είναι ανεξάρτητο (self- sufficient), να είναι χωρίς κόστος χρήσης (free-rent) και να κάνει αποδοτική χρήση των πόρων του (resource-efficient).

Αναλυτικότερα, η διπλωματική εργασία χωρίζεται σε τέσσερα κύρια κεφάλαια καθώς και στα αντίστοιχα κεφάλαια που αφορούν τα συμπεράσματα και την βιβλιογραφία που χρησιμοποιήθηκε για την εκπόνηση της. Το πρώτο κεφάλαιο της διπλωματικής εργασίας έχει ως στόχο να γίνει κατανοητή η εισαγωγή στα βασικά χαρακτηρίστηκα ενός οποιουδήποτε αποκεντροποιημένου καθολικού συναλλαγών blockchain και να κατανοηθεί η χρησιμότητα του, τα πλεονεκτήματα αλλά και τα προβλήματα που εμφανίζονται στην χρήση του στην καθημερινή ζωή. Να αναλυθούν οι βασικές έννοιες που αφορούν την δομή του, τον τρόπο που μπορεί κάποιος να εισέρθει σε ένα blockchain αλλά και τι είδους καινοτόμες εφαρμογές μπορεί να υποστηρίξει. Ακόμη παρουσιάζεται ο τρόπος που επιτυγχάνεται η διακράτηση των αρχείων συναλλαγών, πως αποφεύγονται οι πράξεις ψευδών αναφορών και πως επιτυγχάνεται η ασφάλεια στις συναλλαγές. Τέλος γίνεται αναφορά στο κόστος επαλήθευσης συναλλαγών και χρήσης ενός blockchain σε σχέση με τους κεντροποιημένους τρόπους αλλά και αναλύεται σύμφωνα με διεθνείς μελέτες το κατά πόσο θα ήταν εφικτό να πραγματοποιούνται σε καθημερινή βάση εμπορικές πληρωμές μέσω κρυπτονομισμάτων.

Το δεύτερο κεφάλαιο της διπλωματικής εργασίας επικεντρώνεται γύρω από τρία βασικά θέματα που διέπουν ένα Blockchain. Τα πρωτόκολλα λειτουργίας, τους αλγόριθμους συναίνεσης και το πρόβλημα των διπλών δαπανών. Αναλυτικότερα, παρουσιάζονται τα βασικότερα και πιο διαδεδομένα πρωτόκολλα λειτουργίας που υπάρχουν σήμερα, αναλύεται ο αλγόριθμος συναίνεσης και οι βασικές διαφορές που παρουσιάζει σε σχέση με ένα πρωτόκολλο λειτουργίας αναλύοντας τα βασικά χαρακτηριστικά των γνωστότερων και σημαντικότερων αλγορίθμων συναίνεσης. Ενώ τέλος αναλύουμε ένα σύνηθες πρόβλημα που εμφανίζεται στα blockchain δίκτυα που είναι το πρόβλημα των διπλών δαπανών (Double spending problem) και αναφερόμαστε και αναλύουμε υπό ποιες περιπτώσεις είναι πιθανό να προκληθεί.

Το τρίτο κεφάλαιο της διπλωματικής εργασίας αποσκοπεί αρχικά να γίνουν κατανοητές στον αναγνώστη οι διαφορές ανάμεσα στα ιδιωτικά και τα δημόσια Blockchain δίκτυα, οι διαφορετικοί τύποι που μπορούμε να συναντήσουμε αλλά και τι συνδυασμοί μπορούν να υπάρξουν από αυτούς. Επίσης γίνεται ειδική αναφορά στα έξυπνα συμβόλαια

(Smart Contracts) τα οποία όλο και περισσότερο μέσω της τεχνολογίας του Blockchain εισέρχονται στην καθημερινότητα μας. Αναλύεται ο τρόπος με τον οποίο είναι εφικτό να οδηγηθούμε σε έμπιστες συναλλαγές μεταξύ αντισυμβαλλόμενων ατόμων, πως μπορούν να έχουν πεδίο εφαρμογής στο εμπόριο και στις εμπορικές χρηματοδοτήσεις αλλά και πόσο εφικτό είναι να χρησιμοποιούνται από τις κεντρικές τράπεζες σε χρηματοοικονομικές υπηρεσίες και συναλλαγές. Τέλος καταγράφονται παραδείγματα εταιρειών παγκόσμιου βεληνεκούς από διάφορους τομείς δραστηριοποίησης που χρησιμοποιούν ή προτίθενται να χρησιμοποιήσουν στο άμεσο μέλλον την τεχνολογία του Blockchain στις δραστηριότητες τους.

Το τέταρτο κεφάλαιο της διπλωματικής εργασίας έχει ως στόχο να αναλυθεί το μοντέλο των Abadi J. και Brunnermeier M. σχετικά με το Blockchain Trilemma. Σε πρώτο επίπεδο στόχος του κεφαλαίου είναι να παρουσιαστούν οι αλγόριθμοι συναίνεσης που συμμετέχουν στην ανάλυση του μοντέλου, το μαθηματικό μοντέλο και οι μεταβλητές του και τέλος ο μηχανισμός του blockchain μαζί με τα δύο βασικά συμπεράσματα που καταλήγει, δηλαδή το Mimicking Lemma και το Blockchain trilemma. Ενώ σε δεύτερο στάδιο να δοθούν πραγματικές εφαρμογές χειραγώγησης μέσω παραδειγμάτων στους αλγόριθμους συναίνεσης του μοντέλου δηλαδή στο Private blockchain, στο Proof of Stake αλγόριθμο συναίνεσης και στον Proof of Work αλγόριθμο συναίνεσης.

Ενώ τέλος ακολουθούν τα κεφάλαια με τα συμπεράσματα της διπλωματικής εργασίας και της βιβλιογραφίας που χρησιμοποιήθηκε.

ΚΕΦΑΛΑΙΟ 1: Εισαγωγή στα βασικά χαρακτηρίστηκα ενός δικτύου Blockchain

1.1 Εισαγωγή Κεφαλαίου

Το πρώτο κεφάλαιο της διπλωματικής εργασίας έχει ως στόχο να γίνει κατανοητή η εισαγωγή στα βασικά χαρακτηρίστηκα ενός οποιουδήποτε αποκεντροποιημένου καθολικού συναλλαγών Blockchain και να κατανοηθεί η χρησιμότητα του, τα πλεονεκτήματα του στην χρήση του στην καθημερινή ζωή αλλά και τα προβλήματα που βγαίνουν στην επιφάνεια.

Αναλυτικότερα το παρόν κεφάλαιο αποσκοπεί να εισάγει τον αναγνώστη στα βασικά χαρακτηρίστηκα που αφορούν αλλά και διέπουν ένα καθολικό σύστημα συναλλαγών Blockchain. Να αναλυθούν οι βασικές έννοιες που αφορούν την δομή του αρχίζοντας από το τι είναι ένα κρυπτονόμισμα και ποια η σύνδεση του με το Blockchain μέχρι το πως κάποιος μπορεί να εισέρθει σε ένα blockchain αλλά και γίνεται σε καινοτόμες εφαρμογές όπως τα έξυπνα συμβόλαια (Smart Contracts).

Επίσης παρουσιάζεται ο τρόπος που επιτυγχάνεται η διακράτηση των αρχείων συναλλαγών, πως αποφεύγονται οι πράξεις ψευδών αναφορών και πως επιτυγχάνεται η ασφάλεια σε έναν κατανεμημένο καθολικό. Τέλος γίνεται αναφορά στο κόστος επαλήθευσης συναλλαγών και χρήσης ενός blockchain σε σχέση με τους κεντροποιημένους τρόπους αλλά και αναλύεται σύμφωνα με διεθνείς μελέτες το κατά πόσο θα ήταν εφικτό να πραγματοποιούνται σε καθημερινή βάση εμπορικές πληρωμές μέσω κρυπτονομισμάτων.

1.2 Τα βασικά εισαγωγικά χαρακτηριστικά της αρχιτεκτονικής ενός Blockchain

Ως κρυπτονόμισμα (Cryptocurrency) μπορούμε να ορίσουμε ένα ψηφιακό αρχείο ιδιοκτησίας που χρησιμοποιείται για την πραγματοποίηση συναλλαγών. Για κάθε συναλλαγή ο αγοραστής δίνει οδηγίες για την μεταφορά της ιδιοκτησίας ενός συγκεκριμένου ποσού από τον λογαριασμό του σε εκείνον του πωλητή. Το blockchain

είναι ένα καθολικό συναλλαγών που καταγράφονται οι μεταφορές των κρυπτονομισμάτων με το πέρασμα του χρόνου. (Chiu J., Koeppl T. (2018).

Ένα blockchain (βλέπε εικόνα 1) είναι ένα δημόσιο καθολικό βιβλίο συλλογής και καταγραφής πληροφοριών που βρίσκεται στο διαδίκτυο, βασίζεται στην κρυπτογράφηση και αποτελεί την τεχνολογία πίσω από τα περισσότερα κρυπτονομίσματα. Η τεχνολογία blockchain δεν είναι εταιρεία, ούτε είναι μια εφαρμογή όπως ένα application αλλά αποτελεί ένα δίκτυο σαν μια βάση δεδομένων που αποθηκεύει συναλλαγές και όχι μόνο, διατηρώντας την ασφάλεια, την σταθερότητα, την επεκτασιμότητα, τον αυτοματισμό και τα χαμηλά κόστη. Είναι ένας εντελώς νέος τρόπος τεκμηρίωσης δεδομένων και συναλλαγών στο διαδίκτυο αποθηκεύοντας τα ανάλογα με την χρονική σειρά της πραγματοποίησης τους. (Olga Kharif and Matthew Leising, (2018), lisk.io, (2020))

Η τεκμηρίωση των συναλλαγών γίνεται και απαιτεί την επιβεβαίωση από πολλές συσκευές που συμμετέχουν στο δίκτυο του Blockchain καθώς μπορεί να είναι διαμοιρασμένες σε ολόκληρο τον κόσμο. Μόλις επιτευχθεί μια συμφωνία, γνωστή ως συναίνεση, μεταξύ των συσκευών οι συναλλαγές παραμένουν μέσα στο Blockchain και δεν μπορούν να αλλάξουν ή να αμφισβητηθούν χωρίς τη γνώση και την άδεια εκείνων που τις πραγματοποίησαν. Όσο περισσότερες συσκευές (κόμβοι) συμμετέχουν στο δίκτυο blockchain, το καθολικό των συναλλαγών γίνεται όλο και πιο αμετάβλητο διότι κανένα άτομο δεν μπορεί να επεξεργαστεί την εγγραφή αυτή. Το κλειδί για τη διατήρηση της λειτουργικότητας του blockchain είναι η επίτευξη της συναίνεσης. Αυτό σημαίνει ότι επιτυγχάνεται πάντοτε μια απόλυτη αλήθεια στις συναλλαγές και δεν μπορεί να ληφθεί μια απόφαση από ένα μέρος ατόμων ή μια μικρή μειοψηφία του δικτύου που τις επιβεβαιώνει. (Liquid, How to invest in blockchain (2019))

Αναλυτικότερα, το blockchain είναι μια αλυσίδα από block που περιέχει συγκεκριμένες πληροφορίες όπως μια βάση δεδομένων αλλά με έναν ασφαλή τρόπο που είναι όλες ομαδοποιημένες σε ένα δίκτυο peer-to-peer. Με άλλα λόγια, το blockchain είναι ένας συνδυασμός υπολογιστών συνδεδεμένων μεταξύ τους αντί ενός κεντρικού διακομιστή, που σημαίνει ότι ολόκληρο το δίκτυο είναι αποκεντρωμένο. (MLSDev, (2019))

Όπως αναφέρεται στο άρθρο της PwC με τίτλο “Blockchain, a functional introduction” του 2020, τόσο τα κατανεμημένα καθολικά βιβλία όσο και τα blockchains έχουν διάφορες εφαρμογές. Η πρώτη εκτεταμένη εφαρμογή μιας αλυσίδας blockchain που εμφανίστηκε ήταν το κρυπτονόμισμα Bitcoin, με την καινοτομία ότι χρησιμοποίησε έναν

συνδυασμό γνωστών κρυπτογραφικών τεχνικών για την επίλυση του προβλήματος των «διπλών δαπανών» (double spending). Αυτό το πρόβλημα της «διπλής δαπάνης» αναφέρεται στη δυσκολία πρόληψης να αποτραπεί η διπλή χρησιμοποίηση των ψηφιακών χρημάτων για συναλλαγές.

Μετά το Bitcoin, εμφανίστηκαν πολλές άλλες αλυσίδες blockchain, με στόχο την επίλυση άλλων προβλημάτων ή τη χρήση διαφορετικών εφαρμογών. Υπάρχουν πολλά διαφορετικά είδη blockchains σήμερα και μερικά λειτουργούν δημόσια, μερικά ιδιωτικά. Το πιο σημαντικό παράδειγμα blockchain είναι εκείνο του Bitcoin από το οποίο άλλα 667 κρυπτονομίσματα το χρησιμοποίησαν.

Το πιο δημοφιλές blockchain μετά το Bitcoin είναι το Ethereum, το οποίο έρχεται με το δικό του νόμισμα το Ether, το οποίο επιτρέπει την εκτέλεση λογικών ακολουθιών σε ένα κατανεμημένο δίκτυο. Άλλες οικογένειες κρυπτονομισμάτων είναι NXT και το XRP. Άλλα blockchain που δεν βασίζονται σε κατανεμημένα καθολικά βιβλία είναι το HyperLedger, το Fabric, το Corda, το BigChainDB και το Rchain τα οποία αναλύονται στην συνέχεια.

Επίσης αξιοσημείωτο είναι να αναφέρουμε πως η Βενεζουέλα ήταν η πρώτη χώρα που εξέδωσε κρυπτονόμισμα, το οποίο όμως αμφισβητήθηκε ιδιαίτερα τόσο τεχνικά όσο και σε επίπεδο διακυβέρνησης.

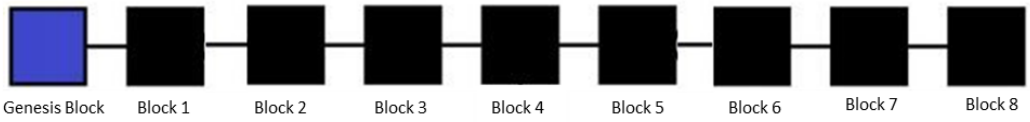
Ενώ μεταξύ άλλων κάποια από τα πλεονεκτήματα του Blockchain είναι τα ακόλουθα (Lastovetska A., (2019)):

- Η Κρυπτογράφηση (Cryptography)
- Η Αμετάβλητοτητα (Immutability)
- Η Προέλευση (Provenance)
- Η Αποκέντρωση (Decentralization)
- Η Ανωνυμία (Anonymity)
- Η Διαφάνεια (Transparency)
- Η Δυνατότητα ολοκλήρωσης συναλλαγών πολύ πιο γρήγορα και με εμπιστοσύνη
- Η Μείωση κόστους για επιχειρήσεις ή διεπιχειρησιακές διεργασίες, ενώ ταυτόχρονα απομακρύνονται οι μεσάζοντες
- Η Αναποτελεσματικότητα

- Η ψηφιακή αλληλεπίδραση
- Η διατήρηση του ελέγχου των επιχειρηματικών διαδικασιών και συναλλαγών χωρίς κεντρικό σημείο ελέγχου
- Η κατάργηση της εξαπάτησης, των επιθέσεις στον κυβερνοχώρο ή άλλου είδους ηλεκτρονικά εγκλήματα

Ένα πολύ σημαντικό στοιχείο ενός blockchain είναι τα blocks τα οποία αποτελούν τα σημεία εκείνα του δικτύου blockchain που συγκεντρώνονται, καταγράφονται και αποθηκεύονται τα δεδομένα, οι πληροφορίες και οι συναλλαγές που πραγματοποιούνται (βλέπε εικόνα 1). Ένα block συνήθως αποτελείται από μια σειρά μηνυμάτων, μια ένωση (Pointer) στο επόμενο block και μια κεφαλή (Header). Οι ενώσεις (Pointers) είναι εκείνες που περιέχουν την εντολή του μηνύματος που βρίσκεται σε κάθε block. Αυτά τα blocks είναι διατεταγμένα και συνδεδεμένα σε μια γραμμική ακολουθία μέσω της χρήσης κρυπτογραφικών τεχνικών σχηματίζοντας μια αλυσίδα χωρίς τέλος επομένως προκύπτει και ο όρος blockchain. Επειδή η αλυσίδα των συνδεδεμένων block αποθηκεύει όλα τα δεδομένα συναλλαγών που παράγονται από την εκκίνηση ενός συγκεκριμένου blockchain, στα αρχεία αυτά μπορεί να υπάρξει η πρόσβαση στις συναλλαγές και στα δεδομένα από το τελικό μέχρι το αρχικό block της αλυσίδας Blockchain. Να αναφέρουμε πως τα blocks συνήθως γίνονται αντικείμενο συζήτησης όταν συνδέονται με τις συναλλαγές κρυπτονομισμάτων, αλλά να επισημάνουμε πως δεν περιορίζονται μόνο εκεί αλλά και σε άλλου είδους ψηφιακά δεδομένα που αποθηκεύονται σε ένα σύστημα blockchain. Κάθε block στο blockchain αποτελείται από δεδομένα, από το hash του block και από το hash του προηγούμενου block. (Binance Academy, Blocks (2020), Abadi J., Brunnermeier M. (2019))

Εικόνα 1.1: Μια τυπική αλυσίδα blockchain



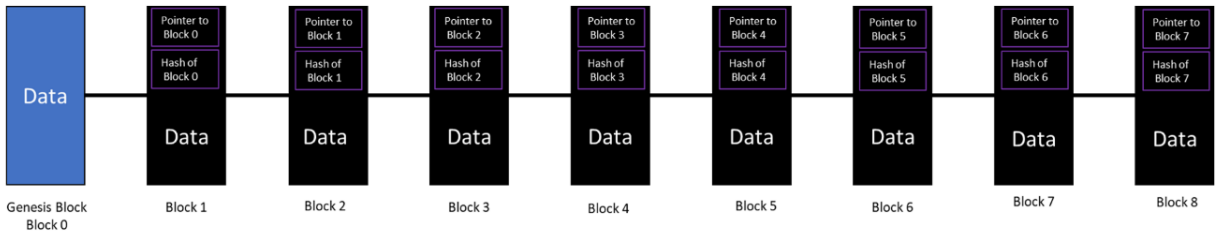
Πηγή: coinguides.org (2018), Ιδία επεξεργασία

Ένα blockchain ξεκινά από το block που ονομάζεται genesis block και σε αυτό προσαρμόζονται όλα τα επόμενα (βλέπε εικόνα 2). Αποτελεί το αρχικό block του blockchain και περιλαμβάνει μηνύματα, την ένωση με το επόμενο block (pointer) και την ψήφο. Κάθε block καταγράφει τις πραγματοποιθείσες συναλλαγές και ο κάθε κόμβος συνεργάζεται για να συνδέσει νέα blocks στο Blockchain δημιουργώντας ένα καθολικό που δεν μπορεί να αλλάξει τις προηγούμενες καταγεγραμμένες του συναλλαγές. (PwC, Marc Sel, (2020), AbadiJ., Brunnermeier M. (2019))

Όπως προαναφέραμε η δημιουργία ενός νέου block περιλαμβάνει πάντα τον κατακερματισμό (hash) με το προηγούμενο για να μπορούν να είναι κρυπτογραφικά συνδεδεμένα. Μια τέτοια δομή επιτρέπει τη δημιουργία μιας ασφαλούς βάσης δεδομένων που είναι ιδιαίτερα ανθεκτική στις παραβιάσεις και τις επιθέσεις. Ο κατακερματισμός λειτουργεί ως αναγνωριστικό στοιχείο και είναι μοναδικός για κάθε νέο block που παράγεται. Το hash αποτελεί δηλαδή μια λύση σε ένα περίπλοκο μαθηματικό πρόβλημα που το άτομο που πραγματοποιεί την εξόρυξη καλείται να επιλύσει για να μπορέσει να δημιουργήσει το επόμενο block και να επικυρώσει την συναλλαγή στα καινούργια blocks. (PwC Global FinTech Report, (2016))

Στην περίπτωση του Bitcoin η προσθήκη ενός νέου block γίνεται μέσω μιας διαδικασίας που ονομάζεται εξόρυξη. Επειδή η εξόρυξη απαιτεί σημαντικό αριθμό υπολογιστικών πόρων, τα blocks που επιτυχώς εξορύχνονται παράγουν αυτόματα νέα Bitcoins για να ανταμείψουν τα άτομα για την δουλειά που πραγματοποίησαν.

Εικόνα 1.2: Μια τυπική αλυσίδα blockchain με δεδομένα, την ένωση με το επόμενο block και τον κατακερματισμό



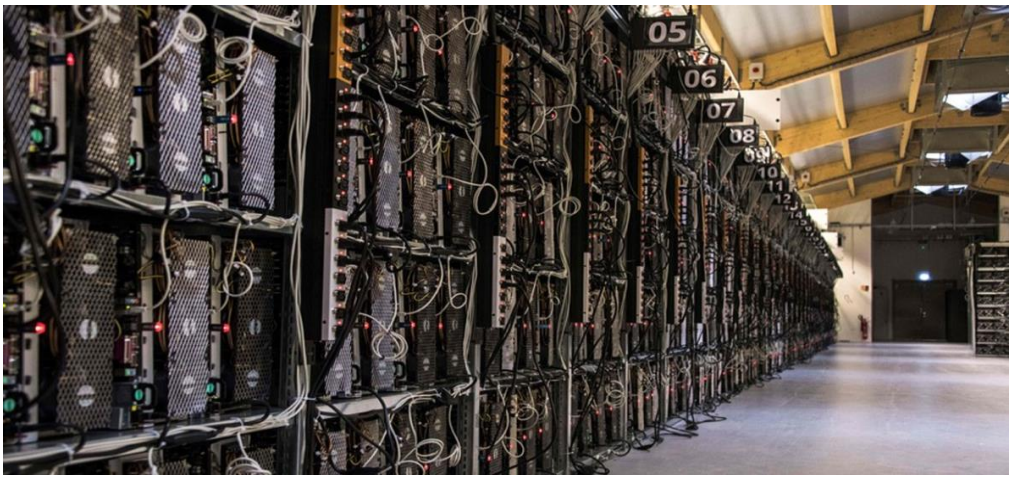
Πηγή: medium.com (2018), Ιδία επεξεργασία

Μέσα σε ένα blockchain διεξάγεται μια διαδικασία που ονομάζεται ψηφοφορία (voting) και αυτή η διαδικασία ακολουθείται από τα άτομα που συμμετέχουν σε ένα δίκτυο blockchain για να προσθέσουν ένα νέο block σε αυτό. Η ψήφος μπορεί να πραγματοποιείται τόσο ανάλογα με τα φυσικά χαρακτηριστικά του συστήματος όπως στο PoW αλγόριθμο συναίνεσης όσο και με τα ψηφιακά περιουσιακά στοιχεία όπως στο PoS αλγόριθμο συναίνεσης. Στο PoW η ψήφος είναι ένας πραγματικός αριθμός που εξαρτάται από την υπολογιστική ισχύ στο κάθε block, ενώ στο PoS και στο Private Blockchain η ψήφος συνδέεται με τους λογαριασμούς και τα διαφορετικά γνωρίσματα για την ψηφοφορία σε κάθε block. (Abadi J., Brunnermeier M. (2019))

Επίσης όταν αναφερόμαστε σε ένα blockchain πολλές φορές γίνεται η αναφορά στα Κατανεμημένα ή διαμοιρασμένα καθολικά (Distributed Ledgers), τα οποία είναι ένας τύπος βάσης δεδομένων με αρχεία συναλλαγών ή πληροφορίες που είναι κατανεμημένα μεταξύ πολλαπλών συμμετεχόντων στο δίκτυο και αποθηκεύονται το ένα μετά το άλλο σε αυτό το καθολικό ανάλογα με την χρονική στιγμή που πραγματοποιήθηκαν. (Christina Majaski, Distributed Ledgers (2019))

Ακόμη να αναφέρουμε πως τα άτομα εκείνα που είναι διασκορπισμένα στην αλυσίδα του Blockchain και κρατάνε τα αρχεία των συναλλαγών είναι οι keepers και επειδή είναι διασκορπισμένοι δικαιολογείται και ο χαρακτηρισμός του αποκεντροποιημένου δικτύου. Σε πολλά δίκτυα blockchain για να μπορέσει να γίνει η επέκταση του δικτύου χρειάζεται να πραγματοποιηθεί η διαδικασία της εξόρυξης (Mining) η οποία παρέχει επίσης και προστασία του δικτύου από χρήστες που προσπαθούν να προβούν σε «διπλές δαπάνες» (double spending) (Budish E., (2018)). Ουσιαστικά η εξόρυξη είναι η διαδικασία με την οποία κρατιέται σε συναίνεση το αρχείο των ιστορικών συναλλαγών όπως στο δίκτυο Blockchain του Bitcoin, του Ethereum, του Ripple, του R3 CEV. Όταν μέσω της διαδικασίας του Mining προστεθεί ένα νέο block στην αλυσίδα του blockchain δίνεται στον miner η αμοιβή του νέου block που είναι καθορισμένη από το δίκτυο με την μορφή κάποιων coins αλλά και κάποιων πιθανών εσόδων από τους χρήστες του δικτύου στα πλαίσια της επικύρωσης της συναλλαγή τους. (Lin William Cong, Zhiguo He (2018)). Ο πιο συνηθισμένος τρόπος εξόρυξης είναι μέσω του αλγορίθμου συναίνεσης Proof Of Work. Φυσικά εκτός από τον αλγόριθμο συναίνεσης PoW υπάρχουν και άλλες εναλλακτικές λύσεις όπως είναι ο αλγόριθμος Proof of Stake (Lastovetska A., (2019))

Εικόνα 1.3: Μια μονάδα 300MW εξόρυξης κρυπτονομισμάτων στο Τέξας των ΗΠΑ



Πηγή: theblockcrypto.com (2020)

Όπως αναφέραμε και προηγουμένως, σε ένα blockchain όταν προστίθεται ένα νέο block στην αλυσίδα υπάρχει μια αμοιβή που ονομάζεται block reward η οποία αναφέρεται στην ανταμοιβή που λαμβάνει ένα άτομο που πραγματοποιεί την εξόρυξη και επικυρώσει επιτυχώς ένα νέο block. Η ανταμοιβή του block αποτελείται από δύο συνιστώσες. Πρώτον την επιδότηση του block και δεύτερον τις αμοιβές από τις συναλλαγές. Το πρώτο κομμάτι αφορά το ποσό των κρυπτονομισμάτων που δίνεται ως αμοιβή από το δίκτυο για την εξόρυξη κάποιου καινούργιου block και το άλλο μέρος αφορά τις αμοιβές που καταβάλλονται από τους χρήστες του blockchain για να πραγματοποιήσουν σε προτεραιότητα οι miners τις συναλλαγές τους. (Caner Taçoğlu, Block Reward (2020))

Για παράδειγμα στην περίπτωση της Bitcoin, η αμοιβή εξόρυξης ενός νέου block όταν πρωτοξεκίνησε να λειτουργεί ήταν 50 BTC και μειωνόταν στο μισό κάθε 210.000 block που αντιστοιχούσε με περίπου μια φορά κάθε τέσσερα χρόνια. Το 2012 η ανταμοιβή αυτή βρισκόταν στα 25 BTC ενώ το 2016 στα 12,5 BTC για κάθε νέο block. Η επόμενη μείωση στην μισή αμοιβή αναμένεται να πραγματοποιηθεί τον Μάιο του 2020. (Bitcoinvisuals.com)

Να αναφέρουμε πως τα νεοσύστατα κρυπτονομίσματα που δημιουργούνται γίνονται από ένα ειδικό είδος συναλλαγής που ονομάζεται «coinbase transaction» και αποτελεί την πρώτη συναλλαγή που γίνεται σε κάθε νέο block που δημιουργείται και

προστίθεται στην αλυσίδα του blockchain, παράγοντας κρυπτονομίσματα από το μηδέν. (Jerome Morrow, What is a Coinbase Transaction? (2014))

Στην αρχιτεκτονική ενός blockchain πολύ σημαντικό ρόλο έχει το πρωτόκολλο του (Protocol), το οποίο αποτελεί του κύριους κανόνες λειτουργίας του. Δηλαδή καθορίζει και ορίζει τον τρόπο λειτουργίας ολόκληρου του συστήματος. (Binance Academy,What Is a Blockchain Consensus Algorithm?, (2020)). Πολλές φορές το πρωτόκολλο λειτουργίας ενός blockchain συγχέεται με τον αλγόριθμο συναίνεσης που χρησιμοποιείται αλλά είναι δύο εντελώς διαφορετικά πράγματα. Ένας αλγόριθμος συναίνεσης είναι ουσιαστικά ο τρόπος συμφωνίας για την επέκταση του κάθε νέου block στην blockchain αλυσίδα. Είναι ένας αλγόριθμος που καθορίζει τον τρόπο επίτευξης συναίνεσης στο δίκτυο των συμμετεχόντων για την επαλήθευση των συναλλαγών που πραγματοποιούνται. Ο αλγόριθμος συναίνεσης είναι συστήματα ψηφοφορίας στα οποία όταν υπάρχουν πολλές επιλογές για το επόμενο block της αλυσίδας του blockchain οι πράκτορες (agents) κοιτούν το επίπεδο ψηφοφορίας σε αυτές τις επιλογές για να συναινέσουν γι' αυτήν την επέκταση. (Abadi J., Brunnermeier M. (2019)). Το πρωτόκολλο λειτουργίας και ο αλγόριθμος συναίνεσης ενός Blockchain δικτύου αναλύεται διεξοδικά στο δεύτερο κεφάλαιο της διπλωματικής εργασίας.

Πολύ σημαντικό είναι σε αυτό το σημείο να αναφέρουμε με λίγα λόγια τους δύο πιο διαδεδομένους αλγόριθμους συναίνεσης σε δίκτυα Blockchain που είναι ο Proof of Work (PoW) και ο Proof of Stake (PoS). Σε ένα πλήρως κεντροποιημένο σύστημα καταγραφής συναλλαγών η κάθε οντότητα ψηφίζει στο καθολικό μέσω της ψηφιακής του υπογραφής. Αντιθέτως στο PoW και στο PoS η ψήφος για την επέκταση του blockchain μπορεί να γίνει ανάλογα με την υπολογιστική ισχύ του κάθε συμμετέχοντα ή τον αριθμό των token που έχει στην κατοχή του. Ο αλγόριθμος συναίνεσης PoW δίνει την δυνατότητα στα άτομα να μπορούν να ψηφίσουν την επέκταση του καθολικού δικτύου Blockchain ανάλογα με την υπολογιστική ισχύ που έχουν. Ενώ ο αλγόριθμος συναίνεσης PoS ανάλογα με τον αριθμό tokens που έχει κάθε λογαριασμός στην κατοχή του. (Abadi J., Brunnermeier M. (2019)).

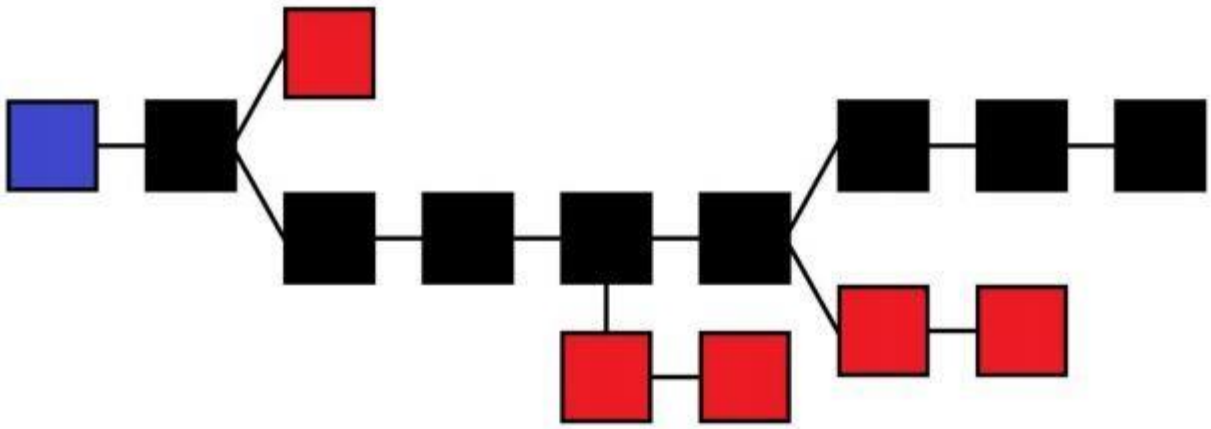
Σε ένα Blockchain που χρησιμοποιείται ο αλγόριθμος συναίνεσης PoW μπορεί να υπάρξει «Η επίθεση 51%» η οποία αναφέρεται στην ικανότητα ενός χρήστη να ελέγχει περισσότερο από το 50% των κόμβων του δικτύου και να μπορεί να αναθεωρήσει το ιστορικό των πεπερασμένων συναλλαγών και να επιδοθεί σε πράξεις όπως οι «διπλές

δαπάνες» (double spending). (Το ζήτημα των διπλών δαπανών αναλύεται στο δεύτερο κεφάλαιο της διπλωματικής εργασίας)

Σε ένα blockchain πολλές φορές υπάρχει η αναφορά στον όρο ορφανό block (Orphan Block). Ο όρος αυτός αναφέρεται σε έγκυρα block που έχουν εξορυχθεί αλλά απορρίπτονται για την επέκταση του δικτύου. Ένα ορφανό block παράγεται όταν δύο διαφορετικά άτομα που πραγματοποιούν την διαδικασία της εξόρυξης αναμεταδίδουν ταυτόχρονα τα επαληθεύσιμα και έγκυρα blocks τους. Αυτό αναγκάζει το δίκτυο του blockchain να χωριστεί σε δύο ανταγωνιστικές εκδοχές μέχρι να απορριφθεί ένα από τα block και να μείνει μόνο ένα προσαρτημένο στην κύρια αλυσίδα του blockchain. (John Ma, (2020), Orphan Block)

Από τεχνική άποψη, αυτά τα block θα πρέπει να ονομάζονται "Stale blocks" ή "Extinct blocks". Η δημιουργία "Stale blocks" είναι απολύτως φυσική και στις περισσότερες περιπτώσεις συμβαίνει τυχαία. Παρόλα αυτά, να αναφέρουμε πως μπορεί επίσης να παραχθούν ταυτόχρονα blocks όταν κακόβουλα άτομα προσπαθούν να δημιουργήσουν μια εναλλακτική έγκυρη αλυσίδα για να κατευθύνουν και να χειραγωγήσουν το δίκτυο του blockchain. (Simon Chandler, (2020))

Εικόνα 1.4: Τα Ορφανά blocks σε μια Blockchain αλυσίδα



Πηγή: firstpost.com (2019)

Παρατηρώντας την εικόνα 1.4 γίνεται κατανοητό πως τα ορφανά blocks (blocks με κόκκινο χρώμα) είναι εκείνα που βρίσκονται εκτός της βασικής αλυσίδας του blockchain (blocks με μαύρο χρώμα).

Στο περιεχόμενο ενός blockchain και γενικότερα των κρυπτονομισμάτων, ένας κόμβος (node) είναι ο κάθε υπολογιστής δηλαδή η κάθε συσκευή που χρησιμοποιείται στο δίκτυο αυτό από έναν χρήστη. Έτσι για παράδειγμα το δίκτυο του Bitcoin αποτελείται από χιλιάδες κόμβους υπολογιστών που βρίσκονται διαμοιρασμένοι σε όλο τον κόσμο και αυτό προσδίδει στο Bitcoin την ιδιότητα του διαμοιρασμένου συστήματος δηλαδή το peer-to-peer. (Binance Academy, Node (2020))

Κάθε κόμβος αποτελεί ένα σημείο επικοινωνίας στο δίκτυο του blockchain και είναι ένα σημείο όπου ένα μήνυμα μπορεί να δημιουργηθεί, να ληφθεί ή να μεταδοθεί. Όλοι οι πλήρεις κόμβοι είναι ισοδύναμοι από άποψη λειτουργικότητας και συνδέονται σε δίκτυο peer-to-peer. Για τον λόγο αυτό δεν υπάρχει ιεραρχία μεταξύ των κόμβων και όλοι οι κόμβοι μπορούν να επικοινωνούν μεταξύ τους. (PwC, Marc Sel, (2020))

Ο ορισμός ενός κόμβου μπορεί να διαφέρει σημαντικά ανάλογα με το πλαίσιο που χρησιμοποιείται. Όταν πρόκειται για δίκτυα υπολογιστών ή τηλεπικοινωνιών, οι κόμβοι μπορούν να προσφέρουν διαφορετικούς σκοπούς, ενεργώντας είτε ως σημείο ανακατανομής είτε ως τελικό σημείο επικοινωνίας. Συνήθως, ένας κόμβος αποτελείται από μια φυσική συσκευή δικτύου, αλλά υπάρχουν ορισμένες συγκεκριμένες περιπτώσεις όπου χρησιμοποιούνται εικονικοί κόμβοι. (Binance Academy, What are Nodes (2020))

Σε ένα δίκτυο blockchain σύμφωνα με το Binance Academy υπάρχουν διαφορετικοί τύποι κόμβων και κάθε τύπος είναι υπεύθυνος για την εκτέλεση διαφορετικού συνόλου λειτουργιών. Λαμβάνοντας το Bitcoin ως παράδειγμα, οι κόμβοι του δικτύου του μπορούν να χωριστούν σε τέσσερις κύριες κατηγορίες:

- Πλήρεις κόμβοι (full nodes),
- Κόμβοι ακρόασης (listening nodes)- (supernodes),
- Κόμβοι εξόρυξης (miner’s nodes) και
- Ελαφριού βάρους ή SPV πελάτες (lightweight or SPV clients)

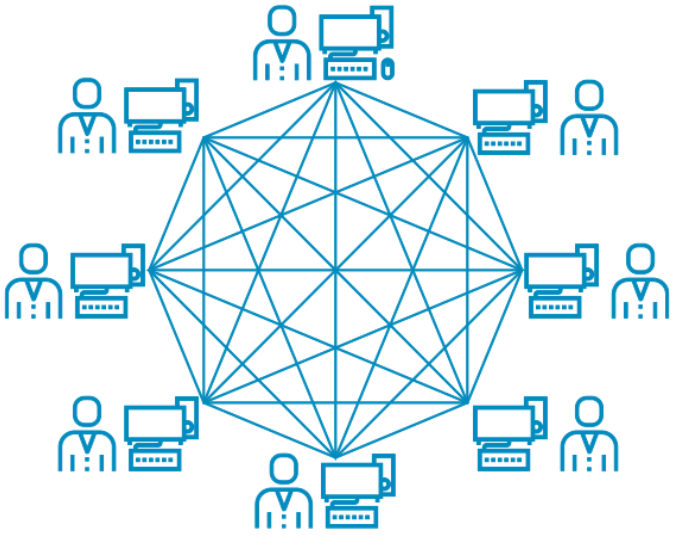
Οι πλήρεις κόμβοι (full nodes) είναι αυτοί που πραγματικά υποστηρίζουν και ασφαλίζουν το blockchain του Bitcoin και είναι απαραίτητοι για το δίκτυο. Οι πλήρεις κόμβοι (ή πλήρως επικυρωμένοι κόμβοι) είναι υπεύθυνοι για την επαλήθευση των συναλλαγών και των blocks σύμφωνα με τους κανόνες του πρωτοκόλλου λειτουργίας του Bitcoin. Και δεδομένου ότι το δίκτυο είναι διαμοιρασμένο, οι κανόνες επιβάλλονται από τον αλγόριθμο συναίνεσης του Bitcoin.

Οι λεγόμενοι κόμβοι ακρόασης (listening nodes)- (supernodes), είναι οι πλήρεις κόμβοι που καθίστανται δημόσιοι και ορατά προσβάσιμοι. Ως εκ τούτου, μπορούν να επικοινωνούν με οποιονδήποτε άλλο κόμβο που δημιουργεί μια σύνδεση μαζί τους. Έτσι, κάθε πλήρως επικυρωμένος κόμβος που δεν είναι κρυμμένος μπορεί να θεωρηθεί ως κόμβος ακρόασης. Αυτός ο τύπος κόμβου είναι υπεύθυνος για την παροχή δεδομένων του blockchain σε άλλους κόμβους, αλλά μπορεί επίσης να λειτουργήσει ως γέφυρα επικοινωνίας.

Οι κόμβοι εξόρυξης (miner's nodes) του Bitcoin είναι αυτοί που εκτελούν εξειδικευμένο λογισμικό εξόρυξης, μαζί με hardware λογισμικό ASIC (στις περισσότερες περιπτώσεις). Τα άτομα αυτά επενδύουν πολλούς πόρους και ελπίζουν να κερδίσουν την ανταμοιβή της εξόρυξης του Bitcoin.

Τέλος οι ελαφριού βάρους ή SPV πελάτες (lightweight or SPV clients) είναι αυτοί που χρησιμοποιούν το blockchain του Bitcoin αλλά δεν λειτουργούν με τον ρόλο της επικύρωσης. Συλλέγουν απλά πληροφορίες από τους κόμβους ακρόασης ενεργώντας ως τελικό σημείο επικοινωνίας. Ως εκ τούτου, αυτοί οι κόμβοι δεν διατηρούν ένα αντίγραφο του blockchain και δεν συμβάλλουν στην ασφάλεια του δικτύου.

Εικόνα 1.5: Οι κόμβοι ενός Blockchain και η μεταξύ τους σύνδεση



Πηγή: medium.com (2019)

Στην επιστήμη των υπολογιστών, ένα ομότιμο δίκτυο peer-to-peer (P2P) αποτελείται από μια ομάδα συσκευών που συλλογικά αποθηκεύουν και μοιράζονται

αρχεία. Κάθε άτομο που συμμετέχει με την συσκευή του δηλαδή τον κόμβο του (Node) στο δίκτυο ενεργεί ως μεμονωμένος ομότιμος (peer). Τυπικά, όλοι οι κόμβοι έχουν την ίδια ισχύ και εκτελούν τις ίδιες εργασίες. Μια πλατφόρμα P2P επιτρέπει για παράδειγμα στους αγοραστές και τους πωλητές να εκτελούν συναλλαγές χωρίς να χρειάζονται τρίτα άτομα στο να τις επιβεβαιώσουν δηλαδή γίνονται οι μεσάζοντες σε αυτές.(Binance Academy, Peer-to-Peer Networks Explained (2020))

Συνήθως, δεν υπάρχει κεντρικός διαχειριστής ή διακομιστής επειδή κάθε κόμβος διατηρεί ένα αντίγραφο των αρχείων ενεργώντας τόσο ως «πελάτης» όσο και ως διακομιστής σε άλλους τους κόμβους του δικτύου. Έτσι στον κάθε κόμβο μπορούν να κατέβουν αρχεία από άλλους συνδεδεμένους κόμβους ή να μεταδοθούν αρχεία σε αυτούς. Αυτό το γεγονός διαφοροποιεί τα δίκτυα P2P από τα πιο παραδοσιακά συστήματα σύνδεσης με έναν διακομιστή στα οποία οι συσκευές δηλαδή τα άτομα κατεβάζουν αρχεία από έναν κεντρικό διακομιστή (PwC, Marc Sel, (2020)).

Αναλυτικότερα σε δίκτυα P2P, οι συνδεδεμένες συσκευές μοιράζονται αρχεία που είναι αποθηκευμένα στους σκληρούς δίσκους τους και μόλις ένας χρήστης κατεβάσει ένα δεδομένο αρχείο, τότε μπορεί να λειτουργήσει ως πηγή αυτού του αρχείου. Στην πράξη όμως και οι δύο λειτουργίες αυτές μπορούν να εκτελεστούν ταυτόχρονα από κάποιον συμμετέχοντα δηλαδή να γίνει τόσο η λήψη του αρχείου όσο και η φόρτωση ενός άλλου αρχείου σε ολόκληρο το δίκτυο. (Jim Chappelow, Peer-to-Peer (P2P) Service (2019))

Η αρχιτεκτονική P2P μπορεί να είναι κατάλληλη για διάφορες χρήσεις, αλλά έγινε ιδιαίτερα δημοφιλής στη δεκαετία του 1990 όταν δημιουργήθηκαν τα πρώτα προγράμματα κοινής χρήσης αρχείων. Σήμερα, τα δίκτυα P2P βρίσκονται στον πυρήνα των περισσότερων κρυπτονομισμάτων αποτελώντας ένα μεγάλο κομμάτι της βιομηχανίας του blockchain. Δεδομένου ότι κάθε κόμβος αποθηκεύει, μεταδίδει και λαμβάνει αρχεία, τα δίκτυα P2P τείνουν να είναι ταχύτερα και πιο αποδοτικά καθώς η βάση των ατόμων του συμμετέχουν σε αυτό το είδος διαμοιρασμού συνεχώς μεγαλώνει. Επίσης, η κατανεμημένη αρχιτεκτονική τους καθιστά τα συστήματα P2P πολύ ανθεκτικά στις διαδικτυακές επιθέσεις (cyberattacks).

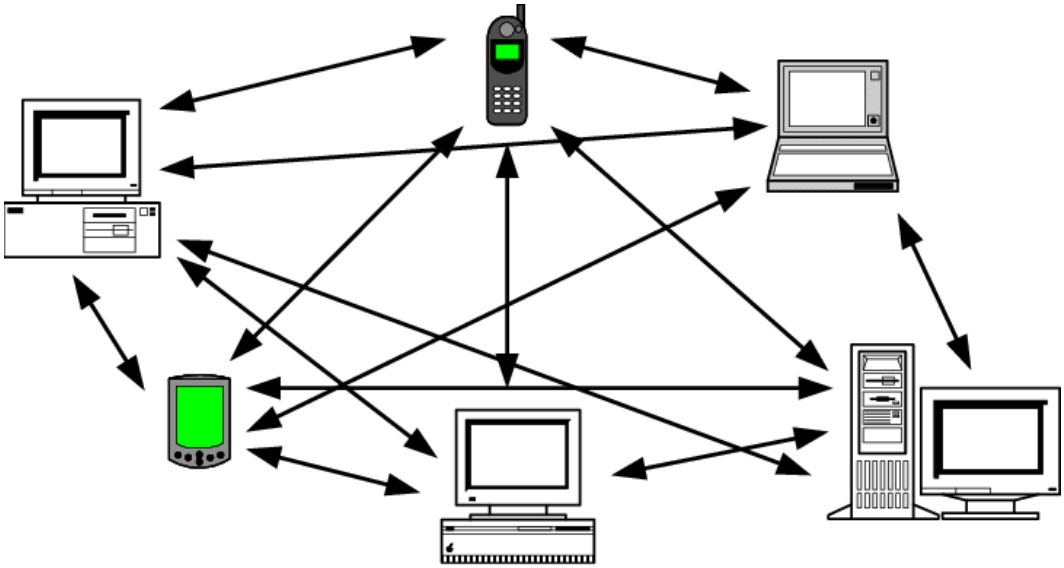
Παρακάτω σύμφωνα με το Binance Academy ακολουθεί η ανάλυση της κατηγοριοποίησης των peer-to-peer συστημάτων ανάλογα με την αρχιτεκτονική τους. Οι τρεις κύριοι τύποι ονομάζονται μη δομημένα δίκτυα P2P (unstructured), δομημένα δίκτυα P2P (structured) και υβριδικά δίκτυα P2P (Hybrid P2P networks).

Τα μη δομημένα δίκτυα P2P (Unstructured P2P networks) δεν παρουσιάζουν καμία συγκεκριμένη οργάνωση των κόμβων. Οι συμμετέχοντες επικοινωνούν τυχαία μεταξύ τους και αυτά τα συστήματα θεωρούνται ισχυρά όταν υπάρχει υψηλή δραστηριότητα και αρκετοί κόμβοι εισέρχονται και φεύγουν από το δίκτυο. Παρόλο που είναι ευκολότερο να δημιουργηθούν τα μη δομημένα δίκτυα P2P ενδεχομένως να απαιτούν υψηλότερη χρήση CPU και μνήμης του υπολογιστή καθώς τα ερωτήματα αναζήτησης αποστέλλονται στον μεγαλύτερο δυνατό αριθμό συμμετεχόντων.

Αντίθετα, τα δομημένα δίκτυα P2P(Structured P2P networks) παρουσιάζουν μια οργανωμένη αρχιτεκτονική, επιτρέποντας στους κόμβους να αναζητούν αποτελεσματικά αρχεία, ακόμη και αν το περιεχόμενο δεν είναι σε μεγάλο βαθμό διαθέσιμο. Στις περισσότερες περιπτώσεις, αυτό επιτυγχάνεται μέσω της χρήσης λειτουργιών κατακερματισμού που διευκολύνουν τις αναζητήσεις σε βάσεις δεδομένων. Ενώ τα δομημένα δίκτυα μπορεί να είναι πιο αποδοτικά, τείνουν να παρουσιάζουν υψηλότερα επίπεδα συγκέντρωσης και συνήθως απαιτούν υψηλότερο κόστος εγκατάστασης και συντήρησης.

Τέλος τα υβριδικά δίκτυα P2P (Hybrid P2P networks) συνδυάζουν το συμβατικό μοντέλο μεταξύ ενός συμβαλλόμενου και ενός διακομιστή με ορισμένες πτυχές της αρχιτεκτονικής peer-to-peer. Για παράδειγμα, μπορεί να σχεδιαστεί ένας κεντρικός διακομιστής που να διευκολύνει τη σύνδεση μεταξύ των συμμετεχόντων στο P2P δίκτυο. Σε σύγκριση με τους άλλους δύο τύπους, τα υβριδικά μοντέλα τείνουν να παρουσιάζουν βελτιωμένη συνολική απόδοση. Συνδυάζουν συνήθως μερικά από τα βασικά πλεονεκτήματα των παραπάνω επιτυγχάνοντας ταυτόχρονα σημαντικούς βαθμούς αποτελεσματικότητας και αποκέντρωσης.

Εικόνα 1.6: Ένα peer-to-peer (P2P) δίκτυο



Πηγή: researchgate.net (2003)

Όπως παρατηρούμε στην εικόνα 1.6 φαίνεται η σύνδεση διάφορων συσκευών που υπάρχει μεταξύ των ομότιμων κόμβων ενός peer-to-peer δικτύου. Όλοι οι κόμβοι είναι ισότιμοι μεταξύ τους, έχουν την ίδια ισχύ και μοιράζονται τις ίδιες πληροφορίες.

Γεγονός είναι πως κάθε πρωτόκολλο blockchain λόγω της ψηφιακής του μορφής, χρειάζεται ένα ψηφιακό περιουσιακό στοιχείο για να κρατήσει το δίκτυο σε λειτουργία. Αυτό το ψηφιακό στοιχείο είναι τα Coins ή tokens τα οποία χρησιμοποιούνται και ως χρηματικά κίνητρα για τους συμμετέχοντες στο δίκτυο.

Οι δύο αυτοί όροι χρησιμοποιούνται πολλές φορές ως ισοδύναμοι στον χώρο του blockchain καθώς και τα δύο χρησιμοποιούνται για να τροφοδοτούν ένα δίκτυο Blockchain αλλά υπάρχει μια λεπτή διαφορά μεταξύ τους. Η μόνη τους διαφοροποίηση είναι στο επίπεδο του πρωτοκόλλου που καθορίζονται. (Harsh Agrawal, Coins vs Tokens: Know The Difference, (2019))

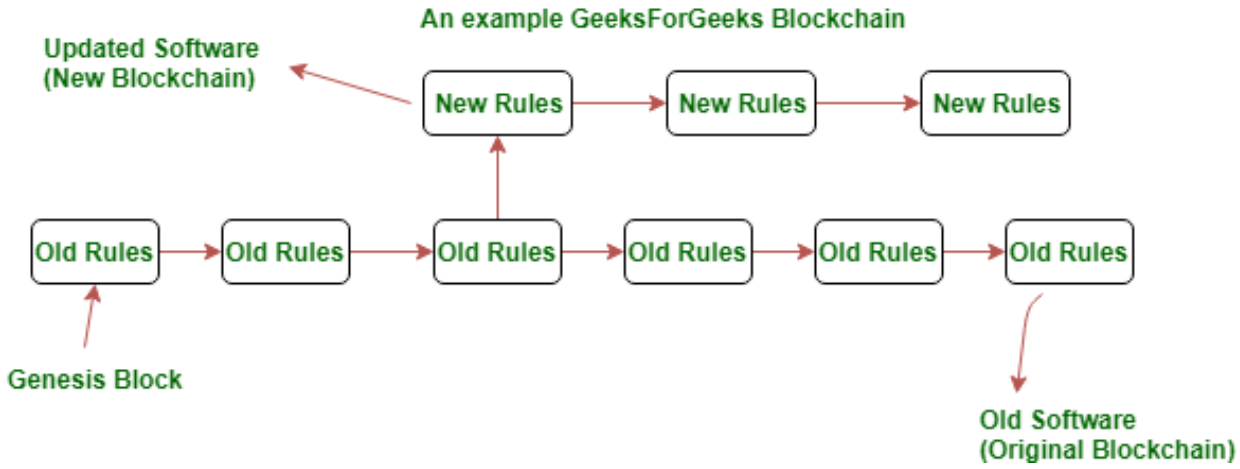
Τα μεν coins ορίζονται στο χαμηλότερο επίπεδο από το ίδιο το πρωτόκολλο και είναι εγγενώς ψηφιακό περιουσιακό στοιχείο ενός δικτύου blockchain. Για παράδειγμα το φυσικό νόμισμα του πρωτοκόλλου του Bitcoin είναι το coin «Bitcoin». Τα δε tokens είναι ψηφιακά στοιχεία που ορίζονται σε υψηλότερο επίπεδο και όχι από το πρωτόκολλο αλλά

από τις εφαρμογές του σε αυτό όπως από τα smart contracts. Για παράδειγμα το πρωτόκολλο του Ethereum έχει ως φυσικό νόμισμα το coin «Ether», αλλά το Ethereum επιτρέπει στους προγραμματιστές να δημιουργήσουν, μεταξύ άλλων και τα dApps στο πρωτόκολλό του. Οι κανόνες επικοινωνίας μεταξύ των κόμβων για ένα dApp μπορούν να διαφέρουν από τους εκείνους ενός άλλου dApp που ορίζονται από τα smart contracts. Για τον λόγο αυτό τα tokens αποτελούν το εγγενές ψηφιακό στοιχείο των dApps. (Genesis DevCon, What are Blockchain Protocols and How Do they Work? (2018))

Σε ένα blockchain πολλές φορές μπορεί να υπάρξει ο διαχωρισμός της αλυσίδας του δηλαδή να γίνει ένα Blockchain Fork. Το Fork αποτελεί μια πράξη ανανέωσης και επέκτασης του λογισμικού blockchain που οδηγεί στον διαχωρισμό ενός blockchain σε δύο ή περισσότερες έγκυρες blockchains αλυσίδες, οι οποίες έχουν κοινό genesis block. (Parikshit Hooda, Important Blockchain terminologies, (2020), Abadi J., Brunnermeier M. (2019))

Ο αποκεντρωμένος χαρακτήρας των δημόσιων blockchains όπως είναι για παράδειγμα του Bitcoin και του Ethereum σημαίνει ότι οι συμμετέχοντες στο δίκτυο πρέπει να μπορούν να καταλήξουν σε συμφωνία ως προς την κοινή κατάσταση του blockchain δηλαδή ως προς το κοινό δημόσιο καθολικό και το πρωτόκολλο του blockchain. Η ομόφωνη συναίνεση μεταξύ των κόμβων του δικτύου έχει ως αποτέλεσμα ένα ενιαίο blockchain που περιέχει επαληθευμένα δεδομένα, όπως τις συναλλαγές που το δίκτυο βεβαιώνει ότι είναι σωστά. Ωστόσο, πολλές φορές, οι κόμβοι του δικτύου δεν μπορούν να έρθουν με ομόφωνη συναίνεση όσον αφορά τη μελλοντική κατάσταση που αφορά το blockchain. Αυτό το γεγονός οδηγεί σε Forks που σημαίνει ότι η αλυσίδα του Blockchain χωρίζεται σε δύο ή περισσότερες αλυσίδες που είναι όλες έγκυρες. (Parikshit Hooda, Blockchain Forks)

Εικόνα 1.7: Ο διαχωρισμός (fork) μιας blockchain αλυσίδας



Πηγή: geeksforgeeks.org (2020)

Ένα Fork μπορεί να εμφανιστεί σε μια blockchain αλυσίδα για την προσθήκη νέων λειτουργιών στο blockchain, για βελτιώσεις, για νέες εκδόσεις, για την επίλυση ζητημάτων ασφαλείας που προκύπτουν σε σχέση με το πρωταρχικό πρωτόκολλο του καθώς και σε άλλες περιπτώσεις. Ένα Fork του blockchain μπορεί να λάβει τρεις διαφορετικούς τύπους και να είναι Soft Fork, Hard Fork και Temporary Fork / Accidental Fork (Προσωρινό ή τυχαίο Fork).

Το Soft Fork συμβαίνει όταν το πρωτόκολλο του blockchain τροποποιηθεί ανάποδα αλλά με συμβατό τρόπο. Δηλαδή υπάρχει αλλαγή στο λογισμικό που εκτελείται στους κόμβους και τα νέα block εξορύσσονται με βάση νέους κανόνες. Για παράδειγμα η ενημερωμένη έκδοση SegWit του δικτύου Bitcoin πρόσθεσε μια νέα κατηγορία διευθύνσεων (Bech32). Ωστόσο, αυτό δεν ακυρώνει τις υπάρχουσες διευθύνσεις P2SH. Ένας πλήρης κόμβος με διεύθυνση τύπου P2SH θα μπορούσε να κάνει μια έγκυρη συναλλαγή με έναν κόμβο της διεύθυνσης τύπου Bech32.

Το Hard Fork συμβαίνει όταν το πρωτόκολλο blockchain έχει αλλάξει με τρόπο που δεν είναι συμβατός προς τα προηγούμενα Blocks και τα νέα Blocks εξορύσσονται βάσει νέων κανόνων. Όταν εμφανίζονται Hard Forks δημιουργείται νέο κρυπτονόμισμα, χωρίς να καταργείται το αρχικό και ισοδύναμη ποσότητα νομίσματος διανέμεται στους πλήρεις κόμβους οι οποίοι επιλέγουν να αναβαθμίσουν το λογισμικό τους.

Παράδειγμα Hard Fork είναι στην περίπτωση του Ethereum όταν το Blockchain του χωρίστηκε σε Ethereum και Ethereum Classic, στου Bitcoin όταν χωρίστηκε σε Bitcoin και Bitcoin Cash αλλά και όταν η blockchain αλυσίδα του Ethereum στην οποία το πρωτόκολλο συναίνεσης από Proof of Work (PoW) θα αλλάξει σε Proof of Stake (PoS) μέσω του λογισμικού Casper.

Επίσης η τρίτη κατηγορία είναι το Temporary Fork / Accidental Fork (Προσωρινό ή τυχαίο Fork) είναι όταν δύο άτομα πραγματοποιούν την εξόρυξη του νέου block την ίδια χρονική στιγμή και δεν είναι ξεκάθαρο ποιο από τα δύο προηγείται χρονικά του άλλου. Τα δύο blocks έχουν το ίδιο ύψος και ολόκληρο το δίκτυο μπορεί να μην συμφωνήσει αμέσως στην επιλογή του νέου block.

Τέλος να αναφέρουμε πως όταν για το Fork σε ένα blockchain έχουμε μια κατάσταση με δύο αντιμαχόμενες καθολικές αλυσίδες blocks δηλαδή έχουμε δύο διαφορετικά καθολικά που θέλουν να αποτελέσουν την διακλάδωση του αρχικού blockchain τότε έχουμε την κατάσταση των αντιμαχόμενών blocks (conflicting blocks). (Abadi J., Brunnermeier M. (2019))

Επειδή τα περισσότερα κρυπτονομίσματα βασίζονται στην τεχνολογία blockchain και γεγονός είναι πως η επένδυση σε ένα blockchain δεν γίνεται άμεσα σε αυτό αλλά μέσω των κρυπτονομισμάτων που χρησιμοποιούν την τεχνολογία αυτή. Άρα η επένδυση σε ένα κρυπτονομίσματα συνεπάγεται με την επένδυση στο blockchain που χρησιμοποιεί, αποκτώντας ουσιαστικά μέρος του. Πως όμως γίνεται αυτή η επένδυση στα κρυπτονομίσματα; Η διαδικασία είναι απλή. Το μόνο που χρειάζεστε είναι μια ανταλλαγή σε ένα ανταλλακτήριο κρυπτονομισμάτων που υποστηρίζει fiat νομίσματα όπως είναι το δολάριο (USD), το ευρώ (EUR), το γιέν (JPY) κλπ. Μπορείτε να καταθέσετε το fiat νόμισμα με τραπεζική μεταφορά ή χρησιμοποιώντας την πιστωτική ή χρεωστική σας κάρτα στον λογαριασμό του ανταλλακτηρίου και να ζητήσετε το κρυπτονόμισμα της επιλογής σας. Τα κρυπτονομίσματα που αποκτάτε τα αποθηκεύετε σε ένα ψηφιακό πορτοφόλι που λειτουργεί όπως ένας λογαριασμός τραπέζης. (Liquid, How to invest in blockchain (2019))

Τέλος μια καινοτόμα εφαρμογή που προσφέρεται σε πολλά blockchains ανάλογα με το πρωτόκολλο λειτουργίας τους είναι τα Έξυπνα συμβόλαια (Smart Contracts). Τα έξυνα συμβόλαια είναι ένα σύνολο λογικών κανόνων υπό μορφή κωδικοποίησης που μπορούν να ενσωματωθούν στο blockchain με την μορφή εφαρμογών (applications) για να καθορίσουν μια συναλλαγή. Είναι ουσιαστικά ένα πρωτόκολλο ηλεκτρονικών

υπολογιστών που συμφωνεί ψηφιακά, ελέγχει ή επιβάλλει κάποιους διαπραγματευτικούς κανόνες που έχουν συμφωνηθεί μεταξύ κάποιων ατόμων χωρίς να υπάρχει κάποια κεντρική αρχή ή τρίτο άτομο για τον έλεγχο αυτό. (Genesis DevCon, What are Blockchain Protocols and How Do they Work? (2018))

Οι συναλλαγές αυτές καταγράφονται στο blockchain και είναι μη αναστρέψιμες. Για παράδειγμα, ας υποθέσουμε πως έχουμε ένα έξυπνο συμβόλαιο μεταξύ δύο συμβαλλόμενων μερών, της Παίχτριας 1 και του Παίχτη 2, σχετικά με την τιμή των μετοχών που είναι εισηγμένες στο χρηματιστήριο. Η υποθετική μας σύμβαση ορίζει ότι η Παίχτριας 1 μια συγκεκριμένη ημερομηνία στο μέλλον πληρώνει ένα συγκεκριμένο ποσό από τον Παίχτη 2 εάν ας πούμε η τιμή της μετοχής γίνει μεγαλύτερη ή ίση των 100 ευρώ, διαφορετικά, ο Παίχτης 2 πληρώνει στην Παίχτρια 1 το ίδιο ποσό. Αυτό το απλό είδους συμβολαίου μπορεί να γίνει μέσω ενός έξυπνου συμβολαίου σε μια γλώσσα προγραμματισμού όπως η Solidity η οποία στη συνέχεια μπορεί να ενεργοποιηθεί σε ένα blockchain. Όταν στο παράδειγμα μας έρθει η καθορισμένη στο μέλλον χρονική στιγμή, τότε το έξυπνο συμβόλαιο θα πραγματοποιήσει την πληρωμή σύμφωνα με τους αρχικούς όρους του συμβολαίου.

Ουσιαστικά τα έξυπνα συμβόλαια καθορίζουν τους κανόνες και τις συνέπειες με τον ίδιο τρόπο όπως τα παραδοσιακά νομικά έγγραφα. Λαμβάνουν πληροφορίες ως εισροές και εκτελούν συγκεκριμένες ενέργειες ως αποτελέσματα. Περιέχουν επίσης ένα συνδυασμό δεδομένων και κώδικα. Οι συμβάσεις αυτές δημιουργούνται από μια λειτουργία που ονομάζεται constactor κατά την εκτέλεση του συμβολαίου από τον κατασκευαστή του και την ώρα που εισάγεται στο blockchain στην διεύθυνση εκείνη που το συμβόλαιο εκτελείται. Η εκτέλεση του συμβολαίου χρειάζεται τυπικά την ύπαρξη ενός κρυπτονομίσματος. Σήμερα, η πιο δημοφιλής εφαρμογή έξυπνων συμβολαίων είναι πιθανώς η πλατφόρμα Ethereum, η οποία είναι δημόσια και δεν απαιτείται άδεια πρόσβασης.

1.3 Η αρχή του πρώτου Blockchain

Η μελέτη πάνω στην κρυπτογραφική ασφάλεια της αλυσίδας των blocks χρονολογείται από το 1991 από τους S.Haber και W. Scot Stoenetta. Μέχρι το 2008 έμεινε αναξιοποίητη όταν το πρώτο blockchain ήρθε στο φως της δημοσιότητας από τον εμπνευστή του Satoshi Nakamoto και εφαρμόστηκε και διαδόθηκε δια μέσου του κρυπτονομίσματος Bitcoin. (Lin William Cong, Zhiguo He (2018)

Σύμφωνα με τους Catalini C., Gans J. (2016), τον Οκτώβριο του 2008 λίγες εβδομάδες μετά την έκτακτη οικονομική σταθεροποίηση της Αμερικής και του χρηματοπιστωτικού της συστήματος από την κατάρρευση, ο Satoshi Nakamoto παρουσίασε το peer-to-peer ηλεκτρονικό σύστημα πληρωμών του Bitcoin το οποίο βασιζόμενο στην εμπιστοσύνη μεταξύ δυο συμβαλλόμενων μερών επέτρεπε την απευθείας συναλλαγή τους χωρίς την ενδιάμεση παρέμβαση ενός τρίτου έμπιστου συμβαλλόμενου. Με αυτόν τον τρόπο μέσω του Bitcoin το Internet ήταν έτοιμο να βιώσει τα αποτελέσματα της δραστικής μείωσης σε δύο συνδεδεμένα κόστη. (Nakamoto S., 2008). Στο κόστος της επιβεβαίωσης της συναλλαγής και στο κόστος χρησιμοποίησης του δικτύου. Για πρώτη φορά στην ιστορία θα συναντούσαμε την μεταφορά ενός περιουσιακού στοιχείου με αξία μεταξύ δύο απομακρυσμένων ατόμων που μπορεί και να μην γνωρίζονται μεταξύ τους για να διέπεται από εμπιστοσύνη η συναλλαγή, χωρίς την διαμεσολάβηση ενός ενδιάμεσου που θα παίρνει κάποια προμήθεια (Diamond D., (1996)).

Το bitcoin αποτελεί το πρώτο παράδειγμα της κλιμακωτής μείωσης του κόστους συναλλαγών, για το πως ένα ανοιχτής επικοινωνίας πρωτόκολλο μπορεί να χρησιμοποιηθεί για να εφαρμοστεί σε έναν χώρο συναλλαγών χωρίς την διαμεσολάβηση κάποιας κεντρικής αρχής αλλά και του πρώτου παραδείγματος για το πως ένα ασφαλές δίκτυο μπορεί να υπάρξει χωρίς επενδύσεις αλλά παρά μόνο βασιζόμενο στα ατομικά κίνητρα του κάθε συμβαλλόμενου σε αυτό. ο blockchain που χρησιμοποιεί δίνει την δυνατότητα της αποθήκευσης εγγραφών δια μέσου ενός κατανεμημένου δικτύου, με το να μετατρέπεται το κρυπτονόμισμα σε πιο ευέλικτο και εύχρηστο για την ανάπτυξη νέων εφαρμογών στην πλατφόρμα του δικτύου.

Ακόμα και σήμερα το bitcoin αποτελεί το πιο διαδεδομένο και ασφαλές κρυπτονόμισμα αλλά και ένα τρανταχτό παράδειγμα για το πως το κόστος επιβεβαίωσης

των συναλλαγών και της χρήσης του δικτύου μειώθηκαν δραματικά και νέοι τύποι συναλλαγών, ενδιάμεσων αλλά και επιχειρηματικών μοντέλων έγιναν διαθέσιμα.

Ας μην ξεχνάμε πως το κόστος της χρήσης ενός κεντροποιημένου δικτύου έπεσε πάρα πολύ με την χρήση του ίντερνετ, ενώ το κόστος χρήση ενός αποκεντροποιημένου δικτύου ήταν ιδιαίτερα υψηλό πριν την χρήση του blockchain.

1.4 Τι είναι όμως η τεχνολογία blockchain;

Όπως αναφέρουν οι Abadi J., Brunnermeier M. στο άρθρο τους με τίτλος «Blockchain Economics» (2019), τα παραδοσιακά κεντροποιημένα συστήματα καταγραφής συναλλαγών βασίζονται στην κοινή συναίνεση των μερών για την εμπιστοσύνη στην φύλαξη των αρχείων. Η εμπιστοσύνη αυτή διεγείρεται από τα κατάλληλα κίνητρα στο να παραμένουν διαφανείς οι συναλλαγές. Ας μην ξεχνάμε επίσης πως σε ένα κεντροποιημένο δίκτυο η διακράτηση των αρχείων των συναλλαγών επιφέρει επιπλέον κόστος. Στο αποκεντροποιημένο σύστημα συναλλαγών η δημιουργία του Blockchain προώθησε έναν διαφορετικό τρόπο της διατήρησης του αρχείου των συναλλαγών και της καταγραφής των πληροφοριών στις οποίες δεν χρειάζεται να διακατέχεται από εμπιστοσύνη μεταξύ των διαφορετικών οντοτήτων που συμμετέχουν σε αυτές με παράλληλη μείωση του κόστους.

Το blockchain αποτελεί μια τεχνολογία που επιτρέπει στα άτομα που συμμετέχουν να πραγματοποιούν πολύ χαμηλές σε κόστος συναλλαγές, μειώνοντας το κόστος ελέγχου των γενικών πληροφοριών που τις διέπουν και επιτρέπει να αναδυθούν νέες αγορές και τομείς. Επίσης όταν ένα κατανεμημένο δίκτυο συνδυάζεται με ένα κρυπτογραφημένο νόμισμα όπως το bitcoin οι συναλλαγές μπορούν να πραγματοποιηθούν χωρίς την διαμεσολάβηση μιας παραδοσιακά κεντρικής έμπιστης αρχής αλλά και με μικρότερο κόστος χρήσης του δικτύου. Catalini C., Gans J. (2016)

Η απλούστερη μορφή του συνεπάγεται με μια διαμοιρασμένη βάση που αυτόνομα διατηρεί μια συνεχώς αυξανόμενη λίστα με δημόσιες εγγραφές μέσα σε blocks τα οποία είναι ασφαλή και αναλλοίωτα. Κάθε block περιέχει μια σύνδεση με το αμέσως προηγούμενο Block. Φυσικά δεν υπάρχει μια μόνο μορφή blockchain αλλά υπάρχουν

διαφορετικά σχεδιασμένα, με άλλο επίπεδο διαφάνειας και άλλο τρόπο διατήρησης των αρχείων. (Yermack 2017 summarize how blockchain work)

Αναλυτικότερα το blockchain είναι ένα αποκεντροποιημένο καθολικό που συνήθως δημιουργείται από ανώνυμου χρήστες και σπανίως από κεντροποιημένα και γνωστά συμβαλλόμενα μέρη. Στα αποκεντροποιημένα blockchain δίκτυα τα άτομα που κρατούν τα αρχεία των συναλλαγών ψηφίζουν στα ιστορικά γεγονότα που πιστεύουν πως είναι σωστά και οι χρήστες (agents) του συστήματος ανάλογα με αυτές τις ψήφους αποφασίζουν την κατάσταση του βρίσκεται το blockchain χρησιμοποιώντας έναν συναινετικό αλγόριθμο. Τα ανώνυμα άτομα που κρατούν τα αρχεία των συναλλαγών ονομάζονται miners και επεκτείνουν την αλυσίδα των blocks. Μετά οι πράκτορες (agents) ψάχνουν να βρουν στο blockchain το μεγαλύτερο μέρος του που έχει καταγράψει την μεγαλύτερη υπολογιστική δύναμη για την επέκταση του. Έτσι ένας νέος χρήστης που δεν γνωρίζει που έχουν κινηθεί οι υπόλοιποι, μπορεί με αυτόν τον τρόπο να εισέλθει στο Blockchain. Για να μπορέσει το blockchain να διατηρήσει και να παράγει την αποκεντροποιημένη συναίνεση χωρίς να χρειάζεται η διαμεσολάβηση μιας κεντρικής αρχής ή ενός τρίτου, από κατασκευής του ανταμείβει τους Miners με την προσθήκη κάθε νέου Block. Φυσικά όλα τα είδη Blockchain αποσκοπούν να δημιουργήσουν ένα σύστημα μιας βάσης δεδομένων στην οποία τα αντισυμβαλλόμενα άτομα θα μπορούν να διορθώνουν, να αλλάζουν και να επεξεργάζονται με αποκεντροποιημένο τρόπο χωρίς ενδιάμεσα άτομα και κεντρικό έλεγχο τις συναλλαγές. Αυτό αποτελεί ένα αδιαμφισβήτητο χαρακτηριστικό της αρχιτεκτονικής του blockchain και ας μην ξεχνάμε πως ο καθένας μοιράζεται και εμπιστεύεται το ίδιο καθολικό δίκτυο. (Abadi J., Brunnermeier M. (2019), Lin William Cong, Zhiguo He (2018))

Το βασικό πρόβλημα στην ηλεκτρονική καταγραφή είναι ο τρόπος που διασφαλίζεται η συναίνεση των αντισυμβαλλόμενων μερών και η πραγματικότητα στην ιστορία των γεγονότων/συναλλαγών. Πολλά blockchain είναι ατελή και έχουν προβλήματα λόγο ότι αναπτύχθηκαν ιδιαίτερα γρήγορα και υπήρχε η ανάγκη ύπαρξης τους κυρίως για την χρησιμότητα που προάγουν. Έχουν υπάρξει αρκετά περιστατικά χακαρίσματος στο blockchain με το πιο αξιοσημείωτο να είναι στο DAO (Decentralized Autonomous Organization) στην blockchain αλυσίδα του Ethereum.[1]

[1] Για λεπτομέρειες δείτε: https://www.coindesk.com/understanding-dao-hack-journalists

Η καταγραφή των αποκεντροποιημένων καθολικών πρέπει να μην διακατέχεται από απατηλές πράξεις των ατόμων που συμμετέχουν στο δίκτυο. Για να αποφευχθεί αυτό και οι αντισυμβαλλόμενοι να μην προβούν σε τέτοιες ενέργειες συνήθως επιβάλλονται ποινές στο ευρύτερο κοινωνικό δίκτυο, χρηματικές ποινές από απώλεια εσόδων αλλά και φυσικά κόστη που συνδέονται με τους πόρους του καθολικού δικτύου. Στα κεντροποιημένα δίκτυα πληρωμών η ομοφωνία επιτυγχάνεται με την εμπιστοσύνη στην καταγραφή των συναλλαγών. Η εμπιστοσύνη αυτή μπορεί να επιτυγχάνεται είτε επειδή δίνονται επιπλέον χρήματα για την διασφάλιση των αληθών συναλλαγών είτε επειδή επιβάλλονται ποινές στην περίπτωση απάτης.

Σύμφωνα με τους Lin William Cong, Zhiguo He (2018), οι δύο πιο διακεκριμένοι τρόποι σχεδιασμού ενός δικτύου Blockchain για την διατήρηση της συναίνεσης είναι ο αλγόριθμος συναίνεσης Proof of Work (PoW) και ο αλγόριθμος συναίνεσης Proof of Stake (PoS). Αναλυτική καταγραφή τόσο αυτών των αλγορίθμων συναίνεσης όσο και άλλων πολύ σημαντικών που υπάρχουν σήμερα γίνεται στο δεύτερο κεφάλαιο της διπλωματικής εργασίας. Παρόλα αυτά ακολουθεί μια μικρή αναφορά στο σύστημα συναίνεσης Proof of Work (PoW) και ο Proof of Stake (PoS).

Το PoW ως αλγόριθμος συναίνεσης ανταμείβει τα άτομα που κρατούν τα αρχεία συναλλαγών του δικτύου (record keepers) όταν λύσουν δύσκολα κρυπτογραφικά προβλήματα με απώτερο σκοπό να επιβεβαιώσουν μια συναλλαγή και να δημιουργήσουν ένα νέο block κάνοντας την διαδικασία της εξόρυξης (Mining). Αντιθέτως στο PoS ο δημιουργός του επόμενου block εξαρτάται από τον πλούτο των κρυπτονομισμάτων που ουσιαστικά έχει κάποιο άτομο που συμμετέχει στο δίκτυο.

Οι αλγόριθμοι συναίνεσης λειτουργούν με τέτοιο τρόπο ώστε να μπορέσουν να κάνουν πρόληψη επιθέσεων και να εξασφαλίσουν την πραγματική κατάσταση του καθολικού των συναλλαγών. Οι συναλλαγές καταγράφονται ανάλογα με την χρονική σειρά της πραγματοποίησης τους δηλαδή ανάλογα με το πότε πραγματοποιήθηκαν και διατηρούνται στο δίκτυο. Για να μπορέσει κάποιος να επηρεάσει το δίκτυο, ανάλογα με τον αλγόριθμο συναίνεσης που χρησιμοποιείται, συνήθως χρειάζεται να έχει πάρα πολύ μεγάλη υπολογιστική δύναμη ή πάρα πολλά κρυπτονομίσματα.

Όπως έχει προαναφερθεί ένα blockchain πετυχαίνει πολλά πράγματα ταυτόχρονα. Δηλαδή τον διαμοιρασμό της πληροφορίας, την αποθήκευση των δεδομένων, την ανωνυμία, την ύπαρξη καθολικών, τον μετριασμό της ασυμμετρίας πληροφόρησης, την

ενθάρρυνση συμμετοχής νέων ατόμων κλπ. Το blockchain ιδιαίτερα τα τελευταία χρόνια έχει κεντρίσει το ενδιαφέρον και αποτελεί αντικείμενο επιστημονικής έρευνας με πολλά θέματα γύρω από αυτό. Για παράδειγμα μελέτες που έχουν πραγματοποιηθεί είναι για την πιθανή επίπτωση του Blockchain στην εταιρική διακυβέρνηση, στους μάνατζερ, στους θεσμικούς επενδυτές, στους μικρομετόχους και τους οικονομικούς ελεγκτές. (Yermack 2017).Αλλά και στις κεντρικές τράπεζες που θα μπορούσαν να χρησιμοποιήσουν την τεχνολογία για να δημιουργήσουν το δικό τους ψηφιακό νόμισμα. (Yermack 2016). Καθώς και για την χρήση του ως ένα μοντέλο εσωτερικής ανάπτυξης που παρέχει ένα σύστημα αποτίμησης για crypto- currencies και crypto- tokens (Cong, Li, Wang 2017). Επίσης για τον ρόλο των Smart contracts σε διάφορες πλατφόρμες blockchain (Bartoletti, Pompianu 2017). Καθώς και μεταξύ άλλων πως η τεχνολογία blockchain μπορεί να μειώσει τα κόστη επικύρωσης συναλλαγών και χρήσης του δικτύου. Catalini C., Gans J. (2016)

Τέλος είναι ήδη γεγονός πως κυβερνήσεις, δικαστήρια, συμβολαιογραφικά γραφεία, τράπεζες κλπ ήδη εφαρμόζουν την χρήση του blockchain αλλά είναι ιδιαίτερα δαπανηρή και θέτονται θέματα ασφάλειας αλλά και εκμετάλλευσής από μονοπωλιακές δυνάμεις. Υπό αυτό το πρίσμα το Blockchain είναι πολλά υποσχόμενο στο να διαταράξει πολλές βιομηχανίες μέσω της προαγωγής του συναινετικού τρόπου λειτουργίας του με έναν πιο αποκεντροποιημένο συναινετικό τρόπο.

1.5 Διακράτηση αρχείων συναλλαγών και ψευδείς αναφορές στο blockchain

Το μοναδικό πλεονέκτημα που το Blockchain και η αποκεντροποίηση απορρέουν είναι πως αυτός ο αποκεντροποιημένος χαρακτήρας αυξάνει την ποιότητα της συναίνεσης μειώνοντας τα κίνητρα χειραγώγησης του κάθε ατόμου που κρατάει τα αρχεία των συναλλαγών στο blockchain. Τα άτομα όμως αυτά μπορεί να έχουν κίνητρο να κάνουν ψευδείς αναφορές ιδιαίτερα όταν είναι παράλληλα και εμπλεκόμενα μέρη σε μια εμπορική και χρηματοοικονομική συναλλαγή. (Lin William Cong, Zhiguo He (2018)) Ας μην ξεχνάμε πως οι συμμετέχοντες στο δίκτυο (Miners) συμβάλλουν στο να αναμεταδίδουν και να επιβεβαιώνουν τις νέες συναλλαγές δημιουργώντας ταυτόχρονα νέα Blocks. (Catalini C., Gans J. (2016))

Ας πούμε πως για παράδειγμα οι Bitcoin Miners πιθανώς κρύβουν αναφορές που αφορούν την προσωπική εξόρυξη ή το λεγόμενο double spending ή περιπτώσεις χακαρίσματος που μπορεί να παρατηρήσουν ή που μπορεί να προέρχονται και από τους ίδιους. Παρόμοια κίνητρα μπορεί να υπάρχουν και να ισχύουν και στις πραγματικές οικονομίες. Ας μην ξεχνάμε όπως αναφέρεται και από τους Lin William Cong, Zhiguo He (2018) το double spending ήταν ένα θέμα που δημιουργήθηκε στις παραδοσιακές on line πληρωμές και ουσιαστικά η επίλυση αυτού του προβλήματος αποτέλεσε ερέθισμα και πηγή έμπνευσης για την δημιουργία του Bitcoin.

Μπορεί οι αναφορές που γίνονται στα μέσα μαζικής ενημέρωσης, σε συζητήσεις αλλά και σε περιοδικά από άτομα με γνώσεις στον χώρο να αναφέρουν πως το blockchain βοηθάει στην μείωση του παρεμβατισμού, της χειραγώγησης, του χακαρίσματος και των ψευδών αναφορών, όμως όλα αυτά για να υπάρξουν σε ένα αποκεντροποιημένο δίκτυο συναλλαγών χρειάζεται να πραγματοποιηθεί ένα είδος συναίνεσης. Αυτή η συναίνεση είναι συνυφασμένη με την απόκλιση από την τήρηση του αρχείου των συναλλαγών από την πραγματικότητα.

Εξετάζοντας την ανάλυση των Abadi J., Brunnermeier M. (2019) για τις δύο περιπτώσεις των γνωστότερων και πιο διαδεδομένων αλγορίθμων συναίνεσης στα δίκτυα blockchain, δηλαδή το Proof of Work και το Proof of Stake αλλά και το τι υφίσταται στην περίπτωση ενός κεντροποιημένου ιδιωτικού Blockchain δηλαδή που χρειάζεται άδεια εισόδου για τους χρήστες καταλήξαμε στα ακόλουθα.

Αρχικά όσον αφορά τις ψευδείς αναφορές και την απάτη σε ένα κεντροποιημένο Private blockchain system, ο δημιουργός του blockchain αυτού που ουσιαστικά είναι και ο μονοπωλιούχος του δικτύου συνήθως δημιουργεί δύο genesis blocks. Έτσι μπερδεύει τους χρήστες και δημιουργεί αμφιβολία επιμένοντας κάθε φορά πως το άλλο block είναι το μη πραγματικό. Έτσι υποκλέπτει την ψηφιακή υπογραφή από τα άτομα που θέλουν να αναβαθμίσουν το blockchain και έχει πρόσβαση στα προσωπικά στοιχεία των λογαριασμών τους.

Επίσης στην περίπτωση που ένα blockchain δίκτυο χρησιμοποιεί αλγόριθμο συναίνεσης POS η εξαπάτηση γίνεται όπως και σε ένα κεντροποιημένο ιδιωτικό δίκτυο blockchain δηλαδή στο genesis block της αλυσίδας του Blockchain. Στην περίπτωση αυτή η δύναμη της ψηφοφορίας συνδέεται με τον αριθμό των tokens που υπάρχουν στους λογαριασμούς των χρηστών. Η απάτη σε αυτό τον τύπο επιβεβαίωσης γίνεται όταν μια

μεγάλη μερίδα ατόμων δημιουργεί ένα πλαστό genesis block με όλους τους λογαριασμούς μέσα σε αυτό το Block και σε συνδυασμό με όλη την δύναμη ψηφοφορίας που έχουν και χρησιμοποιούν κάνουν δυσδιάκριτες τις οικονομικές συναλλαγές του καθολικού που έχουν γίνει στην πραγματική οικονομία. Αποκτούν τα ιδιωτικά κλειδιά (Private keys) των ατόμων που αντιστοιχούν στους λογαριασμούς τους που ήδη βρίσκονται στο δίκτυο ή που νέοι σκοπεύουν να εισέλθουν στο Blockchain και δημιουργούν ένα fork που μοιάζει να είναι έγκυρο με την πραγματική ομόφωνη αλυσίδα κάνοντας την επίθεση που αποκαλείται Long range attack.

Τέλος σε ένα blockchain δίκτυο που χρησιμοποιεί αλγόριθμο συναίνεσης POW η εξαπάτηση γίνεται στο τελευταίο Block της αλυσίδας του Blockchain. Όταν τα άτομα που θέλουν να αποκλίνουν ή να επιτεθούν στο Blockchain πληρώνουν ή έχουν πρόσβαση σε πάνω από το 51% της υπολογιστικής δύναμης του δικτύου, τότε μπορούν να δημιουργήσουν ένα block παρόμοιο με το τελευταίο του δικτύου χωρίς να φαίνεται η δόλια πράξη τους και να κατευθύνουν προς αυτό την ψηφοφορία των ατόμων που συμμετέχουν στην διαδικασία της συναίνεσης. Έτσι υπάρχει σύγκλιση προς αυτή την διαδρομή για την αναβάθμιση του blockchain και κατ' επέκταση υποκλοπή τους. Να επισημάνουμε πως το κόστος πραγματοποίησης της απόκλισης για το άτομο ή τα άτομα που επιτίθονται συνήθως είναι ιδιαίτερα υψηλό λόγο του κόστους της υπολογιστικής δύναμης που χρειάζονται να χρησιμοποιήσουν.

1.6 Επίτευξη ασφάλειας ενός κατανεμημένου καθολικού

Η ασφάλεια ενός κατανεμημένου καθολικού δικτύου blockchain αποτελεί καθοριστικό παράγοντα για την διατήρηση της ακεραιότητας του τόσο για την διάχυση της εμπιστοσύνης που απορρέει στους χρήστες όσο και για την ορθή επαλήθευση και καταγραφή των συναλλαγών.

Ο σχεδιασμός μιας τεχνολογίας blockchain εξαρτάται από το πόσο αποκεντροποιημένη είναι μια αγορά αλλά σε σχέση με το πόσο η χρησιμότητα του χρειάζεται να βασίζεται σε έμπιστα ενδιάμεσα άτομα. Στην περίπτωση της χρήσης του Bitcoin, από την πρώτη στιγμή στόχος ήταν να γίνει όσο το δυνατόν γίνεται περισσότερο αποκεντροποιημένο. Δεν υπάρχουν έμπιστοι ενδιάμεσοι, οποιοσδήποτε μπορεί να γίνει miner, οποιοσδήποτε μπορεί να προσθέσει νόμιμες συναλλαγές στο Blockchain, ενώ

κανένας δεν μπορεί να σταματήσει τους συμμετέχοντες από τις συναλλαγές στο να τις επιβεβαιώνουν και να προσθέτουν καινούργιες. Βέβαια αυτό είναι που κάνει το Bitcoin ιδιαίτερα ελαστικό σε επιθέσεις και στην λογοκρισία.

Σύμφωνα με τους Catalini C., Gans J. (2016), για να επιτευχθεί η ασφάλεια σε ένα κατανεμημένο καθολικό δίκτυο blockchain η δημιουργία κινήτρων μέσω κάποιου χρηματικού εσόδου στα άτομα που προσθέτουν τα νέα blocks (Miners) είναι ο βασικότερος παράγοντας. Αναλυτικότερα, στο σύστημα αλγοριθμικής συναίνεσης PoW όπως είναι αυτό που χρησιμοποιεί το Bitcoin, οι Miners εκτελούν περίπλοκα υπολογιστικά προβλήματα που είναι ιδιαίτερα δαπανηρά και εξασφαλίζουν ένα δικαίωμα για την προσθήκη ενός νέου block στην αλυσίδα του Blockchain. Μια μονάδα Hardware λογισμικού CPU αντιστοιχεί σε μια ψήφο στην διαδικασία της συναίνεσης. Οι αμοιβές που λαμβάνουν οι Miners με την επιβεβαίωση των συναλλαγών και την προσθήκη με ορθό τρόπο νέων blocks αποτελεί κίνητρό προς αυτούς. Η ανάγκη δημιουργίας κινήτρων για τους miners για να επιβεβαιώνουν τα αποκεντροποιημένα δίκτυα και πρωτόκολλα συναλλαγών δημιούργησε ένα ψηφιακό νόμισμα κάποιας αξίας όπως το Bitcoin σαν ένα στοιχείο του συστήματος.

Κάθε φορά μου εισάγεται ένα νέο Block στην αλυσίδα οι Miners παίρνουν ένα προκαθορισμένο ποσό από το ψηφιακό αυτό νόμισμα για τον εαυτό τους σαν ανταμοιβή. Αυτή η ανταμοιβή συνδυασμένη με το έσοδο από την πραγματοποίηση της συναλλαγής που μπορεί κάποιος χρήστης να έχει συμπεριλάβει για να αυξήσει το κίνητρο του Miner να την πραγματοποιήσει σε προτεραιότητα σε σχέση με άλλες, στην κατασκευή του επόμενου Block, είναι το έσοδο του Miner.

Στα PoW συστήματα η ασφάλεια τους στο πραγματικό επίπεδο του κατανεμημένου δικτύου γίνεται ισχυρότερη όσο προστίθενται νέα blocks. Συνήθως στο δίκτυο η μεγαλύτερη αλυσίδα επιλέγεται ως η πραγματική κατάσταση του καθολικού του και ένα κακόβουλο άτομο που θέλει να προβεί σε κάποια απάτη, χρειάζεται να κατέχει όλη την ενέργεια της αλυσίδας που έχει δαπανηθεί μέχρι εκείνη την στιγμή και να επανυπολογίσει εκ νέου όλα τα Blocks από την αρχή. Η ασφάλεια λοιπόν του δικτύου αυτού συνδέεται με τον βαθμό υπολογιστικής ενέργειας που έχει χρησιμοποιηθεί στην εξόρυξη.

Ας μην ξεχνάμε όμως πως το 2014 μια και μοναδική Mining pool (δεξαμενή εξόρυξης) έφτασε το 50% του δικτύου και δημιούργησε ανησυχίες σε σχέση με την ακεραιότητα της διαδικασίας επιβεβαίωσης. Ένας miner με τέτοιο επίπεδο μεριδίου του

δικτύου θα μπορούσε να κατευθύνει κάποια συναλλαγή όπως εκείνος ήθελε, αντιστρέφοντας την ή κάνοντας το λεγόμενο double spending.

Γεγονός είναι πως όσο περισσότεροι συμμετέχοντες χρησιμοποιούν το κρυπτονόμισμα του δικτύου, η αξία του αυξάνεται γιατί το νόμισμα γίνεται πιο χρήσιμο και προσελκύει περισσότερους Miners χάρις στην υψηλότερη ανταμοιβή που τους δίνει και κατ' επέκταση δεν έχουν λόγο να αποκλίνουν από την πραγματικότητα των συναλλαγών αυξάνοντας την ασφάλεια του δικτύου.

Επίσης άλλου είδους υποστηρικτές αλγορίθμων όπως το Proof of Stake, το Proof of burn και οι υβριδικοί αλγόριθμοι συναίνεσης, ασκούν κριτική στο Proof of Work για την σπατάλη πόρων, δηλαδή ηλεκτρικής ενέργειας αλλά και λογισμικού. Φυσικά ας μην ξεχνάμε πως αυτή η σπαταλώδης φύση του συστήματος είναι που του διατηρεί υψηλά τα επίπεδα ασφαλείας του. Ακόμη ένα ιδιωτικό (private) ή ένα με άδεια (permissioned) blockchain δεν χρειάζεται να επαφίεται σε PoW διαχείριση επιτυγχάνοντας μεγαλύτερα επίπεδα ασφάλειας. Όταν η διαδικασία της εξόρυξης απουσιάζει εντελώς από αυτά τα δίκτυα, ο έλεγχος δεν είναι προστατευμένος από υπολογιστική ισχύ και μόνο εάν οι έμπιστοι μεταξύ τους κόμβοι συμβιβαστούν με άλλο από το πραγματικό σενάριο τότε η ακεραιότητα της αλυσίδας κινδυνεύει (Budish E. (2018)).

Επειδή κάθε Blockchain φυσικό είναι να μην εξυπηρετεί κάθε τύπο συναλλαγής καθώς παίζουν ρόλο πολλοί παράγονται όπως το μέγεθος των συναλλαγών, το επίπεδο ασφαλείας του, ο χρόνος επιβεβαίωσης, οι συνθήκες της κάθε συμφωνημένης συναλλαγής, τα αντισυμβαλλόμενα μέρη κλπ. για παράδειγμα όταν δημιουργήθηκε το Bitcoin, οι χρήστες του κυρίως το έβλεπαν ως ένα φθηνό δίκτυο πληρωμών με μεγάλο αριθμό συναλλαγών ανά δευτερόλεπτο που κρατούσε τα κόστη συναλλαγών χαμηλά. Πλέον αυτό δεν υφίσταται καθώς το bitcoin εισάγει ένα νέο Block κάθε 10 λεπτά με το μέγεθος τους να είναι αρκετά μικρό, μόλις 1MB ενώ παραδείγματος χάριν ένα άλλο κρυπτονόμισμα το Litecoin εισάγει ένα νέο Block κάθε 2,5 λεπτά. Φυσικά αυτό συνεπάγεται με το ότι χρειάζεται λιγότερη υπολογιστική δουλειά για την δημιουργία κάθε Block άρα και ο βαθμός ασφάλειας του είναι χαμηλότερος κάνοντας το περισσότερο κατάλληλο για μικρότερες σε αξία συναλλαγές. Ένα άλλο παράδειγμα είναι πως με την χρήση των smart contracts, το Bitcoin αποκτά την ικανότητα στιγμιαίων πληρωμών ανάμεσα σε χρήστες μέσα από αμφίδρομα δίκτυα πληρωμής, ενώ και πάλι ένα άλλο

blockchain το Ethereum έχει συγκριτικό πλεονέκτημα για την ανάπτυξη εφαρμογών έξυπνων συναλλαγών αλλά και Smart Contracts, με χρήση του κρυπτονομίσματος του.

Τέλος τα πλήρως ανοιχτά και ελεύθερα σε πρόσβαση δίκτυα (όπως του bitcoin) θέτουν πλήρη πρόκληση στις κανονιστικές αρχές να δημιουργήσουν κανόνες ασφαλείας για αυτά. Ας μην ξεχνάμε όμως πως τα δίκτυα αυτά μπορούν να χρησιμοποιηθούν για να αυξήσουν την ανταγωνιστικότητα μεταξύ αγορών όπου οι ενδιάμεσοι έχουν συγκεντρωτικά σημαντικό βαθμό δύναμης στην αγορά (Diamond D., (1996)).

1.7 Το κόστος επαλήθευσης συναλλαγών και χρήσης ενός blockchain σε σχέση με τους κεντροποιημένους τρόπους

Όπως αναλύεται από τους Catalini C., Gans J. στο άρθρο τους με τίτλο Some Simple Economics of the Blockchain (2016), όταν μια συναλλαγή πραγματοποιείται μεταξύ ενός αγοραστή και ενός πωλητή συνήθως η πρόσβαση είναι άμεση από την πλευρά του αγοραστή στην ποιότητα των αγαθών και επιβεβαιώνεται η αυθεντικότητα της πληρωμής με τα μετρητά. Θα μπορούσαμε να πούμε πως ο μόνος ενδιάμεσος σε αυτή την περίπτωση είναι η τράπεζα που επιβεβαιώνει την αξία του χαρτονομίσματος που χρησιμοποιείται στην συναλλαγή αυτή.

Στην περίπτωση χρήσης ενός ψηφιακού νομίσματος είναι γεγονός πως περισσότεροι ενδιάμεσοι επιβεβαιώνουν την συναλλαγή από την αρχή μέχρι το τέλος της που είναι η μεταφορά των χρημάτων. Αυτά τα άτομα για την παροχή της υπηρεσίας τους χρεώνουν ένα κόστος που το υφίστανται και οι δύο πλευρές όταν προφανώς δεν μπορούν οι ίδιοι να επιβεβαιώνουν μόνοι τους την συναλλαγή. Η ανάγκη χρήσης ενδιάμεσων ατόμων αυξήθηκε όσο το μέγεθος της κάθε αγοράς, η γεωγραφική περιοχή που καλύπτει και ο αριθμός των ατόμων που συμμετέχουν αυξάνονται. Όσο τα κόστη επιβεβαίωσής μεγαλώνουν τόσο οι αγορές γίνονται χαμηλής εμπορευσιμότητας και όλο και λιγότεροι αγοραστές και πωλητές βρίσκουν κερδοφόρα την συμμετοχής τους στις συναλλαγές.

Καθώς το κόστος επιβεβαίωσης των συναλλαγών έχει μειωθεί, οι συναλλαγές έχουν μεγαλύτερη επίδοση και οι αγορές έχουν αυξήσει την εμπορευσιμότητα τους και την ασφάλεια τους. Η ψηφιοποίηση έχει ωθήσει το κόστος της επιβεβαίωσης των συναλλαγών κοντά στο μηδέν. Ενώ η Blockchain τεχνολογία έχει την δυναμική να ολοκληρώσει αυτή την διαδικασία με το να επιτρέπει από την πρώτη στιγμή για τους

συμμετέχοντες την ακόμα χαμηλότερη επιβεβαίωση, δίνοντας τους την δυνατότητα να αποθηκεύουν και να αποκτούν καθοριστικής σημασίας πληροφορίες γύρω από ένα ασφαλές επίπεδο επικοινωνίας.

Οι συναλλαγές μέσω Internet, είναι τυπικά ασφαλείς βασιζόμενες στους έμπιστους κόμβους και στους ενδιάμεσους εμπλεκόμενους για την επιβεβαίωση και την επικύρωση των ψηφιακών πληρωμών. Από την άλλη πλευρά οι συναλλαγές μέσω blockchain, αντί το Internet να αποτελεί τον αγωγό μεταξύ των μη έμπιστων μερών, το κρυπτονόμισμα από μόνο του με το πρωτόκολλο του μπορεί να περιέχει τους κανόνες και τα κίνητρα για να υπάρχει ένα αποκεντροποιημένο δίκτυο και ασφαλώς μοιρασμένες πληροφορίες στο καθολικό των συναλλαγών την ίδια στιγμή. Υπό αυτό το πρίσμα τα χαρακτηριστικά των συναλλαγών αποθηκεύονται στο Blockchain και ο σχεδιασμός της αγοράς του κρυπτονομίσματος ορίζει πότε, αλλά και από ποιόν αυτά τα χαρακτηριστικά μπορούν να ανανεωθούν, να επιβεβαιωθούν και να επαναχρησιμοποιηθούν σε μελλοντική ημερομηνία.

Όταν επέρχεται ο διαχωρισμός των κανονικών από τους μη έγκυρους κόμβους ένα κρυπτονόμισμα μπορεί να δημιουργήσει μια αγορά χωρίς την συμβολή ενδιάμεσων τρίτων ατόμων. Για παράδειγμα το Bitcoin μπορεί να μιμηθεί την κεντρική λειτουργικότητα του SWIFT, του ACH δικτύου που χρησιμοποιούν τα χρηματοπιστωτικά ιδρύματα ως ενδιάμεσους έμπιστους κόμβους.

Όταν μια συναλλαγή πραγματοποιείται στην οικονομία δημιουργείται μια πληροφορία για τον αγοραστή και τον πωλητή για το που τα στοιχεία εισόδου βγαίνουν και που τα στοιχεία εξόδου πρέπει να πάνε, για το ποιες ενέργειες πρέπει να πραγματοποιηθούν όπως για την μεταφορά των χρημάτων αλλά και των αγαθών αλλά και πως επιβεβαιώνονται όλα αυτά. Δηλαδή από την αρχή μέχρι το τέλος της συναλλαγής χρειάζεται να πραγματοποιείται ένας έλεγχος που έχει κάποιο κόστος και γίνεται από ένα τρίτο συμβαλλόμενο. Ουσιαστικά όταν γίνεται μια συναλλαγή βλέπουμε από ποιόν αρχίζει και σε ποιον πηγαίνει, ποιες επιπλέον ενέργειες γίνονται πχ μεταφέρθηκαν τα αγαθά, μεταφέρθηκαν τα χρήματα και υπάρχει ο έλεγχος των παραπάνω ενεργειών από τρίτα συμβαλλόμενα άτομα.

Με την χρήση του Blockchain μειώνεται το κόστος επαλήθευσης των παραπάνω και φυσικά μόνο τα επιτρεπόμενα άτομα έχουν πρόσβαση σε αυτές τις πληροφορίες. Η

ακεραιότητα και η ασφάλεια του κάθε Blockchain εγγυάται την ακεραιότητα των χαρακτηριστικών των συναλλαγών.

Τέλος πολύ σημαντικό να αναφερθεί είναι πως ενώ το κόστος επιβεβαίωσης με το Blockchain πλησιάζει στο μηδέν μέρος των πληροφοριών που πριν ήταν μη οικονομικό να διαμοιραστεί πλέον μπορεί να γίνει μέρος της αγοράς. Είναι γεγονός πως το Blockchain είναι ένας φθηνός τρόπος για την επικαιροποίηση της ακεραιότητας των μεμονωμένων συναλλαγών ή των χαρακτηριστικών τους καθώς όχι μόνο μια πληροφορία μπορεί να ελεγχθεί σε πραγματικό χρόνο αλλά ταυτόχρονα και η ακεραιότητα του κάθε συμμετέχοντα στο δίκτυο αυτό. Δηλαδή η επιβεβαίωση μπορεί να εφαρμοστεί σε πιο ουσιαστικό επίπεδο απ΄ ότι προηγουμένως καθώς για παράδειγμα αυτό που προηγουμένως περιελάβανε την κατανάλωση χρόνου και δαπανηρού ελέγχου, τώρα η διαδικασία αυτή μπορεί να πραγματοποιηθεί σε συνεχόμενο χρόνο στο υπόβαθρο για να εξασφαλιστεί η ασφάλεια και η συμμόρφωση στην αγορά καθώς και η μείωση του ηθικού κινδύνου.

1.8 Εμπορικές πληρωμές και κρυπτονομίσματα

Από την δημιουργία του Bitcoin το 2008 μέχρι ακόμα και σήμερα ασκήθηκαν σε αυτό πολλές κριτικές που το καταδίκαζαν ως μια απάτη ή ως μια φούσκα. Επίσης υπήρχαν και άλλες απόψεις, μικρότερες βέβαια, που υποστήριζαν πως τέτοιου είδους νομίσματα είναι μόνο για να υποστηρίξουν παράνομες δραστηριότητες και συναλλαγές. Αντιθέτως υπήρξαν και υποστηρικτές που βασίστηκαν πως η κρυπτογράφηση των κρυπτονομισμάτων μπορεί να διασφαλίσει την ασφάλεια και πως αυτά τα νέα νομίσματα μπορούν να υποστηρίξουν πληρωμές χωρίς την ανάγκη διαμεσολάβησης ενός τρίτου ατόμου που θα ελέγχει το νόμισμα ή τις πληρωμές για δικό του κέρδος πιθανώς.

Να αναφερθεί πως κάποιες κεντρικές τράπεζες πρόσφατα άρχισαν να εξερευνούν την υιοθέτηση των κρυπτονομισμάτων και της τεχνολογίας blockchain για την χρήση τους στο εμπόριο και στις μεγάλες σε αξία πληρωμές. Για παράδειγμα η τράπεζα Peoples Bank of China, που στοχεύει να αναπτύξει σε όλη την επικράτεια της ένα ψηφιακό νόμισμα που θα βασίζεται στην blockchain τεχνολογία. Η τράπεζα του Καναδά, η Monetary Authority of Singapore που μελετάει την χρήση του για συστήματα ενδοτραπεζικών πληρωμών αλλά και η Deutsche Bundesbank που έχει αναπτύξει σε αρχικό στάδιο ένα πρωτότυπο

Blockchain που βασίζεται στους συμβιβασμούς χρηματοοικονομικών περιουσιακών στοιχείων.

Οι παραπάνω λόγοι κέντρισαν το ενδιαφέρον μας και ορμώμενοι από την έρευνα που πραγματοποιήσαμε παρουσιάζονται τα συμπερασμάτων των Chiu J., Koeppl T. (2018) από την επιστημονική έρευνα που διεξήγαγαν γύρω από το εάν θα μπορούσε να αποτελέσει η χρήση του Blockchain του Bitcoin τον κύριο τρόπο πληρωμών σε μια οικονομία.

Γεγονός είναι πως είναι πολύ σημαντικό για να μπορέσει να πραγματοποιηθεί μια σύγκριση μεταξύ των παραδοσιακών τρόπων πληρωμής και των κρυπτονομισμάτων και της δυνατότητας που έχουν να αποτελέσουν μια πρόκληση για το σύστημα πληρωμών των εμπορικών συναλλαγών είναι εξ αρχής να εστιάσουμε στην κατανόηση του σχεδιασμού που διέπει ένα κρυπτονόμισμα. Δηλαδή να δοθεί έμφαση στα χαρακτηριστικά που διέπουν την τεχνολογία του συστήματος του δηλαδή του Blockchain, του Mining, της επίδρασης τους μεταξύ των συμμετεχόντων σε ένα δίκτυο, αλλά και των κινήτρων που έχουν για να κάνουν με απατηλές πράξεις (του double spending).

Ο λόγος που αναφερόμαστε στο double spending είναι γιατί τα κρυπτονομίσματα βασίζονται σε ψηφιακά αρχεία συναλλαγών και μπορούν να αντιγραφούν εύκολα και χωρίς κόστος το οποίο σημαίνει ότι μπορούν να έχουν την δυνατότητα να χρησιμοποιηθούν αρκετές φορές σε συναλλαγές.

Σύμφωνα με τους Jonathan Chiu και Thorsten Koeppl (2018) και το μοντέλο που ανέπτυξαν, καθώς είναι οι πρώτοι που αναλύουν θεωρητικά το βέλτιστο σχεδιασμό ενός κρυπτονομίσματος και δίνουν μια ποσοτική απάντηση στις αποτελεσματικές ιδιότητες τους κατέληξαν στα ακόλουθα. Αρχικά πως το Bitcoin έχει ιδιαίτερα υψηλά κόστη για να μπορέσει να αποτελέσει το βασικό μέσω πληρωμών σε μια οικονομία, αλλά κάποιο άλλο κρυπτονόμισμα με άλλο σχεδιασμό θα μπορούσε να υποστηρίξει και τις πληρωμές αρκετά καλά. Επίσης με την χρήση δεδομένων του Bitcoin έδειξαν πως το κόστος εφαρμογής ενός τέτοιου κρυπτονομίσματος μπορεί να συγκριθεί με το σύστημα πληρωμών μιας χώρας με μέτριο πληθωρισμό. Ενώ με την χρήση στατιστικών για τις συναλλαγές πιστωτικών καρτών στις ΗΠΑ βρήκαν πως ένα κρυπτονόμισμα μπορεί να λειτουργήσει πολύ καλά ως μέσω συναλλαγών για μικρής αξίας εμπορικές πληρωμές που πραγματοποιούνται με μικρά κόστη. Αυτό εγείρει το θέμα πως πολλά κρυπτονομίσματα

στην παρούσα φάση δεν μπορούν να αποτελέσουν αντικαταστάτη των μεγάλων εμπορικών δικτύων πληρωμών.

Είναι γεγονός πως τα περισσότερα μοντέλα κρυπτονομισμάτων δημιουργήθηκαν από άτομα που γνώριζαν την επιστήμη των υπολογιστών και επικεντρώνονταν στην δυνατότητα τους να εφαρμοστούν αλλά και να είναι ασφαλή. Σημαντικά θέματα όπως τα κίνητρα των συμμετεχόντων για να τα υποκλέψουν, η πραγματική αξία του κρυπτονομίσματος αλλά και άλλοι παράγοντες αγνοήθηκαν παντελώς. Τέτοιες σκέψεις είναι καθοριστικές για να καταλάβουμε τον βέλτιστο σχεδιασμό για να μπορέσει ένα κρυπτονόμισμα να αποκτήσει οικονομική αξία και να γίνει μέσω πληρωμών.

Επίσης να αναφέρουμε πως μέσω του μοντέλου τους κατέληξαν πως η χρήση του bitcoin ως μέσω συναλλαγών στο ευρύτερο κοινωνικό σύνολο είναι 500 φορές μεγαλύτερη σε κόστος απ' ότι ενός παραδοσιακού νομίσματος με επίπεδα χαμηλού πληθωρισμού. Αυτό είναι ένα αποτέλεσμα του μη αποτελεσματικού σχεδιασμού του Bitcoin ως κρυπτονόμισμα. Παρόλα οφείλουν να αναγνωρίσουν πως αποτελεί μια ιδιαίτερα ασφαλή μορφή πληρωμής διότι η δομή των αμοιβών προς τους Miners είναι ιδιαίτερα αρκετές οπότε αποκλείεται το double spending.

Ακόμη χρησιμοποιώντας δεδομένα από τις Fedwire και US Debit cards επιβεβαιώνουν στην έρευνα τους πως τα κρυπτονομίσματα είναι αρκετά καλύτερη εναλλακτική λύση για χαμηλής αξίας και υψηλής σε όγκο συναλλαγές παρά σε μεγάλης αξίας πληρωμές. Τα αποτελέσματα τους έδειξαν πως τα κρυπτονομίσματα μπορούν να αποτελέσουν έναν έγκυρο εναλλακτικό τρόπο εμπορικών πληρωμών που θα πραγματοποιείται με πολύ χαμηλά έξοδα αρκεί οι περιορισμοί που υπάρχουν σήμερα να ξεπεραστούν. Να επισημάνουμε πως όσο αυξάνεται το μέγεθος των συναλλαγών σε αξία, τα κίνητρα για double spending αυξάνονται και αυτά ενώ αντιθέτως σε συναλλαγές με χαμηλό μέγεθος τα κίνητρα για double spending είναι χαμηλά. Επομένως χρειάζεται περισσότερη διαδικασία εξόρυξης και καθυστέρηση της επιβεβαίωσης της συναλλαγής, που είναι και τα δύο δαπανηρά. Ένα κρυπτονόμισμα λοιπόν συμπεριφέρεται καλύτερα όταν ο όγκος συναλλαγών είναι μεγαλύτερος απ΄ ότι για μια μεμονωμένη σε μέγεθος συναλλαγή. Να αναφέρουμε πως το υπάρχον κόστος μεταφοράς στις ΗΠΑ για τις Debit cards είναι 23 cents και για το Fedwire και 82, με αποτέλεσμα να μην υπάρχει κρυπτονόμισμα που να μπορεί να ανταγωνιστεί αυτές τις συναλλαγές.

Επιπροσθέτως μεταξύ άλλων η έρευνα τους κατέληξε στο συμπέρασμα πως ο τωρινός σχηματισμός του Bitcoin δημιουργεί μια απώλεια κοινωνικής ευημερίας (welfare loss) κατά 1,4% στην κατανάλωση σε σχέση με το παραδοσιακό σύστημα πληρωμών. Αυτή η απώλεια ευημερίας μπορεί να μειωθεί στο 0,08% υπό την υιοθέτηση ενός βέλτιστου σχεδιασμού που μειώνει την διαδικασία του mining η οποία διαπιστώθηκε πως είναι περίπου 360 εκατομμύρια δολάρια τον χρόνο. Αυτό σημαίνει πως τα άτομα είναι διατεθειμένα να αποδεχτούν ένα νόμισμα το οποίο έχει πληθωρισμό 230 % πριν αποδεχτούν το ίδιο το bitcoin πρώτα ως μέσω συναλλαγής.

Ενώ τέλος οι Catalini C., Gans J. (2016), διαπίστωσαν πως το Bitcoin έχει λιγότερη επίδοση σε σχέση με ένα κεντροποιημένο δίκτυο πληρωμών όπως η Visa. Και ιδιαίτερα μετά το 2014 από τα stress test που έγιναν στο δίκτυο της Visa βρέθηκε πως μπορεί να διαχειριστεί σε ιδιαίτερα αυξημένη περίοδο 56.582 συναλλαγές μηνυμάτων το δευτερόλεπτο ενώ αντίθετα το Bitcoin μπορεί να διαχειριστεί μόλις 7 συναλλαγές το δευτερόλεπτο.

Συμπερασματικά λοιπόν παρόλο που το Bitcoin προσομοιάζει με μετρητά χρήματα, παραμένει αρκετά αναποτελεσματικό σύστημα για να διευκολύνει τον βέλτιστο τρόπο συναλλαγών. Ως αποτέλεσμα αυτού αλλά και των παραπάνω λόγων που αναλύθηκαν, ειδικά το Bitcoin από την δομή του και μόνο δεν μπορεί να διαχειριστεί μεγάλες σε όγκο συναλλαγές που απαιτούνται από το μοντέρνο εμπορικό δίκτυο πληρωμών.

1.9 Συμπεράσματα Κεφαλαίου

Ένα blockchain είναι ένα δημόσιο καθολικό βιβλίο συλλογής και καταγραφής πληροφοριών, συναλλαγών και όχι μόνο διατηρώντας την ασφάλεια, την σταθερότητα, την επεκτασιμότητα, τον αυτοματισμό και τα χαμηλά κόστη. Είναι ένας εντελώς νέος τρόπος τεκμηρίωσης δεδομένων και συναλλαγών στο διαδίκτυο και δεν αποτελεί εταιρεία, ή μια εφαρμογή όπως ένα application αλλά ένα δίκτυο σαν μια βάση δεδομένων που αποθηκεύει γεγονότα και συναλλαγές ανάλογα με την χρονική σειρά της πραγματοποίησης τους.

Το blockchain βρίσκεται στο διαδίκτυο και είναι ένας συνδυασμός υπολογιστών συνδεδεμένων μεταξύ τους αντί ενός κεντρικού διακομιστή, που σημαίνει ότι ολόκληρο το δίκτυο είναι αποκεντρωμένο. Στην επιστήμη των υπολογιστών, ένα ομότιμό δίκτυο peer-to-peer (P2P) αποτελείται από μια ομάδα συσκευών που συλλογικά αποθηκεύουν και μοιράζονται αρχεία. Κάθε άτομο που συμμετέχει με την συσκευή του δηλαδή τον κόμβο του (Node) στο δίκτυο ενεργεί ως μεμονωμένος ομότιμος (peer).

Υπάρχουν πολλά διαφορετικά είδη blockchains σήμερα και μερικά λειτουργούν δημόσια, μερικά ιδιωτικά. Βασίζονται στην κρυπτογράφηση και αποτελούν την τεχνολογία πίσω από τα περισσότερα κρυπτονομίσματα. Η μελέτη πάνω στην κρυπτογραφική ασφάλεια της αλυσίδας των blocks χρονολογείται από το 1991 ενώ η πρώτη εκτεταμένη εφαρμογή μιας αλυσίδας blockchain που εμφανίστηκε ήταν το κρυπτονόμισμα Bitcoin, ενώ σήμερα άλλα δημοφιλή blockchain μετά το Bitcoin είναι το Ethereum, το Ripple κλπ.

Ένα πολύ σημαντικό στοιχείο ενός blockchain είναι τα blocks τα οποία αποτελούν τα σημεία εκείνα του δικτύου blockchain που συγκεντρώνονται, καταγράφονται και αποθηκεύονται τα δεδομένα, οι πληροφορίες και οι συναλλαγές που πραγματοποιούνται. Ένα block συνήθως αποτελείται από μια σειρά μηνυμάτων, μια ένωση (Pointer) στο επόμενο block και μια κεφαλή (Header). Μέσα σε ένα blockchain διεξάγεται μια διαδικασία που ονομάζεται ψηφοφορία (voting) και αυτή η διαδικασία ακολουθείται από τα άτομα που συμμετέχουν σε ένα δίκτυο blockchain για να προσθέσουν ένα νέο block σε αυτό. Όταν προστίθεται ένα νέο block στην αλυσίδα υπάρχει μια αμοιβή που ονομάζεται block reward η οποία αναφέρεται στην ανταμοιβή που λαμβάνει ένα άτομο όταν επικυρώσει επιτυχώς ένα νέο block. Τα παραδοσιακά κεντροποιημένα συστήματα καταγραφής συναλλαγών βασίζονται στην κοινή συναίνεση των μερών για την εμπιστοσύνη στην φύλαξη των

αρχείων. Η εμπιστοσύνη αυτή διεγείρεται από τα κατάλληλα κίνητρα στο να παραμένουν διαφανείς οι συναλλαγές

Στην αρχιτεκτονική ενός blockchain πολύ σημαντικό ρόλο έχει το πρωτόκολλο του το οποίο αποτελεί του κύριους κανόνες λειτουργίας του αλλά και ο αλγόριθμος συναίνεσης ο οποίος είναι ο τρόπος συμφωνίας για την επέκταση του κάθε νέου block στην blockchain αλυσίδα. Κάθε πρωτόκολλο blockchain λόγω της ψηφιακής του μορφής, χρειάζεται ένα ψηφιακό περιουσιακό στοιχείο για να κρατήσει το δίκτυο σε λειτουργία. Αυτό το ψηφιακό στοιχείο είναι τα Coins ή τα tokens τα οποία χρησιμοποιούνται και ως χρηματικά κίνητρα για τους συμμετέχοντες στο δίκτυο.

Η επένδυση σε ένα blockchain δεν γίνεται άμεσα σε αυτό αλλά μέσω των κρυπτονομισμάτων που χρησιμοποιούν την τεχνολογία αυτή. Άρα η επένδυση σε ένα κρυπτονόμισμα συνεπάγεται με την επένδυση στο blockchain που χρησιμοποιεί, αποκτώντας ουσιαστικά μέρος του. Τέλος μια καινοτόμα εφαρμογή που προσφέρεται σε πολλά blockchains ανάλογα με το πρωτόκολλο λειτουργίας τους είναι τα Έξυπνα συμβόλαια (Smart Contracts). Τα έξυνα συμβόλαια είναι ένα σύνολο λογικών κανόνων υπό μορφή κωδικοποίησης που μπορούν να ενσωματωθούν στο blockchain με την μορφή εφαρμογών (applications) για να καθορίσουν μια συναλλαγή. Ουσιαστικά λειτουργούν όπως τα παραδοσιακά νομικά έγγραφα και λαμβάνουν πληροφορίες ως εισροές και εκτελούν συγκεκριμένες ενέργειες ως αποτελέσματα.

Στο αποκεντροποιημένο σύστημα συναλλαγών η δημιουργία του Blockchain προώθησε έναν διαφορετικό τρόπο της διατήρησης του αρχείου των συναλλαγών και της καταγραφής των πληροφοριών. Αυτός ο αποκεντροποιημένος χαρακτήρας αυξάνει την ποιότητα της συναίνεσης μειώνοντας τα κίνητρα χειραγώγησης του κάθε ατόμου που κρατάει τα αρχεία των συναλλαγών στο Blockchain. Η ασφάλεια ενός κατανεμημένου καθολικού δικτύου blockchain αποτελεί καθοριστικό παράγοντα για την διατήρηση της ακεραιότητας του τόσο για την διάχυση της εμπιστοσύνης που απορρέει στους χρήστες όσο και για την ορθή επαλήθευση και καταγραφή των συναλλαγών.

Το blockchain ιδιαίτερα τα τελευταία χρόνια έχει κεντρίσει το ενδιαφέρον και αποτελεί αντικείμενο επιστημονικής έρευνας με πολλά θέματα γύρω από αυτό. Για παράδειγμα ένα κρυπτονόμισμα μπορεί να δημιουργήσει μια αγορά χωρίς την συμβολή ενδιάμεσων τρίτων ατόμων. Πιο συγκεκριμένα το bitcoin μπορεί να μιμηθεί την κεντρική λειτουργικότητα του SWIFT, του ACH δικτύου που χρησιμοποιούν τα χρηματοπιστωτικά

ιδρύματα ως ενδιάμεσους έμπιστους κόμβους. Παρόλα αυτά μπορεί το Bitcoin να προσομοιάζει με μετρητά χρήματα, παραμένει αρκετά αναποτελεσματικό σύστημα για να διευκολύνει τον βέλτιστο τρόπο συναλλαγών καθώς από την δομή του και μόνο δεν μπορεί να διαχειριστεί μεγάλες σε όγκο συναλλαγές που απαιτούνται από το μοντέρνο εμπορικό δίκτυο πληρωμών. Να αναφερθεί πως κάποιες κεντρικές τράπεζες πρόσφατα άρχισαν να εξερευνούν την υιοθέτηση των κρυπτονομισμάτων και της τεχνολογίας blockchain για την χρήση τους στο εμπόριο και στις μεγάλες σε αξία πληρωμές.

<u>ΚΕΦΑΛΑΙΟ 2:</u> Πρωτόκολλα λειτουργίας, αλγόριθμοι συναίνεσης και το πρόβλημα των διπλών δαπανών στο blockchain

2.1 Εισαγωγή Κεφαλαίου

Το δεύτερο κεφάλαιο της διπλωματικής εργασίας έχει ως στόχο την ανάλυση τριών ζητημάτων γύρω από ένα Blockchain. Την ανάλυση των πρωτοκόλλων λειτουργίας, των αλγορίθμων συναίνεσης και του προβλήματος των διπλών δαπανών.

Πιο συγκεκριμένα στο κεφάλαιο, γίνεται αναφορά και ανάλυση των κυριότερων πρωτόκολλων blockchain που υπάρχουν σήμερα, όπως ενδεικτικά να αναφέρουμε είναι το πρωτόκολλο λειτουργίας Bitcoin, το πρωτόκολλο λειτουργίας Ethereum, το πρωτόκολλο λειτουργίας Ripple, το πρωτόκολλο λειτουργίας Hyperledger κλπ, δίνοντας έμφαση στα πλεονεκτήματα που παρουσιάζει το καθένα αλλά και στα χαρακτηριστικά που τα καθιστούν κατάλληλα ανάλογα με την χρήση του blockchain δικτύου. Στην συνέχεια αναλύουμε τι είναι ο αλγόριθμος συναίνεσης στο blockchain επισημαίνοντας τις βασικές διαφορές από το πρωτόκολλο λειτουργίας και δίνουμε έμφαση για στους λόγους που είναι απαραίτητος για την διασφάλιση της σωστής λειτουργίας και της ασφάλειας ενός blockchain δικτύου. Ενώ επίσης αναφερόμαστε και αναλύουμε τα βασικά χαρακτηριστικά στους σημαντικότερους και πιο διαδεδομένους αλγόριθμους συναίνεσης που προτιμώνται σήμερα στα Blockchain δίκτυα όπως είναι ο Proof of Work (PoW)», ο «Proof of Stake (PoS)», ο «Delegated Proof of Stake (DPoS)», ο « Proof of Activity (PoA)» κλπ και παρουσιάζουμε την πρακτική χρήση ανάλογα με τις ανάγκες των ατόμων που συμμετέχουν σε ένα Blockchain.

Τέλος αναφερόμαστε στο πρόβλημα των διπλών δαπανών (Double spending problem) που μπορεί να παρουσιαστεί σε ένα blockchain, πως και υπό ποιες περιπτώσεις είναι πιθανό να προκληθεί.

2.2 Τι είναι ένα πρωτόκολλο λειτουργίας;

Εάν κοιτάξουμε το διαδίκτυο, τότε θα διαπιστώσουμε ότι όλα λειτουργούν σύμφωνα με ένα πλάνο. Ένα πρόγραμμα περιήγησης (Browser) στέλνει μηνύματα σε ένα διακομιστή (Server) και σε αντάλλαγμα, το πρόγραμμα περιήγησης λαμβάνει τον ιστότοπο (Website) ή τους πόρους που αναζητά ο χρήστης. Όλα αυτά είναι δυνατά χάρη στα πρωτόκολλα του Διαδικτύου. (Nitish Sinch, Top 5 Blockchain Protocols That You Should Know (2019))

Ένα πρωτόκολλο είναι βασικά ένα θεμελιώδες επίπεδο κώδικα που ορίζει κάτι για το πως θα λειτουργήσει πως θα επιτευχθεί μια συγκεκριμένη αποστολή. Ένα πρωτόκολλο στην επιστήμη των υπολογιστών, είναι ένα σύνολο κανόνων ή διαδικασιών που διέπουν τη μεταφορά δεδομένων μεταξύ δύο ή περισσότερων ηλεκτρονικών συσκευών. Το πρωτόκολλο είναι απαραίτητο να βοηθά στον καθορισμό του τρόπου, δηλαδή των κανόνων με τους οποίους, οι υπολογιστές επικοινωνούν και ανταλλάσσουν πληροφορίες. Οι πληροφορίες αυτές πρέπει να είναι δομημένες με τέτοιον τρόπο ώστε ο κάθε συμβαλλόμενος να μπορεί να τις στέλνει αλλά και να μπορεί να τις λαμβάνει. (Genesis DevCon, What are Blockchain Protocols and How Do they Work?, (2018), Liquid, What are protocols in crypto and blockchain? (2018))

Για παράδειγμα στο διαδίκτυο τα πρωτόκολλα επιτρέπουν στους ιστότοπους να λειτουργούν. Τα πιο συνηθισμένα πρωτόκολλα Διαδικτύου είναι τα, HTTP και HTTPS - αν και μπορεί να συναντήσουμε το TCP / IP, το DNS, και το SMTP. Αυτά τα πρωτόκολλα είναι ο υποκείμενος κώδικας που επιτρέπει σε όλες τις εφαρμογές του Διαδικτύου να εκτελούνται. Το Facebook, το Amazon, το Twitter, το Google, το Netflix, οι τραπεζικοί ιστότοποι, οι ιστοχώροι ειδήσεων αλλά και σχεδόν κάθε ιστοσελίδα που χρησιμοποιούμε τρέχει σε ένα από αυτά τα πρωτόκολλα διαδικτύου. (Liquid, What are protocols in crypto and blockchain? (2018))

Τα πρωτόκολλα δεν περιορίζονται μόνο στο διαδίκτυο αλλά έχουν και πεδίο εφαρμογής και στα κρυπτονομίσματα μέσω του blockchain τους.

2.3 Τι είναι το πρωτόκολλο λειτουργίας ενός blockchain;

Όλα τα blockchains δεν είναι ίδια και δεν έχουν την ίδια δομή. Ο τρόπος λειτουργίας τους καθορίζεται από ένα πρωτόκολλο που ακολουθούν (Liquid, What are protocols in crypto and blockchain? (2018))

Τα πρωτόκολλα του blockchain δεν διαφέρουν σε γενικές γραμμές από αυτά του διαδικτύου και έχουν σχεδιαστεί για να διατηρούν τις διάφορες πτυχές του blockchain. Αυτό σημαίνει πως υπάρχουν πρωτόκολλα ασφαλείας, πρωτόκολλα δικτύου, πρωτόκολλα συναίνεσης κλπ. Όταν όλα αυτά τα πρωτόκολλα συνδυάζονται μεταξύ τους τότε ένα Blockchain αρχίζει να αποκτά διάσταση. (Nitish Sinch, Top 5 Blockchain Protocols That You Should Know (2019))

Για παράδειγμα σε κάθε κρυπτονόμισμα, όπως το Bitcoin, το Ethereum, το XRP έχει το δικό του ξεχωριστό πρωτόκολλο λειτουργίας και το πρωτόκολλο του blockchain του είναι η αξία για εκείνο. Είναι αυτό που δίνει ζωή στο blockchain του και δίνει τη δυνατότητα στην κρυπτογράφηση να κάνει ό,τι προορίζεται να κάνει. Καθώς το οικοσύστημα των κρυπτονομισμάτων έχει επεκταθεί ώστε να περιλαμβάνει περισσότερα περιουσιακά στοιχεία και να πραγματοποιεί περισσότερες συναλλαγές, τα πρωτόκολλα έχουν λάβει μεγαλύτερη σημασία. (Tobias A. HuberWhat Makes Crypto Protocols Valuable? (2018))

Το πρωτόκολλο λειτουργίας ενός blockchain βρίσκεται στο Genesis Block του και καλεί τους προγραμματιστές να δημιουργήσουν λύσεις για προβλήματα επιδόσεων και κλιμάκωσης τόσο των υφιστάμενων πρωτοκόλλων blockchain όσο και για να κατασκευάσουν εξ ολοκλήρου νέα πρωτόκολλα από την αρχή. (Genesis DevCon, What are Blockchain Protocols and How Do they Work? (2018)

Όπως έχει αναφερθεί, επειδή η βασική ιδέα πίσω από το blockchain είναι ο αποκεντρωμένος χαρακτήρας του, ένα blockchain είναι ένα δίκτυο πολλαπλών συσκευών (κόμβων) οι οποίες είναι όλες εξίσου σημαντικές και ταυτόχρονα είναι συνδεδεμένες μεταξύ τους μέσω του διαδικτύου. Ουσιαστικά, ένα blockchain είναι ένα καθολικό βιβλίο που αποθηκεύει και καταγράφει για το τι ακριβώς πληροφορίες και συναλλαγές έχουν πραγματοποιηθεί με κατανεμημένο τρόπο Peer- 2- Peer αφού η συναλλαγή αυτή έχει επαληθευτεί από όλους τους συμμετέχοντες στο δίκτυο των κόμβων αυτών. Προκειμένου όμως να μπορέσει να λειτουργήσει σωστά και ομαλά αυτή η ιδέα χρειάζονται πρωτόκολλα

για ακολουθούν οι συμμετέχοντες στο δίκτυο, για να διασφαλίζεται η σωστή και έγκυρη καταγραφή των συναλλαγών και να διατηρείται η συναίνεση και η λειτουργία στο δίκτυο των blocks. (Genesis DevCon, What are Blockchain Protocols and How Do they Work?, (2018)

Αυτό το κατανεμημένο καθολικό λειτουργεί με προκαθορισμένους κανόνες οι οποίοι συμφωνούνται από όλους τους συμμετέχοντες δηλαδή τους peers του δικτύου. Κάποιοι από τους κανόνες αυτούς είναι οι ακόλουθοι:

- Για το πως διακυβερνώνται και επικυρώνονται οι συναλλαγές
- Για την ασφάλεια και την πρόσβαση
- Για το πως γίνεται η αλληλεπίδραση για όλους τους συμμετέχοντες κόμβους
- Για την διασύνδεση εφαρμογών (applications) προγραμματισμού σε συγκεκριμένες περιπτώσεις

Αυτοί οι κανόνες που διέπουν και ορίζουν την λειτουργία ενός δικτύου blockchain ονομάζονται πρωτόκολλο του blockchain και ουσιαστικά είναι με απλά λόγια οι κοινοί κανόνες επικοινωνίας των συσκευών δηλαδή των ατόμων που συμμετέχουν και χρειάζεται το δίκτυο για να λειτουργήσει. Το πρωτόκολλο δίνει ζωή στις εφαρμογές που βρίσκονται πάνω του παρέχοντας ασφάλεια σε μια ποικιλία υπηρεσιών που εξυπηρετεί κάθε διαφορετικό blockchain καθώς εξυπηρετούν διαφορετικούς σκοπούς και στόχους.

Τέλος να επισημάνουμε πως αρχίζουμε να μεταβαίνουμε από το κεντροποιημένο μοντέλο παραδοσιακής οικονομικής διαχείρισης δηλαδή από την εμπιστοσύνη που δείχνουμε σε μια τράπεζα για να μπορεί να διατηρεί την ακεραιότητα του τραπεζικού μας λογαριασμού και να διασφαλίζει ότι τα χρήματά μας δεν θα χρησιμοποιούνται παραπάνω από μια φορά, στον αποκεντρωμένο κόσμο του blockchain όπου η ασφάλεια παρέχεται από το πρωτόκολλο το οποίο επιτρέπει την επικοινωνία των δεδομένων μεταξύ των ομότιμων κόμβων. Άρα έχει μεγάλη σημασία το πρωτόκολλο λειτουργίας του κάθε blockchain.

2.4 Ανάλυση κάποιων από τα κυριότερα πρωτόκολλα blockchain

Αρχικά το **Bitcoin Protocol** είναι το πιο γνωστό πρωτόκολλο κρυπτονομισμάτων. Πρόκειται για σύστημα συμμετεχόντων που είναι όλοι ομότιμοι μεταξύ τους (peer-to-peer) που επιτρέπει στα άτομα που συμμετέχουν σε αυτό, να πραγματοποιούν συναλλαγές μεταξύ τους χωρίς την παρεμβολή κάποιου έμπιστου τρίτου συμβαλλόμενου όπως είναι για παράδειγμα μια τράπεζα. Το πρωτόκολλο αυτό επιτρέπει οι συναλλαγές να είναι μη αναστρέψιμες και να αποτρέπεται η διπλή δαπάνη των χρημάτων (double spending). Οι τεχνολογίες του Blockchain του Bitcoin περιλαμβάνουν τον κατακερματισμό (hash), την ψηφιακή υπογραφή (digital signature), το δημόσιο κρυπτογραφημένο κλειδί (public-key), το P2P σύστημα επικοινωνίας και τον αλγόριθμο επιβεβαίωσης Proof – of – Work. (Liquid, How to invest in blockchain (2019))

Η αρχή του πρωτοκόλλου του Bitcoin blockchain χρονολογείται από τον Νοέμβριο του 2008 και πρόκειται για το πιο γνωστό πρωτόκολλο κρυπτονομισμάτων. Δημοσιεύθηκε από τον Nakamoto με τίτλο Bitcoin: A peer-to-peer electronic cash system" και πρόκειται για σύστημα συμμετεχόντων που είναι όλοι ομότιμοι μεταξύ τους (peer-to-peer) που επιτρέπει στα άτομα που συμμετέχουν σε αυτό να πραγματοποιούν συναλλαγές μεταξύ τους χωρίς την παρεμβολή κάποιου έμπιστου τρίτου συμβαλλόμενου όπως είναι για παράδειγμα μια τράπεζα. Το πρωτόκολλο αυτό επιτρέπει οι συναλλαγές να είναι μη αναστρέψιμες και να αποτρέπεται η «διπλή δαπάνη» των χρημάτων (double spending) .

Οι κύριες τεχνολογίες που διέπουν το Blockchain του Bitcoin περιλαμβάνουν τον κατακερματισμό (hash), την ψηφιακή υπογραφή (digital signature), το δημόσιο κρυπτογραφημένο κλειδί (public-key), το P2P σύστημα επικοινωνίας και τον αλγόριθμο επιβεβαίωσης Proof of Work.

Τα χαρακτηριστικά του πρωτοκόλλου του bitcoin blockchain σύμφωνα με τον Bryant Nielson (2020) είναι τα ακόλουθα:

- Να επιτρέπει τη απευθείας συναλλαγή χωρίς την ανάγκη συμβολής σε αυτή οποιουδήποτε αξιόπιστου τρίτου μέρους
- Ενεργοποιεί τις μη αναστρέψιμες συναλλαγές

- Μειώνει το κόστος σε μικρές και απλές συναλλαγές και γενικώς τα κόστη συναλλαγών
- Αποτρέπει το Double spending
- Δημόσιο, ελεύθερο σε συμμετοχή από τον οποιοδήποτε, χωρίς φραγμούς εισόδου
- Κάθε κόμβος του δικτύου έχει πρόσβαση σε όλες τις πληροφορίες του blockchain και εκεί υφίσταται η αποκεντροποιημένη του φύση.
- να επιτρέπει τις πληρωμές και τις συναλλαγές μέσω του φυσικού του νομίσματος που είναι το bitcoin

Επίσης ένα άλλο πρωτόκολλο είναι το blockchain **Ethereum** το οποίο αποτελεί ένα διαφορετικό πρωτόκολλο από εκείνο του Bitcoin. Είναι ένα δημόσιο πρωτόκολλο ανοιχτής πηγής (open source) που χρησιμοποιείται ως πρωτόκολλο για αποκεντρωμένες εφαρμογές, αποκεντρωμένες αυτόνομες οργανώσεις με αρκετές λειτουργικές εφαρμογές όπως την ανάπτυξη Smart Contracts, δηλαδή των έξυπνων συμβολαίων. Τα Smart Contracts είναι εφαρμογές που εκτελούνται με ελάχιστες παρεμβάσεις από τρίτους και μπορούν να καταγράψουν από συναλλαγές μέχρι μετακινήσεις κεφαλαίων εάν ικανοποιούν κάποιες συγκεκριμένες συνθήκες. (Olga Kharif, Ethereum 'Almost Full' as Controversial Coin Gobbles Up Capacity, (2019))

Το πρωτόκολλο του blockchain Ethereum παρέχει μια αποκεντρωμένη εικονική μηχανή που ονομάζεται Ethereum Virtual Machine (EVM), η οποία χρησιμοποιώντας την Turning τεχνολογία χρησιμοποιεί τόσο ένα παγκόσμιο δίκτυο δημόσιων κόμβων όσο και το token που ονομάζεται Ether για την κατανομή των πόρων αυτών. Τα στοιχεία που συνδέονται με την τεχνολογία του είναι ο κρυπτογραφικός κατακερματισμός, οι ψηφιακές υπογραφές, η P2P κρυπτογράφηση, τα δημόσια και ιδιωτικά κλειδιά, ο PoW αλγόριθμος συναίνεσης. (Bryant Nielson, Review of the 6 Major Blockchain Protocols, (2020))

Στα χαρακτηριστικά του πρωτοκόλλου του Ethereum Blockchain περιλαμβάνονται:

- Ότι είναι δημόσιο και δεν χρειάζεται η άδεια συμμετοχής σε αυτό
- Ότι κάθε κόμβος του δικτύου έχει πρόσβαση σε όλες τις πληροφορίες του blockchain και εκεί υφίσταται η αποκεντροποιημένη του φύση.

- Ότι οι χρήστες μπορούν να πραγματοποιούν μη αναστρέψιμες συναλλαγές χωρίς να χρειάζεται να εμπιστεύονται κάποιο τρίτο αντισυμβαλλόμενο άτομο.
- Επιτρέπει τις πληρωμές και τις συναλλαγές μέσω του φυσικού του νομίσματος που είναι το Ether

Το blockchain του Ethereum έδωσε έναν μεγαλύτερο και ευρύτερο ορίζοντα σε αυτά που θα μπορούσε να έχει χρησιμότητα ένα blockchain. Για παράδειγμα έχουν ξεκινήσει πολλά ερευνητικά σχέδια όπως το OmiseGo και το VeChain που χρησιμοποιούν την πλατφόρμα του Ethereum. Επίσης έγιναν πλατφόρμες που αναπτύχθηκαν από προγραμματιστές για να μπορούν να εισάγουν το δικό τους blockchain και να ξεκινήσουν τα δικά τους projects και τις αποκεντροποιημένες εφαρμογές (decentralized applications-dApps) αλλά και αναπτύχθηκαν κρυπτονομίσματα όπως το Cryptokitties, το Brave και το PundiX σε αυτήν. Τέλος να αναφερθεί πως αυτή η πλατφόρμα του Ethereum αποτέλεσε πηγή έμπνευσης πολλών πρωτοκόλλων για να εισάγουν διαφορετικές καινοτομίες. Για παράδειγμα, η λειτουργία επαλήθευσης κάθε κόμβου του blockchain καθιστούσε αργή τη διαδικασία, οδηγώντας σε ζητήματα κλιμάκωσης. Το Zillica, το EOS και το Cardano είναι μερικά παραδείγματα αλυσίδων blockchain που επιχείρησαν να δημιουργήσουν λύσεις για τέτοιου είδους ζητήματα.(Genesis DevCon, What are Blockchain Protocols and How Do they Work?, (2018))

Ακόμη ένα άλλο πρωτόκολλο λειτουργίας είναι το **Enterprise Ehereum Alliance**. Όπως αναφέρθηκε και προηγουμένως το Ethereum είναι ένα από τα καλύτερα πρωτόκολλα δημόσιου χαρακτήρα στην επιλογή ενός blockchain καθώς προσφέρει ένα ευρύ φάσμα χαρακτηριστικών, συμπεριλαμβανομένων των έξυπνων συμβολαίων (Smart Contracts), την δημιουργία των dApps και πολλά άλλα.

Ωστόσο, για να καταστούν εφικτές οι παραπάνω χρήσεις από την πλευρά των επιχειρήσεων, χρειάζεται να παρέχεται με άδεια η συμμετοχή σε αυτό το Blockchain, έτσι ώστε να επιτρέπεται στις επιχειρήσεις να δημιουργούν δίκτυα ιδιωτικής ιδιοκτησίας πλήρως ικανά για να κλιμακώνονται στις ανάγκες των επιχειρήσεων. Η βασική διαφορά λοιπόν μεταξύ του Ethereum και του Enterprise Ethereum Alliance είναι η άδεια για συμμετοχή σε αυτό (Permission). (Nitish SinchTop 5 Blockchain Protocols That You Should Know, (2019))

Σύμφωνα με τον επίσημο ηλεκτρονικό ιστότοπο του Enterprise Ehereum Alliance (entethalliance.org) ο βασικός στόχος του είναι να διατηρήσει ένα πρότυπο ανοικτού κώδικα, να βελτιώνεται παράλληλα μαζί με το Ethereum blockchain και να αναπτυχθεί μεταξύ διάφορων τομέων δραστηριότητας.

Να αναφερθεί πως οι ιδιωτικές αλυσίδες Blockchain που δημιουργούνται χρησιμοποιώντας το Enterprise Ethereum Alliance διαχωρίζονται από τις δημόσιες αλυσίδες Blockchain που χρησιμοποιούν το Ethereum, αλλά οι ιδιωτικές είναι πλήρως ικανές να αλληλοεπιδράσουν με τις δημόσιες αν χρειαστεί. Η Enterprise Ethereum Alliance προσφέρει ένα καλύτερο επίπεδο προστασίας προσωπικών δεδομένων με βελτιωμένες επιδόσεις και δυνατότητα κλιμάκωσης. Αυτή τη στιγμή υπάρχουν 300 και πλέον εταιρείες μέλη και περισσότερα από 1400 μεμονωμένα μέλη και 45 και πάνω χώρες που συμμετέχουν σε αυτό το Blockchain.

Ακόμη ένα ιδιαίτερα διαδεδομένο πρωτόκολλο λειτουργίας blockchain είναι το **Ripple Network** που ξεκίνησε το 2012. Ο κύριος σκοπός της λειτουργίας του είναι να επιτρέπει στις τράπεζες, στα άτομα που θέλουν να πραγματοποιήσουν πληρωμές αλλά και ψηφιακές ανταλλαγές περιουσιακών στοιχείων σε παγκόσμιο επίπεδο να το πράξουν με σχεδόν άμεσο τρόπο. Το Ripple είναι γνωστό ως σύστημα διακανονισμού πληρωμών, ανταλλαγής στοιχείων και εμβασμάτων που λειτουργεί περισσότερο σαν SWIFT υπηρεσία για διεθνείς μεταφορές χρημάτων και παρέχοντας ασφάλεια που μπορεί να χρησιμοποιείται από ένα δίκτυο τραπεζών και χρηματοπιστωτικών διαμεσολαβητών. (Jake Frankenfield, (2019), Ripple (Cryptocurrency)

Πολύ συχνά επειδή οι πληρωμές είναι δαπανηρές, αναξιόπιστες και αργές, το πρόβλημα αυτό έρχεται να το λύσει το RippleNet προσφέροντας την πιο εξελιγμένη τεχνολογία blockchain για παγκόσμιες πληρωμές, διευκολύνοντας έτσι τα χρηματοπιστωτικά ιδρύματα να φτάσουν σε ένα αξιόπιστο, αναπτυσσόμενο δίκτυο. Χρησιμοποιεί μιας ανοιχτής πηγής διαμοιρασμένη συναίνεση καθολικού και υποστηρίζει tokens που μπορούν να έχουν τη μορφή νομισμάτων συμπεριλαμβανομένων των fiat, άλλων κρυπτονομισμάτων αλλά και άλλων περιουσιακών στοιχείων.

Το Ripple Blockchain χρησιμοποιεί ένα κοινό καθολικό μητρώο είναι υπό την διαχείριση ενός δικτύου ανεξάρτητων επικυρωμένων διακομιστών που συγκρίνουν συνεχώς τα αρχεία συναλλαγών. Τέλος το ψηφιακό νόμισμα του δικτύου είναι το XRP και

ενώ στην περίπτωση του Bitcoin που τα νέα κρυπτονομίσματα εισάγονται στο δίκτυο από τους Miners, στην περίπτωση του XRP απελευθερώνεται μέσω smart contracts.

Επιπροσθέτως ένα ακόμα ιδιαίτερα καινοτόμο και διαδεδομένο πρωτόκολλο λειτουργίας blockchain είναι το **Hyperledger** το οποίο ξεκίνησε το 2015. Είναι ένα ανοικτού κώδικα επιχειρηματικό blockchain που η συμμετοχή σε αυτό χρειάζεται άδεια. Δεν είναι ούτε εταιρεία, ούτε κρυπτονόμισμα αλλά αποτελεί έναν κόμβο για την ανάπτυξη ανοικτών βιομηχανικών blockchain. Δεν υποστηρίζει κάποιο κρυπτονόμισμα όπως είναι το Bitcoin αλλά η πλατφόρμα αυτή συνδέεται άμεσα με την τεχνολογία του blockchain, παρέχοντας επιχειρηματικές λύσεις. (Ameer Rosic, (2017), Roshan Raj, (2019)

Σύμφωνα με την επίσημη ιστοσελίδα του Hyperledger (hyperledger.org), το Hyperledger είναι μια συνεργατική προσπάθεια ανοικτού κώδικα που δημιουργήθηκε για να προωθήσει τις τεχνολογίες blockchain μεταξύ των βιομηχανιών. Πρόκειται για μια παγκόσμια συνεργασία,η οποία φιλοξενείται από το Ίδρυμα Linux, συμπεριλαμβανομένων των ηγετών στον τομέα της χρηματοδότησης, της τραπεζικής, του IoT, της αλυσίδας εφοδιασμού, των κατασκευών κλπ. Το έργο δίνει έμφαση στην πραγματοποίηση συνεργατικών προσπαθειών για την καθιέρωση ανοικτών προτύπων και πρωτοκόλλων, υποστηρίζεται μέσω της γλώσσας προγραμματισμού Python και παρέχει ένα ασφαλές κανάλι στο οποίο τα άτομα μπορούν να μοιράζονται ιδιωτικές πληροφορίες.

Τέλος μεταξύ των πλεονεκτημάτων του Hyperledger είναι πως διαθέτει τεχνολογία αιχμής, ότι αυξάνει την παραγωγικότητα, αποτελεί μια συνεργατική προσέγγιση, έχει καλή ποιότητα κώδικα λόγω της ανοιχτής του μορφής.

Κάποια από τα βασικά έργα εντός του πλαισίου του Hyperledger είναι τα ακόλουθα, ενώ προσφέρει επίσης πολλά εργαλεία, όπως το Avalon, το Cello, το Caliper κλπ: :

- Hyperledger Besu
- Hyperledger Fabric
- Hyperledger Iroha
- Hyperledger Indy
- Hyperledger Sawtooth
- Hyperledger Burrow

Το **Corda** είναι υπό την διαχείριση της εταιρείας R3 και αποτελεί ένα ελπιδοφόρο επιχειρησιακό πρωτόκολλο κατανεμημένου καθολικού, ανοιχτού κώδικα, χωρίς κάποιο φυσικό κρυπτονόμισμα. Χρησιμοποιεί αλγόριθμους συναίνεσης για τη διασφάλιση της διαφάνειας, της ανιχνευσιμότητας και της επικύρωσης των συναλλαγών, ενώ έχει αναπτυχθεί με σκοπό να καταγράφει, να εποπτεύει και να συγχρονίζει τις χρηματοοικονομικές συμφωνίες μεταξύ χρηματοπιστωτικών ιδρυμάτων και οργανισμών. Η αρχιτεκτονική του χαρακτηρίζεται από την μακροζωία, την ασφάλεια και την σταθερότητα. (r3.com, Platform Corda Enterpris –a next gen blockchain platform, (2020)

Τα κυριότερα χαρακτηριστικά του R3 Corda είναι η ικανότητα να δημιουργεί έξυπνες συμβάσεις, να προσφέρει υπηρεσίες μοναδικότητας και χρονοσήμανσης αλλά και να επιτρέπει στις επιχειρήσεις να γράφουν πολύπλοκα πρωτόκολλα και να τα δουλεύουν με τους χρήστες. Σε μεγάλο βαθμό εμπερικλείει τα πλεονεκτήματα των δικτύων blockchain, χωρίς φυσικά να μετατρέπει όλα τα Blockchains να είναι κατάλληλα για τραπεζικά σενάρια. Ενώ όπως προαναφέρθηκε προσφέρει επίσης την δυνατότητα των Smart Contracts, πράγμα που σημαίνει ότι οι περισσότερες τραπεζικές λύσεις μπορούν να αυτοματοποιηθούν. Αυτή τη στιγμή, το οικοσύστημα Corda αναπτύσσεται και έχει περισσότερα από 200 μέλη από διαφορετικούς βιομηχανικούς τομείς (Nitish Sinch, Top 5 Blockchain Protocols That You Should Know, (2019))

Ακόμη το πρωτόκολλο λειτουργίας **Quorum** είναι επίσης άλλη μια εταιρεία πρωτόκολλου blockchain που στοχεύει στην επίλυση προβλημάτων του χρηματοπιστωτικού τομέα. Το Quorum είναι αρκετά παρόμοιο με το Hyperledger, αλλά η ομάδα προγραμματιστών της JPMorgan Chase ανέπτυξε ένα ιδιωτικό blockchain βασιζόμενο σε εκείνο του Ethereum επεκτείνοντας το πρωτόκολλο Zether. Είναι ένα πλήρως αποκεντρωμένο, κρυπτογραφικό πρωτόκολλο για εμπιστευτικές πληρωμές, συμβατό με το Ethereum, άλλες έξυπνες πλατφόρμες συμβολαίων (smart contracts) και σχεδιασμένο να προσθέτει ένα επιπλέον επίπεδο ανωνυμίας στις συναλλαγές. (Ian Allison (2019), JPMorgan Adds Privacy Features to Ethereum-Based Quorum Blockchain, Nitish Sinch, Top 5 Blockchain Protocols That You Should Know, (2019))

Τα βασικά χαρακτηριστικά του blockchain της Quorum είναι η καλή απόδοση που προσφέρει, οι μηχανισμοί συναίνεσης με βάση την ψηφοφορία, η ανοιχτή πηγή κώδικα, η αξιοπιστία για τις επιχειρήσεις οι ενισχυμένες συναλλαγές σε επίπεδο ιδιωτικού απορρήτου καθώς και πολλά άλλα. Με την χρήση του πρωτοκόλλου να μην περιορίζεται

μόνο σε χρηματοοικονομικές επιχειρήσεις, αλλά να μπορεί να χρησιμοποιηθεί και σε άλλες βιομηχανικές περιπτώσεις. (goquorum.com, (2020) Evolve with Quorum.)

Τέλος άλλο ένα πολύ γνωστό πρωτόκολλο λειτουργίας είναι το **Openchain το** οποίο αποτελεί μια τεχνολογία κατανεμημένου λογισμικού ανοιχτού κώδικα. Είναι κατάλληλη για οργανισμούς που επιθυμούν να εκδώσουν και να διαχειριστούν ψηφιακά στοιχεία ενεργητικού με ισχυρό, ασφαλή και κλιμακωτό τρόπο. (docs.openchain.org, Overview of Openchain, (2020))

Θα μπορούσαμε να πούμε πως το Openchain πέφτει κάτω από την ομπρέλα της τεχνολογίας Blockchain αλλά δεν είναι μια αλυσίδα από Blocks. Δηλαδή δεν είναι δομημένη στο να παράγει block συναλλαγών και να τα συνδέεται κρυπτογραφικά μέσω του hashing αλλά οι συναλλαγές είναι άμεσα συνδεδεμένες μεταξύ τους όπως γίνεται με έναν πελάτη- διακομιστή (client server) Η ενοποίηση των συναλλαγών σε block εισάγει καθυστέρηση στο δίκτυο, ενώ στο Openchain οι συναλλαγές συνδέονται με την αλυσίδα μόλις υποβληθούν και επιβεβαιώνονται σε πραγματικό χρόνο. (openchain.org, (2020),Blockchain technology for the enterprise)

Βασικά χαρακτηριστικά του πρωτοκόλλου του Openchain είναι πως δεν υπάρχουν κόστη εξόρυξης, είναι εξαιρετικά μεγάλη η δυνατότητα κλιμάκωσης καθώς και ότι παρέχεται ασφάλεια μέσω των ψηφιακών υπογραφών. Τέλος πολύ σημαντικό ρόλο έχουν τα πολλαπλά επίπεδα ελέγχου όπως ότι είναι ένα πλήρως ανοιχτό καθολικό που μπορεί να εισέλθει κάποιος ανώνυμα, όπως ότι είναι ένα καθολικό όπου οι συμμετέχοντες πρέπει να εγκριθούν από τον διαχειριστή αλλά και ένας συνδυασμός των δύο με τους εγκεκριμένους χρήστες να απολαμβάνουν περισσότερα δικαιώματα από τους ανώνυμους χρήστες. (Liquid, What are protocols in crypto and blockchain?, (2018))

2.5 τι ορίζεται ως αλγόριθμος συναίνεσης σε ένα blockchain;

Η συναίνεση (Consensus) σαν έννοια συνδέεται με ένα σύνολο κανόνων και ρυθμίσεων για την πραγματοποίηση των λειτουργιών του blockchain. Ο αλγόριθμος συναίνεσης θα μπορούσαμε να πούμε πως είναι ένα είδος συμφωνίας που ικανοποιεί όλες τις πλευρές που συμμετέχουν σε ένα blockchain. Αποτελεί το κλειδί της δημοκρατίας και γενικότερα της αποκέντρωσης και φυσικά της διαμοιρασμένης καταγραφής γεγονότων. Ένας αλγόριθμος συναίνεσης μπορεί να οριστεί ως ο μηχανισμός μέσω του οποίου ένα δίκτυο blockchain φτάνει σε συμφωνία. (MLSDev, Blockchain Architecture Basics: Components, Structure, Benefits & Creation, (2019)

Τα δημόσια (αποκεντρωμένα) blockchains δημιουργούνται ως κατανεμημένα συστήματα και δεδομένου ότι δεν βασίζονται σε κεντρική αρχή, οι κατανεμημένοι κόμβοι πρέπει να συμφωνήσουν σχετικά με την εγκυρότητα των συναλλαγών. Εδώ λοιπόν έρχονται οι αλγόριθμοι της συναίνεσης να διαβεβαιώσουν ότι ακολουθούνται οι κανόνες πρωτοκόλλου και να εγγυηθούν ότι όλες οι συναλλαγές πραγματοποιούνται με έναν βέβαιο τρόπο.

Στο πλαίσιο των κρυπτονομισμάτων, οι αλγόριθμοι συναίνεσης είναι ένα κρίσιμο στοιχείο κάθε δικτύου blockchain, καθώς είναι υπεύθυνοι για τη διατήρηση της ακεραιότητας, της ασφάλειας και της χρησιμοποίησης τους μόνο μια φορά σε κάθε συναλλαγή. Η διαδικασία της συναίνεσης είναι μια διαδικαστική απόφαση. Ο στόχος της είναι να διασφαλίσει ότι οι συμμετέχοντες στο δίκτυο συμφωνούν σε μια συγκεκριμένη κατάσταση προσθέτοντας πληροφορίες, δεδομένα αλλά και συναλλαγές μέσω νέων block. Με λίγα λόγια η διαδικασία της συναίνεσης διασφαλίζει πως η αλυσίδα του blockchain παραμένει σωστή και παρέχει τα κίνητρα για να μην αποκλίνουν από την πραγματική κατάσταση οι συμμετέχοντες στην διαδικασία. Η συναίνεση είναι απαραίτητη για την διασφάλιση σε όλους τους κανόνες συμμόρφωσης του δικτύου. Ας πάρουμε για παράδειγμα το Bitcoin, ο αλγόριθμος συναίνεσης του, το Proof of Work ήταν ο πρώτος αλγόριθμος συναίνεσης κρυπτονομισμάτων και δημιουργήθηκε και σχεδιάστηκε από τον Satoshi Nakamoto. Στο blockchain του Bitcoin, κάθε κόμβος του δικτύου είναι διαφανής και ανοιχτός δημοσίως έχοντας όλοι οι συμμετέχοντες ισότητα στο δίκτυο. αυτό επιτυγχάνεται μέσω του αλγορίθμου αυτού. (blog.rokkex.com, PoS, PoW, and 12 Other Blockchain Protocols You Didn’t Know About,,(2019), Binance Academy,What Is a Blockchain Consensus Algorithm?, (2020))

2.6 Ο αλγόριθμος συναίνεσης και το πρωτόκολλο λειτουργίας

Σύμφωνα με το Binance Academy / What Is a Blockchain Consensus Algorithm?, (2020) σε πολλές περιπτώσεις οι όροι αλγόριθμος και πρωτόκολλο χρησιμοποιούνται εναλλακτικά αλλά δεν εκφράζουν το ίδιο. Με απλά λόγια, μπορούμε να ορίσουμε ένα πρωτόκολλο ως τους κύριους κανόνες ενός blockchain και τον αλγόριθμο ως τον μηχανισμό μέσω του οποίου θα ακολουθηθούν αυτοί οι κανόνες. Ένα δίκτυο blockchain θα χτιστεί επάνω σε ένα πρωτόκολλο που θα καθορίσει και θα ορίσει τον τρόπο λειτουργίας του συστήματος, έτσι ώστε όλα τα διαφορετικά μέρη του και όλοι οι συμμετέχοντες στο δίκτυο θα πρέπει να ακολουθούν. Ενώ το πρωτόκολλο καθορίζει ποιοι είναι οι κανόνες, ο αλγόριθμος λέει στο σύστημα τι μέτρα πρέπει να πάρει για να συμμορφωθεί με αυτούς τους κανόνες και να παράγει τα επιθυμητά αποτελέσματα. Για παράδειγμα, ο αλγόριθμος συναίνεσης ενός blockchain καθορίζει την εγκυρότητα των συναλλαγών και των blocks. Έτσι, το blockchain του Bitcoin και το blockchain του Ethereum είναι πρωτόκολλα, ενώ το Proof of Work και το Proof of Stake είναι οι αλγόριθμοι συναίνεσής τους.

Για να γίνει πιο κατανοητό αυτό, το πρωτόκολλο του Bitcoin ορίζει πώς πρέπει να αλληλοεπιδρούν οι κόμβοι, πώς πρέπει να μεταδίδονται τα δεδομένα μεταξύ τους και ποιες είναι οι απαιτήσεις για μια επιτυχημένη επικύρωση ενός block. Από την άλλη πλευρά, ο αλγόριθμος συναίνεσης είναι υπεύθυνος για την επαλήθευση των ισορροπιών και των υπογραφών, την επιβεβαίωση των συναλλαγών και την πραγματική εκτέλεση της επικύρωσης των blocks.

Υπάρχουν διάφοροι τύποι αλγόριθμων συναίνεσης. Οι πιο συνηθισμένες εφαρμογές είναι οι PoW και PoS. Καθένας έχει τα δικά του πλεονεκτήματα και μειονεκτήματα όταν προσπαθεί να εξισορροπήσει την ασφάλεια με την λειτουργικότητα και την κλιμάκωση στο δίκτυο. Παρακάτω ακολουθεί η ανάλυση κάποιων εκ των γνωστότερων, πιο διαδεδομένων αλγορίθμων συναίνεσης που υπάρχουν σήμερα σε δίκτυα Blockchain, ενώ δίνεται έμφαση στο Proof of Work (PoW) και στο Proof of Stake (PoS) καθώς ως πρωταρχικά συστήματα συναίνεσης αποτελούν τις βάσεις για μεταγενέστερα πρωτόκολλα που δημιουργήθηκαν.

2.7 Ανάλυση των σημαντικότερων και πιο διαδεδομένων αλγορίθμων συναίνεσης

2.7.1 Αλγόριθμός Συναίνεσης «Proof of Work (PoW)»

Θεμελιώδης αρχή: Η επίλυση του είναι δύσκολη αλλά είναι εύκολο το να ελέγξεις το αποτέλεσμα της διαδικασίας

Απόδοση: Χαμηλή

Τεχνολογία κατανομής του περιβάλλοντος του καθολικού δικτύου: Δημόσιο Blockchain

Τρόπος συναίνεσης: Πιθανολογικός

Παραδείγματα Χρήσης: Bitcoin, Ethereum, Litecoin

2.7.1.1 Ανάλυση Αλγόριθμου συναίνεσης PoW

Η ιδέα για το Proof or Work δημοσιεύθηκε για πρώτη φορά το 1993 από τους Cynthia Dwork και Moni Naor ως τρόπος πρόληψης των επιθέσεων spam σε ένα δίκτυο και χρειαζόταν κάποιου είδους υπολογιστικής εργασίας και επεξεργασίας από τους χρήστες. Ο όρος " Proof or Work " χρησιμοποιήθηκε για πρώτη φορά από τους Markus Jakobsson και Ari Juels σε μια δημοσίευση που πραγματοποίησαν το 1999 ενώ το 2008 εφαρμόστηκε από τον Satoshi Nakamoto στο έγγραφο του Bitcoin ως ένα καινοτόμο συναινετικό μηχανισμό για την επικύρωση των συναλλαγών που βρίσκονται μέσα σε blocks και είναι συνδεδεμένα σε ένα blockchain. Σήμερα το PoW χρησιμοποιείται από την πλειοψηφία των κρυπτονομισμάτων που βρίσκονται σε κυκλοφορία. (Parikshit Hooda, Proof of Work (PoW) Consensus (2020))

Ο αλγόριθμος συναίνεσης PoW περιλαμβάνει την επίλυση ενός μαθηματικού προβλήματος που απαιτεί υπολογιστικές προκλήσεις προκειμένου να δημιουργηθούν νέα block στην αλυσίδα του blockchain. Η διαδικασία είναι γνωστή ως «εξόρυξη» και οι κόμβοι με τα άτομα του δικτύου που ασχολούνται με την εξόρυξη είναι γνωστοί ως «ανθρακωρύχοι» (miners). Συγκεκριμένα στόχος είναι η επίλυση των δύσκολων υπολογιστικών μαθηματικών προβλημάτων για την εύρεση της κατάλληλης διαδικασίας που ολοκληρώνει ταυτόχρονα την τήρηση κάποιων συγκεκριμένων κανόνων και μπορεί να προσθέσει νέα blocks στην αλυσίδα του blockchain. (blog.rokkex.com, PoS, PoW, and 12 Other Blockchain Protocols You Didn’t Know About (2019))

Τα άτομα που είναι υπεύθυνα για την εξόρυξη ενός νέου block ανταγωνίζονται μεταξύ τους για να βρουν την λύση σε έναν ψευδοτυχαίο αριθμό που σε συνδυασμό με τα δεδομένα που βρίσκονται στα blocks αλλά και μιας συνάρτησης κατακερματισμού (hash) πρέπει να παράξουν ένα αποτέλεσμα που να ταιριάζει με συγκεκριμένες συνθήκες. Όπως για παράδειγμα ένα hash που αρχίζει με τέσσερα μηδενικά. (Binance Academy, Proof of Work Explained, (2020))

Όταν βρεθεί ένα αποτέλεσμα που ταιριάζει, εκπέμπεται ταυτόχρονα σε ολόκληρο το δίκτυο και οι άλλοι κόμβοι επαληθεύουν την εγκυρότητα του αποτελέσματος. Κίνητρο για την εργασία τους είναι πως ο κόμβος αυτός που θα βρει την λύση, δηλαδή ο Miner που έρχεται πρώτος στην εύρεση της σωστής διαδικασίας, θα ανταμειφθεί με την προκαθορισμένη αμοιβή που υπάρχει από το blockchain για κάθε νέο block που προστίθεται αλλά και με το έσοδο για την περάτωση της συναλλαγής που δόθηκε προς πραγματοποίηση. Για παράδειγμα στην περίπτωση του Bitcoin η αμοιβή ανέρχεται σε 12,5 Bitcoin ανά block, το οποίο θα μειώνεται με το πέρασμα του χρόνο στο μισό.

Η συμμετοχή στην διαδικασία του PoW συνδέεται με κόστος των υπολογιστικών πόρων αλλά και ότι η διαδικασία αυτή μπορεί να εφαρμοστεί σε ένα περιβάλλον όπου οι συμμετέχοντες δεν εμπιστεύονται απολύτως ο ένας τον άλλον. Η συμμετοχή στο δίκτυο αυτό μπορεί να γίνει από οποιονδήποτε, καθώς δεν απαιτεί την άδεια στην συμμετοχή από κανέναν. Βασική αρχή του αλγόριθμου αυτού είναι πως αποτελεί μια λύση που είναι δύσκολο να βρεθεί αλλά είναι εύκολο να επαληθευτεί. Ενώ ο σκοπός αυτού του μηχανισμού συναίνεσης είναι να φέρει όλους τους κόμβους σε συμφωνία, δηλαδή να εμπιστεύονται ο ένας τον άλλο σε ένα περιβάλλον όπου δεν υπάρχει εμπιστοσύνη μεταξύ των κόμβων. (blog.rokkex.com, PoS, PoW, and 12 Other Blockchain Protocols You Didn’t Know About, (2019))

Με περισσότερα άτομα να συμμετέχουν στην διαδικασία της εξόρυξης, ο χρόνος που χρειάζεται για να προστεθεί ένα νέο block μειώνεται άρα βρίσκονται με ταχύτερο τρόπο. Το Proof of Work παρέχει προστασία στο δίκτυο από επιθέσεις. Για να στεφθεί με επιτυχία μια επίθεση από κάποιο κακόβουλο άτομο απαιτεί πολλή μεγάλη υπολογιστική ισχύ και πολύ χρόνο για να κάνει τους υπολογισμούς που απαιτούνται για την προσθήκη ενός απατηλού block. Για να προστεθεί ένα τέτοιο Block απαιτείται ο επαναυπολογισμός όλων των προηγούμενων Blocks και να επαναληφθεί ολόκληρη η διαδικασία της εξόρυξης τους, που είναι πρακτικά αδύνατο. Ως εκ τούτου θα ήταν αναποτελεσματική μια επίθεση

δεδομένου ότι το κόστος για την προσθήκη του θα ήταν μεγαλύτερο από τις πιθανές αμοιβές για επίθεση στο δίκτυο. Έτσι μέσω του PoW επιτυγχάνεται και η ασφάλεια του δικτύου και αυτό προστατεύει το blockchain από τις παραβιάσεις των ατόμων που θέλουν να αλλάξουν τις πραγματικές συναλλαγές. (Binance Academy, Proof of Work Explained (2020), Parikshit Hooda, Proof of Work (PoW) Consensus(2020))

Να αναφέρουμε πως κάποια κοινά κρυπτογραφικά πρωτόκολλα που χρησιμοποιούνται στα συστήματα Proof-of-Work και τα συναντάμε πολύ συχνά είναι το SHA-256 που εισήχθη ως μέρος του Bitcoin, το Scrypt, το SHA-3, το scrypt-jane, το scrypt-n, ενώ μεταξύ άλλων κάποια από τα γνωστότερα κρυπτονομίσματα που χρησιμοποιούν ως αλγόριθμο συναίνεσης το PoW είναι το Litecoin, το Ethereum, το Monero coin, το Dogecoin

2.7.1.2 Χαρακτηριστικά και προβλήματα του συστήματος PoW

Σύμφωνα με τον Parikshit Hooda, (2020) υπάρχουν κυρίως δύο χαρακτηριστικά που έχουν συμβάλει στην αποδοχή του συγκεκριμένου πρωτοκόλλου συναίνεσης στον χώρο των κρυπτονομισμάτων και αυτά είναι:

- Η δυσκολία να βρεθεί μια λύση για το μαθηματικό πρόβλημα
- Και η ευκολία να επαληθευτεί η ορθότητα αυτής της λύσης

Ενώ τα κύρια προβλήματα που συνδέονται με τον μηχανισμό συναίνεσης Proof-of-Work έχουν ως εξής:

Ο κίνδυνος 51%: Εάν μια ελεγχόμενη οντότητα κατέχει 51% ή περισσότερο από το 51% των κόμβων στο δίκτυο, η οντότητα μπορεί να εξαπατήσει το blockchain κερδίζοντας το μεγαλύτερο μέρος του δικτύου.

Διαδικασία ιδιαίτερα χρονοβόρα: Οι ανθρακωρύχοι πρέπει να ελέγξουν πολλές τιμές για να βρουν τη σωστή λύση για το παζλ που πρέπει να λυθεί και να εξορύξουν ένα νέο block πράγμα που χρειάζεται αρκετό χρόνο σαν διαδικασία.

Κατανάλωση πόρων: Οι ανθρακωρύχοι καταναλώνουν μεγάλες ποσότητες υπολογιστικής ισχύος για να βρουν τη λύση στο δύσκολο μαθηματικό παζλ. Αυτό οδηγεί

σε σπατάλη πολύτιμων πόρων (χρήματα, ενέργεια, χώρο, υπολογιστικό εξοπλισμό). Φημολογείται πως το 0,3% της παγκόσμιας ηλεκτρικής ενέργειας δαπανήθηκε για την επαλήθευση των συναλλαγών το 2018.

Μεγάλος χρόνος επιβεβαίωσης συναλλαγών: Η επιβεβαίωση μιας συναλλαγής δεν είναι απολύτως στιγμιαία και μπορεί να διαρκέσει από 10 μέχρι και 60 λεπτά.

Συμπερασματικά μπορεί το Proof of Work σύστημα συναίνεσης να μην είναι η πιο αποτελεσματική λύση, όμως εξακολουθεί να είναι μία από τις πιο δημοφιλείς μεθόδους επίτευξης συναίνεσης σε μια blockchain αλυσίδα. Τέλος φυσικά υπάρχουν και άλλες εναλλακτικές λύσεις έναντι της συναίνεσης του PoW καθώς λόγω των αδυναμιών και των μειονεκτημάτων που παρουσιάζει οδήγησαν στην ανάπτυξη νέων πρωτοκόλλων συναίνεσης όπως είναι το Proof of stake, το Proof of burn, το Proof of capacity, το Proof of importance, τα οποία όπως και αρκετά ακόμα αναλύονται στην συνέχεια του κεφαλαίου. Φυσικά όμως μόνο ο χρόνος και οι ανάγκες θα δείξουν ποιος ή ποιοι αλγόριθμοι συναίνεσης θα επικρατήσουν στο μέλλον.

2.7.2 Αλγόριθμος Συναίνεσης «Proof of Stake (PoS)»

- **Θεμελιώδης αρχή:** Η εμπιστοσύνη στο δίκτυο υπάρχει μέσω των ατόμων που επικυρώνουν τις συναλλαγές που θέτουν ως δέσμευση τους δικούς του πόρους για την δημιουργία ενός νέου Block. Όσο μεγαλύτερος είναι ο αριθμός των κρυπτονομισμάτων που κατέχει κάποιος, τόσο μεγαλύτερη είναι η πιθανότητα το δίκτυο να επιτρέψει την δημιουργία ενός νέου Block.
- **Απόδοση:** Υψηλή
- **Τεχνολογία κατανομής του περιβάλλοντος του καθολικού δικτύου:** Δημόσιο και Ιδιωτικό Blockchain
- Τρόπος συναίνεσης: Πιθανολογικός
- **Παραδείγματα Χρήσης:** NXT, Tezos, Nxt, Ethereum(Casper update)

2.7.2.1 Ανάλυση Αλγόριθμου συναίνεσης PoS

Το Proof of Stake (PoS) είναι ένας τύπος αλγόριθμου συναίνεσης στο blockchain. Ο τρόπος αυτού του είδους συναίνεσης προτάθηκε αρχικά από τον Quantum Mechanic και αργότερα από τον Sunny King που δημοσίευσαν σχετικό άρθρο που τον παρουσίαζαν, με το πρώτο κρυπτονόμισμα με αλγόριθμο PoS να είναι το Peercoin. Στοχεύει στην επίτευξη της κατανεμημένης συναίνεσης και μαζί με τον αλγόριθμο Proof-of-Work (που εφαρμόζεται στο Bitcoin) αποτελούν τους πιο δημοφιλείς τρόπους. Το χαρακτηριστικό που διέπει την αρχιτεκτονικού του συγκεκριμένου συναινετικού αλγορίθμου είναι η απουσία επίλυσης περίπλοκων υπολογιστικών προβλημάτων για την επίτευξη της. (Parikshit Hooda, Proof of Stake (PoS) in Blockchain, (2020))

Ενώ το το Proof-of-Work χρειάζεται αρκετή ηλεκτρική ενέργεια και υπολογιστικούς πόρους για την διαδικασία της εξόρυξης το Proof-of-Stake πρόκειται για έναν μηχανισμό συναίνεσης όπου επιλέγονται τα άτομα που επικυρώνουν τα blocks με βάση τον αριθμό των coins που στοιχηματίζουν (staking). Το σχέδιο PoS σχεδιάστηκε ως εναλλακτική λύση στο PoW και είναι μηχανισμός που συνδέεται με κάτι που έχει αξία. Στην περίπτωση αυτή αντί να υφίσταται ανταγωνισμός με άλλους συμμετέχοντες στο δίκτυο, η δημιουργία ενός νέου Block εξαρτάται από τον αριθμό των κρυπτονομισμάτων που έχουν στην κατοχή τους. Συνεπώς επειδή οι ίδιοι οι συμμετέχοντες κατέχουν τα κρυπτονομίσματα αυτά,

ενδιαφέρονται και για την ασφάλεια του δικτύου. (blog.rokkex.comPoS, PoW, and 12 Other Blockchain Protocols You Didn’t Know About,(2019),

Ο όρος "staking" αναφέρεται στην πράξη των επικυρωτών που δεσμεύουν πόρους στο σύστημα, επομένως, οι επικυρωτές μπορούν να συμμετάσχουν στη διαδικασία παραγωγής νέων μονάδων μόνον εάν «κλειδώσουν» τα coins τους. Τα «κλειδωμένα» αυτά κεφάλαια θα λειτουργήσουν τότε ως εξασφάλιση, πράγμα που σημαίνει ότι εάν κάποια άτομα προβούν σε κακόβουλες επικυρώσεις πιθανότατα θα χάσουν το ποντάρισμά τους και θα εκδιωχθούν από το δίκτυο εάν δεν επέλθει η συναίνεση. Σε αντίθετη περίπτωση οι έντιμοι επικυρωτές θα επιβραβευτούν με την αμοιβή του νέου block που θα παραχθεί. Στον αλγόριθμο η επιλογή του ατόμου που επικυρώνει την διαδικασία, γίνεται ανάλογα με το μερίδιο που του ανήκει. Δηλαδή εάν ένας κατέχει το 10% των κρυπτονομισμάτων θα μπορεί να επικυρώσει το 10% των συναλλαγών. Η ιδέα είναι ότι όσο μεγαλύτερη αναλογία κρυπτονομισμάτων έχουν τα άτομα που επικυρώνουν τις συναλλαγές, τόσο λιγότερο ενδιαφέρον θα έχουν στο να χειραγωγήσουν την διαδικασία της επικύρωσης των συναλλαγών. (Binance Academy (Aaron), Proof of Stake (PoS) (2020), blog.rokkex.com, PoS, PoW, and 12 Other Blockchain Protocols You Didn’t Know About, (2019)

Σε αντίθεση με το PoW, το μοντέλο PoS απαιτεί πολύ λίγη υπολογιστική ισχύ και οι επικυρωτές μπορούν να εξασφαλίσουν την συναίνεση στο δίκτυο χρησιμοποιώντας τις επιμέρους υπολογιστικές μηχανές τους και όχι κάποιο εξειδικευμένο υλικό και λογισμικό για την εξόρυξη. Κατά συνέπεια, τα συστήματα PoS μπορούν να παρέχουν αυξημένα επίπεδα κλιμάκωσης, ενεργειακής απόδοσης, αποκέντρωσης και ασφάλειας. Οι συναλλαγές στον συγκεκριμένο τύπο αλγοριθμικής συναίνεσης είναι σχετικά γρήγορες σε σύγκριση με τις συναλλαγές στο δίκτυο όπως του Bitcoin. Και ας μην ξεχνάμε πως τα άτομα που κατέχουν μεγάλο αριθμό κρυπτονομισμάτων θα επικυρώνουν τις συναλλαγές πιο συχνά για να λαμβάνουν ακόμα περισσότερα έσοδα, άρα θα αυξάνουν τον πλούτο τους. (blog.rokkex.com, PoS, PoW, and 12 Other Blockchain Protocols You Didn’t Know About, (2019))

Τα blockchains που αναπτύσσουν το μοντέλο PoS επιτυγχάνουν συναίνεση σε μια διαδικασία που επιλέγει τα άτομα που επικυρώνουν τα Blocks βάσει ενός συνδυασμού παραγόντων. Η επιλογή το επόμενου block ποικίλλει τόσο με βάση το μέγεθος του στοιχήματος όσο και με βάση την ηλικία των coins. Εάν το νέο block επικυρωθεί από το

δίκτυο ο επικυρωτής παίρνει το ποντάρισμα και την ανταμοιβή του block επίσης (Binance Academy (Aaron), (2020), Proof of Stake (PoS))

.

2.7.2.2 Χαρακτηριστικά που διέπουν τον αλγόριθμο συναίνεσης PoS:

Σταθερός αριθμός coins για ανταλλαγή: Υπάρχει μόνο ένας πεπερασμένος αριθμός νομισμάτων που κυκλοφορούν πάντα στο δίκτυο. Δεν υπάρχει η ύπαρξη νέων coins (όπως στην εξόρυξη π.χ. του Bitcoin και άλλων συστημάτων που βασίζονται σε PoW). Να σημειώσουμε πως το δίκτυο ξεκινάει με ένα πεπερασμένο αριθμό coins ή αρχίζει αρχικά με PoW και μετά μεταβαίνει σε PoS σε ορισμένες περιπτώσεις. Αυτή η εκκίνηση με PoW προορίζεται να φέρει coins/ κρυπτονομίσματα στο δίκτυο

Έσοδα συναλλαγών ως ανταμοιβή: Κάθε συναλλαγή που πραγματοποιείται στο δίκτυο έχει και κάποια χρέωση. Αυτές οι χρεώσεις συσσωρεύονται και δίνονται στα άτομα που δημιουργούν το νέο block. Στην περίπτωση που προσπαθήσει κάποιος να προσθέσει ένα «πλαστό» Block τότε δεν επιβραβεύεται προφανώς με το έσοδο της συναλλαγής αλλά χάνει και το ποντάρισμα του ως επικυρωτής.

Ανεπάρκεια της επίθεσης του 51%: Για να εκτελέσει μια επίθεση 51%, ο επιτιθέμενος θα πρέπει να κατέχει το 51% του συνόλου των κρυπτονομισμάτων του δικτύου, πράγμα που είναι πολύ ακριβό. Μια τέτοιου είδους επίθεση είναι πολύ δαπανηρή, έχει προβλήματα καθώς δεν θα υπάρχουν πολλά κρυπτονομίσματα να αγοραστούν από άλλους και θα ανέβει η τιμή τους. Επίσης, η επικύρωση λανθασμένων συναλλαγών θα προκαλέσει την απώλεια του πονταρίσματος των επικυρωτών με αποτέλεσμα να έχουν αρνητική ουσιαστικά αμοιβή.

2.7.2.3 Πλεονεκτήματα που παρουσιάζει ο αλγόριθμος συναίνεσης PoS:

Ενεργειακή απόδοση: Επειδή όλοι οι κόμβοι δεν ανταγωνίζονται μεταξύ τους για να φέρουν ένα νέο block στο blockchain, εξοικονομείται ενέργεια. Επίσης, δεν χρειάζεται να

βρεθεί η λύση σε κάποιο δύσκολο υπολογιστικό πρόβλημα όπως στην περίπτωση του Proof-of-Work, και έτσι εξοικονομείται ενέργεια.

Αποκέντρωση: Σε blockchains όπως το Bitcoin το Proof of Work μπορεί να επιτυγχάνει την κατανεμημένη συναίνεση αλλά υπάρχει ένα επιπλέον κίνητρο για εκθετικού είδους ανταμοιβές εάν ενταχθούν οι Miners σε μια «mining pool» που οδηγεί σε έναν πιο κεντροποιημένο χαρακτήρα του blockchain. Στην περίπτωση χρήσης αλγόριθμου συναίνεσης Proof-of-Stake, οι ανταμοιβές είναι ανάλογες (γραμμικές) με το ποσό του στοιχήματος. Έτσι, δεν παρέχει απολύτως κανένα επιπλέον πλεονέκτημα για συμμετοχή σε μια «mining pool»[2].

Ασφάλεια: Ένα άτομο που επιχειρεί να επιτεθεί σε ένα δίκτυο θα πρέπει να κατέχει το 51% των coins πράγμα που είναι αρκετά ακριβό. Αυτό οδηγεί σε ένα ασφαλές δίκτυο blockchain.

2.7.2.4 Μειονεκτήματα που παρουσιάζει ο αλγόριθμος συναίνεσης POS:

Μεγάλες επικυρώσεις στοιχημάτων: Εάν μια ομάδα υποψηφίων επικύρωσης συνδυαστεί και κατέχει ένα σημαντικό μερίδιο των συνολικών κρυπτονομισμάτων, θα έχουν περισσότερες πιθανότητες να πραγματοποιήσουν την έγκριση μιας συναλλαγής. Οι αυξημένες πιθανότητες οδηγούν σε αυξημένες επιλογές, οι οποίες οδηγούν σε ολοένα και περισσότερα έσοδα, οι οποίες οδηγούν στην κατοχή ενός μεγαλύτερου μεριδίου από το κρυπτονόμισμα. Αυτό μπορεί να προκαλέσει κεντροποίηση του δικτύου με την πάροδο του χρόνου.

Νέα τεχνολογία: Το PoS εξακολουθεί να είναι σχετικά νέο. Η έρευνα βρίσκεται σε εξέλιξη για να βρεθούν ατέλειες, να διορθωθούν και να καταστούν βιώσιμες για ένα ζωντανό δίκτυο με πραγματικές συναλλαγές νομισμάτων.

[2] Με την έννοια mining pool αναφερόμαστε σε μια «δεξαμενή εξόρυξης» που ένα σύνολο ατόμων που πραγματοποιούν εξόρυξη κρυπτονομισμάτων συνδυάζουν τους υπολογιστικούς τους πόρους με ένα δίκτυο για να συμβάλουν στην εξόρυξη ενός νέου Block. Για λεπτομέρειες δείτε: https://www.investopedia.com/terms/m/mining-pool.asp

2.7.3 Αλγόριθμος Συναίνεσης « Delegated Proof of Stake (DPoS)»

- **Θεμελιώδης αρχή**: Οι συμμετέχοντες αναθέτουν την παραγωγή νέων block σε ένα μικρό και σταθερό αριθμό εκλεγμένων ατόμων που επικυρώνουν τις συναλλαγές. Ο ανταγωνισμός είναι υψηλός, αλλά πολύ κερδοφόρος.
- **Απόδοση:** Υψηλή
- **Τεχνολογία κατανομής του περιβάλλοντος του καθολικού δικτύου:** Δημόσιο και Ιδιωτικό Blockchain
- **Τρόπος συναίνεσης:** Πιθανολογικός
- **Παραδείγματα Χρήσης:** EOS, BitShares

Η αλγοριθμική συναίνεση Delegated Proof of Stake (DPoS) επιτρέπει τη δημιουργία block σε υψηλή ταχύτητα και την επεξεργασία περισσότερων συναλλαγών ανά δευτερόλεπτο μειώνοντας τον αριθμό των ατόμων που πραγματοποιούν την επικύρωση τους. Κατά τη διάρκεια της ψηφοφορίας, οι κάτοχοι κρυπτονομισμάτων, επιλέγουν τα άτομα που θα επικυρώσουν τα νέα block. Η στάθμιση με την οποία λαμβάνεται η κάθε ψηφοφορία, ορίζεται από το άθροισμα των περιουσιακών στοιχείων του ψηφοφόρου. Οι κάτοχοι κρυπτονομισμάτων, μπορούν να ψηφίσουν τα άτομα που θα επικυρώσουν την συναλλαγή ανά πάσα χρονική στιγμή. Αυτό καθορίζει την υψηλή ευελιξία του δικτύου συναίνεσης, με αποτέλεσμα εάν η πλειοψηφία των εκτελεστών αποτύχει, η κοινότητα θα ψηφίσει αμέσως για να τους αντικαταστήσει.

Η παραγωγή νέων block γίνεται κάθε 1-2 δευτερόλεπτα. ο πρωτόκολλο αυτό είναι ταχύτερο και πιο δίκαιο σε σύγκριση με το PoS, αφού το άτομο που ορίζεται για να επικυρώνει τις συναλλαγές, αργότερα μοιράζεται τα κρυπτονομίσματα που λαμβάνει ως αμοιβή με τους ψηφοφόρους του. Παρόλα αυτά η επιβεβαίωση των τελικών blocks, εξακολουθεί να βρίσκεται στα χέρια άλλων των μελών του δικτύου.

2.7.4 Αλγόριθμος Συναίνεσης « Proof of Activity (PoA)»

- **Θεμελιώδης αρχή:** ένα hybrid μεταξύ του δικτύου PoW και PoS
- **Απόδοση:** Χαμηλή
- **Τεχνολογία κατανομής του περιβάλλοντος του καθολικού δικτύου:** Δημόσιο
- **Τρόπος συναίνεσης:** Πιθανολογικός
- **Παραδείγματα Χρήσης:** Decred

Η αλγοριθμική συναίνεση Proof-of-Activity (PoA) αποτελεί έναν συνδυασμό των πρωτοκόλλων PoW και του PoS, που σημαίνει ότι οι συμμετέχοντες στην συναίνεση μπορούν να εξορύξουν ή να ορίσουν το μερίδιο τους ανάλογα με τον αριθμό των tokens που κατέχουν στην επικύρωση του νέου block. Έτσι, το πρωτόκολλο PoA παρέχει μια ισορροπία μεταξύ των miners και των μελών του δικτύου.

2.7.5 Αλγόριθμος Συναίνεσης « Proof-of-Location (PoL)»

- **Θεμελιώδης αρχή:** τα beacons[3] χρησιμοποιούνται ως μέσω παρατήρησης ενός κόμβου σε συγχρονισμένη κατάσταση και στη συνέχεια για να επισημάνουν την παρουσία τους με μια προσωρινή σφραγίδα.
- **Απόδοση:** ενδιάμεση
- **Τεχνολογία κατανομής του περιβάλλοντος του καθολικού δικτύου:** Δημόσιο
- **Τρόπος συναίνεσης:** άμεσως
- **Παραδείγματα Χρήσης:** FOAM, Platin.

Το Proof-of-Location (PoL) επιτρέπει στους χρήστες να εξασφαλίσουν μια συγκεκριμένη θέση GPS και έτσι να πιστοποιήσουν τον εαυτό τους στο δίκτυο. Είναι ενδιαφέρον ότι αυτό το πρωτόκολλο blockchain βασίζεται στο BFT beacons[4], το οποίο καταγράφει το γεωγραφικό σημείο και τους χρονικούς δείκτες στο blockchain. Το blockchain αυτό εμποδίζει τις διαταραχές και την απάτη στο σύστημα.

[3] [4] Τα beacons είναι ένας μικρός ραδιοπομπός Bluetooth που μεταδίδει επανειλημμένα ένα μόνο σήμα που μπορούν να δουν άλλες συσκευές. Για λεπτομέρειες δείτε: https://kontakt.io/beacon-basics/what-is-a-beacon/

2.7.6 Αλγόριθμος Συναίνεσης « Proof-of-Importance (PoI)»

- **Θεμελιώδης αρχή:** είναι όπως στο PoS αλλά με επιπλέον ιδιότητες που επηρεάζουν την κατάταξη των συμμετεχόντων
- **Απόδοση:** Υψηλή
- **Τεχνολογία κατανομής του περιβάλλοντος του καθολικού δικτύου:** Δημόσιο
- **Τρόπος συναίνεσης:** Πιθανολογικός
- **Παραδείγματα Χρήσης:** NEM.

Ο αλγόριθμος λειτουργεί σχεδόν όπως το PoS, αλλά περιλαμβάνει τρία συστατικά στοιχεία επιπλέον:

- τον αριθμό των tokens στο λογαριασμό των συμμετεχόντων
- δραστηριότητα συναλλαγών του λογαριασμού των συμμετεχόντων
- τον χρόνο που δαπανά ο κάτοχος του λογαριασμού που συμμετέχει στο δίκτυο

Η πρώτη παράμετρος κατέχει ουσιαστικό ρόλο στην αξιολόγηση για την επαλήθευση των συναλλαγών όπως και στην προηγούμενη περίπτωση. Η δεύτερη και η τρίτη παράμετρος συμβάλλουν μόνο στη δημιουργία της "αξίας" του λογαριασμού. Όσο μικρότερο είναι το άθροισμα των tokens, τόσο ισχυρότερη είναι η επίδραση άλλων παραμέτρων. Συνεπώς, ένας λογαριασμός που τοποθετεί εκατοντάδες χιλιάδες tokens μπορεί να αυξήσει τον συντελεστή σπουδαιότητας (Importance) σχεδόν 3 φορές χάρις στην δραστηριότητά του και την συνεχή παρουσία του στο δίκτυο. Από την άλλη πλευρά, αυτό δεν έχει ιδιαίτερη σημασία για εκείνους που έχουν εκατοντάδες εκατομμύρια tokens.

2.7.7 Αλγόριθμος Συναίνεσης « Proof-of-Elapsed-Time (PoET)»

- **Θεμελιώδης αρχή:** τα μπλοκ δημιουργούνται σε ένα αξιόπιστο περιβάλλον με ίσες περιόδους
- **Απόδοση:** Ενδιάμεση
- **Τεχνολογία κατανομής του περιβάλλοντος του καθολικού δικτύου:** Ιδιωτικό Blockchain με και χωρίς άδεια συμμετοχής
- **Τρόπος συναίνεσης:** Πιθανολογικός
- **Παραδείγματα Χρήσης:** Intel.

Η εταιρεία τεχνολογίας Intel δεν παρέμεινε πίσω και ανέπτυξε το δικό της blockchain πρωτόκολλο που ονομάζεται IntelLedger. Το σύστημα αυτό είναι παρόμοιο με το Proof of Work αλλά χρησιμοποιεί λιγότερη ηλεκτρική ενέργεια για την επιβεβαίωση των blocks. Αντί οι συμμετέχοντες να επιλύουν ένα κρυπτογραφικό παζλ, ο αλγόριθμος λειτουργεί σε ένα περιβάλλον Trusted Execution Environment (TEE) όπως το Intel Software Guard Extensions (SGX). Το πρωτόκολλο PoET εγγυάται ότι τα block παράγονται τυχαία και χωρίς πολύ υψηλές προσπάθειες.

2.7.8 Αλγόριθμος Συναίνεσης « Proof of Authority (PoA)»

- **Θεμελιώδης αρχή:** ημι-κεντρικό blochchain για τις τράπεζες και τις ασφαλιστικές εταιρείες
- **Απόδοση:** υψηλή
- **Τεχνολογία κατανομής του περιβάλλοντος του καθολικού δικτύου:** Δημόσιο, Ιδιωτικό ή κοινοπρακτικό
- **Τρόπος συναίνεσης:** Πιθανολογικός
- **Παραδείγματα Χρήσης:** Kovan, Rinkeby, Giveth, TomoChain, Rublix, Swarm City, Colony, Go Chain.

Η λογική του είναι παρόμοια με το με το PoS και το DPoS,, όπου οι επικυρωτές του PoA εξασφαλίζουν ότι το blockchain και είναι σε θέση να παράγει νέα block. Τα νέα Block στην αλυσίδα του blockchain δημιουργούνται μόνο όταν επιτυγχάνεται Υπερπλειοψηφία από τα άτομα που επικυρώνουν τις συναλλαγές.

Με τον προσδιορισμό των προεπιλεγμένων ατόμων, τότε η συναίνεση του PoA γίνεται κεντροποιημένη. Ως εκ τούτου το PoA είναι κατάλληλο για blockchains και κοινοπραξίες, όπως μια ομάδα τραπεζών ή ασφαλιστικές εταιρείες για την επίτευξη καλύτερης κλιμάκωσης. Οι ταυτότητες όλων των ατόμων που επικυρώνουν τις συναλλαγές είναι δημόσιες και επαληθεύσιμες από οποιοδήποτε τρίτο άτομο το επιθυμεί. Έχοντας σε δημόσια κατάσταση την ταυτότητα τους, τα άτομα που πραγματοποιούν τις επικυρώσεις ενεργούν προς το συμφέρον του δικτύου.

2.7.9 Αλγόριθμος Συναίνεσης « Proof of Burn (PoB)»

- **Θεμελιώδης αρχή:** η καύση ενός εξορυγμένου κρυπτονομίσματος από την διαδικασία PoW για την ανταλλαγή προνομίων εξόρυξης ή coins/tokens ενός εναλλακτικού νομίσματος
- **Απόδοση:** Μέτρια
- **Τεχνολογία κατανομής του περιβάλλοντος του καθολικού δικτύου:** Δημόσιο
- **Τρόπος συναίνεσης:** -
- **Παραδείγματα Χρήσης:** Slimcoin

`Οι miners στέλνουν τα coins σε μια διεύθυνση που δεν ξοδεύονται με τέτοιο τρόπο που ουσιαστικά τα καίουν και δεν μπορούν ούτε να έχουν πρόσβαση ούτε να ξοδευτούν ξανά. Καθώς οι συναλλαγές PoB καταγράφονται στο blockchain, υπάρχει αναμφισβήτητη απόδειξη ότι τα κέρματα είναι απρόσιτα και ο χρήστης ανταμείβεται.

Η ιδέα είναι ότι ο χρήστης επιδεικνύει την προθυμία να υποστεί μια βραχυπρόθεσμη απώλεια για μακροπρόθεσμες επενδύσεις, που αποτελεί προνόμιο του συστήματος. Όσο περισσότερα νομίσματα καίει ένας χρήστης, τόσο μεγαλύτερη είναι η πιθανότητα εξόρυξης του επόμενου τμήματος.

2.7.10 Αλγόριθμος Συναίνεσης « Proof of Capacity (PoC) or Proof of Space (PoS)»

- **Θεμελιώδης αρχή:** Η ποσότητα εργασίας που θα εκτελέσει ένας ανθρακωρύχος εξαρτάται από το ποσό του ελεύθερου χώρου στο δίσκο που αφιερώνεται στη διαδικασία plotting
- **Απόδοση:** Υψηλή και αποτελεσματική
- **Τεχνολογία κατανομής του περιβάλλοντος του καθολικού δικτύου:** Δημόσιο
- **Τρόπος συναίνεσης**: -
- **Παραδείγματα Χρήσης:** Burstcoin και Bitcoin Ore

Το PoC είναι παρόμοιο με το PoW με μια σημαντική διαφορά. Το PoC, αντί να κάνει μια μεγάλη εργασία για να επαληθεύσει κάθε block, η εργασία γίνεται εκ των προτέρων στη διαδικασία που ονομάζεται "plotting". τα αποτελέσματα αυτής της διαδικασίας χρησιμοποιούνται αργότερα για την επαλήθευση κάθε block.

Το plotting είναι η διαδικασία παραγωγής ειδικών αρχείων που ονομάζονται " plot files” τα οποία αποθηκεύουν μεγάλο αριθμό Προϋπολογισμένων κατακερματισμών (precomputed hashes). Η συντομότερη λύση του αλγορίθμου μέσω της διαδικασίας εξόρυξης παρέχει το δικαίωμα να εξορυχθεί το επόμενο block. Το PoC είναι αποτελεσματικό, φθηνό και παρέχει διαμοιρασμό.

2.7.11 Αλγόριθμος Συναίνεσης « Proof-of-Stake-Time (PoST)»

- **Θεμελιώδης αρχή:** Εισάγει ένα μερίδιο χρόνου συμμετοχής, όπου η πιθανότητα αυτής της συμμετοχής αυξάνεται με την πάροδο του χρόνου, ενισχύοντας την ασφάλεια και την αποκέντρωση.
- **Απόδοση:** Υψηλή
- **Τεχνολογία κατανομής του περιβάλλοντος του καθολικού δικτύου:** Δημόσιο
- **Τρόπος συναίνεσης**: -
- **Παραδείγματα Χρήσης:** VeriCoin Blockchain Explorer

Το PoST επιτρέπει έναν σχεδόν άμεσο και δωρεάν τρόπο συναλλαγής σε όλο τον πλανήτη. Είναι ανεξάρτητο από γεωγραφικά σύνορα, έθνη, κυβερνήσεις και τράπεζες. Το PoST διατηρεί την αποτελεσματικότητα του PoS αλγόριθμου συναίνεσης αλλά ταυτόχρονα αυξάνει τον διαμοιρασμό και την ασφάλεια με κάποια πιθανότητα να βρει κάποιος απόδειξη (Proof) και να λάβει ανταμοιβή για αυτό.

Αυτό επιτυγχάνεται μέσω μιας κυκλικής συνάρτησης αποδοχής χρόνου ανάλογης με τα coins που κρατούνται και αντιστοιχούν στην ισχύ του δικτύου. Το μοντέλο αποδοχής χρόνου εγγυάται ότι αυξάνεται ο ανταγωνισμός αλλά και η ευκαιρία να δημιουργηθεί συναίνεση μέσω της απόδειξης (proof).

2.7.12 Αλγόριθμος Συναίνεσης « Proof-of-Brain (PoB)»

- **Θεμελιώδης αρχή:** το πρωτόκολλο επιτρέπει ένα έξυπνο και κοινωνικό νόμισμα για εκδότες και επιχειρήσεις παρόμοιου περιεχομένου
- **Απόδοση:** Υψηλή και γρήγορη
- **Τεχνολογία κατανομής του περιβάλλοντος του καθολικού δικτύου:** Δημόσιο
- **Τρόπος συναίνεσης**: -
- **Παραδείγματα Χρήσης:** Steemit

Το PoB είναι ένα κλιμακωτό πρωτόκολλο blockchain για ανοιχτής πρόσβασης και αμετάβλητο περιεχόμενο που συνοδεύεται από ένα γρήγορο και λιγότερο δαπανηρό ψηφιακό token το STEEM. Το STEEM βοηθά τους ανθρώπους να κερδίζουν χρήματα χρησιμοποιώντας το μυαλό τους. Το STEEM είναι ένα μέσο για τη δημιουργία αδιάκοπα αναπτυσσόμενων κοινοτήτων με μέλη που προσθέτουν αξία μέσω της ενσωματωμένης δομής ανταμοιβών του.

Το PoB είναι μια δημόσια δημοσιευμένη πλατφόρμα που ονομάζεται Steemit από την οποία οποιαδήποτε εφαρμογή στο Διαδίκτυο μπορεί να μοιράζεται δεδομένα με τρόπο που ανταμείβει όσους συμβάλλουν σε αυτό το πολύτιμο περιεχόμενο.

2.7.13 Αλγόριθμος Συναίνεσης «Proof-of-Physical-Address (PoPA)/ Proof-of-Bank-Account (PoBA)»

- **Θεμελιώδης αρχή:** Επαλήθευση ταυτότητας αποκεντροποιημένων εφαρμογών (DApp)
- **Απόδοση:** Υψηλή
- **Τεχνολογία κατανομής του περιβάλλοντος του καθολικού δικτύου:** Ιδιωτικό
- **Τρόπος συναίνεσης:** -
- **Παραδείγματα Χρήσης**: ConsenSys και POA Network

Το Proof of Physical Address (PoPA) είναι μια αποκεντροποιημένη εφαρμογή (Decentralized Application -DApp) που συνδέει ένα πραγματικό φυσικό στοιχείο με την τεχνολογία blockchain. Αυτό βοηθά ιδιαίτερα στην επαλήθευση της ταυτότητας ενός ατόμου. Το PoPA συνδέει τη φυσική διεύθυνση ενός ατόμου με μια διεύθυνση ψηφιακού πορτοφολιού στην οποία ελέγχει το αντίστοιχο ιδιωτικό κλειδί που του αναλογεί.

Κάθε φορά που ένας χρήστης επαληθεύει την κάρτα του στο DApp και το πρωτόκολλο PoPA ανανεώνει το ιστορικό του και «καλεί» το σύμφωνο ERC780 [5] να αποθηκεύσει τον ηλεκτρονικό κωδικό χρήστη ή την διεύθυνση που έχει συνδεθεί ως κεντρικό σημείο αναφοράς επί της blockchain αλυσίδας επί του Ethereum.

[5] Ethereum Claims Registry (ECR) επιτρέπει σε άτομα, έξυπνες συμβάσεις και μηχανήματα να εκδίδουν αξιώσεις το ένα για το ένα το άλλο. Για λεπτομέρειες δείτε: https://github.com/ethereum/EIPs/issues/780

2.7.14 Αλγόριθμος Συναίνεσης « Proof-of-concept (PoC)»

- **Θεμελιώδης αρχή:** Παρουσιάζει την εφαρμοστικότητα οποιουδήποτε blockchain project
- **Απόδοση:** Άγνωστη
- **Τεχνολογία κατανομής του περιβάλλοντος του καθολικού δικτύου:** Ιδιωτικό
- **Τρόπος συναίνεσης**: -
- **Παραδείγματα Χρήσης:** Άγνωστα

Στο αλγόριθμο επιβεβαίωσης Proof of Concept (POC) μπορεί να χρησιμοποιηθεί σε οποιαδήποτε πεδίο συμπεριλαμβανομένων των ιστορικών ψηφοφορίας, της αποθήκευσης εγγραφών, των νομικών εγγράφων κτλ. Ένα δίκτυο POC μπορεί να είναι είτε πρωτότυπο χωρίς να υποστηρίζεται από κάποιον κώδικα είτε ως ελάχιστο βιώσιμο προϊόν (Minimum Viable Product (MVP)). Ένα POC είναι ένα μοντέλο που χρησιμοποιείται για μια εσωτερική οργάνωση για να υπάρχει καλύτερη κατανόηση ενός συγκεκριμένου έργου.

2.8 Το πρόβλημα των διπλών δαπανών (Double spending problem)

2.8.1 Οι διπλές δαπάνες σε ένα blockchain

Σύμφωνα με τους Chiu J., Koeppl T. (2018) λόγω της ψηφιακής φύσης τους τα κρυπτονομίσματα είναι κατάλληλο πεδίο εφαρμογής των διπλών δαπανών (double spending). Η πρόκληση αυτή θέτει βασικό ερώτημα για το πως θα ξεπεραστεί το πρόβλημα αυτό που υπάρχει στον καθημερινό ανταγωνισμό έτσι ώστε να μπορεί να ενημερώνονται σωστά τα Blockchain αλλά και να μην καθυστερούν οι συναλλαγές που συμφωνούνται προς πραγματοποίηση.

Αυτό όμως που οι Abadi J. και Brunnermeier M. ορίζουν ως double spending στο άρθρο τους με τίτλο “Blockchain Economics” (2019) είναι όταν δύο δημόσια μηνύματα δίνουν εντολή για την μεταφορά ενός token από έναν λογαριασμό σε δύο άλλους και δεν είναι πάντα ευδιάκριτο ποιο μήνυμα προηγείται από πιο. Τα δύο αυτά μηνύματα μπορεί να έχουν σταλεί για την μεταφορά του token είτε το ένα πολύ κοντά στο άλλο είτε να μην μπορεί να διακριθεί πιο προηγείται του άλλου. Το πρόβλημα της διάκρισης της αλληλουχίας αυτής της αποστολής της εντολής από τον Α λογαριασμό στον Β ή στον Γ ονομάζεται double spend problem.

Είναι πολύ σημαντικό να επισημάνουμε πως για κάθε κρυπτονόμισμα που βασίζεται στον αλγόριθμο συναίνεσης PoW τα πρωτόκολλα των αρχείων των συναλλαγών δεν μπορούν να είναι αμέσως τα τελικά οπότε μπορεί κάποιο αντισυμβαλλόμενο μέρος σε μια συμφωνία να υποπέσει θύμα εξαπάτησης και να χάσει τα χρήματά του.

Παρακάτω καταγράφονται δυο ιδιαίτερες και πολύ σημαντικές περιπτώσεις που μπορεί να επιτευχθεί το double spending σε έναν αλγόριθμο συναίνεσης Proof of Work (PoW), όπως ανέλυσαν οι Chiu J., Koeppl T. στο άρθρο τους με τίτλο The economics of Cryptocurrencies – Bitcoin and Beyond (2018)

2.8.2 Περιπτώσεις που πραγματοποιείται το double spending

Η πρώτη περίπτωση πραγματοποίησης του **Double spending είναι μέσω της μυστικής εξόρυξης (Double spending secret mining**). Η συγκεκριμένη περίπτωση υφίσταται όταν ένας αγοραστής θέλει να κάνει μια πληρωμή σε έναν πωλητή, πρέπει να στείλει μια εντολή στους Miners για να ενημερώσουν το blockchain με αυτή την συναλλαγή. Αυτό όμως δεν είναι ιδιαίτερα ξεκάθαρο πως ο πωλητής θα λάβει την πληρωμή. Ένας πωλητής μπορεί να εμπλακεί στο secret mining προσπαθώντας να εξορύξει ένα Block στο οποίο οι πληρωμές δεν θα προκύψουν.

Ο πωλητής του προϊόντος από την μεριά του μπορεί να προστατέψει τον εαυτό του από το να λάβει την πληρωμή περιμένοντας να παραδώσει τα αγαθά μέχρι η πληρωμή να καταχωρηθεί στο blockchain. Αλλά σε αρκετές περιπτώσεις η επιβεβαίωση της συναλλαγής αυτής με την εμφάνιση της στο blockchain μπορεί να μην είναι αρκετή. Ένας αγοραστής μπορεί κρυφά να κάνει εξόρυξη ενός διαφορετικού Blockchain που θα το εμφανίσει μερικές περιόδους μετά την παράδοση των αγαθών από τον πωλητή τους και θα αντικαταστήσει το πραγματικό blockchain. Από την στιγμή που το κρυφό Mining επιτύχει, ο αγοραστής κρατά τις πραγματικές αξίες των αγαθών ενώ ο πωλητής μένει με απολύτως τίποτα.

Με το κρυφό mining ο αγοραστής δεν μπορεί να ξοδέψει τα υπόλοιπα κρυπτονομίσματα άλλων εμπλεκόμενων ατόμων καθώς χρειάζεται την ψηφιακή τους υπογραφή. Μπορεί μόνο να αλλάξει τις εντολές πληρωμής της δικής του συναλλαγής αλλά και να αφαιρέσει άλλες εντολές πληρωμής που έχουν εξορυχθεί και επιβεβαιωθεί σε ένα Block.

Η δεύτερη περίπτωση πραγματοποίησης **Double spending** είναι η διπλή δαπάνη **παρά την εμφάνιση μιας συναλλαγής (double spending proof contracts)**. Η συγκεκριμένη περίπτωση είναι το για να πραγματοποιηθεί ένας αγοραστής μπορεί κρυφά να εξορύξει μια εναλλακτική ιστορία συναλλαγής από την πραγματική για να αναιρέσει τις πληρωμές που πραγματοποιήθηκαν αφού έχει παραλάβει τα αγαθά που θέλει.

Αυτό συνεπάγεται πως το άτομο της απατηλής πράξης πρέπει να είναι το πρώτο άτομο που θα λύσει τον αλγόριθμο PoW με $N + 1$ περιόδους συναίνεσης. Σε αυτήν την περίπτωση ο αγοραστής του προϊόντος δεν αναμεταδίδει το νέο Block αμέσως, γι' αυτό κάποιοι άλλοι Miners θα ανανεώσουν το blockchain και θα επιβεβαιώσουν την πληρωμή

στον πωλητή την χρονική στιγμή N. Ο αγοραστής μεταδίδει το μυστικό του εξορυγμένο blockchain μετά την παραλαβή των αγαθών και αφού έχει λύσει $N+1$ περιόδους blocks. Όταν το double spending σαν επίθεση επιτύχει, η πραγματική πληρωμή επιτυγχάνει και ακυρώνεται η προηγούμενη με αυτή που βρίσκεται στην $N+1$ να δοθεί τελικώς στον αγοραστή.

Ένας αγοραστής δηλαδή που δεν είναι πραγματικός αλλά θέλει να εξαπατήσει χρειάζεται να νικήσει την διαδικασία της εξόρυξης με $N+1$ φορές στην σειρά. Όσο ο αριθμός των υστερήσεων μεγαλώνει, το συνολικό PoW που χρειάζεται για να αντιστραφεί η μεταφορά αυξάνεται και γίνεται πιο δαπανηρή για έναν αγοραστή στο να κάνει το double spending σαν πράξη.

Τέλος επειδή το Bitcoin όπως και πολλά κρυπτονομίσματα σε γενικές γραμμές είναι έτσι δομημένα για να αποφεύγουν τις επιθέσεις του double spending. Επειδή η δόμηση του συστήματος των κρυπτονομισμάτων λόγω του αποκεντροποιημένου χαρακτήρα τους οι πωλητές αγαθών περιμένουν για πολλαπλές επιβεβαιώσεις της μεταφοράς των χρημάτων από τους αγοραστές το double spending δεν είναι εύκολο να πραγματοποιηθεί ιδιαίτερα άμα εξορυχθούν αρκετά blocks μετά την περάτωση της συναλλαγής (μεγάλος χρόνος υστέρησης).

Όταν οι πωλητές περιμένουν για πολλαπλές επιβεβαιώσεις μιας συναλλαγής, το να έχουν πέσει σε κάποια απατηλή πράξη μειώνεται πάρα πολύ σαν γεγονός. Παρόλα αυτά να αναφέρουμε πως μια επιτυχημένη πράξη double spending είχε καταγραφεί όταν ο χρόνος υστέρησης ήταν ανεπαρκής. Σύμφωνα με το Bicoinwiki (2016), το Νοέμβριο του 2013 ανακαλύφθηκε πως το GHash.io μια συγκεντρωτική μονάδα εξόρυξης (minning pool), εμφανίστηκε να είναι μπλεγμένη σε επαναλαμβανόμενες απατηλές διαδικασίες πληρωμών σε ένα σίτε συναλλαγών στοιχήματος το BetCoin Dice που δεν περίμενε το σωστό χρονικό διάστημα για την επιβεβαίωση των συναλλαγών.

Αξίζει να αναφερθεί και να επισημανθεί πως η διαδικασία της εξόρυξης (Mining) σε κάθε χρονική περίοδο βασίζεται στην ισορροπία Nash (Nash equilibrium). Όσο το Mining τείνει στο άπειρο η ουσιαστική αξία σαν ανταμοιβή που λαμβάνουν οι Miners είναι μηδέν και η συνολική υπολογιστική δύναμη που χρησιμοποιούν εξαφανίζει όλα τα κέρδη της διαδικασίας για double spending να μετατρέπεται σε όλο και πιο δύσκολο και δαπανηρό.

2.9 Συμπεράσματα Κεφαλαίου

Ένα πρωτόκολλο σε γενικές γραμμές είναι ένα θεμελιώδες επίπεδο κώδικα που ορίζει τον τρόπο δηλαδή τους κανόνες και τις διαδικασίες με τους οποίους θα μεταφέρονται δεδομένα μεταξύ δύο ή περισσότερων ηλεκτρονικών συσκευών. Για παράδειγμα το Facebook, το Amazon, το Twitter, το Google, το Netflix, οι τραπεζικοί ιστότοποι, οι ιστοχώροι ειδήσεων αλλά και σχεδόν κάθε ιστοσελίδα που χρησιμοποιούμε «τρέχει» σε ένα από αυτά τα πρωτόκολλα διαδικτύου.

Τα πρωτόκολλα δεν περιορίζονται μόνο στο διαδίκτυο αλλά έχουν και πεδίο εφαρμογής και στα κρυπτονομίσματα μέσω του blockchain τους. Επειδή όλα τα blockchains δεν είναι ίδια και δεν έχουν την ίδια δομή, ο τρόπος λειτουργίας τους καθορίζεται από το πρωτόκολλο που ακολουθούν. Επειδή ένα blockchain είναι ένα καθολικό βιβλίο που αποθηκεύει και καταγράφει τι ακριβώς πληροφορίες και συναλλαγές έχουν πραγματοποιηθεί με κατανεμημένο τρόπο Peer- 2- Peer προκειμένου όμως να μπορέσει να λειτουργήσει σωστά και ομαλά αυτή η ιδέα χρειάζονται πρωτόκολλα για ακολουθούν οι συμμετέχοντες στο δίκτυο, για να διασφαλίζεται η σωστή και έγκυρη καταγραφή των συναλλαγών και να διατηρείται η συναίνεση και η λειτουργία στο δίκτυο των blocks. Αυτοί οι κανόνες που διέπουν και ορίζουν την λειτουργία ενός δικτύου blockchain ονομάζονται πρωτόκολλο του Blockchain και ουσιαστικά είναι με απλά λόγια οι κοινοί κανόνες επικοινωνίας των συσκευών δηλαδή των ατόμων που συμμετέχουν και χρειάζεται το δίκτυο για να λειτουργήσει. Το λειτουργίας ενός blockchain βρίσκεται στο Genesis Block και δίνει ζωή στις εφαρμογές που βρίσκονται πάνω του παρέχοντας ασφάλεια σε μια ποικιλία υπηρεσιών που εξυπηρετεί κάθε διαφορετικό blockchain καθώς εξυπηρετούν διαφορετικούς σκοπούς και στόχους. Για παράδειγμα ένα κάθε κρυπτονόμισμα που χρησιμοποιεί διαφορετικό blockchain, όπως το Bitcoin, το Ethereum, το XRP έχει το δικό του ξεχωριστό πρωτόκολλο λειτουργίας προσδίδοντας αξία για εκείνο.

Εκτός από το πρωτόκολλο λειτουργίας σε ένα Blockchain υπάρχουν και οι αλγόριθμοι συναίνεσης. Η συναίνεση (Consensus) σαν έννοια συνδέεται με ένα σύνολο κανόνων και ρυθμίσεων για την πραγματοποίηση των λειτουργιών του blockchain. Αποτελεί ένα είδος συμφωνίας που ικανοποιεί όλες τις πλευρές που συμμετέχουν σε ένα blockchain και είναι ο μηχανισμός μέσω του οποίου ένα δίκτυο blockchain φτάνει σε συμφωνία. Ουσιαστικά οι αλγόριθμοι της συναίνεσης διαβεβαιώσουν ότι ακολουθούνται

οι κανόνες πρωτοκόλλου και εγγυώνται ότι όλες οι συναλλαγές πραγματοποιούνται με έναν βέβαιο τρόπο. Στο πλαίσιο των κρυπτονομισμάτων οι αλγόριθμοι συναίνεσης είναι υπεύθυνοι για τη διατήρηση της ακεραιότητας, της ασφάλειας και της χρησιμοποίησης των tokens μόνο μια φορά σε κάθε συναλλαγή. Υπάρχουν διάφοροι τύποι αλγόριθμων συναίνεσης με τους πιο συνηθισμένους να είναι ο PoW και ο PoS. Ο καθένας έχει τα δικά του πλεονεκτήματα και μειονεκτήματα όταν προσπαθεί να εξισορροπήσει την ασφάλεια μαζί με την λειτουργικότητα και την κλιμάκωση στο δίκτυο.

Ενώ το πρωτόκολλο και ο αλγόριθμος χρησιμοποιούνται εναλλακτικά πολλές φορές, δεν εκφράζουν το ίδιο πράγμα. Η ειδοποιός διαφορά μεταξύ τους είναι πως το πρωτόκολλο σχετίζεται με τους κύριους κανόνες ενός blockchain ενώ ο αλγόριθμος συναίνεσης με τον μηχανισμό μέσω του οποίου θα ακολουθούνται αυτοί οι κανόνες. Δηλαδή ενώ το πρωτόκολλο καθορίζει ποιοι είναι οι κανόνες, ο αλγόριθμος λέει στο σύστημα τι μέτρα πρέπει να πάρει για να συμμορφωθεί με αυτούς τους κανόνες και να παράγει τα επιθυμητά αποτελέσματα.

Τέλος όσον αφορά το πρόβλημα των διπλών δαπανών (Double spending) αυτό μπορεί να υπάρξει όταν δύο δημόσια μηνύματα δίνουν εντολή για την μεταφορά ενός token από έναν λογαριασμό σε δύο άλλους και δεν είναι πάντα ευδιάκριτο ποιο μήνυμα προηγείται από πιο. Τα δύο αυτά μηνύματα μπορεί να έχουν σταλεί για την μεταφορά του token είτε το ένα πολύ κοντά στο άλλο είτε να μην μπορεί να διακριθεί πιο προηγείται του άλλου. Το πρόβλημα της διάκρισης της αλληλουχίας αυτής της αποστολής της εντολής από τον Α λογαριασμό στον Β ή στον Γ ονομάζεται double spend problem. Οι πιο συνηθισμένοι τρόποι που μπορεί να πραγματοποιηθεί το Double spending είναι μέσω της μυστικής εξόρυξης αλλά και μετά την εμφάνιση μιας συναλλαγής

<u>ΚΕΦΑΛΑΙΟ 3:</u> Διάκριση και ανάλυση δημόσιων, ιδιωτικών blockchain, τα έξυπνα συμβόλαια (Smart Contracts) και το blockchain στην καθημερινότητά μας

3.1 Εισαγωγή Κεφαλαίου

Το τρίτο κεφάλαιο της διπλωματικής εργασίας στοχεύει αρχικώς να γίνουν κατανοητές οι διαφορές ανάμεσα στα ιδιωτικά και τα δημόσια Blockchain, να αναλυθούν τα έξυπνα συμβόλαια (Smart Contracts) τα οποία εφαρμόζονται μέσω του Blockchain και πλέον αρχίζουν να αποτελούν κομμάτι της καθημερινότητας μας αλλά και να εξετάσουμε περιπτώσεις που ήδη επιχειρήσεις εφαρμόζουν το Blockchain τις δραστηριότητες τους. .

Αναλυτικότερα, όταν αναφερόμαστε σε ένα blockchain οφείλουμε να το διαχωρίζουμε ανάλογα με το είδος του καθώς υπάρχουν πολλοί διαφορετικοί τύποι που μπορεί να υπάγεται. Συνήθως μπορεί να υπάρχουν αναφορές για το εάν είναι δημόσια (public) ή ιδιωτικά (Private) αλλά και εάν είναι ανοιχτού (open) ή κλειστού (close) τύπου. Παρακάτω λοιπόν ακολουθεί η καταγραφή και ανάλυση αυτών των διαφορετικών τύπων που μπορούμε να συναντήσουμε αλλά και τι συνδυασμοί μπορούν να υπάρξουν από αυτούς.

Στην συνέχεια του κεφαλαίου επειδή η φύση της τεχνολογίας Blockchain βοηθάει στην σύναψη συμβολαίων που πιθανώς πριν να ήταν δύσκολο να πραγματοποιηθούν, δίνεται έμφαση και αναλύεται η περίπτωση των έξυπνων συμβολαίων ή έξυπνών συμβάσεων (smart contracts). Στόχος είναι να γίνει κατανοητό πως τα blockchains δεν είναι απλώς μια τεχνολογία βάσης δεδομένων που μειώνει το κόστος διακράτησης και διαμοιρασμού των δεδομένων αλλά έχει βαθύτερη οικονομική εφαρμογή. Αναλυτικότερα γίνεται η ανάλυση των smart contracts, ο τρόπος που μπορούν να οδηγήσουν σε έμπιστες συναλλαγές, πως μπορούν να εφαρμοστούν στο εμπόριο και στις εμπορικές χρηματοδοτήσεις αλλά και πόσο εφικτό είναι να χρησιμοποιούνται από τις κεντρικές τράπεζες σε χρηματοοικονομικές υπηρεσίες και συναλλαγές.

Ενώ τέλος ακολουθεί η καταγραφή κάποιων από τις μεγαλύτερες εταιρειες παγκοσμίως που χρησιμοποιούν την τεχνολογία του Blockchain στις δραστηριότητες τους

βλέποντας μερικά παραδείγματα από τον τραπεζικός και χρηματοοικονομικό τομέα, την εφοδιαστική αλυσίδα, την ιατροφαρμακευτική περίθαλψη, την ασφάλιση, τον κλάδο της ενέργειας, το εμπόριο, το Internet of Thinks (IoT), τα ταξίδια, τα ακίνητα και τον κυβερνητικό τομέα.

3.2 Διάκριση και ανάλυση δημόσιων και ιδιωτικών blockchain

3.2.1 Δημόσιο Blockchain (Public Blockchain)

Όταν μιλάμε για δημόσια (public) blockchain αυτό που οι περισσότεροι άνθρωποι αναφέρονται είναι για ένα δημόσιο ανοικτού (open) τύπου blockchain αλλά μπορεί να υπάρξει και δημόσιο κλειστού (closed) τύπου Blockchain. Όσον αφορά το δημόσιο ανοικτού τύπου σε αυτό το Blockchain μπορεί να συμμετέχει ο οποιοσδήποτε χωρίς άδεια εισόδου (permissionless) γράφοντας δεδομένα και αλλά και διαβάζοντας τα δεδομένα αυτά. Αντιθέτως στις δημόσιες πλατφόρμες κλειστού τύπου μπορεί ο οποιοσδήποτε να εισέλθει σε αυτές αλλά δεν μπορεί να διαβάσει τα δεδομένα αυτά.

Τα δημόσια blockchains είναι αποκεντροποιημένα και κανένας δεν μπορεί να έχει έλεγχο του δικτύου τους, καθώς διατηρείται η ασφάλεια διότι τα δεδομένα τους δεν μπορούν να αλλάξουν από την στιγμή που επιβεβαιωθούν σε αυτό, προστατεύοντας παράλληλα και την ανωνυμία. Οι δημόσιες ανοιχτές πλατφόρμες blockchain όπως του Bitcoin, του Ethereum, του Litecoin είναι αυτές που λέμε πλατφόρμες blockchain χωρίς άδεια εισόδου πράγμα που σημαίνει ότι προσπαθούν πραγματικά να αυξήσουν και να προστατεύσουν την ανωνυμία του χρήστη. Υπάρχει μια αντίληψη ότι αυτές οι πλατφόρμες όπως το Ethereum δεν μπορούν να χρησιμοποιηθούν για την κατασκευή σεναρίων ή για τον έλεγχο της πρόσβασης στα δεδομένα. Η αλήθεια είναι ότι μπορούν, απλά δεν δίνουν όλα τα ενσωματωμένα εργαλεία που μπορεί να βρούμε σε μια ιδιωτική ή με άδεια εισόδου πλατφόρμα blockchain. (Maisie Borrows, Eleonora Harwich, Luke Heselwood, The future of public service identity: blockchain, (2017), Demiro Massessi, Public Vs Private Blockchain In A Nutshell, (2018))

Πολύ σημαντικό είναι οι ανοιχτές δημόσιες πλατφόρμες να εναπόκειται στις ανάγκες σας τόσο με βάση την αρχιτεκτονική τους όσο και με τον προγραμματισμό του μοντέλου αδειοδότησης. Σε γενικές γραμμές εάν δεν γνωρίζουμε ποιος θα είναι ο τελικός

χρήστης της πλατφόρμας, δεν μπορούμε να δημιουργήσουμε μια με άδεια πρόσβασης ή πρόσβαση ανάλογα με τον ρόλο που θα έχουν ή να ελέγξουμε τα δεδομένα που θα μπορούν να διαβάσουν ή να γράψουν. Γι αυτό σε πολλές περιπτώσεις βλέπουμε κρυπτονομίσματα που είναι βασισμένα σε δημόσιες πλατφόρμες blockchain γιατί η ανωνυμία είναι ένα από τα κύρια πλεονεκτήματα των κρυπτονομισμάτων. Για παράδειγμα εάν ένας χρήστης έχει ένα νόμισμα ή κάποιο περιουσιακό στοιχείο με αξία θα πρέπει να μπορεί να το ανταλλάξει ή να το ξοδέψει, κάνοντας ότι επιθυμεί με αυτό. Επειδή όλοι οι χρήστες του πρέπει να έχουν ίδια δικαιώματα, τότε το περιουσιακό στοιχείο αυτό υπάγεται σε ένα δημόσιο blockchain.

Στο δημόσιο Blockchain, πρέπει να ελέγχουμε το κίνητρο για καλή συμπεριφορά των συμμετεχόντων καθώς δεν γνωρίζουμε ποιοι είναι οι χρήστες. Βασιζόμαστε στα κίνητρα της οικονομίας και της θεωρίας παιγνίων για να διασφαλίσουμε ότι όλοι στο σύστημα συμπεριφέρονται ειλικρινά και σύμφωνα με τους κανόνες που ορίζονται από το εκάστοτε πρωτόκολλο λειτουργίας. Δημιουργούμε καταστάσεις μέσω της ομαδικής συναίνεσης, μέσω της οποίας οι τίμιοι συμμετέχοντες επιβραβεύονται οικονομικά, όπου οι μη τίμιοι υπάγονται μόνο στο κόστος εργασία τους χωρίς να έχουν δυνατότητα ανάκτησης αυτού του κόστους.

Ακόμη να αναφέρουμε ενδεικτικά πως ένα δημόσιο ανοιχτού τύπου Blockchain συνήθως υποστηρίζει κρυπτονομίσματα, στοιχηματισμό (betting), αλλά και video games. Ενώ ένα δημόσιο κλειστού τύπου blockchain συνήθως υποστηρίζει μια ψηφοφορία ή τα αρχεία της. (World Energy Council, The Developing Role of Blockchain (White Paper version 10.0), (2018), PwC.com, Blockchain a catalyst for new approaches in insurance, (2017))

Τέλος ακολουθούν επιγραμματικά κάποια από τα πλεονεκτήματα που παρουσιάζουν τα δημόσια blockchain και τα έχουν ωθήσει στην ευρεία αποδοχή τους και προτίμηση τους από πολλά άτομα παγκοσμίως.

- **Ανοιχτά τόσο για γραφή όσο και για ανάγνωση:** Οποιοσδήποτε μπορεί να συμμετέχει και να υποβάλει τις συναλλαγές στο blockchain, όπως είναι τα παραδείγματα του Ethereum ή του Bitcoin
- **Τα καθολικά των συναλλαγών είναι διαμοιρασμένα:** Η βάση δεδομένων δεν είναι κεντροποιημένη όπως συμβαίνει με έναν server και

όλοι οι κόμβοι του blockchain συμμετέχουν στην επικύρωση της συναλλαγής.

- **Αμετάβλητα:** Όταν γράφεται κάτι στο blockchain, δεν μπορεί να αλλάξει.
- **Ασφάλεια χάρις το 51%:** Στην περίπτωση των Blockchain που χρησιμοποιούν αλγόριθμο συναίνεσης PoW όπως για παράδειγμα το Bitcoin, η απόκτηση του 51% της ισχύς του δικτύου είναι συνήθως αδύνατη και αποτρέπεται πράξεις «διπλής δαπάνης» (double spending) καθώς και άλλων κακόβουλων πράξεων που σχετίζονται με την επιβεβαίωση των συναλλαγών

3.2.2 Ιδιωτικό Blockchain (Private Blockchain)

Αντιθέτως με τα δημόσια Blockchain υπάρχουν τα ιδιωτικά (private) Blockchain που λειτουργούν με άδεια εισόδου (permission) και έχουν θέσει περιορισμούς για το ποιος επιτρέπεται να συμμετέχει στο δίκτυο αλλά και τι συναλλαγές να πραγματοποιεί. Τα ιδιωτικά blockchains μπορούν να παρομοιαστούν με τις κατανεμημένες βάσεις δεδομένων που ήδη υπάρχουν και χρησιμοποιούνται από τις επιχειρήσεις (Catalini C., Gans J. (2016). Τα ιδιωτικά Blockchain έχουν την δυνατότητα και αυτά να χωριστούν σε κλειστού και ανοιχτού τύπου. Στις περισσότερες όμως περιπτώσεις αναφερόμαστε σε ιδιωτικού και κλειστού τύπου στα οποία θέλουμε να ελέγξουμε ποιος μπορεί να γράψει σε αυτό και να διαβάσει από αυτό δεδομένα. (Laura Shiff, Public vs Private Blockchains: What's the Difference?, (2018)).

Για να γίνει αυτό, το πρώτο βήμα είναι η ταυτότητα των συμμετεχόντων, δηλαδή ας σκεφτούμε ένα Blockchain που από την αρχή γνωρίζει ποιοι είναι μέρος του δικτύου και ποιος είναι ο χρήστης. Σε αντίθετη περίπτωση γίνεται δύσκολο, αν όχι αδύνατο, να καθορίσουμε κανόνες σχετικά με τα δεδομένα που μπορούν να καταγραφούν και να αντληθούν στο καθολικό.

Τις περισσότερες φορές, τα ιδιωτικά blockchains τείνουν να έρχονται με εργαλεία διαχείρισης ταυτότητας ή με αρχιτεκτονική, όπου μπορείτε να συνδέσετε τον δικό σας τρόπο διαχείρισης της ταυτότητας σας. Αυτή είναι η ιδέα πίσω από τα ιδιωτικά blockchains. Όλα αρχίζουν με την κατανόηση του ποιος είναι ο χρήστης, διότι μόλις γίνει κατανοητό αυτό, μπορούμε να προσδιορίσουμε τον ρόλο που έχει και μπορούμε να

χρησιμοποιήσουμε αυτόν τον ρόλο για να καθορίσουμε ποιες πληροφορίες θα πρέπει ή δεν πρέπει να έχει πρόσβαση. Και αυτό είναι πολύ διαφορετικό από μια δημόσια πλατφόρμα όπως το Ethereum που όπως είπαμε προηγουμένως, από τον σχεδιασμό τους, δεν γνωρίζουν ποιος είναι ο χρήστης και προσπαθούν να προστατεύσουν και να μεγιστοποιήσουν την ανωνυμία. Παραδείγματα ιδιωτικών blockchain είναι το Hyperledger, το Hashgraph, το Corda, κλπ. (Codefirst.co.uk, Public vs Private Blockchain, (2019).

Στο ιδιωτικό Blockchain, συνήθως δεν ελέγχουμε το κίνητρο για καλή συμπεριφορά των συμμετεχόντων καθώς βασιζόμαστε στο γεγονός ότι γνωρίζουμε ποιος είναι ο χρήστης. Έτσι, σε ένα εταιρικό σενάριο με ένα Blockchain επειδή γνωρίζουμε ποια άτομα συμμετέχουν, με ποια οργάνωση ή ποια άτομα συνδέονται και ποιος είναι ο ρόλος τους, υποθέτουμε πως θα συμπεριφέρονται δίκαια και σωστά χωρίς να αποκλίνουν καθώς θα έχουν συνέπειες σε περίπτωση απόκλισης. (errna.com, Private, Public, and Consortium Blockchains, (2018))

Ακόμη οι λόγοι που οδηγούν τις επιχειρήσεις να χρησιμοποιούν ιδιωτικά blockchain είναι επειδή πρέπει να εξασφαλίσουν κάποιο επίπεδο ασφάλειας, ιδιωτικότητας, συμμόρφωσης, απόδοσης και πολλών άλλων ιδιοτήτων που προσφέρονται από αυτά. Οι συναλλαγές επεξεργάζονται μόνο από επιλεγμένους κόμβους στο blockchain και διεκπεραιώνονται με απόδοση και ταχύτητα έναντι χιλιάδων κόμβων στην περίπτωση ενός δημόσιου δικτύου όπως του Ethereum που χρειάζονται παραπάνω χρόνο και είναι ορατές σε όλους τους κόμβους που έχουν πρόσβαση στο καθολικό. Aziz, PUBLIC VS PRIVATE BLOCKCHAIN: WHAT'S THE DIFFERENCE?,(2020).

Επίσης να αναφέρουμε ενδεικτικά πως ένα ιδιωτικό κλειστού τύπου Blockchain συνήθως υποστηρίζει εφαρμογές του κατασκευαστικού κλάδου, της δημόσιας ασφάλειας, του στρατού, του κράτους για την φορολογία αλλά και θέματα επιβολής του νόμου. Ενώ ένα ιδιωτικό ανοιχτού τύπου blockchain συνήθως εφαρμόζεται σε θέματα εφοδιαστικής αλυσίδας, σε κυβερνητικά οικονομικά αρχεία, εταιρικές οικονομικές εκθέσεις κλπ. (Maisie Borrows, Eleonora Harwich, Luke Heselwood, The future of public service identity: blockchain, (2017))

Τέλος ακολουθούν επιγραμματικά κάποια από τα πλεονεκτήματα που παρουσιάζουν τα ιδιωτικά blockchain και τα έχουν ωθήσει στο να επιλέγονται τόσο από άτομα όσο και από επιχειρήσεις σε παγκόσμιο επίπεδο.

- **Κατάλληλα για επιχειρήσεις:** με την χρήση των ιδιωτικών Blockchain οι επιχειρήσεις ελέγχουν τους πόρους της αλλά και την πρόσβαση σε αυτό από τις ομάδες ενδιαφέροντος.
- **Ταχύτερες συναλλαγές:** Όταν γίνεται διανομή της πληροφόρησης σε τοπικό επίπεδο συγκεκριμένων ατόμων που συμμετέχουν έχουμε λιγότερους κόμβους για να συμμετάσχουν στο καθολικό άρα και η απόδοση του δικτύου είναι ταχύτερη.
- **Καλύτερη κλιμάκωση και συμμόρφωση:** Η δυνατότητα προσθήκης κόμβων και υπηρεσιών κατόπιν αιτήματος μπορεί να προσφέρει μεγάλο πλεονέκτημα στην επιχείρηση αλλά και καλύτερα επίπεδα ελέγχου των υποδομών.
- **Η Συναίνεση γίνεται πιο αποτελεσματική:** Οι επιχειρησιακές ή οι ιδιωτικές αλυσίδες blockchain έχουν λιγότερους κόμβους και συνήθως έχουν διαφορετικό αλγόριθμο συναίνεσης προσθέτοντας μεγαλύτερα επίπεδα αποτελεσματικότητας.

3.3 Blockchain, έξυπνα συμβόλαια (Smart Contracts) και εφαρμογές

Οι οικονομικές συναλλαγές που συνεπάγονται με διαμοιρασμό πληροφοριών που συνδέονται με αποκεντροποιημένη συναίνεση είναι ιδιαίτερα ενδιαφέρουσες τόσο από πρακτικής όσο και από την θεμελιώδη πλευρά. Στον χώρο του Blockchain για παράδειγμα στο Bitcoin η συναίνεση επιτυγχάνεται με την διατήρηση σε δημόσια πρόσβαση όλων των αρχείων και όλων των πληροφοριών. Φυσικά αυτό από την πλευρά των χρηματοπιστωτικών ιδρυμάτων δεν μπορεί να επιτευχθεί καθώς υπάρχει η ευαισθησία των πληροφοριών σε άτομα που δεν είναι συνδεδεμένα με αυτές. Παρακάτω ακολουθούν παραδείγματα που γίνεται κατανοητή η χρήση του Blockchain και των smart contracts αρχίζοντας από απλές εφαρμογές τους αλλά και πιο περίπλοκες με κατανοητά παραδείγματα από τον κόσμο σήμερα, διαπιστώνοντας την κερδοφορία που μπορεί να έχουμε τόσο από το χαμηλότερο κόστος επιβεβαίωσης όσο και από το χαμηλό κόστους χρήσης του δικτύου. ((Lin William Cong, Zhiguo He (2018), Catalini C., Gans J. (2016))

3.3.1Τι είναι τα Smart Contracts

Σύμφωνα με τους Lin William Cong, Zhiguo He (2018), στο άρθρο τους με τίτλο “Blockchain Disruption and Smart Contracts”, τα Smart Contracts αρχικά οραματίστηκαν το 1994 από τον Szabo (Tapscott and Tapscott 2016) και είναι ένα υπολογιστικό πρωτόκολλο συναλλαγών που εκτελείται σε όρους ψηφιακού συμβολαίου. Στόχος τους είναι να ικανοποιήσει συνθήκες κοινές μεταξύ επαφών όπως είναι οι πληρωμές, οι δεσμεύσεις, οι επιβολές αλλά και να μειώνει τις κακεντρέχειες και την ανάγκη κεντρικής αρχής ελέγχου. Σκοπός είναι να μειωθούν οι απάτες, τα κόστη που επιβάλλονται και τα άλλα κόστη συναλλαγών. Η λειτουργικότητα τους είναι ξεκάθαρη, δηλαδή λειτουργούν ως αμοιβαία συμβόλαια υπό συνθήκες ομοφωνίας και αποκεντροποιημένου αλγορίθμου χαμηλού κόστους.

Η χρήση τους μπορεί να αυξήσει την τεχνολογία του Blockchain τόσο στην συμβατότητα, στην εκτελεστικότητα και στην διευκόλυνση της ανταλλαγής χρημάτων, οικημάτων, μετοχών αλλά και υπηρεσιών καθώς και οτιδήποτε άλλο έχει αξία μέσω αλγορίθμων και μπορεί να γίνει με αυτοματοποιημένο τρόπο. Για παράδειγμα μπορούν

να είναι χρήσιμα και σε κεντροποιημένες συνθήκες όπως είναι η περίπτωση της Γεωργίας με τις υπηρεσίες υποθηκοφυλακίου.[6]

Οι εφαρμογές της τεχνολογίας του blockchain Και των smart contract είναι αρκετές και ξεπερνούν ακόμα και την Fintech βιομηχανία. Ο Bartoletti Και Pompianu το 2017 στην έρευνα τους ανέλυσαν 834 εφαρμογές smart contracts που υφίστανται στο bitcoin και στο Ethereum και είδαν πως χωρίζονται σε πέντε κύριες κατηγορίες εφαρμογής. Στο χρηματοοικονομικό κομμάτι (finance), στο συμβοαλιογραφικο (notary), στα παιχνίδια (games), στα ψηφιακά πορτοφόλια (wallets), και στα θέματα βιβλιοθήκης (library)

Η ευκολία που προσφέρουν οι smart contracts στις αυτοματοποιημένες συναλλαγές και μεταφορές εμφανίζεται ιδιαιτέρως στις χρηματοοικονομικές υπηρεσίες και στο εμπόριο.

3.3.2 Smart Contracts και έμπιστες συναλλαγές

Τα Smart Contracts μπορούν να αποτελέσουν εξαιρετικό πεδίο για την πραγματοποίηση έμπιστων συναλλαγών μεταξύ δύο αντισυμβαλλόμενων ατόμων. Ας υποθέσουμε λοιπόν πως το Άτομο 1 στο Σικάγο και το Άτομο 2 στην Αφρική θέλουν να κάνουν μια συναλλαγή και ο πρώτος θέλει να πληρώσει το Άτομο 2 αλλά ανησυχεί τόσο για το εάν το Άτομο 2 είναι ο αληθινός όσο και αν οι πληροφορίες που του δίνει για την τράπεζα της μεταφοράς των χρημάτων είναι πραγματικές. Φυσικά εάν και οι δυο τράπεζες είναι στο σύστημα συναλλαγών Swift τότε μειώνεται ο κίνδυνος απάτης αλλά παρόλα αυτά το Άτομο 2 μπορεί να έχει ζητήσει η τράπεζα να βρίσκεται στο σύστημα συναλλαγών και το χρηματοπιστωτικό ίδρυμα να βρίσκεται υπό Χρεωκοπία (bankrupt) ή εξαπάτηση των πιστούχων και να χρειάζεται μεγάλο χρονικό διάστημα να διαπιστωθεί. Το ίδιο κανονικά πρέπει να γίνει και από την πλευρά της τράπεζας για τον λογαριασμό του Ατόμου 2 πριν εγκρίνει την συναλλαγή. Φυσικά ας μην ξεχνάμε πως μπορεί το Άτομο 1 να πρέπει να αντιμετωπίσει το πρόβλημα υψηλής συναλλαγματικής ισοτιμίας ή να πρέπει να περιμένει μερικές μέρες για την ολοκλήρωση της συναλλαγής και να επιμερίζεται με επιπλέον κόστος. Αυτή η ανησυχία μεγεθύνεται με τις ψηφιακές συναλλαγές όπου το πρόβλημα του

[6] Για λεπτομέρειες δείτε: https://agenda.ge/en/news/2018/396

double spending δηλαδή της χρησιμοποίησης ενός ψηφιακού νομίσματος παραπάνω από μια φορά είναι εφικτή. (Lin William Cong, Zhiguo He (2018)

Το Bitcoin λοιπόν αποτέλεσε το πρώτο νόμισμα ψηφιακής μορφής που δημιουργήθηκε και έδωσε την λύση στο θέμα του double spending. Στην παραπάνω περίπτωση, το bitcoin είναι κατάλληλο για τέτοιου είδους συναλλαγές καθώς επιτρέπει σε άτομα να έρχονται σε ανώνυμη επαφή με peer to peer τρόπο που είναι ασφαλής και χρονικά σταθερός (time stamped) αλλά και τους miners να επιβεβαιώνουν την συναλλαγή και τα στοιχεία που βρίσκονται δημόσια. Για τον λόγο αυτό το Άτομο 1 και το Άτομο 2 με την χρήση Bitcoins θα μπορούν να κάνουν την συναλλαγή άμεσα.

Να αναφέρουμε βέβαια πως επειδή το Bitcoin χρησιμοποιεί το σύστημα συναίνεσης αλγορίθμου PoW το οποίο είναι ιδιαίτερα δαπανηρό καθώς πρέπει οι miners να λύσουν ιδιαίτερα δύσκολα υπολογιστικά προβλήματα και έχει περιορισμένη χωρητικότητα το κάνει ακατάλληλο για μεγάλο όγκο χρηματοοικονομικών συναλλαγών. Φυσικά υπάρχουν και επεκτάσεις ή άλλες πλατφόρμες blockchain για να εξυπηρετούν καλύτερα τις ανάγκες των συναλλαγών. Για παράδειγμα άλλου είδους πλατφόρμες είναι η Lighting που είναι βασισμένη βέβαια στο blockchain του Bitcoin αλλά και η Stellar που χρησιμοποιεί διαφορετικό blockchain και μπορούν να βοηθήσουν να αυξηθεί η χωρητικότητα σε τοπικά κανάλια διανομής πληροφοριών αλλά και σε πολλαπλών υπογραφών λογαριασμούς.

Οι παραπάνω αναφορές blockchains από την φύση τους δεν είναι και οι πλέον κατάλληλες για την δημιουργία Smart Contracts, χωρίς αυτό να σημαίνει πως δεν μπορούν να τις υποστηρίξουν. Για τον λόγο αυτό το Ethereum, το οποίο είναι η 2η μεγαλύτερη σε κεφαλαιοποίηση πλατφόρμα Blockchain μετά του Bitcoin επιτρέπει περίπλοκου είδους συναίνεση μέσω της χρήσης της γλώσσας προγραμματισμού Turing (1937) η οποία παρέχει την αρχιτεκτονική της εφαρμογής των Smart Contracts. (Buterin 2014). Στο Blockchain του Ethereum, οι εθελοντές που συμμετέχουν ονομάζονται Ether Miners και διατηρούν την αποκεντροποιημένη συναίνεση των αρχείων των καταστάσεων και άλλα και άλλα άτομα που αλληλοεπιδρούν εφαρμόζουν την συναίνεση σε όρους συμβολαίου. Επιπλέον εφαρμογές όπως το Monax και το Phi (String Lab) που χτίστηκαν πάνω στην πλατφόρμα του Ethereum εμπλουτίζουν και αξιοποιούν με τον καλύτερο τρόπο τις εφαρμογές των Smart Contracts και όχι μόνο.

Επίσης να αναφέρουμε πως οι παραδοσιακοί παίχτες στην χρηματοπιστωτική βιομηχανία είναι ιδιαιτέρως ενεργοί στο να υιοθετήσουν το blockchain και την τεχνολογία του για να επιλύσουν προβλήματα πληρωμών. Ιδιαιτέρως το Ripple που δημιουργήθηκε το 2012 παρέχει παγκόσμιες διασυνοριακές οικονομικές συναλλαγές σε πραγματικό χρόνο. Έχει ιδιαιτέρως υιοθετηθεί από σημαντικές τράπεζες και δίκτυα πληρωμών ως η κύρια τεχνολογία τους. Η αποκεντροποιημένη συναίνεση των επιβεβαιωμένων κόμβων γίνεται μέσω του πρωτόκολλου RTXP, μιας επαναλαμβανόμενης διαδικασίας εναλλακτικής του PoW συστήματος στην οποία οι συναλλαγές μεταδίδονται αμέσως στο ιστορικό του δικτύου όταν επέλθει η συμφωνία. Οι ψηφιακές μεταφορές είναι αυτοματοποιημένες μέσω της ηλεκτρονικής ένωσης με τους τραπεζικούς λογαριασμούς ή με την χρήση του κρυπτονομίσματος που είναι συνδεδεμένο με αυτό το Blockchain, το Ripple XRP.

Οπότε σύμφωνα με τα παραπάνω, με βάση το αρχικό μας παράδειγμα ένα σύστημα πληρωμής όπως του Ripple ανακουφίζει τις ανησυχίες του Ατόμου 1 για του Ατόμου 2 και εάν Ατόμου 2 δεν τηρήσει την συμφωνία, τα χρήματα επιστρέφονται στο Άτομο 1.

3.3.3 Εφαρμογή στο εμπόριο και εμπορικές χρηματοδοτήσεις

Το Blockchain μπορεί να συνδεθεί με το παγκόσμιο εμπόριο και τις δραστηριότητες του. Για παράδειγμα πολλές φορές οι έμποροι μπορεί να αποτυγχάνουν να αποκτήσουν έγκαιρα μια εγγυητική επιστολή ή μια ενέγγυα πίστωση από ένα χρηματοπιστωτικό ίδρυμα ή η τράπεζα που τα εγγυάται να μην έχει την απαραίτητη εμπιστοσύνη και το στιβαρό όνομα στον χώρο. Αντίστοιχα μπορεί ο δανειζόμενος να μην λάβει την δανειοδότηση που ζητάει λόγο της φύσης των εμπορευμάτων που θέλει να αγοράσει ή να μην μπορεί να διασφαλίσει την πληρωμή του εισαγωγέα. Επίσης συναλλαγματικοί κίνδυνοι μπορούν να οξύνουν την κατάσταση των συναλλαγών.

Για τον λόγο αυτό όπως αναλύεται από τους Lin William Cong, Zhiguo He (2018) τα παραπάνω προβλήματα έρχεται να τα λύσει το blockchain και η τεχνολογία του. Πρώτον η φύση των αγαθών σίγουρα μπορεί καλύτερα να καταγραφεί σε αποκεντροποιημένα καθολικά ιδιαίτερα κατά την διάρκεια που τα αγαθά μεταφέρονται ή

αποθηκεύονται ή παραδίδονται. Ακόμα και για το σε ποια φυσική τοποθεσία βρίσκονται, που ακριβώς φυλάσσονται αλλά και εάν βρίσκονται στην κατάλληλη θερμοκρασία καθώς και άλλες σχετικές λεπτομέρειες. Έτσι δίνεται ουσιαστικά σε όλα τα εμπλεκόμενα άτομα ίση πρόσβαση στις πληροφορίες αυτές διευκολύνεται η γρηγορότερη επιβεβαίωση και μειώνεται η αμφιβολία. Επίσης το blockchain παρέχει δυνητική λύση στο σύστημα των πιστώσεων μέσω της συμμετοχής όλων των ατόμων κάτω από το ίδιο δίκτυο αλληλοεπιδρώντας στο ίδιο Blockchain σε πραγματικό χρόνο. Από την πληρωμή των προϊόντων, μέχρι το λιμάνι μεταφοράς τους, αλλά και μέχρι τις τράπεζες και τις μεταφορές βρίσκονται σε ήδη σε εξέλιξη. Εδώ έρχεται και η συμβολή των Smart Contracts καθώς με την εφαρμογή τους μειώνουν με δραματικά γρήγορο τρόπο το κόστος στην εκτέλεση των μεταφορών, επιβεβαιώνοντας σε πραγματική κατάσταση που βρίσκονται τα φορτία που μεταφέρονται.

Ήδη σήμερα έχουν αναπτυχθεί και υπάρχουν πολλές εφαρμογές blockchain για το εμπόριο και τον χρηματοπιστωτικό τομέα.

Το 2016 η τράπεζα Barclays και η startup Wave που δραστηριοποιείται στο FinTech έγιναν ο πρώτος οργανισμός που πραγματοποίησε παγκόσμια εμπορική συμφωνία χρησιμοποιώντας την διαμοιρασμένη καθολική τεχνολογία του blockchain. Η ενέγγυα πίστωση (Letter of credit) ανάμεσα στην Ornua (Ιρλανδική γαλακτοβιομηχανία) και στην Seychelles Trading company αποτέλεσε την πρώτη εμπορική πράξη που έγινε στην πλατφόρμα της Wave.

Επίσης ο τεχνολογικός κολοσσός IBM ήταν και αυτή πρωταγωνιστής στο να χρησιμοποιήσει το 2016 εφαρμογές του blockchain και των Smart Contracts στις εμπορικές χρηματοδοτήσεις παρέχοντας λύσεις στην Indian Mahindra Group σε συνεργασία της με την δανέζικη ναυτιλιακή εταιρεία Maersk. Ακόμη τον Μάρτιο του 2017 η IBM και η Maersk συνεργάστηκαν με την πλατφόρμα Hyperledger και ανακοίνωσαν την δημιουργία μιας ψηφιακής αλυσίδας εφοδιασμού που χρησιμοποιεί την τεχνολογία blockchain και επιτρέπει στα εμπλεκόμενα μέρη να έχουν πρόσβαση σε πληροφορίες λιμανιών και άλλου είδους σχετικές πληροφορίες. Επιπρόσθετα στα τέλη του 2017 η IBM επεκτάθηκε επιπλέον, εισάγοντας το Yijian Blockchain Technology Application System για τον κινέζικο φαρμακευτικό τομέα. Αλλά και τέλος έχει συνεργαστεί η IBM με μεγάλο αριθμό επιχειρήσεων για να αναπτύξει μια εμπορική πλατφόρμα blockchain που θα δραστηριοποιείται στην βιομηχανία του αργού πετρελαίου.

Άλλες πλατφόρμες Blockchain που βασίζονται σε θέματα δανειοδοτήσεων, ενέγγυων πιστώσεων, εξαγωγών, εμπορίου και ασφαλιστικών θεμάτων είναι η HK Blockchain, η TradeSafe και η Digital Trade Chain.

Επίσης σε θέματα εφαρμογών blockchain και λογιστικών θεμάτων τον Σεπτέμβριο του 2017 η Maersk συνεργάστηκε με την EY, την Microsoft, την Willis Tower Watson και διάφορες σημαντικές ασφαλιστικές εταιρείες για να επιτύχουν ασφαλή διαμοιρασμό δεδομένων στο KSI, ένα blockchain που αναπτύχθηκε από την Guardtime.

3.3.4 Εφαρμογή στις κεντρικές τράπεζες

Όπως αναλύεται από τους Catalini C., Gans J. (2016), ένα πολύ ενδιαφέρον παράδειγμα είναι η ανάπτυξη ενός Blockchain που θα βασίζεται στα fiat νομίσματα και θα στηρίζει το ψηφιακό νόμισμα. Εάν μια κεντρική τράπεζα αλλάξει την υπάρχουσα δομή της σε μια με κρυπτονόμισμα, θα μπορεί απευθείας να παρέχει στους πολίτες ψηφιακά τραπεζικά νομίσματα.

Βέβαια αυτό αποτελεί πρόκληση για μοντέλα εσόδων των τραπεζών αλλά και για τους πολίτες που μπορεί να προτιμούν τα κλασικά χαρτονομίσματα για τις συναλλαγές τους, αλλά ακόμα και για το κράτος για το πως θα υιοθετήσει φορολογικά εργαλεία, το πώς θα κατευθύνει την προσφορά και την ζήτηση χρήματος, πως θα γίνεται το qe αλλά και γενικώς πως θα γίνονται διαχρονικές συναλλαγές σε ολόκληρη την οικονομία.

Φυσικά ένα τέτοιο είδος νομίσματος θα μπορούσε να αποτελέσει ιδανική λύση για πολίτες της χώρας που βρίσκονται εκτός και αντιμετωπίζουν προβλήματα υποτίμησης ή δεν εμπιστεύονται την κυβέρνηση που το εκδίδει. Όπως η περίπτωση της Ινδίας με την υποτίμηση των χαρτονομισμάτων 500 και 1000 rupees που ωθεί προς τον μεγαλύτερο παρεμβατισμό και παρακολούθηση των συναλλαγών μειώνοντας την αξία των μετρητών χρημάτων και αυξάνοντας το ενδιαφέρον των πολιτών για νομίσματα ψηφιακού τύπου όπως το bitcoin.

3.3.5 Διαπιστευτήρια και επαλήθευσης ταυτότητας μέσω Blockchain

Το Blockchain και η τεχνολογία του μπορούν να μειώσουν τον κίνδυνο της αποκάλυψης ευαίσθητων πληροφοριών με την πραγματοποίηση της επαλήθευσης των στοιχείων μας. Κάθε φορά που κάνουμε μια ηλεκτρονική συναλλαγή επιτρέπουμε σε ένα τρίτο συμβαλλόμενο μέρος να πιστοποιήσει και να εγκρίνει μια πράξη. Τέτοιου είδους στοιχεία μπορεί να είναι από λιγότερο ευαίσθητα δηλαδή όπως είναι ο βαθμός πτυχίου, η άδεια οδήγησης, μέχρι πιο ευαίσθητα που μπορεί να είναι ο αριθμός ασφάλισης, οι κωδικοί πρόσβασης, τα διαβατήρια, οι ψηφιακές υπογραφές κλπ. (Catalini C., Gans J. (2016))

Μια ικανότητα του blockchain είναι να καταγράφει και να διαβιβάζει όταν χρειάζεται σε ένα τρίτο άτομο όπως μια τράπεζα συγκεκριμένες πληροφορίες ή να επιβεβαιώνει το ιστορικό ενός ατόμου αφού έχει λάβει την άδεια του. Φανταστείτε την ευκολία που δίνει στην περίπτωση πρόσβασης σε ιστορικά αρχεία συναλλαγών ή υγειονομικό ιστορικό φυσικά αντιστοιχώντας μόνο μια ψηφιακή υπογραφή ή ένα δακτυλικό αποτύπωμα του ατόμου.

3.3.6 Άλλες εφαρμογές του Blockchain και των έξυπνων συμβολαίων

Εκτός από το σύστημα πληρωμών και τον χρηματοπιστωτικό τομέα το blockchain και τα smart contracts μπορούν να χρησιμοποιηθούν σε χρηματιστήρια, σε ψηφοφορίες, σε κοινοπρακτικά δάνεια αλλά και σε θέματα εταιρικής διακυβέρνησης. Το blockchain θέτει μια σειρά ερωτημάτων γύρω από το ποιες εφαρμογές του είναι πιθανότερο να αναπτυχθούν πρώτες; Ποιοι τύποι συναλλαγών είναι πιθανότερο να ωφεληθούν από την τεχνολογία αυτή πρώτα; Πως θα προσδώσει διαφορετικούς βαθμούς ιδιωτικότητας ενώ προωθούνται τα χαμηλά κόστη συναλλαγών; Είναι πιθανό να αποτελέσει σημείο υπεροχής στην έρευνα και ανάπτυξη συγκεκριμένων θεμάτων;

Ο απλούστερος τρόπος να επιτευχθεί επιβεβαίωση μιας συναλλαγής σε ένα Blockchain είναι όταν πραγματοποιείται μεταξύ δύο μόνο αντισυμβαλλόμενων μερών. Για παράδειγμα συναλλαγές που γίνονται μεταξύ ενός αγοραστή και ενός πωλητή με την χρήση κρυπτονομισμάτων. Αυτές οι ατομικές συναλλαγές είναι πιθανό να γίνουν ιδιαίτερα χρήσιμες και ανταγωνιστικές όσο δεν παρεμβάλλεται κάποιος ενδιάμεσος που να

προσδίδει επιπλέον αξία σε αυτές όπως για παράδειγμα με το να κρατάει αρχεία των πληρωμών. Η βασική χρησιμότητα ενός Online ενδιάμεσου μέρους είναι να σχεδιάσει και να διατηρήσει μια στιβαρή φήμη για το σύστημα του για να διευκολύνει τις συναλλαγές μεταξύ αγοραστών και πωλητών. Παρόλα αυτά η τεχνολογία blockchain μπορεί να χρησιμοποιηθεί για να αυξήσει την διαφάνεια, να διασφαλίσει ότι τα έσοδα παράγονται μετά από μια επιβεβαιωμένη συναλλαγή αλλά και να χτίσει μια ανοιχτή με φήμη πλατφόρμα, αυξάνοντας τον ανταγωνισμό και μειώνοντας τα εμπόδια εισόδου στις αγορές. (Catalini C., Gans J. (2016)))

Το blockchain και κατ' επέκταση τα smart contracts μπορούν να επεκτείνουν τις ατομικές συναλλαγές και να συνδεθούν σε ένα hardware λογισμικό όπως μια βάση δεδομένων μέσω του κρυπτονομίσματος. Καθώς και να συνδυαστεί με συσκευές IoT όπως είναι τα ρομπότ για να επιτρέπει την χρήση ιστορικών αρχείων που βρίσκονται σε ασφαλή μέρη αποθηκευμένα με χρήση ψηφιακών υπογραφών.

Ας αναλογιστούμε την χρησιμότητα του Blockchain σε εφαρμογές που περιλαμβάνουν εγγραφές και πνευματικά δικαιώματα. Για παράδειγμα οι καλλιτέχνες έχουν δώσει τα πνευματικά τους δικαιώματα στο Spotify ή στη Apple μπορούν να μετρήσουν πόσες φορές τα τραγούδια τους παίζονται από τους καταναλωτές ή να λαμβάνουν δικαιώματα χρήσης από τα remix που φτιάχνονται από τα τραγούδια αυτά σύμφωνα με μια προκαθορισμένη Smart contract.

Ακόμη φανταστείτε ένα κρυπτονόμισμα να είναι συνδεδεμένο με το να ταιριάζει επαγγελματίες οδηγούς με πελάτες για παράδειγμα στις εταιρείες Uber και Lyft. Να βασίζεται το νόμισμα αυτό στις συνθήκες της αγοράς, στις προτιμήσεις των πελατών όπως το επίπεδο της υπηρεσίας που επιθυμούν, στην ποιότητα του αυτοκινήτου, στην ηλικία του οδηγού κλπ και οι πελάτες και οι οδηγοί να είναι συνδεδεμένοι κάτω από την ίδια πλατφόρμα και να μπορούν να κάνουν ταυτόχρονα την επιλογή τους για εκείνον που προσθέτει την μεγαλύτερη αξία σε αυτούς την δεδομένη χρονική στιγμή. Έτσι πλέον δεν θα υπάρχει η ανάγκη ενός ενδιάμεσου να ταιριάζει τα αιτήματα σε ένα σύστημα peer to peer car pooling service.

Επίσης στον τομέα των χρηματοοικονομικών και της λογιστικής, το Blockchain μπορεί να χρησιμεύσει στο να δημιουργήσει μια πιο ανοιχτή και ασφαλή χρηματοοικονομική πλατφόρμα. Για παράδειγμα ένα στεγαστικό δάνειο μπορεί να είναι καταγεγραμμένο στο blockchain και να είναι προσβάσιμο σε ενδιαφερόμενα μέλη σε

πραγματικό χρόνο συμπεριλαμβανομένου και των ρυθμιστικών αρχών. Ακόμη λογιστικά ιστορικά μπορούν να ελέγχονται με αυτοματοποιημένο τρόπο με πρωταρχικό στόχο την τήρηση του απορρήτου και από τις δύο πλευρές. Επιπρόσθετα χρηματοοικονομικές πλατφόρμες μπορούν να μειώσουν αισθητά το κόστος εισόδου νέων ατόμων ιδιαίτερα σε αγορές με αυστηρούς κανονισμούς. Το 2015 η Nasdaq Inc εισήγαγε την Linq πλατφόρμα που διαχειρίζεται μετοχές που είναι σε στάδιο IPO, καθώς επίσης και το χρηματιστήριο της Κορέας (KRX) εισήγαγε ένα δικό του Blockchain. Άλλες προσπάθειες εφαρμογής του Blockchain και των Smart Contracts για ανταλλαγές και εμπόριο εφαρμόστηκαν στην Αυστραλία στο χρηματιστήριο αξιογράφων, καθώς και τα Smart Contracts μπορούν να συμβάλουν στην οριοθέτηση των κανόνων για παράγωγα προϊόντα αλλά και χρηματοοικονομικές συμφωνίες. Τέλος πολύ πρόσφατα, η Walmart, η IMB και η JD.com συνεργάστηκαν μεταξύ τους για να εισάγουν ένα Blockchain που θα παρακολουθεί την παραγωγή προϊόντων, στις συνθήκες ασφαλείας τους και την διανομή τους. (Lin William Cong, Zhiguo He (2018))

Επίσης το blockchain μπορεί να έχει εφαρμογή στην περίπτωση χρήσης hardware λογισμικού. Για παράδειγμα οι αισθητήρες καιρού ενός μετεωρολογικού κέντρου μπορούν να αποθηκεύουν τις πληροφορίες του καιρού και τις διανέμουν μέσω ενός δικτύου Blockchain σε όλα τα ενδιαφερόμενα άτομα. Επίσης ένα κλειδί αυτοκινήτου θα έχει την δυνατότητα να διαβάζει πληροφορίες από ένα blockchain χρησιμοποιώντας ένα δημόσιο κρυπτογραφημένο κλειδί και να επαληθεύσει τον χρήστη του αυτοκινήτου. Φανταστείτε στην περίπτωση πώλησης του αυτοκινήτου αυτού με την συναλλαγή να γίνεται μέσω κρυπτονομίσματος στο blockchain θα γίνει αυτόματη αλλαγή στην ιδιοκτησία όταν πληρωθεί το ποσό που έχει οριστεί μέσω κάποιας smart contract καταγράφοντας την πράξη άμεσα και γρήγορα στο καθολικό του δικτύου.

Ενώ στην περίπτωση χρήση του IoT σε συνδυασμό με το blockchain μέσω κρυπτονομίσματος να ανταλλάσσουν πόρους κάτω από το ίδιο δίκτυο. Σκεφτείτε πως στο μέλλον ένα αυτοοδηγούμενο όχημα μέσω της σύνδεσης του σε ένα blockchain δίκτυο θα μπορεί να έχει πρόσβαση σε δεδομένα για την κίνηση στους αυτοκινητόδρομους και να αγοράζει χρησιμοποιώντας το κρυπτονόμισμα του δικτύου γραμμές οδήγησης για να έχει προτεραιότητα στην κυκλοφορία.

Τέλος με το IoT ας αναλογιστούμε πόσο πιο αποτελεσματικό και με λιγότερη σπατάλη πόρων θα μπορούσε να είναι η διαδικασία της εξόρυξης (mining) ενός κρυπτονομίσματος.

3.4 Καταγραφή των μεγαλύτερων εταιρειών παγκοσμίως που χρησιμοποιούν την τεχνολογία του Blockchain

Παρόλο που το blockchain θεωρήθηκε κατάλληλο μόνο για τους τραπεζικούς τομείς, άρχισε να διαταράσσει και άλλες βιομηχανίες. Με τη δημοτικότητα του έχει αποκτήσει τα τελευταία χρόνια το blockchain, πολλές εταιρείες παγκοσμίως εκμεταλλεύονται τα πλεονεκτήματα του και το χρησιμοποιούν από εφαρμογές που σχετίζονται με την εφοδιαστική αλυσίδα, την η υγειονομική περίθαλψη μέχρι και τον χώρο των ακινήτων. Σύμφωνα λοιπόν με πρόσφατο άρθρο του 2020 που δημοσιεύτηκε στον ηλεκτρονικό ιστότοπο 101blockchains.com από τον Hasib Anwar παρουσιάζονται κάποιες από οι εταιρείες που χρησιμοποιούν και ωφελούνται σήμερα από την Blockchain τεχνολογία.

3.4.1 Τραπεζικός και Χρηματοοικονομικός τομέας (Bank and Finance)

Στον Τραπεζικό και Χρηματοοικονομικό τομέα (Bank and Finance), ο τραπεζικός κολοσσός BBVA είναι μια από τις εταιρείες που χρησιμοποιούν την τεχνολογία blockchain σε συνεργασία με την Red Electrica Corporation. Γεγονός είναι πως πρόσφατα ολοκληρώθηκε ένα κοινοπρακτικό δάνειο χρησιμοποιώντας την τεχνολογία Blockchain. Η MUFG, η BNP Paribas και η BBVA χορήγησαν αυτή την τη συμφωνία των 150 εκατ. ευρώ. Πιο συγκεκριμένα, το δάνειο έφθασε σε ταχύτητα ρεκόρ από την πλατφόρμα της BBVA. Προς το παρόν, η εταιρεία είναι ιδιαίτερα αισιόδοξη για τη χρήση της τεχνολογίας και για μελλοντικές δραστηριότητες. Επίσης η Banca Intesa Sanpaolo ένας ιταλικός τραπεζικός όμιλος χρησιμοποιεί τεχνολογία blockchain για την επικύρωση δεδομένων συναλλαγών. Η Deloitte, η Eternity Wall, και η τράπεζα άρχισαν να δοκιμάζουν πρόσφατα την τεχνολογία. Πιο συγκεκριμένα, χρησιμοποιούν το πρωτόκολλο OpenTimestamps που

χρησιμοποιεί το Bitcoin για την τροφοδοσία του συστήματος. Ο βασικός συνεργάτης του Bitcoin, ο Peter Todd βρίσκεται πίσω από την τεχνολογία αυτή. Ακόμη η δεύτερη μεγαλύτερη τράπεζα της Βρετανίας, η Barclays, χρησιμοποιεί την τεχνολογία blockchain για την βελτιστοποίηση διαδικασιών μεταφοράς κεφαλαίων και διαδικασιών KYC (Know-Your-Customer). Ακόμη, καταχώρησε και διπλώματα ευρεσιτεχνίας για αυτά τα δύο πεδία. Η τράπεζα HSBC σχεδιάζει την πλατφόρμα της βασισμένη στην τεχνολογία Blockchain μέχρι το τέλος του Μαρτίου του 2020. Στόχος είναι να μετατοπιστούν από το παραδοσιακό γραφειοκρατικό σύστημα εγγράφων σε πλήρως ψηφιακή και αποκεντρωμένη πλατφόρμα Vault. Έτσι, οι επενδυτές τους μπορούν με ιδιωτικό τρόπο να παρακολουθήσουν τα χρήματά τους σε πραγματικό χρόνο. Τέλος η Visa χρονολογείται να ασχολείται με την τεχνολογία blockchain από το 2016. Το 2016, παρουσίασαν μια πλατφόρμα blockchain που ασχολείται με τις υπηρεσίες πληρωμών μεταξύ επιχειρήσεων. Ωστόσο, χρειάστηκε χρόνος για να υλοποιήσουν αυτό το έργο. Μέχρι το τέλος του 2019, ήθελαν να καλύψουν 90 αγορές στις οποίες μπορούν να πραγματοποιήσουν πληρωμές οι επιχειρήσεις.

3.4.2 Εφοδιαστική αλυσίδα (Supply Chain)

Στον τομέα της εφοδιαστικής αλυσίδας, η εταιρεία DE Beers χρησιμοποιεί το blockchain στην αλυσίδα εφοδιασμού. Για να βοηθήσουν στη ρύθμιση του συστήματος διαχείρισης της αλυσίδας εφοδιασμού τους, εισήγαγαν μια blockchain πλατφόρμα που ονομάζεται Tracr. Πιο συγκεκριμένα, σε αυτήν την πλατφόρμα, μπορούν να παρακολουθήσουν την πορεία οποιοδήποτε μεγέθους διαμαντιών από την περιοχή εξόρυξης έως το κατάστημα λιανικής πώλησης. Αποτελεί κι όλας έναν πραγματικά πολύ καλό τρόπο να αποδεικνύεται ότι τα διαμάντια τους είναι 100% πραγματικά. Επίσης η Unilever είναι από τις εταιρείες που χρησιμοποιούν blockchain στον κατάλογο εφοδιαστικής αλυσίδας. Στην πραγματικότητα, η Unilever χρησιμοποιεί σήμερα τεχνολογία για να διαχειριστεί την βιομηχανία τσαγιού της. Με τη βοήθεια της τεχνολογίας, μπορούν να παρακολουθήσουν όλες τις συναλλαγές τους, να παρακολουθήσουν τους προμηθευτές τους για να διατηρήσουν σε υψηλά επίπεδα την ποιότητα τους συνεχώς. Ακόμη η Walmart υπήρξε μια εταιρεία που αγκάλιασε εδώ και πολύ καιρό την τεχνολογία

Blockchain. Στην πραγματικότητα, η εταιρεία χρησιμοποιεί την τεχνολογία της αλυσίδας εφοδιασμού της IBM - την πλατφόρμα Hyperledger Fabric για να υποστηρίξει τη διαδικασία της εφοδιαστικής της αλυσίδας. Επιπλέον, σχεδιάζουν να παρακολουθήσουν τα τρόφιμά τους απευθείας από τους αγρότες τους και να προσφέρουν στους πελάτες τους τον έλεγχο της προέλευσης πριν αγοράσουν ένα προϊόν. Η Anheuser Busch InBev είναι μια από τις μεγαλύτερες εταιρείες ζυθοποιίας που χρησιμοποιούν το Blockchain και αυτοί στην αλυσίδα εφοδιασμού. Μαζί με την BanQu, θέλουν να αυξήσουν τη συνολική διαφάνεια των συστημάτων τους αλλά και τις διαδικασίες καλλιέργειας του κασσάβα δίνοντας δύναμη σε περισσότερους από 2000 αγρότες στη Ζάμπια. Τέλος να αναφέρουμε πως η Ford είναι μια άλλη δημοφιλής εταιρεία που χρησιμοποιεί την τεχνολογία blockchain. Στην πραγματικότητα, η IBM συνεργάζεται μαζί τους και μαζί σχεδιάζουν να παρακολουθήσουν τις πρώτες ύλες τους όπως το κοβάλτιο από τους προμηθευτές. Θέλουν να σιγουρευτούν ότι παίρνουν ένα αυθεντικό προϊόν για να διατηρήσουν την ποιότητά τους από την στιγμή της εξόρυξης μέχρι την ολοκλήρωση των βημάτων μεταφοράς του.

3.4.3 Ιατροφαρμακευτική περίθαλψη (Healthcare)

Στον τομέα Ιατροφαρμακευτικής περίθαλψης η Change Healthcare είναι μια από τις μεγάλες εταιρείες που χρησιμοποιούν τεχνολογία blockchain. Στην πραγματικότητα, δραστηριοποιούνται μέσω του Intelligent Healthcare Network το οποίο χρησιμοποιεί την πλατφόρμα Hyperledger Fabric για να το τροφοδοτήσει. Σε κάθε περίπτωση η πλατφόρμα θα τους βοηθήσει να διαχειριστούν τους ασθενείς τους και την κατάσταση της υγείας τους σε πραγματικό χρόνο. Έτσι, το σύστημα μπορεί εύκολα να ελέγξει, να αναπτύξει και να προωθήσει την εμπιστοσύνη των χρηστών. Η FDA εργάζεται επίσης σε λύσεις υγειονομικής περίθαλψης χρησιμοποιώντας τεχνολογία blockchain. Ως αποτέλεσμα, χρησιμοποιούν αυτήν τη στιγμή το Hyperledger για να τροφοδοτήσουν μια πλατφόρμα που θα εξασφάλιζε δεδομένα υγείας. Στόχος είναι να διασφαλίσουν εμπιστευτικές πληροφορίες των ασθενών τους όπως το ιατρικό ιστορικό τους. Επίσης η DHL είναι μια άλλη από τις μεγάλες εταιρείες που χρησιμοποιούν τεχνολογία blockchain. Μαζί με την Accenture, εργάζονται μέσω του proof of concept για να εντοπίζουν την αυθεντικότητα των φαρμακευτικών προϊόντων από το σημείο προέλευσης τους μέχρι τον καταναλωτή. Ο λόγος είναι για να μπορούν να απαλλαγούν από τυχόν προβλήματα παραποίησης ή

απομίμησης των φαρμάκων τους που τίθενται αντιμέτωπες κάθε μέρα. Ακόμη η Centers for Disease Control and Prevention θέλουν να αξιοποιήσουν τις νέες τεχνολογίες για τη βελτίωση της γενικής υγείας των Αμερικανών πολιτών. Αυτός είναι ο λόγος που συνεργάζονται με την IBM για την ανάπτυξη ενός κρυπτογραφημένου καθολικού συστήματος που θα τους βοηθήσει να καταγράφουν όλα τα Ηλεκτρονικά Αρχεία Υγείας χωρίς ποτέ να τίθενται σε κίνδυνο η ασφάλεια τους. Τέλος η Pfizer είναι ακόμη μία από τις μεγάλες εταιρείες που χρησιμοποιούν τεχνολογία blockchain. Η Biogen και η Pfizer με επικεφαλής την Clinical Supply Blockchain Working Group (CSBWG), μόλις ολοκλήρωσαν το proof of concept για την παρακολούθηση αρχείων και τη διαχείριση του ψηφιακού αποθέματος των φαρμακευτικών προϊόντων. Στην πραγματικότητα, ο όμιλος συνεργάζεται και με άλλες εταιρείες όπως η GlaxoSmithKline, η Merck, η AstraZeneca και η Deloitte.

3.4.4 Ασφάλιση (Insurance)

Στον ασφαλιστικό τομές, ο Όμιλος AIA είναι επίσης μια από τις μεγάλες εταιρείες που χρησιμοποιούν τεχνολογία blockchain για ασφαλιστικούς σκοπούς. Στην πραγματικότητα, η εταιρεία ξεκίνησε ένα έργο για λύσεις τραπεζοασφάλισης με άλλες συνεργαζόμενες τράπεζες. Αυτή η πλατφόρμα θα αξιοποιήσει τη δύναμη του blockchain και θα βοηθήσει στην ανταλλαγή εγγράφων και δεδομένων σε πραγματικό χρόνο σε ασφαλές κανάλι. Μια άλλη από τις μεγαλύτερες εταιρείες που χρησιμοποιούν τεχνολογία blockchain είναι η MetLife. Στην πραγματικότητα, η LumenLab είναι η εταιρεία θυγατρική της MetLife στη Σιγκαπούρη και συνεργάζονται με την εταιρεία NTUC Income και τη Singapore Press Holdings (SPH) για τη δημιουργία του Lifechain. Χρησιμοποιώντας αυτήν την πλατφόρμα, μπορούν να προσδιορίσουν ποια άτομα καλύπτονται ασφαλιστικά και ποια όχι αλλά και όταν χρειαστεί αυτόματα να υποβάλλεται αίτηση ασφαλιστικής κάλυψης. Επίσης η Prudential Financial είναι μία από τις δημόσιες εταιρείες που χρησιμοποιούν τεχνολογία blockchain για ασφάλιση. Η εταιρεία σχεδιάζει να χρησιμοποιήσει την τεχνολογία για να εξασφαλίσει ότι δεν υπάρχουν δόλιες δραστηριότητες στις ασφαλίσεις και όλοι οι πελάτες έχουν καλύτερη εξυπηρέτηση και μπορούν να διαβιβάσουν τα έγγραφα και τα στοιχεία τους χωρίς καμία ταλαιπωρία. Η εταιρεία θα συνεργαστεί με άλλες ασφαλιστικές εταιρείες για την ανάπτυξη του έργου αυτού σε μια πλατφόρμα που μπορεί

να προσφέρει αγορά και πώληση αγαθών, παρακολούθηση αλλά και υποβολές για ασφάλιση. Επίσης η εταιρεία American International Group ή όπως είναι γνωστή AIG είναι μία από τις δημόσιες εταιρείες που χρησιμοποιούν τεχνολογία blockchain. Προς το παρόν, συνεργάζονται με την IBM για την ανάπτυξη μιας έξυπνης ασφαλιστικής πλατφόρμας. Με τη βοήθεια της πλατφόρμας, μπορούν να καλύψουν όλα τα περίπλοκα διεθνή ασφαλιστικά προβλήματα. Τέλος η Aegon είναι άλλη μια εταιρεία που χρησιμοποιεί την τεχνολογία blockchain. Στην πραγματικότητα αποτελούν μέρος της πρωτοβουλίας B3i που χρησιμοποιεί την πλατφόρμα R3 Corda για την υποστήριξη της ασφαλιστικής τους πλατφόρμας.

3.4.5 Ενέργεια (Energy)

Στον τομέα της ενέργειας η Shell είναι μία από τις ενεργειακές εταιρείες που χρησιμοποιούν τεχνολογία blockchain μαζί με την Sinochem Energy Technology Co Ltd και τη Macquarie και σχεδιάζουν να την χρησιμοποιήσουν για το εμπόριο αργού πετρελαίου. Με τη βοήθεια της πλατφόρμας, είναι εύκολο να εντοπίσουν τα προϊόντα τους μαζί με την προώθηση της διαφάνειας και την πρόληψη από πράξεις απάτης. Επίσης η Siemens είναι άλλη μια εταιρεία που επενδύει σε blockchain για την ενέργεια. Πιο συγκεκριμένα, η εταιρεία δήλωσε πρόσφατα ότι θέλει να φέρει καινοτομία στον ενεργειακό τομέα και σχεδιάζει να επεκτείνει τις λύσεις τις στις υπηρεσίες παραγωγής ηλεκτρικής ενέργειας. Με αυτό τον τρόπο σχεδιάζουν να καταστήσουν πιο βιώσιμα τα ενεργειακά τους συστήματα. Η εταιρεία TenneT έχει αντιληφθεί πως η ζήτηση για ηλεκτρική ενέργεια αυξάνεται, αλλά η προσφορά παραμένει πολύ χαμηλή. Ως αποτέλεσμα, είναι δύσκολο να τροφοδοτείται συνεχώς η κατανάλωση ενέργειας στους καταναλωτές. Για τον λόγο αυτό χρησιμοποιεί την τεχνολογία blockchain και μέσω του Hyperledger Fabric αποσκοπεί να παρακολουθεί την χρήση ηλεκτρικής ενέργειας και να είναι σε θέση να αποθηκεύει ενέργεια και να την διοχετεύει σε περιπτώσεις υψηλής ζήτησης. Ακόμη η ADNOC ή Abu Dhabi National Oil Company είναι άλλη μια εταιρεία στον κλάδο της ενέργειας που χρησιμοποιεί την τεχνολογία blockchain. Χρησιμοποιούν την τεχνολογία για να αυξήσουν τη διαφάνεια σε όλες τις επιχειρήσεις τους και θα επεκταθούν και στη διαχείριση της εφοδιαστικής αλυσίδας. Τέλος να αναφέρουμε πως και η Εθνική Επιτροπή Ενέργειας της Χιλής πρόκειται να χρησιμοποιήσει ένα δίκτυο με βάση το Ethereum για την καταγραφή όλων των στοιχείων του ενεργειακού τους τομέα Δεδομένου ότι υπάρχουν πολλές

αποκλίσεις στον ενεργειακό τομέα θέλουν ένα αμετάβλητο αρχείο που δεν θα μπορεί να αλλάξει από κανέναν.

3.4.6 Εμπόριο (Trade)

Στον τομέα του εμπορίου η Mizuho είναι στις μεγάλες εμπορικές εταιρείες που χρησιμοποιούν την τεχνολογία blockchain. Στην πραγματικότητα, η τράπεζα ολοκλήρωσε την πρώτη συναλλαγή χρηματοδότησης με μεγάλη ακρίβεια χωρίς να έχουν θέματα διαμοιρασμού εμπιστευτικών δεδομένων και έγγραφων στην πλατφόρμα τους. Σχεδιάζουν να συνεχίσουν να χρησιμοποιούν τη πλατφόρμα αυτή και στο μέλλον. Η εταιρεία η ANZ χρησιμοποιεί την τεχνολογία blockchain μαζί με άλλα 6 μέλη σχηματίζοντας μια κοινοπραξία για τους τομείς του εμπορίου. Η Νομισματική Αρχή του Χονγκ Κονγκ έχει αναλάβει το έργο αυτό και ο στόχος είναι να επεξεργαστεί κάθε έγγραφο και να γίνει ψηφιακό. Πιο συγκεκριμένα, η πλατφόρμα σχεδιάζει να απαλλαγεί από διπλότυπα δεδομένα και να κατέχει μόνο ένα δεδομένο για οποιοδήποτε έγγραφο. Επίσης η Scotiabank χρησιμοποιεί την πλατφόρμα της Alphapoint για τον εμπορικό τομέα και στέλνουν ήδη δοκιμαστικά εμπορικά έγγραφα για να ελέγξουν την λειτουργία της. Το έργο αυτό θα βοηθήσει στην ψηφιοποίηση των περιουσιακών στοιχείων και στην διαχείριση γραφειοκρατικών συναλλαγών. Επίσης η εταιρεία SEB χρησιμοποιεί το Blockchain και συγκεκριμένα μέσω της πλατφόρμας Trade360 της CGI έχει απώτερο σκοπό τον χειρισμό όλων των κανονισμών και των συναλλαγών που την διέπουν. Το καλύτερο κομμάτι της πλατφόρμας είναι πως μπορεί πλήρως να χειριστεί τις οικονομικές πτυχές μιας διαπραγμάτευσης και παράλληλα να προσφέρει μια ισχυρή αρχιτεκτονική. Τέλος η Λαϊκή Τράπεζα της Κίνας ψάχνει για λύσεις με την χρήση του blockchain για εμπορικές επιχειρήσεις. Η πλατφόρμα στην οποία εργάζονται να αναπτύξουν θα έχει ένα οικοσύστημα όπου οι επιχειρήσεις θα μπορούν να κάνουν διασυνοριακές συναλλαγές στο Χονγκ Κονγκ, στον κόλπο του Μακάο και στο Guangdong με εύκολο και γρήγορο τρόπο.

3.4.7 Internet of Thinks (IoT)

Στον τομέα του Internet of thinks (IoT) η εταιρεία Maersk συνεργάζεται μαζί με την IBM για την χρήση της τεχνολογίας blockchain για την βελτιστοποίηση της διαχείρισης της αλυσίδας εφοδιασμού. Για να επιτευχθεί αυτό, χρησιμοποιούν συστήματα IoT που βασίζονται στο blockchain για να αποκτήσουν διαφάνεια στην πλατφόρμα. Χρησιμοποιώντας συσκευές IoT κάθε διαδικασία θα πραγματοποιείται online και θα συνδέεται με την πλατφόρμα για την παρακολούθηση διάφορων συνθηκών. Επίσης ένα άλλο καλό παράδειγμα στο IoT και στο blockchain είναι η Commonwealth Bank που χρησιμοποιεί το κατανεμημένο καθολικό για να απαλλαγεί από δύο σημαντικά ζητήματα, του παγκόσμιου εμπορίου και της ανταλλαγής περιουσιακών στοιχείων. Η ενσωμάτωση του IoT στο σύστημα blockchain τους δίνει την δυνατότητα να παρακολουθήσουν όλες τις διαδικασίες παγκόσμιου εμπορίου σε πραγματικό χρόνο. Επίσης η εταιρεία Van Dorp χρησιμοποιεί την τεχνολογία blockchain και τον τομέα του IoT συνεργαζόμενη με την Timeseries για να ξεκινήσει ένα έξυπνο οικιακό έργο όπου κάθε έξυπνη οικιακή συσκευή θα συνδεθεί με την πλατφόρμα blockchain. Δεδομένου ότι το blockchain είναι ασφαλές οι έξυπνες οικιακές συσκευές θα έχουν πλήρη ασφάλεια και θα επικοινωνούν μεταξύ τους. Ακόμη μια άλλη τρομερή λύση στη βιομηχανία του IoT είναι το έργο στο οποίο εργάζεται η εταιρεία SEPA. Χρησιμοποιώντας συσκευές IoT και blockchain, σχεδιάζουν να εξασφαλίσουν και να προσφέρουν καθαρή ενέργεια για εκπαίδευση, έρευνα και σε πολλά άλλα είδη. Βασικά, επειδή οι συσκευές IoT είναι ευάλωτες από την φύση τους, με το Blockchain γίνονται ασφαλείς. Τέλος η MediLedger που σχετίζεται με τον τομέα της υγειονομικής περίθαλψης χρησιμοποιεί το IoT και το blockchain περιλαμβάνοντας ένα συνδυασμό από πολλές φαρμακευτικές εταιρείες μαζί με χονδρεμπόρους. Μεταξύ αυτών βρίσκονται οι πολύ γνωστές εταιρείες McKesson, AmerisourceBergen και Pfizer καθώς οι συσκευές IoT παρακολουθούν τα προϊόντα τους και σε συνδυασμό με το Blockchain προσφέρουν υψηλότερα επίπεδα ασφάλειας.

3.4.8 Ταξίδια (Travel)

Στον τομέα των ταξιδιών, είναι πλέον γεγονός πως το Blockchain επεκτείνεται και στην ταξιδιωτική βιομηχανία. Η Singapore Airlines χρησιμοποιεί ήδη την τεχνολογία για να προσφέρει προσφορές που βασίζονται σε πιστούς πελάτες. Χρησιμοποιώντας το KrisPay προσφέρουν προσφορές και οι πελάτες μπορούν να εγγραφούν στο πρόγραμμα κατεβάζοντας την αντίστοιχη εφαρμογή. Από την μεριά της η UAE's National Airline, η εθνική αεροπορική εταιρεία των ΗΑΕ, η Etihad Airways, συνεργάζεται με το Winding Tree. Που αποτελεί μια ταξιδιωτική πλατφόρμα που προσφέρει διάφορα χαρακτηριστικά και χρησιμοποιεί κατανεμημένη τεχνολογία καθολικού δικτύου για την τροφοδοσία του συστήματος. Η αεροπορική εταιρεία θέλει να χρησιμοποιήσει την πλατφόρμα για να διερευνήσει ευκαιρίες που μπορούν να αυξήσουν την πελατεία της και να κάνουν το Abu Dhabi έναν εξωτικό τουριστικό προορισμό. Επίσης η Lufthansa Industry Solutions ως μια από τις σημαντικότερες αεροπορικές εταιρείες παγκοσμίως αξιοποιεί τις πραγματικές δυνατότητες του blockchain ξεκινώντας την πρωτοβουλία Blockchain for Aviation (BC4A). Σχεδιάζουν σε αυτό να συμπεριλάβουν κατασκευαστές αεροσκαφών, παρόχους εφοδιασμού, παρόχους υπηρεσιών MRO, προγραμματιστές λογισμικού και πολλούς άλλους κάτω από το ίδιο δίκτυο Blockchain. Ακόμη η Delta Airlines μπορεί να βρίσκεται αρκετά πίσω στην χρήση του Blockchain όμως πρόσφατα δήλωσαν πως εργάζονται σε σχετικές τεχνολογίες που υποστηρίζονται από chatbots που μπορούν να προσφέρουν στους καταναλωτές τα οφέλη που θέλουν. Πιο συγκεκριμένα, χρησιμοποιώντας τα chatbots, η εταιρεία μπορεί να επικεντρωθεί περισσότερο σε θέματα high-end των πελατών της. Τέλος η British Airways συνεργάζεται με την VChain εταιρεία start up για να βελτιστοποιήσει τις διαδικασίες ελέγχου της ασφάλειας της. Επειδή στην πραγματικότητα οι διαδικασίες ελέγχου και ασφαλείας απαιτούν πολύ χρόνο και πόρους αρκετές φορές οδηγούν σε καθυστερήσεις στις πτήσεις που συνεπάγεται με ταλαιπωρία και κόστος.

3.4.9 Ακίνητα (Real Estate)

Στον τομέα των ακινήτων η μία από τις μεγάλες εταιρείες που χρησιμοποιούν την τεχνολογία blockchain είναι η Brookfield Asset Management. Αποτελεί μια από τις πολύ γνωστές εταιρείες στον κλάδο αυτό παγκοσμίως και σχεδιάζουν να ενσωματώσουν το Blockchain ως μέρος των συστημάτων τους χρησιμοποιώντας την τεχνολογία για να μειώσουν το κόστος συναλλαγών και να αυτοματοποιήσουν τις επαφές τους. Ακόμη η εταιρεία Allinfra και η Link REIT στο Hongkong συνεργάζονται για να αναπτύξουν ένα έργο blockchain για τους τομείς των ακινήτων. Σε πρώτο στάδιο θα εργαστούν σε ένα πιλοτικό πρόγραμμα για να ελέγξουν πώς το blockchain μπορεί να βοηθήσει τον τομέα των ακινήτων εισάγοντας μια βιώσιμη υποδομή υποστηριζόμενη από το blockchain. Επίσης η JLL είναι μια άλλη από τις μεγάλες εταιρείες που χρησιμοποιούν τεχνολογία blockchain για να αποτιμήσουν τα ισπανικά εμπορικά ακίνητα. Σύμφωνα με την εταιρεία μπορούν να χρησιμοποιήσουν αυτό το εργαλείο στην κατασκευή και στη χρηματοδότηση του τομέα αλλά και στο να πουλήσουν και να νοικιάσουν τα ακίνητα αυτά. Κυρίως η πρωτοβουλία προήλθε από την JLL Japan. Η εταιρεία χρησιμοποιεί και εκείνη το blockchain για εγγυήσεις τραπεζικών ακινήτων. Πρόκειται κυρίως για τα άτομα που είναι μισθωτές στις αγορές λιανικής και το έργο τους αποσκοπεί μέσω του blockchain να μπορούν να εκδίδουν εύκολα εμπορικές μισθώσεις. Τέλος η εταιρεία Coldwell Banker χρησιμοποιεί την τεχνολογία Blockchain μέσω της πλατφόρμας της εταιρείας Propy για να απαριθμήσει τους πωλητές και τους πράκτορες της, προσφέροντας επίσης και συναλλαγές και συμβάσεις.

3.4.10 Κυβερνήσεις (Government)

Στον κυβενητικό τομέα η συμβολή του blockchain αρχίζει ήδη να διαχέεται. Η κυβέρνηση του Ντουμπάι στοχεύει στην πρώτη έξυπνη πόλη στον κόσμο μέχρι το 2021. Για το σκοπό αυτό, σχημάτισαν το κυβερνητικό γραφείο του Smart Dubai και με την συνεργασία μιας σειρά εταιρειών τεχνολογίας για να σχεδιάσουν το μελλοντικό σχέδιο της έξυπνης πόλης χρησιμοποιώντας το blockchain. Μέχρι στιγμής έχουν ήδη λίγους τομείς που χρησιμοποιούν την τεχνολογία αλλά σχεδιάζουν να την συμπεριλάβουν και σε άλλους. Ακόμη η μητροπολιτική κυβέρνηση της Σεούλ θα εγκαταστήσει το νέο της διοικητικό σύστημα βασισμένο στην blockchain τεχνολογία. Πιο συγκεκριμένα μαζί με το

έργο αυτό οι κάτοικοι της πόλης θα έχουν το S-coin που θα μπορούν να χρησιμοποιήσουν στις δημόσιες υπηρεσίες, να πληρώνονται αλλά και να πληρώνουν φόρους και να συμμετέχουν στις δημόσια κοινά μέσω της πλατφόρμας. Επίσης η Lantmäteriet που είναι το εθνικό κτηματολόγιο της Σουηδίας πλέον συνεργάζεται με τράπεζες και επιχειρήσεις για ένα δοκιμαστικό blockchain. Πιστεύουν πως η αγορά ενός ακινήτου είναι πολύ χρονοβόρα και με το blockchain μπορεί να εξοικονομηθούν πόροι και χρόνος. Όλα τα έγγραφα θα είναι σε ψηφιακές μορφές και όχι χειρόγραφα. Επιπροσθέτως η Εθνική Υπηρεσία Φαρμάκων της Ουγκάντα συνεργάζεται με τη MediConnect για να αντιμετωπίσει τα προβλήματα παραποίησης / απομίμησης φαρμάκων στην χώρα. Σύμφωνα με όσα δηλώνουν, το έργο αυτό θα παρακολουθεί όλα τα φάρμακα από τις φαρμακευτικές εταιρείες για να εξασφαλίσει ότι κανείς δεν μπορεί να τα κλέψει ή να τα αντικαταστήσει με απομιμήσεις των αληθινών. Τέλος η Νομισματική Αρχή της Σιγκαπούρης οδηγείται σ ένα blockchain που προσφέρει πληρωμές σε διαφορετικά νομίσματα στο ίδιο δίκτυο. Σε συνεργασία με την Temasek και την J.P. Morgan, το MAS σχεδιάζει να βελτιώσει τη συνολική αποδοτικότητα του κόστους των επιχειρήσεων σε ολόκληρη τη χώρα. Προς το παρόν, εξακολουθούν να το δοκιμάζουν για βιομηχανικές εφαρμογές.

3.5 Συμπεράσματα κεφαλαίου

Όταν αναφερόμαστε σε δημόσια και ιδιωτικά blockchain είναι σημαντικό να κατανοήσουμε ότι η βασική διαφορά μεταξύ τους είναι η διαχείριση της ταυτότητας. Σε ένα ιδιωτικό blockchain γνωρίζουμε ποιοι είναι όλοι οι συμμετέχοντες από την αρχή ενώ σε ένα δημόσιο blockchain δεν γνωρίζουμε ποιοι είναι οι συμμετέχοντες αλλά θα πρέπει οι αρχιτέκτονες και οι προγραμματιστές να αναπτύξουν τη λογική και τους μηχανισμούς διαχείρισης της ταυτότητας. Οι δύο αυτοί διαφορετικοί τύποι είναι δύο πολύ διαφορετικοί μεταξύ τους και εξυπηρετούν διαφορετικούς σκοπούς.

Για παράδειγμα σε ένα κρυπτονόμισμα όπως το Bitcoin, το Litecoin, το Ethereum κ.λπ., δεν θέλουμε να έχουμε περιπτώσεις όπου χρειάζεται πρόσβαση ή άδεια για την συμμετοχή σε αυτό καθώς οποιοσδήποτε πρέπει να είναι σε θέση να τα κατέχει αλλά και να τα εμπορεύεται με κάποιον άλλον. Έτσι αυτό οδηγεί σε ένα ανοιχτό χωρίς άδεια μοντέλο με πλήρη διαφάνεια όπου όλοι οι χρήστες αντιμετωπίζονται το ίδιο. Αντιθέτως στον εταιρικό κόσμο τα πράγματα είναι πολύ διαφορετικά. Θέλουμε στις επιχειρήσεις να γνωρίζουμε ακριβώς ποιοι είναι όλοι οι συμμετέχοντες επειδή επιθυμούμε την πλήρη διαφάνεια. Δεν θέλουμε προφανώς να μοιραστούμε όλα μας τα επιχειρηματικά δεδομένα με όλα τα άτομα του επιχειρηματικού κόσμου ή με το ευρύ κοινό. Θέλουμε να ελέγχουμε ποιος βλέπει τι είδους πληροφορία, υπό ποιες συνθήκες και επίσης να ελέγξουμε ποιος είναι σε θέση να γράψει τις πληροφορίες αυτές στο blockchain. Για παράδειγμα θα μπορούσαμε να χρησιμοποιήσουμε ένα ιδιωτικό blockchain για να διαχειριστούμε την σχέση μεταξύ μιας εταιρείας πωλήσεων και των προμηθευτών της. Δηλαδή μόνο ένα συγκεκριμένο αντισυμβαλλόμενο μέρος χρειάζεται να βλέπει τις λεπτομέρειες της σύμβασης που έχουν συνάπτει και όχι τις λεπτομέρειες μιας σύμβασης που μπορεί να έχει η εταιρεία με άλλους προμηθευτές ή άλλα άτομα. Επιπροσθέτως μπορεί η εταιρεία πωλήσεων να θέλει να μοιραστεί μερικά από αυτά τα δεδομένα με κάποιους καταναλωτές για να δουν την προέλευση και τα χαρακτηριστικά των προϊόντων που αγοράζουν.

Επίσης αυτό που παρατηρούμε είναι πως τα δημόσια blockchains έχουν την τάση να επικεντρώνονται περισσότερο σε σενάρια B2C ή C2C ενώ ένα ιδιωτικό blockchain, όπως το Hyperledger που είναι πραγματικά καλά δομημένο, να επικεντρώνεται σε σενάρια B2B, σε θέματα αλυσίδας εφοδιασμού, σε αλυσίδες αξίας αλλά και στην δημιουργία οποιασδήποτε κοινής υποδομής μεταξύ επιχειρήσεων.

Όσον αφορά την χρήση του Blockchain και των smart contracts μπορεί αυτή να μην είναι άμεσα ευδιάκριτη στους καταναλωτές, αλλά είναι ιδιαίτερα υποσχόμενη στο να επιτρέψει στις επιχειρήσεις να διανείμουν υπηρεσίες με χαμηλότερο κόστος από τον ανταγωνισμό. Τα smart contracts μπορούν να αποτελέσουν εξαιρετικό πεδίο για την πραγματοποίηση έμπιστων συναλλαγών μεταξύ δύο αντισυμβαλλόμενων ατόμων.

Από την στιγμή που το κόστος χρήσης της Blockchain τεχνολογίας ήταν ιδιαίτερα υψηλό στην αρχή της δημιουργίας του κυρίως λόγο των ανειδίκευτων ατόμων, της χαμηλής μάθησης και του κόστους υιοθέτησης, είναι σήμερα πιθανότερο να δούμε υψηλής αξίας εφαρμογές να εφαρμοστούν στα υπάρχοντα Blockchain. Το blockchain και οι εφαρμογές αυτές, όπως τα Smart Contracts μπορούν να αποτελέσουν πηγή έμπνευσης για τις κυβερνήσεις και τις ρυθμιστικές τους αρχές στο να δούμε για παράδειγμα ένα κυβερνητικό κρυπτονόμισμα με φθηνότερο σύστημα πληρωμών που θα βρίσκεται σε ένα κατανεμημένο καθολικό δίκτυο.

Τέλος όπως παρατηρούμε και από τα παραδείγματα των μεγαλύτερων εταιρειών παγκοσμίως που χρησιμοποιούν την τεχνολογία του Blockchain, αυτό αποτελεί πραγματικά μια νέα ανερχόμενη δύναμη που κανείς δεν μπορεί να δαμάσει (ακόμα) αλλά ούτε να αδιαφορήσει και για την ύπαρξη της. Ήδη διαταράσσει πολλές βιομηχανίες και σύντομα, θα αποτελέσει κομμάτι σε πολλούς τομείς σε όλο τον κόσμο. Προς το παρόν οι εταιρείες που χρησιμοποιούν την τεχνολογία blockchain εξασφαλίζουν στην πραγματικότητα τη θέση τους στο συνεχώς μεταβαλλόμενο παγκόσμιο περιβάλλον, ενώ αντίθετα εκείνες που δεν θα επενδύσουν στην τεχνολογία αυτή θα αντιμετωπίσουν προβλήματα από τον ανταγωνισμό.

Κεφάλαιο 4: Ανάλυση του μοντέλου των Abadi J. και Brunnermeier M.

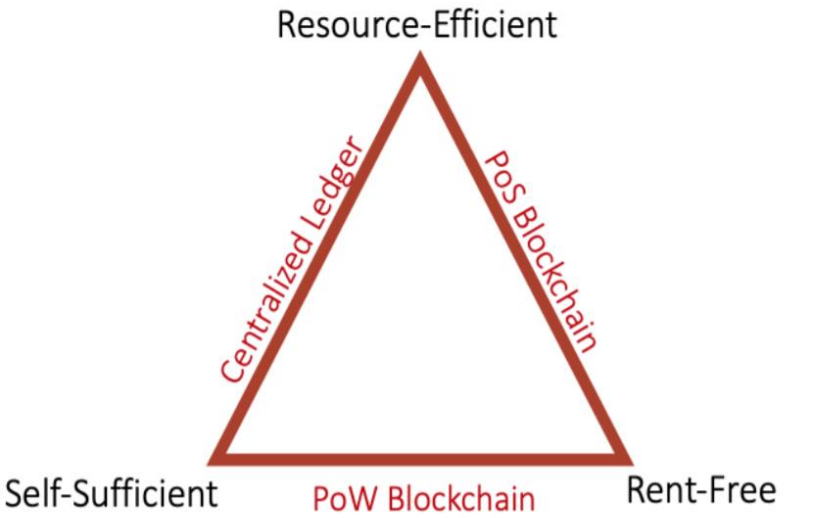
8.1 Εισαγωγή Κεφαλαίου

Οι Abadi J. και Brunnermeier M. στο άρθρο τους Blockchain Economics (2019) απαντώντας στο βασικό ερώτημα που ενέπνευσε την δημιουργία των δημόσιων καθολικών δικτύων δηλαδή εάν μπορεί να επιτευχθεί συναίνεση χωρίς την διαμεσολάβηση μιας κεντρικής έμπιστης αρχής απέδειξαν ότι είναι απίθανο για ένα ψηφιακό καθολικό σύστημα καταγραφής συναλλαγών blockchain ταυτόχρονα να εξυπηρετεί τρεις σκοπούς. Δηλαδή να είναι ανεξάρτητο (self- sufficient), να είναι χωρίς κόστος χρήσης (free-rent) και να κάνει αποδοτική χρήση των πόρων του (resource-efficient).

Ουσιαστικά αυτούς τους τρεις παράγοντες τους ονόμασαν το τρίλημμα του Blockchain ή Blockchain Trilemma και αναφέρουν πως ένα ψηφιακό καθολικό σύστημα καταγραφής συναλλαγών που δεν βασίζεται στο κόστος χρήσης του δικτύου ούτε στα κόστη που συνδέονται με τους πόρους, τότε θα βασίζεται σε κάποια εξωτερική πηγή εμπιστοσύνης. Όλα αυτές οι ιδέες που αποτυπώθηκαν από τους Abadi J. και Brunnermeier M. αποτέλεσαν σημείο έμπνευσης και αναζήτησης για το πως κατέληξαν στα παραπάνω αυτά συμπεράσματα και σε τι δεδομένα και υποθέσεις βασίστηκαν. Για τον λόγο αυτό το συγκεκριμένο κεφάλαιο αποσκοπεί να παρουσιάσει το μοντέλο και τις μεταβλητές που ανέπτυξαν οι δύο ερευνητές με στόχο να γίνει περισσότερο κατανοητό το τρίλημμα του Blockchain και οι πτυχές που βασίζεται αλλά και να το εφαρμόσουμε σε ένα πρακτικό παράδειγμα που θα μπορούσε να συμβαίνει στον πραγματικό κόσμο λαμβάνοντας υπόψιν τις τρεις περιπτώσεις αλγορίθμων συναίνεσης που χρησιμοποιούν.

Στην ακόλουθη εικόνα παρουσιάζονται οι τρεις πτυχές που βασίζεται το τρίλημμα του Blockchain.

Εικόνα 8.1.1: Το τρίλημμα του blockchain



\

Πηγή: Abadi J., Brunnermeier M. (2019)

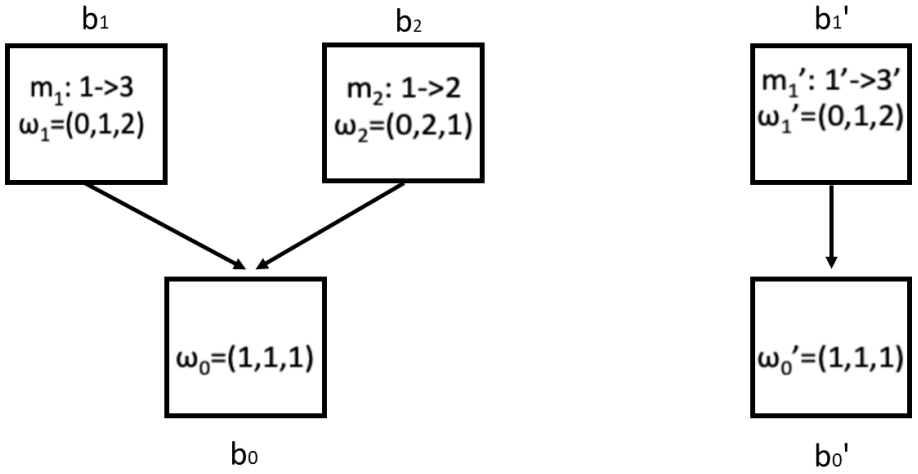
8.2. Παραδείγματα αλγόριθμων συναίνεσης στην ανάλυση του μοντέλου

Ο αλγόριθμος συναίνεσης αποτελεί τον μηχανισμό μέσω του οποίου σε ένα ιδιωτικό blockchain (Private Blockchain), σε ένα που χρησιμοποιεί σύστημα Proof of Stake (PoS), και σε ένα που χρησιμοποιεί σύστημα ο Proof of Work (PoW) να επιτρέπει στους πράκτορες του δικτύου, να έχουν γνώση πρώτον του προηγούμενου επιπέδου της συναίνεσης που δίνεται από μια αλυσίδα που θα την συμβολίζουμε με C και δεύτερον την παρούσα κατάσταση που έχουν τα blocks που θα την συμβολίζονται με (B), να έρθουν σε μια συμφωνία με ένα νέο επίπεδο συναίνεσης όταν προστίθεται ένα νέο block. Ο αλγόριθμος συναίνεσης μπορεί λοιπόν να περιγράφει ως μια συνάρτηση $g(C, B) = C'$. Σε αυτή την συνάρτηση θα έχουμε ως υπόθεση πως ο αλγόριθμος συναίνεσης εξαρτάται μόνο από τις κεφαλές (header) που υπάρχουν σε κάθε block όπως συμβαίνει δηλαδή στην πραγματικότητα. Αναλυτικότερα, να αναφέρουμε πως η κεφαλή (header) που υπάρχει σε κάθε block (b) περιέχει ένα μήνυμα το οποίο ονομάζεται ψήφος και το συμβολίζουμε με $\upsilon\ (b)$. Ουσιαστικά ο αλγόριθμος συναίνεσης είναι αποτελεσματικά

ένας τρόπος με τον οποίον αποφασίζεται η επόμενη κατάσταση του θα επέλθει το Blockchain έχοντας ως γνώμονα αυτή την κατάσταση που βρισκόταν προηγουμένως με την κάθε ψήφο να μεταδίδεται στο επόμενο block που σχηματίζεται.

Στο σημείο αυτό θα ακολουθήσει η περιγραφή τριών ιδιαίτερα διαδεδομένων κατηγοριών που επιτυγχάνεται η αλγοριθμική συναίνεση που αναφερθήκαμε προηγουμένως και θα υπογραμμίσουμε τα προβλήματα που μπορεί να εγείρονται σε κάθε περίπτωση. Αρχική υπόθεση για να πραγματοποιηθεί η ανάλυση μας είναι πως έχουμε ένα παιχνίδι με τρείς παίχτες, την Παίχτρια 1, τον Παίχτη 2 και την Παίχτρια 3 και πως υπάρχουν δύο χρονικές περίοδοι η $t = 1,2$. Σε αυτές τις δύο περιόδους η Παίχτρια 1 και ο Παίχτης 2 βρίσκονται στο παρόν στην περίοδο $t = 1$ και γνωρίζουν το αληθινό genesis block το οποίο θα έχει τον συμβολισμό b_o και η αληθινή κατάσταση θα συμβολίζεται με ω_o η οποία είναι ίση με $\omega_o = (1,1,1)$. Παρόλα αυτά να επισημάνουμε πως έχουμε σαν προϋπόθεσή πως η Παίχτρια 3 δεν γνωρίζει αυτή την πληροφορία και εισέρχεται μόνο την δεύτερη περίοδο δηλαδή την $t = 2$

Εικόνα 8.2.1: Η κατάσταση των blocks και της πληροφόρησης των παιχτών



Πηγή: Abadi J., Brunnermeier M. (2019)

Ας υποθέσουμε πως η Παίχτρια 1 θέλει να δημιουργήσει ένα νέο genesis block την χρονική στιγμή $t = 1$ το οποίο θα είναι το ${b'}_o$ και η κατάσταση του θα είναι η ${\omega'}_o$ η οποία θα είναι ίση με ${\omega'}_o = (1,1,1)$. Σε αυτή την κατάσταση η Παίχτρια 1 διαθέτει όλα τα ιδιωτικά κλειδιά που αντιστοιχούν στους λογαριασμούς στο νέο genesis block που δημιούργησε αλλά αυτή η πράξη της δεν είναι δημοσίως γνωστή στους υπόλοιπους συμμετέχοντες στο δίκτυο. Ακόμη η Παίχτρια 1 θα στείλει ένα μήνυμα ${m'}_1$ με το οποίο ο λογαριασμός με αριθμό 1 θα πραγματοποιεί μια αποστολή ενός token από τον λογαριασμό αυτόν στον λογαριασμό νούμερο 3 στην καινούργια αλυσίδα που διακατέχεται από την κατάσταση ${\omega'}_1 = (0,1,2)$ και βρίσκεται στο block ${b'}_1$ που ακολουθεί το ${b'}_o$. Επομένως στην κατάσταση που έχει πλέον διαμορφωθεί, όπως μπορούμε να παρατηρήσουμε στην εικόνα 8.2.1, αυτά τα δύο block είναι αντιφατικά μεταξύ τους καθώς το b_1 και το b_2 περιέχουν τα μηνύματα m_1 και m_2.

Να σημειώσουμε πως ένας αλγόριθμος συναίνεσης $g(C, B)$ δεν εγγυάται απαραίτητα την συναίνεση όταν κάποιος πράκτορας δεν γνωρίζει την αρχική κατάσταση. Στο παράδειγμα μας η Παίχτρια 3 μπορεί να ζητήσει επιπλέον πληροφορίες σχετικά με την αρχική κατάσταση του συστήματος την στιγμή που εισέλθει στο δίκτυο έτσι ώστε να επέλθει η συναίνεση. Φυσικά για να συμβεί αυτό υποθέτουμε βέβαια πως η Παίχτρια 3 είναι κοινωνικά συνδεδεμένη με την Παίχτρια 1 και τον Παίχτης 2 και μπορούν να επικοινωνούν μεταξύ τους με ιδιωτικής φύσεως μηνύματα.

8.2.1 Ιδιωτικό Blockchain (Private Blockchain)

Στην περίπτωση ενός ιδιωτικού Blockchain, για την απλούστευση της ανάλυσης αυτής θα υποθέσουμε πως έχουμε μια κατάσταση στην οποία ένα άτομο αποτελεί και τον μονοπωλιούχο του δικτύου. Το άτομο αυτό κατέχει ταυτόχρονα την μια και μοναδική μη μεταφερόμενη ψήφο υπό την μορφή token σε έναν λογαριασμό. Η ψήφος αυτή περιέχει και την υπογραφή του μονοπωλιούχου καθώς είναι ο μόνος που έχει το ιδιωτικό κλειδί που μπορεί να χρησιμοποιηθεί για να υπογράφει μηνύματα που στέλνονται από τους υπόλοιπους αντίστοιχους λογαριασμούς του δικτύου. Στην ανάλυση μας θα θεωρήσουμε πως μια ψήφος στο block b θα συμβολίζεται με $\upsilon\ (b) = 1$.

Ο αλγόριθμος συναίνεσης δίνει σε κάθε πράκτορα που γνωρίζει το genesis block την ικανότητα να έχει γνώση στην κατάσταση που βρίσκεται το δίκτυο. για την επέκταση

του δικτύου οι πράκτορες πολύ απλά αναζητούν κάθε φορά την μακρύτερη σε μήκος αλυσίδα στην οποία το token έχει ψηφίσει κάθε φορά το νέο block. Παρόλα αυτά ας υποθέσουμε πως ο μονοπωλιούχος έχει ψηφίσει αντιφατικές μεταξύ τους αλυσίδες για να μπερδέψει τους πράκτορες του δικτύου, τότε εάν οι πράκτορες αντιληφθούν την απόκλιση του, θα χαθεί η συναίνεση και μπορεί ακόμα χειρότερα να υπάρξει και η περίπτωση εγκατάλειψης του συστήματος από τους συμμετέχοντες σε αυτό. Τυπικά ο αλγόριθμος συναίνεσης επιλέγει εκείνο το $g(C,B)=C'$ να αποτελεί την μακρύτερη αλυσίδα C' στην οποία εμπεριέχεται το γνωστό genesis block έτσι ώστε να ισχύει $v=1$ για κάθε block στην αλυσίδα C'. Να αναφέρουμε πως στην περίπτωση που υπάρχει παραπάνω από μια τέτοια αλυσίδα, τότε δεν επιλέγεται καμία και ουσιαστικά επιλέγεται το κενό σύνολο $g(C,B)=\emptyset$ ανεξάρτητα από την αρχική αλυσίδα C.

Να επισημάνουμε πως στην περίπτωση μας δεν υπάρχει κάποιος εκ των προτέρων τρόπος διάκρισης των δύο blockchains με τα διαφορετικά genesis blocks. Δηλαδή οι πράκτορες δεν γνωρίζουν σε ποια κατάσταση ο μονοπωλιούχος έχει βάλει την υπογραφή του το οποίο εγείρει την πιθανότητα να διαπράττει κάποια πράξη απάτης.

Με βάση λοιπόν τα δεδομένα που αναλύσαμε προηγουμένως ας υποθέσουμε πως η Παίχτρια 1 είναι ο μονοπωλιούχος και έχει την δυνατότητα να επιλέξει στο blockchain με genesis block το b_0 είτε να περιλαμβάνεται το μήνυμα m_1 είτε το μήνυμα m_2. Αλλά δεν είναι όμως εφικτό να επιλέξει το m_1 και μετά να αντιστρέψει την προτίμηση της αυτή και να δημιουργήσει ένα block στο οποίο θα περιλαμβάνεται το m_2. Επομένως σε αυτή την περίπτωση εάν είναι ο Παίχτης 2 είναι να λάβει μια πληρωμή, τότε η Παίχτρια 1 πρέπει να έχει ψηφίσει στο b_1 την χρονική στιγμή $t=1$ και η συναλλαγή καθίσταται μη αναστρέψιμη από την μεριά του Παίχτη 2.

Ας υποθέσουμε τώρα πως η Παίχτρια 3 είναι να εξαπατηθεί και έχουμε την περίπτωση που η Παίχτρια 1 μεταδίδει την μια ψήφο της $v=1$ στο block b'_1. Τότε η Παίχτρια 3 που έρχεται εκείνη την χρονική στιγμή διακρίνει ένα blockchain που η παρούσα κατάσταση του είναι η ω_1 και ένα άλλο που είναι η ω'_1 χωρίς να υπάρχει κανένας τρόπος να τα διακρίνει από μόνη της αλλά μπορεί να βασιστεί μόνο στα κοινωνικά μηνύματα μεταξύ των παιχτών. Εάν για παράδειγμα η Παίχτρια 3 εμπιστεύεται την Παίχτρια 1 που είναι ο μονοπωλιούχος για να της παρέχει αυτές τις πληροφορίες, τότε η Παίχτρια 1 μπορεί να ισχυριστεί ότι το genesis block b_0 είναι μη αληθές και η κανονική κατάσταση του δικτύου που βρίσκεται η υπογραφή της είναι το b'_0.

Ποιος όμως μπορεί να είναι ο τρόπος με τον οποίο η Παίχτρια 1 θα παρακινηθεί από την Παίχτρια 3 έτσι ώστε να της μεταδόσεις την σωστή κατάσταση του δικτύου; Ο τρόπος παρακίνησης μπορεί να είναι στο ότι η Παίχτρια 3 εάν αντιληφθεί ή μαθευτεί το ψέμα της απόκλισης από την πραγματική κατάσταση μπορεί να τιμωρήσει την Παίχτρια 1 για το ψέμα της εγκαταλείποντας το δίκτυο. Έτσι στην περίπτωση που η Παίχτρια 1 εξάγει έσοδα από τους χρήστες του μονοπωλιακού συστήματος της, τότε θα προτιμήσει να κρατήσει την Παίχτρια 3 ως χρήστη του δικτύου και να την έχει σε μακροπρόθεσμο ορίζοντα απ' ότι να την εξαπατήσει και να κερδίσει βραχυπρόθεσμα.

8.2.2 Proof of stake blockchain (PoS)

Στην περίπτωση ενός PoS συστήματος, η δύναμη της ψήφου είναι συνδέεται με τα χρηματικά tokens που έχει ο καθένας. Όταν καθορίζεται ποιο μήνυμα τελικά περιλαμβάνεται στο blockchain, η ψηφοφορία γίνεται με βάση τον αριθμό των tokens που κατέχουν τα άτομα πριν την εκτέλεση της μεταφοράς. Αυτό στο παράδειγμα μας είναι στο block b_0 που η Παίχτρια 1 ας πούμε πως έχει τα 2/3 από τις ψήφους του δικτύου και ο Παίχτης 2 τις υπόλοιπες, χωρίς να έχει σημασία για αυτόν ποιο μήνυμα επιλέγεται. Το PoS σύστημα blockchain τυπικά λειτουργεί με τον κανόνα της μεγαλύτερης πλειοψηφίας. Μια ψήφος που συμβολίζεται με υ αποτελείται από τις ταυτότητες των λογαριασμών που ψηφίζουν σε κάθε block και λέμε πως ένα μέρος α από tokens αποτελούν την ψήφο σε ένα block εάν αυτό το μερίδιο των tokens περιλαμβάνεται στους λογαριασμούς που ψηφίζουν στο block και είναι ίσο με α. Ο αλγόριθμος συναίνεσης λοιπόν επιλέγει το $g(C, B) = C'$ όπου το C' είναι η μεγαλύτερη σε μήκος αλυσίδα που περικλείει την C αλυσίδα καθώς τουλάχιστον τα 2/3 όλων των tokens ψήφισαν το κάθε block στην C' και τα μέρη των tokens που ψήφισαν τα αντιφατικά blocks είναι λιγότερο από το 1/3.

Να αναφέρουμε πως η δεύτερη συνθήκη σημαίνει πως λιγότερο από το 1/3 από τα tokens χρησιμοποιήθηκαν για να μεταδώσουν πολλαπλές αντιφατικές ψήφους. Να αναφέρουμε πως στην περίπτωση που το C εσωκλείεται σε ένα δέντρο από blocks στο οποίο κάποιες αντιφατικές ψήφοι έχουν μεταδοθεί τότε δεν επιλέγεται καμία αλυσίδα και ουσιαστικά επιλέγεται το κενό σύνολο $g(C, B) = \emptyset$. Εάν όμως υπάρχει επαρκής αμφιλεγόμενη κατάσταση συναίνεσης τότε τιμωρείται με την απώλεια της συναίνεσης αυτής με τον ίδιο ακριβώς τρόπο που συμβαίνει και στο private blockchain που

περιγράψαμε προηγουμένως, με την μόνη διαφορά να είναι πως υπάρχει κάποιο επίπεδο ανοχής για μικρά επίπεδα αμφιλεγόμενης ψηφοφορίας.

Έτσι με τον τρόπο που περιγράψαμε είναι πολύ εύκολο να ελεγχθεί εάν μια κατάσταση που περιέχεται στην αλυσίδα C μπορεί να αντιστραφεί με αυτόν τον κανόνα ανανέωσης του δικτύου. Ας υποθέσουμε για παράδειγμα πως η Παίχτρια 1 και ο Παίχτης 2 χρησιμοποιούν ένα token για να ψηφίσουν στο block b_1, τότε η Παίχτρια 1 θα πρέπει να χρησιμοποιήσει όλα τα 2/3 των tokens της για να ψηφίσει ένα block που περιέχει το b_2 εάν θέλει η κατάσταση ω_2 για να έχει μια πιθανότητα να θεωρηθεί το σημείο συναίνεσής. Αυτό μπορεί βέβαια να απαιτεί από την Παίχτρια 1 να χρησιμοποιήσει τουλάχιστον έναν λογαριασμό για να ψηφίσει τόσο το ω_1 όσο και το ω_2 εάν θέλει να μεταβούνε στην κατάσταση ω_2. Με αυτόν τον τρόπο αντί να δημιουργήσει μια κατάσταση στην οποία η Παίχτρια 3 θα μπερδευτεί και θα πιστεύει πως το ω_2 είναι το επίπεδο της συναίνεσης, η Παίχτρια 1 θα καταφέρει να καταστρέφει την συναίνεση δημιουργώντας αμφιβολία με δύο καταστάσεις. Όπως και στην περίπτωση του Private blockchain, η γνώση μιας αρχικής κατάστασης είναι ικανή στο να δημιουργήσει μη αναστρέψιμη συναίνεση. Παρόλα αυτά όπως μπορούμε να κατανοήσουμε η χρήση αυτού του τρόπου συναίνεσης είναι υποκειμενική και έτσι υπάρχει η έκθεση στον ίδιο τύπο επίθεσης όπως στην περίπτωση του ιδιωτικού (private) συστήματος. Ο λόγος που συμβαίνει αυτό είναι γιατί η Παίχτρια 1 έχει την δυνατότητα να χρησιμοποιήσει την υπερ πλειοψηφία της για την ψηφοφορία στην κατάσταση ω'_0 για να ψηφίσει το ω'_1 στο οποίο θα ξεγελάσει την Παίχτρια 3 στην περίπτωση που η Παίχτρια 1 μεταδίδει ανακριβή κοινωνικά μηνύματα λέγοντας στην Παίχτρια 3 ότι οποιοδήποτε λογισμικό εμπεριέχει το b_0 ως genesis block είναι απατηλό.

Υπό αυτή την υπόθεση, η πληρωμή ενός χρηματικού ποσού για την χρήση του δικτύου ως ενοίκιο δεν αποτελεί λύση για την ύπαρξη ασφάλειας σε αυτό έτσι ώστε η Παίχτρια 1 να μην ξεγελάσει την Παίχτρια 3. Όταν ο κάτοχος του λογαριασμού είναι ανώνυμος, η Παίχτρια 3 πιθανώς να μην είναι σε θέση να κατασταλάξει εάν η Παίχτρια 1 εξάγει χρηματικά ενοίκια από το σύστημα, οπότε η απειλή για την εγκατάλειψη του δικτύου μπορεί να μην επηρεάζει την Παίχτρια 1. Πιθανώς η Παίχτρια 3 θα πρέπει να βασιστεί στην κοινωνική εμπιστοσύνη που υπάρχει ανάμεσα σε εκείνη και την Παίχτρια 1 που είναι φυσικά εξωτερική από το σύστημα όπως ακριβώς συμβαίνει σε μια αμοιβαίας ωφέλειας διαπροσωπική ή επιχειρησιακή σχέση η οποία μπορεί να καταρρεύσει εάν η Παίχτρια 1 πει ψέματα.

8.2.3 Proof of Work blockchain (PoW)

Στην περίπτωση ενός PoW συστήματος blockchain η κατανομή της δύναμης της ψήφου γίνεται ως ποσοστό της συνολικής υπολογιστικής ισχύος που δαπανάται από τους πράκτορες του δικτύου. Μια ψήφος υπό αυτή την συνθήκη συναίνεσης είναι ένας πραγματικός αριθμός υ που αντιστοιχεί στο σύνολο των υπολογιστικών πόρων που δαπανώνται από τους πράκτορες στο κάθε αντίστοιχο block του δικτύου. Η διαδικασία με την οποία ανανεώνεται η αλυσίδα με το PoW σύστημα συναίνεσης είναι ιδιαίτερα απλή. Υποθέτουμε πως έχουμε ένα σταθερό κόστος που το συμβολίζουμε με α και είναι μεγαλύτερο του μηδενός $\alpha > 0$, πως έχουμε την κατανομή των blocks που την συμβολίζουμε με B και πως έχουμε και την σειρά της έγκυρης αλυσίδας των B που την συμβολίζουμε $\check{\mathrm{C}}_{\upsilon}$.

Η $\check{\mathrm{C}}_{\upsilon}$ ισχύει πως είναι ίση με την αλυσίδα C που αποτελεί υποσύνολο του B με την ψήφο $\upsilon(b)$ να είναι μεγαλύτερη ή ίση από το α για κάθε b που ανήκει στο C. Αυτή είναι η σειρά των έγκυρων αλυσίδων που περιλαμβάνει όλες τις αλυσίδες εκείνες στις οποίες κάθε block έχει λάβει τουλάχιστον ψήφους ίσες με α. Τότε το $g(C, B) = C_{max}$ όπου το C_{max} είναι η αλυσίδα με το μεγαλύτερο συνολικό υπολογιστικό κόστος που δαπανήθηκε και δίνεται από την ακόλουθη σχέση.

$$C_{max} = \alpha gr \max_{C' \subset \check{\mathrm{C}}_{\upsilon}} \upsilon\,(C') \equiv \alpha gr \max_{C' \subset \check{\mathrm{C}}_{\upsilon}} \sum_{b \in C'} \upsilon\,(b) \qquad (1)$$

Στον συγκεκριμένο τρόπο συναίνεσης οι πράκτορες δεν ζητούν επιπλέον πληροφορίες για να έρθουν σε συναίνεση, αλλά όπως συμβαίνει στα PoW blockchain ακολουθούν τον κανόνα της μεγαλύτερης αλυσίδας. Ουσιαστικά αυτό σημαίνει πως το επίπεδο της συναίνεσης στο PoW δίνεται από την αλυσίδα εκείνη με την μεγαλύτερη συνολική δυσκολία της λύσης των μαθηματικών προβλημάτων στον αλγόριθμο PoW και της προσθήκης ενός επιπλέον block που χρειάζεται ένα σταθερό κόστος υπολογιστικής εργασίας.

Ας υποθέσουμε λοιπόν πως την χρονική στιγμή $t = 1$ το block b_1 λαμβάνει ψήφους ίσες με α τόσο από την Παίχτρια 1 όσο και από τον Παίχτης 2. Το επίπεδο συναίνεσης στο τέλος της χρονικής στιγμής $t = 1$ είναι το ω_1. Εάν όμως η Παίχτρια 1 στο τέλος της περιόδου $t = 2$ επιθυμεί η Παίχτρια 3 να πιστεύει πως η παρούσα κατάσταση είναι το ω_2

πρέπει απλά να πληρώσει ένα κόστος $\alpha + \varepsilon$,όπου το ε είναι μεγαλύτερο του μηδενός, για να μπορέσει να ψηφίσει το block b_2. Μόλις το κάνει αυτό τότε το ω_2 θα γίνει το επίπεδο συναίνεσης και τόσο η Παίχτρια 3 όσο και για τον Παίχτης 2 οι οποίοι θα δράσουν με βάση αυτό το επίπεδο και όχι με το s_1. Έτσι με αυτόν τον τρόπο η πληρωμή που πραγματοποιείται στο αρχικό παράδειγμα μας προς τον Παίχτη 2 αντιστρέφεται με επιτυχία. Να αναφέρουμε πως οι επιθέσεις αυτού του είδους είναι πολύ συχνά αναφερόμενες από τους ανθρώπους της επιστήμης των υπολογιστών ως «επιθέσεις 51%» στις οποίες ένας πράκτορας αποκτά το μεγαλύτερο μέρος της διαθέσιμης υπολογιστικής δύναμης.

Τέλος αυτό που αξίζει να αναφέρουμε είναι πως ενώ η Παίχτρια 1 υφίσταται εκ των υστέρων κόστη με την εξαπάτηση της Παίχτρια 3 σε ένα ιδιωτικό (private) blockchain και σε ένα σύστημα συναίνεσης PoS, αντιθέτως στο PoW το κόστος για την εξαπάτηση της Παίχτρια 3 συμβαίνει εκ των προτέρων. Το μόνο ουσιαστικά που αποτρέπει την Παίχτρια 1 από το να αντιστρέψει την πληρωμή της από τον Παίχτης 2 όπως γίνεται κατανοητό είναι το κόστος της υπολογιστικής ενέργειας που απαιτείται για να καταπατηθεί η αρχική πληρωμή. Απλώς να αναφέρουμε πως για την απλότητα της κατάστασης στο παράδειγμα που αναφερθήκαμε προηγουμένως υποθέτουμε πως ο Παίχτης 2 αποδέχεται την πληρωμή αφού έχει συμπεριληφθεί σε ένα μοναδικό block. Στην πραγματικότητα όμως όταν ένας πωλητής παραδίδει ένα αγαθό σε έναν αγοραστεί περιμένει να έχουν μεσολαβήσει αρκετά blocks από εκείνα που περιλαμβάνουν την πληρωμή. Έτσι σε αυτή την περίπτωση η Παίχτρια 1 θα έπρεπε να αντικαταστήσει πολλά blocks και όχι μόνο ένα για να προβεί στην εξαπάτηση.

8.3. Το μαθηματικό μοντέλο των Abadi J. και Brunnermeier M.

Στο σημείο αυτό της διπλωματικής εργασίας ακολουθεί η παρουσίαση του μαθηματικού μοντέλου των Abadi J. και Brunnermeier M. Πραγματοποιείται αρχικά μια περιληπτική αναφορά στα θεμελιώδη στοιχεία που αφορούν την διαδικασία πραγματοποίησης μιας αλληλεπίδρασης μεταξύ παιχτών-διαφορετικών ατόμων σε ένα Blockchain.

8.3.1 Η κατάσταση του μοντέλου

Ο βασικός σκοπός του Blockchain στο μοντέλο που αναλύουμε είναι στο να παρακολουθεί εάν διατηρείται μια κατάσταση ω που ανήκει σε ένα σύνολο Ω που αποτελείται από διαφορετικούς τύπους ψηφιακών νομισμάτων που αντιστοιχούν σε μετρήσιμους ανώνυμους λογαριασμούς. Τα μηνύματα θα συμβολίζονται από το σημείο αυτό με m όπου το $m = (n, n', s)$ με το n να συμβολίζει τον έναν λογαριασμό, το n' τον άλλον λογαριασμό και το s τα tokens που μεταφέρονται από τον λογαριασμό n στον n'. Εάν το n είναι ίσο με το μηδέν τότε σημαίνει πως τα tokens που είναι s σε πλήθος κατανέμονται στον λογαριασμό n'. Όπως είναι κατανοητό τα μηνύματα χρησιμοποιούνται για να ανανεώνουν την κατάσταση του δικτύου.

8.3.2 Ορισμοί του blockchain

Blocks: το genesis block είναι το πρώτο block του Blockchain. Είναι ένα σύνολο δεδομένων που περιέχει μια μοναδική κατάσταση ω. Η κατάσταση αυτή που εμπεριέχεται στο genesis block b μερικές φορές αναφέρεται ως $\omega(b)$. Ένα συνηθισμένο block ουσιαστικά περιέχει ένα σύνολο μηνυμάτων $\tilde{\mathrm{m}}$ που είναι υποσύνολο των συνολικών μηνυμάτων M, ένα σημείο σύνδεσης (pointer) με το επόμενο block και μια ψήφο (vote). Τα μηνύματα, η σύνδεση και η ψήφος όταν αναφέρονται σε ένα συγκεκριμένο block συμβολίζονται ως $\tilde{\mathrm{m}}(b), \mathrm{p(b)}$ και $\upsilon(\mathrm{b})$ αντίστοιχα.

Ένα **blockchain** C είναι μια διατεταγμένη σειρά από blocks. Η διάταξη αυτή πραγματοποιείται χάρις τις ενώσεις που έχουν τα blocks μεταξύ τους. Δηλαδή η

κατάσταση ενός Blockchain C ισούται με το επιμέρους blocks καθώς $C = (b_0, b_1 \dots b_k)$ η οποία αρχίζει με την αρχική κατάσταση που αναφερθήκαμε προηγουμένως την $\omega\ (b_0)$ η οποία συνεχώς ενημερώνεται με τα μηνύματα που εμπερικλείονται σε κάθε διαδοχικό block που ακολουθεί. Εμείς θα συμβολίζουμε μια κατάσταση ως $\omega(C)$ όταν αυτή σχετίζεται με ένα blockchain C.

Voting. Η ψηφοφορία μπορεί να διεξαχθεί είτε από τα ενδογενή ψηφιακά περιουσιακά στοιχεία του συστήματος όπως γίνεται στα επιτρεπόμενα (Permissioned) Blockchains ή σε εκείνα που χρησιμοποιούν αλγόριθμο συναίνεσης PoS, αλλά και με φυσικούς εξωτερικούς πόρους από το σύστημα όπως στην περίπτωση του PoW αλγορίθμου στον οποίο μια ψήφος που συμβολίζεται με υ , είναι ένας πραγματικός θετικός αριθμός που υποδηλώνει το ποσό της υπολογιστικής ενέργειας που δαπανήθηκε για κάθε block. Να αναφέρουμε πως στα επιτρεπόμενα (Permissioned) blockchains και σε εκείνα με PoS συναίνεση μια ψήφος υ υποδεικνύει την ταυτότητα των λογαριασμών που ψήφισαν σε ένα συγκεκριμένο block.

Τα blocks αποτελούνται από μηνύματα ψήφων τα οποία μπορούν να σταλούν από οποιονδήποτε λογαριασμό n αρκεί να περιλαμβάνουν έναν αριθμό tokens που μεταφέρουν μηνύματα $\tilde{\mathfrak{m}}$ σε ένα νέο block στο τέλος της αλυσίδας του blockchain C. Κάθε μήνυμα ψηφοφορίας περιλαμβάνει είτε την ψήφο υ που αντιστοιχεί στα tokens που βρίσκονται στον κάθε λογαριασμό για τα PoS σύστημα ή τα ιδιωτικά blockchain είτε το κόστος της υπολογιστικής ισχύς που απαιτείται από το άτομο που κατέχει κάθε λογαριασμό για το PoW σύστημα. Άρα τα μηνύματα της ψηφοφορίας εξαρτώνται από τα άτομα n, τα μηνύματα που μεταφέρονται $\tilde{\mathfrak{m}}$ το blockchain C και την ίδια την ψήφο υ. Επομένως έχουν ως $m_\upsilon = (\mathrm{n}, \tilde{\mathfrak{m}}, \mathrm{C}, \upsilon)$

Όταν μια συλλογή από μηνύματα ψηφοφορίας μοιράζεται ένα κοινό μήνυμα $\tilde{\mathfrak{m}}$ και μια κοινή αλυσίδα C τότε ένα νέο block που δημιουργείται περιέχει αυτά τα μηνύματα $\tilde{\mathfrak{m}}$. Επιπλέον μια συλλογή από ψήφους ανταμοιβής μηνυμάτων $\tilde{\mathfrak{m}}'$ μπορεί να προστεθεί στο block, οπότε τα μηνύματα του block είναι $\tilde{\mathfrak{m}}(b) = \tilde{\mathfrak{m}} \mathrm{U} \tilde{\mathfrak{m}}$. Αυτή η ανταμοιβή μηνυμάτων κατανέμει ένα κυρίαρχο δικαίωμα στους λογαριασμούς που ψηφίζουν για ένα νέο block κατά κάποιο τρόπο. Η ψήφος στο block που συμβολίζεται με $\upsilon(b)$ είναι απλά ένα σύνολο από ψήφους που περιλαμβάνονται στα μηνύματα ψηφοφορίας. Το σημείο σύνδεσης με το επόμενο block που συμβολίζεται με $p(b)$ βρίσκεται στο τελευταίο block της αλυσίδας C του blockchain.

Consensus algorithms (αλγόριθμος συναίνεσης): για να μπορέσει να υπάρχει η καταγραφή των ιστορικών αρχείων συναλλαγών σε ένα blockchain χρειάζεται η ύπαρξη ενός αλγόριθμου συναίνεσης που διατηρεί ενημερωμένη την κατάσταση του δικτύου και συμβολίζεται με $g(C,B)$. Όπου C η αλυσίδα και B ένα σύνολο blocks. Θα υποθέσουμε πως ο κανόνας g εξαρτάται μόνο από τις ενώσεις των blocks (pointers) και από τις ψήφους και όχι από τα μηνύματα που περιέχονται μέσα σε κάθε block.

Επίσης είναι απαραίτητο να προσδιορίσουμε τον τρόπο με τον οποίο οι πράκτορες ερμηνεύουν την κατάσταση που βρίσκεται το blockchain όταν δεν αρχίζουν την αρχική του κατάσταση. Στην πράξη όμως αυτό το θέμα είναι σημαντικό καθώς αυτή είναι η κατάσταση που έρχεται αντιμέτωπος ένας νέος χρήστης που μπαίνει στο Blockchain (όπως η Παίχτρια 3 προηγουμένως). Η διαδικασία κατά την οποία έρχεται ένας νέος χρήστης ονομάζεται bootstrapping. Στο μοντέλο που αναλύουμε, η κατάσταση που ανανεώνει το πρωτόκολλο του κανόνα g περιλαμβάνει ένα bootstrapping πρωτόκολλο $\hat{g}$ το οποίο παίρνει ένα σύνολο blocks B και εξάγει μια συλλογή από αλυσίδες στο B, $\hat{g}(B) = \{C'_1, C'_2, \dots C'_k\}$ με το C'_k να είναι υποσύνολο του B για όλες τις τιμές του k. Το bootstrapping πρωτόκολλο εξάγεται από την ακόλουθη σχέση:

$$\hat{g}(B) = \{C' \subset B : g(C,B) = C' \text{ για κάποιο } C \subset B\} \qquad (2)$$

8.3.3 Βασικές έννοιες του μοντέλου

Ο χρόνος είναι διακεκριμένος και ατελείωτος , $t = 0,1,2,\dots$.Υπάρχουν N παίχτες που μπορεί να συμμετέχουν ή να μην συμμετέχουν κάθε χρονική στιγμή t. Οι παίχτες που υπάρχουν στο παρόν συμβολίζονται με $P_t \subset N$. Υποθέτουμε ότι η πιθανότητα της παρουσίας ενός παίχτη εξαρτάται μόνο από την παρουσία του στην προηγούμενη περίοδο. Ενώ εάν οι παίχτες απουσιάσουν χάνουν την γνώση τους από το προηγούμενο παιχνίδι που έχει γίνει. Επίσης εάν ένας παίχτης φύγει μπορεί να αντικατασταθεί και εκείνος που εισέρχεται στην θέση του θεωρείται σαν να είναι νέος χρήστης.

Στο μοντέλο αυτό υπάρχουν δύο τύποι δραστηριότητας. Οι θεμελιώδεις δραστηριότητες και οι κοινωνικές δραστηριότητες. Οι θεμελιώδεις δραστηριότητες (fundamental activities) οι οποίες αντιστοιχούν σε ένα blockchain καθολικό μηχανισμό

στον οποίο οι παίχτες ανώνυμα μπορούν να ανταλλάξουν ένα μοναδικό αριθμητικό απτό αγαθό. Αυτές οι δραστηριότητες περιλαμβάνουν την κατανάλωση και την παραγωγή των αγαθών αλλά και οποιαδήποτε δαπάνη του συστήματος PoW που χρειάζεται για την διατήρηση των αρχείων των συναλλαγών. Οι κοινωνικές δραστηριότητες (Social activities) συνδέονται με τις διμερείς σχέσεις μεταξύ των παιχτών. Είναι πλήρως εξωτερικές από τον μηχανισμό που παρέχει την διατήρηση των αρχείων των συναλλαγών στο blockchain και όπως δείχνουμε στην συνέχεια είναι απαραίτητες για το χτίσιμο της κοινωνικής εμπιστοσύνης στους νέους χρήστες του blockchain για να έχουν πρόσβαση στο σωστό επίπεδο της κατάστασης που βρίσκεται το blockchain.

Θεμελιώδης Δραστηριότητες (Fundamental Activities):

Ο παίχτης n έχει έναν θεμελιώδη τύπο δράσης που είναι ο $\theta_{n,t}$, όπου το $\theta_{n,t} \in \Theta_n$. Ο παίχτης αυτός έχει μια κατανάλωση την χρονική στιγμή t που συμβολίζεται με $c_{n,t}$και μια συνάρτηση παραγωγής που συμβολίζεται με $y_{n,t}$. Ενώ η συνάρτηση χρησιμότητας του ατόμου είναι η $u\ (c, y, \theta)$ η οποία υποδηλώνει πως η χρησιμότητα του εξαρτάται από την κατανάλωση του, την παραγωγή του αλλά και τις προτιμήσεις του. Επίσης για τους παίχτες υπάρχει ένας συντελεστής προεξόφλησης που συμβολίζεται με δ καθώς στην διάρκεια του παιχνιδιού έχουμε την έννοια του χρόνου. Οι τιμές που μπορεί να λάβει ο συντελεστής είναι μεταξύ του μηδέν και του ένα, δηλαδή $\delta \in (0,1)$. Ο λόγος που θέτουμε θεμελιώδεις προτιμήσεις είναι γιατί μέσω αυτού του τρόπου μπορούμε να εξετάσουμε μια απλή δομή στην οποία οι παίχτες μπορεί να συμφωνούν στο εμπεριέχουν υπηρεσίες έναντι αμοιβής σε tokens.

Οι παίχτες μπορεί να υφίστανται επίσης φυσικά υπολογιστικά κόστη σε ένα PoW σύστημα με στόχο να παράγουν υ ψήφους. Για αυτές πρέπει να πληρώσουν ένα γραμμικό κόστος $\kappa\ \upsilon$ όπου το κ αντιπροσωπεύει το κόστος μιας μονάδας υπολογιστικής ισχύος. Το αποτέλεσμα αυτό γενικεύεται όταν υπάρχουν επιπλέον σταθερά κόστη της υπολογιστικής ισχύος. Η ακόλουθη σχέση παρουσιάζει την συνάρτηση χρησιμότητας των θεμελιωδών χαρακτηριστικών των παιχτών.

$$U_{n,t}^{F} = E_t\left[\sum_{s=0}^{\infty} \delta^s \left(u\left(c_{n,t+s}, y_{n,t}, \theta_{n,t+s}\right) - k\ \nu_{n,t+s}\right)\right] \qquad (3)$$

Σύμφωνα με την Σχέση 3, η συνάρτηση χρησιμότητας με βάση τα θεμελιώδη χαρακτηριστικά ενός παίχτη εξαρτάται από το προεξοφλημένο με συντελεστή δ άθροισμα της μεταβλητής u μείον τα κόστη χρήσης του δικτύου από την χρονική στιγμή μηδέν έως άπειρο. Όπου η μεταβλητή u περιλαμβάνει την κατανάλωση (c) του παίχτη την χρονική στιγμή $t+s$ καθώς αυτή πραγματοποιείται σε βάθος χρόνου, την παραγωγή (y) του παίχτη την χρονική στιγμή t και την προτίμηση που έχει την χρονική στιγμή $t+s$ δηλαδή σε βάθος χρόνου. Ενώ τα υπολογιστικά κόστη $(k\ v)$ αφορούν την καταναλωτική δαπάνη του παίχτη n επί τον αριθμό των ψήφων του την χρονική στιγμή $t+s$ δηλαδή σε βάθος χρόνου.

Κοινωνικές δραστηριότητες (Social activities)

Στις κοινωνικές δραστηριότητες οι παίχτες είναι συνδεδεμένοι σε ένα κοινωνικό δίκτυο G το οποίο ισούται με $G=(N,E)$ όπου N είναι οι παίχτες και E οι ακμές σύνδεσης των παιχτών. Εάν οι παίχτες n και n' βρίσκονται στο E τότε είναι προφανές πως είναι συνδεδεμένοι μεταξύ τους. Η σύνδεση των δύο παιχτών έχει κοινά οφέλη και στους δύο καθώς μπορούν να ανταλλάσσουν ιδιωτικά μηνύματα. Έχουν ουσιαστικά μια αμφίδρομη σχέση η οποία μπορεί να καταρρεύσει εάν κάποιος από τους δύο απουσιάσει. Η συνάρτηση χρησιμότητας του n παίχτη ισούται με εκείνη του n' και ισχύει $z_{n,n'} = z_{n',n}$ και δίνεται από την ακόλουθη σχέση.

$$U_{n,t}^{S} = E_t\left[\sum_{n'} \mathbf{1}\{n' \in P_{t+s}\}\ z_{n,n'}\right] \qquad (4)$$

Σύμφωνα με την σχέση η συνάρτηση χρησιμότητας των παιχτών με βάση τα χαρακτηριστικά του κοινωνικού δικτύου εξαρτάται με το εάν η ψευδομεταβλητη πάρει τιμή 1 τότε συνδέονται μεταξύ τους και αποκομίζουν αμοιβαία χρησιμότητα ενώ εάν πάρει τιμή 0 δεν συνδέονται και δεν έχουν αμοιβαία χρησιμότητα. Η συγκεκριμένη συνάρτηση χρησιμότητας είναι σημαντική στην ανάλυση μας καθώς αντιπροσωπεύει μια εξωτερική πηγή εμπιστοσύνης μεταξύ των παιχτών που είναι απαραίτητη για την επίτευξη της συναίνεσής. Αυτού του είδους η κοινωνική εμπιστοσύνη θα μπορούσε να έχει

αποθαρρύνει την Παίχτρια 1 να πει ψέματα στην Παίχτρια 3 στο παράδειγμα του αλγόριθμου συναίνεσης PoS. Η αμφίδρομη σχέση χρησιμότητας που δημιουργείται λειτουργεί ως ένα μέσο που επιτρέπει στους χρήστες να εμπιστεύονται πληροφορίες σχετικές με την κατάσταση του blockchain και να τις μεταφέρουν μεταξύ του κοινωνικού δικτύου που έχουν αναπτύξει. Η εμπιστοσύνη όμως υποθέτουμε για ευκολία στο μοντέλο πως προέρχεται από εξωτερικές διμερείς σχέσεις αλλά τα αποτελέσματα αυτά μπορούν να επεκταθούν σε μια πιο γενική μορφή στην οποία η εμπιστοσύνη προέρχεται από το πλεόνασμα που δημιουργείται από τις μεγαλύτερες συμπαιγνίες των ατόμων.

Στην Σχέση 5 παρουσιάζεται η συνολική χρησιμότητα των ατόμων η οποία έχει ως ακολούθως

$$U_{n,t} = U_{n,t}^{F} + U_{n,t}^{S} \qquad (5)$$

Σύμφωνα με την σχέση 5 το συνολικό προφίλ χρησιμότητας των παιχτών για κάθε περίοδο αποτελείται πρώτον από την χρησιμότητα των θεμελιωδών χαρακτηριστικών στο να δημιουργούν και να λαμβάνουν υπηρεσίες, δεύτερον από την χρησιμότητα του κοινωνικού δικτύου και τρίτον από τις υπολογιστικές δαπάνες που απαιτούνται.

Οι συντονισμένες πολυμερείς αποκλίσεις τουλάχιστον στην επικοινωνία των κοινωνικών μηνυμάτων στο κοινωνικό δίκτυο G θέτουν την ύπαρξη συνασπισμών που συμβολίζονται με g και αποτελούν υποσύνολο των συνολικών παικτών N. Κάθε πιθανός συνασπισμός g είναι συνδεδεμένος με κάποιο γράφο G και οι προτιμήσεις αυτές δίνονται από την ακόλουθη Σχέση 6:

$$U_{g,t} = \sum_{n \in g} U_{n,t} \qquad (6)$$

Υπό αυτό το πρίσμα, είναι σημαντικό να επιτρέπουμε μερικές αποκλίσεις συμπαιγνιών για να μεταφέρουν το επίπεδο. Εάν μερικές από αυτές τις αποκλίσεις δεν είναι εφικτές, η καταγραφή των αρχείων των συναλλαγών από δύο κεντροποιημένα όργανα θα ήταν πλήρως ασφαλής γιατί εάν ένα από τα δύο επιθυμεί να αποκλίνει τότε όλοι οι πράκτορες θα λάβουν αντιφατικές αναφορές και αμέσως θα εντοπιστεί η απόκλιση αυτή.

8.3.4 Επικοινωνία και αλληλεπίδραση

Σε αυτή την ενότητα θα παρουσιάσουμε το μοντέλο με το οποίο οι παίχτες επικοινωνούν μεταξύ τους και αλληλοεπιδρούν χρησιμοποιώντας το blockchain. Πρώτα θα αναφερθούμε στην αρχική δομή με την οποία οι παίχτες διατηρούν μια κατάσταση. Στην συνέχεια θα περιγράψουμε το μοντέλο από την πλευρά των χρηστών το οποίο περιλαμβάνει τόσο την μεταφορά των tokens ανάμεσα στους χρήστες όσο και τις ενέργειες εκείνες που δίνονται ως απάντηση στις μεταφορές αυτές. Τέλος συζητείται η διατήρηση των αρχείων των συναλλαγών στην οποία εμπλέκεται η δημιουργία των blocks.

Η δομή της αρχικής κατάστασης

Στην αρχή της χρονικής στιγμής $t = 0$ ένα σύνολο παιχτών P_o που είναι υποσύνολο του N βρίσκεται στο παρόν. Υπάρχει ένα genesis block b_o το οποίο είναι γνωστό στους παίχτης του P_o αλλά όχι στους υπόλοιπους, που αντιστοιχεί σε μια κατάσταση $\omega\,(b_o)$. Όπως και προηγουμένως η κατάσταση αυτή ω ανήκει στην κατάσταση Ω αποτελούμενη από εκχωρήσεις tokens σε λογαριασμούς. Υπάρχει αρχικά ένα $|P_o|$ μετρήσιμό μέγεθος λογαριασμών, με τον κάθε ένα λογαριασμό να ανήκει σε κάθε παίχτη n που ανήκει στο P_o. Τα blocks γίνονται με περιοδικό τρόπο δημόσια όσο εξελίσσεται το παιχνίδι - η διαδικασία. Όταν ένα block δημοσιοποιείται γίνεται ορατό σε όλους τους παρόντες παίχτες σε όλες τις μελλοντικές περιόδους.

Οι παίχτες πρέπει από μόνοι τους ατομικά να διατηρούν την δομή της κατάστασης. Κάθε παίχτης έχει υπό την επίβλεψη του μια αλυσίδα από blocks που ονομάζεται αρχική αλυσίδα (Initial chain) και είναι μια σύνοψη της υπάρχουσας κατάστασης. Αυτό το συνοπτικό επίπεδο που αφορά την αρχική κατάσταση της αλυσίδας των παιχτών ονομάζεται αρχικό επίπεδο (Internal state). Όταν για όλους τους παρόντες παίχτες η αρχική κατάσταση είναι σε συμφωνία για μια τελική κατάσταση τότε αυτή η κατάσταση ονομάζεται κατάσταση συναίνεσης (Consensus state). Όταν παράγονται νέα blocks οι παίχτες που βρίσκονται στο παρόν αναβαθμίζουν την αρχική τους κατάσταση χρησιμοποιώντας τον αλγόριθμο συναίνεσης g.

Οι νεοεισερχόμενοι παίχτες χρησιμοποιούν το Bootstrapping πρωτόκολλο $\hat{g}$ για να περιορίσουν την λίστα από τα πιθανά επίπεδα συναίνεσης αλλά πιθανώς να χρειάζονται κάποιες επιπλέον πληροφορίες. Σε αυτή την περίπτωση ο νέος παίχτης

n ζητάει από τα υπόλοιπα γειτονικά του άτομα στο G να του δείξουν την αλυσίδα C η οποία αντιστοιχεί στην παρούσα κατάσταση της συναίνεσης. Εάν όλα τα γειτονικά άτομα στο G αναφερθούν στην ίδια αλυσίδα, τότε επακόλουθο είναι να αποδεχτεί το νέο άτομο αυτό την αρχική αλυσίδα που αναφέρονται. Διαφορετικά αμέσως φεύγει ο νέος παίχτης και γίνεται απών. Εάν ένας γειτονικός παίχτης του n που ανήκει στον συνασπισμό G αναφέρει μια ψευδή κατάσταση την χρονική στιγμή t, και ο παίχτης αυτός το ανακαλύψει την $t + 1$ τότε θα εγκαταλείψει το δίκτυο. Οπότε το να αναφέρεις μια ψευδή κατάσταση σε έναν νέο χρήστη μπορεί να προσφέρει βραχυπρόθεσμα οφέλη από την στρέβλωση της εικόνας της κατάστασης αλλά τα αποτελέσματα θα είναι αντίθετα μακροπρόθεσμα. Πρώτα απ' όλα οι παίχτες που αναφέρουν μια ψευδή κατάσταση χάνουν την κοινωνική εμπιστοσύνη ανακόπτοντας την αμοιβαίως ωφέλιμη σχέση με τους νέους χρήστες (βλέπε κοινωνική σχέση στο G). Δεύτερον με την ψευδή κατάσταση οι παίχτες χάνουν τα ενοίκια που εξάγουν από τους νέους χρήστες διαμέσου της χρησιμοποίησης του μηχανισμού. Αυτές οι δύο δυνάμεις αντανακλούν την αντισταθμισμένη σχέση που έρχεται αντιμέτωπη η Παίχτρια 1 από το Private blockchain και το PoS σύστημα στο παράδειγμα μας όταν αποφασίζει να αναφέρει μια ψευδή κατάσταση στην Παίχτρια 3.

Από την πλευρά του χρήστη

Η ύπαρξη tokens σε λογαριασμούς είναι δημοσίως γνωστή, αλλά ο αριθμός που περιλαμβάνεται σε αυτούς είναι ιδιωτική πληροφορία. Σε οποιαδήποτε χρονική περίοδο μπορεί να υπάρχουν ιδιοκτήτες λογαριασμών που δημιουργούν νέους λογαριασμούς που δεν περιέχουν μέσα καθόλου tokens.

Όσον αφορά την χωρητικότητα που έχουν οι χρήστες, οι παίχτες μπορεί να στέλνουν μηνύματα για να μεταφέρουν tokens από έναν λογαριασμό n σε έναν λογαριασμό n'. Όλα αυτά τα μηνύματα στέλνονται με αναφορά στην αλυσίδα C που περιέχει την κατάσταση στην οποία τα tokens είναι να μεταφερθούν. Βασική αρχή είναι πως οι παίχτες μπορούν να στείλουν μηνύματα που αφορούν μόνο την δικιά τους αρχική κατάσταση αλλά μπορεί να αποκλίνουν όπως γίνεται στην περίπτωση του double spending. Μόνο ο παίχτης που του ανήκει ο λογαριασμός n μπορεί να στείλει μηνύματα στα οποία ο n στέλνει tokens σε άλλους λογαριασμούς και κανένας άλλος παίχτης δεν μπορεί να στείλει tokens από αυτόν τον λογαριασμό.

Οι παίχτες έρχονται σε συμφωνίες για να παράγουν αγαθά και να τα ανταλλάσσουν με tokens. Οι συμφωνίες αυτές είναι ανώνυμες και βασικό χαρακτηριστικό

τους είναι πως γίνονται ανάμεσα σε δύο παίχτες. Μια συμφωνία ορίζει πως ένας παραγωγός n θα στείλει $y_{n,n'}$ αγαθά στον πελάτη n' εάν ένα συγκεκριμένο μήνυμα $m_{n,n'}$ αναφέρεται σε μια πληρωμή και περιλαμβάνεται στο blockchain στο τέλος της αλυσίδας C. Σε αυτό το μοντέλο που αναλύουμε, οι συμφωνίες μεταξύ των διάφορων ατόμων είναι απαραίτητες γιατί η διαδικασία μεταφοράς μηνυμάτων μέσω tokens πρέπει να γίνει πριν λάβουν γνώση εάν θέλουν να τελικά να συμπεριληφθούν στο blockchain.

Πολύ σημαντικό είναι να αναφερθεί πως το αρχικό επίπεδο της αλυσίδας των παιχτών συνδέεται με τις ενέργειες που θα λάβουν. Θα συμφωνήσουν στην δημιουργία ενός αγαθού μόνο εάν πιστεύουν πως μια πληρωμή θα περιλαμβάνεται στο αρχικό επίπεδο συναίνεσης, με αποτέλεσμα οι συμφωνίες τους αυτές να απαιτούν τα μηνύματα των συναλλαγών να περιλαμβάνονται στις αρχικές τους αλυσίδες. Όπως πρακτικά συμβαίνει και με τους πωλητές στον πραγματικό κόσμο οι οποίοι θα περιμένουν μέχρι να πιστέψουν πως οι πληρωμές έχουν ολοκληρωθεί και μετά να μεταφέρουν τα αγαθά στους αγοραστές. Οι πραγματικές συναλλαγές μέσω κρυπτονομισμάτων πολλές φορές χρειάζονται τα ακόλουθα βήματα. Πρώτον ο αγοραστής να στείλει ένα μήνυμα που μεταφέρει τα tokens στον πωλητή και δεύτερον ο πωλητής με την σειρά του να περιμένει μέχρι το μήνυμα να εισέλθει στο blockchain και τέλος τρίτον μετά να μεταφέρει τα αγαθά στον αγοραστή.

Η πλευρά της καταγραφής των αρχείων των συναλλαγών

Υπάρχουν δύο είδη μηνυμάτων που οι παίχτες μπορούν να στείλουν για την καταγραφή των αρχείων των συναλλαγών. Το πρώτο είδος είναι όταν οι παίχτες στέλνουν μηνύματα ψηφοφορίας. Με αυτόν τον τρόπο ένας παίχτης μεταδίδει μια ψήφο v μόνο εάν ο λογαριασμός του n ,σε ένα PoW σύστημα, ολοκληρώνει την απαιτούμενη εργασία που χρειάζεται. Επίσης όταν οι παίχτες επιλέγουν να παραλείψουν μερικά μηνύματα από τις αναφορές τους $\tilde{m}$ δεν θα αναφέρουν μηνύματα που έχουν δει και τα οποία δεν στάλθηκαν ποτέ.

Δεύτερον, οι παίχτες μπορεί να δημιουργήσουν νέα genesis blocks με τυχαίο αριθμό λογαριασμών και tokens που βρίσκονται σε αυτά. Όταν το κάνουν αυτό αυτομάτως παίρνουν υπό την κατοχή τους όλους τους λογαριασμούς στο νέο genesis block. Υπό αυτό το πρίσμα οι παίχτες μπορεί να πραγματοποιήσουν αποκλίσεις όπως παρουσιάστηκαν στην προηγούμενη ενότητα (8.3.3) με απώτερο στόχο να εξαπατήσουν τους νεοεισερχόμενους χρήστες.

Χρονική διάρκεια

Υπάρχουν δύο υποπερίοδοι η $\tau = 0, 1$ σε κάθε περίοδο t. Η διαδικασία του παιχνιδιού σε αυτές της υποπεριόδους έχει ως εξής:

1. Στην αρχή της $\tau = 0$ οι παρόντες παίχτες είναι ενημερωμένοι χάρις τους γείτονες τους στο G που έρχονται σε αυτή την περίοδο. Στο τέλος της $\tau = 0$ οι νέοι παίχτες έρχονται και επικοινωνούν με τους παρόντες παίχτες για να λάβουν πληροφορίες αναφορικά με την κατάσταση.
2. Στην $\tau = 1$ υπάρχουν τρία στάδια παιχνιδιού:
   Η πρώτη φάση: Στην οποία οι παίχτες έρχονται σε συμφωνία
   Η δεύτερη φάση: Στην οποία οι παίχτες στέλνουν μηνύματα με tokens
   Η Τρίτη φάση: Στην οποία οι παίχτες διεξάγουν ψηφοφορία και υπόκεινται σε υπολογιστικό κόστος εάν είναι απαραίτητο.

Όταν η Τρίτη φάση τελειώσει οι παίχτες αναβαθμίζουν την αρχική τους κατάσταση και διεξάγουν συμφωνίες. Επίσης η χρησιμότητα των σχέσεων που πραγματοποιείται στο G είναι αμοιβαία.

8.3.5 Ο μηχανισμός του Blockchain

Σε αυτή την ενότητα θα αναφερθούμε στον μηχανισμό του blockchain που επιβάλει την μεταφορά tokens μεταξύ των παιχτών, τις στρατηγικές ψηφοφορίας και τις ενέργειες που κάνουν οι παίχτες. Και επίσης θα χαρακτηρίσουμε μια συνάρτηση χρησιμότητας που πηγάζει από τις ενέργειες και τις αλλαγές καταστάσεων στον μηχανισμό.

Η ιδιωτική πληροφόρηση του παίχτη n στην κατάσταση ω περιλαμβάνει έναν τύπο θ_n που του αντιστοιχεί και τον συνολικό αριθμό των λογαριασμών που του ανήκουν A_n. Αυτοί οι τύποι ιδιωτικής πληροφορίας μπορούν να παρουσιαστούν συνοπτικά ως $\tilde{\theta}_n = (\theta_n, A_n)$. Ενός παίχτη η αρχική αλυσίδα $C_{n,t}$ είναι ένα επιπλέον κομμάτι ιδιωτικής πληροφορίας που καθορίζει ποιο επίπεδο ο παίχτης αυτός πιστεύει πως θα είναι το επίπεδο της συναίνεσης.

Άρα ο μηχανισμός του blockchain που λαμβάνουμε υπόψιν μας είναι ουσιαστικά ένα πρωτόκολλο επικοινωνίας. Λαμβάνει υπόψιν του ένα σύνολο αναφορών $(\tilde{\theta}_n, C_n)$ και

προτείνει μια στρατηγική να παιχτεί στην χρονική στιγμή $\tau = 1$. Σε αυτή την στιγμή οι παίχτες είναι ενημερωμένοι σε ποιες συμφωνίες πρέπει να εισέλθουν, ποια μηνύματα πρέπει να στείλουν για μια ενδεχόμενη συμφωνία και ποιες ψήφους πρέπει ενδεχομένως να αναμεταδώσουν για τα μηνύματα που παρατηρούν.

Η επικοινωνία είναι ανώνυμη οπότε αυτό οδηγεί τους παίχτες να υποβάλουν οποιαδήποτε πληροφορία επιθυμούν. Έτσι ένας παίχτης n που γνωρίζει πως το πραγματικό επίπεδο συναίνεσης είναι η αλυσίδα C^* αλλά έχει εξαπατήσει τον παίχτη n' κάνοντας τον να πιστεύει πως η πραγματική αλυσίδα συναίνεσης είναι η C' πιθανώς να επικοινωνήσει και να κάνει αναφορά μόνο σε εκείνους που γνωρίζουν πως το αληθινό επίπεδο συναίνεσης είναι το $(\tilde{\theta}_n, C^*)$. Ταυτόχρονα μπορεί ο παίχτης n να μεταδώσει ένα διαφορετικό σύνολο αναφορών στο C' με απώτερο σκοπό να κοροϊδέψει τον n' πριν ενεργήσει. Συνεπώς η επικοινωνία υφίσταται μόνο μεταξύ παιχτών που αναφέρονται στο ίδιο επίπεδο αρχικής αλυσίδας και οι συστάσεις για αυτήν γίνονται μόνο στους παίχτες που γνωρίζουν το αληθινό επίπεδο συναίνεσης και δεν εξαρτώνται από εκείνες που γίνονται στους παίχτες που έχουν ψευδώς πληροφορηθεί για το επίπεδο της συναίνεσης. Με άλλα λόγια οι παίχτες πολύ απλά αγνοούν εκείνους που διαφωνούν μαζί τους για την κατάσταση που υπάρχει στο blockchain.

Λέμε πως ο μηχανισμός εφαρμόζεται όταν τα κίνητρα συνάδουν για τους παίχτες να ακολουθήσουν τις συστάσεις και να μην κάνουν κάποια διαφορετική ενέργεια. Όταν ο μηχανισμός εφαρμόζεται προκύπτει η ακόλουθη σχέση:

$$T^*(\tilde{\theta}, \omega) = (c, y, \omega') \qquad (7)$$

Στην Σχέση 7 το $\tilde{\theta}$, το c και το y αναφέρονται και αντιπροσωπεύουν τον τύπο του ατόμου, την κατανάλωση του και την παραγωγή του. Ενώ το παιχνίδι έχει ως αρχική κατάσταση την ω με βάση τους προαναφερθέντες παράγοντες, στην συνέχεια ενώ πραγματοποιηθεί μεταβαίνει στην κατάσταση ω'. Υποθέτουμε πως η συνάρτηση αυτή είναι ανώνυμη το οποίο σημαίνει πως ο συνδυασμός των ταυτοτήτων των ατόμων που συμμετέχουν είναι σταθερά αμετάβλητος. Από την παραπάνω σχέση είναι εφικτό να οδηγηθούμε στην ακόλουθη δυναμική συνάρτηση χρησιμότητας (Σχέση 8) που συνδέεται με τα θεμελιώδη χαρακτηριστικά του παίχτη.

$$V_n(\tilde{\theta}_n, \omega) = E\left[u_n(\tilde{\theta}, \omega) - \kappa\, \upsilon\,(\tilde{\theta}, \omega) + \delta\, V_n\,(\tilde{\theta}'_n, \omega') | \theta_n, \omega\right] \qquad (8)$$

όπου $u_n(\tilde{\theta}, \omega) \equiv u(c_n(\tilde{\theta}, \omega), y_n(\tilde{\theta}, \omega), \theta_n)$ και είναι η συνεχώς μεταβαλλόμενη χρησιμότητα που προέκυψε από την παραγωγή και κατανάλωση του παίχτη n.

Επίσης υπάρχει και η ακόλουθη δυναμική συνάρτηση χρησιμότητας (Σχέση 9) που συνδέεται με τα κοινωνικά χαρακτηριστικά του παίχτη.

$$V_n^S(\tilde{\theta}_n) = \sum_{n'=1}^{N} V_{n,n'}^S(\tilde{\theta}_n) = \sum_{n'=1}^{N} E\left[\mathbf{1}\{n' \in P\} z_{n,n'} + \delta\, V_{n,n'}^S(\tilde{\theta'}_n) \,|\tilde{\theta}_n\right] \qquad (9)$$

Να επισημάνουμε πως από την στιγμή που η πιθανότητα του παίχτη να έχει παρουσία στην συγκεκριμένη περίοδο εξαρτάται μόνο από το εάν ο παίχτης αυτός είχε παρουσία και στην προηγούμενη περίοδο, τότε θα μπορούσαμε να γράψουμε πως $V_n^S(\tilde{\theta}_n) = V_{n,n'}^S(P_{n'})$, όπου το $P_{n'}$ είναι ένας δείκτης που παίρνει τιμή ένα όταν ο παίχτης n' έχει παρουσία και στην προηγούμενη περίοδο.

8.3.6 Το Blockchain trilemma

Το βασικό αποτέλεσμα από την ανάλυση που έχει πραγματοποιηθεί είναι το τρίλημμα του Blockchain. Το τρίλημμα του Blockchain αναφέρει πως δεν μπορεί να υπάρξει κανένα ψηφιακό σύστημα καταγραφής συναλλαγών που να ικανοποιεί ταυτόχρονα τις ακόλουθες τρεις ιδιότητες. Να έχει αυτοεπάρκεια, να μην χρειάζεται η πληρωμή κάποιου ποσού για την χρήση του δικτύου αυτού και να μην δαπανούνται πόροι. Στην ανάλυση μας το να έχει αυτοεπάρκεια το σύστημα σημαίνει πως μπορεί να λειτουργεί χωρίς τις αμοιβαίας ωφέλειας σχέσεις στο κοινωνικό δίκτυο G. Επίσης η πληρωμή κάποιου ποσού για την χρήση του δικτύου αυτού σημαίνει πως οι νέοι χρήστες εξάγουν το πλήρες πλεόνασμα που μπορούν να έχουν από την χρήση του δικτύου αυτού. Τέλος να μην δαπανούνται πόροι σημαίνει πως το PoW σύστημα συναίνεσης είναι περιττό.

Το πρώτο βασικό κομμάτι που διεξήχθη ως αποτέλεσμα είναι το Mimicking Lemma. Το Mimicking Lemma δείχνει πως ένας παίχτης ο οποίος είναι μόνος του μπορεί

να δημιουργήσει ένα blockchain που μιμείται το αποτέλεσμα που παράγεται σε μια αλυσίδα συναίνεσης σε κατάσταση ισορροπίας. Με αυτό το αποτέλεσμα στα χέρια μας θα δείξουμε μια γενική περιγραφή των αποτελεσμάτων του Τριλήμματος του Blockchain.

Mimicking Lemma. Ας υποθέσουμε πως το $C = \{b_0, \dots, b_k\}$ και είναι ένα blockchain που δημιουργήθηκε από N αριθμό παιχτών, ενώ το c^* είναι η σωρευτική υπολογιστική ενέργεια στο proof of work σύστημα συναίνεσης που πληρώθηκε από τους παίχτες αυτούς για να δημιουργήσουν το C. Είναι γεγονός πως ένας και μοναδικός παίχτης από μόνος του μπορεί να δημιουργήσει ένα blockchain πανομοιότυπο με το C με κόστος c^*.

Απόδειξη. Πρώτα ο παίχτης n δημιουργεί ένα genesis block b'_0 με λογαριασμούς και περιουσιακά στοιχεία πανομοιότυπα με αυτά που στο b_0 και με την κατάσταση να παραμένει ίδια, δηλαδή $\omega(b_0) = \omega(b'_0)$, φυσικά με την μόνη διαφορά πως πλέον ο παίχτης n είναι ο κάτοχος όλων των λογαριασμών που αντιστοιχούν στο b'_0.

Αφού δημιουργεί το νέο genesis block b'_0 ο παίχτης n πρέπει με επιτυχία να δημιουργήσει b'_k blocks με $1 \leq \kappa \leq K$ με τον παρακάτω ακόλουθο τρόπο:

1. Δημιουργώντας όλους τους λογαριασμούς που εμφανίζονται από την πρώτη στιγμή μέχρι το block b_k
2. Να στείλει μηνύματα $\widetilde{m_k}$πανομοιότυπα με εκείνα που είχαν σταλεί μέχρι το block b_k
3. Να μεταδώσει όλες τις ψήφους υ_k όπως αυτές μεταδόθηκαν μέχρι τα b_k blocks με τα μηνύματα $\widetilde{m_k}$ και τις ψήφους υ_k αλλά με το σημείο ένωσης (pointer) στο block να είναι το b'_{k-1}

Και τα τρία αυτά βήματα είναι εφαρμόσιμα για τον παίχτη n. Μέσω μιας επαγωγικής διαδικασίας η κατάσταση που υποδηλώνεται από το b'_{k-1} είναι πανομοιότυπη με εκείνη που υποδηλώνεται από το b_{k-1}, έτσι ο παίχτης n έχει τα tokens που χρειάζεται για να στείλει τα μηνύματα στο δεύτερο βήμα. Ύστερα στο τρίτο βήμα, ο παίχτης n και πάλι έχει τα tokens που απαιτούνται για να μεταδώσει τις απαραίτητες ψήφους στην περίπτωση που το επιθυμεί. Εάν το σύστημα συναίνεσης είναι proof of work, ο παίχτης n πληρώνει ένα κόστος $\kappa\, \upsilon\, (b'_k) = \kappa\, \upsilon\, (b_k)$ έτσι το σωρευτικό κόστος της μετάδοσης των ψήφων είναι ακριβώς το ίδιο με αυτό που πλήρωσαν οι πραγματικοί παίχτες N που δημιούργησαν το C.

Η ιδέα πίσω από την απόδειξη είναι απλή. Για την πιστή αναπαράσταση ενός blockchain που δημιουργείται από N παίχτες, ο παίχτης n θα πρέπει να βρει τον τρόπο να στείλει πανομοιότυπα μηνύματα και να αναμεταδώσει πανομοιότυπες ψήφους. Σε αυτό το μοντέλο οι παίχτες αποτρέπονται από το να στείλουν τυχαία μηνύματα και ψήφους γιατί δεν κατέχουν συγκεκριμένα tokens. Παρόλα αυτά εάν ο n δημιουργήσει ένα genesis block b'_0, και ένα σύνολο λογαριασμών πανομοιότυπο με εκείνους στο αρχικό genesis block b_0 τότε θα κατέχει όλα τα tokens στην εναλλακτική αυτή blockchain αλυσίδα και θα μπορεί να αντικαταστήσει τα μηνύματα και τις ψήφους που στάλθηκαν στο πρώτο block. Εάν οι ψήφοι χρειάζονται proof of work αλγόριθμο συναίνεσης τότε πολύ απλά ο παίχτης n μπορεί να παράξει τον ίδιο αριθμό ψήφων πληρώνοντας το ίδιο υπολογιστικό κόστος που οι πραγματικοί παίχτες N έχουν πληρώσει. Η κατάσταση $\omega(b'_1)$, είναι ίδια με την κατάσταση $\omega(b_1)$, και ο παίχτης n μπορεί να ακολουθήσει αυτή την διαδικασία σε κάθε ξεχωριστό block για να παράξει ένα πανομοιότυπο blockchain.

Ενώ το Mimicking Lemma επαφίεται στους παίχτες και στην ικανότητα τους να δημιουργήσουν ένα εντελώς ίδιο genesis block το οποίο θα είναι πιστευτό προς τους υπόλοιπους, στην πραγματικότητα αυτό μπορεί να μην είναι πάντα απαραίτητο για ένα άτομο που επιτίθεται να είναι σε θέση να το κάνει αυτό. Πολλές φορές αυτό που χρειάζεται ένας επιτιθέμενος είναι να κερδίσει την απαραίτητη δύναμη των ψήφων για να δημιουργήσει μια αλυσίδα από blocks πανομοιότυπη με εκείνη της αληθινής κατάστασης συναίνεσης. Αυτό μπορεί να είναι και μια ολόκληρη καινούργια αλυσίδα όπως στην απόδειξη που αναλύσαμε ή μπορεί να είναι μια διακλάδωση (fork) της ήδη υπάρχουσας αλυσίδας συναίνεσης.

Σε ένα PoW σύστημα ένας επιτιθέμενος πάντα έχει την ικανότητα να δημιουργήσει μια πανομοιότυπη αλυσίδα αρκεί να αποκτήσει την απαραίτητη υπολογιστική δύναμη που χρειάζεται το δίκτυο. Σε ένα PoS σύστημα, ένας επιτιθέμενος θα χρειαστεί να αποκτήσει τα tokens που αποτελούσαν την μεγαλύτερη πλειοψηφία των ψήφων σε μερικά προηγούμενα blocks. Εάν το τωρινό block συναίνεσης είναι το b_t είναι εύλογο πως ο λογαριασμός που έχει την μεγαλύτερη πλειοψηφία από tokens σε ένα block πολύ πιο πριν, για παράδειγμα στο b_{t-s} μπορεί να είναι εντελώς άδειος. Έτσι ένας επιτιθέμενος μπορεί να προσπαθήσει να αποκτήσει τα ιδιωτικά κλειδιά από τους ιδιοκτήτες αυτών των λογαριασμών και να κερδίσει την ικανότητα να δημιουργήσει μια διακλάδωση που μιμείται και αρχίζει από το b_{t-s} όπως στην περίπτωση του lemma. Σε ένα μονοπωλιακό ιδιωτικό

σύστημα blockchain, παρόλο που μια διακλάδωση μπορεί να είναι σαφής απόδειξη απόκλισης από τον μονοπωλιούχο, έτσι ένας επιτιθέμενος χρειάζεται πραγματικά να παρουσιάσει «θύματα» με ένα εντελώς διαφορετικό blockchain.

Το Blockchain Trilemma ακολουθεί ως μια συνέπεια του Mimicking Lemma. Πρώτα εξηγήσαμε τις σκέψεις που εγείρονται για το κόστος χρήσης του δικτύου, τις κοινωνικές σχέσεις αλλά και για το κόστος των πόρων που απαιτούνται και ύστερα παρείχαμε την ανακοίνωση των αποτελεσμάτων και της σύντομης περιγραφής της απόδειξης.

Τα έσοδα που εξάγονται από έναν συνασπισμό g από έναν παίχτη n' που δεν ανήκει στο g σε μια κατάσταση ω όταν οι παίχτες στο g έχουν χαρακτηριστικά $\tilde{\theta}_n$ προσδιορίζεται ως ακολούθως:

$$r^*(g, n', \omega, \tilde{\theta}) = \sum_{n \in g} \left(E\left[V_n(\tilde{\theta}_n, \omega) | n' \in P\right] - E\left[V_n(\tilde{\theta}_n, \omega) | n' \notin P\right] \right) \quad (10)$$

Όπου πιο απλά το $r^*(g, n', \omega, \tilde{\theta})$ (Σχέση 10) είναι το άθροισμα της αξίας που αναμένουμε να αποκτήσει ο συνασπισμός g όταν ο παίχτης n' είναι εντός αυτού μείον την αξία που αναμένουμε να αποκτήσει ο g όταν ο παίχτης n' απουσιάζει από αυτόν. Όταν το έσοδο που εξάγεται από τον συνασπισμό g είναι θετικό, τότε ο n' δεν αποτυπώνει το πλήρες πλεόνασμα που παράγεται από την παρουσία του.

Η κοινωνική εμπιστοσύνη του παίχτη n' σε έναν συνασπισμό g είναι η αξία από τις σχέσεις αμοιβαίας ωφέλειας για τον συνασπισμό g που δημιουργούνται από την παρουσία του n' και προσδιορίζεται ως ακολούθως:

$$s^*(g, n', \theta) = \sum_{n \in g} \left(E\left[V^S_{n,n'} | n' \in P\right] - E\left[V^S_{n,n'} | n' \notin P\right] \right) \quad (11)$$

Όπου η κοινωνική αξία $s^*(g, n', \theta)$ (Σχέση 11) είναι απλώς το άθροισμα της προεξοφλημένης αναμενόμενης αξίας των ροών ωφέλειας $z_{n,n'}$ που παράγονται από την παρουσία του παίχτη n'.

Ενώ η σπατάλη των πόρων c^* που αντιστοιχεί σε ένα blockchain C είναι απλώς ένα άθροισμα του κόστους της συναίνεσης Proof of Work που έχει δαπανηθεί στην αλυσίδα όπως φαίνεται στην Σχέση 12.

$$c^*(C) = \sum_{b \in C} \kappa\, \upsilon\,(b) \qquad (12)$$

Να αναφέρουμε πως τόσο τα κόστη χρήσης του δικτύου όσο και η κοινωνική εμπιστοσύνη καθορίζονται από το επίπεδο των σχέσεων ανάμεσα στους παίχτες σε έναν μηχανισμό, ενώ η σπατάλη πόρων καθορίζεται από το επίπεδο που βρίσκεται το καθολικό των συναλλαγών.

Πλέον σε αυτό το σημείο έχουμε όλες τις απαραίτητες παραμέτρους που χρειάζονται για να παρουσιάσουμε τα βασικά αποτελέσματα του blockchain Trilemma.

Blockchain Trilemma. Κανένας μηχανισμός διακράτησης αρχείων συναλλαγών δεν μπορεί να εφαρμοστεί χωρίς να έχει κόστος που συνδέεται με την χρήση του, χωρίς να χρειάζεται τις κοινωνικές σχέσεις και να μην χρειάζεται κάποια σπατάλη πόρων.

Απόδειξη. Ας σκεφτούμε ένα οποιοσδήποτε μηχανισμό καταγραφής αρχείων συναλλαγών και ας υποθέσουμε πως το C^* είναι ένα blockchain το οποίο μπορεί να φαίνεται δημοσίως όταν ένας παίχτης n' εισέρχεται σε αυτό. Θέλουμε να δείξουμε πως εάν το σύνολο των κοινωνικών επαφών του n' είναι ο συνασπισμός g τότε υπάρχει ένα $u^A > 0$ έτσι ώστε να ισχύει:

$$V^A \leq r^* + s^* + c^* \qquad (13)$$

Όπου σύμφωνα με την Σχέση 10, Σχέση 11 και Σχέση 12 το r^* , και το s^*εκφράζουν το κόστος χρήσης του δικτύου, και τα οφέλη των κοινωνικών σχέσεων που εξάγονται από τον συνασπισμό g από την ύπαρξη του n'. Ενώ το c^*είναι η σωρευτική υπολογιστική ενέργεια που απαιτείται σε έναν αλγόριθμο συναίνεσης Proof of Work για την δημιουργία ενός blockchain C^*

Με βάση το Mimicking Lemma όταν υπάρχει η πληροφόρηση πως την στιγμή (t, τ) ο παίχτης n' θα εισέλθει, ο συνασπισμός g έχει την δυνατότητα να πληρώσει ένα κόστος $c^*(C^*)$ για να δημιουργήσει ένα blockchain C^A πανομοιότυπο με το C^* στο οποίο ένας

παίχτης n_0 που ανήκει στο g έχει στην κατοχή του όλους τους λογαριασμούς και όλα τα tokens. Όταν ο παίχτης n' εισέρχεται βλέπει δύο πανομοιότυπα blockchains το C^* και το C^A, με αποτέλεσμα να χρειάζεται περισσότερη πληροφόρηση από τον συνασπισμό g για να του εξηγήσει ποιο θα είναι το αρχικό του επίπεδο. Τα άτομα όμως στο g μπορούν να έρθουν σε συνεννόηση μεταξύ τους και να πουν στον n' πως η αλυσίδα συναίνεσης είναι η C^A .

Καθώς ο παίχτης n' έχει πειστεί πως το επίπεδο συναίνεσης είναι η αλυσίδα C^A ο παίχτης n_0 μπορεί να παρομοιάσει την συμπεριφορά ισορροπίας των $\tilde{N}$ παιχτών στην κατάσταση ω για οποιονδήποτε τύπο $\tilde{\theta}^A = (\tilde{\theta}_1^A, \dots \tilde{\theta}_{\tilde{N}}^A)$ που μπορεί να έχουν. Στην $\tau = 1$, ο παίχτης n_0 απλά υποβάλλει αναφορές $(\tilde{\theta}_k^A, C^A)$ όταν ο παίχτης n' υποβάλλει $\left(\tilde{\theta}_{n'}, C^A\right)$. Πιο συγκεκριμένα ο παίχτης n_0 μπορεί να επιλέξει το $\tilde{\theta}^A$ για να μεγιστοποιήσει τα αγαθά που ο n' μπορεί να παράγει.

$$\tilde{\theta}^A = \arg\max_{\tilde{\theta}} E\left[y_{n'}\left(\left(\tilde{\theta}, \tilde{\theta}_{n'}\right), \omega\right)\right] \quad (14)$$

Ο παίχτης n_0 ενεργεί ακριβώς όπως οι παίχτες του τύπου $\tilde{\theta}_k^A$ που θα είχαν ενεργήσει στην $\tau = 1$, παράγοντας ένα σύνολο μηνυμάτων και ψήφων με αποτέλεσμα ο n' να του στείλει αγαθά ίσα με $c^A = y_{n'}\left(\left(\tilde{\theta}, \tilde{\theta}_{n'}\right), \omega\right)$.

Ο συνασπισμός g ενδέχεται να πράξει σε σχέση με άλλους παίχτες με τον ίδιο ακριβώς τρόπο που θα είχε πράξει εάν ο n' ήταν απόντας. Ο παίχτης n' φεύγει από τον μηχανισμό, ακολουθώντας το συντονισμένο ψέμα από τον συνασπισμό g άρα τόσο η αξία που παράγεται από τον μηχανισμό όσο και η αξία από το κοινωνικό δίκτυο που απολαμβάνεται από τον g είναι ίδια με εκείνη εάν ο παίχτης n' δεν είχε ποτέ εισέλθει σε αυτόν. Παρόλα αυτά αντί να παρατηρούμε την μεταβαλλόμενη μεταβλητή $u\left(c^*, y^*, \tilde{\theta}_{n_0}\right)$ που θα μπορούσε να έχει παρατηρηθεί εάν ο παίχτης n' δεν είχε εισέλθει, ο παίχτης n_0 έχει χρησιμότητα $u\left(c^* + c^A,\ y^*, \tilde{\theta}_{n_0}\right)$. Η αξία λοιπόν αυτής της επίθεσης από τον n_0 στον συνασπισμό g έχει ως ακολούθως.

$$V^A = u\left(c^* + c^A, y^*, \tilde{\theta}_{n_0}\right) - u\left(c^*, y^*, \tilde{\theta}_{n_0}\right) + \sum_{n \in g} E\left[V_n(\tilde{\theta}_{n,}\omega) + V_n^s\left(\tilde{\theta}_{n,}\right) | n' \notin P\right] - c^*$$

$$\equiv u^A + \textstyle\sum_{n \in g} E\left[V_n(\tilde{\theta}_{n,}\omega) + V_n^s\left(\tilde{\theta}_{n,}\right) | n' \notin P\right] - c^* \quad (15)$$

Όπου η μεταβλητή u^A αντιπροσωπεύει την αξία των αγαθών εκείνων που εκλάπηκαν από τον συνασπισμό g σε βάρος του παίχτη n'.

Αντιθέτως εάν ο συνασπισμός g δεν είχε αποκλίνει οι παίχτες θα είχαν λάβει την ακόλουθη αξία:

$$V^* = \sum_{n \in g} E\left[V_n(\tilde{\theta}_{n,}\omega) + V_n^s(\tilde{\theta}_{n,})|n \in P\right] \qquad (16)$$

Ο συνασπισμός g πληρώνει ουσιαστικά δύο κόστη που εξαπατάει τον n'. Το πρώτο αφορά πως πληρώνει ένα εκ των προτέρων κόστος για την υπολογιστική ενέργεια που απαιτείται για να μιμηθεί το πραγματικό blockchain το οποίο είναι ίσο με c^*. Το δεύτερο αφορά την αξία που θα χάσει η οποία θα προερχόταν από την παρουσία του παίχτη n' τόσο δια μέσου του μηχανισμού όσο και λόγω των σχέσεων αμοιβαίας ωφέλειας μεταξύ του παίχτη n' και του συνασπισμού g.

Η σχετική συνθήκη συμβατότητας κινήτρων όπου το $V^A \leq V^*$ ξεκάθαρα μειώνεται όπως επιθυμούνταν εξ αρχής καθώς η ωφέλεια είναι πάντα μικρότερη ή ίση από το άθροισμα που έχουν τα κόστη από την πλευρά του ατόμου που προβαίνει στην εξαπάτηση, και ισχύει πως:

$$u^A \leq r^* + s^* + c^* \qquad (17)$$

Το trilemma μπορεί να γίνει κατανοητό μέσα από ένα απλό παράδειγμα. Ένας νέος χρήστης n' έχει κοινωνικές σχέσεις με έναν συνασπισμό g και τα άτομα αυτά του συνασπισμού θέλουν να δημιουργήσουν ένα νέο Blockchain που μιμείται την συμπεριφορά της πραγματικής αλυσίδας συναίνεσης. Ο παίχτης n' αυτό που θα έχει να κάνει είναι να ρωτήσει τα άτομα στο g ποιο είναι το πραγματικό επίπεδο συναίνεσης. Οι παίχτες που βρίσκονται στο g μπορούν να του πουν ψέματα και να χρησιμοποιήσουν τον ανώνυμο λογαριασμό του στην αλυσίδα που δημιούργησαν για να πείσουν τον παίχτη n' να πραγματοποιήσει την μεταφορά μερικών αγαθών προς εκείνους.

Τα άτομα στον συνασπισμό g αντιμετωπίζουν εκ των προτέρων και εκ των υστέρων κόστη για αυτή την απόκλιση τους. Το εκ των προτέρων κόστος είναι πως πρέπει να ξοδέψουν χρήματα για να δημιουργήσουν το blockchain της απάτης που μιμείται το πραγματικό εάν χρησιμοποιούν PoW αλγόριθμο. Και τα εκ των υστέρων κόστη είναι πως πρώτον όταν ο παίχτης n' καταλάβει την απόκλιση του συνασπισμού g θα φύγει

από το δίκτυο και θα χάσει ο συνασπισμός τα χρήματα των ενοικίων που λαμβάνει για την χρήση του δικτύου αλλά και δεύτερον θα καταρρεύσουν οι κοινωνικές σχέσεις του συνασπισμού g καθώς θα μαθευτεί το γεγονός της απόκλισης τους. Άρα αυτά τα τρία κόστη πρέπει να αποτρέπουν τον συνασπισμό g από μια τέτοια συμπεριφορά εξαπάτησης και κλοπής του n'.

8.4 Παραδείγματα χειραγώγησης στους αλγόριθμους συναίνεσης του μοντέλου των Abadi J. Και Brunnermeier M.

8.4.1 Χειραγώγηση στο μοντέλο με αλγόριθμο συναίνεσης Proof of Stake (PoS)

Στον αλγόριθμο συναίνεσης PoS όπως αναφέρθηκε προηγουμένως, η ψήφος που έχει κάθε παίχτης στο σύστημα είναι συνδεδεμένη με τον αριθμό των tokens που περιλαμβάνονται σε έναν λογαριασμό. Για την επέκταση της αλυσίδας του blockchain χρειάζεται να γίνει η επιλογή της μεγαλύτερης αλυσίδας η οποία πρέπει να περιέχει τουλάχιστον τα 2/3 όλων των tokens που ψήφισαν το συγκεκριμένο block επέκτασης.

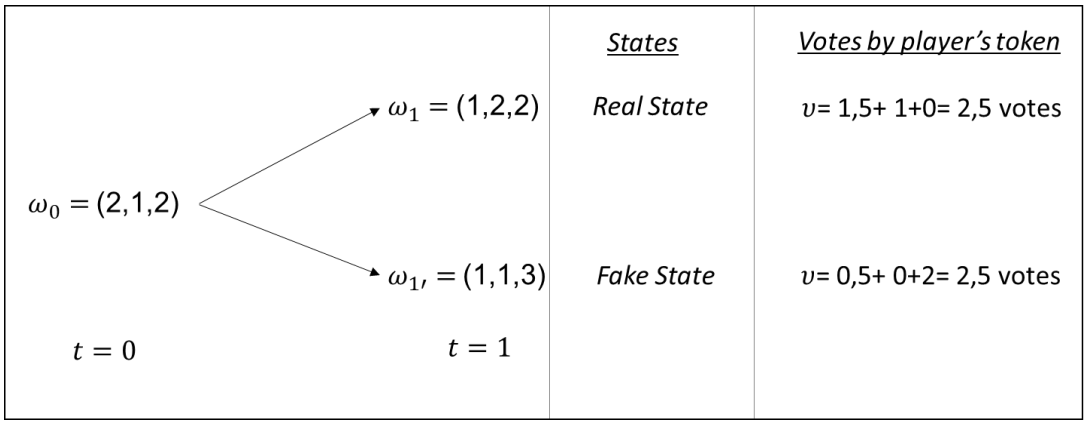
Ας υποθέσουμε πως βρισκόμαστε σε μια αρχική κατάσταση ω_0 και έχουμε σε αυτήν τρεις παίχτες. Τον Παίχτη 1, τον Παίχτη 2 και τον Παίχτη 3. Ο κάθε παίχτης στην κατάσταση αυτή έχει στον λογαριασμό του έναν συγκεκριμένο αριθμό tokens τα οποία είναι κατανεμημένα ως εξής. Ο Παίχτης 1 έχει δύο tokens, ο Παίχτης 2 έχει ένα token και ο παίχτης 3 έχει δύο tokens. Συνεπώς ισχύει πως η κατάσταση του παιχνιδιού είναι η $\omega_0 = (2,1,2)$.

Εάν για παράδειγμα ο Παίχτης 1 θέλει να μεταβιβάσει στον Παίχτη 2 ένα token την στιγμή $t = 1$ η αληθινή κατάσταση θα που πρέπει να επιβεβαιωθεί θα είναι η $\omega_1 = (1,2,2)$. Παρόλα αυτά την $t = 1$ μπορεί να υπάρξει και μια ψευδή κατάσταση στην οποία να μην συναινέσουν και τα τρία άτομα σε αυτή την μεταφορά του token. Δηλαδή η εναλλακτική αυτή κατάσταση που είναι και ψευδής υποθέτουμε πως αφορά την μεταφορά του ενός token από τον παίχτη 1 στον λογαριασμό του Παίχτη 3 και να διαμορφωθεί ως $\omega_{1'} = (1,1,3)$.

Σε αυτή την περίπτωση για την ψήφιση μεταξύ των δύο καταστάσεων η κατανομή των ψήφων θα έχει ως εξής. Ο Παίχτης 1 από τις 2 ψήφους που του αντιστοιχούν λόγω των δύο tokens που έχει στον λογαριασμό του την ω_0 βάζει 1,5 ψήφο στην κατάσταση ω_1 και 0,5 ψήφους στην κατάσταση ω_1,. Αντίστοιχα ο Παίχτης 2 βάζει και εκείνος την 1 ψήφο του καθώς έχει ένα token στην κατάσταση ω_1γιατί έχει συνολικά 2 tokens ενώ στην κατάσταση ω_1,δεν θα λάβει κανένα token από τον παίχτη 1 και θα μείνει με το 1 token που είχε εξαρχής. Τέλος ο Παίχτης 3 ψηφίζει με τα 2 tokens που έχει στην κατοχή του την κατάσταση ω_1, διότι είναι προς όφελός του καθώς έτσι θα λάβει εκείνος το ένα token που μεταφέρει ο Παίχτης 1 και θα βρεθεί στην $t = 1$ να έχει στον λογαριασμό του 3 tokens.

Συνεπώς η κατάσταση ω_1 και η κατάσταση $\omega_1{}'$ έχουν από 2,5 ψήφους αντίστοιχα. Ο λόγος που οι ψήφοι είναι ίδιοι και στις δύο καταστάσεις είναι γιατί εάν υποθέσουμε πως θέλει να εισέλθει ένας νέος παίχτης, ο Παίχτης 4 στην χρονική στιγμή $t = 1$ τότε θα παρατηρεί πως και οι δύο καταστάσεις έχουν 2,5 ψήφους και πρέπει να διαλέξει και να αποφασίσει μόνος του ποια είναι η αληθής. Άρα καταλήγουμε στο συμπέρασμα πως ο Παίχτης 4 για την επιλογή της κατάστασης πιθανώς να πρέπει να βασιστεί σε κάποιες κοινωνικές επαφές με το δίκτυο για να τον πληροφορήσουν για το πια κατάσταση είναι η αληθής και ποια είναι η ψευδής.

Διάγραμμα 8.4.1: Χειραγώγηση στο μοντέλο με αλγόριθμο συναίνεσης Proof of Stake (PoS) (Ιδία Επεξεργασία)



8.4.2 Χειραγώγηση στο μοντέλο με αλγόριθμο συναίνεσης Proof of Work (PoW)

Στον αλγόριθμο συναίνεσης PoW η ψήφος που έχει κάθε παίχτης και αντιστοιχεί στον λογαριασμό του στο σύστημα είναι συνδεδεμένη με την υπολογιστική ισχύ που δαπανάται από κάθε λογαριασμό. Δηλαδή όσο περισσότερη υπολογιστική ισχύ δαπανά ένας παίχτης τόσο μεγαλύτερο μερίδιο ψηφοφορίας θα κατέχει.

Ας υποθέσουμε πως βρισκόμαστε σε μια αρχική κατάσταση ω_0 και έχουμε σε αυτήν τρεις παίχτες. Τον Παίχτη 1, τον Παίχτη 2 και τον Παίχτη 3. Ο κάθε παίχτης στην κατάσταση αυτή έχει στον λογαριασμό του έναν συγκεκριμένο αριθμό tokens τα οποία είναι κατανεμημένα ως εξής. Ο Παίχτης 1 έχει 2 tokens, ο Παίχτης 2 έχει 1 token και ο Παίχτης 3 έχει 2 tokens. Συνεπώς ισχύει πως η κατάσταση του παιχνιδιού είναι η $\omega_0 = (2,1,2)$.

Εάν για παράδειγμα ο παίχτης 1 θέλει να μεταβιβάσει στον Παίχτη 2 ένα token την στιγμή $t = 1$ η αληθινή κατάσταση θα που πρέπει να επιβεβαιωθεί θα είναι η $\omega_1 = (1,2,2)$. Παρόλα αυτά την $t = 1$ μπορεί να υπάρξει και μια ψευδή κατάσταση στην οποία να μην συναινέσουν και τα τρία άτομα σε αυτή την μεταφορά του token. Δηλαδή η εναλλακτική αυτή κατάσταση που είναι και ψευδής υποθέτουμε πως αφορά την μεταφορά του ενός token από τον παίχτη 1 στον λογαριασμό του παίχτη 3 και να διαμορφωθεί ως $\omega_{1'} = (1,1,3)$.

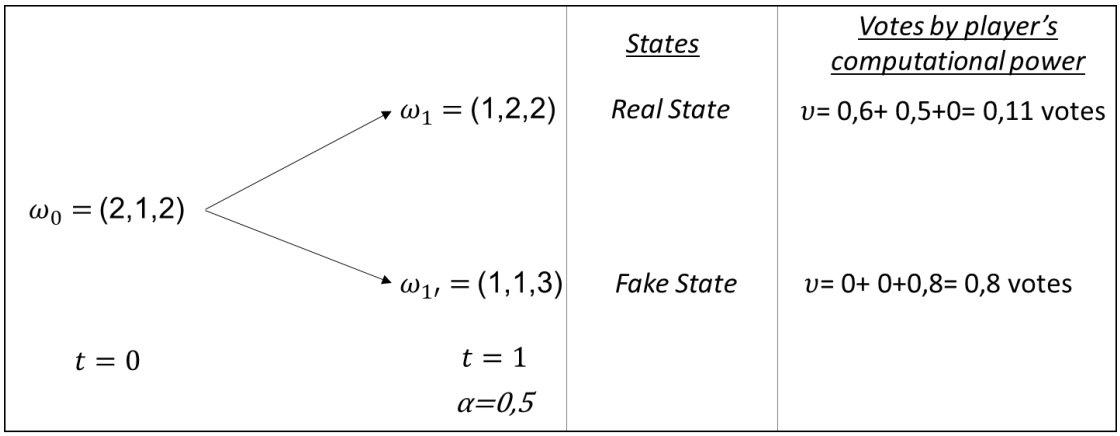
Περίπτωση 1

Στο σημείο αυτό ορίζουμε ένα σταθερό κόστος που το συμβολίζουμε με α και είναι θετικός αριθμός, το οποίο αντιστοιχεί στο ελάχιστο υπολογιστικό κόστος που απαιτείται να δαπανηθεί από τους παίχτες έτσι ώστε να επιβεβαιωθεί η επόμενη κατάσταση του Blockchain. Παράλληλα ορίζουμε και ένα διάνυσμα υ που αντιστοιχεί στον αριθμό των ψήφων με βάση τον PoW αλγόριθμο συναίνεσης. Για παράδειγμα υποθέτουμε πως το σταθερό κόστος είναι ίσο με $\alpha = 0{,}5$ και οι αντίστοιχοι ψήφοι των τριών παιχτών με βάση το υπολογιστικό κόστος που δαπανούν για την επιβεβαίωση της κατάστασης την χρονική στιγμή $t = 1$ είναι $\upsilon = (0{,}6\ ,\ 0{,}5\ ,\ 0{,}8)$ για κάθε παίχτη αντίστοιχα.

Σε αυτή την περίπτωση για την ψήφιση μεταξύ των δύο καταστάσεων η κατανομή των ψήφων θα έχει ως εξής. Ο Παίχτης 1 είναι αδιάφορος εάν θα μεταβεί στην κατάσταση ω_1 ή $\omega_1{}'$ καθώς και στις δύο έχει στην κατοχή του από 1 token. Ο Παίχτης 2 επιθυμεί να

μεταβεί στην κατάσταση ω_1 παρά στην ω_1,καθώς στην ω_1, έχει 2 tokens ενώ ο Παίχτης 3 επιθυμεί την κατάσταση ω_1, παρά στην ω_1 καθώς θα έχει στην κατοχή του 3 tokens. Άρα ο Παίχτης 1 και ο Παίχτης 2 ψηφίζουν την κατάσταση ω_1 που λαμβάνει συνολικά 0,6 και 0,5 ψήφους άρα συνολικά 0,11 ψήφους, ενώ ο Παίχτης 3 ψηφίζει την κατάσταση ω_1, που λαμβάνει 0,8 ψήφους. Άρα σε αυτή την περίπτωση δεν γίνεται χειραγώγηση του δικτύου και επικρατεί η αληθής κατάσταση.

Διάγραμμα 8.4.2: Πρώτη περίπτωση χειραγώγησης στο μοντέλο με αλγόριθμο συναίνεσης Proof of Work (PoW) (Ιδία Επεξεργασία)

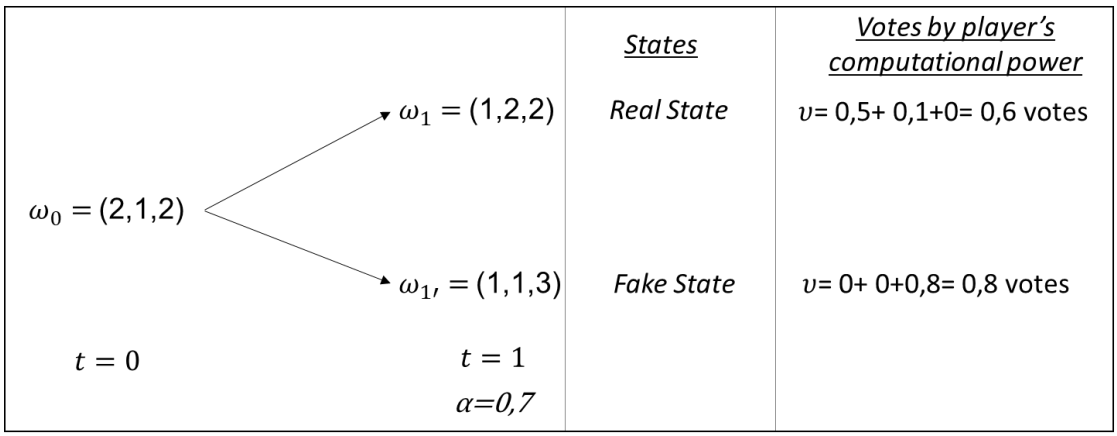


Περίπτωση 2

Ας υποθέσουμε πως το σταθερό κόστος α αντιστοιχεί στο ελάχιστο υπολογιστικό κόστος που απαιτείται να δαπανηθεί από τους παίχτες έτσι ώστε να επιβεβαιωθεί η επόμενη κατάσταση του Blockchain είναι $\alpha = 0{,}7$. Αυτό συνεπάγεται πως η ελάχιστη υπολογιστική ενέργεια που πρέπει να δαπανήσουν οι παίχτες για την επιλογή μιας κατάστασης πρέπει να είναι 0,7. Ενώ υποθέτουμε πως πλέον το διάνυσμα υ που αντιστοιχεί στον αριθμό των ψήφων με βάση τον PoW αλγόριθμο συναίνεσης είναι την χρονική στιγμή $t = 1$ είναι $\upsilon = (0{,}5\,,\, 0{,}1\,,\, 0{,}8)$. Ας υποθέσουμε όπως και προηγουμένως πως ο Παίχτης 1 είναι αδιάφορος εάν θα μεταβεί στην κατάσταση ω_1 ή ω_1, καθώς και στις δύο έχει στην κατοχή του από 1 token. Ο παίχτης 2 επιθυμεί να μεταβεί στην κατάσταση ω_1 παρά στην ω_1, καθώς στην ω_1, έχει δύο tokens ενώ ο Παίχτης 3 επιθυμεί την κατάσταση ω_1,παρά στην ω_1 καθώς θα έχει στην κατοχή του τρία tokens. Άρα ο Παίχτης

1 και ο Παίχτης 2 ψηφίζουν την κατάσταση ω_1 που λαμβάνει συνολικά 0,5 και 0,1 ψήφους άρα συνολικά 0,6 ψήφους, ενώ ο παίχτης 3 ψηφίζει την κατάσταση $\omega_{1'}$ που λαμβάνει 0,8 ψήφους. Οπότε παρατηρούμε πως παρόλο που ο Παίχτης 1 και ο Παίχτης 2 θέλουν την ω_1 κατάσταση επειδή το ελάχιστο κόστος υπολογιστικής ενέργειας που απαιτείται είναι ίσο με 0,7 θα επικρατήσει η επιθυμία του Παίχτη 3 που έχει κόστος 0,8 και επιθυμεί την κατάσταση ω_1, .Συνεπώς το Mimicking lemma που αναλύσαμε στην υποενότητα 8.3.6 έχει πρακτική εφαρμογή καθώς ο Παίχτης 3 έχει αρκετό υπολογιστικό κόστος από μόνος του και μπορεί να εξαπατήσει τους άλλους δύο παρόλο που η αληθινή κατάσταση συναίνεσης είναι η ω_1

Διάγραμμα 8.4.3: Δεύτερη περίπτωση χειραγώγησης στο μοντέλο με αλγόριθμο συναίνεσης Proof of Work (PoW) (Ιδία Επεξεργασία)



8.4.3 Χειραγώγηση στο μοντέλο με Ιδιωτικό Blockchain (Private Blockchain)

Στην περίπτωση ενός ιδιωτικού Blockchain υποθέτουμε πως ένα άτομο που είναι και ο μονοπωλιούχος του δικτύου αυτού κατέχει μια μοναδική μη μεταφερόμενη ψήφο υπό την μορφή token σε έναν λογαριασμό.

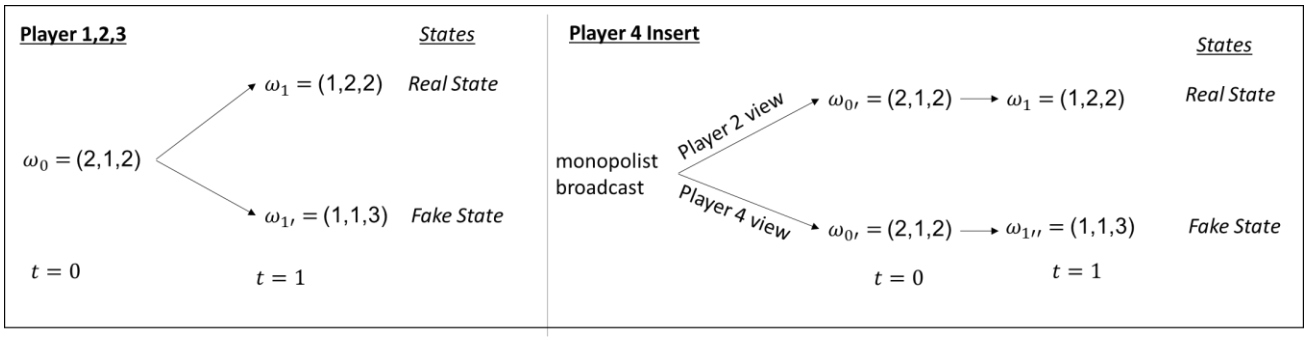
Υποθέτουμε πως βρισκόμαστε σε μια αρχική κατάσταση ω_0 και έχουμε σε αυτήν τρεις παίχτες. Τον Παίχτη 1, τον Παίχτη 2 και τον Παίχτη 3. Ο κάθε παίχτης στην κατάσταση αυτή έχει στον λογαριασμό του έναν συγκεκριμένο αριθμό tokens τα οποία είναι κατανεμημένα ως εξής. Ο Παίχτης 1 έχει 2 tokens, ο Παίχτης 2 έχει 1 token και ο Παίχτης 3 έχει 2 tokens. Συνεπώς ισχύει πως η κατάσταση του παιχνιδιού είναι η $\omega_0 = (2,1,2)$.

Εάν για παράδειγμα ο Παίχτης 1 θέλει να μεταβιβάσει στον Παίχτη 2 ένα token την στιγμή $t = 1$ η αληθινή κατάσταση θα που πρέπει να επιβεβαιωθεί θα είναι η $\omega_1 = (1,2,2)$. Παρόλα αυτά την $t = 1$ μπορεί να υπάρξει και μια ψευδή εναλλακτική κατάσταση που υποθέτουμε πως αφορά την μεταφορά του ενός token από τον παίχτη 1 στον λογαριασμό του παίχτη 3 και να διαμορφωθεί ως $\omega_1' = (1,1,3)$.

Σε αυτή την περίπτωση για την ψήφιση μεταξύ των δύο καταστάσεων η κατανομή της μίας και μοναδικής ψήφου $\upsilon(b) = 1$ μπορεί να γίνει μόνο από τον μονοπωλιούχο. Ο μονοπωλιούχος αποφασίζει πως θα βάλει την ψήφο του στην πραγματική κατάσταση δηλαδή την $\omega_1 = (1,2,2)$ για να μεταδίδεται στα άλλα 2 άτομα του δικτύου.

Ας υποθέσουμε πως παράλληλα ένας τέταρτος παίχτης θέλει να εισέλθει στο Blockchain την $t = 1$ και ο μονοπωλιούχος του μεταδίδει πως είναι η αρχική κατάσταση την χρονική στιγμή $t = 0$ ήταν η $\omega_{0,} = (2,1,2)$ αλλά πλέον το δίκτυο έχει μεταβεί στην $\omega_{1,,} = (1,1,3)$ για να νομίζει πως είναι το αληθινό επίπεδο. Συνεπώς επειδή δεν υπάρχει κανένας εκ των προτέρων τρόπος διάκρισης μεταξύ των καταστάσεων εάν ο Παίχτης 4 εμπιστευτεί τον Παίχτη 1 τότε θα έχει εξαπατηθεί. Αυτό συμβαίνει γιατί άλλη κατάσταση βλέπει ο παίχτης 2 δηλαδή την κατάσταση ω_1 και άλλη κατάσταση ο Παίχτης 4 δηλαδή την $\omega_{1,,}$.

Διάγραμμα 8.4.3: Χειραγώγηση στο μοντέλο με Ιδιωτικό Blockchain (Private Blockchain) (Ιδία Επεξεργασία)



Συμπεράσματα

Για να μπορέσει να επέλθει η ευημερία των αγορών, τα άτομα που συμμετέχουν σε αυτές πρέπει να είναι σε θέση να επικυρώσουν με πολύ χαμηλό κόστος αλλά και να ελέγχουν επιτυχώς τις συναλλαγές που πραγματοποιούν. Επίσης ο φθηνότερος διαμοιρασμός των αρχείων των συναλλαγών, τα μοιρασμένα καθολικά, οι νέοι τύποι συναλλαγών και οι νέες αγορές που είναι να αναδυθούν θα επικρατήσουν τα επόμενα χρόνια. Κομμάτι σε αυτές τις αλλαγές αποτελεί και η τεχνολογία Blockchain.

Ένα blockchain είναι ένα δημόσιο καθολικό βιβλίο συλλογής και καταγραφής πληροφοριών, συναλλαγών αλλά και όχι μόνο, που διατηρεί την ασφάλεια, την σταθερότητα, την επεκτασιμότητα, τον αυτοματισμό και τα χαμηλά κόστη. Βρίσκεται στο διαδίκτυο και είναι ένας συνδυασμός υπολογιστών συνδεδεμένων μεταξύ τους με ομότιμό peer-to-peer (P2P) τρόπο και αποτελείται από μια ομάδα συσκευών που συλλογικά αποθηκεύουν και μοιράζονται αρχεία. Ο τρόπος λειτουργίας του βασίζεται στην κρυπτογράφηση και αποτελεί την τεχνολογία πίσω από τα περισσότερα κρυπτονομίσματα. Η μελέτη γύρω από την κρυπτογραφική ασφάλεια της αλυσίδας των blocks χρονολογείται από το 1991 ενώ η πρώτη εκτεταμένη εφαρμογή μιας αλυσίδας blockchain που εμφανίστηκε ήταν το κρυπτονόμισμα Bitcoin.

Στην αρχιτεκτονική ενός blockchain πολύ σημαντικό ρόλο έχει το πρωτόκολλο του το οποίο αποτελεί του κύριους κανόνες ομαλής λειτουργίας του αλλά και ο αλγόριθμος συναίνεσης ο οποίος είναι ο τρόπος συμφωνίας για την επέκταση του κάθε νέου block στην blockchain αλυσίδα. Το πρωτόκολλο σχετίζεται με τους κύριους κανόνες ενός blockchain ενώ ο αλγόριθμος συναίνεσης με τον μηχανισμό μέσω του οποίου θα ακολουθούνται αυτοί οι κανόνες. Ένα βασικό πρόβλημα που μπορεί να εμφανιστεί σε ένα blockchain είναι το πρόβλημα των διπλών δαπανών (Double spending). Αυτό μπορεί να υπάρξει όταν δύο δημόσια μηνύματα δίνουν εντολή για την μεταφορά ενός token από έναν λογαριασμό σε δύο άλλους και δεν είναι πάντα ευδιάκριτο ποιο μήνυμα προηγείται από πιο. Οι πιο συνηθισμένοι τρόποι που μπορεί να πραγματοποιηθεί το Double spending είναι μέσω της μυστικής εξόρυξης αλλά και μετά την εμφάνιση μιας συναλλαγής.

Σήμερα υπάρχουν πολλά διαφορετικά είδη blockchains και μερικά λειτουργούν δημόσια και μερικά ιδιωτικά. Όταν αναφερόμαστε σε δημόσια και ιδιωτικά blockchain είναι σημαντικό να κατανοήσουμε ότι η βασική διαφορά μεταξύ τους είναι η διαχείριση της

ταυτότητας των ατόμων που συμμετέχουν. Αναλυτικότερα σε ένα ιδιωτικό blockchain γνωρίζουμε τις ταυτότητες των συμμετέχοντων από την αρχή ενώ σε ένα δημόσιο blockchain δεν γνωρίζουμε τις ταυτότητες τους και η συμμετοχή τους είναι ψευδώνυμη. Για παράδειγμα σε ένα κρυπτονόμισμα όπως το Bitcoin, το Litecoin, το Ethereum που δεν χρειάζεται να υπάρχει πρόσβαση ή άδεια για την συμμετοχή σε αυτό καθώς οποιοσδήποτε πρέπει να είναι σε θέση να μπορεί να τα κατέχει αλλά και να τα εμπορεύεται με κάποιον άλλον. Ενώ αντίθετα στην περίπτωση του εταιρικού κόσμου οι επιχειρήσεις επιθυμούν να γνωρίζουν ποιοι είναι όλοι οι συμμετέχοντες έχοντας πλήρη διαφάνεια διότι δεν θέλουν να μοιράζονται όλα τα επιχειρηματικά δεδομένα με όλα τα άτομα του επιχειρηματικού κόσμου ή με το ευρύ κοινό.

Το blockchain ιδιαίτερα τα τελευταία χρόνια έχει κεντρίσει το ενδιαφέρον και αποτελεί αντικείμενο επιστημονικής έρευνας με πολλά θέματα γύρω από αυτό. Ένα βασικό πεδίο είναι εάν τα κρυπτονομίσματα θα μπορούσαν να αποτελέσουν μέσο πληρωμών αντικαθιστώντας τα παραδοσιακά νομίσματα. Επειδή η επένδυση σε ένα κρυπτονόμισμα συνεπάγεται με την επένδυση στο blockchain που χρησιμοποιεί, αποκτώντας ουσιαστικά μέρος του, ειδικά στην περίπτωση του Bitcoin παραμένει αρκετά αναποτελεσματικό σύστημα για να διευκολύνει τον βέλτιστο τρόπο συναλλαγών. Η δομή του δεν είναι κατάλληλη να διαχειριστεί μεγάλες σε όγκο συναλλαγές που απαιτούνται από το μοντέρνο εμπορικό δίκτυο πληρωμών, όμως παρόλα αυτά εάν βελτιστοποιηθεί η χρησιμοποίηση των coins και μειωθούν τα κόστη συναλλαγών μπορεί να έχει προοπτική είτε αυτό είτε κάποιο άλλο. Να αναφερθεί πως κάποιες κεντρικές τράπεζες πρόσφατα άρχισαν να εξερευνούν την υιοθέτηση των κρυπτονομισμάτων και της τεχνολογίας blockchain για την χρήση τους στο εμπόριο και στις μεγάλες σε αξία πληρωμές.

Επίσης ιδιαίτερο ενδιαφέρον παρουσιάζουν οι έξυπνες συμβάσεις (Smart Contracts) καθώς αποτελούν μια ιδιαίτερα υποσχόμενη τεχνολογική καινοτομία πάνω στις blockchain πλατφόρμες. Τα Smart Contracts μπορούν να αποτελέσουν εξαιρετικό πεδίο για την πραγματοποίηση έμπιστων συναλλαγών μεταξύ δύο αντισυμβαλλόμενων ατόμων. Επειδή οι αποκεντροποιημένες καθολικές τεχνολογίες όπως το blockchain που χαρακτηρίζεται από αποκεντροποιημένη συναίνεση, χαμηλά κόστη και αναλλοίωτες αλγοριθμικές εκτελέσεις, διευκολύνουν την δημιουργία των Smart Contracts με αποτέλεσμα αυτή η θεμελιώδης τάση να μπορεί να αποτελέσει σημείο αναδιοργάνωσης στον βιομηχανικό κλάδο και στον ανταγωνισμό καθώς και να οδηγήσει σε μεγαλύτερη ευημερία και πλεόνασμα στον καταναλωτή μέσω της αύξησης της ανταγωνιστικότητας. Σε

γενικές γραμμές το Blockchain και τα Smart Contracts μπορούν να διατηρήσουν την ισορροπία στην αγορά και να οδηγήσουν σε μεγαλύτερο εύρος οικονομικού αποτελέσματος. Ο αντίκτυπος που έχει το blockchain και τα Smart Contracts στον χρηματοοικονομικό κόσμο και στην πραγματική οικονομία είναι ήδη εμφανής με πολλές επιχειρήσεις παγκοσμίως να χρησιμοποιούν την τεχνολογία του Blockchain. Ήδη διαταράσσει πολλές βιομηχανίες και σύντομα, θα αποτελέσει κομμάτι σε πολλούς τομείς. Προς το παρόν οι εταιρείες που χρησιμοποιούν την τεχνολογία blockchain εξασφαλίζουν στην πραγματικότητα τη θέση τους στο συνεχώς μεταβαλλόμενο παγκόσμιο περιβάλλον, ενώ αντίθετα εκείνες που δεν θα επενδύσουν στην τεχνολογία αυτή θα αντιμετωπίσουν προβλήματα από τον ανταγωνισμό.

Ακόμη σύμφωνα με την ανάλυση του του μοντέλου των Abadi J., Brunnermeier M., (2019), βασικό συμπέρασμα είναι πως το Mimicking Lemma και κατ' επέκταση το Blockchain trilemma απαντούν στην βασική ερώτηση που οδήγησε στην έμπνευση της εφεύρεσης των δημόσιων blockchain δηλαδή στο εάν η συναίνεση μπορεί να επιτευχθεί χωρίς να υπάρχει εμπιστοσύνη σε κάποια συγκεκριμένη αρχή. Αναλύοντας τρεις περιπτώσεις blockchain, του ιδιωτικού Blockchain, εκείνου που βασίζεται σε αλγόριθμο συναίνεσης PoW και εκείνο που βασίζεται σε αλγόριθμο συναίνεσης PoS, το blockchain trilemma απαντάει σε αυτή την ερώτηση και αναφέρει πως είναι εφικτό να αντικαταστήσεις αυτή την εμπιστοσύνη της κεντρικής αρχής είτε με την επιβολή κόστους που συνδέεται με τους πόρους του δικτύου είτε εάν βασίζεσαι σε κάποια εξωτερική του δικτύου πηγή εμπιστοσύνης μεταξύ των συμβαλλόμενων ατόμων.

Επίσης μέσω των παραδειγμάτων που εφαρμόσαμε για να εξετάσουμε την χειραγώγηση των τριών αυτών περιπτώσεων μπορούμε να πούμε πως εντοπίσαμε αδυναμίες του μοντέλου ιδιαίτερα στην περίπτωση της συναίνεσης PoW καθώς δεν σημαίνει πως το κόστος υπολογιστικής ενέργειας είναι ίδιο για κάθε επόμενο block συναλλαγών. Ένα παράδειγμα από τον πραγματικό κόσμο είναι η περίπτωση του Bitcoin που χρησιμοποιεί αλγόριθμο συναίνεσης PoW στο οποίο η δυσκολία εξόρυξης του κάθε επόμενου block είναι μεγαλύτερη απ ότι στο προηγούμενο.

Τέλος αξίζει να κλείσουμε με τις δηλώσεις της Christine Lagarde, η οποία ως επικεφαλής του ΔΝΤ είχε αναφέρει πως τα κρυπτονομίσματα μπορούν να γίνουν αποδεκτά και να αγκαλιαστούν σε γενικές γραμμές από όλο τον κόσμο. Αλλά για τώρα τα εικονικά νομίσματα όπως το Bitcoin, θέτουν λίγο ή και καθόλου ανταγωνισμό στο υπάρχον

σύστημα των fiat νομισμάτων και των κεντρικών τραπεζών. Φυσικά αξίζει να αναφερθεί πως πολλά από αυτά αποτελούν τεχνολογικές προκλήσεις με μεγάλη εξέλιξη που μπορούν να υιοθετηθούν με το πέρασμα του χρόνου. Ας μην ξεχνάμε πως όχι και πολύ παλιά πολλοί ειδικοί υποστήριζαν πως οι προσωπικοί υπολογιστές δεν θα έχουν καμία χρησιμότητα, αλλά και τα τάμπλετ δεν θα υιοθετηθούν και θα χρησιμοποιούνται ως ακριβοί δίσκοι μεταφοράς του καφέ. Οπότε πιστεύω πως δεν είναι σοφό να αποκλείουμε τα εικονικά νομίσματα.

Βιβλιογραφία

Επιστημονική

Abadi J., Brunnermeier M., (2019), Blockchain Economics, ηλεκτρονικός ιστότοπος: https://scholar.princeton.edu/markus/publications/blockchain-economics

Bartoletti M., Pompianu L., (2017), An empirical analysis of smart contracts: platforms, applications, and design patterns, ηλεκτρονικός ιστότοπος: https://www.researchgate.net/publication/315454656_An_Empirical_Analysis_of_Smart_Contracts_Platforms_Applications_and_Design_Patterns

Budish E. (2018), The Economics Limits of Bitcoin and the Blockchain, Ηλεκτρονικός ιστότοπος: https://faculty.chicagobooth.edu/eric.budish/research/Economic-Limits-Bitcoin-Blockchain.pdf

Catalini C., Gans J. (2016), Some Simple Economics of the Blockchain, ηλεκτρονικός ιστότοπος: https://pdfs.semanticscholar.org/4592/c1f009aba8b0c31e54255a1ac5aa392dd542.pdf

Chiu J., Koeppl T. (2018), The economics of Cryptocurrencies – Bitcoin and Beyond, ηλεκτρονικός ιστότοπος: https://www.bis.org/events/eopix_1810/chiu_paper.pdf

Diamond D., (1996), Financial Intermediation as Delegated Monitoring: A Simple Example, ηλεκτρονικός ιστότοπος: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2125936

Lin William Cong, Zhiguo He (2018), blockchain Disruption and Smart Contracts,ηλεκτρονικός ιστότοπος: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2985764

Nakamoto S., (2008), Bitcoin: A Peer-to-Peer Electronic Cash System, ηλεκτρονικός ιστότοπος: https://bitcoin.org/bitcoin.pdf

Philippon T., (2015), Has the US Finance Industry Become Less Efficient? On the Theory and Measurement of Financial Intermediation, ηλεκτρονικός ιστότοπος: https://www.aeaweb.org/articles?id=10.1257/aer.20120578

Vitalik Buterin, (2014), Ethereum White Paper, ηλεκτρονικός ιστότοπος: https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

Διαδικτυακή

agenda.ge, (2018), Georgia to use smart contracts in real estate registrations, ηλεκτρονικός ιστότοπος: https://agenda.ge/en/news/2018/396

Ameer Rosic, (2017), What Is Hyperledger? [The Most Comprehensive Step-by-Step Guide!], ηλεκτρονικός ιστότοπος: https://blockgeeks.com/guides/hyperledger/

Aziz, (2020), PUBLIC VS PRIVATE BLOCKCHAIN: WHAT'S THE DIFFERENCE?, ηλεκτρονικός ιστότοπος: https://masterthecrypto.com/public-vs-private-blockchain-whats-the-difference/

"Binance Academy (Aaron), (2020), Proof of Stake (PoS), ηλεκτρονικός ιστότοπος: https://www.binance.vision/glossary/proof-of-stake"

"Binance Academy, (2020), Block, ηλεκτρονικός ιστότοπος: https://www.binance.vision/glossary/block"

"Binance Academy, (2020), Node, ηλεκτρονικός ιστότοπος: https://www.binance.vision/glossary/node"

"Binance Academy, (2020), Peer-to-Peer Networks Explained, ηλεκτρονικός ιστότοπος: https://www.binance.vision/blockchain/peer-to-peer-networks-explained"

"Binance Academy, (2020), Proof of Work Explained, ηλεκτρονικός ιστότοπος: https://www.binance.vision/blockchain/proof-of-work-explained"

"Binance Academy, (2020), What are Nodes, ηλεκτρονικός ιστότοπος: https://www.binance.vision/blockchain/what-are-nodes"

"Binance Academy, (2020), What Is a Blockchain Consensus Algorithm?, ηλεκτρονικός ιστότοπος: https://www.binance.vision/blockchain/what-is-a-blockchain-consensus-algorithm"

bitcoinvisuals.com (2020), Block Reward Per Block, ηλεκτρονικός ιστότοπος: https://bitcoinvisuals.com/chain-block-reward

blog.rokkex.com,(2019), PoS, PoW, and 12 Other Blockchain Protocols You Didn't Know About, ηλεκτρονικός ιστότοπος: https://blog.rokkex.com/pos-pow-and-12-other-blockchain-protocols-you-didn-t-know-about-3634b089d119/

Bryant Nielson, (2020), Review of the 6 Major Blockchain Protocols, ηλεκτρονικός ιστότοπος: https://richtopia.com/emerging-technologies/review-6-major-blockchain-protocols

"Caner Taçoğlu, (2020), Block Reward, ηλεκτρονικός ιστότοπος: https://www.binance.vision/glossary/block-reward Share"

Christina Majaski, (2019), Distributed Ledgers, ηλεκτρονικός ιστότοπος: https://www.investopedia.com/terms/d/distributed-ledgers.asp

codefirst.co.uk, (2019),Public vs Private Blockchain, ηλεκτρονικός ιστότοπος: https://www.codefirst.co.uk/blog/public-vs-private-blockchain/

coinguides.org, (2018), What are Uncle Block, Orphaned Block and Stale Block in Blockchain, ηλεκτρονικός ιστότοπος::https://coinguides.org/uncle-orphan-stale-blocks/

Demiro Massessi, (2018), Public Vs Private Blockchain In A Nutshell, ηλεκτρονικός ιστότοπος: https://medium.com/coinmonks/public-vs-private-blockchain-in-a-nutshell-c9fe284fa39f

DimitarM. (2020), Crypto Coins vs Tokens: Difference Explained, ηλεκτρονικός ιστότοπος: https://www.publish0x.com/welcome-to-my-life/crypto-coins-vs-tokens-difference-explained-xgzeyl

docs.corda.net, (2020),Welcome to Corda, ηλεκτρονικός ιστότοπος: https://docs.corda.net/

docs.openchain.org,(2020), Overview of Openchain, ηλεκτρονικός ιστότοπος: https://docs.openchain.org/en/latest/general/overview.html

en.bitcoin.it, (2016), itGHash.IO, ηλεκτρονικός ιστότοπος: https://en.bitcoin.it/wiki/GHash.IO

errna.com, (2018), Private, Public, and Consortium Blockchains, ηλεκτρονικός ιστότοπος: https://errna.com/private-public-blockchain.htm

Genesis DevCon, (2018), What are Blockchain Protocols and How Do they Work?, ηλεκτρονικός ιστότοπος: https://medium.com/@genesishack/draft-what-are-blockchain-protocols-and-how-do-they-work-94815be5efa7

github.com, (2017), ERC: Ethereum Claims Registry #780, ηλεκτρονικός ιστότοπος: https://github.com/ethereum/EIPs/issues/780

goquorum.com, (2020), Evolve with Quorum.The proven blockchain solution for business., ηλεκτρονικός ιστότοπος: https://www.goquorum.com/

Harsh Agrawal, (2019), Coins vs Tokens: Know The Difference [Crypto Basics], ηλεκτρονικός ιστότοπος: https://coinsutra.com/coin-vs-token-difference-cryptocurrency/

Huabing Zhao, (2018), Hash Pointers and Data Structures, ηλεκτρονικός ιστότοπος: https://medium.com/@zhaohuabing/hash-pointers-and-data-structures-f85d5fe91659

hyperledger (2020), About Hyperledger, ηλεκτρονικός ιστότοπος: https://www.hyperledger.org/about

Ian Allison (2019), JPMorgan Adds Privacy Features to Ethereum-Based Quorum Blockchain, ηλεκτρονικός ιστότοπος: https://www.coindesk.com/jpmorgan-adds-new-privacy-features-to-its-ethereum-based-quorum-blockchain

JAKE FRANKENFIELD, (2019), Mining Pool, ηλεκτρονικός ιστότοπος: https://www.investopedia.com/terms/m/mining-pool.asp

JAKE FRANKENFIELD, (2019), Ripple (Cryptocurrency), ηλεκτρονικός ιστότοπος: https://www.investopedia.com/terms/r/ripple-cryptocurrency.asp

Jerome Morrow, (2014),What is a Coinbase Transaction?, ηλεκτρονικός ιστότοπος: https://blog.cex.io/bitcoin-dictionary/coinbase-transaction-12088

Jim Chappelow, (2019), Peer-to-Peer (P2P) Service, ηλεκτρονικός ιστότοπος: https://www.investopedia.com/terms/p/peertopeer-p2p-service.asp

"John Ma, (2020), Orphan Block, ηλεκτρονικός ιστότοπος: https://www.binance.vision/glossary/orphan-block"

Jura Protocol Media, (2019), Let's talk about nodes!, ηλεκτρονικός ιστότοπος: https://medium.com/@juraprotocol/lets-talk-about-nodes-5aa8e4d9f9c6

kontakt.io, (2020), What is a beacon?, ηλεκτρονικός ιστότοπος: https://kontakt.io/beacon-basics/what-is-a-beacon/

Lastovetska A., (2019), Blockchain Architecture Basics: Components, Structure, Benefits & Creation, ηλεκτρονικός ιστότοπος: https://mlsdev.com/blog/156-how-to-build-your-own-blockchain-architecture

Laura Shiff, (2018),Public vs Private Blockchains: What's the Difference?, ηλεκτρονικός ιστότοπος: https://www.bmc.com/blogs/public-vs-private-blockchain/

Liquid, (2018), What are protocols in crypto and blockchain?, ηλεκτρονικός ιστότοπος: https://blog.liquid.com/what-are-protocols-and-why-are-they-important

Liquid, (2019), How to invest in blockchain, ηλεκτρονικός ιστότοπος: https://blog.liquid.com/how-to-invest-in-blockchain

lisk.io, (2020), What is Blockchain?, ηλεκτρονικός ιστότοπος: https://lisk.io/what-is-blockchain

Maisie Borrows, Eleonora Harwich, Luke Heselwood, (2017), The future of public service identity: blockchain, ηλεκτρονικός ιστότοπος: https://www.accenture.com/t00010101T000000Z__w__/gb-en/_acnmedia/PDF-67/Accenture-Blockchain-Report.pdf

Marc Sel, (2020), Blockchain, a functional introduction, ηλεκτρονικός ιστότοπος: https://www.pwc.be/en/news-publications/insights/2017/blockchain-functional-introduction.html

MLSDev, (2019), Blockchain Architecture Basics: Components, Structure, Benefits & Creation, ηλεκτρονικός ιστότοπος: https://medium.com/@MLSDevCom/blockchain-architecture-basics-components-structure-benefits-creation-beace17c8e77

MLSDev, (2019), Blockchain Architecture Basics: Components, Structure, Benefits & Creation, ηλεκτρονικός ιστότοπος: https://medium.com/@MLSDevCom/blockchain-architecture-basics-components-structure-benefits-creation-beace17c8e77

Nitish Sinch, (2019), Top 5 Blockchain Protocols That You Should Know, ηλεκτρονικός ιστότοπος: https://101blockchains.com/blockchain-protocol/

Olga Kharif and Matthew Leising, (2018), Bitcoin and Blockchain, ηλεκτρονικός ιστότοπος: https://www.bloomberg.com/quicktake/bitcoins

Olga Kharif, (2019), Ethereum ‘Almost Full’ as Controversial Coin Gobbles Up Capacity, ηλεκτρονικός ιστότοπος: https://www.bloomberg.com/news/articles/2019-08-26/ethereum-almost-full-as-controversial-coin-gobbles-up-capacity

openchain.org, (2020),Blockchain technology for the enterprise, ηλεκτρονικός ιστότοπος: https://www.openchain.org/

Parikshit Hooda, (2020), Blockchain Forks, ηλεκτρονικός ιστότοπος: https://www.geeksforgeeks.org/blockchain-forks/

Parikshit Hooda, (2020), Important Blockchain terminologies, ηλεκτρονικός ιστότοπος: https://www.geeksforgeeks.org/important-blockchain-terminologies/

Parikshit Hooda, (2020), Proof of Stake (PoS) in Blockchain, ηλεκτρονικός ιστότοπος: https://www.geeksforgeeks.org/proof-of-stake-pos-in-blockchain/

Parikshit Hooda, (2020), Proof of Work (PoW) Consensus, ηλεκτρονικός ιστότοπος: https://www.geeksforgeeks.org/proof-of-work-pow-consensus/

Peter Sestoft, (2003), A distributed, value-oriented XML Store, ηλεκτρονικός ιστότοπος: https://www.researchgate.net/figure/Illustration-of-a-peer-to-peer-network_fig1_2605250

PwC.com, (2015), Peer Pressure How peer- to- peer platforms are transforming the consumer lending industry, ηλεκτρονικός ιστότοπος: https://www.pwc.com/us/en/consumer-finance/publications/assets/peer-to-peer-lending.pdf

PwC.com, (2016) Global FinTech Report, ηλεκτρονικός ιστότοπος: https://www.pwc.com/gx/en/industries/assets/pwc-blockchain-opportunity-for-energy-producers-and-consumers.pdf

PwC.com, (2017), Blockchain a catalyst for for new approaches in insurance, ηλεκτρονικός ιστότοπος: https://www.pwc.com/gx/en/insurance/assets/blockchain-a-catalyst.pdf

r3.com, (2020), Platform Corda Enterpris –a next gen blockchain platform, ηλεκτρονικός ιστότοπος: https:/ www.r3. om/cord -platform/

Roshan Raj, (2019), Hyperledger, ηλεκτρονικός ιστότοπος: https://intellipaat.com/blog/tutorial/blockchain-tutorial/hyperledger/

Shaan Ray, (2019), Understanding blockchain technology and its implications on the future of transactions, ηλεκτρονικός ιστότοπος: https://www.firstpost.com/tech/news-analysis/understanding-blockchain-technology-and-its-implications-on-the-future-of-transactions-7033731.html

Siegel D. (2016), Understanding The DAO Attack, ηλεκτρονικός ιστότοπος: https://www.coindesk.com/understanding-dao-hack-journalists

Simon Chandler, (2020),'Stale' Block Reminds the Importance of Bitcoin Confirmations, ηλεκτρονικός ιστότοπος: https://cryptonews.com/exclusives/stale-block-reminds-the-importance-of-bitcoin-confirmations-5737.htm

Stephen O'Neal, (2019), Differences Between Tokens, Coins and Virtual Currencies, Explained, ηλεκτρονικός ιστότοπος: https://cointelegraph.com/explained/differences-between-tokens-coins-and-virtual-currencies-explained

Tobias A. Huber, (2018), What Makes Crypto Protocols Valuable?, ηλεκτρονικός ιστότοπος: https://hackernoon.com/what-makes-crypto-protocols-valuable-957bdadd4ac0

World Energy Council, (2018), The Developing Role of Blockchain (White Paper version 10.0), ηλεκτρονικός ιστότοπος: https://www.pwc.se/sv/pdf-reports/energi/the-developing-role-of-blockchain.pdf

Yilun Cheng, SBI Holdings, GMO Internet set to mine Bitcoin at 300MW facility in Texas, ηλεκτρονικός ιστότοπος: https://www.theblockcrypto.com/post/52286/sbi-holdings-gmo-internet-set-to-mine-bitcoin-at-300mw-facility-in-texas