ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
& ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΕΦΑΡΜΟΓΕΣ ΣΥΛΛΟΓΗΣ ΚΑΙ ΑΝΙΧΝΕΥΣΗΣ ΠΛΗΡΟΦΟΡΙΩΝ ΜΕ ΤΗ ΧΡΗΣΗ ΕΞΥΠΝΩΝ ΣΥΣΚΕΥΩΝ ΤΩΝ ΧΡΗΣΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

ΠΑΠΑΝΙΚΟΛΑΟΥ ΑΘΑΝΑΣΙΟΥ

Επιβλέπων: Λούτα Μαλαματή

Καθηγήτρια Πανεπιστημίου Δυτικής Μακεδονίας

Κοζάνη, Μάϊος 2024

HELLENIC DEMOCRACY
UNIVERSITY OF WESTERN MACEDONIA
SCHOOL OF ENGINEERING
DEPARTMENT OF ELECTRICAL
& COMPUTER ENGINEERING
ece.uowm.gr

MOBILE CROWDSENSING SYSTEMS AND APPLICATIONS WITH THE UTILIZATION OF USERS' SMART DEVICES

THESIS

---

of

PAPANIKOLAOU ATHANASIOS

Supervisor: Louta Malamati

Professor at University of Western Macedonia

Kozani, May 2024

ΔΗΛΩΣΗ ΜΗ ΛΟΓΟΚΛΟΠΗΣ ΚΑΙ ΑΝΑΛΗΨΗΣ ΠΡΟΣΩΠΙΚΗΣ ΕΥΘΥΝΗΣ Δηλώνω ρητά ότι, σύμφωνα με το άρθρο 8 του Ν. 1599/1986 και τα άρθρα 2,4,6 παρ. 3 του Ν . 1256/1982, η παρούσα Διπλωματική Εργασία με τίτλο **"ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΕΦΑΡΜΟΓΕΣ ΣΥΛΛΟΓΗΣ ΚΑΙ ΑΝΙΧΝΕΥΣΗΣ ΠΛΗΡΟΦΟΡΙΩΝ ΜΕ ΤΗ ΧΡΗΣΗ ΕΞΥΠΝΩΝ ΚΙΝΗΤΩΝ ΣΥΣΚΕΥΩΝ ΤΩΝ ΧΡΗΣΤΩΝ"** καθώς και τα ηλεκτρονικά αρχεία και πηγαίοι κώδικες που αναπτύχθηκαν ή τροποποιήθηκαν στα πλαίσια αυτής της εργασίας και αναφέρονται ρητώς μέσα στο κείμενο που συνοδεύουν, και η οποία έχει εκπονηθεί στο Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Πανεπιστημίου Δυτικής Μακεδονίας, υπό την επίβλεψη του μέλους του Τμήματος κας Λούτας Μαλαματής. αποτελεί αποκλειστικά προϊόν προσωπικής εργασίας και δεν προσβάλλει κάθε μορφής πνευματικά δικαιώματα τρίτων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής, οι πηγές δε που χρησιμοποιήθηκαν περιορίζονται στις βιβλιογραφικές αναφορές και μόνον. Τα σημεία όπου έχω χρησιμοποιήσει ιδέες, κείμενο, αρχεία ή / και πηγές άλλων συγγραφέων, αναφέρονται ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή. Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας εργασίας, εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Ερωτήματα που αφορούν τη χρήση της εργασίας για κερδοσκοπικό σκοπό πρέπει να απευθύνονται προς τον συγγραφέα. Οι απόψεις και τα συμπεράσματα που περιέχονται σε αυτό το έγγραφο εκφράζουν τον συγγραφέα και μόνο.

Υπογραφή Φοιτητή:

Περίληψη

Η ταχεία πρόοδος της τεχνολογίας των κινητών συσκευών έχει ως αποτέλεσμα την ανάπτυξη πρωτοποριακών μεθόδων όσον αφορά τη συλλογή δεδομένων των χρηστών και την αντιμετώπιση προβλημάτων της καθημερινή τους ζωής. Μια από αυτές τις μεθόδους είναι το Mobile Crowdsensing, το οποίο αξιοποιεί την ύπαρξη των κινητών τηλεφώνων και άλλων συσκευών με σκοπό την συλλογή και τη μετάδοση δεδομένων. Οι τομείς εφαρμογής του Mobile Crowdsensing είναι μεταξύ άλλων η υγεία, οι υποδομές, το περιβάλλον κα.

Η τεχνολογία Blockchain αναδείχθηκε ως μια επαναστατική λύση για τη διασφάλιση της ακεραιότητας των δεδομένων και της ασφάλειας των χρηστών που τα συλλέγουν. Αποτελεί μια κατανεμημένη βάση δεδομένων, η οποία επιτρέπει τη καταγραφή συναλλαγών με ασφάλεια, διαφάνεια και αμεταβλητότητα. Με την αποκεντρωμένη φύση της και την κρυπτογράφηση, εξασφαλίζει ότι τα δεδομένα παραμένουν αναλλοίωτα και προστατευμένα από κακόβουλες επιθέσεις, ενώ τα χαρακτηριστικά της την καθιστούν ιδανική για εφαρμογές που απαιτούν εμπιστοσύνη και διαφάνεια.

Μία μέθοδος για την ανάπτυξη της εμπιστοσύνης αυτής μεταξύ των χρηστών σε πλατφόρμες συνεργατικής ανίχνευσης είναι τα Συστήματα Φήμης.. Οι χρήστες παρέχουν αξιολογήσεις, δημιουργώντας ένα δείκτη αξιοπιστίας και ποιότητας των δεδομένων που συλλέγονται από τους συμμετέχοντες.

Στη παρούσα διπλωματική παρουσιάζονται τα χαρακτηριστικά της εφαρμογής των συστημάτων φήμης τόσο στο Blockchain όσο και στο MCS. Επίσης, αναπτύσσεται ένα έξυπνο συμβόλαιο στη πλατφόρμα Ethereum για να αντιμετωπίσει τα προβλήματα αυτής της εφαρμογής. Σκοπός του συμβολαίου είναι η βαθμολόγηση των χρηστών, η ενημέρωση της διαδικτυακής φήμης και η αποθήκευση της στο Blockchain.

Λέξεις Κλειδιά

Mobile Crowdsensing, Συστήματα Φήμης, Τεχνολογία Blockchain, Πληροφορίες, Δεδομένα, Χρήστης, Έξυπνο Συμβόλαιο

Abstract

The rapid advance of mobile devices' technology has resulted in the development of innovative methods for data collection by the users and addressing daily problems. One of these methods is Mobile Crowdsensing, which leverages the presence of mobile phones and other devices to collect and transmit data. The application fields of Mobile Crowdsensing include health, infrastructure, environment, and more.

Blockchain technology has emerged as a revolutionary solution for ensuring data integrity and the security of the users who collect it. It is a distributed database that allows for the recording of transactions with security, transparency, and immutability. With its decentralized nature and encryption, it ensures that the data remains unaltered and protected from malicious attacks, meanwhile its characteristics make it ideal for applications requiring trust and transparency.

One method for developing this trust between the users in collaborative sensing platforms are Reputation Systems. These users provide ratings, creating an index of reliability and quality for the data collected by the participants.

This thesis presents the characteristics of reputation system implementation in both Blockchain and MCS. Additionally, a smart contract is developed on the Ethereum platform to address the issues of this implementation. The purpose of the contract is to rate users, update their online reputation, and store it on the Blockchain.

Keywords

Mobile Crowdsensing, Reputation Systems, Blockchain Technology, Informations, Data, User, Smart Contract

Ευχαριστίες

Πρώτον θα ήθελα να ευχαριστήσω την οικογένεια μου για τη συνεχή τους ανιδιοτελή στήριξη προς το πρόσωπο μου. Επίσης, θα ήθελα να ευχαριστήσω αρχικά την Επιβλέπουσα Καθηγήτρια κα Μαλαματή Λούτα και εν συνεχεία την κα Μπαντή Κωνσταντίνα, για την διαρκή επίβλεψη και την πολύτιμη βοήθεια που μου προσέφεραν καθ' όλη τη διάρκεια της εκπόνησης της παρούσας διπλωματικής εργασίας.

Κοζάνη,Μάϊος 2024

Περιεχόμενα

Συντομογραφίες

Internet of Things	IoT
Mobile Crowdsensing	MCS
Peer-to-Peer	P2P
Proof-of-Authority	PoA
Proof-of-Work	PoW
Proof-of-Stake	PoS
Distributed denial-of-service	DDoS

Κατάλογος Εικόνων

Κατάλογος Πινάκων

Κεφάλαιο 1:ΕΙΣΑΓΩΓΗ

Σε αυτή την ενότητα θα δούμε συνοπτικά το αντικείμενο της παρούσας Διπλωματικής Εργασίας, τις βασικές θεματικές που προκύπτουν και την οργάνωση τους στον τόμο.

1.1 Αντικείμενο της Διπλωματικής

Η ταχεία πρόοδος στις τεχνολογίες κινητής τηλεφωνίας και στο Διαδίκτυο έχει επιφέρει την ανάπτυξη πρωτοποριακών μεθόδων για τη συλλογή δεδομένων και την αντιμετώπιση προβλημάτων της καθημερινής ζωής. Μία από αυτές τις μεθόδους είναι το Mobile Crowdsensing ή MCS, μια τεχνική όπου τα έξυπνα κινητά τηλέφωνα και άλλες φορητές συσκευές χρησιμοποιούνται για τη συλλογή και τη μετάδοση δεδομένων από ένα ευρύ φάσμα χρηστών. Αυτή η συλλογή δεδομένων μπορεί να περιλαμβάνει πληροφορίες σχετικά με την ποιότητα του αέρα, την κυκλοφορία, την υγεία και πολλές άλλες εφαρμογές, προσφέροντας πολύτιμα δεδομένα για τη λήψη αποφάσεων και τη βελτίωση της ζωής των χρηστών.

Η τεχνολογία Blockchain αναδείχθηκε ως μια επαναστατική λύση για την ασφάλεια και την ακεραιότητα των δεδομένων που προκύπτουν από τη διαδικασία της συλλογής που αναφέρθηκε παραπάνω. Το Blockchain είναι μια κατανεμημένη βάση δεδομένων που επιτρέπει την καταγραφή συναλλαγών με τρόπο ασφαλή, διαφανή και αμετάβλητο. Μέσω της αποκέντρωσης και της κρυπτογράφησης, εξασφαλίζει ότι τα δεδομένα παραμένουν αναλλοίωτα και προστατευμένα από κακόβουλες επιθέσεις, γεγονός που την καθιστά ιδανική για εφαρμογές που απαιτούν υψηλή εμπιστοσύνη και διαφάνεια.

Όσον αφορά την εδραίωση εμπιστοσύνης μεταξύ των χρηστών, τα Συστήματα Φήμης διαδραματίζουν κρίσιμο ρόλο σε πλαίσια συμμετοχικής ανίχνευσης, όπως το mobile crowdsensing. Μέσα από αξιολογήσεις και βαθμολογίες που παρέχονται από τους ίδιους τους χρήστες, δημιουργείται μια εικόνα σχετικά με την αξιοπιστία και την ποιότητα των δεδομένων που συνεισφέρουν οι συμμετέχοντες. Τα συστήματα φήμης ενθαρρύνουν τους χρήστες να συνεισφέρουν και να διατηρούν υψηλά πρότυπα συμμετοχής, προάγοντας την αξιοπιστία και την ποιότητα των συλλεγόμενων δεδομένων.

Ο συνδυασμός του mobile crowdsensing με την τεχνολογία Blockchain και τα Συστήματα Φήμης δημιουργεί μια ισχυρή πλατφόρμα για τη συλλογή και τη διαχείριση δεδομένων. Το Blockchain μπορεί να εξασφαλίσει την ακεραιότητα και την ανιχνευσιμότητα των δεδομένων που συλλέγονται από τους χρήστες, ενώ τα συστήματα φήμης μπορούν να προσδιορίσουν και να επιβραβεύσουν την αξιοπιστία των συνεισφερόντων. Αυτή η συνδυαστική προσέγγιση μπορεί να προσφέρει λύσεις σε πολλές προκλήσεις, όπως η διασφάλιση της ποιότητας των δεδομένων, η ενθάρρυνση της συμμετοχής των χρηστών και η δημιουργία ενός ασφαλούς και διαφανούς πλαισίου για την ανάλυση και τη χρήση των δεδομένων.

1.2 Οργάνωση του τόμου

Αρχικά, στο Κεφάλαιο 2 γίνεται αναλυτική παρουσίαση του MCS, των χαρακτηριστικά του καθώς και των εφαρμογών που αναπτύσσονται με βάση αυτά τα χαρακτηριστικά. Στη συνέχεια, το Κεφάλαιο 3 αναλύει τη τεχνολογία Blockchain και τα συστήματα της, τις απειλές που ενδέχεται να αντιμετωπίζει, τα πλεονεκτήματα και τα μειονεκτήματα της εφαρμογής της. Έπειτα, στο Κεφάλαιο 4 γίνεται αναφορά στα Συστήματα Φήμης, στη δομή και στις οντότητες τους. Παρουσιάζονται επίσης διάφορα παραδείγματα τέτοιων συστημάτων, αλλά και τρόποι εφαρμογής τους σε συνδυασμό τόσο με το MCS, όσο και με το Blockchain. Τέλος, στο κεφάλαιο 5 παρουσιάζεται μια πρόταση-εφαρμογή των παραπάνω, με τη μορφή ενός έξυπνου συμβολαίου στη πλατφόρμα blockchain του Ethereum.

Κεφάλαιο 2: MOBILE CROWD SENSING (MCS)

Η ραγδαία εξέλιξη της τεχνολογίας στην εποχή μας προσφέρει ένα τεράστιο εύρος δυνατοτήτων στις σημερινές κινητές συσκευές που χρησιμοποιούμε στην καθημερινότητα μας. Οι συσκευές αυτές, όπως τα έξυπνα κινητά τηλέφωνα (smartphones) και οι ταμπλέτες (tablets), είναι εξοπλισμένα με μια πληθώρα ενσωματωμένων αισθητήρων όπως είναι οι κάμερες, τα μικρόφωνα, τα GPS, τα επιταχυνσιόμετρα, οι αισθητήρες φωτός, οι πυξίδες και τα γυροσκόπια[1]. Η ύπαρξη των αισθητήρων αυτών στα έξυπνα κινητά τηλέφωνα παρέχει την ευκαιρία για την ανάπτυξη καινοτόμων εφαρμογών ανίχνευσης πλήθους για τομείς όπως η περιβαλλοντολογική παρακολούθηση, η υγεία και οι μεταφορές[2].

2.1 Συστήματα ανίχνευσης και συλλογής πληροφοριών με τη χρήση έξυπνων συσκευών των χρηστών

Η ανίχνευση πλήθους με τη χρήση έξυπνων συσκευών υπάγεται στην γενική ιδέα του Διαδικτύου των Πραγμάτων (Internet of Things ή IoT). Αναφέρεται στην συλλογή και ανταλλαγή δεδομένων και πληροφοριών με σκοπό την μέτρηση ή την απόκτηση γνώσεων όσον αφορά ένα γεγονός κοινού ενδιαφέροντος, ενώ σε πολλές περιπτώσεις απαιτείται και η ανθρώπινη παρέμβαση με ενέργειες όπως ανίχνευση, μετάδοση, ανάλυση μεγάλου όγκου δεδομένων αλλά και λήψη απόφασης[2]. Ο κύριος σκοπός του MCS είναι η επίλυση προβλημάτων και η παροχή πιθανών λύσεων στους χρήστες με τη χρήση διάφορων εφαρμογών. Το κέντρο του συστήματος αυτού είναι οι χρήστες και οι συσκευές ανίχνευσης πληροφοριών που έχουν στην κατοχή τους. Στο Διαδίκτυο των Πραγμάτων οι συσκευές είναι κινητές και κοινωνικές, ενώ τα δεδομένα είναι χωρικά και χρονικά, τεράστια σε όγκο και μη δομικά. Ο στόχος της ανίχνευσης πλήθους είναι να παρέχει στους χρήστες αποτελεσματικές, διαφανείς και συνεχείς υπηρεσίες αλλά και μια δυναμική αλληλεπίδραση μεταξύ αιτούντων και παροχών μέσω του συνδυασμού των έξυπνων υπηρεσιών αυτών αλλά και μηχανισμών προγραμματισμού[3].

2.2 Mobile Crowd Sensing και Crowd Sourcing

Οι έννοιες της ανίχνευσης πλήθους και του πληθοπορισμού (CrowdSourcing) συνδέονται μεταξύ τους, αλλά διαφέρουν. Το MCS συνδυάζει και τις δυο αυτές έννοιες[5]. Η κύρια διαφορά τους ωστόσο έγκειται στο γεγονός ότι στην πρώτη περίπτωση αξιοποιείται η χρήση κινητών αισθητήρων αλλά και της ανθρώπινης

νοημοσύνης για τη συλλογή δεδομένων, ενώ στην δεύτερη περίπτωση αποκλειστικά η ανθρώπινη νοημοσύνη[4].

2.3 Η Αρχιτεκτονική του MCS

Η αρχιτεκτονική του MCS αποτελείται από τρεις κύριες οντότητες[7,10], τους αιτούντες (requestors), τους εργαζομένους ή συμμετέχοντες (workers ή participants) και την πλατφόρμα. Προσδιορίζονται ως εξής[11]:

Αιτούντες (requestors ή crowdsourcers)

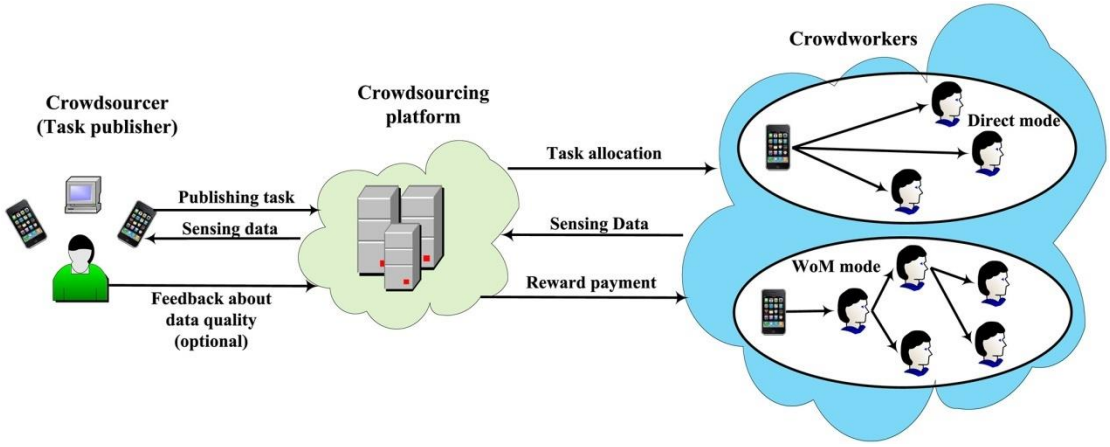
Η οντότητα αυτή αιτείται την δημιουργία μιας εργασίας στην πλατφόρμα. Αφού λάβουν τα δεδομένα/λύσεις από τους συμμετέχοντες, έχουν την δυνατότητα να βαθμολογήσουν την ποιότητα τους.

Εργαζόμενοι-Συμμετέχοντες (Workersή participants)

Οι εργαζόμενοι-συμμετέχοντες χρησιμοποιώντας τη κινητή συσκευή τους και τις δυνατότητες που αυτή τους προσφέρει, διαδραματίζουν βασικό ρόλο στην συλλογή των δεδομένων και των πληροφοριών συμμετέχοντας στην εργασία.

Πλατφόρμα (CrowdsensingPlatform)

Η Πλατφόρμα δημιουργεί ένα σύνδεσμο ανάμεσα στους αιτούντες και τους εργαζομένους. Στη συνέχεια θεσπίζονται κάποιοι κανόνες στην διαδικασία της ανίχνευσης πληροφοριών, όπως παροχή ανταμοιβής για τους συμμετέχοντες, ανάλογα με παράγοντες όπως η διάρκεια της εργασίας, τα αναμενόμενα αποτελέσματα, το ποσοστό διεκπεραίωσης κα.



Εικόνα 1 : ΑΠΕΙΚΟΝΙΣΗ ΣΕΝΑΡΙΟΥ ΕΦΑΡΜΟΓΗΣ MCS [11]

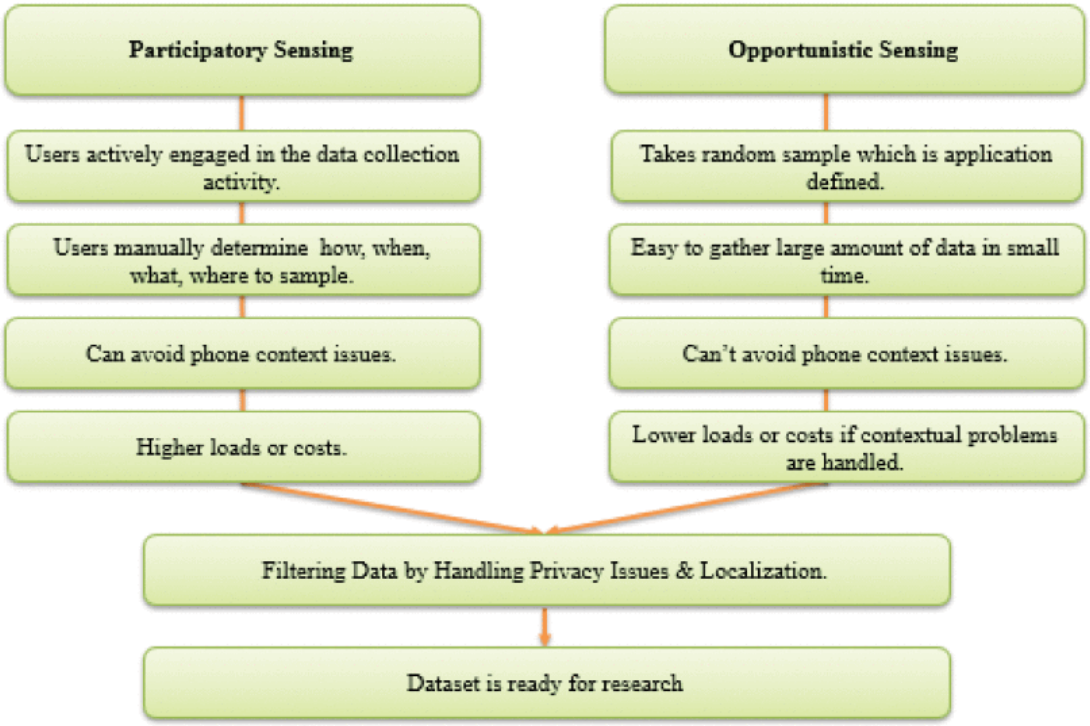
2.4 Τα Χαρακτηριστικά του Mobile Crowd Sensing και της λειτουργίας του

Η ανθρώπινη συμμετοχή αποτελεί ένα από τα πιο σημαντικά χαρακτηριστικά στο MCS, ενώ ποικίλει ανάλογα με τη φύση και τον τρόπο λειτουργίας της εκάστοτε εφαρμογής που χειρίζεται ο χρήστης. Όσον αφορά την φύση της ανθρώπινης κινητικότητας, αυτή προσφέρει πρωτοφανείς ευκαιρίες τόσο στο τομέα της ανίχνευσης και στο εύρος κάλυψης που αυτή θα έχει, όσο και στο τομέα της μετάδοσης δεδομένων[2]. Σύμφωνα με το [8], η ανίχνευση μπορεί να διακριθεί σε δύο κατηγορίες σε σχέση με τη συμμετοχή των χρηστών στην διαδικασία αυτή.

- **Συμμετοχική Ανίχνευση**: η κατηγορία αυτή απαιτεί την συνειδητή επιλογή από τους συμμετέχοντες έτσι ώστε να ικανοποιήσουν τα αιτήματα της εφαρμογής. Μέρος των αποφάσεων τους είναι πιθανό να είναι ο χρόνος, ο τόπος, το αντικείμενο αλλά και ο τρόπος που θα πραγματοποιηθεί η ανίχνευση. Αυτό σημαίνει ότι οι συμμετέχοντες έχουν την ευθύνη της εισαγωγής των δεδομένων.

- **Ευκαιριακή Ανίχνευση**: σε αντίθεση με τη Συμμετοχική Ανίχνευση, η εφαρμογή μπορεί να εκτελείται στο παρασκήνιο και η συλλογή των δεδομένων να εκτελείται ευκαιριακά χωρίς να υπάρχει ενεργή ανάμειξη του χρήστη στην όλη διαδικασία (π.χ. η συνεχής ανίχνευση σήματος Wi-Fi). Με αυτό τον τρόπο η εφαρμογή συλλέγει πληροφορίες χωρίς να ειδοποιεί τον χρήστη. Στην περίπτωση αυτή, απαιτείται μόνο η λήψη της εφαρμογής από το χρήστη και η παροχή άδειας στην κινητή συσκευή έτσι ώστε να συνεργαστεί και να συμμετέχει στη λειτουργία του MCS. Η ανίχνευση αυτού του είδους υποστηρίζει με μεγαλύτερη ευχέρεια την ανάπτυξη εφαρμογών μεγάλης κλίμακας αλλά και ποικιλίας [8].

Λόγω των παραπάνω χαρακτηριστικών και σύμφωνα με τον τρόπο της λειτουργίας τους, η Συμμετοχική Ανίχνευση μπορεί να χαρακτηριστεί ως ενεργή ανίχνευση και η Ευκαιριακή ως παθητική[9]. Σε ορισμένες περιπτώσεις, μπορεί να προκύψει μια υβριδική ανίχνευση, που αποτελεί ένα μείγμα των δύο ξεχωριστών κατηγοριών[7]. Μια τέτοια περίπτωση ενδεχομένως να είναι η περίπτωση φυσικής καταστροφής όπως ένας σεισμός που παρουσιάζεται στο [85]. Αρχικά, το υβριδικό σύστημα μπορεί να χρησιμοποιηθεί για εντοπισμό του γεγονότος και συλλογή αρχικών πληροφοριών (ευκαιριακή ανίχνευση). Στη συνέχεια όμως, μπορεί μέσω άμεσης επαφής με αυτόπτες μάρτυρες να θέσει στοχευόμενες ερωτήσεις (συμμετοχική ανίχνευση). Τα παραπάνω επιτυγχάνονται με τη χρήση εφαρμογών και φορμών ερωτήσεων και απαντήσεων, που είναι ενσωματωμένα στα μέσα κοινωνική δικτύωσης.



Εικόνα 2 : ΣΥΓΚΡΙΣΗ ΣΥΜΜΕΤΟΧΙΚΗΣ ΚΑΙ ΕΥΚΑΙΡΙΑΚΗΣ ΑΝΙΧΝΕΥΣΗΣ[1]

Όσον αφορά την μετάδοση των δεδομένων στα MCS, υπάρχουν δύο κατηγορίες[2]:

- **Μετάδοση με βάση την υποδομή**, στην οποία οι χρήστες αναφέρουν και αποκτούν πρόσβαση στα δεδομένα των αισθητήρων μέσω διαδικτύου με τη χρήση δικτύων κινητής τηλεφωνίας (π.χ. 3G,4G κινητά δίκτυα).

- **Ευκαιριακή Μετάδοση**, στην οποία τα δεδομένα προωθούνται μεταξύ χρηστών κινητών συσκευών μέσω διακοπτόμενων συνδέσεων ραδιοεπικοινωνιών μικρής εμβέλειας (π.χ. Wi-Fi)

Οι περισσότερες υπάρχουσες εφαρμογές MCS υιοθετούν το πρώτο παράδειγμα μετάδοσης, το οποίο όμως έχει κάποιους περιορισμούς, ειδικά σε περιπτώσεις που η κάλυψη δικτύου είναι ελλιπής.

2.5 Πλεονεκτήματα της χρήσης των MCS

Λόγω των ιδιαίτερων χαρακτηριστικών τους, τα MCS προσφέρουν κάποια συγκεκριμένα πλεονεκτήματα σε σύγκριση με τα παραδοσιακά ασύρματα δίκτυα αισθητήρων. Κάποια από αυτά είναι[7]:

2.5.1 Ανάπτυξη και Κάλυψη Δικτύου

Ένα σημαντικό πλεονέκτημα που χαρακτηρίζει το MCS είναι το χαμηλό κόστος σε αντίθεση με τα παραδοσιακά δίκτυα αισθητήρων. Η ύπαρξη δισεκατομμυρίων κινητών συσκευών ισοδυναμεί με εξοικονόμηση χρόνου και κόστους, αλλά και με μεγαλύτερο εύρος κάλυψης σε σχέση με τα σταθερά δίκτυα.

2.5.2 Συσκευές και πόροι

Τα κινητά τηλέφωνα είναι εφοδιασμένα με περισσότερα μέσα όπως υπολογιστική δύναμη και αποθηκευτική μνήμη, αλλά και με μια πληθώρα αισθητήρων (κάμερα, μικρόφωνο) άρα και περισσότερες δυνατότητες σε σύγκριση με τα παραδοσιακά δίκτυα.

2.5.3 Υβριδική Προσέγγιση στην διαδικασία της Ανίχνευσης

Τα MCS επωφελούνται από τη χρήση της ανθρώπινης νοημοσύνης, καθώς οι χρήστες επιλέγουν ποιες πληροφορίες θα συλλέξουν, άρα ελέγχουν την διαδικασία της ανίχνευσης. Αυτό έχει ως αποτέλεσμα να συλλέγονται δεδομένα υψηλής ποιότητας με τη συνεισφορά της ανθρώπινης νοημοσύνης και κινητικότητας.

2.5.4 Διακοπή Δικτύου

Οι περισσότερες εφαρμογές του MCS μπορούν να αντιμετωπίσουν μια πιθανή διακοπή δικτύου, καθώς τα δεδομένα αποθηκεύονται προσωρινά και παραδίδονται όταν η σύνδεση στο δίκτυο είναι και πάλι δυνατή.

2.5.5 Πλατφόρμες Ανίχνευσης

Η λειτουργία του MCS βασίζεται σε διάφορες πλατφόρμες ανίχνευσης (κλασσικά ασύρματα δίκτυα, έξυπνα κινητά τηλέφωνα, έξυπνα ρολόγια). Τα χαρακτηριστικά τους αξιοποιούνται σε μια πληθώρα εφαρμογών ανίχνευσης.

2.5.6 Ασύρματες Τεχνολογίες Δικτύου

Στην διαδικασία της ανίχνευσης πλήθους με τη χρήση κινητών συσκευών, οι συμμετέχοντες επικοινωνούν με τη χρήση διάφορων τεχνικών ασύρματων δικτύων, όπως τα δίκτυα Wi-Fi για τις μικρές αποστάσεις και τα δίκτυα 5G για τις μεγάλες αποστάσεις.

2.7 Προκλήσεις της χρήσης των MCS

Όπως αναφέρθηκε σε προηγούμενη ενότητα, οι εφαρμογές MCS προσφέρουν πολυάριθμες δυνατότητες και πλεονεκτήματα στους χρήστες τους. Παρόλα αυτά, έχουν να αντιμετωπίσουν και κάποιες σοβαρές προκλήσεις, οι οποίες μπορούν να επηρεάσουν την λειτουργία και την αποτελεσματικότητα τους και σχετίζονται με τις κινητές συσκευές που χρησιμοποιούνται κατά τη διαδικασία. Σε αυτή την ενότητα παρουσιάζονται οι βασικές προκλήσεις τις οποίες καλούνται να λύσουν τα συστήματα MCS.

2.7.1 Κίνητρα-Ανταμοιβές

Μια βασική πρόκληση των MCS είναι η ενθάρρυνση των χρηστών να συμμετάσχουν στο σύστημα αλλά και η εξασφάλιση ενός επαρκούς αριθμού συμμετεχόντων για την εφαρμογή. Αυτή η πρόκληση την αύξησης των συμμετεχόντων μπορεί να λυθεί με την προσφορά ανταμοιβής[22], η οποία λειτουργεί ως κίνητρο έτσι ώστε να ολοκληρώσουν την εργασία που τους έχει ανατεθεί. Στα [23][24] αναφέρεται ότι μόλις το 10% των συμμετεχόντων ολοκληρώνουν το 80% της εργασίας τους, ποσοστό το οποίο αυξάνεται δραματικά ανάλογα με την ύπαρξη αντίστοιχης ανταμοιβής. Γενικά, ο χρήστης επιδιώκει το καλύτερο δυνατό αποτέλεσμα με τη μικρότερη δυνατή προσπάθεια από μέρους του, αλλά και το μικρότερο δυνατό κόστος.

2.7.2 Ασφάλεια και Ιδιωτικότητα

Οι συσκευές ανίχνευσης συλλέγουν ευαίσθητα δεδομένα από τους χρήστες[25],[26]. Επομένως, η ασφάλεια και η ιδιωτικότητα είναι μια σημαντική πρόκληση των MCS, έτσι ώστε να εξασφαλιστεί η αυθεντικότητα και η ακεραιότητα των δεδομένων των συμμετεχόντων. Ένας μηχανισμός που λύνει αυτήν την πρόκληση είναι η εξασφάλιση ανωνυμίας των χρηστών με σκοπό την προστασία των δεδομένων και την απόκρυψη της προέλευσης τους[27]. Σε περιπτώσεις που συμμετέχοντες συμβάλλουν με ανακριβή δεδομένα (όπως ψεύτικες ενδείξεις GPS), επηρεάζεται η ακεραιότητα των δεδομένων που συλλέγονται από το σύστημα και έχει ως αποτέλεσμα την έλλειψη εμπιστοσύνης ως προς την εφαρμογή MCS. Η παρακολούθηση αυτής της συμπεριφοράς από το σύστημα μπορεί να επιφέρει περιορισμούς σε μελλοντικές υποβολές και ενδείξεις κακόβουλης συμπεριφοράς ως μέτρο προστασίας των υπόλοιπων χρηστών. Όσον αφορά τον τομέα της ασφάλειας, το MCS έχει να αντιμετωπίσει διαφόρων ειδών απειλές, όπως πιθανές παρεμβολές, υιούς και επιθέσεις Sybil και Dos που επηρεάζουν την διαδικασία της ανίχνευσης.

2.7.3 Εξασφάλιση Ποιότητας των Δεδομένων

Τα χαρακτηριστικά των εφαρμογών MCS μπορούν να επηρεάσουν σε μεγάλο βαθμό την ποιότητα των δεδομένων που συλλέγονται από άποψη ακρίβειας, πληρότητας, καθυστέρησης[7]. Για αυτό το λόγο, χρειάζεται η επιλογή και το φιλτράρισμα των δεδομένων έτσι ώστε να απορρίπτονται αυτά με χαμηλή ποιότητα. Οι συσκευές αυτές περιέχουν διαφόρων τύπων αισθητήρες αναλόγως με τον κατασκευαστή τους. Ένας αποδοτικός τρόπος για να επιτευχθεί αυτή η ανάγκη στα MCS, είναι ο εντοπισμός και η χρήση συσκευών που είναι πιθανότερο να παράγουν ακριβή δεδομένα ανίχνευσης[1]. Η εφαρμογή μηχανισμών ποιοτικού ελέγχου, όπως οι αλγόριθμοι πλειοψηφίας ή συναίνεσης μπορούν να χρησιμοποιηθούν για τον προσδιορισμό των πιο αξιόπιστων σημείων δεδομένων από πολλαπλές υποβολές. Η εκπαίδευση των χρηστών σχετικά με τη σημασία της παροχής δεδομένων υψηλής ποιότητας και τον τρόπο με τον οποίο η συνεισφορά τους επηρεάζει το συνολικό έργο μπορεί να βελτιώσει την αξιοπιστία των δεδομένων. Τα προγράμματα εκπαίδευσης ή τα μαθήματα εντός εφαρμογής μπορούν να βοηθήσουν τους χρήστες να κατανοήσουν τις σωστές μεθόδους συλλογής δεδομένων ανάλογα με την εφαρμογή που χρησιμοποιούν[86].

2.7.4 Περιορισμοί Πόρων

Οι περιορισμοί στους πόρους των συσκευών ανίχνευσης αποτελεί επίσης μια πρόκληση για το MCS [29]. Το φαινόμενο αυτό παρατηρείται ειδικότερα στα κινητά τηλέφωνα[30],[31] και τα χαρακτηριστικά της λειτουργίας τους, όπως η έλλειψη σήματος δικτύου σε απομακρυσμένες περιοχές ή το χαμηλό προσδόκιμο ζωής της μπαταρίας τους. Η κύρια πρόκληση του MCS είναι όπως προαναφέρθηκε η βελτίωση των δεδομένων που προκύπτουν από τους χρήστες κατά την ανίχνευση με την μικρότερη δυνατή κατανάλωση πόρων.

2.8 Η ανθρώπινη συμμετοχή στα MCS

Στα παραδοσιακά δίκτυα αισθητήρων, ο ρόλος του ανθρώπου περιορίζεται ως τελικός καταναλωτής των δεδομένων που συλλέγονται από αυτόνομα συστήματα. Αντίθετα, στα αντίστοιχα δίκτυα MCS, η ανθρώπινη συμμετοχή αποτελεί κύριο χαρακτηριστικό σε διαδικασίες όπως η ανίχνευση, η μετάδοση, η ανάλυση μεγάλου όγκου δεδομένων αλλά και η λήψη απόφασης. Αυτή η ιδιομορφία των MCS έχει τόσο θετικές όσο και αρνητικές επιδράσεις[2].

2.8.1 Πλεονεκτήματα της ανθρώπινης συμμετοχής

Όσον αφορά την θετική επίδραση της ανθρώπινης συμμετοχής, προσφέρει ευκαιρίες που σε διαφορετικό πλαίσιο δεν θα υπήρχαν. Κάποια από τα πλεονεκτήματα είναι:

- Η ανθρώπινη κινητικότητα προσφέρει μεγαλύτερο εύρος κάλυψης δικτύου και μετάδοσης των δεδομένων.

- Η διατήρηση του δικτύου επίσης γίνεται ευκολότερη λόγω των χαρακτηριστικών των κινητών κόμβων. Κάποια από αυτά τα χαρακτηριστικά είναι οι καλύτεροι υπολογισμοί και ικανότητα επικοινωνίας, μεγαλύτερος αποθηκευτικός χώρος. Επίσης, οι χρήστες διατηρούν τις συσκευές τους σε καλή κατάσταση.

- Με τη στρατολόγηση όλο και περισσότερων χρηστών στην κλίμακα του συστήματος, επιτυγχάνεται η επεκτασιμότητα και η ευελιξία του MCS.

2.8.2 Μειονεκτήματα της ανθρώπινης συμμετοχής

Η ανθρώπινη συμμετοχή στην διαδικασία της ανίχνευσης παρουσιάζει με τη σειρά της κάποιες προκλήσεις που πρέπει να αντιμετωπιστούν[2]:

- Λόγω της ανθρώπινης φύσης η διατήρηση της συμμετοχής μπορεί να επηρεάσει αρνητικά τη διαδικασία συλλογής, καθώς ο χρήστης ενδέχεται να χάσει το ενδιαφέρον του.
- Η διαφορά στις δυνατότητες και στις ποιότητες των συσκευών των χρηστών μπορεί να οδηγήσει σε ετερογενή και μη ομοιόμορφα δεδομένα, δυσκολεύοντας την ανάλυση και την αξιολόγησή τους.
- Στην ανίχνευση με MCS, οι χρήστες καταναλώνουν προσωπικούς τους πόρους (όπως η μπαταρία της συσκευής τους, επομένως η διαδικασία ενδέχεται να επηρεάζεται από τη διαχείριση τους.
- Η διαθεσιμότητα του χρήστη μπορεί να αλλάζει με τη πάροδο του χρόνου, επηρεάζοντας της ροή πληροφοριών που συλλέγονται.

2.6 Εφαρμογές MCS

Η ανάπτυξη της τεχνολογίας της κινητής ανίχνευσης, των έξυπνων κινητών τηλεφώνων και των αισθητήρων που αυτά περιέχουν προσφέρουν το πλαίσιο για την δημιουργία μια πληθώρας εφαρμογών με κύριο σκοπό τη βελτίωση της καθημερινότητας των χρηστών[7]. Παρακάτω παρουσιάζονται οι κύριοι τομείς που οι εφαρμογές αυτές απευθύνονται[6].

2.6.1 Περιβάλλον

Η ανθρώπινη παρέμβαση στο περιβάλλον είναι ιδιαίτερα ζημιογόνα σε φυσικούς πόρους όπως οι ωκεανοί και η ατμόσφαιρα. Γι αυτό το λόγο γεννήθηκε η ανάγκη για ανάπτυξη τεχνολογιών και εφαρμογών για την παρακολούθηση του περιβάλλοντος έτσι ώστε να περιοριστεί η μόλυνση του αλλά και για την προστασία των ζώων. Με τη χρήση του MCS παρέχεται η δυνατότητα για παρακολούθηση μεταξύ άλλων της ατμοσφαιρική ρύπανσης και πίεσης, της θερμοκρασίας, της ποιότητας των υδάτων, των επιπέδων θορύβου μιας πόλης[12], των καιρικών φαινομένων που επηρεάζουν την εκάστοτε περιοχή

2.6.2 Υγεία

Η χρήση των αισθητήρων που είναι ενσωματωμένοι στις έξυπνες συσκευές προσφέρουν πολλές δυνατότητες στον τομέα της υγείας και της βελτίωσης των ασθενών[13]. Οι αισθητήρες αυτοί χρησιμοποιούνται για την παρακολούθηση των καρδιακών παλμών, της πίεσης του αίματος και της θερμοκρασίας του σώματος[15]. Μπορούν επίσης να παρέχουν πληροφορίες για την κατάσταση ενός ασθενή σε περιπτώσεις διαβήτη και επιληπτικών κρίσεων[14].

2.6.3 Έξυπνη Πόλη-Smart City

Η ιδέα της Έξυπνης Πόλης αναπτύχθηκε με σκοπό να προσφέρει υπηρεσίες υψηλής ποιότητας στους πολίτες και παράλληλα να περιορίσει το λειτουργικό κόστος. Αυτό επιτυγχάνεται με τη χρήση τεχνολογιών πληροφοριών και επικοινωνίας στο ευρύ πλαίσιο του Διαδικτύου των Πραγμάτων (Internet of Things)[17,16]. Οι εφαρμογές του MCS προσφέρουν τη δυνατότητα για παρακολούθηση καίριων ζητημάτων όπως περιπτώσεις έκτακτης ανάγκης[18], κυκλοφοριακή συμφόρηση[19], περιβάλλον[20], πληθυσμιακή πυκνότητα[21]. Η ανάγκη για εφαρμογή του πλαισίου των Έξυπνων Πόλεων κρίνεται επιτακτική, αν αναλογιστεί κανείς ότι μέχρι το 2050 εκτιμάται ότι το 70% του παγκόσμιου πληθυσμού θα κατοικεί σε μεγάλα αστικά κέντρα[16].

2.6.4 Υποδομές

Οι εφαρμογές MCS παρέχουν την δυνατότητα στους χρήστες να λαμβάνουν πληροφορίες σε πραγματικό χρόνο για τα μέσα μαζικής μεταφοράς (δρομολόγια, ακριβή ώρα άφιξης και αναχώρησης συγκοινωνίας), για την κατάσταση των δρόμων και των γεφυρών που βρίσκονται στη διαδρομή τους. Ένας οδηγός συλλέγει πληροφορίες για την κατανάλωση καυσίμων, τις εκπομπές ρύπων ενώ επίσης λαμβάνει ειδοποιήσεις για τυχών ολισθηρούς δρόμους και λακκούβες που βρίσκονται στην κατεύθυνση του[1], πληροφορίες σχετικές και την εύρεση και την κράτηση θέσης στάθμευσης κα.

2.6.5 Κοινωνική Δικτύωση

Οι χρήστες των μέσων κοινωνικής δικτύωσης διαμοιράζονται πληροφορίες χρησιμοποιώντας συστήματα όπως Facebook, Twitter, LinkedIn. Η συνολική συμβολή τους στην επίλυση ενός προβλήματος υπερέχει σημαντικά σε σχέση με έναν μοναδικό χρήστη[1]. Όσον αφορά την συλλογή κοινωνικών πληροφοριών, οι πληροφοριών συλλέγονται μέσω εφαρμογών και στη συνέχεια αποστέλλονται σε απομακρυσμένο διακομιστή. Οι χρήστες αυτών των συστημάτων έχουν τη δυνατότητα δημοσίευσης πληροφοριών μεταξύ συγκεκριμένων ατόμων, τα οποία απαρτίζουν μια διαδικτυακή κοινότητα.

Στην Εικόνα 3 παρουσιάζονται συνοπτικά οι τομείς εφαρμογών του MCS:

Εικόνα 3 : ΣΥΝΟΨΗ ΤΩΝ ΤΟΜΕΩΝ ΕΦΑΡΜΟΓΩΝ MCS [1]

Κεφάλαιο 3: Η ΤΕΧΝΟΛΟΓΙΑ BLOCKCHAIN

Η ραγδαία ανάπτυξη διαφόρων τεχνολογιών όπως το IoT στη διάρκεια των πρόσφατων δεκαετιών είχε ως αποτέλεσμα εμφάνιση μιας ευκαιρίας για δημιουργία καινοτόμων ιδεών στον τεχνολογικό τομέα. Η ανάπτυξη αυτή είναι γνωστή και ως Τέταρτη Βιομηχανική Επανάσταση (INDUSTRY 4.0). Όσον αφορά τις εφαρμογές του IoT, βασικός στόχος αποτελούσε η βελτιστοποίηση των πόρων και της παραγωγικής διαδικασίας μέσω της διασύνδεσης του εξοπλισμού, ενός εύρους πολυδιάστατων δεδομένων καθώς και του αυτόματου ελέγχου και της επίγνωσης του περιβάλλοντος[69]. Αυτό έγινε δυνατό με την χρησιμοποίηση της τεχνολογίας Blockchain και των χαρακτηριστικών της. Αποτελεί μια κατανεμημένη τεχνολογία καθολικού που με τις δυνατότητες που προσφέρει όπως ανωνυμία, αποκέντρωση, διαφάνεια, μεταξύ άλλων, διαδραμάτισε σημαντικό ρόλο στην ανάπτυξη του IoT.

3.1 Αρχιτεκτονική και Στοιχεία του Blockchain

Το blockchain αποτελεί μια οργανωμένη λίστα ή ακολουθία από blocks τα οποία μπορεί να περιέχουν αρχεία συναλλαγών, αλλά και άλλους τύπους δεδομένων όπως συνάλλαγμα, προγράμματα λογισμικού ή δεδομένα πολυμέσων[37].

Blocks: είναι ουσιαστικά δομές δεδομένων σε μορφή συνεχούς αναπτυσσόμενης λίστας στο blockchain. Τα blocks συνδέονται μεταξύ τους μέσω χρήσης κρυπτογράφησης. Το κάθε block περιέχει μια κρυπτογραφημένη τιμή hash 16 ψηφίων του προηγούμενου block ή parent block (η οποία προκύπτει με τη λειτουργία της συνάρτησης SHA256), ένα timestamp που προσδιορίζει τη δημιουργία του και τα δεδομένα συναλλαγής. Ο λόγος που το κάθε block περιέχει τη τιμή hash του προηγούμενου είναι η αποτροπή της τροποποίησης των συναλλαγών που περιέχονται σε αυτό. Ο ρόλος τους είναι η καταγραφή και η επιβεβαίωση του χρόνου και της ακολουθίας των συναλλαγών στο blockchain. Αυτή του η δομή και η σύνδεση του ενός block με το προηγούμενο του δημιουργεί μια αλυσίδα, η οποία οδηγεί στο αρχικό block (genesis block). Εκτός από την κεφαλίδα, κάθε block περιέχει δεδομένα πληροφοριών και μια λίστα συναλλαγών. Το μέγεθος της κεφαλίδας (header) είναι σταθερό στα 80 bytes, ενώ το μέγεθος των συναλλαγών είναι μεταβαλλόμενο και σχετίζεται με το τύπο της εφαρμογής.

Miner: είναι η κάθε πιθανή οντότητα στο δίκτυο που έχει τη δυνατότητα μέσω της υπολογιστικής του δύναμης να λάβει μέρος σε συναλλαγές κρυπτονομίσματος ή ακόμα και στην εξόρυξη του. Με αυτό τον τρόπο έχει πολύ σημαντικό ρόλο στη δημιουργία νέων κρυπτονομισμάτων και στην επιβεβαίωση συναλλαγών στο blockchain, μέσω των οποίων θα λάβει μια ανταμοιβή. Κάθε ηλεκτρονικός υπολογιστής αποτελεί έναν κόμβο στο δίκτυο και μπορεί να έχει το ρόλο του απλού χρήστη ή του miner. Όταν μια συναλλαγή συμφωνηθεί ανάμεσα σε δύο χρήστες του συστήματος, θα πρέπει να εγκριθεί πριν προστεθεί σε ένα block. Τότε, λεπτομέρειες

της συναλλαγής όπως η τιμή και η ιδιοκτησία καταγράφονται, επιβεβαιώνονται και εγκαθίστανται σε όλους του κόμβους του blockchain.

Ο κάθε λογαριασμός στο δίκτυο Blockchain κατέχει ένα ζευγάρι από ιδιωτικό κλειδί και δημόσιο κλειδί. Το ιδιωτικό κλειδί ελέγχει τον λογαριασμό, πρέπει να είναι κρυφό και χρησιμοποιείται για να επιβεβαιωθούν οι συναλλαγές, ενώ το δημόσιο μπορεί να διαμοιραστεί με ασφάλεια. Τα δύο κλειδιά αποτελούν την **Ψηφιακή Υπογραφή** του χρήστη. Εφόσον το σύστημα επιβεβαιώσει την γνησιότητα της υπογραφής, στη συνέχεια οι κόμβοι απλά ελέγχουν την αντιστοίχιση του υπογράφων με το δημόσιο κλειδί του. Ο μόνος τρόπος να γίνει δεκτή μια πιθανή τροποποίηση σε μια συναλλαγή είναι να εγκριθεί από όλους τους συμβάλλοντες κόμβους.

Το δέντρο **Merkle** χρησιμοποιείται για επαλήθευση δεδομένων. Αποθηκεύει συναλλαγές δημιουργώντας ένα ψηφιακό αποτύπωμα τους και δίνει τη δυνατότητα στο χρήστη να ελέγξει εάν μπορούν να συμπεριληφθούν στο block. Το βασικότερο στοιχείο στη δημιουργία του δέντρου Merkle είναι η λειτουργία hash[87]. Μέσω, αυτής, πολυάριθμα αρχεία συναλλαγών παίρνουν συμπαγή μορφή, την τιμή hash.

Μέγεθος	**Πεδίο**	**Περιγραφή**
4 bytes	Έκδοση	Ο αριθμός έκδοσης λογισμικού και πρωτοκόλλων
32 bytes	Hash Προηγούμενου μπλοκ	Μία αναφορά στο hashtου προηγούμενου μπλοκ
32 bytes	Ρίζα Merkle	Το hash της ρίζας του δέντρου merkle των συναλλαγών αυτού του μπλοκ
4 bytes	Timestamp	Ο κατά προσέγγιση χρόνος δημιουργίας του μπλοκ
4 bytes	Δυσκολία στόχου	Η δυσκολία στόχου του αλγόριθμου proof-of-work για αυτό το μπλοκ
4 bytes	Nonce	Ένας μετρητής που χρησιμοποιείται από τον αλγόριθμο proof-of-work

Πίνακας 1 : Η ΔΟΜΗ ΤΗΣ ΚΕΦΑΛΙΔΑΣ ΕΝΟΣ BLOCK [37]

Η τεχνολογία Blockchain μπορεί να εφαρμοστεί με πολλούς διαφορετικούς τρόπους, δομείται κατά κύριο λόγο όμως από τρία βασικά μέρη τα οποία με τη συνύπαρξη τους εξασφαλίζουν στο σύστημα την απαραίτητη σταθερότητα και εμπιστοσύνη που αποτελούν εξάλλου και τους στόχους της λειτουργίας του.

3.1.1 Καθολικό

Το πρώτο μέρος είναι το καθολικό (ledger), στο οποίο αποθηκεύονται οι συναλλαγές με σειρά προτεραιότητας σε μια ακολουθία από blocks ανάλογα με το χρόνο που πραγματοποιούνται. Το Blockchain λειτουργεί στο πλαίσιο της Τεχνολογίας Κατανεμημένου Καθολικού (Distributed Ledger Technology). Το κατανεμημένο καθολικό αποτελεί μια μορφή ψηφιακής βάσης δεδομένων καταγραφής συναλλαγών η οποία ενημερώνεται και διατηρείται από κάθε μέλος ανεξάρτητα σε ένα δίκτυο[51]. Σε αυτού του είδους το καθολικό δεν υπάρχει κεντρική εξουσία διαχείρισης. Αντίθετα όλοι οι κόμβοι έχουν πρόσβαση σε αυτό και στη λίστα συναλλαγών.

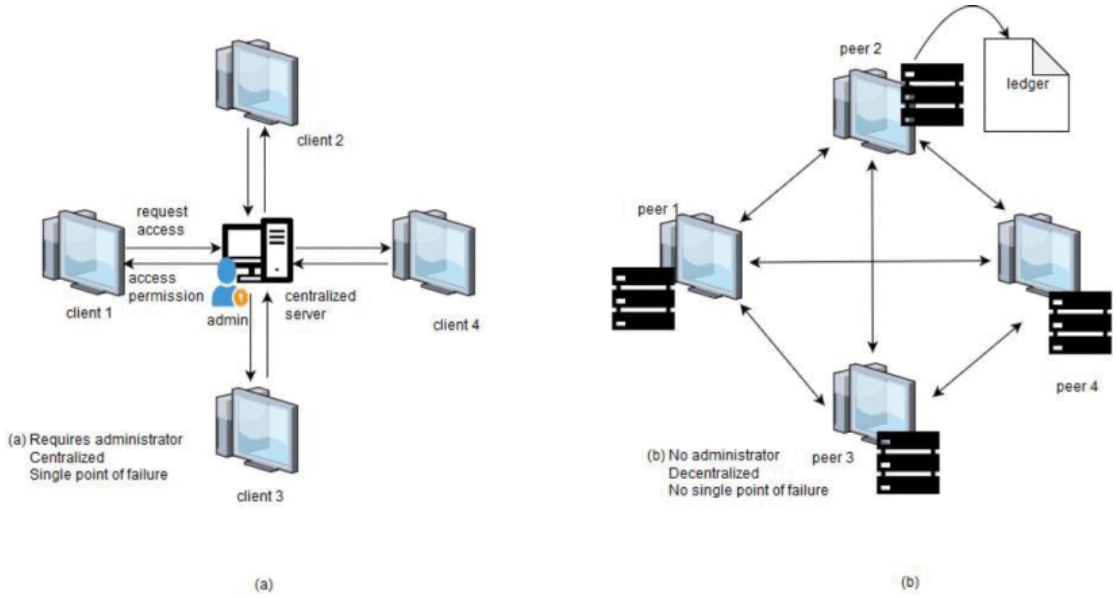
3.1.2 Πρωτόκολλο Συναίνεσης

Η τεχνολογία Blockchain χαρακτηρίζεται από την έλλειψη κεντρικής διαχείρισης. Οι αρχές της και η λειτουργία της βασίζεται για αυτό το λόγο στην σύναψη εμπιστοσύνης και συναίνεσης μεταξύ των συμμετεχόντων. Για να εξαλειφθεί η πιθανότητα απάτης ή επίθεσης στο δίκτυο κατά την διάρκεια των συναλλαγών αναπτύχθηκαν διάφορα πρωτόκολλα (αλγόριθμοι) συναίνεσης έτσι ώστε να είναι δυνατή η συμφωνία για την κατάσταση του δικτύου peer-to-peer. Στην παραπάνω διαδικασία της συναίνεσης συμμετέχουν όλοι οι κόμβοι χρησιμοποιώντας το πρωτόκολλο και πλειοψηφικά κάνουν δεκτά τα block. Η δημιουργία νέων blocks και η πρόσθεση τους στο υπάρχον καθολικό ονομάζεται μηχανισμός συναίνεσης, κάποιοι από τους οποίους είναι ο αλγόριθμος Proof-of-Work, Proof-of-Authority, Proof-of-Stakeοι οποίοι θα παρουσιαστούν αναλυτικότερα μεταξύ άλλων σε επόμενη ενότητα.

3.1.3 Ψηφιακό Νόμισμα

Το Ψηφιακό νόμισμα έχει ιδιαίτερη σημασία στην λειτουργία του Blockchain καθώς λειτουργεί ως ανταμοιβή και αποτελεί το κίνητρο για τους κόμβους Miners έτσι ώστε να προσφέρουν την υπολογιστική τους δύναμη για να υπολογίσουν τις τιμές του nonce και hash ενός block. Ο πρώτος miner που θα φτάσει στη λύση του προβλήματος θα λάβει ένα αντίτιμο ψηφιακού νομίσματος ως την πρώτη συναλλαγή του νέου block. Με αυτό τον τρόπο επιταχύνεται η διαδικασία αποδοχής των block και η εύρεση την επόμενης τιμής hash. Το πρώτο ψηφιακό νόμισμα στο Blockchain, που λειτουργούσε και ως ανταμοιβή ήταν το Bitcoin, στην περίπτωση του οποίου η ανταμοιβή μειώνεται στο μισό κάθε φορά που δημιουργούνται 210.000 blocks [52]. Τα διαφορετικά ψηφιακά νομίσματα λειτουργούν με παρόμοιο τρόπο.

3.2 Τα Χαρακτηριστικά της τεχνολογίας Blockchain



Εικόνα 4 : ΣΥΓΚΡΙΣΗ (Α) ΠΑΡΑΔΟΣΙΑΚΟΥ ΔΙΚΤΥΟΥ ΚΑΙ (Β) BLOCKCHAIN [54]

Σε γενικό πλαίσιο, η τεχνολογία Blockchain είναι μια ασφαλής και αποκεντρωμένη βάση συναλλαγών και παρουσιάζει τα εξής κύρια χαρακτηριστικά[32],[33]:

Αποκέντρωση

Σε αντίθεση με τα συμβατικά συστήματα συναλλαγών, στα οποία η κάθε συναλλαγή πρέπει να επαληθευτεί από τη κεντρική αρμόδια-αξιόπιστη υπηρεσία, κάτι τέτοιο δεν χρειάζεται πλέον όταν εφαρμόζεται η τεχνολογία Blockchain. Συγκεκριμένα, με τη χρήση αλγόριθμων συναίνεσης επιτυγχάνεται η συνοχή των δεδομένων στο κατανεμημένο δίκτυο.

Ακρίβεια και Διαφάνεια στις Συναλλαγές

Η διαδικασία επικύρωσης της κάθε συναλλαγής γίνεται σε μικρό χρονικό διάστημα. Αυτό έχει ως αποτέλεσμα να είναι σχεδόν απίθανο να πραγματοποιηθεί διαγραφή ή επαναφορά της συναλλαγής από τη στιγμή που συμπεριληφθεί στο blockchain. Οι δε άκυρες συναλλαγές μπορούν να ανακαλυφθούν αμέσως.

Ανωνυμία

Η πραγματική ταυτότητα του κάθε χρήστη δεν αποκαλύπτεται, καθώς αυτός αλληλεπιδρά με το blockchain με τη χρήση μιας δημιουργημένης διεύθυνσης. Έτσι

επιτυγχάνεται η ανταλλαγή δεδομένων ανάμεσα στους χρήστες και οι πληροφορίες παραμένουν εντός της αλυσίδας.

Ανιχνευσιμότητα

Οι συναλλαγές στο blockchain είναι διατεταγμένες σε χρονολογική σειρά κατά την οποία πραγματοποιήθηκαν, ενώ κάθε block συνδέεται με άλλα δυο γειτονικά blocks μέσω της συνάρτησης κρυπτογράφησης hash[33]. Με αυτόν τον τρόπο, κάθε συναλλαγή είναι ανιχνεύσιμη μέσω την επεξεργασίας των πληροφοριών του block που συνδέονται με τα κλειδιά hash.

Αμεσότητα

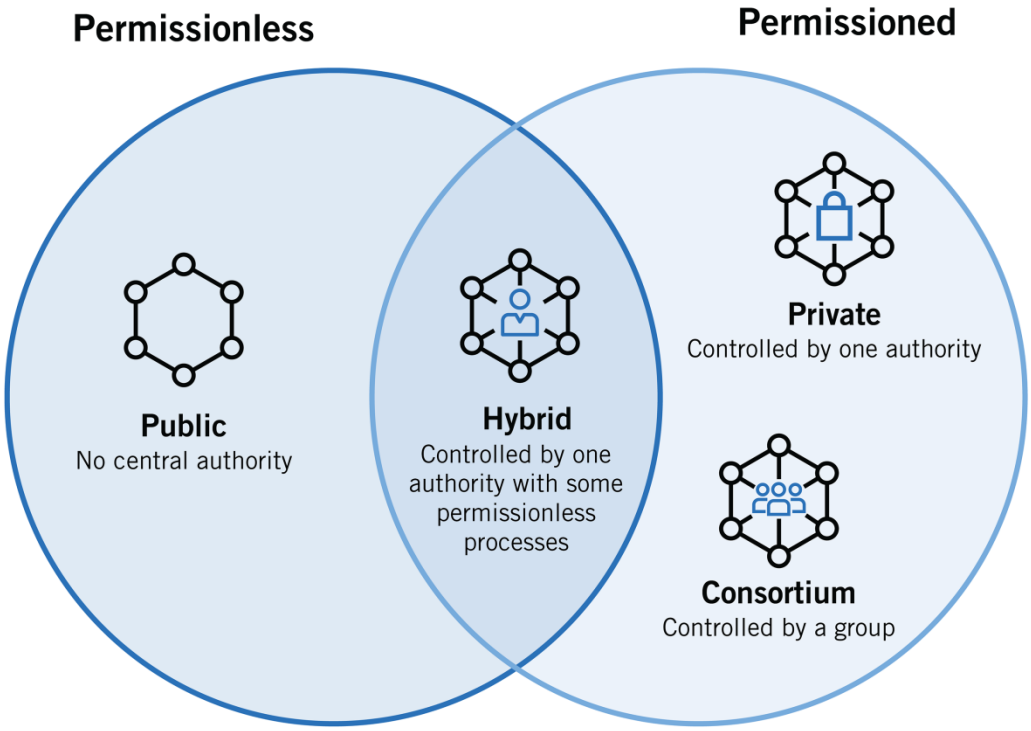
Η επικύρωση των συναλλαγών μπορεί να πραγματοποιηθεί σε σύντομο χρονικό διάστημα, όπως και η απόρριψη των μη έγκυρων αντίστοιχα από τους miners[32] καθώς τα blocks που περιέχουν αυτού του είδους τις συναλλαγές ανακαλύπτονται αμέσως. Είναι πρακτικά αδύνατο να διαγραφούν ή να ανατραπούν συναλλαγές εφόσον έχουν εισαχθεί στο blockchain.

Δυνατότητα Ελέγχου

Κάθε νέα συναλλαγή πρέπει να αναφέρεται σε μια προηγούμενη αδιευθέτητη συναλλαγή και μόλις αυτή καταγραφεί στο blockchain, η κατάσταση τους αλλάζει σε διευθετημένες. Με αυτό τον τρόπο οι συναλλαγές παρακολουθούνται και επαληθεύονται εύκολα.

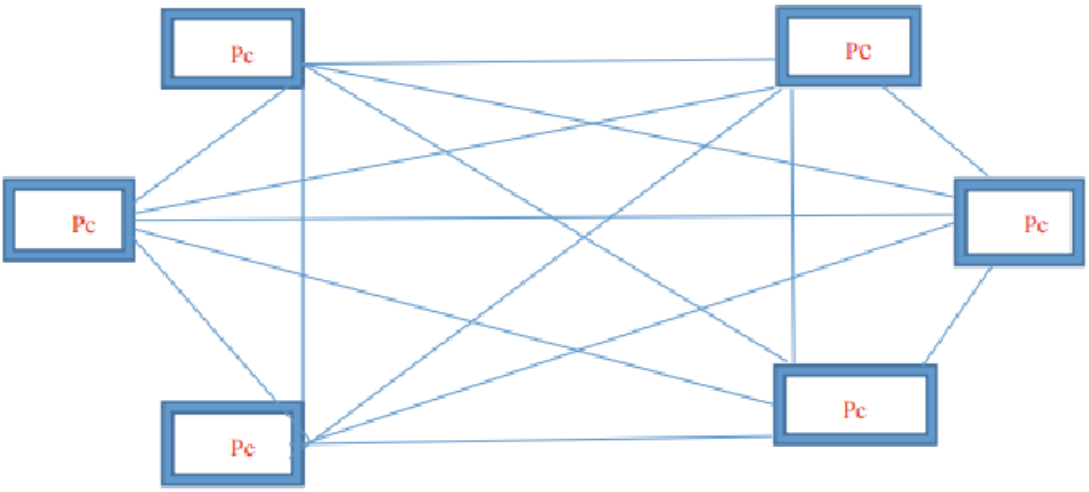
3.3 Κατηγορίες συστημάτων Blockchain

Τα συστήματα Blockchain μπορούν να διαχωριστούν σε τέσσερις κατηγορίες, τα δημόσια ή χωρίς άδεια (public ή permissionless), τα ιδιωτικά ή με άδεια (private ή permissioned), τα κοινοπρακτικά (consortium) και τα υβριδικά (hybrid)[38]. Αυτή η κατηγοριοποίηση γίνεται με κριτήριο την χρήση του κάθε συστήματος και τα διακριτά χαρακτηριστικά τους. Όλα τα παραδείγματα Blockchain παρουσιάζονται σε όλους τους διαφορετικούς τύπους, συμπεριλαμβανομένων των κρυπτονομισμάτων όπως το Bitcoin, των έξυπνων συμβολαίων όπως το Ethereum και των εφαρμογών Blockchain.



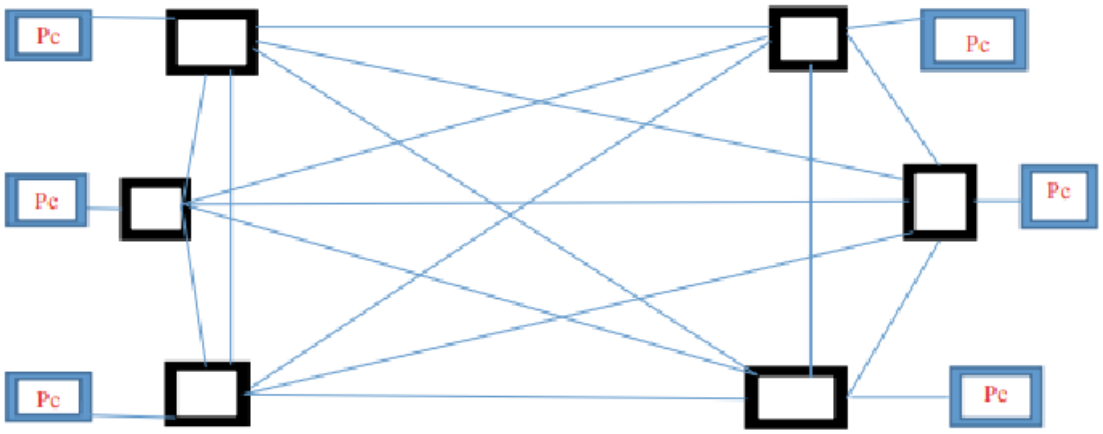
Εικόνα 5 : ΟΙ ΚΑΤΗΓΟΡΙΕΣ ΤΩΝ ΣΥΣΤΗΜΑΤΩΝ BLOCKCHAIN [38]

Public Blockchain: Τα δημόσια συστήματα λειτουργούν χωρίς αρχές και μεσάζοντες και επιτρέπουν σε όλους τους κόμβους του blockchain να έχουν τα ίδια δικαιώματα στην πρόσβαση σε αυτό, στην δημιουργία νέου block δεδομένων αλλά και στη διαδικασία συναίνεσης. Η κύρια χρήση τους είναι η συναλλαγή και η εξόρυξη κρυπτονομισμάτων, με τα πιο γνωστά παραδείγματα δημόσιου συστήματος blockchain να είναι το Bitcoin και το Ethereum. Οι συμμετέχοντες κόμβοι αναλαμβάνουν την επικύρωση των συναλλαγών που έχουν αιτηθεί προς το δίκτυο με τη δημιουργία νέων blockμε τη χρήση κρυπτογράφησης. Ως ανταμοιβή αυτής της διαδικασίας επιστρέφεται μια μικρή ποσότητα κρυπτονομίσματος. Τα μεγαλύτερα πλεονεκτήματα που προσφέρουν αυτού του είδους τα συστήματα είναι η ασφάλεια και το αμετάβλητο των δεδομένων[39], ταυτόχρονα όμως χαρακτηρίζονται από χαμηλή ταχύτητα στις συναλλαγές. Για παράδειγμα, το Bitcoin μπορεί να διαχειριστεί 7 συναλλαγές ανά δευτερόλεπτο, ενώ η VISA στο αντίστοιχο χρονικό διάστημα μπορεί να διαχειριστεί 24.000. Αυτό οφείλεται στο ότι η διαδικασία της συναίνεσης στο δίκτυο απαιτεί αρκετό χρόνο.



Εικόνα 6 : ΑΠΕΙΚΟΝΙΣΗ PUBLIC BLOCKCHAIN [76]

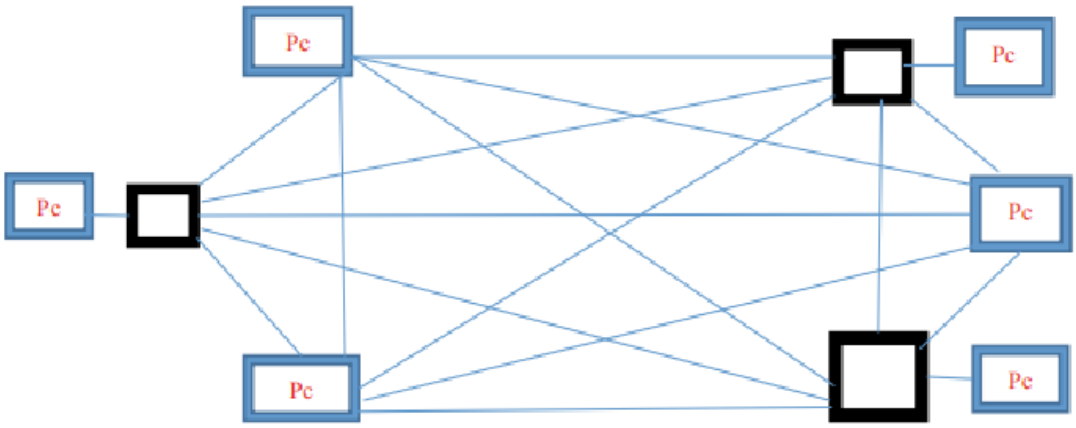
Private Blockchain: Ένα ιδιωτικό σύστημα Blockchain βρίσκεται υπό τον έλεγχο μιας οντότητας ή οργανισμού. Η κεντρική αρχή του συστήματος είναι αυτή που υποδεικνύει ποιοι από τους κόμβους έχουν το δικαίωμα να εκτελέσουν λειτουργίες και να λάβουν μέρος στην διαδικασία της συναίνεσης. Τα ιδιωτικά συστήματα είναι μερικώς αποκεντρωμένα, καθώς η δημόσια πρόσβαση σε αυτά είναι περιορισμένη και καθορίζεται από τον διαχειριστή του δικτύου. Από τους χρήστες ζητείται να είναι εξουσιοδοτημένοι έτσι ώστε να μπορούν να διαβάσουν ή να εισάγουν δεδομένα στο blockchain[40]. Σε αντίθεση με τα δημόσια, τα ιδιωτικά blockchains είναι γρηγορότερα λόγω των λιγότερων συμμετεχόντων στην διαδικασία της συναλλαγής. Το βασικό μειονέκτημα που χαρακτηρίζει τα ιδιωτικά συστήματα είναι ότι είναι ευάλωτα σε πιθανές απάτες λόγω του μικρότερου αριθμού κόμβων. Με κριτήριο το ποιος έχει πρόσβαση στα δεδομένα, προκύπτουν δυο νέες υποκατηγορίες: τα ανοιχτά ιδιωτικά, στα οποία μόνο λίγοι εξουσιοδοτημένοι χρήστες αποκτούν άδεια να εισάγουν δεδομένα αλλά όλοι έχουν την δυνατότητα να τα διαβάσουν εφόσον εισαχθούν στο blockchain και τα κλειστά ιδιωτικά blockchains, στα οποία η πρόσβαση στα δεδομένα αποτελεί προνόμιο συγκεκριμένων εξουσιοδοτημένων χρηστών.



Εικόνα 7 : ΑΠΕΙΚΟΝΙΣΗ PRIVATEBLOCKCHAIN [76]

Consortium Blockchain: Για να αντιμετωπιστούν τα μειονεκτήματα των ιδιωτικών και δημόσιων blockchain, αναπτύχθηκαν τα κοινοπρακτικά συστήματα. Είναι ημι-αποκεντρωμένος τύπος Blockchain που διοικείται από περισσότερους από έναν οργανισμούς, με αποτέλεσμα να είναι πιο αποκεντρωμένος σε σύγκριση με τα ιδιωτικά blockchain. Μια κοινοπραξία Blockchain είναι ένα μερικώς ιδιωτικό σύστημα με ελεγχόμενο σύνολο χρηστών, αλλά λειτουργεί σε διαφορετικούς οργανισμούς[41]. Για το λόγο αυτό, η δημιουργία ενός τέτοιου συστήματος αποτελεί χρονοβόρα διαδικασία καθώς απαιτείται η συνεργασία αυτών των οργανισμών. Η πρόσβαση στο καθολικό από τον χρήστη γίνεται κατόπιν εξουσιοδότησης. Η πιο συχνή χρήση τους είναι στον επιχειρηματικό χώρο, σε περιπτώσεις που ομάδες οργανισμών συνεργάζονται αξιοποιώντας την τεχνολογία Blockchain για την εξυπηρέτηση των αναγκών τους.

Hybrid Blockchain:Τα υβριδικά συστήματα Blockchain αποτελούν συνδυασμό των δημόσιων και των ιδιωτικών συστημάτων[42]. Ελέγχονται από ένα μοναδικό οργανισμό, αλλά με ένα επίπεδο εποπτείας που πραγματοποιείται από το δημόσιο Blockchain με την εκτέλεση ορισμένων επικυρώσεων στις συναλλαγές. Αυτά τα συστήματα επιτρέπουν σε κάθε κόμβο να αποτελεί μέρος της διαδικασίας συναίνεσης, αλλά μόνο κάποιοι συγκεκριμένοι μπορούν να διαμορφώσουν το επόμενο block. Με αυτό τον τρόπο επιτυγχάνονται ορισμένα χαρακτηριστικά του blockchain, όπως ακεραιότητα, ασφάλεια και διαφάνεια στις συναλλαγές. Ο χρήστης εφόσον αποκτήσει άδεια πρόσβασης, έχει την δυνατότητα να πραγματοποιήσει, τροποποιήσει και να διαβάσει συναλλαγές χωρίς να αποκαλύπτει την ταυτότητα του στο δημόσιο δίκτυο.



Εικόνα 8 : ΑΠΕΙΚΟΝΙΣΗ HYBRIDBLOCKCHAIN [76]

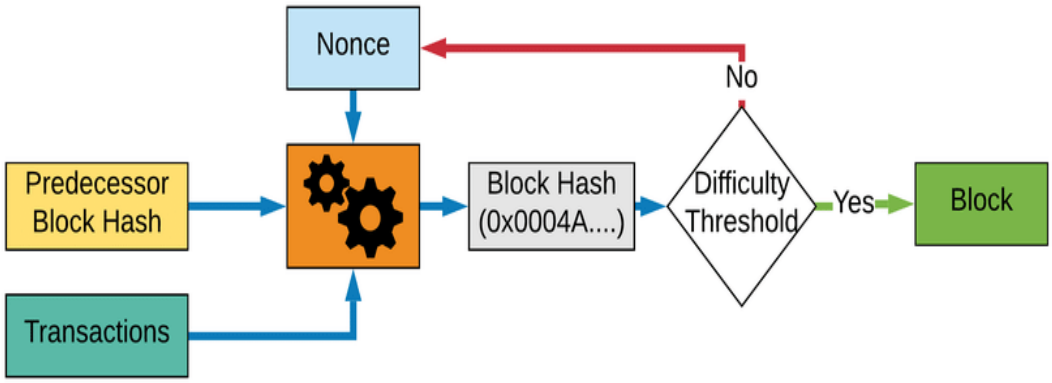
3.4 Μηχανισμοί Συναίνεσης στο Blockchain

Η τεχνολογία Blockchain πραγματοποιεί συναλλαγές μεταξύ δυο οντοτήτων χωρίς την ύπαρξη μεσάζοντα. Για την επικύρωση και επαλήθευση των συναλλαγών αυτών χρησιμοποιούνται μηχανισμοί που είναι γνωστοί ως αλγόριθμοι συναίνεσης. Σύμφωνα με το [43] μηχανισμός συναίνεσης ορίζεται ως μια μέθοδος που επιβεβαιώνει την σωστή κατάσταση δικτύου σε ένα κατανεμημένο σύστημα. Παρακάτω παρουσιάζονται οι πιο ευρέως διαδεδομένοι αλγόριθμοι συναίνεσης που χρησιμοποιούνται στα συστήματα Blockchain.

3.4.1 Ο αλγόριθμος Proof-of-Work

Ο αλγόριθμος Proof-of-Work (PoW) έχει ως στόχο την επίλυση ενός υπολογιστικά απαιτητικού μαθηματικού προβλήματος[40] (όπως για παράδειγμα ο υπολογισμός μιας τιμής SHA 256-bit). Η επίλυση που προκύπτει υποδεικνύει ότι ένας κόμβος έχει πραγματοποιήσει τις απαραίτητες ενέργειες έτσι ώστε ένα block να γίνει δεκτό στο blockchain[44]. Οι κόμβοι miners συνήθως προσπαθούν να λύσουν το πρόβλημα με την εύρεση μιας τιμής η οποία όταν δοθεί και εκτελεστεί μέσω κρυπτογραφικού αλγόριθμου θα προκύψει ως αποτέλεσμα μια νέα τιμή κατακερματισμού που αποτελείται από προκαθορισμένο αριθμό αρχικών μηδενικών[45]. Ο μόνος τρόπος

επίλυσης του προβλήματος είναι η συνεχής δοκιμή για λάθος. Αυτό σημαίνει βέβαια ότι ο αλγόριθμος PoW απαιτεί μεγάλο όγκο πόρων για τη λειτουργία του. Ως ανταμοιβή για τη λύση του προβλήματος, τα περισσότερα συστήματα Blockchain προσφέρουν κάποιας μορφής κρυπτονόμισμα. Η διαδικασία αυτή είναι γνωστή και ως εξόρυξη. Επειδή όμως την ανταμοιβή λαμβάνει μόνο ένας από τους υποψήφιους κόμβους, ο μηχανισμός PoW καταναλώσει μεγάλη ποσότητα ενέργειας καθώς οι miners χρησιμοποιούν ολοένα και δυνατότερους επεξεργαστές με στόχο να υπερισχύσουν έναντι του ανταγωνισμού. Το χαρακτηριστικό αυτό λειτουργεί και ως δικλίδα ασφαλείας για το δίκτυο, καθώς για να καταλάβει ένας κακόβουλος χρήστης το δίκτυο θα πρέπει σε θεωρητικό επίπεδο να κατέχει τουλάχιστον την πλειοψηφία της συνολικής υπολογιστικής δύναμης του δικτύου.

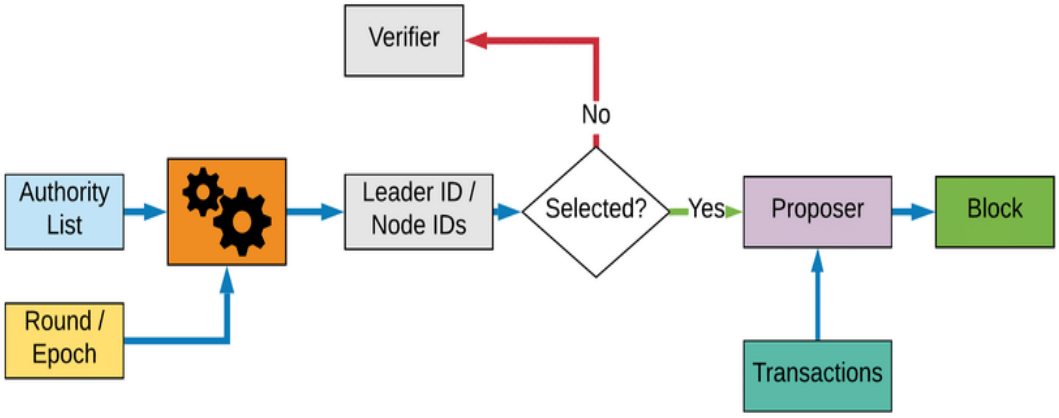


Εικόνα 9 : ΤΟ ΔΙΑΓΡΑΜΜΑ ΡΟΗΣ ΤΟΥ PROOF-OF-WORK[77]

3.4.2 Ο αλγόριθμος Proof-of-Authority

Ο μηχανισμός συναίνεσης Proof-of-Authority (PoA) λειτουργεί με βασικό κριτήριο την εμπιστοσύνη. Σύμφωνα με το [46], στο PoA ένα σύνολο έμπιστων κόμβων επωμίζονται την ικανότητα να δημιουργήσουν νέα blocks. Αυτοί οι κόμβοι αναφέρονται ως sealers και οι ταυτότητες τους πρέπει να μπορούν να επαληθευτούν από το Blockchain, με αποτέλεσμα να επηρεάζεται η φήμη τους. Σε αντίθεση με την περίπτωση του PoW όπου αξιοποιούν κρυπτονομίσματα, στο PoA οι χρήστες ποντάρουν την ταυτότητα τους. Η διαδικασία αυτή δεν απαιτεί ιδιαίτερη υπολογιστική ισχύ. Οι κόμβοι που έχουν χαμηλή φήμη στο δίκτυο έχουν και λιγότερες πιθανότητες να εκδώσουν νέα blocks. Με αυτόν τον τρόπο αποτρέπεται και η κακόβουλη δραστηριότητα ως προς το δίκτυο. Απαραίτητη προϋπόθεση για την λειτουργία του μηχανισμού είναι η εξακρίβωση της πραγματικής ταυτότητας των χρηστών προκειμένου να συμμετάσχουν στο δίκτυο. Με αυτό το χαρακτηριστικό

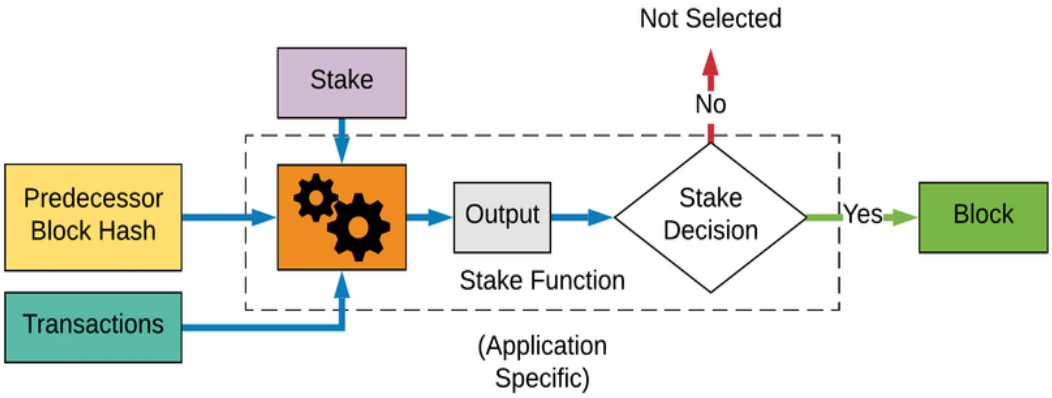
όμως προκύπτει ένα βασικό μειονέκτημα του PoA, καθώς αποκλείει από την ανωνυμία που προσφέρουν άλλοι μηχανισμοί συναίνεσης[40].



Εικόνα 10 : ΤΟ ΔΙΑΓΡΑΜΜΑ ΡΟΗΣ ΤΟΥ PROOF-OF-AUTHORITY [77]

3.4.3 Ο αλγόριθμος Proof-of-Stake

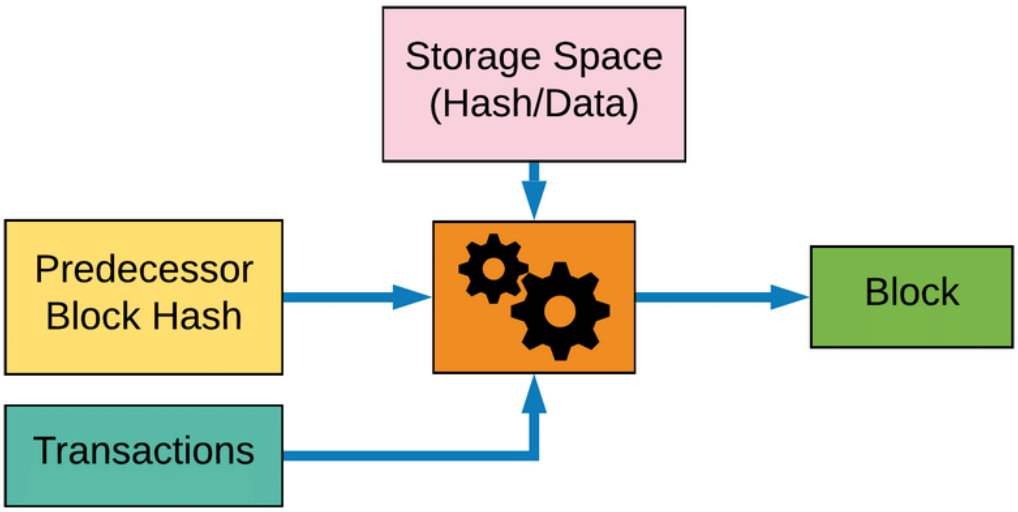
Ο μηχανισμός συναίνεσης Proof-of-Stake (PoS) στοχεύει στην διατήρηση της αποκεντροποίησης του Blockchain δικτύου[42] και επιβραβεύει τους χρήστες που έχουν το μεγαλύτερο διακύβευμα (stake) στο δίκτυο. Αυτό σημαίνει ότι ένας κόμβος που κατέχει n% των πόρων θα έχει αντίστοιχα n% πιθανότητες να δημιουργήσει ένα νέο block. Σε αντίθεση με την περίπτωση του PoW, απαιτούνται λιγότεροι πόροι όπως χρόνος, ενέργεια και υπολογιστική ισχύς καθώς δεν περιλαμβάνει την διαδικασία της εξόρυξης. Για το λόγο αυτό η ανταμοιβή για την έκδοση block πραγματοποιείται μέσω χρεώσεων των συναλλαγών. Οι χρήστες καταθέτουν μέρος του ψηφιακού τους νομίσματος ως εγγύηση για τη επικύρωση του νέου block στο δίκτυο και έτσι επιτυγχάνεται η συναίνεση. Εφόσον επιλεχθεί ο χρήστης που θα εκδώσει το επόμενο block, ελέγχεται η εγκυρότητα όλων των συναλλαγών και έπειτα το υπογράφει πριν προστεθεί στο blockchain. Στην περίπτωση χρήστη που παρουσιάζει κακόβουλη δραστηριότητα, το διακύβευμα του χάνεται. Ο συγκεκριμένος μηχανισμός χρησιμοποιείται κατεξοχήν για αλγόριθμους συναίνεσης κρυπτονομισμάτων λόγω των πλεονεκτημάτων που προσφέρει σε θέματα ασφάλειας, εξοικονόμησης ενέργειας και αποκέντρωσης καθώς και (όπως αναφέρθηκε παραπάνω) χαμηλής υπολογιστικής πολυπλοκότητας.



Εικόνα 11 : ΤΟ ΔΙΑΓΡΑΜΜΑ ΡΟΗΣ ΤΟΥ PROOF-OF-STAKE [77]

3.4.4 Ο αλγόριθμος Proof-of-Space

Ο αλγόριθμος συναίνεσης Proof-of-Space ή Proof-of-Capacity (PoC) όπως είναι γνωστός εναλλακτικά, αναμένει από τους κόμβους να παρέχουν απόδειξη ότι κατέχουν τον επαρκή χώρος αποθήκευσης για την επίλυση ενός υπολογιστικού προβλήματος. Ο αλγόριθμος PoC προορίζεται για υπολογιστικά προβλήματα τα οποία χρειάζονται ιδιαίτερα μεγάλη ποσότητα αποθηκευτικής μνήμης με σκοπό την επίλυση ενός προβλήματος. Συγκεκριμένα ο επαληθευτής αρχικά αναμένει από έναν prover να δεσμευτεί σε μια επισήμανση του γραφήματος και στη συνέχεια, ρωτά τον prover για τυχαίες θέσεις στο δεσμευμένο γράφημα[42]. Η βασική αρχή σε αυτή την προσέγγιση είναι ότι στην περίπτωση που ο prover δεν έχει τον απαραίτητο αποθηκευτικό χώρο, δεν θα επιτευχθεί η επαλήθευση του. Λόγω της προσέγγισης του PoC όσον αφορά την αποδοτικότητα στην χρήση πόρων και αποθηκευτικού χώρου, το αποτέλεσμα είναι η εξοικονόμηση ενέργειας σε σύγκριση με άλλους αλγόριθμους συναίνεσης (PoW).



Εικόνα 12 : ΤΟ ΔΙΑΓΡΑΜΜΑ ΡΟΗΣ ΤΟΥ PROOF-OF-CAPACITY [77]

3.4.5 Ο αλγόριθμος Practical Byzantine Fault Tolerance

Ο αλγόριθμος Practical Byzantine Fault Tolerance (PBFT) προτάθηκε για πρώτη φορά στο [48] και αποτελεί ένα βελτιωμένο και περισσότερο πρακτικό πρωτόκολλο του αρχικού Byzantine Fault Tolerance (BFT). Σε αντίθεση με τους αλγόριθμούς που παρουσιάζονται παραπάνω και βασίζονται στην απόδειξη όπως ο PoW, όπου το όριο ασφαλείας είναι το ποσοστό 51% για τους κακόβουλους χρήστες, το PBFT απαιτεί από τον αριθμό των κακόβουλων χρηστών να είναι μικρότερο από το 33% τους συνόλου των συμμετεχόντων έτσι ώστε να εξασφαλίσει την προστασία του συστήματος από κακόβουλες επιθέσεις που το απειλούν. Το PBFT ενδείκνυται κυρίως για ιδιωτικά και κοινοπρακτικά συστήματα blockchain λόγω της χαμηλής πολυπλοκότητας και κατανάλωσης ενέργειας που το χαρακτηρίζουν και είναι ιδιαίτερα σημαντικά για τις ασύρματες εφαρμογές του Διαδικτύου των Πραγμάτων. Σε αυτό το σύστημα οι κόμβοι ταξινομούνται διαδοχικά και επικοινωνούν μεταξύ τους για την κατάσταση του συστήματος με βάση τον κανόνα της πλειοψηφίας. Έτσι, από την άποψη της πολυπλοκότητας της επικοινωνίας, το blockchain που βασίζεται στο σύστημα PBFT μπορεί να φτάσει μετά βίας τον αριθμό των 100 κόμβων[49][50].

Κάποιοι άλλοι λιγότερο διαδεδομένοι αλγόριθμοι συναίνεσης είναι οι εξής : Proof-of-Activity, Proof-of-Importance, Proof-of-Burn, Proof-of-Weight, Delegated Proof-of-Stake, Leased Proof-of-Stake, Proof of Elapsed Time, Proof-of-Luck, Simplified Byzantine Fault Tolerance, Delegated Byzantine Fault Tolerance, Directed Acyclic Graphs.

3.5 Επιθέσεις στο Blockchain

Η τεχνολογία Blockchain προσφέρει στους χρήστες τις ορισμένες υπηρεσίες ασφαλείας. Κάποιες από αυτές, όπως η ακεραιότητα των δεδομένων, ο έλεγχος ταυτότητας και η διατήρηση του απορρήτου υφίστανται διαφόρων ειδών επιθέσεις που αποσκοπούν στην έκθεση του συστήματος και απειλούν την ασφάλεια του.

3.5.1 Πλειοψηφική Επίθεση 51%

Κατά την Επίθεση 51% στο Blockchain, ένας ή περισσότεροι miners ελέγχουν την πλειοψηφία (δηλαδή ποσοστό ίσο ή μεγαλύτερο του 51%) της υπολογιστικής δύναμης του δικτύου ή της εξόρυξης. Η διαδικασία της επίθεσης ξεκινάει με τη δημιουργία μια ιδιωτικής αλυσίδας που αποτελείται από blocks και είναι πλήρως απομονωμένη από την πραγματική αλυσίδα[53]. Στην συνέχεια, η αλυσίδα αυτή παρουσιάζεται στο δίκτυο ως αυθεντική. Οι επιτιθέμενοι χρησιμοποιούν αυτού του είδους την επίθεση με σκοπό να αντιστρέψουν τις συναλλαγές στο Blockchain και να επηρεάσουν την διαδικασία αποθήκευσης του νέου block. Αποτέλεσμα είναι οι συναλλαγές αυτές να μην επιβεβαιώνονται και ως εκ τούτου τελικά να μην πραγματοποιούνται. Η επίθεση βασίζεται στην αρχή λειτουργίας του blockchain σύμφωνα την οποία η μεγαλύτερη αλυσίδα γίνεται δεκτή, για αυτό τον λόγο είναι και απαραίτητη η κατοχή της πλειοψηφίας της υπολογιστικής δύναμης έτσι ώστε να κατευθυνθούν οι κόμβοι του δικτύου και να κάνουν δεκτή την αλυσίδα. Πρέπει να σημειωθεί ότι η επίθεση μπορεί να πραγματοποιηθεί και με την μειοψηφία της υπολογιστικής δύναμης αλλά στην περίπτωση αυτή οι πιθανότητες επιτυχίας είναι σημαντικά λιγότερες. Το κόστος είναι ανάλογο με τη συνολική υπολογιστικής ισχύ του συστήματος. Για αυτό τον λόγο τα κρυπτονομίσματα με υψηλή ισχύ δικτύου δεν είναι τόσο ευάλωτα στην Επίθεση 51%.

3.5.2 Επίθεση Συμπαιγνίας (Collusion Attack)

Στην επίθεση συμπαιγνίας ο επιτιθέμενος βρίσκει μια παρόμοια τιμή του κατακερματισμού hash για τα δεδομένα που μεταδίδονται στο δίκτυο Blockchain και την χρησιμοποιεί για να κερδίσει την ανταμοιβή[54], γεγονός που αποτελεί παραβίαση του πρωτοκόλλου.

3.5.3 Επίθεση Sybil (Sybil Attack)

Σε αυτή την περίπτωση οι επιτιθέμενοι αναλαμβάνουν τον έλεγχο πολλαπλών κόμβων στο δίκτυο ορίζοντας κόμβους με πολλαπλές ταυτότητες. Με αυτόν τον τρόπο επιτυγχάνουν τη δημιουργία σύγχυσης στο δίκτυο. Οι ψεύτικοι κόμβοι φαίνονται γνήσιοι [53] και στοχεύουν στην παραποίηση του δικτύου μέσω της επικύρωσης μη εξουσιοδοτημένων συναλλαγών αλλά και την αλλαγή κάποιων έγκυρων συναλλαγών. Ως ψεύτικοι κόμβοι για την επίθεση, μπορούν να χρησιμοποιηθούν διάφορες συσκευές, εικονικές μηχανές ή διευθύνσεις πρωτοκόλλου διαδικτύου (IP) και προσφέρουν την δυνατότητα στους επιτιθέμενους να αρνηθούν την μετάδοση των blocks.

3.5.4 Επίθεση Έκλειψης (Eclipse Attack)

Η Επίθεση Έκλειψης στοχεύει στην απομόνωση της επικοινωνίας ανάμεσα στους κόμβους του δικτύου με την απόκρυψη πληροφοριών. Ένας μικρός αριθμός κακόβουλων κόμβων συνεργάζονται ώστε να εισέλθουν στο δίκτυο ως νόμιμοι χρήστες και να αποκρύψουν από τους υπόλοιπους κόμβους την τρέχουσα δραστηριότητα του δικτύου. Εάν η Επίθεση Έκλειψης είναι επιτυχής, ο επιτιθέμενος έχει την δυνατότητα να ελέγχει την κυκλοφορία των πληροφοριών ανάμεσα στους κόμβους του δικτύου και να επιτρέπει την αυθαίρετη άρνηση υπηρεσιών ή επιθέσεις λογοκρισίας [55]. Η επίθεση αυτή σχετίζεται με την επίθεση Sybil, αλλά μπορεί να πραγματοποιηθεί και να παρακάμψει την ύπαρξη αμυντικών μηχανισμών της. Η ύπαρξη ενός μικρού αριθμού κακόβουλων κόμβων αναγνωρισμένων από το δίκτυο με τις πραγματικές ταυτότητες τους είναι αρκετή για να φέρουν εις πέρας την επίθεση. Αντίθετα, η επίθεση Sybil μπορεί να χρησιμοποιηθεί αρχικά έτσι ώστε να προκαλέσει στη συνέχεια μια επίθεση Έκλειψης. Μια προέκταση της είναι η Τοπική Επίθεση Έκλειψης (Localised Eclipse Attack) στην οποία ο επιτιθέμενος κατέχει γνώση σχετικά με την εφαρμογή του δικτύου Peer-to-Peer και με την εφαρμογή της είναι δυνατή η λογοκρισία μεμονωμένων αρχείων ή ακόμα και η ολική διακοπή τροφοδοσίας ρεύματος σε ένα ηλεκτρικό δίκτυο.

3.5.5 Επίθεση Κατανεμημένης Άρνησης Υπηρεσίας (DDoSAttack)

Η επίθεση Distributed-denial-of-service (ή DDoS) λαμβάνει χώρα όταν πολλαπλά συστήματα κατακλύζουν τους πόρους και το εύρος ζώνης του στοχευόμενου κόμβου[54]. Έτσι, ο κόμβος που δέχεται την επίθεση απορρίπτεται από την

συναλλαγή λόγω υπερφόρτωσης του συστήματος. Σε ένα δίκτυο Blockchain κανένας κόμβος δεν είναι απαραίτητος, άρα κάθε κόμβος είναι ευάλωτος σε μια επίθεση DDoS χωρίς την συνολική κατάργηση του δικτύου. Ωστόσο αυτό δεν σημαίνει ότι τα δίκτυα Blockchain είναι απρόσβλητα σε τέτοιου είδους επιθέσεις. Με την υπερφόρτωση του δικτύου με συναλλαγές, ο επιτιθέμενος έχει την δυνατότητα να μειώσει την διαθεσιμότητα του για τους χρήστες.

3.5.6 Κλοπή ταυτότητας χρήστη

Ένα από τα βασικά χαρακτηριστικά ενός συστήματος Blockchain είναι η ανωνυμία και η ασφάλεια που προσφέρει στους χρήστες του. Βασικό ρόλο στην διατήρηση της ασφάλειας του χρήστη κατέχει η προστασία του ιδιωτικού του κλειδιού. Σε περίπτωση που το ιδιωτικό κλειδί κλαπεί, δεν μπορεί να ανακτηθεί και επομένως χάνεται το απόρρητο και τα δικαιώματα ιδιοκτησίας του χρήστη που συνδέονται με το Blockchain.

3.6 Πλεονεκτήματα της χρήσης Blockchain

Με βάση τα χαρακτηριστικά της τεχνολογίας blockchain που παρουσιάστηκαν παραπάνω, προκύπτουν κάποια πλεονεκτήματα των εφαρμογών που χρησιμοποιούν την τεχνολογία αυτή.

Χρόνος Επεξεργασίας

Οι συναλλαγές μέσω του παραδοσιακού τραπεζικού συστήματος απαιτούσαν μεγάλα χρονικά διαστήματα για την επεξεργασία τους. Με την εδραίωση του blockchain, ο χρόνος αναμονής για τη διεκπεραίωση τους μειώθηκε από μέρες σε λεπτά ή ακόμα και δευτερόλεπτα[88].

Κόστος

Η τεχνολογία blockchain αφαιρεί την ανάγκη ύπαρξης μεσάζοντα με σκοπό την παρακολούθηση των συναλλαγών. Στο παράδειγμα των τραπεζικών συστημάτων που αναφέρθηκε παραπάνω, υπάρχουν συγκεκριμένες χρεώσεις ανά συναλλαγή. Με τον τρόπο αυτό, οι συναλλαγές στο blockchain χαρακτηρίζονται από σημαντικά χαμηλότερο κόστος[90].

Ασφάλεια

Το δίκτυο Blockchain χρησιμοποιεί τη μαθηματική λειτουργία του κατακερματισμού (**hash**) που δέχεται ως είσοδο μια συμβολοσειρά μεταβλητού μήκους και τη μετατρέπει σε μια δυαδική ακολουθία σταθερού μήκους. Η διαδικασία αυτή είναι πολύ δύσκολο να αντιστραφεί μόνο με τη χρήση του αποτελέσματος καθώς τα δεδομένα εισόδου δεν μπορούν να προσδιοριστούν[34].

Αυτοματοποίηση

Το blockchain αυτοματοποιεί τις συναλλαγές που γίνονται στο σύστημα εκμεταλλευόμενο την ύπαρξη των έξυπνων συμβολαίων. Με το περιορισμό του ανθρώπινου παράγοντα, επιτυγχάνει να αυξήσει ακόμα περισσότερο την απόδοση και παράλληλα να μειώσει το χρόνο εκτέλεσης. Κάθε βήμα εκτελείται αυτόματα εφόσον πληρούνται οι προκαθορισμένες προϋποθέσεις[89].

3.7 Μειονεκτήματα της χρήσης Blockchain

Παρόλα τα πλεονεκτήματα που προσφέρει η τεχνολογία Blockchain και αναλύθηκαν στην προηγούμενη υποενότητα, έχει να αντιμετωπίσει και ορισμένα εμπόδια-μειονεκτήματα.

Ενέργεια

Το κύριο μειονέκτημα του Blockchain είναι η υψηλή κατανάλωση ενέργειας που το χαρακτηρίζει και απαιτείται για τη διατήρηση του καθολικού (ledger) σε πραγματικό χρόνο[35]. Κάθε νέος κόμβος που δημιουργείται επικοινωνεί με τους υπόλοιπους για να εξασφαλιστεί η διαφάνεια, ενώ οι miners του δικτύου προσφέρουν λύσεις με σκοπό την επικύρωση της συναλλαγής. Αυτό έχει ως αποτέλεσμα την κατανάλωση τεράστιας ποσότητας υπολογιστικής ισχύς, ρεύματος και χρόνου, καθώς για κάθε κόμβο εξασφαλίζεται ανοχή σφάλματος, αποτροπή διακοπής της λειτουργίας του και η αξιοπιστία των δεδομένων που περιέχει. Ένας άλλος σημαντικός παράγοντας όσον αφορά την μεγάλη κατανάλωση ενέργειας είναι και η επαλήθευση της υπογραφής κατά την συναλλαγή, με δεδομένο ότι πρέπει να κρυπτογραφηθεί.

Κόστος

Το Blockchain χαρακτηρίζεται επίσης από το μεγάλο κόστος που επιφέρει. Σύμφωνα με το [36] υπολογίζεται ότι κατά μέσο όρο απαιτούνται 75 έως 160 δολάρια για κάθε συναλλαγή, όπου το μεγαλύτερο μέρος από τα αυτά καλύπτεται από την κατανάλωση ενέργειας. Ένα άλλο μειονέκτημα είναι η ισορροπία ανάμεσα στη ποσότητα των κόμβων και στο ευνοϊκό κόστος για τους χρήστες. Στην πιθανή περίπτωση που κάποιοι κόμβοι δεν λειτουργούν εντατικά στο blockchain, το κόστος αυξάνεται ανάλογα με τις ανταμοιβές που λαμβάνουν οι κόμβοι αλλά παράλληλα αυτό έχει ως

αποτέλεσμα την καθυστέρηση της ολοκλήρωσης κάποιων συναλλαγών. Όταν τα νέα blocks συνδέονται με την αλυσίδα και οι υπολογιστικές απαιτήσεις αυξάνονται το blockchain αναπτύσσεται. Ωστόσο, κάποιοι κόμβοι δεν παρέχουν την απαραίτητη χωρητικότητα και παρουσιάζονται τα εξής προβλήματα: Πρώτον το μικρότερο καθολικό λόγω της αδυναμίας των κόμβων να αποθηκεύσουν το πλήρες αντίγραφο του blockchain και έτσι παραβιάζεται η διαφάνεια αλλά και η αποκεντροποίηση του συστήματος.

Αμεταβλητότητα των Δεδομένων

Μόλις τα δεδομένα καταγραφούν σε μια αλυσίδα μπλοκ, δεν μπορούν να τροποποιηθούν ή να διαγραφούν. Αυτό μπορεί να είναι προβληματικό για τη διόρθωση σφαλμάτων, τη συμμόρφωση με τους νόμους περί προστασίας δεδομένων (όπως το «δικαίωμα στη λήθη» του GDPR) ή τη διαχείριση ευαίσθητων πληροφοριών.

Χωρητικότητα

Η συνεχής προσθήκη δεδομένων στο blockchain συνεπάγεται και με την ανάλογη αύξηση του μεγέθους του καθολικού. Έτσι, μεμονωμένοι κόμβοι δεν μπορούν να ανταποκριθούν στις παραπάνω απαιτήσεις με αποτέλεσμα να μειώνεται ο παράγοντας της αποκέντρωσης που χαρακτηρίζει το σύστημα.

Ευπάθεια σε επιθέσεις

Παρά τη γενική ασφάλεια που χαρακτηρίζει το blockchain, η τεχνολογία δεν έχει ανοσία σε πιθανές εξωτερικές επιθέσεις, όπως επιθέσεις 51%, όπου μια ομάδα από miners ελέγχει περισσότερο από το μισό της ισχύος εξόρυξης του δικτύου, σφάλματα έξυπνων συμβολαίων και επιθέσεις που στοχεύουν διαπιστευτήρια των χρηστών.

3.8 Πλατφόρμες του Blockchain

Η τεχνολογία Blockchain αποτελεί μια από τις σημαντικότερες καινοτομίες του 21ου αιώνα, παρέχοντας στον χρήστη ένα ασφαλές και αποκεντρωμένο περιβάλλον καταγραφής συναλλαγών. Κάθε πλατφόρμα του Blockchain διαθέτει ξεχωριστά χαρακτηριστικά, τα οποία την καθιστούν κατάλληλη για διαφόρους τύπους εφαρμογών. Σε αυτή την υποενότητα παρουσιάζονται κάποιες από τις πιο διαδεδομένες πλατφόρμες ανάπτυξης του Blockchain.

3.8.1 Tezos

Το Tezos παρουσιάστηκε για πρώτη φορά το 2014. Αναπτύχθηκε με σκοπό να βελτιώσει διάφορες πτυχές από τις άλλες περισσότερο διαδεδομένες πλατφόρμες. Μπορεί να χρησιμοποιηθεί ως μια αποκεντρωμένη πλατφόρμα έξυπνων συμβολαίων[91], η οποία σκοπεύει στην βελτίωση της ασφάλειας του συστήματος. Η ιδιαιτερότητα αυτής της πλατφόρμας Blockchain είναι η ικανότητα της να τροποποιεί τον αλγόριθμο συναίνεσης της. Αυτό επιτυγχάνεται με τη χρήση ενός μηχανισμού ψηφοφορίας. Αφού γίνει η λήψη του νέου πρωτοκόλλου από το δίκτυο, αυτό εκτελείται και αντικαθιστά το υπάρχον πρωτόκολλο. Σε αντίθεση με τα άλλα blockchains της εποχής, το Tezos δεν είναι βασισμένο στον αλγόριθμο PoW, αλλά σε ένα αλγόριθμο βασισμένο στο PoS, το Liquid PoS[98]. Συνδυάζει τις δυνατότητες από μια πληθώρα προγραμματιστικών γλωσσών έτσι ώστε να εξασφαλίσει την ορθότητα της υλοποίησης του πρωτοκόλλου και παράλληλα να περιορίσει πιθανά σφάλματα και επιθέσεις.

3.8.2 Ethereum

Το Ethereum δημιουργήθηκε από τον Vitalik Buterinto 2015 με σκοπό να αποτελέσει μια πρωτοποριακή πλατφόρμα για την εκτέλεση smart contracts και αποκεντρωμένων εφαρμογών. Τα έξυπνα συμβόλαια αποτελούν ουσιαστικά εκτελέσιμα προγράμματα που λειτουργούν στο blockchain και επιτυγχάνουν την αυτοματοποίηση των συναλλαγών χωρίς την επίβλεψη μεσαζόντων. Εκτελούνται μέσω του μηχανισμού της πλατφόρμας Ethereum Virtual Machine. Με την αναβάθμιση στην έκδοση Ethereum 2.0, έγινε μετάβαση στον αλγόριθμο PoS, με σκοπό την μείωση της κατανάλωσης ενέργειας κατά 99,95% [84], αλλά και την αύξηση της αποδοτικότητας και της επεκτασιμότητας του δικτύου. Τέλος, το Ethereum υποστηρίζει την έκδοση και διαχείριση διακριτικών (tokens) μέσω του προτύπου ERC-20, το οποίο έχει γίνει το πρότυπο για τη δημιουργία νέων κρυπτονομισμάτων και tokens σε πλατφόρμες crowdfunding όπως τα Initial Coin Offerings (ICOs). Αυτό έχει ανοίξει τον δρόμο για μια πληθώρα νέων έργων και startups που βασίζονται στην τεχνολογία του Ethereum. Η πλατφόρμα συνεχώς αναβαθμίζεται και εξελίσσεται, με το σχέδιο ανάπτυξης να περιλαμβάνει βελτιώσεις όπως η μείωση του κόστους συναλλαγών, η αύξηση της ασφάλειας και η βελτίωση της εμπειρίας χρήστη [97].

3.8.3 Hyperledger Fabric

Η πλατφόρμα Hyperledger Fabric αναπτύχθηκε το 2015 και είναι ένα πλαίσιο Blockchain ανοιχτού κώδικα που είναι υπό την αιγίδα του Linux. Ο σκοπός της

χρήσης του είναι κυρίως εταιρικός και συγκεκριμένα η συνεργασία blockchain εργασιών μεταξύ διάφορων εταιριών για επαγγελματικές ανάγκες τους. Είναι η πρώτη πλατφόρμα που υποστηρίζει γλώσσες προγραμματισμού γενικής χρήσεως όπως Java και Node.js [92]. Λόγω της φύσης της πλατφόρμα, οι συμμετέχοντες γνωρίζουν τις ταυτότητες των άλλων χρηστών και έτσι δεν υπάρχει συνολική ανωνυμία μεταξύ τους. Το πρωτόκολλο λόγω των χαρακτηριστικών του είναι ιδανικό για ιδιωτικά blockchains με σκοπό την ενίσχυση της ταχύτητας και της ασφάλειας τους, καθώς οι επιχειρήσεις δεν ενδείκνυται να χρησιμοποιούν δημόσιες πλατφόρμες. Προσφέρει επίσης την ασφάλεια των δεδομένων μέσω της απομόνωσης των συναλλαγών σε κανάλια[93].

Κεφάλαιο 4: ΣΥΣΤΗΜΑΤΑ ΦΗΜΗΣ

Με την ραγδαία ανάπτυξη της τεχνολογίας, ο κόσμος γίνεται ολοένα και πιο διασυνδεδεμένος. Για αυτό το λόγο προκύπτει πλέον η ανάγκη για ύπαρξη φήμης καθώς ο αριθμός των χρηστών και των υπηρεσιών που αλληλεπιδρούν μέσω διαδικτύου αυξάνεται συνεχώς. Η φήμη είναι ένα εργαλείο με το οποίο διευκολύνεται η σύναψη εμπιστοσύνης μεταξύ οντοτήτων και αυξάνεται η αποδοτικότητα και η αποτελεσματικότητα των υπηρεσιών που χρησιμοποιούν. Εφόσον οι οντότητες αυτές δεν μπορούν να έχουν προηγούμενες άμεσες αλληλεπιδράσεις, βασίζονται στην ύπαρξη των συστημάτων διαδικτυακής φήμης. Μέσω αυτών των συστημάτων και των υπηρεσιών τους, έχουν την δυνατότητα να προβλέψουν ποιες θα είναι οι αξιόπιστες οντότητες βάσει των μηχανισμών ανατροφοδότησης των προηγούμενων αλληλεπιδράσεων που έχουν πραγματοποιήσει.

4.1 Η σημασία των συστημάτων φήμης

Τα τελευταία χρόνια, τα διαδικτυακά συστήματα φήμης συνεχώς εξελίσσονται σε μια προσπάθεια τους να μιμηθούν τα αντίστοιχα του πραγματικού κόσμου. Η αξιολόγηση στο πλαίσιο μιας διαδικτυακής κοινότητας μπορεί να πραγματοποιηθεί με πολλές μορφές και μεθόδους, όπως με τη χρήση αριθμών βαθμολόγησης, αστεριών και κλιμάκων. Οι υποκείμενες μέθοδοι ποικίλουν ανάλογα με τις πηγές πληροφοριών της κοινότητας και την αντίληψη που υπάρχει σε αυτής όσον αφορά την έννοια της φήμης. Η φήμη χρησιμοποιείται ως μια προσέγγιση επίτευξης εμπιστοσύνης μεταξύ των άγνωστων μελών μιας (διαδικτυακής) κοινότητας[56]. Τα διαδικτυακά συστήματα φήμης εξαρτώνται κυρίως από την πρόθυμη συνεργασία των χρηστών τους και τον διαμοιρασμό γνώσεων και απόψεων μεταξύ τους. Στην περίπτωση που οι χρήστες κοινοποιούν λιγότερες πληροφορίες από αυτές που είναι απαραίτητες, το επίπεδο της φήμης θα έχει ασήμαντο νόημα και δεν θα είναι έμπιστο, λόγω της έλλειψης πληροφοριών για την επίτευξη ουσιαστικής και αξιόπιστης εμπιστοσύνης μεταξύ των χρηστών. Για το λόγο αυτό, τα συστήματα φήμης σε αρκετές περιπτώσεις προσφέρουν κάποιου είδους ανταμοιβή έτσι ώστε να ωθήσουν τους χρήστες να συνεργαστούν. Τα συστήματα σχεδιάστηκαν ως κλειστοί τομείς, όπου το κάθε ένα έχει την δικιά του εισαγωγή δεδομένων, αναζήτηση, τρόπο αναπαράστασης και αλληλεπίδρασης με το χρήστη, υπολογισμό τιμών της φήμης. Ο υποκείμενος στόχος για όλα τα συστήματα φήμης όμως είναι η πρόβλεψη των μελλοντικών ενεργειών των μελών της κοινότητας, λαμβάνοντας υπόψη την γνώση όσον αφορά της προηγούμενη συμπεριφορά τους[57]. Η γνώση αυτή συλλέγεται ιδανικά αυτοπροσώπως μέσω συναλλαγών. Ωστόσο η αλληλεπίδραση με κάθε ξεχωριστό μέλος της διαδικτυακής κοινότητας επιφέρει μεγάλο κόστος και κινδύνους, καθώς υπάρχει η περίπτωση των κακόβουλων χρηστών. Για να περιοριστεί το κόστος και να εντοπιστεί

αποτελεσματικά πιθανή κακόβουλη δραστηριότητα, οι χρήστες κοινοποιούν τις πληροφορίες και τις γνώσεις τους μέσω του συστήματος φήμης με τη μορφή συστάσεων. Η χρήση τους γίνεται από διαφόρων ειδών εφαρμογές και η διαδικασία αξιολόγησης της αξιοπιστίας των παρεχόμενων πληροφοριών φήμης είναι ιδιαίτερα σημαντική καθώς με την επέκταση της τεχνολογίας η εκμετάλλευση πόρων και η λήψη επιχειρηματικών αποφάσεων εξαρτώνται από το επίπεδο της εμπιστοσύνης.

4.2 Οντότητες στα Συστήματα Φήμης

Τα βασικά στοιχεία- οντότητες ενός συστήματος που βασίζεται στη φήμη είναι τα εξής[62]:

Trustee: μια οντότητα που λαμβάνει μια τιμή φήμης με βάσης τις ενέργειές του στο πλαίσιο του συστήματος. Η τιμή αυτή μπορεί να προκύψει από το αποτέλεσμα των πιθανών συναλλαγών που πραγματοποιεί η συγκεκριμένη οντότητα ή από τα χαρακτηριστικά της.

Trustor: είναι μια ομότιμη οντότητα που αξιολογεί τις ενέργειες της οντότητας trustee, και σύμφωνα με αυτήν της αξιολόγηση αποφασίζει αν θα αλληλεπιδράσει με αυτή.

Μεσάζοντας: προσφέρει πληροφορίες και προτάσεις που αφορούν την οντότητα trustee με κριτήριο την αλληλεπίδραση τους.

Πλαίσιο Πληροφοριών: είναι πληροφορίες που επηρεάζουν την φήμη ενός μέλους του συστήματος.

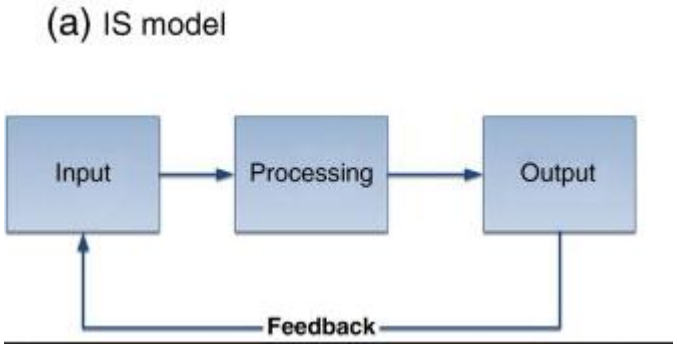
Συστάσεις: αναφέρεται στην ανατροφοδότηση που προσφέρουν τα μέλη της κοινότητας και υποδεικνύει κατά πόσο ένα μέλος είναι έμπιστο.

Φήμη: είναι ένας δείκτης για να προσδιοριστεί η ποιότητα των υπηρεσιών και των χαρακτηριστικών του trustee που βασίζεται στις συστάσεις από τους χρήστες του συστήματος.

4.3 Η δομή ενός συστήματος φήμης

Στον τομέα των πληροφοριακών συστημάτων, η δομή που έχει καθιερωθεί ευρέως όσον αφορά τα συστήματα αποτελείται από τέσσερα βασικά στοιχεία: την είσοδο, την επεξεργασία, την έξοδο και την ανατροφοδότηση, όπως παρουσιάζεται στην Εικόνα 16. Αρχικά, η είσοδος είναι η διαδικασία συλλογής δεδομένων. Η επεξεργασία αναφέρεται στην διαδικασία μετατροπής των δεδομένων που έχουν συλλεχθεί σε πληροφορίες για το σύστημα. Στη συνέχεια, η έξοδος είναι η διαδικασία μετατροπής αυτών των πληροφοριών σε ουσιαστικά αποτελέσματα συγκεκριμένης μορφολογίας.

Τέλος, η ανατροφοδότηση χρησιμοποιείται για να παρέχει πληροφορίες έτσι ώστε να επηρεάσει και εν τέλει να μεταβάλει την είσοδο των δεδομένων ή την διαδικασία της επεξεργασίας.



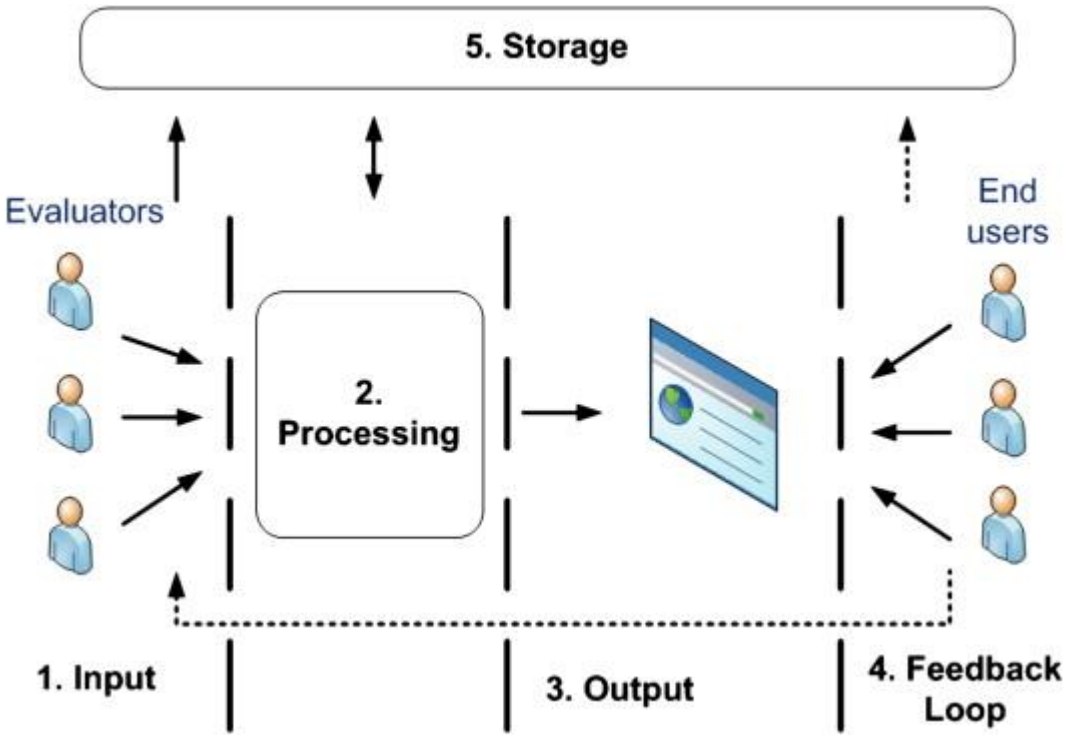
Εικόνα 13 : Η ΔΟΜΗ ΕΝΟΣ ΠΛΗΡΟΦΟΡΙΑΚΟΥ ΣΥΣΤΗΜΑΤΟΣ [78]

Ωστόσο, είναι ευρέως αποδεκτό ότι τα συστήματα φήμης αποτελούν ένα συγκεκριμένο είδος πληροφοριακών συστημάτων. Με βάση τη γενική δομή των πληροφοριακών συστημάτων που παρουσιάζεται παραπάνω, στο [59] προτείνεται μια πιο ολοκληρωμένη δομή για τα διαδικτυακά συστήματα φήμης. Ανεξάρτητα από τη διεπαφή τους, τον ρόλο τους και την λειτουργία τους τα συστήματα φήμης πρέπει να δομούνται από τα εξής στοιχεία:

- **Είσοδος:** είναι η διαδικασία συλλογής πληροφοριών φήμης από διάφορες πηγές.
- **Επεξεργασία:** είναι η διαδικασία υπολογισμού και συγκέντρωσης όλων των πληροφοριών φήμης που προκύπτουν από την είσοδο.
- **Έξοδος:** υποδηλώνει στην διάδοση των πληροφοριών φήμης ανάμεσα στους χρήστες.
- **Βρόχος ανατροφοδότησης:** είναι η συλλογή των κριτικών και της ανατροφοδότησης.
- **Αποθήκευση:** αναφέρεται στην διαδικασία αποθήκευσης όλων των πληροφοριών που έχουν συλλεχτεί και επεξεργαστεί.

Το περιεχόμενο των κριτικών από τους χρήστες έχει ιδιαίτερη σημασία στο πλαίσιο των συστημάτων φήμης[58]. Για να εξετάσουν την ποιότητα κάθε κριτικής, κάποια συστήματα υιοθετούν το στοιχείο του βρόχου ανατροφοδότησης. Αντίθετα με τα άλλα στοιχεία, ο βρόχος ανατροφοδότησης δεν περιέχεται σε όλα τα συστήματα φήμης. Στην Εικόνα 17 παρουσιάζεται η προτεινόμενη δομή και οι αλληλεπιδράσεις ανάμεσα στα στοιχεία ενός συστήματος φήμης. Ως evaluator αναφέρεται η πηγή πληροφοριών φήμης (φυσικό πρόσωπο ή άλλο σύστημα) και ως end user αναφέρεται στις περισσότερες περιπτώσεις οι χρήστες της ιστοσελίδας (συστήματος) οι οποίοι αναζητούν πληροφορίες για μια οντότητα και έχουν την επιλογή να προσφέρουν ανατροφοδότηση στην περίπτωση που το σύστημα τους προσφέρει αυτή την

δυνατότητα. Η διαδικασία ολοκληρώνεται με την αποθήκευση του συνόλου των πληροφοριών.



Εικόνα 14 : Η ΔΟΜΗ ΕΝΟΣ ΣΥΣΤΗΜΑΤΟΣ ΦΗΜΗΣ [79]

4.4 Ταξινόμηση των Συστημάτων Φήμης

Σύμφωνα με το [60], σε αρχικό επίπεδο τα Συστήματα Φήμης διαχωρίζονται σε ρητά και άρρητα. Τα ρητά συστήματα φήμης έχουν σχεδιαστεί έτσι ώστε να διευκολύνουν την εκτίμηση της εμπιστοσύνης μεταξύ των μελών ενός περιβάλλοντος. Κατά κύριο λόγο χρησιμοποιούνται όταν απαιτείται η συχνή αλληλεπίδραση ανάμεσα σε ένα μεγάλο σύνολο μελών. Ο άρρητος μηχανισμός φήμης χαρακτηρίζει συστήματα τα οποία δεν έχουν ορίσει ένα συγκεκριμένο σύστημα φήμης, παρόλα αυτά όμως τα μέλη του χρησιμοποιούν πληροφορίες φήμης έτσι ώστε να λάβουν αποφάσεις για μια οντότητα. Πρόσφατα παραδείγματα άρρητων τέτοιων συστημάτων αποτελούν τα μέσα κοινωνικής δικτύωσης όπως το Facebook και το LinkedIn, στα οποία οι οντότητες μπορούν να εξασφαλίσουν ένα επίπεδο εμπιστοσύνης με τη χρήση πληροφοριών που προέρχονται από ένα δίκτυο επαφών. Ένα άλλο παράδειγμα τέτοιου συστήματος είναι η μηχανή αναζήτησης της Google, στην οποία η σειρά που εμφανίζονται οι ιστοσελίδες συνδέεται άμεσα με την φήμη τους.

4.4.1 Βασικά Χαρακτηριστικά των Συστημάτων Φήμης

Στο δεύτερο επίπεδο της ταξινόμησης των συστημάτων Φήμης προσδιορίζονται οι βασικές διαστάσεις τους, δηλαδή τα χαρακτηριστικά τους.

4.4.1.1 Ιστορικό Χρήστη

Οι συναλλαγές μεταξύ δύο οντοτήτων-χρηστών καταγράφονται. Κατά τη διαδικασία αυτή, κάθε οντότητα έχει τη δυνατότητα να προσφέρει ανατροφοδότηση σχετικά με τη συναλλαγή, αλλά και τις υποχρεώσεις και την επίδοση των συμμετεχόντων σε αυτή. Το σύνολο των αποθηκευμένων πληροφοριών που προκύπτουν από τις αλληλεπιδράσεις μεταξύ των χρηστών και τα αποτελέσματα τους ονομάζεται Ιστορικό του Χρήστη. Χρησιμοποιείται (συχνά με τη μορφή βαθμολόγησης) έτσι ώστε και προσδιορίσει τα πιθανά αποτελέσματα τωρινών αλλά και μελλοντικών συναλλαγών και κατέχει σημαντικό ρόλο στην υλοποίηση της έννοιας της φήμης. Υπάρχουν δύο επεκτάσεις του ιστορικού. Το προσωπικό και το γενικό. Τα προσωπικό ιστορικό προκύπτει από τη συλλογή και τη χρήση πληροφοριών και σχηματίζει την άποψη του χρήστη ως προς τις υπόλοιπες οντότητες. Η υποκειμενική φύση του έχει ως αποτέλεσμα το σχηματισμό διαφορετικών απόψεων μεταξύ των χρηστών.

4.4.1.2 Συμφραζόμενα- Γενικό πλαίσιο Πληροφοριών

Η ύπαρξη ενός γενικού πλαισίου πληροφοριών για τα δεδομένα προσφέρει στο χρήστη τις απαραίτητες λεπτομέρειες σχετικά με τον τρόπο που πραγματοποιούνται οι αλληλεπιδράσεις μεταξύ των οντοτήτων στο σύστημα φήμης. Η πλειονότητα των συστημάτων φήμης μπορεί να ταξινομηθεί ότι λειτουργεί σε ενιαίο πλαίσιο, καθώς ο αριθμός των συστημάτων που λαμβάνουν πληροφορίες από διαφορετικούς τομείς είναι σχετικά μικρός. Οι πληροφορίες φήμης παράγονται μέσω της εκτέλεσης συναλλαγών, κάθε μια από τις οποίες χαρακτηρίζεται από ένα σημαντικό όγκο συμφραζόμενων πληροφοριών. Τα συστήματα φήμης μπορούν να κατηγοριοποιηθούν με βάση τις πηγές που λαμβάνουν τις πληροφορίες είτε σε ενιαία (στην περίπτωση που μια μοναδική πηγή πληροφοριών διατηρείται στο σύστημα), είτε σε πολλαπλά (στην περίπτωση που υπάρχουν παραπάνω από μια πηγές στο σύστημα).

4.4.1.3 Συλλογή Πληροφοριών

Σε ένα σύστημα φήμης, για να καθιερωθεί εμπιστοσύνη ανάμεσα σε δύο οντότητες, πρέπει να καταγραφούν πληροφορίες σχετικές με τη συμπεριφορά τους. Οι τρόποι-

τεχνικές που έχουν αναπτυχθεί για να επιτευχθεί ο παραπάνω στόχος του συστήματος είναι οι εξής:

- **Ευθύς:** οι πληροφορίες παράγονται είτε με κριτήριο τις προσωπικές αλληλεπιδράσεις μιας οντότητας, είτε μέσω της παρατήρησης άλλων αλληλεπιδράσεων. Αυτή η τεχνική αποτελεί της πιο αξιόπιστη μέθοδο συλλογής πληροφοριών όσον αφορά τα συστήματα φήμης[61].
- **Έμμεσος:** οι πληροφορίες συλλέγονται από τα μέλη μιας διαδικτυακής κοινότητας σύμφωνα με τις εμπειρίες τους, ή τους έχουν μεταφερθεί από τρίτους. Λόγω της αβεβαιότητας που περικλείει αυτήν την τεχνική συλλογής πληροφοριών, η χρήση του από το σύστημα είναι εξαιρετικά πολύπλοκη.
- **Συμπληρωματικός:** η πηγή πληροφοριών μπορεί να μην έχει σχεδιαστεί απαραίτητα ώστε να λειτουργεί στο πλαίσιο της φήμης.

4.4.1.4 Σχηματισμός φήμης

Περιγράφει τον τρόπο υπολογισμού της φήμης μια οντότητας, αλλά και την τιμή της. Ο απλούστερος τρόπος σχηματισμού φήμης είναι η πρόσθεση των θετικών και αρνητικών κριτικών για αυτή την οντότητα. Με τη διαδικασία αυτή υπολογίζεται η φήμη για όλες τις οντότητες του συστήματος και στη συνέχεια κατατάσσονται σύμφωνα με το αποτέλεσμα .

4.5 Ζητήματα στον σχεδιασμό Συστημάτων Φήμης

Στην διαδικασία του σχεδιασμού των Peer-to-Peer (P2P) Συστημάτων Φήμης υπάρχουν κάποια σημαντικά ζητήματα που πρέπει να ληφθούν υπόψη[65], τα οποία είναι τα εξής:

- Το σύστημα πρέπει να είναι αυτόνομο. Λόγω της απουσίας κεντρικής αρχής στο πλαίσιο του συστήματος φήμης, οι ίδιοι οι χρήστες προσδιορίζουν και στη συνέχεια επιβάλλουν την κοινή ηθική και δεοντολογία τους.
- Το σύστημα χρειάζεται να διατηρεί την ανωνυμία των χρηστών, των οποίων η φήμη σχετίζεται με ένα αδιαφανές αναγνωριστικό και όχι με μια εξωτερική ταυτότητα όπως η διεύθυνση IP.

- Η διαδικασία απόκτησης φήμης πρέπει να συνδυάζεται με σταθερά καλή συμπεριφορά κατά τη διάρκεια πραγματοποίησης συναλλαγών. Για αυτό το λόγο το σύστημα δεν επιβραβεύει τους νέους χρήστες και έτσι αποτρέπει τους κακόβουλους χρήστες από το να δημιουργούν κατά εξακολούθηση νέα αναγνωριστικά και να αποκτούν τα προνόμια που συνοδεύονται με αυτά.

- Το σύστημα πρέπει να έχει ως στόχο τη λειτουργία τους με το μικρότερο δυνατό κόστος σε θέματα υπολογιστικής ισχύς, υποδομών, αποθηκευτικού χώρου και πολυπλοκότητας των μηνυμάτων.

- Για λόγους ασφαλείας, το σύστημα πρέπει να είναι ανθεκτικό στην αντιμετώπιση κακόβουλης δραστηριότητας ομάδων χρηστών και στην προσπάθεια τους να συνεργαστούν έτσι ώστε να ανατρέψουν το σύστημα.

4.6 Παραδείγματα Συστημάτων Φήμης

4.6.1 Ο αλγόριθμος EigenTrust

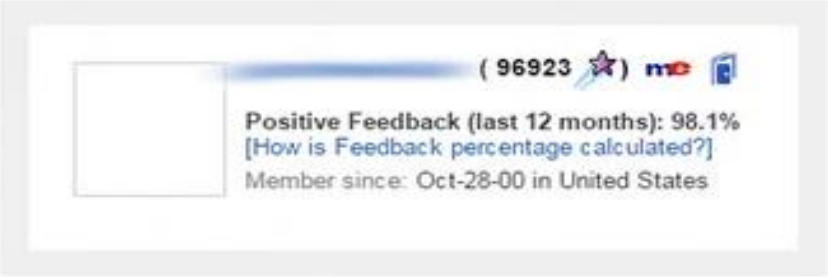
Το [65] παρουσιάζει ένα Peer-to-Peer πλαίσιο φήμης, το οποίο είναι πλήρως αποκεντρωμένο και επιτρέπει στα μέλη του δικτύου να αποφασίσουν ποια από τα υπόλοιπα μέλη θα εμπιστευθούν όσον αφορά την λήψη αρχείων. Ο αλγόριθμος αυτός ονομάστηκε **EigenTrust**. Ο κάθε χρήστης του συστήματος κατέχει ένα προσωπικό ιστορικό για κάθε άλλο μέλος που έχει αλληλεπιδράσει και αποτελείται από το σύνολο των θετικών και αρνητικών κριτικών που έχει προσκομίσει. Οι τιμές εμπιστοσύνης που προκύπτουν για τον κάθε χρήστη είναι μεταξύ του 0 και του 1.

4.6.1.1 Πλεονεκτήματα και Μειονεκτήματα του EigenTrust

Ο αλγόριθμος EigenTrust χαρακτηρίζεται από πολλά γνωστά πλεονεκτήματα, κάποια από τα οποία είναι η απλότητα του, η αποδοτικότητα αλλά και η επεκτασιμότητα του[63] ως ένα μέσο άμεσης εδραίωσης εμπιστοσύνης ανάμεσα στους χρήστες, ειδικά σχεδιασμένο για P2P συστήματα. Το βασικό του μειονέκτημα όμως είναι η υψηλή κατάταξη που αναθέτει σε προ-εγγεκριμένους χρήστες που ενδέχεται να δημιουργήσει κάποια προβλήματα όπως μείωση της αξιοπιστίας του συστήματος ή χαμηλότερη κατάταξη έμπιστων χρηστών που κατέχουν αυθεντικά αρχεία. Στο [66] υποδεικνύεται ότι ο αλγόριθμος είναι λιγότερο αποτελεσματικός σε περιπτώσεις αναξιόπιστων χρηστών που συμπεριφέρονται διαφορετικά από συναλλαγή σε συναλλαγή. Για να αντιμετωπιστεί η πραγματοποίηση μη αυθεντικών λήψεων, αναπτύχθηκε μια πιθανολογική προσέγγιση του EigenTrust που υπολογίζει την αναξιόπιστη συμπεριφορά στο σύστημα και εξαλείφει την ανάγκη για ύπαρξη προ-εγγεκριμένων χρηστών.

4.6.2 EBay

Το eBay αποτελεί παράδειγμα ενός διαδικτυακού συστήματος φήμης και είναι μια από τις μεγαλύτερες διαδικτυακές αγορές παγκοσμίως[61]. Η κοινότητα αυτή αριθμεί πάνω από 50 εκατομμύρια εγγεγραμμένους χρήστες. Το eBay επιτρέπει στους χρήστες του (πωλητές και αγοραστές) την ανταλλαγή προϊόντων μέσω της διαδικασίας δημοπρασίας. Με την ολοκλήρωση της συναλλαγής, οι συμμετέχοντες βαθμολογούν την εμπειρία τους και τον χρήστη που αλληλεπίδρασαν. Με αυτό τον τρόπο, πιθανοί μελλοντικοί ενδιαφερόμενοι έχουν την δυνατότητα να εξετάσουν το βαθμό αξιοπιστίας ενός χρήστη με βάση τις προηγούμενες συναλλαγές που έχει πραγματοποιήσει. Το σύστημα φήμης χρησιμοποιεί διάφορα μέσα ανατροφοδότησης. Αρχικά ο χρήστης μπορεί να βαθμολογήσει την συναλλαγή με τρείς τρόπους: θετική (+1), ουδέτερη (0) ή αρνητική (-1). Στην συνέχεια προσδίδει μια σειρά από αριθμητικές αξιολογήσεις για διάφορες πτυχές της συναλλαγής όπως ακρίβεια του προϊόντος, επικοινωνία με τον πωλητή και χρόνος παράδοσης. Τέλος, έχει την επιλογή να αξιολογήσει την εμπειρία του με ένα σχόλιο, το οποίο συνήθως προσφέρει πληροφορίες στους χρήστες της κοινότητας για την ποιότητα του προϊόντος, την αποστολή του και οποιαδήποτε προβλήματα προέκυψαν. Στην περίπτωση που ο αγοραστής επιλέξει ένα προϊόν, του παρέχονται πληροφορίες σχετικές με τον πωλητή όπως η διαδικτυακή του ταυτότητα και το σύνολο των κριτικών από προηγούμενες συναλλαγές. Η φήμη του κάθε χρήστη υπολογίζεται από το τελικό άθροισμα θετικών και αρνητικών κριτικών ξεχωριστών χρηστών[67].



Εικόνα 15 : ΠΑΡΑΔΕΙΓΜΑ ΜΗΧΑΝΙΣΜΟΥ ΑΝΑΤΡΟΦΟΔΟΤΗΣΗΣ ΤΟΥ EBAY

4.6.3 Το Πρωτόκολλο XRep

Στο [64] προτείνεται το πρωτόκολλο XRep, το οποίο αποτελεί μια επέκταση της αρχιτεκτονικής Gnutella για τα δίκτυα P2P.

4.6.3.1 Η αρχιτεκτονική Gnutella σε δίκτυα P2P

Το XRep επιτρέπει την δημιουργία και τη διατήρηση της φήμης των πόρων και των κόμβων του δικτύου. Στην περίπτωση των πόρων, χρησιμοποιείται μια απλή δυαδική βαθμολόγηση, ενώ στην περίπτωση των κόμβων καταγράφονται και υπολογίζονται ο αριθμός των επιτυχημένων και αποτυχημένων προσπαθειών των λήψεων. Σε αυτού του είδους τα δίκτυα, οι κόμβοι αναλαμβάνουν τον ρόλο τόσο του διακομιστή, όσο και του πελάτη. Για να προσδιοριστεί αυτή η διπλή ευθύνη των κόμβων στο δίκτυο, χρησιμοποιείται ο όρος υπηρέτης (servent), που λειτουργεί ως διακομιστής. Σε άλλες περιπτώσεις λειτουργεί ως πελάτης, υποβάλει κάποιο αίτημα και ανακτά πόρους από άλλους υπηρέτες κόμβους. Η διαδικασία ανταλλαγής αρχείων σε ένα P2P δίκτυο αποτελείται από δύο κύριες φάσεις: την αναζήτηση και την λήψη του αρχείου. Στην πρώτη φάση ο υπηρέτης κόμβος εκδίδει ένα μήνυμα Query προς όλους τους κόμβους με τους οποίους συνδέεται άμεσα. Οι υπόλοιποι κόμβοι αναγνωρίζουν το ζητούμενο αρχείο εφόσον είναι στην κατοχή τους και μεταδίδουν ένα μήνυμα QueryHit προς τον κόμβο που προήλθε το αρχικό αίτημα. Συνοπτικά, κάθε κόμβος Gnutella λειτουργεί ως δρομολογητής για αιτήματα κατά μήκος ενός δικτύου P2P.

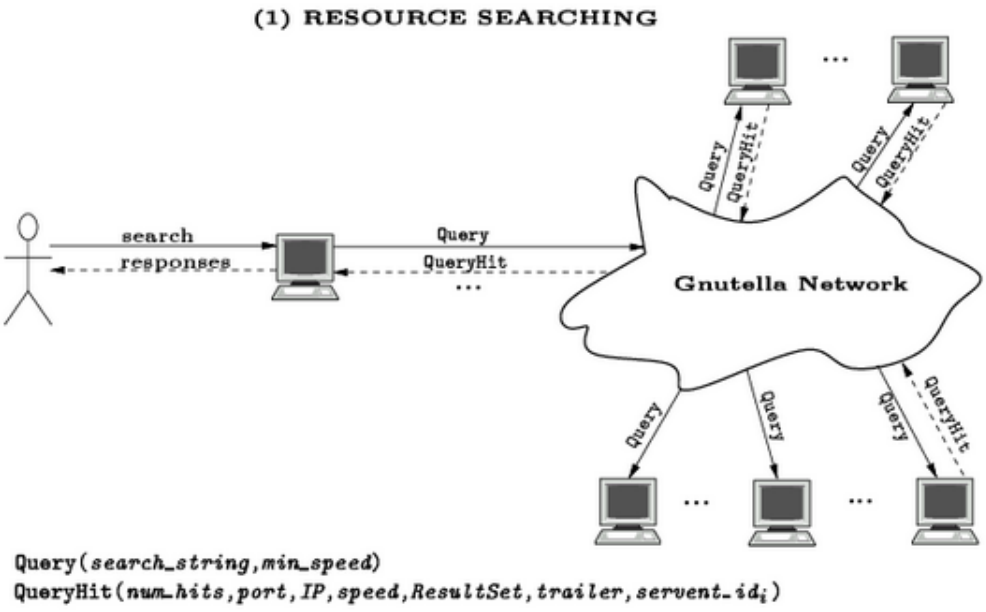
4.6.3.2 Η προσέγγιση του πρωτοκόλλου XRep

Η προσέγγιση του πρωτοκόλλου XRep προσφέρει στα δίκτυα που χρησιμοποιούν την αρχιτεκτονική Gnutella την δυνατότητα ανάθεσης, κοινοποίησης και συνδυασμού της φήμης ανάμεσα στους υπηρέτες κόμβους και τους πόρους τους. Έτσι ο κόμβος p, ο οποίος εκδίδει το αρχικό αίτημα μέσω μηνύματος Query, έχει την δυνατότητα κατά τη διαδικασία επιλογής να αιτείται από το δίκτυο τις γνώμες (ψήφους βαθμολόγησης) των άλλων χρηστών σχετικά με τους πόρους αλλά και τους χρήστες που τους προσφέρουν. Η βασική ιδέα σε αυτή τη προσέγγιση είναι ότι ο κάθε υπηρέτης κόμβος κατέχει πληροφορίες από τις δικές του εμπειρίες και έχει την δυνατότητα να κοινοποιήσει αυτές τις εμπειρίες κατόπιν αιτήματος.

4.6.3.3 Οι φάσεις του πρωτοκόλλου XRep

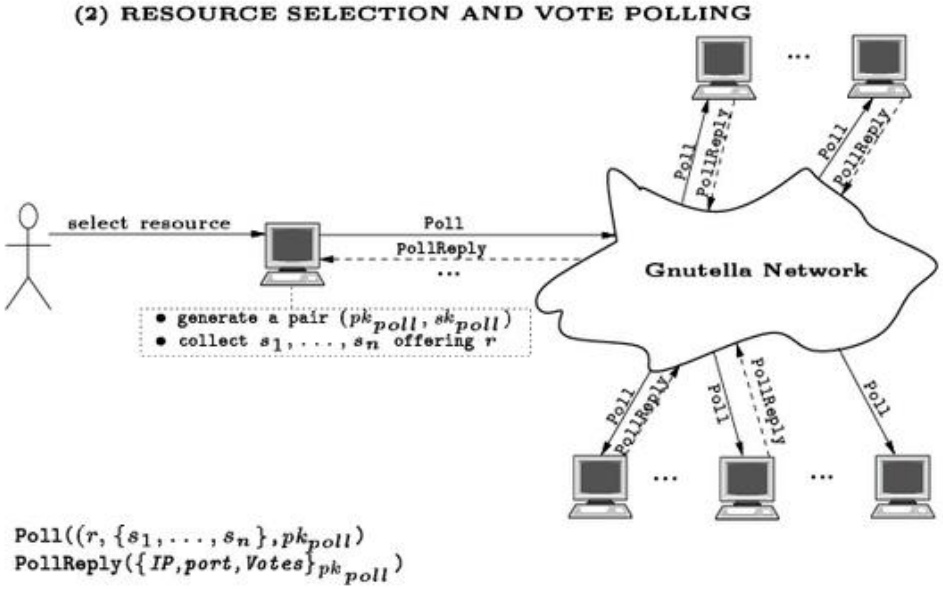
Το πρωτόκολλο XRep αποτελείται από τις εξής πέντε φάσεις:

Αναζήτηση Πόρων: Ο ενδιαφερόμενος μεταδίδει προς τους γειτονικούς του κόμβους ένα μήνυμα Query, το οποίο περιέχει τις χαρακτηριστικές λέξεις κλειδιά. Στην περίπτωση που ένας κόμβος servent αντιστοιχίσει το περιεχόμενο, απαντάει με ένα νέο μήνυμα QueryHit προσφέροντας πληροφορίες όπως τον αριθμό των αρχείων (num_hits), τα ονόματα των αρχείων και σχετικές πληροφορίες με αυτά (ResultSet), την ταυτότητα του (servent_id) και πληροφορίες έτσι ώστε να πραγματοποιηθεί η λήψη των αρχείων.



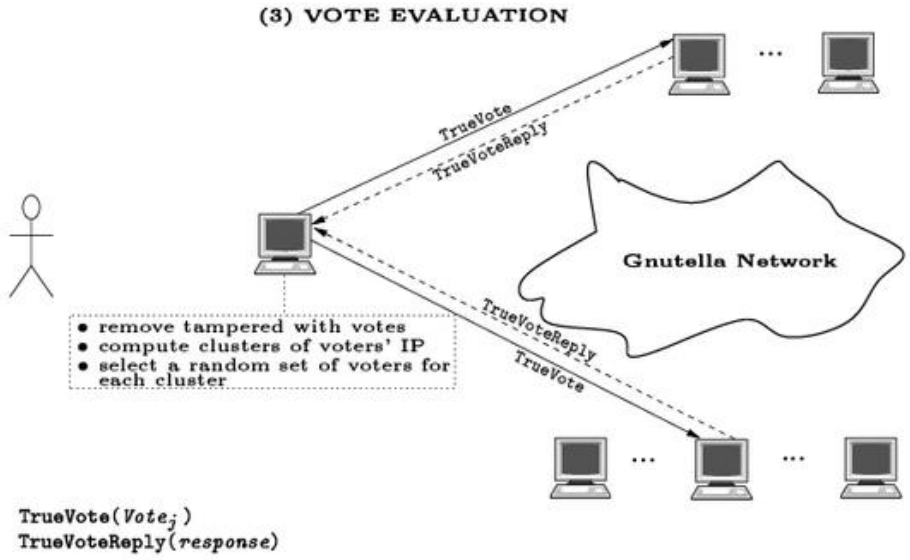
Εικόνα 16 : ΦΑΣΗ 1: ΑΝΑΖΗΤΗΣΗ ΠΟΡΩΝ [64]

Επιλογή Πόρων και Δημοσκόπηση Ψήφων: Εφόσον λάβει τα μηνύματα Queryhits, ο ενδιαφερόμενος καλείται να επιλέξει ανάμεσα στους πιθανούς πόρους που προσφέρονται. Επιπλέον, το πρωτόκολλο XRep του παρέχει τη δυνατότητα να ζητήσει πληροφορίες από τα άλλα μέλη σχετικά με τους πόρους που πρόκειται να λάβει αλλά και την προέλευση τους, δηλαδή τον κόμβο servent. Αυτή η δυνατότητα πραγματοποιείται με την αποστολή αιτήματος στο δίκτυο Gnutella. Η ακεραιότητα και το απόρρητο αυτής την δημοσκόπησης εξασφαλίζεται με τη χρήση ενός δημόσιου κλειδιού (PK_{poll}), το οποίο γνωρίζει μόνο ο ενδιαφερόμενος. Η διαδικασία ολοκληρώνεται καθώς ο ενδιαφερόμενος λαμβάνει τα αποτελέσματα της δημοσκόπησης με το μήνυμα PollReply, που έχουν τη μορφή ψήφου.



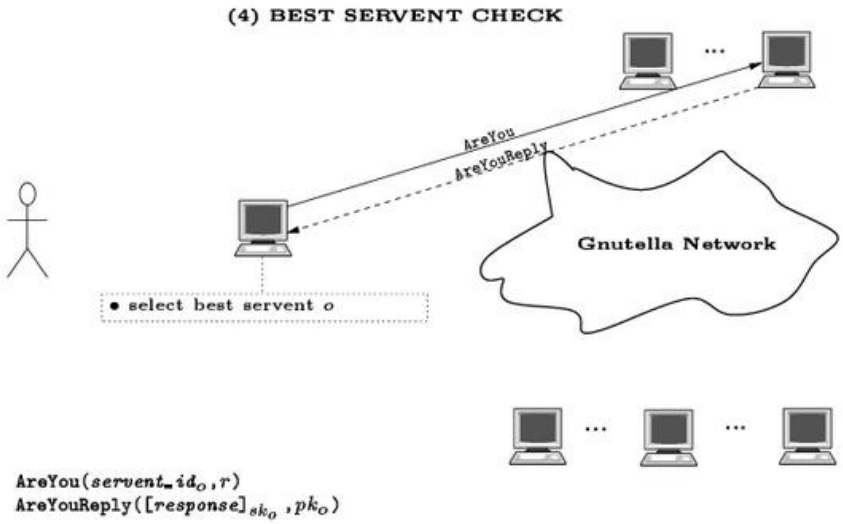
Εικόνα 17 : ΦΑΣΗ 2 : ΕΠΙΛΟΓΗ ΠΟΡΩΝ ΚΑΙ ΔΗΜΟΣΚΟΠΗΣΗ ΨΗΦΩΝ [64]

Αξιολόγηση Ψήφων: Ο ενδιαφερόμενος λαμβάνει τις ψήφους σχετικά με τους πόρους και τους κόμβους servent που εμπλέκονται στη συναλλαγή. Ωστόσο, για να λάβει την απόφαση του, χρειάζεται να αναπτύξει εμπιστοσύνη ως προς την αξιοπιστία αυτών των ψήφων και ενδεχομένως να απορρίψει κάποιες από αυτές. Όταν ολοκληρωθεί η διαδικασία της αξιολόγησης, με τη χρήση αποκρυπτογράφησης έτσι ώστε να εξασφαλιστεί η αξιοπιστία των ψήφων, ο χρήστης εμπιστεύεται το επίπεδο φήμης των πόρων (ή και της προέλευσης τους) και επιλέγει να ολοκληρώσει την διαδικασία της λήψης αρχείων.



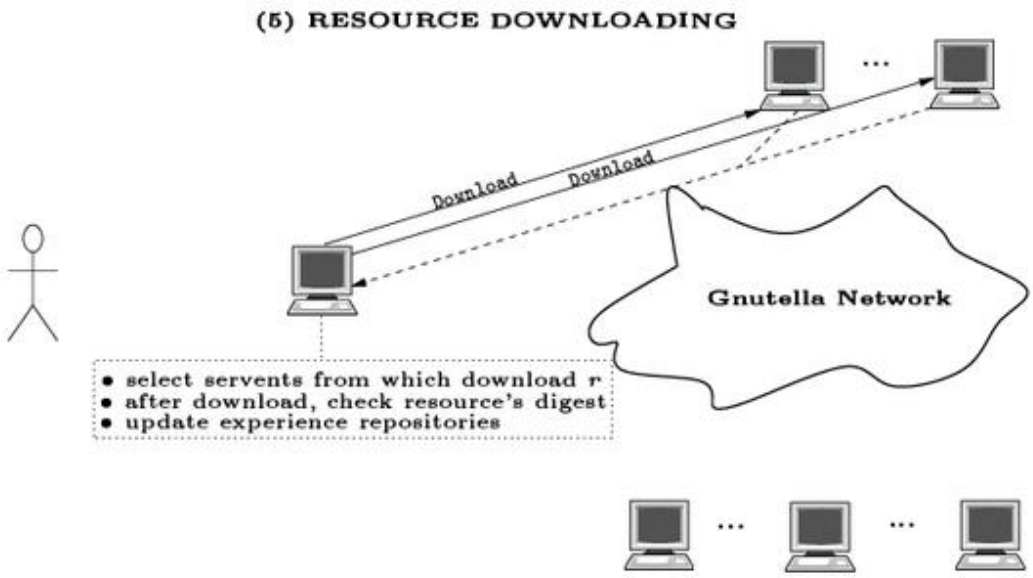
Εικόνα 18 : ΦΑΣΗ 3 : ΑΞΙΟΛΟΓΗΣΗ ΨΗΦΩΝ [64]

Επιλογή Κατάλληλου Κόμβου Servent: Εφόσον ο ενδιαφερόμενος έχει λάβει την απόφαση για τη λήψη των πόρων, πλέον καλείται να επιλέξει τον κατάλληλο προσφέρων κόμβο για να εκτελεστεί η λήψη. Για να αποφευχθούν πιθανοί κίνδυνοι και επιθέσεις, λαμβάνεται υπόψη η αξιοπιστία του κόμβου servent. Ο βασικός τρόπος για να επιτευχθεί το παραπάνω κριτήριο είναι η επιλογή της λήψης πόρων από τον προσφέρων με το καλύτερο επίπεδο φήμης (σύμφωνα με τις ψήφους που έχουν ληφθεί).



Εικόνα 19 : ΦΑΣΗ 4 : ΕΠΙΛΟΓΗ ΚΑΤΑΛΛΗΛΟΥ ΚΟΜΒΟΥ SERVENT [64]

Λήψη Πόρων: Ο ενδιαφερόμενος επικοινωνεί με τον servent και αιτείται τους πόρους. Στην συνέχεια, ελέγχει την ακεραιότητα τους και με τη σειρά του έχει την δυνατότητα να κοινοποιήσει την γνώμη του όσον αφορά τη συναλλαγή που πραγματοποίησε, την ποιότητα των πόρων και την αξιοπιστία του servent.



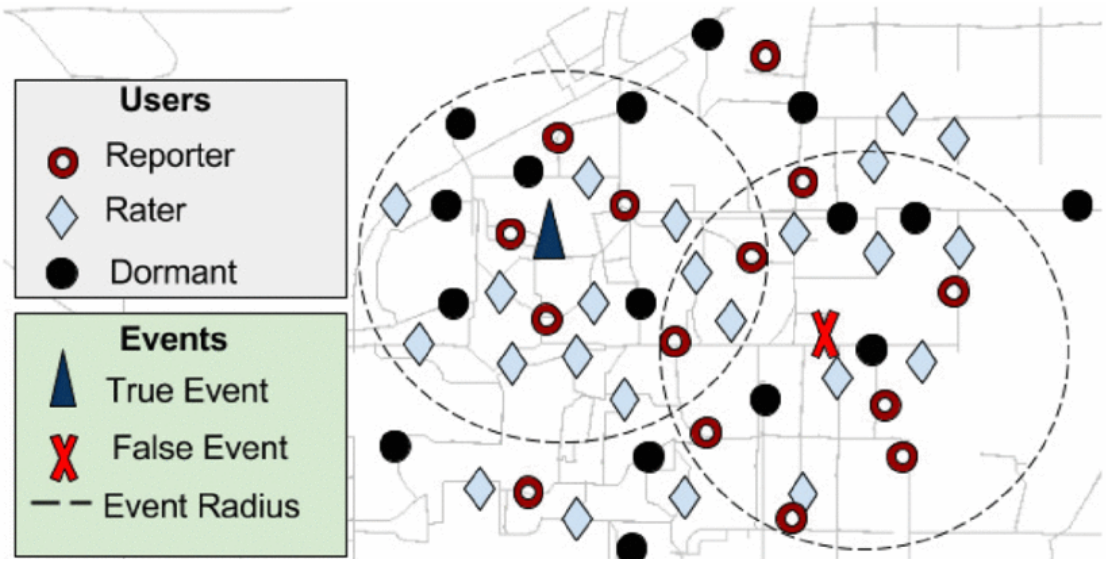
Εικόνα 20 : ΦΑΣΗ 5 : ΛΗΨΗ ΠΟΡΩΝ [64]

4.6.3.4 Στόχος του Xrep

Τα δίκτυα P2P είναι σχεδιασμένα έτσι ώστε να κατανέμουν ευθύνες κατά μήκος του δικτύου, δηλαδή στα μέλη του. Η ιδιαιτερότητα τους αυτή όμως επιφέρει και κάποια μειονεκτήματα όσον αφορά την ασφάλεια του δικτύου. Ένας βασικός στόχος του πρωτοκόλλου XRep είναι να βελτιώσει την ασφάλεια και την ποιότητα της κατανομής των πόρων στο πλαίσιο των P2P δικτύων, παρέχοντας προστασία από τους περισσότερους γνωστούς τύπους επιθέσεων.

4.6.4 QnQ

Στο [68] προτείνει το QnQ, ένα μοντέλο για τον υπολογισμό της εμπιστοσύνης και της φήμης σε ένα σύστημα πληθοπορισμού (CrowdSourcing) με τη παρουσία κακόβουλων χρηστών.



Εικόνα 21 : ΤΟ ΜΟΝΤΕΛΟ ΣΥΣΤΗΜΑΤΟΣ QNQ [80]

Όπως φαίνεται και στην Εικόνα 21, το QnQ καταγράφει μια κατοικημένη αστική περιοχή, στην οποία οι χρήστες έχουν στην κατοχή τους έξυπνες κινητές συσκευές και είναι εγγεγραμμένοι μέσω αυτών σε μια εφαρμογή CrowdSourcing. Το σύστημα αποτελείται από δύο βασικά στοιχεία:

Αναφορά: ο χρήστης δημιουργεί μια ειδοποίηση σε περίπτωση που αντιληφθεί ένα γεγονός (ατύχημα, κυκλοφοριακή συμφόρηση). Ωστόσο, ένας κακόβουλος χρήστης μπορεί να δημιουργήσει μια αναφορά για γεγονότα που δεν έχουν συμβεί.

Εκδήλωση: είναι το σύνολο των πληροφοριών που δημοσιεύονται σε ένα ζωντανό χάρτη σε περίπτωση που η εφαρμογή λάβει ορισμένο αριθμό παρόμοιων αναφορών. Εάν αναφορές από δύο διαφορετικούς χρήστες παρουσιάσουν ομοιότητες σε δείκτες όπως τοποθεσία, τύπος εκδήλωσης και ημερομηνία, τότε υποδεικνύουν την ίδια εκδήλωση.

4.6.4.1 Οι τύποι χρηστών στο QnQ

Στο μοντέλο του QnQ, οι χρήστες προσδιορίζονται ανάλογα με τη δράση τους.
Υπάρχουν δυο βασικοί τύποι χρηστών:

Ανταποκριτής (Reporter): ο ανταποκριτής έχει αναφέρει τουλάχιστον ένα περιστατικό και έχει την τάση να δημιουργεί αναφορές. Κάθε χρήστης τέτοιου τύπου

χαρακτηρίζεται από ένα βαθμό φήμης, σύμφωνα με το οποίο προσδιορίζεται η ποιότητα των αναφορών του και ο βαθμός της συμμετοχής του. Η ανταμοιβή είναι ανάλογη αυτού του βαθμού φήμης. Ωστόσο, ο ανταποκριτής δεν έχει την δυνατότητα να βαθμολογήσει μια κοινοποιημένη εκδήλωση για την οποία έχει εκδώσει αναφορά.

Βαθμολογητής(Rater): είναι ένας χρήστης που παρέχει ανατροφοδότηση όσον αφορά την χρησιμότητα μιας εκδήλωσης. Οι επιλογές του στην διαδικασία της βαθμολόγησης είναι οι εξής : (α) χρήσιμη, (β) μη χρήσιμη, (γ) δεν είμαι σίγουρος. Για οποιαδήποτε κοινοποιημένη εκδήλωση, ο βαθμολογητής επιτρέπεται να υποβάλει μόνο μια εκτίμηση. Η έλλειψη κάποιου είδους αμοιβής για την εκτίμηση αυτή αποτρέπει τους χρήστες από το να υποβάλουν ψευδείς εκτιμήσεις.

4.7 Συστήματα φήμης στο MCS

Συνοψίζοντας, τα οφέλη των συστημάτων φήμης μπορούν να εφαρμοστούν στο MCS με διάφορους τρόπους, ανάλογα με τις συγκεκριμένες ανάγκες και στόχους του συστήματος MCS. Σε αυτή την υποενότητα παρουσιάζονται μερικά παραδείγματα για το πώς τα συστήματα φήμης μπορούν να εφαρμοστούν στο MCS[94][95]:

- Ποιότητα δεδομένων: Στα συστήματα MCS, τα συστήματα φήμης μπορούν να χρησιμοποιηθούν για τη μέτρηση της ποιότητας των δεδομένων που συνεισφέρουν οι χρήστες. Για παράδειγμα, μια βαθμολογία φήμης θα μπορούσε να εκχωρηθεί σε έναν χρήστη με βάση την ακρίβεια και την αξιοπιστία των δεδομένων που έχουν συνεισφέρει στο παρελθόν. Με αυτό τον τρόπο, τα δεδομένα των χρηστών με υψηλότερες βαθμολογίες φήμης είναι πιο πιθανό να γίνουν αποδεκτά από το σύστημα, ενώ όσοι έχουν χαμηλότερες βαθμολογίες μπορεί να χρειαστεί να παράσχουν πρόσθετα στοιχεία ή να υποβληθούν σε πρόσθετη επαλήθευση πριν γίνουν αποδεκτά τα δεδομένα τους.

- Κίνητρα συμμετοχής: Τα συστήματα φήμης μπορούν να χρησιμοποιηθούν στο MCS για να παρακινήσουν τη συμμετοχή και να ενθαρρύνουν τους χρήστες να συνεισφέρουν δεδομένα υψηλής ποιότητας. Για παράδειγμα, οι χρήστες με υψηλές βαθμολογίες φήμης μπορεί να είναι κατάλληλοι για ανταμοιβές ή άλλα κίνητρα για τη συνεισφορά δεδομένων, ενώ όσοι έχουν χαμηλές βαθμολογίες ενδέχεται να απαιτείται να συνεισφέρουν περισσότερα δεδομένα ή να υποβληθούν σε πρόσθετη επαλήθευση πριν λάβουν ανταμοιβές. Έτσι, σε μια υποθετική περίπτωση εφαρμογής υγείας και άθλησης, οι χρήστες με υψηλότερο βαθμό φήμης στο σύστημα θα έχουν την δυνατότητα να λάβουν επιπλέον ανταμοιβές και πρόσβαση σε αποκλειστικό περιεχόμενο άθλησης.

- Αξιοπιστία: Τα συστήματα φήμης μπορούν να χρησιμοποιηθούν στο MCS για τη μέτρηση της αξιοπιστίας των χρηστών που συνεισφέρουν δεδομένα στο δίκτυο. Για παράδειγμα, μια βαθμολογία φήμης θα μπορούσε να εκχωρηθεί με βάση την προηγούμενη συμπεριφορά του χρήστη εντός του δικτύου, όπως το ιστορικό συνεισφοράς ακριβών και αξιόπιστων δεδομένων ή το κατά πόσο ακολουθεί τις οδηγίες της διαδικτυακής κοινότητας και συμμετέχει με εποικοδομητικό τρόπο.

- Επαλήθευση: Τα συστήματα φήμης μπορούν να χρησιμοποιηθούν στο MCS για την επαλήθευση της ταυτότητας και των διαπιστευτηρίων των χρηστών που συνεισφέρουν δεδομένα στο δίκτυο. Για παράδειγμα, μια βαθμολογία φήμης θα μπορούσε να εκχωρηθεί με βάση την ικανότητα του χρήστη να παρέχει επαληθεύσιμη ταυτοποίηση και άλλα στοιχεία της πείρας ή των προσόντων του.

Συνολικά, τα συστήματα φήμης στο MCS έχουν σχεδιαστεί για να μετρούν και να καταγράφουν την αξιοπιστία ατόμων που συνεισφέρουν δεδομένα στο δίκτυο, να δίνουν κίνητρα για καλή συμπεριφορά και να αποτρέπουν κακόβουλη ή ανεπιθύμητη δραστηριότητα. Κάποιοι από τους βασικούς παράγοντες που επηρεάζουν τη φήμη των χρηστών στο MCS:

- Συχνότητα: οι χρήστες που συμμετέχουν με μεγαλύτερη συχνότητα και συνέπεια σε διαδικασίες συλλογής πληροφοριών, αντιμετωπίζονται από το σύστημα ως περισσότερο αξιόπιστοι σε σχέση με τους αντίστοιχους χρήστες που δεν συμμετέχουν συχνά, επηρεάζοντας θετικά τη βαθμολογία φήμης τους.

- Ιστορικό: η συνεχής υποβολή δεδομένων υψηλής ποιότητας σε βάθος χρόνου συνεισφέρει θετικά στη σχηματισμό μια υψηλής βαθμολογίας. Αντίθετα, ένα αναξιόπιστο ιστορικό μπορεί να είναι αποτρεπτικός παράγοντας στην επιδίωξη συναλλαγών μεταξύ των χρηστών.

- Αξιολογήσεις: θετικές αξιολογήσεις και κριτικές από άλλους χρήστες του συστήματος προσδιορίζει τη βαθμολογία.

- Ποιότητα Αισθητήρων: τα ποιοτικά τεχνολογικά μέσα ή αισθητήρες που έχει στη κατοχή του ο χρήστης είναι πιθανό να συλλέξουν υψηλότερης ποιότητας δεδομένα

- Αναφορά Ύποπτης Συμπεριφοράς: οι χρήστες κάποιων συστημάτων έχουν τη δυνατότητα να υποβάλουν αναφορά εφόσον εντοπίσουν ύποπτη (ή και κακόβουλη) συμπεριφορά. Ο χρήστης εφόσον ελεγχθεί από τους αντίστοιχους μηχανισμούς και αποδειχθεί κακόβουλος για το σύστημα, θα βαθμολογηθεί αρνητικά.

4.8 Συστήματα φήμης στο Blockchain

Η εφαρμογή των Συστημάτων Φήμης στη τεχνολογία Blockchain προσφέρει έναν τρόπο προσδιορισμού της αξιοπιστίας των χρηστών σε ένα αποκεντρωμένο δίκτυο. Τα συστήματα αυτά χρησιμοποιούνται έτσι ώστε να παρέχουν κίνητρο και να ανταμείβουν την καλή συμπεριφορά του χρήστη στο πλαίσιο του δικτύου, αλλά και να αποτρέπουν περιπτώσεις κακόβουλης δραστηριότητας στο Blockchain. Αυτό επιτυγχάνεται με την ανάθεση της βαθμολογίας φήμης στον κάθε ξεχωριστό χρήστη, η οποία προσδιορίζεται με βάση της προηγούμενες ενέργειες και αλληλεπιδράσεις με άλλους χρήστες στο δίκτυο.

Συγκεκριμένα, κάποιοι από τους τρόπους εφαρμογής των συστημάτων φήμης στο Blockchain είναι[70][71]:

- Συγκεντρωτικά Συστήματα Φήμης: σε αυτού του είδους τα συστήματα φήμης, μια μοναδική οντότητα φέρει την ευθύνη του προσδιορισμού και της ενημέρωσης της βαθμολογίας της φήμης για τους χρήστες. Αυτή η προσέγγιση μπορεί να είναι αποτελεσματική, αλλά και ευάλωτη σε περιπτώσεις χειραγώγησης ή μεροληψίας. Ένα τέτοιο παράδειγμα συστήματος είναι το Amazon και το Ebay, που αναφέρθηκε αναλυτικότερα σε προηγούμενη ενότητα.

- Αποκεντρωμένα Συστήματα Φήμης: Σε ένα αποκεντρωμένο σύστημα φήμης όπως το προτεινόμενο στο [71], οι βαθμολογίες φήμης των χρηστών υπολογίζονται και ενημερώνονται αντίστοιχα από ένα αποκεντρωμένο δίκτυο κόμβων. Αυτή η προσέγγιση μπορεί να είναι πιο διαφανής και ανθεκτική στη χειραγώγηση, αλλά μπορεί επίσης να είναι πιο περίπλοκη στην εφαρμογή και τη διατήρηση.

- On-chain Συστήματα Φήμης: Σε ένα σύστημα φήμης on-chain, οι βαθμολογίες φήμης καταγράφονται απευθείας στο blockchain, καθιστώντας τα διαφανή και αμετάβλητα. Αυτή η προσέγγιση μπορεί να είναι αποτελεσματική για τη διασφάλιση της ακεραιότητας του συστήματος φήμης, αλλά μπορεί επίσης να οδηγήσει σε αυξημένη χρήση πόρων στο blockchain. Τέτοιου είδους συστήματα είναι τα μη ανταλλάξιμα tokens, γνωστά και ως NFTs.

- Off-chain Συστήματα Φήμης: Σε αντίθεση με τη προηγούμενη περίπτωση, οι βαθμολογίες φήμης καταγράφονται από το blockchain και μόνο η τελική βαθμολογία φήμης καταγράφεται στο blockchain. Αυτή η προσέγγιση μπορεί να είναι πιο αποτελεσματική όσον αφορά τη χρήση των πόρων, αλλά μπορεί επίσης να είναι λιγότερο διαφανής και δυνητικά ευάλωτη σε χειραγώγηση.

Ένα απλό παράδειγμα off-chain συναλλαγής είναι η ανταλλαγή των ιδιωτικών κλειδιών μεταξύ δυο οντοτήτων στο blockchain[96].

Σε γενικό πλαίσιο, η επιτυχία της εφαρμογής των συστημάτων φήμης στο blockchain εξαρτάται κυρίως από την ικανότητά τους να μετρούν με ακρίβεια και δίκαια και να αντικατοπτρίζουν την αξιοπιστία των χρηστών, προωθώντας ένα πιο ασφαλές και αξιόπιστο διαδικτυακό οικοσύστημα για τους ίδιους τους χρήστες.

Κεφάλαιο 5: Εφαρμογή της τεχνολογίας Blockchain σε συνδυασμό με τα Συστήματα Φήμης στο MCS

Τα τελευταία χρόνια, τα συστήματα MCS έχουν αναδειχθεί ως το πλέον υποσχόμενο παράδειγμα για τη συλλογή μεγάλου όγκου πληροφοριών μέσω της χρήσης έξυπνων κινητών συσκευών (κυρίως smartphones), έτσι ώστε να υποστηρίζουν τις ραγδαία εξελισσόμενες εφαρμογές που αυτά προσφέρουν στο χρήστη. Για να εξασφαλιστεί η ποιότητα και η αξιοπιστία αυτής της συλλογής πληροφοριών και να αντιμετωπιστεί το κίνητρο ορισμένων κακόβουλων χρηστών να επηρεάσουν την ποιότητα αυτών των πληροφοριών, προτάθηκε η εφαρμογή των Συστημάτων Φήμης. Με αυτό τον τρόπο, επιβραβεύεται η σωστή συμπεριφορά στη διαδικασία της συλλογής πληροφοριών μέσω του επιπέδου φήμης του κάθε μοναδικού χρήστη. Παρόλα αυτά, η πιθανότητα διαφόρων ειδών επιθέσεων στο σύστημα είναι ρεαλιστική, όπως αναφέρθηκε αναλυτικότερα σε προηγούμενο κεφάλαιο. Τη λύση σε αυτό το μείζων πρόβλημα ασφαλείας προσφέρει η εφαρμογή της τεχνολογίας Blockchain με τη παροχή ενός ασφαλούς, αποκεντρωμένου και διαφανούς περιβάλλοντος για την καταγραφή και επιβεβαίωση της ποιότητας των δεδομένων. Σε αυτό το πλαίσιο, τα συστήματα φήμης μπορούν να ενσωματωθούν με το blockchain για να επιτρέψουν πιο ισχυρά και αξιόπιστα συστήματα συλλογής πληροφοριών με τη χρήση κινητών συσκευών. Στην ενότητα αυτή, θα παρουσιαστούν παραδείγματα και προτάσεις που εφαρμόζεται ο παραπάνω συγκεκριμένος συνδυασμός.

5.1 Το σύστημα BC-MCS

Το [72] προτείνει ένα αξιόπιστο και αποτελεσματικό σύστημα που ενσωματώνει το Blockchain στα συστήματα MCS, το BC-MCS.

5.1.2 Η αρχιτεκτονική του συστήματος BC-MCS

Το σύστημα BC-MCS, για να παρακάμψει τα προβλήματα χρονικών καθυστερήσεων και του υψηλού κόστους που χαρακτηρίζουν τις εφαρμογές MCS, αντλεί έμπνευση από το μοντέλο συστήματος EC-MCS[83]. Όπως φαίνεται στην Εικόνα 22, η σύσταση του αποτελείται από τις εξής τέσσερις οντότητες:

Κέντρο Διανομής Εργασιών

Ο ρόλος της συγκεκριμένης οντότητας είναι ιδιαίτερα σημαντικός, καθώς είναι υπεύθυνη για την διανομή διάφορων εργασιών συλλογής δεδομένων. Συγκεκριμένα, λαμβάνει τις εργασίες από τον requester και στη συνέχεια αναζητά τους καταλληλότερους χρήστες, οι οποίοι με τη σειρά τους παρέχουν τα δεδομένα. Στόχος του Κέντρου Διανομής Εργασιών είναι η εξασφάλιση της ποιότητας των δεδομένων.

Κέντρο Διανομής Κλειδιών

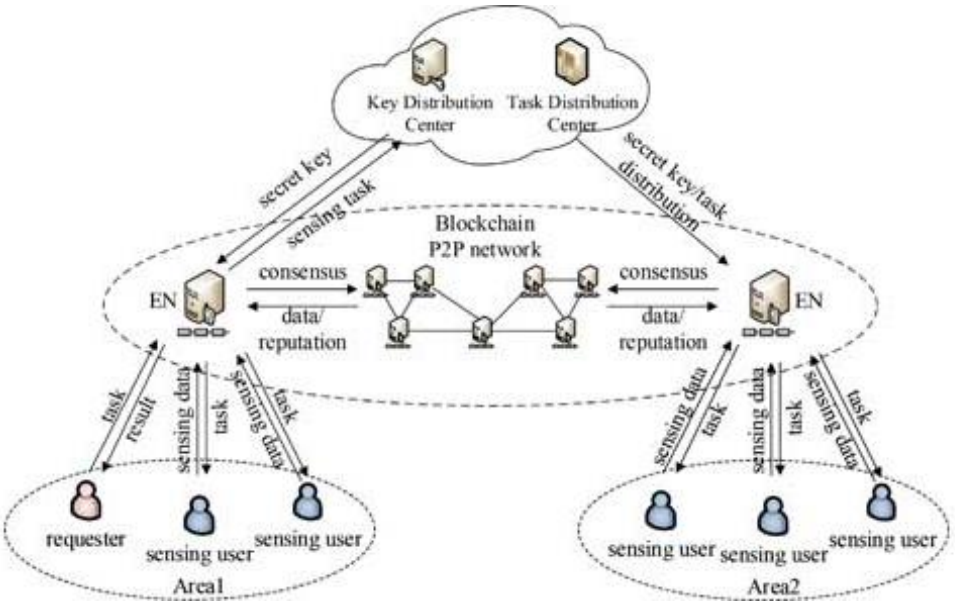
Το Κέντρο Διανομής Κλειδιών έχει ως κύρια λειτουργία του την εξασφάλιση του απορρήτου των χρηστών. Αυτό επιτυγχάνεται μέσω της διατήρησης και της διανομής εμπιστευτικών κλειδιών.

Υπολογιστικός Κόμβος

Έχει το ρόλο του υπολογιστικού κόμβου σε ένα περιβάλλον τεχνολογίας Blockchain, καθώς αποθηκεύσει δεδομένα καθολικού και εκτελεί αλγόριθμους συναίνεσης. Η ενημέρωση του επιπέδου φήμης και η συλλογή δεδομένων εκτελούνται επίσης από τον Υπολογιστικό Κόμβο.

Συμμετέχοντες Χρήστες

Στο σύστημα BC-MCS, υπάρχουν δύο είδη χρηστών, ο αιτών, ο οποίος είναι υπεύθυνος για την έκδοση εργασιών ανίχνευσης πληροφοριών και ο εργαζόμενος, καθήκον του οποίου είναι η παροχή δεδομένων ανίχνευσης με τη χρήση κινητών συσκευών.



Εικόνα 22 : Η ΓΕΝΙΚΗ ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΤΟΥ BC-MCS [72]

Η διαδικασία της διαχείρισης του επιπέδου φήμης αποτελείται από δύο συνεχείς διαδικασίες: την διαδικασία της ανίχνευσης πληροφοριών και της ενημέρωσης της φήμης. Στην πρώτη, ο αιτών (αναφέρεται ως p) δημοσιεύει την εκάστοτε εργασία μέσω του Κέντρου Διανομής Κλειδιών. Στην συνέχεια, ο κάθε εργαζόμενος (αντίστοιχα αναφέρεται ως u) αποδέχεται την εργασία με σκοπό να παρέχει τα απαιτούμενα δεδομένα ανίχνευσης. Το σύστημα BC-MCS συλλέγει τον όγκο των δεδομένων και κατά τη διαδικασία ενημέρωσης της φήμης, ο P παρέχει την ανατροφοδότηση για κάθε χρήστη U όσον αφορά τις συλλεγμένες πληροφορίες και τις αποθηκεύει ως βαθμολογία τοπικής φήμης. Όταν ολοκληρωθούν όλες οι εργασίες που έχουν δημοσιευθεί, το σύστημα συλλέγει το σύνολο των βαθμολογιών τοπικής φήμης από τους αιτούντες από όπου προκύπτει το συνολικό επίπεδο φήμης των χρηστών ανίχνευσης.

5.1.3 Απαιτήσεις Ασφαλείας

Για να εξασφαλιστεί η αξιοπιστία και η ασφάλεια του συστήματος, οι χρήστες οφείλουν να ακολουθούν κάποιους συγκεκριμένους κανόνες διατήρησης απορρήτου. Συγκεκριμένα, από τη μεριά των χρηστών ανίχνευσης, κατά τη διαδικασία της συλλογής πληροφοριών τα δεδομένα που παρέχονται από τους χρήστες θα πρέπει να διατηρούνται εμπιστευτικά και να μην διαμοιράζονται μεταξύ των χρηστών. Σε γενικό πλαίσιο, μόνο ο αιτών και οι αντίστοιχοι χρήστες ανίχνευσης έχουν πρόσβαση σε αυτά τα δεδομένα. Όσον αφορά τους αιτούντες, αφού γίνει η συλλογή των πληροφοριών από το σύστημα, το τελικό αποτέλεσμα είναι διαθέσιμο αποκλειστικά και μόνο στον εκάστοτε αιτούντα χρήστη. Με αυτό τον τρόπο εξασφαλίζεται η προστασία των δεδομένων από τους κακόβουλους χρήστες του συστήματος αλλά και πιθανή συνεργασία τους με σκοπό αποκτήσουν πρόσβαση σε αυτά. Αντίστοιχα, κατά τη διάρκεια της ενημέρωσης φήμης, η ανατροφοδότηση του αιτούντα όσον αφορά τη ποιότητα των δεδομένων που έχουν συλλεχθεί είναι ατομική έτσι ώστε να μην διαμοιράζεται στους ίδιους κακόβουλους χρήστες που αναφέρθηκαν παραπάνω.

5.1.4 Προκλήσεις του μοντέλου BC-MCS

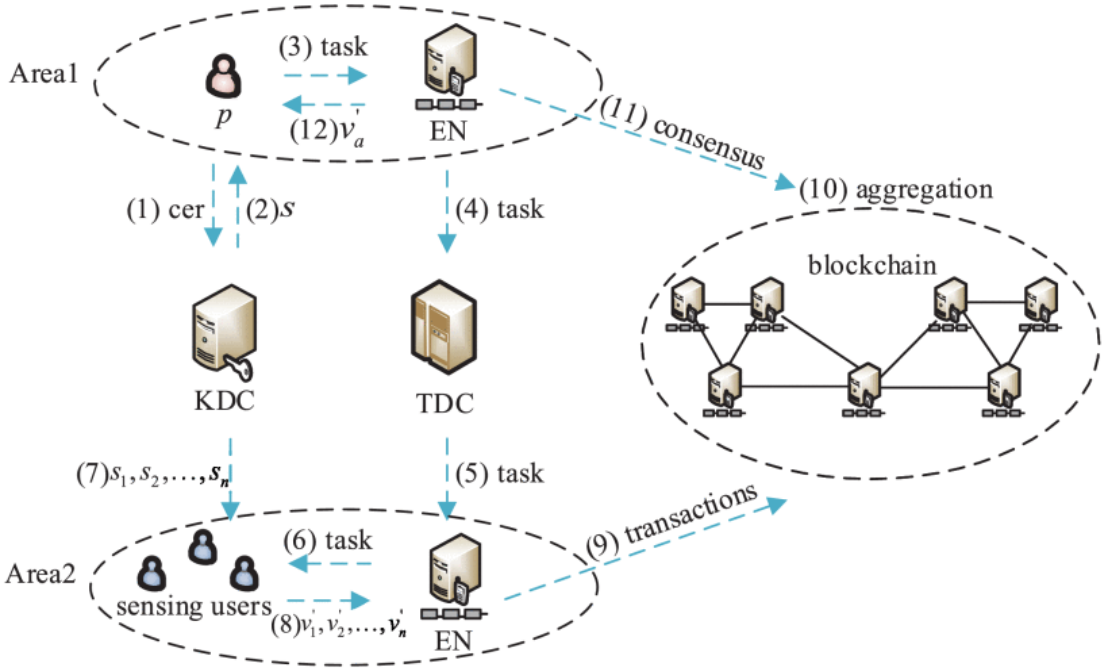
Στο συγκεκριμένο μοντέλο, το Κέντρο Διανομής είναι αυτό που κατέχει το σύνολο των κρυφών κλειδιών του συστήματος και ως εκ τούτου θεωρείται πλήρως αξιόπιστο μεταξύ των οντοτήτων του. Υπάρχει όμως πάντα η πιθανότητα, είτε ο υπολογιστικός κόμβος είτε οι συμμετέχοντες χρήστες να εκδηλώσουν κακόβουλη συμπεριφορά προς το σύστημα. Οι τρόποι για να δεχθεί εξωτερική επίθεση το BC-MCS είναι οι εξής:

- Ο κακόβουλος χρήστης μπορεί να εκδηλώσει επιθέσεις σε έναν ή περισσότερους υπολογιστικούς κόμβους έτσι ώστε να παρέμβει και να επηρεάσει τη διαδικασία της διαχείρισης της φήμης των χρηστών που συλλέγουν τις πληροφορίες.

- Όσον αφορά τον τομέα των χρηστών, ο επιτιθέμενος με τη παροχή πληροφοριών κακής ποιότητας έχει τη δυνατότητα να διαταράξει την ομαλή λειτουργία του συστήματος.

- Επίσης, ο επιτιθέμενος μπορεί να συνεργαστεί με τους ίδιους τους χρήστης και ένα μέρος από τους υπολογιστικούς κόμβους έτσι ώστε να παρακάμψει τις δικλείδες ασφαλείας και να αποκτήσει πρόσβαση στα δεδομένα που έχουν συλλεχθεί από τους υπόλοιπους χρήστες του συστήματος.

Τα χαρακτηριστικά και η φύση της τεχνολογίας blockchain προσφέρουν τις απαραίτητες λύσεις έτσι ώστε να αντιμετωπιστούν οι παραπάνω προκλήσεις. Καταρχάς, ο επιτιθέμενος δεν έχει την δυνατότητα να ελέγχει σε οποιαδήποτε στιγμή ποσοστό ανώτερο του 51% του συνόλου των υπολογιστικών κόμβων στο blockchain, διότι αναγνωρίζεται και δεν είναι δυνατό να πλαστογραφήσει την απαραίτητη ψηφιακή υπογραφή χωρίς το κρυφό κλειδί του εκάστοτε χρήστη. Η επικοινωνία των χρηστών πραγματοποιείται σε ασφαλή κανάλια και έτσι αυτοί που εκδηλώνουν κακόβουλη συμπεριφορά αποτελούν τη μειοψηφία



Εικόνα 23 : Η ΔΙΑΔΙΚΑΣΙΑ ΣΥΛΛΟΓΗΣ ΠΛΗΡΟΦΟΡΙΩΝ ΣΤΟ BC-MCS [72]

5.1.5 Η διαδικασία της συλλογής πληροφοριών στο BC-MCS

Στην εικόνα 26 απεικονίζεται αναλυτικά η διαδικασία συλλογής πληροφοριών στο σύστημα BC-MCS. Η διαδικασία αυτή αποτελείται από έξι φάσεις[72]:

Έκδοση Εργασιών και Κλειδιού

Το Κέντρο Διανομής Κλειδιών δημιουργεί ένα κρυφό κλειδί για λογαριασμό των αιτούντων, οι οποίοι με τη σειρά τους προωθούν την εργασία στο κοντινότερο κόμβο έτσι ώστε να ξεκινήσει η διαδικασία συλλογής πληροφοριών.

Ανάθεση Εργασίας

Η εργασία που έχει ανατεθεί προωθείτε από τους υπολογιστικούς κόμβους στο Κέντρο Διανομής Εργασιών, το οποίο αντίστοιχα αναζητεί χρήστες υψηλής ποιότητα έτσι ώστε να φέρουν εις πέρας την εργασία που δημοσίευσε ο αιτών χρήστης.

Εξασφάλιση της ασφάλειας των δεδομένων

Αφού έχει ξεκινήσει η διαδικασία συλλογής πληροφοριών με τη χρήση κινητών συσκευών από τους διαθέσιμους χρήστες, προκύπτει το σοβαρό ζήτημα της προστασίας των δεδομένων. Τα προστατευμένα δεδομένα ενσωματώνονται σε μια συναλλαγή στο blockchain και στέλνονται στο κοντινότερο υπολογιστικό κόμβο.

Επαλήθευση της Συναλλαγής

Ο υπολογιστικός κόμβος ξεκινά την εκτέλεση του έξυπνου συμβολαίου αυτόματα αφού λάβει τις συναλλαγές από το blockchain από τους χρήστες. Στη συνέχεια και αφού ελεγχθεί η εγκυρότητα των δεδομένων των συναλλαγών αυτών, που επαληθεύεται με την χρήση της ψηφιακής υπογραφής του χρήστη και τον έλεγχο των προστατευμένων δεδομένων, οι μη έγκυρες συναλλαγές απορρίπτονται και οι έγκυρες καταγράφονται στο Blockchain από τον υπολογιστικό κόμβο.

Συνάθροιση Δεδομένων

Το σύνολο των κόμβων παρέχουν τα δεδομένα που έχουν συλλεχτεί και οι συναλλαγές έχουν καταγραφεί στο Blockchain. Τότε ξεκινά η συνάθροιση των

δεδομένων όπως προκύπτει από το έξυπνο συμβόλαιο. Η σημασία των δεδομένων αποθηκεύεται δημόσια με βάση το βαθμό φήμης του χρήστη από τον οποίο προέρχονται. Το αποτέλεσμα αυτής της διαδικασίας δημοσιοποιείται στον αιτούντα χρήστη.

Τελικό Αποτέλεσμα της Συνάθροισης των Δεδομένων

Επιτυγχάνεται με τη χρήση του κρυφού κλειδιού του αιτούντα, ο οποίος αφαιρεί τον παράγοντα προστασίας των δεδομένων και υπολογίζει το αποτέλεσμα της διαδικασίας συνάθροισης.

5.2 Ένα ανώνυμο σύστημα Φήμης για συλλογή πληροφοριών σε διπλό Blockchain

Στο [73] προτείνεται ένα σύστημα διαχείρισης διαδικτυακής φήμης, το οποίο είναι βασισμένο στη αρχιτεκτονική διπλού Blockchain, στην οποία τα επίπεδα φήμης αποκρύπτονται. Ειδικότερα, η μία αλυσίδα Block χρησιμοποιείται για την αποθήκευση και την ενημέρωση του βαθμού φήμης στο εσωτερικό του συστήματος, ενώ η δεύτερη αλυσίδα είναι υπεύθυνη για τη δημοσίευση εργασιών προς τους χρήστες και την αποθήκευση των δεδομένων που προκύπτουν από αυτές τις εργασίες.

5.2.1 Αρχιτεκτονική συστήματός MCS διπλού Blockchain

Το συγκεκριμένο αποκεντρωμένο σύστημα MCS συγκροτείται από τέσσερις βασικές οντότητες. Αυτές είναι ο αιτών χρήστης (ή requester), οι εργάτες (ή workers) και οι δύο αλυσίδες αποτελούμενες από blocks, η αλυσίδα συλλογής πληροφοριών Sensing Chain και η αλυσίδα φήμης Reputation Chain(αναφέρονται για συντομία ως SChain και RChain αντίστοιχα).

<u>Αιτών</u>

Ο αιτών πρέπει να εγγραφεί ξεχωριστά σε κάθε μια από τις αλυσίδες SChain και RChain. Αφού ολοκληρωθεί η διαδικασία της εγγραφής, ο requester μπορεί να

δημιουργήσει και να δημοσιεύσει εργασίες στο Schain, και στη συνέχεια θα ελέγξει και θα αξιολογήσει τα δεδομένα-πληροφορίες που υποβάλει ο εκάστοτε εργάτης για τη συγκεκριμένη εργασία. Μόλις ολοκληρωθεί η αξιολόγηση αυτή, ο requester θα δημοσιεύσει μια κρυπτογραφημένη βαθμολογία που αντιστοιχεί στον εργάτη. Η διαδικασία αυτή εξασφαλίζει την ασφάλεια και την ακρίβεια των δεδομένων ανίχνευσης αλλά και το επίπεδο φήμης των χρηστών του συστήματος.

Εργάτης

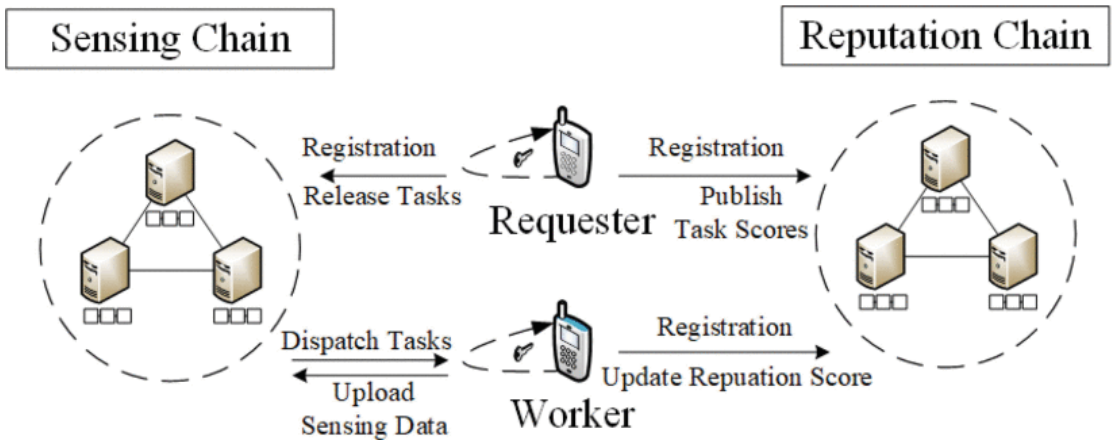
Σε αντίθεση με τον requester, ο εργάτης χρειάζεται να εγγραφεί μονάχα στην αλυσίδα φήμης του συστήματος. Εφόσον πραγματοποιηθεί η εγγραφή, αναλαμβάνει να φέρει εις πέρας εργασίες που έχουν δημοσιευτεί στην αλυσίδα συλλογής αφού συλλέξει τις απαραίτητες πληροφορίες, τις κρυπτογραφήσει και τις ανεβάσει στην αλυσίδα. Όταν έχει πλέον συμπληρώσει τον απαιτούμενο αριθμό εργασιών και λάβει τις αξιολογήσεις που του αντιστοιχούν, έχει τη δυνατότητα να ενημερώσει τη βαθμολογία φήμης του, καθώς είναι ο μόνος που γνωρίζει τον αριθμό των εργασιών που έχει ολοκληρώσει στο σύστημα.

Αλυσίδα Συλλογής SChain

Αποτελεί ουσιαστικά ένα δίκτυο Blockchain και είναι υπεύθυνη για την εγγραφή των requesters, την δημοσίευση εργασιών σε αυτή αλλά και την αποθήκευση των δεδομένων και των πληροφοριών που προκύπτουν από τις κινητές συσκευές των εργατών.

Αλυσίδα Φήμης RChain

Ομοίως με την έταιρη αλυσίδα, είναι ένα δίκτυο Blockchain στο οποίο γίνονται οι εγγραφές τόσο των requesters όσο και των workers, αποθηκεύονται (ή ενημερώνονται) οι βαθμολογίες φήμης των χρηστών αλλά και οι αξιολογήσεις των εργασιών από τους requesters.



Εικόνα 24 : Η ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ ΔΙΑΧΕΙΡΙΣΗΣ ΦΗΜΗΣ [73]

5.2.2 Η διαδικασία συλλογής πληροφοριών στο σύστημα

Η λειτουργία του προτεινόμενου συστήματος όσον αφορά τη συλλογή πληροφοριών περιγράφεται στις εξής πέντε φάσεις:

Εγγραφή

Οι χρήστες του συστήματος παράγουν το δικό τους τοπικό ζεύγος ιδιωτικού και δημόσιου κλειδιού. Οι αιτούντες πραγματοποιούν την εγγραφής τους και στις δύο αλυσίδες του συστήματος με τη χρήση του δημοσίου κλειδιού τους και στη συνέχεια τους ανατίθεται ένα αρχικό επίπεδο φήμης, ενώ οι εργάτες αντίστοιχα πραγματοποιούν την εγγραφή τους στο RChain.

Δημοσίευση Εργασίας

Για να δημοσιεύσει μια εργασία στο SChain, ο requester πρέπει να χρησιμοποιήσει την ψηφιακή του υπογραφή (κρυφό κλειδί). Στη συνέχεια αυτή η υπογραφή επαληθεύεται μέσω του ψηφιακού συμβολαίου, το οποίο περιέχει και πληροφορίες σχετικές με τις απαιτήσεις της συγκεκριμένης εργασίας. Μόνο τότε είναι δυνατή η δημοσίευση της εργασίας και η αναμετάδοση της προς τους χρήστες στο δίκτυο της αλυσίδας SChain.

Μετάδοση Δεδομένων

Η συμμετοχή των εργατών σε μια εργασία συλλογής πληροφοριών αφού αυτή δημοσιευτεί στο Blockchain είναι προαιρετική. Σε περίπτωση που ένας εργάτης συλλέγει πληροφορίες για μια εργασία, χρειάζεται να συντάξει ένα συμβόλαιο υποβολής αυτών των δεδομένων το οποίο περιέχει τον ξεχωριστό αριθμό ID της κάθε εργασίας, το δημόσιο κλειδί της, τα κρυπτογραφημένα δεδομένα που έχει συλλέξει αλλά και το επίπεδο φήμης του.

Επαλήθευση φήμης

Ο αιτών από μεριά του λαμβάνει τα δεδομένα που έχει καταχωρήσει ο εργάτης, τα αποκρυπτογραφεί και στη συνέχεια επιβεβαιώνει εάν το επίπεδο φήμης ανήκει σε κάποιον από τους εργάτες.

Ενημέρωση φήμης

Αφού ολοκληρωθεί η διαδικασία επαλήθευσης της διαδικτυακής φήμης, ο αιτών αποδέχεται το σύνολο των δεδομένων που έχουν συλλεχθεί μέσω της εργασίας και τα αποθηκεύει στην αλυσίδα SChain. Παράλληλα αξιολογεί τη ποιότητα των δεδομένων που έχει συλλέξει ο κάθε χρήστης η οποία μεταφράζεται σε ένα κρυπτογραφημένο βαθμό αντίστοιχα. Μέσω του RChain, οι εργάτες επιβλέπουν το βαθμό φήμης που τους αναλογεί και τον αποκρυπτογραφούν. Είναι επίσης υπεύθυνοι έτσι ώστε να ενημερώνουν τακτικά αυτόν τον βαθμό φήμης τους στο σύστημα, ανάλογα με το πόσες εργασίες έχουν ολοκληρώσει.

5.2.3 Διατήρηση του απορρήτου στο σύστημα

Για να διατηρηθεί η ομαλή λειτουργία του συστήματος, είναι ιδιαίτερα σημαντική η προστασία του απορρήτου των εργατών κατά τη διάρκεια της συμμετοχής τους στην ολοκλήρωση των εργασιών MCS. Τα στοιχεία που πρέπει να διατηρηθούν απόρρητα αφορούν τα δεδομένα που συλλέγονται από τους εργάτες και ο βαθμός φήμης τους. Όσον αφορά τα συλλεγμένα δεδομένα μέσω της εργασίας που έχει δημοσιοποιηθεί, το σύστημα παρέχει πρόσβαση σε αυτά μονάχα στον requesterκαι στον εργάτη που τα παρέχει και μπορούν να αποκρυπτογραφηθούν με τη χρήση του δημόσιου κλειδιού της εργασίας. Επίσης, ο βαθμός φήμης τους εργάτη κρυπτογραφείτε και στη συνέχεια αποθηκεύεται στο RChain. Με αυτό το χαρακτηριστικό προστατεύεται το απόρρητο στο σύνολο του συστήματος καθώς μόνο ένας requester έχει πρόσβαση στη

συγκεκριμένη πληροφορίας ανά πάσα στιγμή . Τέλος, ο κάθε εργάτης χρησιμοποιεί το κρυφό του κλειδί έτσι ώστε να λάβει το βαθμό φήμης που του έχει ανατεθεί από τον requester χωρίς να έχει πρόσβαση στους αντίστοιχους βαθμούς των υπολοίπων εργατών του συστήματος.

5.3 Το σύστημα PP-RM

Στην σημερινή εποχή, η λογική της συλλογής πληροφοριών με τη χρήση έξυπνων κινητών συσκευών έχει καθιερωθεί ευρέως και έχει εφαρμοστεί επιτυχώς στους περισσότερους τομείς της καθημερινής κοινωνικής ζωής, όπως την επίβλεψη των (μαζικών) μεταφορών, τις υπηρεσίες υγείας, τις ψηφιακές πόλεις κα. Αποτέλεσμα αυτής της εξέλιξης είναι η αναμφίβολη βελτίωση της ποιότητας ζωής των πολιτών. Παρ' όλα αυτά, εξακολουθούν να υφίστανται δύο σοβαρά αναπάντητα προβλήματα, τα οποία καλείται να αντιμετωπίσει η πλειοψηφία των εφαρμογών MCS που έχουν αναπτυχθεί: η διατήρηση της ιδιωτικότητας και του απορρήτου στο σύστημα, αλλά και η ευπάθεια αυτού απέναντι στην δραστηριότητα των πιθανών κακόβουλων χρηστών. Η παροχή ανωνυμίας είτε η χρήση ενός ψευδώνυμου είναι μια πιθανή μέθοδος για τη επίλυσης απώλειας της ιδιωτικότητας, καθώς οι χρήστες με αυτό τον τρόπο δεν μπορούν να προσδιορίσουν τον πάροχο συγκεκριμένων δεδομένων. Όσον αφορά την προστασία από κακόβουλους χρήστες, η διαχείριση της διαδικτυακής φήμης είναι μια αποτελεσματική προσέγγιση, καθώς κάθε χρήστης που συμμετέχει στο σύστημα έχει ένα βαθμό φήμης ο οποίος ενημερώνεται σε συνάρτηση με την αξιοπιστία των δεδομένων που ο χρήστης παρέχει.

5.3.1 Η αρχιτεκτονική του συστήματος PP-RM

Η δομή του συστήματος [74] σχηματίζεται ως εξής:

Blockchain

Η ύπαρξη και τα χαρακτηριστικά του Blockchain σχηματίζουν ένα ασφαλές και ανοιχτό υπολογιστικό περιβάλλον, στα πλαίσια του οποίου εξασφαλίζεται η αξιοπιστία των πληροφοριών ως αποτέλεσμα της διαδικασίας συλλογής.

Κέντρο Διανομής Κλειδιών

Η συγκεκριμένη οντότητα έχει ως κύριο ρόλο της την διανομή κλειδιών στους χρήστες του συστήματος, θεωρείται αξιόπιστη και ως αποτέλεσμα εξασφαλίζεται η διατήρησης της ασφάλειας των δεδομένων. Θα πρέπει να σημειωθεί ότι απαραίτητη προϋπόθεση για την αξιοπιστία του συστήματος είναι το ποσοστό των κακόβουλων χρηστών να μην υπερβαίνει το 50%.

Requester

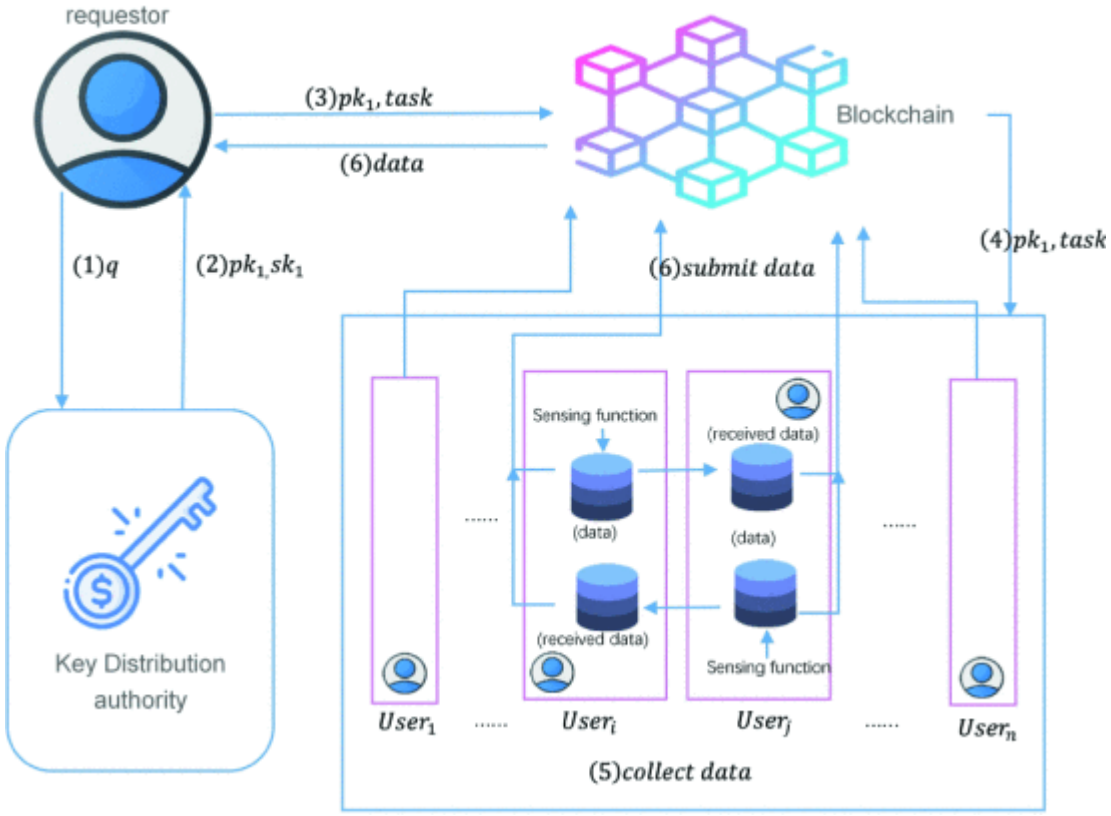
Ο ρόλος του requester είναι η έκδοση εργασιών συλλογής πληροφοριών προς τους χρήστες του συστήματος.

Εργαζόμενος

Είναι υπεύθυνοι για τη συλλογή πληροφοριών που προκύπτουν από τις εργασίες που εκδίδουν οι requesters στα χρονικά περιθώρια που έχουν τεθεί αναλόγως.

5.3.2 Η λειτουργία του συστήματος

Το σύστημα που έχει αναπτυχθεί προτείνει τη στρατηγική της συλλογικής απόκρυψης διαδρομής πληροφοριών. Πρόκειται για μια αποτελεσματική λύση για την προστασία του απορρήτου της ταυτότητας των χρηστών που συμμετέχουν στο σύστημα, αφού τους διαχωρίζει σε σχέση με τα δεδομένα που έχει συλλεχθεί μέσω των εργασιών χωρίς την ύπαρξη τρίτης κεντρικής οντότητας για την επίβλεψη του συστήματος. Ο requester αιτείται την έκδοση ζεύγους κλειδιών μέσω του κέντρου διανομής έτσι ώστε να διατηρήσει την ανωνυμία των άλλων χρηστών. Διατηρεί στη κατοχή του το κρυφό κλειδί ενώ διαμοιράζει το δημόσιο κλειδί σε συνδυασμό με την δημοσιευμένη εργασία στο Blockchain. Με τη σειρά τους, οι χρήστες ανίχνευσης παρατηρώντας το Blockchain ανταποκρίνονται και αναλαμβάνουν τις εργασίες που θεωρούν πως θα φέρουν εις πέρας. Αφού συλλέξουν τα ζητούμενα δεδομένα, τα κρυπτογραφούν με τη χρήση του δημόσιου κλειδιού και τα αποθηκεύουν τοπικά. Κάθε υποσύνολο τέτοιων δεδομένων προσδιορίζεται από ένα μοναδικό αριθμό ID, ο ποίος προκύπτει από μια hash λειτουργία με τη χρήση στοιχείων της ταυτότητας του χρήση που έχει προσφέρει τα δεδομένα, καθώς και το τόπο και τον χρόνο που έγινε η συγκεκριμένη ενέργεια. Τέλος ο requester παρατηρεί την τωρινή κατάσταση στο Blockchain και μόλις ολοκληρωθούν όλες οι ενέργειες συλλογής δεδομένων από τους χρήστες, αποκρυπτογραφεί τα δεδομένα και τα αξιοποιεί.



Εικόνα 25 : Η ΔΙΑΔΙΚΑΣΙΑ ΟΛΟΚΛΗΡΩΣΗΣ ΤΗΣ ΕΡΓΑΣΙΑΣ ΣΥΛΛΟΓΗΣ ΔΕΔΟΜΕΝΩΝ [74]

5.3.3 Πιθανά προβλήματα και απειλές του συστήματος

Η κύρια απειλή της ομαλής λειτουργίας του συστήματος PP-RM είναι η ύπαρξη κακόβουλων χρηστών, οι οποίοι παρέχουν βαθμούς φήμης σε άλλους χρήστες που δεν αντικατοπτρίζουν την πραγματική συνεισφορά τους και την ποιότητα των δεδομένων και των υπηρεσιών τους. Με τον τρόπο αυτό επηρεάζουν το συνολικό αποτέλεσμα που επιστρέφει στον requester. Επίσης, η συνύπαρξη πολλών κακόβουλων χρηστών και η συνεργασία τους ως ομάδα δημιουργεί προβλήματα στη διαδικασία συλλογής πληροφοριών, καθώς προσφέρουν ψηλές βαθμολογίες φήμης ο ένας στον άλλον και χαμηλές αντίστοιχα στους υπόλοιπους χρήστες. Μια διαφορετική προσέγγιση που μπορεί να υιοθετήσουν είναι η απόκτηση υψηλής βαθμολογίας φήμης από τους χρήστες του συστήματος με τη κατά διαστήματα προσφορά υψηλής ποιότητας υπηρεσιών. Με αυτό τον τρόπο επωφελούνται καθώς συνεχίζουν να μην βαθμολογούν αξιόπιστα το σύνολο των χρηστών ανεξάρτητα με τη πραγματική συνεισφορά τους. Τέλος, κάποιοι από αυτούς συνεργάζονται με σκοπό να παρακάμψουν τα απόρρητα στοιχεία του συστήματος και των συμμετεχόντων σε αυτό.

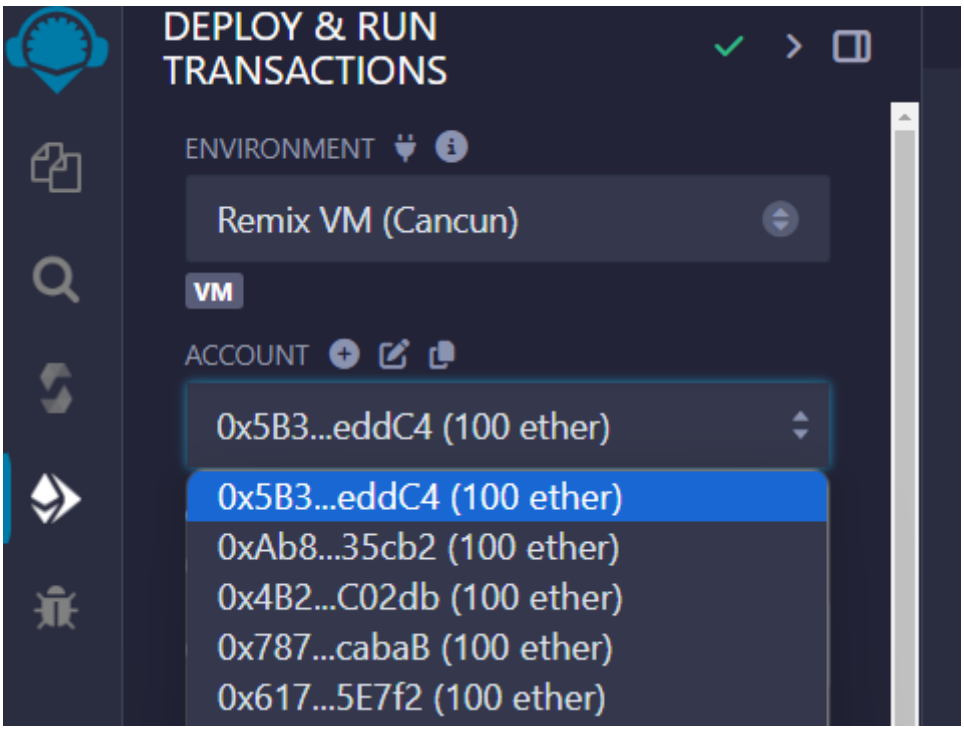
Κεφάλαιο 6 : Έξυπνο συμβόλαιο για τον υπολογισμό της διαδικτυακή φήμης στο Ethereum

Με βάση τα προαναφερθέντα προβλήματα και προκλήσεις, γίνεται παρουσίαση ενός έξυπνου συμβολαίου το οποίο θα υπολογίζει και παράλληλα θα ενημερώνει και αποθηκεύει τον βαθμό της διαδικτυακής φήμης των workers που συμμετέχουν στο δίκτυο. Αυτό επιτυγχάνεται με το συνδυασμό των χαρακτηριστικών της τεχνολογίας Blockchain με τα αντίστοιχα του MCS, έτσι ώστε να δημιουργήσει ένα ισχυρό και αποκεντρωμένο σύστημα για τη συλλογή και την επαλήθευση δεδομένων από ένα μεγάλο αριθμό κινητών συσκευών των χρηστών, διασφαλίζοντας παράλληλα την προστασία τους. Η αρχιτεκτονική του Ethereum είναι ευρέως γνωστή και χρησιμοποιείται για την ανάπτυξη smart contracts (κάτι που δεν ισχύει στην αντίστοιχη περίπτωση του Bitcoin), το οποίο επιτυγχάνεται με το δικό της κρυπτονόμισμα, το Ether ως αντίτιμο. Ως smart contracts λογίζονται τα αυτό εκτελέσιμα προγράμματα που τρέχουν στο blockchain. Για να συνταχθούν και να αναπτυχθούν τα smart contracts, οι κόμβοι που συμμετέχουν στην εκτέλεση τους ανταμείβονται με μια αντίστοιχη ποσότητα Ether. Η χρήση ενός Ethereum Blockchain γίνεται δωρεάν, παρόλα αυτά η εκτέλεση των συμβολαίων από τους κόμβους τους κοστίζει ether. Ένα επίσης σημαντικό χαρακτηριστικό του Ethereum ως πλατφόρμα είναι η ασφάλεια που παρέχει στους χρήστες και στους προγραμματιστές, η οποία συνεχώς αναβαθμίζεται. Αυτό επιτυγχάνεται με το γεγονός ότι όλοι οι κόμβοι στο blockchain λειτουργούν σε πραγματικό χρόνο, έτσι ώστε οποιαδήποτε συναλλαγή πραγματοποιείται θα πρέπει να εγκριθεί από το σύνολο τον κόμβων ή αντίστοιχα από κανέναν από αυτούς[82]. Τα συμβόλαια στο blockchain εκτελούνται από όλους τους κόμβους και οι ενημερωμένες πληροφορίες μοιράζονται μεταξύ άλλων κόμβων μετά από ένα μικρό χρονικό διάστημα. Αυτά τα συμβόλαια θα πρέπει να επικυρωθούν από τουλάχιστον 2 κόμβους του συστήματος για να ενεργοποιηθούν. Επίσης, τα συμβόλαια δεν χρησιμοποιούν το αλγόριθμο PoW, καθώς πραγματοποιούν συναλλαγές με τον κάθε κόμβο.

Η προγραμματιστική γλώσσα που είναι ευρέως διαδεδομένη και χρησιμοποιείται κατά κόρον στα συστήματα που χρησιμοποιούν την αρχιτεκτονική του Ethereum στο blockchain είναι η Solidity και είναι ειδικά σχεδιασμένη για δημιουργία και χρήση των smart contracts. Προτάθηκε αρχικά το 2014 από το Gavin Wood και τελικά αναπτύχθηκε το 2015. Χρησιμοποιείται επίσης και σε άλλα private blockchains και όχι μόνο στο Ethereum, όπως το Hyperledger Fabric (το οποίο έχει κυρίως εταιρική χρήση) και το Monax. Η ανάπτυξη της έχει επηρεαστεί από διαδεδομένες γλώσσες προγραμματισμού όπως η C, η Javascript και η Python.

6.1 Ανάπτυξη του συμβολαίου ReputationManagementSystem

Για την ανάπτυξη του συμβολαίου χρησιμοποιείται το online εργαλείο **Remix**. Είναι ένα ολοκληρωμένο online περιβάλλον ανάπτυξης για smart contracts, το οποίο δίνει τη δυνατότητα στον χρήστη να δημιουργήσει το δικό του περιβάλλον εργασίας, να διαχειριστεί τα διάφορα συμβόλαια που έχει αναπτύξει, να δημιουργήσει νέα κα. Εκτός από τη διαχείριση αρχείων, το συγκεκριμένο εργαλείο προσφέρει τη δυνατότητα Solidity Compile. Ουσιαστικά, το Remix προσφέρει στο χρήστη ένα τοπικό δίκτυο Ethereum, με πολυάριθμους δοκιμαστικούς λογαριασμούς. Όπως φαίνεται και στην παρακάτω εικόνα, ο κάθε ένας από αυτούς τους λογαριασμούς αντιστοιχεί και σε μια εικονική ποσότητα ether, για την ανάπτυξη του συμβολαίου στο δοκιμαστικό δίκτυο.



Στο παρών συμβόλαιο χρησιμοποιείται η έκδοση της Solidity 0.8.0. Κάθε smart contract ξεκινάει με την αντίστοιχη εντολή η οποία δηλώνει την έκδοση και φαίνεται παρακάτω:

```
pragmasolidity^0.8.0;
```

Πλέον, το επόμενο βήμα είναι να ονομάσουμε το συμβόλαιο που δημιουργήσαμε. Επιλέγουμε το χαρακτηριστικό όνομα:

```
Contract ReputationManagementSystem{
```

Ο κύριος σκοπός της χρήσης του συμβολαίου **ReputationManagementSystem** είναι η ενημέρωση της διαδικτυακής φήμης του εκάστοτε χρήστη, ο υπολογισμός της ύστερα από κάθε νέα βαθμολογία που προκύπτει και η αποθήκευση του βαθμού αυτού στο Blockchain.

Τα mappings στη solidity χρησιμοποιούνται για την αποτελεσματική αποθήκευση και ανάκτηση όγκου δεδομένων βάση κάποιων μοναδικών χαρακτηριστικών. Δηλαδή αντιστοιχίζει κλειδιά συγκεκριμένου τύπου με τιμές διαφορετικού τύπου δεδομένων.

Το συγκεκριμένο mapping αποθηκεύει τις βαθμολογίες του χρήστη.

```
mapping(address =>uint256)public ratings;
```

Το επόμενο mapping κρατάει σε ένα counter τον αριθμό των συνολικών βαθμολογιών που αντιστοιχούν στον χρήστη:

```
mapping(address =>uint256)publicnumRatings;
```

Τέλος, ένα ακόμα mapping χρησιμοποιείται για τη αποθήκευση πληροφοριών σχετικά με τον αν ένας χρήστης έχει υποβάλλει βαθμολογία για κάποιον άλλο χρήστη:

```
mapping(address =>mapping(address =>bool))publichasRated;
```

Το event **NoPreviousRatings** καλείται στην περίπτωση που ο χρήστης δεν έχει λάβει κάποια βαθμολογία μέχρι στιγμής:

```
eventNoPreviousRatings(addressindexed user,string message);
```

Στη συνέχεια, η συνάρτηση **rateUser**, με την οποία γίνεται η υποβολή της βαθμολογίας από έναν χρήστη σε έναν άλλο.

```
functionrateUser(address user,uint8 rating)public{
        require(rating >=1&& rating <=5,"Rating must be between 1 and
5");
        require(user !=msg.sender,"You can't rate yourself");
        require(!hasRated[msg.sender][user],"You have already rated
this user");
```

Βλέπουμε πως υπάρχουν κάποιοι περιορισμοί στην συνάρτηση. Συγκεκριμένα, η βαθμολογία που υποβάλλεται πρέπει να έχει ελάχιστη τιμή το 1 και μέγιστη το 5. Επιπρόσθετα, ο χρήστης δεν έχει τη δυνατότητα να βαθμολογήσει τον εαυτό του.

Τέλος, σε περίπτωση που προσπαθήσει να βαθμολογήσει κάποιον χρήστη για παραπάνω από 1 φορές, λαμβάνει μήνυμα με τη σχετική ειδοποίηση.

```
    if(numRatings[user]==0){

            emitNoPreviousRatings(user,"This user hasn't received any
ratings yet.");
            ratings[user]= rating;
            numRatings[user]=1;
        }else{

            ratings[user]=(ratings[user]*numRatings[user]+
rating)/(numRatings[user]+1);
            numRatings[user]++;
        }
```

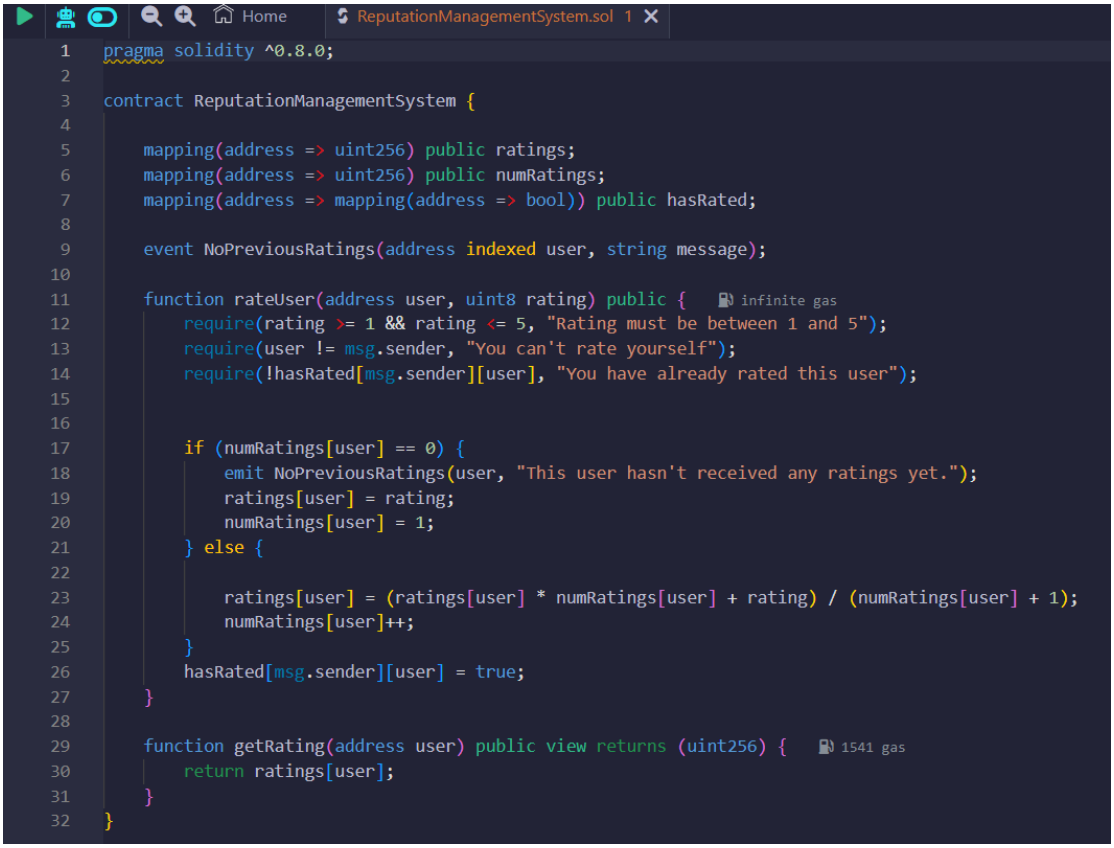
Βλέπουμε επίσης πως σε περίπτωση που αναφέραμε παραπάνω στη οποία ο χρήστης δεν έχει λάβει κάποια βαθμολόγηση στο παρελθόν, ο βαθμολογητής ενημερώνεται με νέο μήνυμα και στη συνέχεια καλείται το event **NoPreviousRatings**.Επειδή προφανώς δεν μπορεί ο παρανομαστής να έχει την τιμή 0, το σύστημα προσδίδει ως αρχική τιμή φήμης του νέου χρήστη το 1.

Η ενημέρωση της βαθμολογίας, η οποία προκύπτει με την πρόσθεση της νέας βαθμολογίας **rating** στο σύνολο των προηγούμενων και στη συνέχεια διαιρείται με τον αριθμό των υποβολών **numRatings**. Με την ολοκλήρωση του υπολογισμού, καταχωρείται πως ο βαθμολογητής έχει υποβάλλει αντίστοιχη βαθμολογία προς τον συγκεκριμένο χρήστη με το **hasRated**:

```
    hasRated[msg.sender][user]=true;
```

Τέλος, με τη συνάρτηση **getRating,** λαμβάνουμε την υπάρχουσα βαθμολογία για έναν συγκεκριμένο χρήστη.

```
functiongetRating(address user)publicviewreturns(uint256){
        returnratings[user];
  }
```



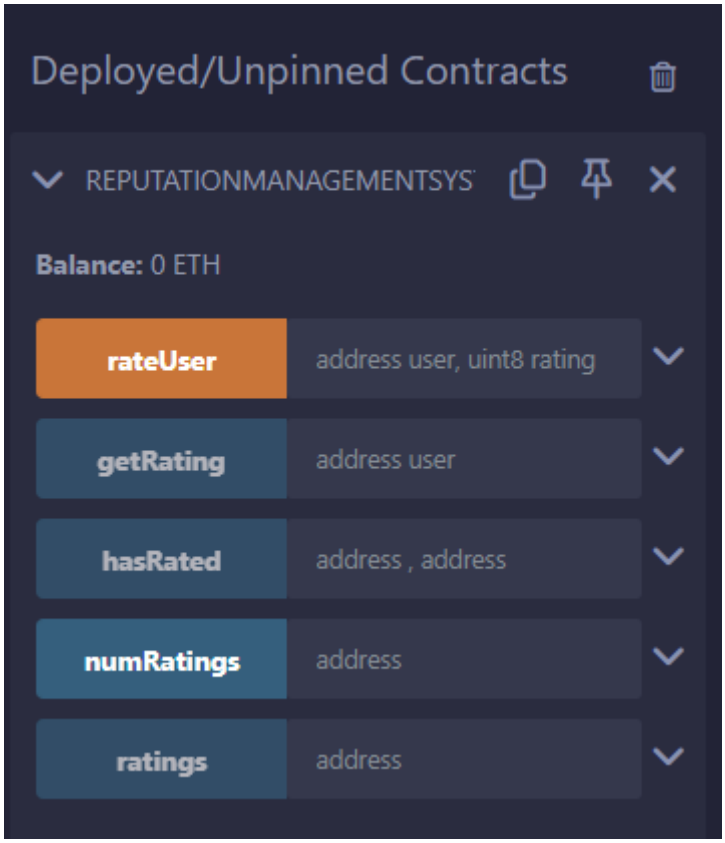
6.2 Η φιλοσοφία του ReputationManagementSystem

Η λογική πίσω από την υλοποίηση του smart contract ReputationManagementSystem είναι η διευκόλυνση της υποβολής αξιολογήσεων μεταξύ των χρηστών σε ένα αποκεντρωμένο περιβάλλον. Ενσωματώνοντας έτσι τα χαρακτηριστικά του MCS αξιοποιείται η συλλογική συμβολή των χρηστών του συστήματος στη διαχείριση της διαδικτυακής φήμης. Το συγκεκριμένο smart contract διασφαλίζει ότι ο κάθε έχει τη δυνατότητα να αξιολογήσει μόνο άλλους χρήστες και όχι τον εαυτό του. Επίσης, δεν έχει τη δυνατότητα να αξιολογήσει κάποιον παραπάνω από μία φορά. Με αυτόν τον τρόπο εξασφαλίζεται η αξιοπιστία της βαθμολόγησης. Όταν υποβάλλεται μια νέα βαθμολόγηση, το συμβόλαιο ενημερώνει την συνολική αξιολόγηση και τον αριθμό των αξιολογήσεων για τον εκάστοτε αξιολογούμενο χρήστη, αρχικοποιώντας τις τιμές αυτές σε περίπτωση που ο χρήστης δεν έχει λάβει αξιολογήσεις στο παρελθόν. Αυτή η προσέγγιση διασφαλίζει ότι οι αξιολογήσεις των χρηστών είναι ακριβείς και διαφανείς.

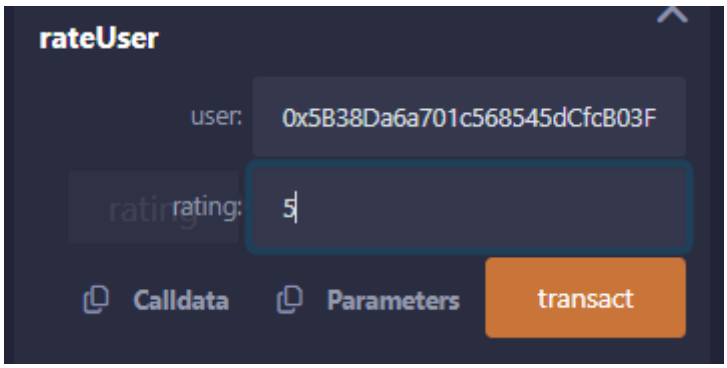
Με την αξιοποίηση της λειτουργίας του MCS, το σύστημα μπορεί να συλλέγει αξιολογήσεις από έναν τεράστιο αριθμό κινητών χρηστών και συσκευών, βελτιώνοντας την αξιοπιστία των δεδομένων. Οι χρήστες ενθαρρύνονται να συμμετέχουν μέσω ανταμοιβών που διαχειρίζεται το έξυπνο συμβόλαιο, προάγοντας την ενεργή συμμετοχή. Αυτό το σύστημα συνδυάζει τη αποκεντρωμένη φύση του blockchain με την εκτεταμένη προσέγγιση των κινητών συσκευών, δημιουργώντας μια ισχυρή και διαφανή πλατφόρμα διαχείρισης φήμης.

Επόμενο βήμα είναι να εκτελέσουμε το ReputationManagementSystem, επιλέγοντας ένα από τα διαθέσιμα address που μας προμηθεύει το Online tool που έχουμε επιλέξει. Φαίνεται από το μήνυμα παρακάτω ότι η προσπάθεια ήταν επιτυχής.

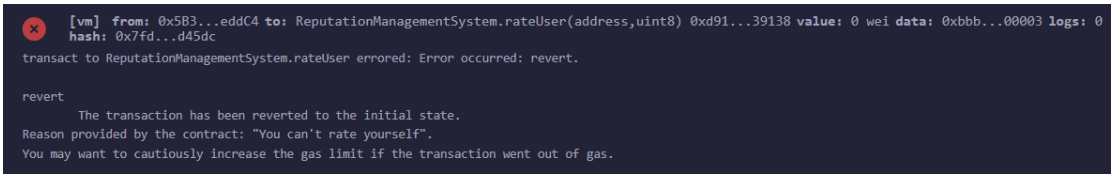
Εφόσον εκτελέσουμε το συμβόλαιο, βλέπουμε ότι εμφανίζονται τα functions με τη μορφή κουμπιών.



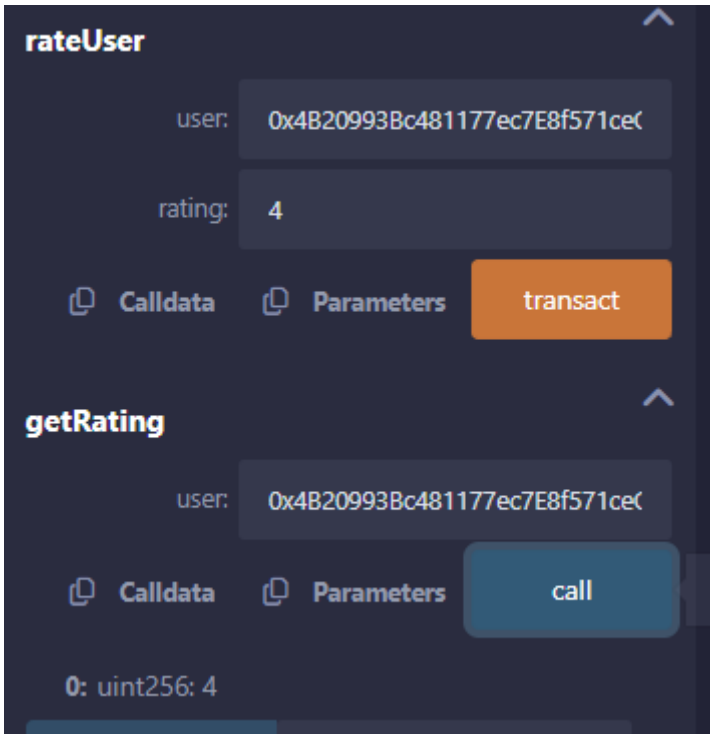
Με μια δοκιμή, χρησιμοποιούμε την address που έχουμε εκτελέσει το συμβόλαιο και δοκιμάζουμε να τη βαθμολογήσουμε με τη χρήση της συνάρτησης rateUser.



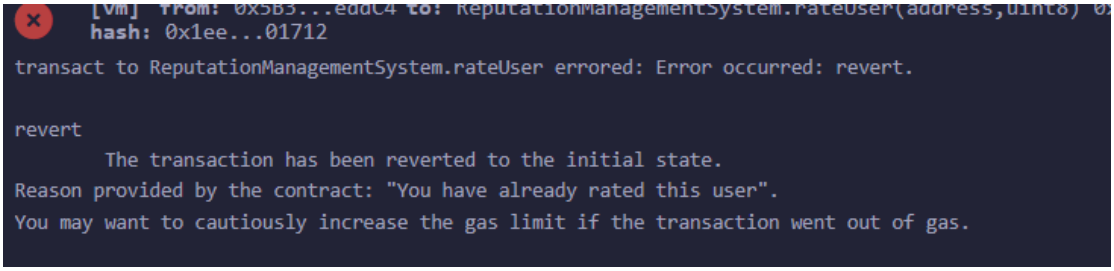
Επειδή σαφώς υπάρχει σχετικός περιορισμός, για τη διατήρηση της αξιοπιστίας των δεδομένων στο MCS το σύστημα δεν εκτελεί την ενέργεια και δεν μας αφήνει να βαθμολογήσουμε ουσιαστικά τον εαυτό μας. Παρακάτω φαίνεται και το σχετικό μήνυμα errorμε τη προειδοποίηση προς τον χρήστη.



Επιλέγοντας μια άλλη address, καλώντας εκ νέου τη συνάρτηση rateUser, βαθμολογούμε με αρχικά με τη τιμή 4 τον χρήστη και στη συνέχεια καλούμε τη συνάρτηση getRating για να μας επιβεβαιώσει τη επιτυχή καταχώρηση.

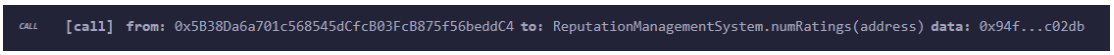


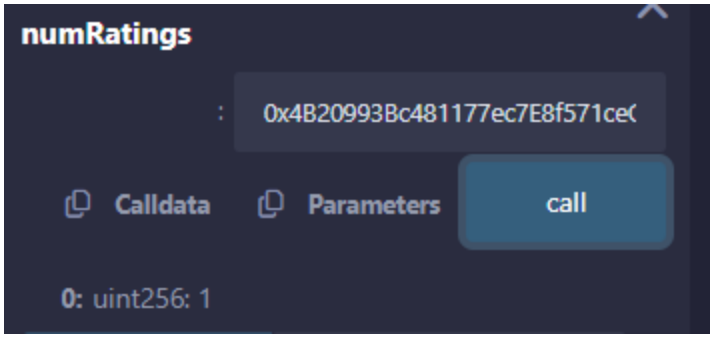
Βλέπουμε ότι η μεταβλητή uint256 έχει όντως πάρει τη τιμή 4. Στη συνέχει αν επιλέξουμε να βαθμολογήσουμε τον ίδιο χρήστη, το σύστημα απορρίπτει τη νέα καταχώρηση, εμφανίζοντας το σχετικό μήνυμα.



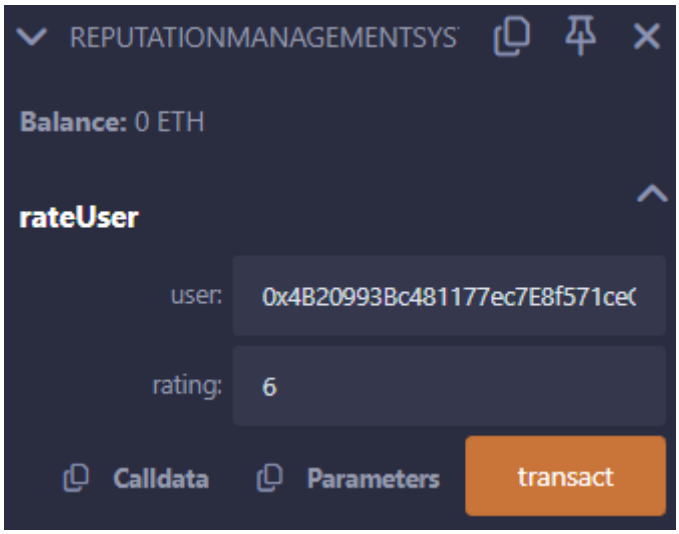
Τέλος, γίνεται και ο σχετικός έλεγχος όταν καλούμε τη συνάρτηση numRatings χρησιμοποιώντας την παραπάνω διεύθυνση, για να επιβεβαιώσουμε ότι γίνεται όντως

η ενημέρωση και αποθήκευση της φήμης και του αριθμού των καταχωρήσεων. Και όντως βλέπουμε ότι ο αριθμός των βαθμολογιών έχει αυξηθεί κατά 1.

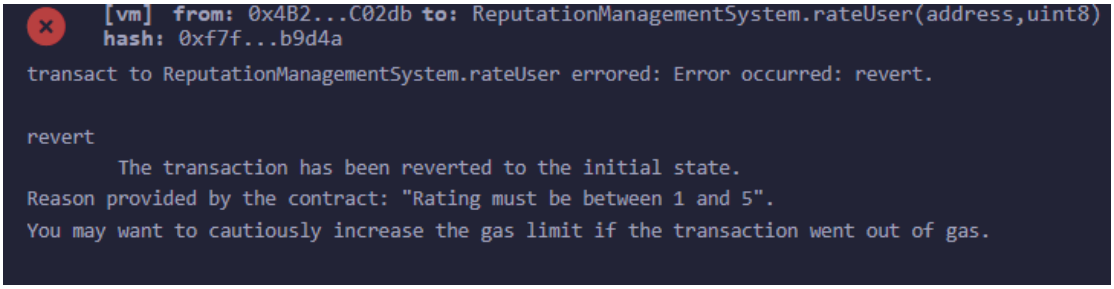




Στη συνέχεια, γίνεται έλεγχος για τις αποδεκτές τιμές που δέχεται ως βαθμολόγηση το σύστημα από τον rater. Δοκιμάζουμε να καταχωρήσουμε μια βαθμολογία που δεν είναι μεταξύ 1 και 5, συγκεκριμένα το 6.



Πράγματι βλέπουμε ότι όταν γίνει η συναλλαγή, το σύστημα εμφανίζει error.



Κεφάλαιο 7 : Επίλογος

Στη παρούσα διπλωματική παρουσιάστηκε εκτενώς η έννοια της συλλογής και ανίχνευσης πληροφοριών με τη χρήση έξυπνων κινητών συσκευών των χρηστών. Έγινε εκτενής αναφορά στα χαρακτηριστικά του MCS, στους τομείς της καθημερινής ζωής των χρηστών που βρίσκει εφαρμογή, καθώς και στα πλεονεκτήματα του, αλλά και στις πιθανές προκλήσεις που καλείται να αντιμετωπίσει.

Στη συνέχεια, παρουσιάζεται η τεχνολογία Blockchain, ως μια πρόταση για την αντιμετώπιση των προκλήσεων στο πλαίσιο εφαρμογής του MCS. Αρχικά γίνεται αναφορά στα χαρακτηριστικά της συγκεκριμένης τεχνολογίας, στην αρχιτεκτονική της και στις κατηγορίες συστημάτων της. Επίσης, αναφέρονται οι διάφοροι αλγόριθμοι που χρησιμοποιούνται από τις διαδεδομένες πλατφόρμες Blockchain ως μηχανισμοί συναίνεσης έτσι ώστε να εξασφαλίσουν την αξιοπιστία του συστήματος, αλλά και διάφοροι τύποι επιθέσεων από κακόβουλους χρήστες. Αναλύονται επιπροσθέτως τα πλεονεκτήματα και τα μειονεκτήματα που ενδέχεται να προκύπτουν από την εφαρμογή της τεχνολογίας αυτής.

Μια ενδεδειγμένη λύση για την εξασφάλιση της εμπιστοσύνης μεταξύ των χρηστών του Blockchain είναι η εφαρμογή των συστημάτων φήμης. Στο αντίστοιχο κεφάλαιο παρουσιάζονται τα κύρια χαρακτηριστικά που διαμορφώνουν τη δομή τους καθώς και συγκεκριμένες περιπτώσεις-παραδείγματα συστημάτων φήμης που εφαρμόζονται σε διάφορους τομείς της καθημερινότητας.

Για τον συνδυασμό των παραπάνω εννοιών, παρουσιάζεται ένα έξυπνο συμβόλαιο σε προγραμματιστική γλώσσα Solidity, ανεπτυγμένο στη Blockchain πλατφόρμα Ethereum, με σκοπό του σε πρώτη βάση την ενημέρωση και αποθήκευση της διαδικτυακής φήμης μεταξύ των χρηστών και έπειτα την εξασφάλιση της αξιοπιστίας των δεδομένων που καταχωρεί ο χρήστης σε αυτό.

Ως μελλοντική επέκταση του συγκεκριμένου έξυπνου συμβολαίου προτείνεται η εξέταση παραγόντων που θα επηρεάζουν την φήμη του χρήστη, όπως το ιστορικό του, ο αριθμός των καταχωρήσεων που έχει πραγματοποιήσει βαθμολογώντας άλλους χρήστες του συστήματος, ακόμα και η επιβράβευση χρηστών που κατέχουν βαθμό φήμης μεγαλύτερης από το μέσο όρο των υπόλοιπων χρηστών και επομένως θεωρούνται αξιόπιστοι.

ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ

1. K. Abualsaud*et al*., "A Survey on Mobile Crowd-Sensing and Its Applications in the IoT Era," in *IEEE Access*, vol. 7, pp. 3855-3881, 2019, doi: 10.1109/ACCESS.2018.2885918.
2. H. Ma, D. Zhao and P. Yuan, "Opportunities in mobile crowd sensing," in *IEEE Communications Magazine*, vol. 52, no. 8, pp. 29-35, Aug. 2014, doi: 10.1109/MCOM.2014.6871666.
3. J. An, X. Gui, J. Yang, S. Yu and X. He, "Mobile Crowd Sensing for Internet of Things: A Credible Crowdsourcing Model in Mobile-Sense Service," *2015 IEEE International Conference on Multimedia Big Data*, 2015, pp. 92-99, doi: 10.1109/BigMM.2015.62.
4. Shu, L.; Chen, Y.; Huo, Z.; Bergmann, N.; Wang, L. When mobile crowd sensing meets traditional industry. IEEE Access 2017, 5, 15300–15307.
5. Pilloni, Virginia. 2018. "How Data Will Transform Industrial Processes: Crowdsensing, Crowdsourcing and Big Data as Pillars of Industry 4.0" *Future Internet* 10, no. 3: 24. https://doi.org/10.3390/fi10030024
6. R. K. Ganti, F. Ye and H. Lei, "Mobile crowdsensing: current state and future challenges," in *IEEE Communications Magazine*, vol. 49, no. 11, pp. 32-39, November 2011, doi: 10.1109/MCOM.2011.6069707.
7. Boubiche, Djallel& Imran, Muhammad & Maqsood, Aneela & Shoaib, Muhammad. (2018). Mobile Crowd Sensing – Taxonomy, Applications, Challenges, and Solutions. Computers in Human Behavior. 101. 10.1016/j.chb.2018.10.028.
8. N. Lane, "Urban Sensing Systems: Opportunistic or Participatory?", *Proc. HotMobile*, pp. 11-16, 2008.
9. M. Srivastava, T. Abdelzaher and B. Szymanski, "Human-centric sensing", *Philos. Trans. Roy. Soc. A Math. Phys. Eng. Sci.*, vol. 370, no. 1958, pp. 176-197, 2012.
10. Bin Guo, Huihui Chen, Wenqian Nan, Zhiwen Yu, Xing Xie, Daqing Zhang, Xingshe Zhou."TaskMe: Toward a Dynamic and Quality-Enhanced Incentive Mechanism for Mobile Crowd Sensing",International Journal of Human Computer Studies, vol. 102, no. 6, 2017, pp. 14-26 (IF: 2.863) (ESI High Citation Paper)
11. Wang, Yufeng & Jia, Xueyu& Jin, Qun & Ma, Jianhua. (2016). Mobile crowdsourcing: Framework, challenges, and solutions. Concurrency and Computation: Practice and Experience. 29. n/a-n/a. 10.1002/cpe.3789.
12. O. Saukh, D. Hasenfratz and L. Thiele, "Route selection for mobile sensor nodes on public transport networks", *J. Ambient Intell. HumanizedComput.*, vol. 5, no. 3, pp. 307-321, Jun. 2014.

13. G. Virone et al., "An Advanced wireless sensor network for health monitoring", *Proc. TransdisciplinaryConf. Distrib. DiagnosisHomeHealthcare*, pp. 95-100, Apr. 2006.
14. K. Abualsaud, M. Mahmuddin, M. Saleh and A. Mohamed, "Ensemble classifier for epileptic seizure detection for imperfect EEG data", *Sci. World J.*, vol. 2015, Dec. 2015.
15. M. A. Hanson, "Wireless body area sensor network technology for motion-based health assessment", Aug. 2009.
16. J. Jin, J. Gubbi, S. Marusic and M. Palaniswami, "An information framework for creating a smart city through Internet of Things", *IEEE Internet Things J.*, vol. 1, no. 2, pp. 112-121, Apr. 2014.
17. A. Zanella, N. Bui, A. Castellani, L. Vangelista and M. Zorzi, "Internet of Things for smart cities", *IEEE Internet Things J.*, vol. 1, no. 1, pp. 22-32, Feb. 2014.
18. T. Ludwig, T. Siebigteroth and V. Pipek, "CrowdMonitor: Monitoring physical and digital activities of citizens during emergencies" in SocInfo, Cham, Switzerland:Springer, vol. 8852, pp. 421-428, 2015.
19. B. Pan, Y. Zheng, D. Wilkie and C. Shahabi, "Crowd sensing of traffic anomalies based on human mobility and social media", *Proc. ACM SIGSPATIAL Int. Conf. Adv. Geograph. Inf. Syst.*, pp. 344-353, Nov. 2013.
20. N. Thepvilojanapong, T. Ono and Y. Tobe, "A deployment of fine-grained sensor network and empirical analysis of urban temperature", *J. Sensors*, vol. 10, no. 3, pp. 2217-2241, 2010.
21. J. Weppner and P. Lukowicz, "Bluetooth based collaborative crowd density estimation with mobile phones", *Proc. IEEE Int. Conf. PervasiveComput. Commun. (PerCom)*, pp. 193-200, Mar. 2013.
22. H. Zhou, J. Chen, J. Fan, Y. Du and S. K. Das, "ConSub: Incentive-based content subscribing in selfish opportunistic mobile networks", *IEEE J. Sel. AreasCommun.*, vol. 31, no. 9, pp. 669-679, Sep. 2013.
23. Y. Xiao, P. Simoens, P. Pillai, K. Ha and M. Satyanarayanan, "Lowering the barriers to large-scale mobile crowdsensing", *Proc. 14th Workshop Mobile Comput. Syst. Appl.*, Feb. 2013.
24. Musthag M, Ganesan D. Labor dynamics in a mobile micro-task market, In Proc. of SIGCHI Conference on Human Factors in Computing Systems, 2013.
25. I. Krontiris and T. Dimitriou, "Privacy-respecting discovery of data providers in crowd-sensing applications", *Proc. of DCoSS*, 2013.
26. P. Rothenpieler, B. Altakrouri, O. Kleine and L. Ruge, "Distributed crowd-sensing infrastructure for personalized dynamic iot spaces", *Proc of URB-IOT*, October 2014.
27. M. Xie, M. Huang, Y. Bai and Z. Hu, "The anonymization protection algorithm based on fuzzy clustering for the ego of data in the Internet of Things", *J. Elect. Comput. Eng.*, vol. 2017, Jun. 2017.
28. M. Shin, C. Cornelius, A. Kapadia, N. Triandopoulos and D. Kotz, "Location privacy for mobile crowd sensing through population mapping", *J. Sensors*, vol. 15, no. 7, pp. 15285-15310, 2015.

29. J. Liu, H. Shen and X. Zhang, "A Survey of Mobile Crowdsensing Techniques: A Critical Component for the Internet of Things," *2016 25th International Conference on Computer Communication and Networks (ICCCN)*, 2016, pp. 1-6, doi: 10.1109/ICCCN.2016.7568484.
30. E. Miluzzo, N. D. Lane, K. Fodor, R. Peterson, H. Lu, M. Musolesi, et al., "Sensing meets mobile social networks: The design implementation and evaluation of the cenceme application", *Proc. of SenSys*, November 2008.
31. B. Guo, Z. Wang, Z. Yu, Y. Wang, N. Y. Yen, R. Huang, et al., "Mobile crowd sensing and computing: The review of an emerging human-powered sensing paradigm", *ACM CSUR*, vol. 48, no. 1, pp. 1-31, Aug. 2015.
32. Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," 2017 IEEE International Congress on Big Data (BigData Congress), 2017, pp. 557-564, doi: 10.1109/BigDataCongress.2017.85.
33. Chen, G., Xu, B., Lu, M. *et al.* Exploring blockchain technology and its potential applications for education. *Smart Learn. Environ.***5,** 1 (2018). https://doi.org/10.1186/s40561-017-0050-x
34. J Yli-Huumo, D Ko, S Choi, S Park, K Smolander, Where is current research on Blockchain technology?—A systematic review. PLoSOne**11**(10), e0163477 (2016) https://doi.org/10.1371/journal.pone.0163477
35. Strebko, Julija & Romanovs, Andrejs. (2018). The Advantages and Disadvantages of the Blockchain Technology. 1-6. 10.1109/AIEEE.2018.8592253.
36. https://data-flair.training/blogs/advantages-and-disadvantages-of-blockchain/
37. Khan, Mohammad & Quasim, Mohammad &Algarni, Fahad & Alharthi, Abdullah. (2020). Decentralised Internet of Things A Blockchain Perspective: A Blockchain Perspective. 10.1007/978-3-030-38677-1.
38. https://www.foley.com/en/insights/publications/2021/08/types-of-blockchain-public-private-between
39. https://selfkey.org/understanding-public-vs-private-blockchain/
40. T. Ncube, N. Dlodlo and A. Terzoli, "Private Blockchain Networks: A Solution for Data Privacy," *2020 2nd International Multidisciplinary Information Technology and Engineering Conference (IMITEC)*, 2020, pp. 1-8, doi: 10.1109/IMITEC50163.2020.9334132.
41. T. Meng, Y. Zhao, K. Wolter and C. -Z. Xu, "On Consortium Blockchain Consistency: A Queueing Network Model Approach," in *IEEE Transactions on Parallel and Distributed Systems*, vol. 32, no. 6, pp. 1369-1382, 1 June 2021, doi: 10.1109/TPDS.2021.3049915.
42. Gupta, Suyash &Sadoghi, Mohammad. (2018). Blockchain Transaction Processing. 10.1007/978-3-319-63962-8_333-1.
43. S. Sayeed and H. Marco-Gisbert, "Assessing Blockchain Consensus and Security Mechanisms against the 51 % Attack", *Applied Sciences*, vol. 9, no. 1788, pp. 1-17, 2019.
44. D. Yaga, P. Mell, N. Roby and K. Scarfone, "Blockchain Technology Overview", *National Institute of Standards and Technology*, 2018.
45. A. Rosie, *Proof of Work vs Proof of Stake: Basic Mining Guide*, 2017.
46. S. De Angelis, L. Aniello, R. Baldoni, F. Lombardo, A. Margheri and V. Sassone, "PBFT vs Proof-of-Authority: Applying the CAP Theorem to Permissioned Blockchain", *Sapienza University of Rome*, 2018.
47. P. Vasin, BlackCoin's Proof of Stake Protocol v2, New York, 2014.

48. M. Castro et al., "Practical Byzantine fault tolerance", *Proc. 3rd Symp. OperatingSyst. Des. Implementation*, pp. 173-186, 1999.
49. W. Li, C. Feng, L. Zhang, H. Xu, B. Cao and M. A. Imran, "A Scalable Multi-Layer PBFT Consensus for Blockchain," in *IEEE Transactions on Parallel and Distributed Systems*, vol. 32, no. 5, pp. 1146-1160, 1 May 2021, doi: 10.1109/TPDS.2020.3042392.
50. H. Sukhwani, J. M. Martinez, X. Chang, K. S. Trivedi and A. Rindos, "Performance modeling of PBFT consensus process for permissioned blockchain network", *Proc. IEEE 36th Symp. ReliableDistrib. Syst.*, pp. 253-255, 2017.
51. A. Panwar and V. Bhatnagar, "Distributed Ledger Technology (DLT): The Beginning of a Technological Revolution for Blockchain," *2nd International Conference on Data, Engineering and Applications (IDEA)*, 2020, pp. 1-5, doi: 10.1109/IDEA49133.2020.9170699.
52. Waldo, Jim. (2019). A hitchhiker's guide to the blockchain universe. Communications of the ACM. 62. 38-42. 10.1145/3303868.
53. Sayeed, Sarwar & Marco-Gisbert, Hector. (2019). Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack. Applied Sciences. 9. 1788. 10.3390/app9091788.
54. N. Anita. and M. Vijayalakshmi., "Blockchain Security Attack: A Brief Survey," *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 2019, pp. 1-6, doi: 10.1109/ICCCNT45670.2019.8944615.
55. A. Singh, T. . -W. Ngan, P. Druschel and D. S. Wallach, "Eclipse Attacks on Overlay Networks: Threats and Defenses," *Proceedings IEEE INFOCOM 2006. 25TH IEEE International Conference on Computer Communications*, 2006, pp. 1-12, doi: 10.1109/INFOCOM.2006.231.
56. R. Alnemr and C. Meinel, "Why rating is not enough: A study on online reputation systems," *7th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom)*, 2011, pp. 415-421, doi: 10.4108/icst.collaboratecom.2011.247145.
57. S. Ruohomaa, L. Kutvonen and E. Koutrouli, "Reputation Management Survey," *The Second International Conference on Availability, Reliability and Security (ARES'07)*, 2007, pp. 103-111, doi: 10.1109/ARES.2007.123.
58. Liu, Ling & Munro, Malcolm. (2012). Systematic analysis of centralized online reputation systems. Decision Support Systems. 52. 438-449. 10.1016/j.dss.2011.10.003.
59. L. Liu, M. Munro, W. Song, *Evaluation of collecting reviews in centralized online reputation systems*, in: 6th International Conference on Web Information Systems and Technologies (WEBIST), 2010, pp. 281–286.
60. Hendrikx, Ferry &Bubendorfer, Kris & Chard, Ryan. (2014). Reputation systems: A survey and taxonomy. Journal of Parallel and Distributed Computing. 75. 10.1016/j.jpdc.2014.08.004.
61. Sabater-Mir, Jordi & Sierra, Carles. (2005). Review on Computational Trust and Reputation Models. Artif. Intell. Rev.. 24. 33-60. 10.1007/s10462-004-0041-5.
62. Koutrouli, Eleni &Tsalgatidou, Aphrodite. (2006). Reputation-Based Trust Systems for P2P Applications: Design Issues and Comparison Framework. 152-161. 10.1007/11824633_16.

63. Kurdi, Heba. (2015). HonestPeer: An Enhanced EigenTrust Algorithm for Reputation Management in P2P Systems. Journal of King Saud University - Computer and Information Sciences. 19. 10.1016/j.jksuci.2014.10.002.
64. Damiani, Ernesto &Vimercati, De &Paraboschi, Stefano &Samarati, Pierangela& Violante, Fabio. (2002). A Reputation-Based Approach for Choosing Reliable Resources in Peer-to-Peer Networks. Proceedings of the ACM Conference on Computer and Communications Security. 10.1145/586110.586138.
65. Kamvar, Sepandar& Schlosser, Mario & Garcia-molina, Hector. (2003). The EigenTrust Algorithm for Reputation Management in P2P Networks. The EigenTrust Algorithm for Reputation Management in P2P Networks.
66. Nishikawa, T., Fujita, S., 2010. An effective risk avoidance scheme for the EigenTrust reputation management system. In Proc. of the First International Conference on Networking and Computing, pp. 36–43.
67. Resnick, Paul. (2002). Trust Among Strangers in Internet Transactions: Empirical Analysis of eBay's Reputation System. Advances in Applied Microeconomics. 11. 10.1016/S0278-0984(02)11030-3.
68. S. Bhattacharjee, N. Ghosh, V. K. Shah and S. K. Das, "QnQ: A reputation model to secure mobile crowdsourcing applications from incentive losses," *2017 IEEE Conference on Communications and Network Security (CNS)*, 2017, pp. 1-9, doi: 10.1109/CNS.2017.8228635
69. R. Huo *et al*., "A Comprehensive Survey on Blockchain in Industrial Internet of Things: Motivations, Research Progresses, and Future Challenges," in *IEEE Communications Surveys & Tutorials*, vol. 24, no. 1, pp. 88-122, Firstquarter 2022, doi: 10.1109/COMST.2022.3141490.
70. Y. Wang and J. Vassileva, "A Review on Trust and Reputation for Web Service Selection," 27th International Conference on Distributed Computing Systems Workshops (ICDCSW'07), 2007, pp. 25-25, doi: 10.1109/ICDCSW.2007.16.
71. J. Arshad, M. A. Azad, A. Prince, J. Ali and T. G. Papaioannou, "REPUTABLE–A Decentralized Reputation System for Blockchain-Based Ecosystems," in IEEE Access, vol. 10, pp. 79948-79961, 2022, doi: 10.1109/ACCESS.2022.3194038.
72. K. Zhao, S. Tang, B. Zhao and Y. Wu, "Dynamic and Privacy-Preserving Reputation Management for Blockchain-Based Mobile Crowdsensing," in *IEEE Access*, vol. 7, pp. 74694-74710, 2019, doi: 10.1109/ACCESS.2019.2920922.
73. H. -T. Wu, Y. Zheng, B. Zhao and J. Hu, "An Anonymous Reputation Management System for Mobile Crowdsensing Based on Dual Blockchain," in IEEE Internet of Things Journal, vol. 9, no. 9, pp. 6956-6968, 1 May1, 2022, doi: 10.1109/JIOT.2021.3113997.
74. W. Zhang, Y. Luo, S. Fu and T. Xie, "Privacy-Preserving Reputation Management for Blockchain-Based Mobile Crowdsensing," 2020 17th Annual IEEE International Conference on Sensing, Communication, and Networking *(SECON)*, Como, Italy, 2020, pp. 1-9, doi: 10.1109/SECON48991.2020.9158420.
75. Ma, Arulprakash&Rethnaraj, Jebakumar. (2021). People-centric collective intelligence: decentralized and enhanced privacy mobile crowd sensing based on blockchain. The Journal of Supercomputing. 77. 10.1007/s11227-021-03756-x.

76. Siddiqui, Shams & Ahmad, Riaz & Shuaib, Mohammed & Alam, Shadab. (2020). Blockchain Security Threats, Attacks and Countermeasures. 10.1007/978-981-15-1518-7_5.
77. Natoli, Christopher & Yu, Jiangshan &Gramoli, Vincent & Veríssimo, Paulo. (2019). Deconstructing Blockchains: A Comprehensive Survey on Consensus, Membership and Structure.
78. Johnstone, D., Bonner, M., & Tate, M. (2004) "Bringing human information behaviour into information systems research: an application of systems modelling" *Information Research*, **9**(4) paper 191 [Available at http://InformationR.net/ir/9-4/paper191.html]
79. Liu, Ling. (2011). Systematic Measurement of Centralized Online Reputation Systems.
80. S. Bhattacharjee, N. Ghosh, V. K. Shah and S. K. Das, "QnQQnQ: Quality and Quantity Based Unified Approach for Secure and Trustworthy Mobile Crowdsensing," in IEEE Transactions on Mobile Computing, vol. 19, no. 1, pp. 200-216, 1 Jan. 2020, doi: 10.1109/TMC.2018.2889458.
81. N. Naik and P. Jenkins, "uPort Open-Source Identity Management System: An Assessment of Self-Sovereign Identity and User-Centric Data Platform Built on Blockchain," 2020 IEEE International Symposium on Systems Engineering (ISSE), Vienna, Austria, 2020, pp. 1-7, doi: 10.1109/ISSE49799.2020.9272223.
82. R. A. Canessane, N. Srinivasan, A. Beuria, A. Singh and B. M. Kumar, "Decentralised Applications Using Ethereum Blockchain," 2019 Fifth International Conference on Science Technology Engineering and Mathematics (ICONSTEM), Chennai, India, 2019, pp. 75-79, doi: 10.1109/ICONSTEM.2019.8918887. keywords: {Contracts;Peer-to-peercomputing;STEM;Electronicvoting;Mathematics;Blockchain;Ethereum;Bitcoin;SmartContracts;Solidity;e-Voting},
83. L. Ma, X. Liu, Q. Pei and Y. Xiang, "Privacy-Preserving Reputation Management for Edge Computing Enhanced Mobile Crowdsensing," in IEEE Transactions on Services Computing, vol. 12, no. 5, pp. 786-799, 1 Sept.-Oct. 2019, doi: 10.1109/TSC.2018.2825986.
84. https://ethereum.org/en/roadmap/
85. Avvenuti, Marco & Bellomo, Salvatore & Cresci, Stefano & La Polla, Mariantonietta& Tesconi, Maurizio. (2017). Hybrid Crowdsensing: A Novel Paradigm to Combine the Strengths of Opportunistic and Participatory Crowdsensing.
86. T. Luo, J. Huang, S. S. Kanhere, J. Zhang and S. K. Das, "Improving IoT Data Quality in Mobile Crowd Sensing: A Cross Validation Approach," in IEEE Internet of Things Journal, vol. 6, no. 3, pp. 5651-5664, June 2019, doi: 10.1109/JIOT.2019.2904704.
87. H. Liu, X. Luo, H. Liu and X. Xia, "Merkle Tree: A Fundamental Component of Blockchains," 2021 International Conference on Electronic Information Engineering and Computer Science (EIECS), Changchun, China, 2021, pp. 556-561, doi: 10.1109/EIECS53707.2021.9588047. keywords: {Computer science;Authentication;Binarytrees;Educationaltechnology;Tools;Datastructures;Blockchains;Merkletree;Hashfunctions;Blockchain;Bitcoin},
88. J. Golosova and A. Romanovs, "The Advantages and Disadvantages of the Blockchain Technology," 2018 IEEE 6th Workshop on Advances in

Information, Electronic and Electrical Engineering (AIEEE), Vilnius, Lithuania, 2018, pp. 1-6, doi: 10.1109/AIEEE.2018.8592253. keywords: {Blockchain;Smartcontracts;Databases;Supplychains;Security;Government;Blockchaintechnology;industrialcases;Blockchain implementation success factors},
89. https://www.ibm.com/topics/benefits-of-blockchain
90. https://academy.bsvblockchain.org/blog/11-benefits-of-blockchain-technology
91. V. Allombert, M. Bourgoin and J. Tesson, "Introduction to the Tezos Blockchain," 2019 International Conference on High Performance Computing & Simulation (HPCS), Dublin, Ireland, 2019, pp. 1-10, doi: 10.1109/HPCS48598.2019.9188227. Z. Zhao, "Comparison of Hyperledger Fabric and Ethereum Blockchain," 2022 IEEE Asia-Pacific Conference on Image Processing, Electronics and Computers (IPEC), Dalian, China, 2022, pp. 584-587, doi: 10.1109/IPEC54454.2022.9777292.
92. Z. Zhao, "Comparison of Hyperledger Fabric and Ethereum Blockchain," 2022 IEEE Asia-Pacific Conference on Image Processing, Electronics and Computers (IPEC), Dalian, China, 2022, pp. 584-587, doi: 10.1109/IPEC54454.2022.9777292.
93. https://101blockchains.com/best-blockchain-development-platforms/
94. Zhang, Jialin & Li, Xianxian & Shi, Zhenkui & Zhu, Cong. (2022). A reputation-based and privacy-preserving incentive scheme for mobile crowd sensing: a deep reinforcement learning approach. Wireless Networks. 10.1007/s11276-022-03111-9.
95. Zhang, Heng & Bagchi, Saurabh & Wang, He. (2017). Integrity of Data in a Mobile Crowdsensing Campaign: A Case Study. 50-55. 10.1145/3139243.3139255.
96. https://cryptowallet.com/glossary/off-chain/
97. M. M. Haque, S. Kumer Paul, R. R. Paul, M. Ekramul Hamid, S. Fahim and S. Islam, "A Comprehensive Study on Ethereum Blockchain-based Digital Marketplace using NFT Smart Contract Infrastructure," 2022 25th International Conference on Computer and Information Technology (ICCIT), Cox's Bazar, Bangladesh, 2022, pp. 348-353, doi: 10.1109/ICCIT57492.2022.10056108.
98. https://opentezos.com/tezos-basics/liquid-proof-of-stake/