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

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

# Μελέτη Μηχανισμών Ψηφοφορίας στο Blockchain και Ανάπτυξη Αποκεντρωμένης Εφαρμογής Ψηφοφορίας στο Private Ethereum Blockchain

**Ορέστης Α. Αλμπανούδης**

**Επιβλέπων**:
Δημήτριος Ασκούνης,
Καθηγητής ΕΜΠ

Αθήνα, Οκτώβριος 2020

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

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

# Μελέτη Μηχανισμών Ψηφοφορίας στο Blockchain και Ανάπτυξη Αποκεντρωμένης Εφαρμογής Ψηφοφορίας στο Private Ethereum Blockchain

**Ορέστης Α. Αλμπανούδης**

**Επιβλέπων**:
Δημήτριος Ασκούνης,
Καθηγητής ΕΜΠ

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 19η Οκτωβρίου 2020.

| ..... | ..... | ..... |
|---|---|---|
| Δημήτριος Ασκούνης | Ιωάννης Ψαρράς | Χάρης Δούκας |
| Καθηγητής Ε.Μ.Π. | Καθηγητής Ε.Μ.Π. | Αν. Καθηγητής Ε.Μ.Π. |

Αθήνα, Οκτώβριος 2020

Ορέστης Α. Αλμπανούδης

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

# Περίληψη

Η διεξαγωγή ψηφοφορίας θεωρούταν ανέκαθεν η πρωταρχική δημοκρατική μέθοδος που χρησιμοποιείται για την επίσημη έκφραση των απόψεων ενός κοινωνικού συνόλου σχετικά με κάποιο αμφιλεγόμενο θέμα η για την εκλογή κάποιου αντιπροσώπου. Με στόχο την μεγιστοποίηση της ασφάλειας και την ελαχιστοποίηση του κόστους διεξαγωγής εκλογών, η επιστήμη των αποκεντρωμένων κατανεμημένων δικτύων έχει εισαγάγει και προτείνει μεθόδους ώστε να καταστεί το σύστημα ηλεκτρονικής ψηφοφορίας ασφαλές.

Η εφαρμογή κατανεμημένων ψηφιακών συστημάτων ψηφοφορίας για λόγους εμπιστοσύνης, οικονομίας, ταχύτητας, ευκολίας και προστασίας των δεδομένων αποτελεί επιτακτική πρόκληση των σύγχρονων κοινωνιών. Αρχικά, στο πλαίσιο της παρούσας διπλωματικής, αναδεικνύουμε τα επίπεδα διακυβέρνησης μιας αποκεντρωμένης εφαρμογής. Έπειτα, ερευνούμε την διακυβέρνηση των αποκεντρωμένων συστημάτων και την διακρίνουμε σε ‘διακυβέρνηση της υποδομής’ και σε ‘διακυβέρνηση από την υποδομή’.

Έπειτα, αξιολογούμε μερικά από τα δημοφιλή πλαίσια ψηφοφορίας blockchain ως προς την εξυπηρέτηση των απαιτήσεων ενός συστήματος ψηφοφορίας.

Στη συνέχεια αναλύουμε διεξοδικά την λειτουργία και τα βασικά χαρακτηριστικά του Ethereum Blockchain Network και αναδεικνύουμε την καταλληλόλητα του για ανάπτυξη αποκεντρωμένων εφαρμογών.

Τέλος αναπτύσσουμε ένα ηλεκτρονικό σύστημα ψηφοφορίας βασισμένο στο Ethereum blockchain με στόχο να περιγράψουμε τα βασικά εργαλεία ανάπτυξης αποκεντρωμένων εφαρμογών και αξιολογούμε την τεχνολογία του blockchain ως υπηρεσία για την εφαρμογή κατανεμημένων ηλεκτρονικών συστημάτων ψηφοφορίας.

**Λέξεις κλειδιά:** Blockchain Voting, Decentralized Applications, On chain & Off chain Governance, Ethereum Blockchain, Ασφάλεια, GDPR

# Abstract

Voting has always been considered the primary democratic method used to formally express the views of a social group on a controversial issue. In order to maximize security and minimize the cost of conducting elections, the science of decentralized distributed networks has introduced and proposed methods to make the electronic voting system secure.

The implementation of distributed digital voting systems for reasons of trust, economy, speed, convenience and data protection is an urgent challenge in modern societies. At first, we point out the different levels of governance in Decentralised Applications.Then we analyse the governance of decentralized systems and distinguish the terms of ‘governance by infrastructure’ and of ‘governance of infrastructure’.

We evaluate some of the popular blockchain voting frameworks in terms of meeting the requirements of a voting system.

Furthermore, we analyze in detail the function and the basic features of Ethereum Blockchain Network and highlight its suitability for development of decentralized applications

Finally, we develop an electronic voting system based on Ethereum blockchain in order to describe the basic tools for the development of decentralized applications and evaluate the technology of blockchain as a service for the implementation of distributed electronic voting systems.

Keywords: Blockchain Voting, Decentralized Applications, On chain & Off chain Governance Ethereum Blockchain, Security, GDPR,

# Ευχαριστίες

Η παρούσα διπλωματική εργασία εκπονήθηκε στον τομέα Συστημάτων Αποφάσεων και Διοίκησης του τομέα Ηλεκτρικών Βιομηχανικών Διατάξεων και Συστημάτων Αποφάσεων της Σχολής Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Εθνικού Μετσόβιου Πολυτεχνείου.

Με την ολοκλήρωση της διπλωματικής μου εργασίας θα ήθελα να ευχαριστήσω θερμά σύσσωμη την τριμελή εξεταστική επιτροπή και ιδιαιτέρως τον καθηγητή κ. Ασκούνη Δημήτριο, για την επίβλεψη της παρούσας διπλωματικής εργασίας και για την ευκαιρία που μου έδωσε να ασχοληθώ με ένα τόσο ενδιαφέρον επιστημονικό πεδίο.

Ιδιαιτέρως θα ήθελα να ευχαριστήσω τον υποψήφιο διδάκτορα του εργαστηρίου Συστημάτων Αποφάσεων & Διοίκησης κ. Χρήστο Κοντζίνο, ο οποίος από την πρώτη στιγμή μου παρείχε τις κατάλληλες κατευθύνσεις, προκειμένου να επιτευχθεί το επιθυμητό αποτέλεσμα.

Κλείνοντας θα ήθελα να ευχαριστήσω την οικογένεια και τους φίλους μου για την υποστήριξή τους όλα αυτά τα χρόνια.

# Περιεχόμενα

# Πίνακας Σχημάτων

# 1. Εισαγωγή

## 1.1. Σκοπός

Η διεξαγωγή ψηφοφορίας θεωρούταν ανέκαθεν η πρωταρχική δημοκρατική μέθοδος που χρησιμοποιείται για την επίσημη έκφραση των απόψεων ενός κοινωνικού συνόλου σχετικά με κάποιο αμφιλεγόμενο θέμα ή συζήτηση όπως τα δημοψηφίσματα, η εκλογή πολιτικών εκπροσώπων και πολιτικών κομμάτων. Σε κάθε δημοκρατία, η ασφάλεια των εκλογών είναι θέμα εθνικής ασφάλειας. Επί σειρά δεκαετιών, οι δημοκρατικές εκλογές υποψηφίων βασίζονται στο παραδοσιακό σύστημα ψηφοφορίας με στυλό και χαρτί. Το σύστημα αυτό, ωστόσο, δεν εξασφαλίζει την ιχνηλασιμότητα και επαληθευσιμότητα της διαδικασίας. Επιπλέον οι κεντρικά ελεγχόμενες εκλογικές διαδικασίες και τα αποτελέσματα αυτών αμφισβητούνται από τους ψηφοφόρους.

Με στόχο την μεγιστοποίηση της ασφάλειας και την ελαχιστοποίηση του κόστους διεξαγωγής εκλογών, η επιστήμη των υπολογιστών έχει εισαγάγει και προτείνει μεθόδους ώστε να καταστεί το σύστημα ηλεκτρονικής ψηφοφορίας πιο ασφαλές.

Τα περισσότερα υπάρχοντα συστήματα ηλεκτρονικής ψηφοφορίας έχουν κατηγορηθεί από την κοινότητα κυρίως για ζητήματα φυσικής ασφάλειας, καθώς βασίζονται σε κεντρικούς διακομιστές όπου οι ψηφοφόροι οφείλουν να εμπιστεύονται την κεντρική οργανωτική αρχή (authority) αναφορικά με την ακεραιότητα των αποτελεσμάτων. Αυτός είναι και ο βασικός λόγος που, ως σήμερα, δεν έχουν επικρατήσει ανάλογες διαδικασίες ηλεκτρονικής ψηφοφορίας. Οποιοσδήποτε έχει φυσική πρόσβαση στον κεντρικό διακομιστή μπορεί να πάρει τον έλεγχο ή να αλλοιώσει τις ψήφους, ακυρώνοντας ουσιαστικά την εκλογική διαδικασία. Στο πλαίσιο αυτής της εργασίας, προτείνεται μια αποκεντρωμένη πλατφόρμα ηλεκτρονικής ψηφοφορίας που βασίζεται στο Ethereum Blockchain.

Η εφαρμογή κατανεμημένων ψηφιακών συστημάτων ψηφοφορίας για λόγους εμπιστοσύνης, οικονομίας, ταχύτητας και ευκολίας αποτελεί επιτακτική πρόκληση των σύγχρονων κοινωνιών. Τα κατανεμημένα συστήματα αποτελούν μια τεχνολογική εξέλιξη στον κόσμο της πληροφορικής, στην οποία στηρίχτηκαν οι τεχνολογίες Blockchain με στόχο να προσφέρουν ένα ευρύ φάσμα εφαρμογών που επωφελούνται από την οικονομία διαμοιρασμού. Εδώ αξιολογούμε την εφαρμογή του blockchain ως υπηρεσία για την εφαρμογή κατανεμημένων ηλεκτρονικών συστημάτων ψηφοφορίας. Αξιολογούμε μερικά από τα δημοφιλή πλαίσια blockchain που προσφέρουν blockchain ως υπηρεσία. Στη συνέχεια προτείνουμε ένα ηλεκτρονικό σύστημα ψηφοφορίας βασισμένο σε blockchain που αντιμετωπίζει κάποιους περιορισμούς. Τα κύρια χαρακτηριστικά αυτού του συστήματος περιλαμβάνουν τη διασφάλιση της ακεραιότητας και της διαφάνειας των δεδομένων, και την διασφαλισμένη κατοχύρωση μίας ψήφου για κάθε ψηφοφόρο με εξασφαλισμένο απόρρητο, ασφάλεια και μείωση του κόστους διοργάνωσης ψηφοφορίας. Για να επιτευχθεί αυτό, η Εικονική Μηχανή Ethereum (EVM) χρησιμοποιείται ως το περιβάλλον εκτέλεσης Blockchain, στο οποίο θα διοργανωθούν διαφανείς, συνεπείς και ντετερμινιστικές έξυπνες συμβάσεις, τα αποκαλούμενα smart contracts για την εκτέλεση των προσαρμοσμένων κανόνων ψηφοφορίας σε κάθε διαδικασία ψηφοφορίας.

Η τεχνολογία blockchain προσφέρει αυξημένο επίπεδο ασφαλείας, κατά πολλούς το μέγιστο που έχει παράσχει οποιαδήποτε μορφή βάσης δεδομενων ως σήμερα, λόγω των αλγορίθμων προηγμένης κρυπτογραφίας. Ως εκ τούτου, θεωρείται από πολλούς ως το ιδανικό εργαλείο για τη δημιουργία ενός νέου σύγχρονου δημοκρατικού συστήματος ηλεκτρονικής ψηφοφορίας. Στη παρούσα εργασία, αξιολογούμε τη χρήση του blockchain ως υπηρεσία εφαρμογής συστήματος ηλεκτρονικής ψηφοφορίας.

## 1.2 Δομή Εργασίας

Στο δεύτερο κεφάλαιο, θα κάνουμε μια σύντομη εισαγωγή στο blockchain, θα περιγράψουμε τις βασικές αρχές του Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων και θα διαπιστώσουμε τρόπους συμμόρφωσης της τεχνολογίας blockchain στον GDPR.

Στο τρίτο κεφάλαιο, θα εξηγήσουμε την διαφορά μεταξύ κεντρικών και αποκεντρωμένων δικτύων και θα μελετήσουμε δείκτες αποκεντροποίησης που εμφανίζονται στην βιβλιογραφία. Στη συνέχεια θα περιγράψουμε τα διάφορα επίπεδα διακυβέρνησης στα αποκεντρωμένα δίκτυα και θα διακρίνουμε τον όρο «διακυβέρνηση της υποδομή» από τον όρο «διακυβέρνηση από την υποδομή».

Στο τέταρτο κεφάλαιο θα ορίσουμε την ψηφιακή ψηφοφορία και τις αρχές από τις οποίες αυτή διέπεται. Θα παρουσιάσουμε τις βασικές ερευνητικές προσεγγίσεις και τα βασικά ζητήματα που προκύπτουν από αυτές.

Στο πέμπτο κεφάλαιο, θα κάνουμε μια αναλυτική παρουσίαση του τρόπου λειτουργίας του Ethereum και θα ορίσουμε την αρχιτεκτονική των αποκεντρωμένων εφαρμογών.

Στο έκτο κεφάλαιο, θα ασχοληθούμε με την ανάπτυξη της αποκεντρωμένης εφαρμογής και θα παρουσιάσουμε τα έξυπνα συμβόλαια και τις άλλες παραμέτρους του συστήματος.

Στο έβδομο κεφάλαιο, θα παρουσιάσουμε τα βήματα πίσω από την ανάπτυξη της εφαρμογής καθώς επίσης και τα εργαλεία που χρησιμοποιήθηκαν. Επίσης θα παραθέσουμε τον κώδικα που χρησιμοποιήθηκε.

Στο όγδοο και τελευταίο κεφάλαιο, θα παρουσιάσουμε τα συμπεράσματα από την μελέτη αυτή και τις μελλοντικές προοπτικές.

# 2 .Θεωρητικό Υπόβαθρο

## 2.1 Εισαγωγή στο blockchain

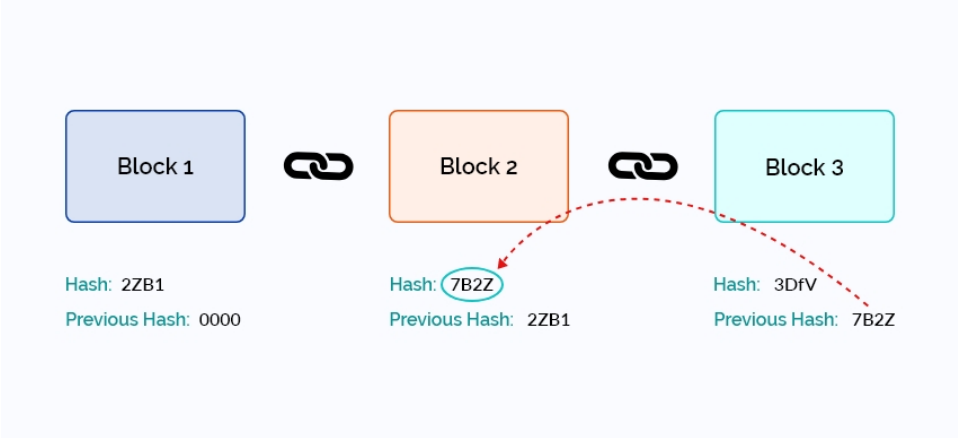
### 2.1.1 Ορισμός

Το blockchain είναι μια συνεχώς αυξανόμενη λίστα από αρχεία, καθένα από τα οποία ειναι συνδεδεμένο με το προηγούμενο. Τα αρχεία αυτά ονομάζονται blocks και η σύνδεση τους επιτυγχάνεται με συγκεκριμένες μεθόδους κρυπτογράφησης ούτως ώστε κάθε μπλοκ να περιέχει έναν κρυπτογραφημένο κατακερματισμό (cryptographic hash) του προηγούμενου του. Τα blocks ενός blockchain δεν αποθηκεύονται σε μια κεντρική βάση δεδομένων, αλλά διανέμονται σε έναν αριθμό από κατανεμημένους peer-to-peer κόμβους (nodes) ενός δικτύου (network). Με τον τρόπο αυτό, δίνεται η δυνατότητα σε χρήστες ανεξαρτήτου θέσεως που πιθανόν να μην έχουν επικοινωνήσει ποτέ μεταξύ τους να κάνουν κάποια «διομότιμη» (peer-to-peer) συναλλαγή χωρίς την ανάγκη ύπαρξης κάποιας κεντρικής διαχειριστικής αρχή, η οποία είναι υπεύθυνη για την επικύρωση και την επαλήθευση των συναλλαγών.

Κάθε block περιέχει μεταξύ άλλων τα εξής:

- το hash του block
- το hash του προηγούμενου block
- μία χρονοσφραγίδα (timestamp) που υποδεικνύει πότε δημιουργήθηκε το block και
- τα δεδομένα που σχετίζονται με την εφαρμογή στην οποία χρησιμοποιείται το blockchain.

Για παράδειγμα, τα δεδομένα στο blockchain κάποιου κρυπτονομίσματος είναι δεδομένα συναλλαγών τα οποία αποθηκεύονται συνήθως σαν ένα Merkle Tree. Για την δημιουργία ενός blockchain απαιτείται να δημιουργηθεί το πρώτο block, που ονομάζεται genesis block. Το genesis block, ως πρώτο block, είναι το μοναδικό που δεν περιέχει το κρυπτογραφημένο κατακερματισμό του προηγούμενού του. Το hash του κάθε block αποτελεί την αναπαράσταση των δεδομένων του block και δημιουργείται μέσω της χρήσης κρυπτογραφικών συναρτήσεων κατακερματισμού (hash functions). Συνεπώς, το hash κάθε block εξαρτάται άμεσα από τα δεδομένα, γεγονός που το καθιστά ικανό να επαληθεύει την ακεραιότητα των συναλλαγών (transactions) που περιέχονται στο εκάστοτε block. Επιπλέον, το hash κάθε block εξαρτάται και από το hash του προηγούμενου σε σειρά block, γεγονός που εξασφαλίζει ότι το blockchain είναι αμετάβλητο, καθώς η παραποίηση ενός block συνεπάγεται την αλλαγή του hash του συγκεκριμένου block και άρα και των hashes όλων των επόμενων blocks.Στην παρακάτω εικόνα παρουσιάζεται σχηματικά η δομή ενός blockchain.



Σχήμα 1: Η δομή ενός blockchain

Η νέα αυτή τεχνολογία διαφοροποιείται σε σχέση με τις υπάρχουσες τεχνολογίες ως προς την αρχή ότι τα δεδομένα δεν αποθηκεύονται σε ένα μόνο κεντρικό αποθετήριο και ότι δεν απαιτείται κεντρικό σημείο διαχείρισης και ελέγχου. Αντί της κεντρικής αποθήκευσης και διαχείρισης, η Blockchain τεχνολογία βασίζεται στην αρχή ότι μοιράζεται σε ολόκληρο το δίκτυο ένας κατάλογος (Blockchain ledger) με τις πλήρεις συναλλαγές/δραστηριότητες και η διαχείριση των συναλλαγών/δραστηριοτήτων βασίζεται στην κατανεμημένη μορφή του δικτύου. Καθίσταται, με τον τρόπο αυτό, αδύνατη η αλλοίωση ή η κλοπή δεδομένων από τρίτους και δημιουργείται εμπιστοσύνη μεταξύ των κόμβων του δικτύου.

Για παράδειγμα, στο Bitcoin, δεδομένου ότι τα πορτοφόλια είναι σε κατανεμημένη δομή, η συνολική ποσότητα κερμάτων και ο άμεσος όγκος συναλλαγών στον κόσμο μπορούν να ακολουθηθούν στιγμιαία και με σαφήνεια. Δεν υπάρχει ανάγκη κεντρικής αρχής να εγκρίνει ή να ολοκληρώσει τις διαδικασίες σε αυτό το σύστημα που βασίζεται σε P2P συνδέσεις. Το Bitcoin αποτελεί μία από τις πρώτες μεγάλες υλοποιήσεις αποκεντρωμένου συστήματος. Σε ένα τέτοιο σύστημα, οι χρήστες έχουν τη δυνατότητα να αναδιοργανώσουν κάθε είδους δραστηριότητα λόγω της δυνατότητας τους να αλληλεπιδρούν χωρίς τριβές με τρίτους μεσολαβητές και με έμπιστο τρόπο.

Η επικύρωση και η επαλήθευση οποιαδήποτε συναλλαγής του blockchain επαφίεται στο συναινετικό πρωτόκολλο, το οποίο αποτελεί βασικό μέρος κάθε δικτύου blockchain και είναι υπεύθυνο για τη διατήρηση της ακεραιότητας του ιστορικού των συναλλαγών στο σύστημα. Ένας αλγόριθμος συναίνεσης (consensus algorithm) είναι μία διαδικασία μέσω της οποίας όλοι οι κόμβοι ενός δικτύου καταλήγουν σε μία συμφωνία για την παρούσα κατάσταση του κατανεμημένου blockchain. Δηλαδή οι μηχανισμοί συναίνεσης εξασφαλίζουν ότι όλοι οι μη-ελαττωματικοί χρήστες του δικτύου εκτελούν τις ίδιες ανανεώσεις κατάστασης του συστήματος με τη σειρά που συνέβησαν τα γεγονότα που άλλαξαν την κατάστασή του.

### 2.1.2 Ιστορία του blockchain

Η πρώτη φορά που παρουσιάστηκε η ιδέα του blockchain ήταν το 1991, όταν οι ερευνητές Stuart Haber και ο W. Scott Stornetta, παρουσίασαν μια λύση στο πρόβλημα ψηφιακών δεδομένων με χρονοσφραγίδες. Συγκεκριμένα, η έρευνα τους βασίστηκε στην διατήρηση της ασφάλειας των δεδομένων και της χρονικής σειράς αυτών χωρίς δυνατότητα αλλοίωσης. Έτσι, δημιούργησαν μια κρυπτογραφημένη αλυσίδα από blocks, κάθε ένα εκ των οποίων περιείχε ένα χρονοσφραγισμένο ψηφιακό έγγραφο. Το 1992, με την χρήση των Merkle trees, κάθε block ήταν δυνατό να περιέχει περισσότερα του ενός ψηφιακά έγγραφα.

Ωστόσο, η τεχνολογία αυτή δεν χρησιμοποιήθηκε και δεν υπήρξε κάποιο περαιτέρω ανάπτυξη της πρώτης αυτής μορφής του blockchain ως το 2004, όταν ο Harold Thomas Finney, δημιούργησε το RPoW (Reusable Proof of Work) με σκοπό να αντιμετωπίσει το πρόβλημα της διπλής σπατάλης [1].

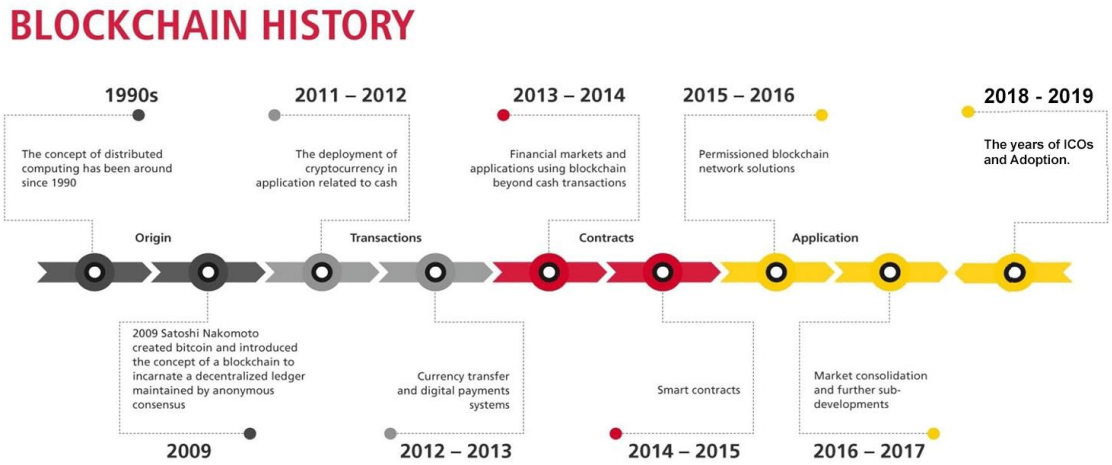
Συνοπτικά, το πρόβλημα της διπλή σπατάλης έγκειται στην περίπτωση όπου ένα ψηφιακό αντικείμενο αξίας μπορεί να σπαταληθεί παραπάνω από μία φορά. Συγκεκριμένα, το σύστημα λάμβανε ως είσοδο ένα μη ανταλλάξιμο Hash-Cash token βασιζόμενο στην απόδειξη εργασίας (proof of work) και δημιουργούσε ένα άλλο ανταλλάξιμο και κρυπτογραφικά υπογεγραμμένο (RSA-signed) token. Το RPoW ήταν το πρώτο σύστημα του οποίου το πρωτόκολλο ασφάλειας, βασίζεται σε αρχές παρόμοιες με το σημερινό blockchain καθώς όλοι οι χρήστες μπορούσαν να επαληθεύσουν την ορθότητα και ακεραιότητα μιας πραγματικής συναλλαγής μέσω ενός ασφαλούς server.

Στα τέλη του 2008, δημοσιεύτηκε ένα 'white paper', το οποίο εισήγαγε ένα αποκεντρωμένο διομότιμο (peer-to-peer) ηλεκτρονικό χρηματικό σύστημα το Bitcoin, υπογεγραμμένο με το ψευδώνυμο 'Satoshi Nakamoto'. Βασιζόταν στον αλγόριθμο του RPoW, με τη διαφοροποίηση ότι το πρόβλημα της διπλής σπατάλης αντιμετωπίζεται μέσω ενός αποκεντρωμένου διομότιμου πρωτοκόλλου, αντί ενός server.

Το πρώτο block (genesis block) δημιουργήθηκε από τον/την/τους 'Satoshi Nakamoto' στις 9 Ιανουαρίου του 2009, το οποίο είχε έπαθλο 50 Bitcoin. Στις 12 Ιανουαρίου του 2009, ο Harold Thomas Finney, ο δημιουργός του RPoW ήταν ο πρώτος αγοραστής καθώς αγόρασε από τον/την/τους 'Satoshi Nakamoto' 10 Bitcoins. Αυτή ήταν η πρώτη συναλλαγή κρυπτονομίσματος στην ιστορία.

Στην αρχή, το Blockchain σχεδιάστηκε μόνο για νομισματικές συναλλαγές και εμπόριο, αλλά γρήγορα οι μελέτες έδειξαν ότι μπορεί να χρησιμοποιηθεί σε περισσότερους τομείς με την πάροδο του χρόνου, λόγω του υψηλού βαθμού διαφάνειας. Μπορούν να καταγραφούν πολλές πληροφορίες σε αυτή την κατανεμημένη αλυσίδα με σχετικές τροποποιήσεις. Για παράδειγμα, όλα τα είδη διαρθρωτικών πληροφοριών, όπως τα στοιχεία του ενεργητικού των ανθρώπων, τα δημόσια πιστοποιητικά, τα βιβλία τραπεζικών λογαριασμών, οι ιατρικές πληροφορίες μπορούν να διατηρηθούν με ασφάλεια λόγω της χρήσης ορισμένων μεθόδων κρυπτογράφησης [2].

Το 2013, ο συνιδρυτής του περιοδικού 'Bitcoin Magazine', Vitalic Buterin, ισχυρίστηκε ότι το Bitcoin χρειάζεται κάποια βοηθητική γλώσσα προγραμματισμού, ώστε να καθίσταται δυνατή στους διάφορους προγραμματιστές η δημιουργία Αποκεντρωμένων Εφαρμογών, δηλαδή Decentralized Applications (DAPPS).[2] Λόγω, όμως, του ότι δεν κατάφερε να έρθει σε συμφωνία με την υπόλοιπη κοινότητα, ξεκίνησε με τη βοήθεια του Anthony Di Iorio και κάποιων επενδυτών, την ανάπτυξη ενός άλλου κρυπτονομίσματος, βασιζόμενου και πάλι στο blockchain, του Ethereum. Εισήγαγε ένα καινούριο χαρακτηριστικό, τα λεγόμενα έξυπνα συμβόλαια (smart contracts), δηλαδή προγράμματα τα οποία αναπτύσσονται και εκτελούνται στο ίδιο το Ethereum Blockchain. Μέσω των έξυπνων συμβολαίων ο δρόμος για τη δημιουργία DAPPS άνοιξε για τα καλά. Περισσότερες πληροφορίες για τα έξυπνα συμβόλαια (smart contracts), καθώς και για τις αποκεντρωμένες εφαρμογές (DAPPS) δίνονται σε επόμενη ενότητα. Συνεχώς δημιουργούνται νέα κρυπτονομίσματα βασιζόμενα στο blockchain, ενώ το blockchain χρησιμοποιείται ευρέως ολοένα και σε ποικίλες άλλες εφαρμογές




Σχήμα 2. Χρονολογική εξέλιξη της τεχνολογίας Blockchain

Το Blockchain βρίσκεται ακόμα στα πρώτα στάδια της ανάπτυξής του.

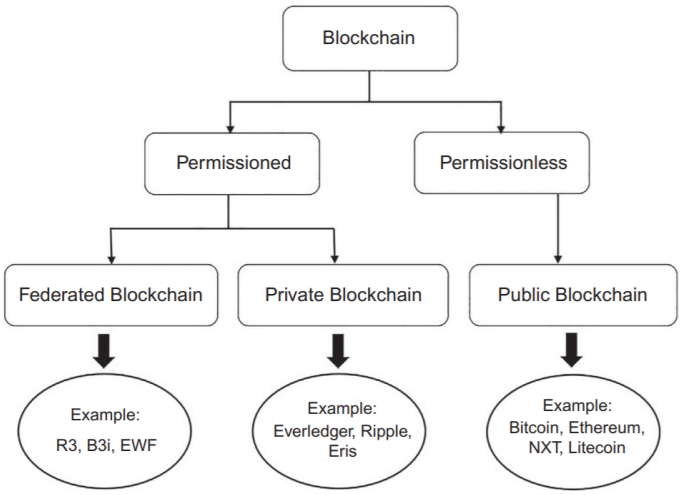
Η πρώτη φάση είναι η φάση εμβρύου. Τα κρυπτονομίσματα είναι αντιπροσωπευτικά αυτού του σταδίου, και το Bitcoin είναι το πιο σημαντικό.

Στη δεύτερη φάση του Blockchain, υποστηρίζεται πια και η δημιουργία προηγμένων έξυπνων συμβολαίων (Smart Contracts) για επιτεύξιμα προγράμματα και εντολές, που επεκτείνουν σταδιακά την περιοχή και το πεδίο εφαρμογής του. Αυτή η φάση επεκτείνει την εφαρμογή Blockchain σε διαφορετικές βιομηχανίες και κάνει εφικτή τη συνεργασία μεταξύ τους. Η υιοθέτηση τεχνολογίας Blockchain όχι μόνο επιλύει το πρόβλημα της εμπιστοσύνης, αλλά και επιτρέπει την όλο και πιο αυτοματοποιημένη κατανομή πόρων σε παγκόσμια κλίμακα. Σε αυτή τη φάση, το έξυπνο συμβόλαιο έχει χρησιμοποιηθεί και ενσωματωθεί στο σύστημα Blockchain για την αντιμετώπιση των ζητημάτων αμοιβαίας εμπιστοσύνης και ταυτότητας μεταξύ των κόμβων του δικτύου. Συγκεκριμένα, η πλατφόρμα Hyperledger είναι μία από τις δημοφιλείς υποδομές Blockchain που συνδέονται με τα έξυπνη συμβόλαια και την εξουσιοδοτημένη αρχή.

Στην επόμενη γενιά οι πτυχές που σχετίζονται με το Blockchain δεν θα επηρεάσουν μόνο την ανθρώπινη ιδεολογία αλλά εν γένει την κοινωνία. Οι κατανεμημένες εφαρμογές συστημάτων τεχνητής νοημοσύνης, όπως η Αποκεντρωμένη Εφαρμογή (Dapp- Decentralized Application), ο Αποκεντρωμένος Αυτόνομος Οργανισμός (DAODecentralized Autonomous Organization), η Αποκεντρωμένη Αυτόνομη Εταιρεία (DAC-Decentralized Autonomous Corporation), αρχίζουν να εμφανίζονται. Επίσης τα τελευταία χρόνια έχουν διατυπωθεί πολύ ενδιαφέρουσες ιδέες για εφαρμογή της Blockchain τεχνολογίας σε ποικίλα επιστημονικά πεδία αλλά και στην εξέλιξη “αμφιλεγόμενων” διαδικασιών με τις οποίες ερχόμαστε αντιμέτωποι στην καθημερινότητά μας, όπως για παράδειγμα στη διεξαγωγή μιας ψηφορίας χωρίς νωθεία και με αποδοχή του αποτελέσματος από όλους τους συμμετέχοντες. Το σχήμα 2 δείχνει τη χρονολογική εξέλιξη της τεχνολογίας Blockchain

### 2.1.3 Τύποι blockchain

Επί του παρόντος, υπάρχουν τουλάχιστον τέσσερις τύποι δικτύων blockchain - δημόσια blockchain, ιδιωτικά blockchain, κοινοπραξίες blockchain και πλευρικά blockchain. Στην παρακάτω εικόνα γίνεται διάκριση μεταξύ των κατηγοριών permissioned και permissionless blockchains. Στην κατηγορία permissioned ανήκουν τόσο τα ιδιωτικά όσο και οι κοινοπραξίες blockchain.




Σχήμα 3. Τύποι Blockchain

- Δημόσιο Blockchain: Είναι ένα blockchain που επιτρέπει σε οποιονδήποτε ανώνυμο χρήστη να προστεθεί στο δίκτυο blockchain, να πραγματοποιήσει μια νέα συναλλαγή, να επαληθεύσει τα μπλοκ που προστέθηκαν πρόσφατα και να διαβάσει το περιεχόμενο του blockchain. Το δημόσιο blockchain είναι ανοιχτό για όλους τους τύπους οντοτήτων για συμμετοχή στο δίκτυο. Δεν υπάρχουν περιορισμοί πρόσβασης. Οποιοσδήποτε διαθέτει σύνδεση στο Διαδίκτυο μπορεί να στείλει συναλλαγές σε αυτό και να γίνει επικυρωτής (δηλαδή, να συμμετάσχει στην εκτέλεση ενός πρωτοκόλλου συναίνεσης). Η διασφάλιση της λειτουργίας του δημόσιου blockchain γίνεται με χρήση κρυπτο-οικονομικών που αποτελεί ένα μείγμα κρυπτογραφικής επαλήθευσης και οικονομικών κινήτρων χρησιμοποιώντας μηχανισμούς συναίνεση όπως PoW ή PoS. Τα πιο γνωστά παραδείγματα blockchain αυτού του τύπου είναι το Ethereum, το Bitcoin και το NXT.
- Ιδιωτικό Blockchain: Σε αυτόν τον τύπο blockchain, μόνο ένας συγκεκριμένος οργανισμός έχει την εξουσία να συμμετάσχει στο δίκτυο blockchain, να στείλει μια νέα συναλλαγή, ενώ στον μηχανισμό συναίνεσης συμμετέχουν χρήστες, οι οποίοι πρέπει να αποκτήσουν δικαιώματά συμμετοχής τους από τον οργανισμό πριν εγγραφούν στο δίκτυο. Πιθανές εφαρμογές των ιδιωτικών blockchain περιλαμβάνουν τη διαχείριση βάσεων δεδομένων και τον έλεγχο. Συνήθεις περιπτώσεις ιδιωτικών blockchain είναι τα Ripple, Everledger και Eris. Σε σύγκριση με το δημόσιο blockchain, οι ομάδες των συμμετεχόντων χρηστών ενός ιδιωτικού blockchain είναι μικρές, ώστε η επαλήθευση των νέων μπλοκ να μην απαιτεί τεράστια δύναμη επεξεργασίας και χρόνο. Επίσης, το ιδιωτικό blockchain παρέχει καλύτερο απόρρητο, καθώς μόνο οι χρήστες που αναγνωρίζονται στο δίκτυο blockchain μπορούν να διαβάσουν τις συναλλαγές.
- Κοινοπραξίες Blockchain: Θεωρείται εν μέρει ιδιωτικό blockchain. Λειτουργεί υπό την εποπτεία ενός ομίλου εταιρειών ή οργανισμών. Ουσιαστικά αποτελεί ένα ιδιωτικό blockchain για ένα συγκεκριμένο σύνολο οργανισμών. Σε αντίθεση με το κοινό blockchain, το federated blockchain είναι ταχύτερο και προσφέρει καλύτερη επεκτασιμότητα και διατήρηση του απόρρητου. Παραδείγματα ενοποιημένων μπλοκ αλυσίδων είναι τα R3, EWF και B3i
- Πλευρικές αλυσίδες: Μια πλευρική αλυσίδα block (sidechain) είναι μια ονομασία για blockchain που λειτουργεί παράλληλα με ένα πρωτεύον blockchain. Οι καταχωρίσεις από το κύριο blockchain (όπου οι εν λόγω καταχωρήσεις συνήθως αντιπροσωπεύουν ψηφιακά στοιχεία) μπορούν να συνδεθούν με στοιχεία από και προς τα το sidechain Αυτό επιτρέπει στην πλευρική αλυσίδα να λειτουργεί διαφορετικά ανεξάρτητα από την κύρια μπλοκ αλυσίδας (π.χ., χρησιμοποιώντας εναλλακτικά μέσα τήρησης αρχείων, εναλλακτικό αλγόριθμο συναίνεσης κ.λπ.).

Ο παρακάτω πίνακας παρέχει σύγκριση μεταξύ δημόσιου, ιδιωτικού και κοινοπραξίας blockchain όσον αφορά την άδεια πρόσβασης, την ταχύτητα εκτέλεσης συναλλαγών, την αποτελεσματικότητα, την ασφάλεια, την διατήρηση του αμετάβλητου, τον μηχανισμό συναίνεσης, το δίκτυο και τα περιουσιακά στοιχεία.

| Item | Public | Private | Federated |
|---|---|---|---|
| Access | Read/write for anyone | Read/write for a single organization | Read/write for multiple selected organizations |
| Speed | Slower | Lighter and faster | Lighter and faster |
| Efficiency | Low | High | High |
| Security | Proof of work, proof of stake, and other consensus mechanisms | Pre-approved participants and voting/multi-party consensus | Pre-approved participants and voting/multi-party consensus |
| Immutability | Nearly impossible to tamper | Could be tampered | Could be tampered |
| Consensus process | Permissionless and anonymous | Permissioned and known identities | Permissioned and known identities |
| Network | Decentralized | Partially decentralized | Partially decentralized |
| Asset | Native Asset | Any Asset | Any Asset |

Σχήμα 4:Συγκριτικός Πίνακας public,private & federated Blockchain

Όπως ειπώθηκε νωρίτερα, το blockchain είναι μια αποκεντρωμένη και κατανεμημένη αρχιτεκτονική που διατηρεί την ασφάλεια και την ακεραιότητα των συναλλαγών. Για να γίνει αντιληπτός ο τρόπος λειτουργίας του blockchain, θα περιγράψουμε σύντομα την κεντρική αρχιτεκτονική. Για μεγάλο χρονικό διάστημα, τα βιβλία χρησιμοποιήθηκαν ως μέσα για τους τραπεζίτες και τις κυβερνήσεις να αποθηκεύουν διάφορες συναλλαγές σχετικά με την κατοχή γης και άλλες δραστηριότητες που απαιτούν τη διατήρηση αρχείων συναλλαγής. Στα συστήματα αυτά, η διατήρηση και η οικοδόμηση σχέσης εμπιστοσύνης μεταξύ των μερών μιας συγκεκριμένης συναλλαγής ήταν το μεγάλο πρόβλημα, με αποτέλεσμα να απαιτείται κάποια τράπεζα ή κεντρική κυβερνητική αρχή για την πραγματοποίηση των απαιτούμενων αλλαγών στις συναλλαγές και το σχεδιασμό των συμβάσεων που καθορίζουν ποιοι κατέχουν τι. Κατ' επέκταση, η διάκριση μεταξύ γνήσιων και πλαστών συναλλαγών διενεργούταν μόνο από την κεντρική αρχή. Ο διαχειριστής όλων των συμβάσεων και συναλλαγών (τράπεζα ή κυβερνητική αρχή) έχτιζε την απαιτούμενη εμπιστοσύνη ώστε οι άνθρωποι να μπορούν να πουλήσουν και να αγοράσουν με ασφάλεια περιουσιακά στοιχεία.

Η διατήρηση όλων των συμβάσεων και συναλλαγών (ledger) εξ' ορισμού είναι εντελώς συγκεντρωτική, καθώς ένα άτομο ή οργανισμός από όλους τους χρήστες έχει πλήρη έλεγχο της διαχείρισης συναλλαγών. Επίσης, αυτά τα ledger είναι ουσιαστικά μαύρα κουτιά για τους χρήστες, αφού τα περιεχόμενα τους είναι ορατά μόνο στον διαχειριστή τους.

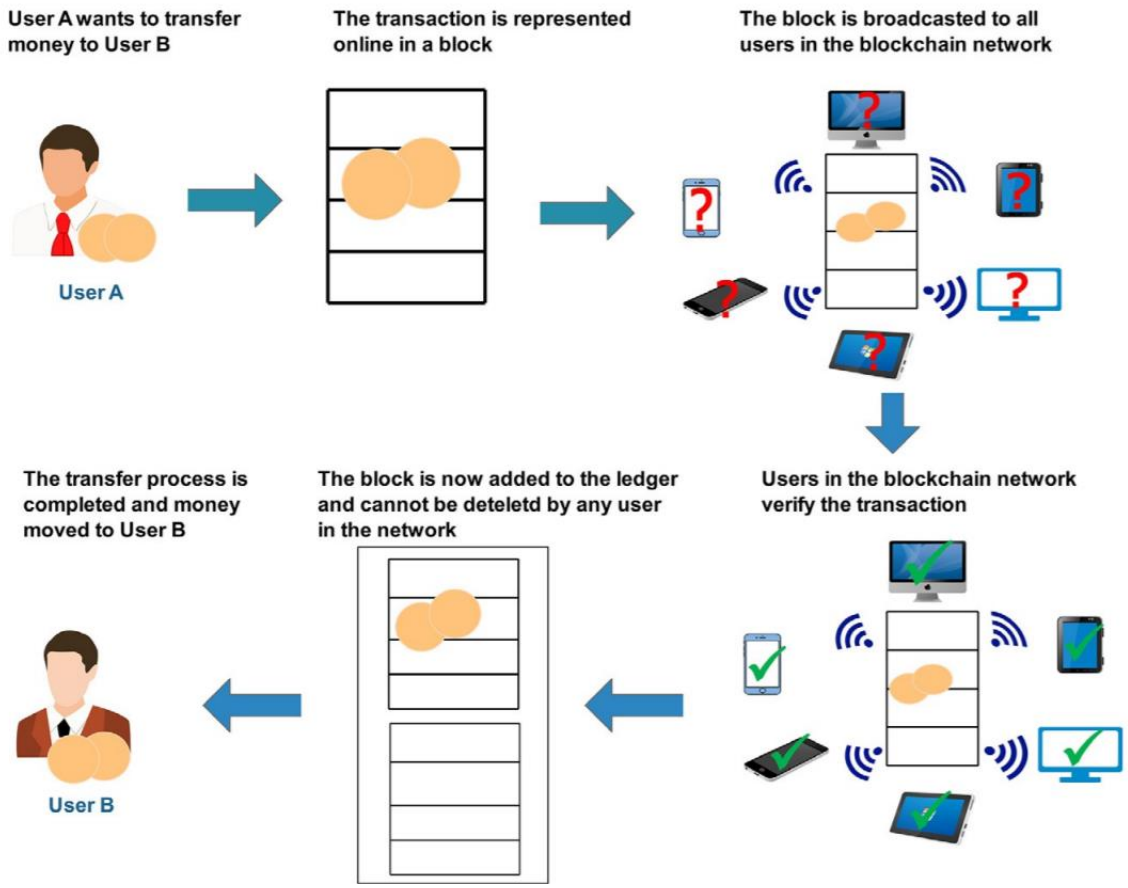
Σε αντιδιαστολή με τα παραπάνω συστήματα κεντρικής διαχείρισης και αποθήκευσης, το blockchain παρέχει παρόμοιες λειτουργίες σε όρους αποθήκευσης και συντήρησης συναλλαγών χωρίς να απαιτείται κάποιος διαχειριστής. Το ζήτημα της επαλήθευσης των συναλλαγών λύνεται με την αρχή του blockchain, σύμφωνα με την οποία κάθε χρήστης του δικτύου blockchain κρατά ένα αντίγραφο του αρχικού ledger. Επιπλέον, κάθε συμμετέχων χρήστης μπορεί να ζητήσει να προσθέσει μια συναλλαγή. Ωστόσο, η συναλλαγή προστίθεται

στο μπλοκ μόνο εάν η πλειοψηφία των συμμετεχόντων χρηστών στο δίκτυο blockchain επιβεβαιώνει αυτή την συναλλαγή. Μόλις επαληθευτεί μια συναλλαγή, θα προστεθεί και θα συνδεθεί με άλλες συναλλαγές σε ένα μπλοκ, το οποίο συνδέεται με προηγούμενα μπλοκ στο ledger μέσω μιας χρονικής σήμανσης και μιας συνάρτησης κατακερματισμού. Η διαδικασία αυτή σχηματίζει αλυσίδες μπλοκ, τα οποία αποτελούν αυτό που είναι γνωστό ως blockchain.

Μόλις δημιουργηθεί το μπλοκ, όλοι οι συμμετέχοντες στο δίκτυο blockchain αρχίζουν να αναζητούν το επόμενο μπλοκ προσπαθώντας να λύσουν την περίπλοκη μαθηματική συνάρτηση και να δημιουργήσουν ένα γνήσιο κρυπτογραφημένο μπλοκ συναλλαγών με στόχο να το προσθέσουν στο ledger. Αυτή η διαδικασία ονομάζεται εξόρυξη, στην οποία όλοι οι χρήστες ανταγωνίζονται για τη δημιουργία του νέου block. Ο πρώτος χρήστης που δημιουργεί ένα γνήσιο μπλοκ και το προσθέτει στο ledger ανταμείβεται με το ποσό των τελών για τις συναλλαγές που περιέχει. Δεδομένου ότι κάθε συναλλαγή με το blockchain κοστίζει κάποια τέλη (gas) και ότι τα μπλοκ περιλαμβάνουν μεγάλο αριθμό συναλλαγών, οι εξορύκτες θα μπορούσαν να εισπράξουν υψηλά κέρδη.

Η καθολική λίστα συναλλαγών (ledger) που κατέχουν όλοι οι συμμετέχοντες χρήστες στο δίκτυο ενημερώνεται κάθε φορά που προστίθεται νέο μπλοκ. Εάν το μπλοκ που προστέθηκε πρόσφατα έχει επαληθευτεί από όλους τους συμμετέχοντες χρήστες και όλες οι συναλλαγές του είναι γνήσιες, το μπλοκ θα προστεθεί και παραμένει μόνιμα στο καθολικό ως δημόσιο αρχείο. Εάν εντοπιστεί διένεξη, το μπλοκ θα απορριφθεί. Η καταστροφή ενός κλασικού κεντρικά ελεγχόμενου ledger, θα απαιτούσε μια επίθεση στον κεντρικό διαχειριστή του ενώ το blockchain είναι αμετάβλητο, οπότε αν υπάρχει κακόβουλη προσπάθεια αλλαγής της εγγραφής οποιασδήποτε συναλλαγής, αυτό θα απαιτήσει επαναλαμβανόμενους υπολογισμούς του PoW για το εμπλεκόμενο μπλοκ καθώς και όλα τα άλλα μπλοκ που ακολουθούν. Αυτοί οι υπολογισμοί είναι πολύ δύσκολο να πραγματοποιηθούν, εκτός εάν οι περισσότεροι χρήστες στο δίκτυο blockchain είναι κακόβουλοι. Επίσης, η πιθανότητα ύπαρξης ψεύτικου ledger δεν υπάρχει αφού όλοι οι χρήστες έχουν το δικό τους γνήσιο αντίγραφο του ledger για σύγκριση.

Το παρακάτω σχήμα δείχνει τη διαδικασία ροής μιας τυπικής χρηματοοικονομικής συναλλαγής χρησιμοποιώντας το blockchain όταν ένας Χρήστης Α θέλει να στείλει χρήματα στον Χρήστη Β. Η ροή ξεκινά όταν ο Χρήστης Α ζητά να προσθέσει ένα μπλοκ στο ledger που περιέχει πληροφορίες σχετικά με τη συναλλαγή χρηματοοικονομικής μεταφοράς. Μετά τη δημιουργία του μπλοκ, αυτό μετδίδεται μεταξύ όλων των συμμετεχόντων χρηστών στο δίκτυο blockchain προς επαληθεύση. Όταν το νέο μπλοκ επαληθευτεί από όλους τους συμμετέχοντες χρήστες στο δίκτυο, το μπλοκ θα προστεθεί στο ledger και μόνο τότε θα ολοκληρωθεί η διαδικασία της μεταφοράς. Ο Χρήστης Β μπορεί να λάβει τα χρήματα.




Σχήμα 5: Διαδικασία ροής μιας τυπικής χρηματοοικονομικής συναλλαγής χρησιμοποιώντας το blockchain όταν ένας Χρήστης Α θέλει να στείλει χρήματα στον Χρήστη Β

### 2.1.4 Χαρακτηριστικά του Blockchain

Σε αυτή την ενότητα στοχεύουμε να αναλύσουμε τα χαρακτηριστικά που σχετίζονται με κάθε τεχνολογία Blockchain. Όλα τα κρυπτο-νομίσματα στηρίζουν την λειτουργία τους στο blockchain και ζουν μέσα σε αυτό. Το Blockchain μπορεί να θεωρηθεί ως μια αποκεντρωμένη αρχιτεκτονική με ενσωματωμένους μηχανισμούς ασφάλειας για την αύξηση της εμπιστοσύνης και της ακεραιότητας των συναλλαγών. Υπάρχουν βασικοί λόγοι που καθιστούν το blockchain, ως το πλέον απαραίτητο και ασφαλέστερο εργαλείο δημιουργίας κρυπτονομισμάτων.

Πρωταρχικός λόγος χρήσης του blockchain είναι ο τρόπος ανίχνευσης και αποθήκευσης των δεδομένων. Όπως αναφέρθηκε, το blockchain είναι μια αλυσίδα από blocks, τα οποία περιέχουν δεδομένα. Όταν προστεθεί ένα μπλοκ στην αλυσίδα, αποτελεί μέρος του blockchain και δεν αλλάζει ποτέ. Όταν τα δεδομένα κάποιου block πρέπει να αλλάξουν, δεν αλλάζει το ήδη δημιουργημένο block, αλλά αυτά τα δεδομένα προστίθενται σε ένα καινούριο block της αλυσίδας αυτής, με δικιά τους χρονοσφραγίδα. Υπακούει, δηλαδή, στο γενικό λογιστικό κανόνα (general financial ledger), στον οποίο δεν καταργούνται ούτε τροποποιούνται τα ήδη υπάρχοντα δεδομένα. Οποιαδήποτε ανανέωση απαιτεί τη δημιουργία μιας νέας καταχώρησης, ώστε να διατηρείται όλη η προϊστορία. Για παράδειγμα, αν δύο άτομα ισχυρίζονταν ότι τους ανήκει η ίδια ιδιοκτησία, βάσει του κανόνα αυτού, το ιστορικό αλλαγών των ιδιοκτητών από την αρχή ύπαρξης της ιδιοκτησίας θα αποδείκνυε την αλήθεια. Ωστόσο, το blockchain λειτουργεί λίγο διαφορετικά στο πώς αποθηκεύει τα δεδομένα αυτά όπως θα μελετήσουμε σε επόμενο κεφάλαιο. Πριν το blockchain, τα δεδομένα αυτά ήταν συγκεντρωμένα σε ένα βιβλίο, σε έναν server ή οπουδήποτε, που, όμως, δεν είχαν όλοι πρόσβαση.

Ο δεύτερος λόγος χρήσης της τεχνολογίας αυτής είναι ότι λειτουργεί αποκεντρωτικά (decentralized) και κατανεμημένα (distributed). Όταν κάποιος γίνεται κάτοχος ενός κρυπτονομίσματος, ταυτόχρονα γίνεται κάτοχος και του ίδιου του blockchain. Δηλαδή, όλοι όσοι αποτελούν μέρος αυτού του συστήματος δεν έχουν στη διάθεσή τους μόνο τις συναλλαγές και τα δεδομένα που τους αφορούν, αλλά όλα τα δεδομένα και όλες τις συναλλαγές που έχουν ποτέ δημιουργηθεί. Για να εισαχθεί ένα block στο blockchain, ακολουθείται μια διαδικασία αποκρυπτογράφησης του κρυπτογραφημένου ίχνους του block από κάποια άτομα, που ονομάζονται εξορύκτες (miners). Όποιος αποκρυπτογραφήσει πρώτος το block ‘κερδίζει’, ενημερώνει τους υπόλοιπους miners ότι αποκρυπτογράφησε το ίχνος και ότι το block είναι έτοιμο να εισαχθεί στο blockchain. Αν το μεγαλύτερο ποσοστό των υπόλοιπων miners εγκρίνουν το γεγονός αυτό, τότε το block προστίθεται στο blockchain, και ο miner που ‘κέρδισε’, λαμβάνει μια ανταμοιβή για την υπηρεσία του, η οποία είναι κάποιο ποσό του κρυπτονομίσματος, στου οποίου το blockchain έγινε η διαδικασία.

Ο τρίτος βασικός λόγος χρήσης του blockchain αποτελεί η αποφυγή μεσαζόντων και η προστασία των προσωπικών δεδομένων από τρίτους στις διάφορες συναλλαγές. Πριν το blockchain, δύο άτομα για να κανονίσουν μια συναλλαγή χρησιμοποιούσαν ένα άλλο άτομο ή εταιρεία ως μεσάζοντα, ο οποίος αποθήκευε τα οικονομικά τους ή εταιρικά τους στοιχεία, ώστε να υπάρξει ασφάλεια και μυστικότητα στη συναλλαγή αυτή. Ο μεσάζοντας, μετά από κάποιο χρονικό διάστημα, αποφάσιζε και ρύθμιζε με τα ενδιαφερόμενα μέρη τις διάφορες λεπτομέρειες τις συναλλαγής. Στη συνέχεια αυτή πραγματοποιούνταν, με το μεσάζοντα να παίρνει ένα σύνολο χρημάτων για την παροχή των υπηρεσιών του. Πλέον, με το blockchain, η αποφυγή του μεσάζοντα είναι γεγονός, καθώς τα δεδομένα είναι διαθέσιμα σε όλους, ενώ ο καθένας μπορεί να παρουσιάσει στον άλλον όσα δεδομένα επιθυμεί, διατηρώντας ταυτόχρονα τη μυστικότητα των υπόλοιπων δεδομένων. Οι δύο πλευρές αποφασίζουν ποια κριτήρια πρέπει να ικανοποιηθούν και μόλις αυτό συμβεί, πραγματοποιείται αυτόματα η συναλλαγή. Παράλληλα με τον τρόπο αυτό, εξοικονομείται τόσο πολύτιμος χρόνος όσο και χρήμα.

Παρακάτω παρουσιάζονται οι ιδιότητες από τις οποίες διέπεται κάθε δίκτυο blockchain:

- Συνεχής διαθεσιμότητα: Σε αντίθεση με παραδοσιακούς κεντρικούς διακομιστές, το blockchain ουσιαστικά δεν σταματάει ποτέ να λειτουργεί, ούτε λόγω βλάβης ούτε λόγω συντήρησης.
- Αξιοπιστία: Το σύστημα ολοκληρώνει τις λειτουργίες του σταθερά και με επιτυχία, ενώ παράλληλα παρέχει εξηγήσεις για ενδεχόμενες αποτυχίες συναλλαγών.
- Ανοιχτό: Το blockchain δεν ξεχωρίζει συγκεκριμένους χρήστες ή υπολογιστές καθώς είναι ανοιχτό και προσβάσιμο από όλους.
- Ασφάλεια: Στο επίπεδο της κάθε συναλλαγής διασφαλίζει ότι η ιδιοκτησία μένει και μεταφέρεται στους σωστούς χρήστες. Όσον αφορά τη λειτουργία ολόκληρου του συστήματος, το blockchain προστατεύει τους χρήστες από κλοπές, μη εξουσιοδοτημένες προσβάσεις, διπλές πληρωμές (double spending) και ψεύτικες συναλλαγές.
- Ανθεκτικότητα: Ακόμα και υπό δύσκολες συνθήκες, το blockchain μπορεί να επιβεβαιώσει, αλλά και να μεταφέρει σωστά την ιδιοκτησία των δεδομένων του, ενώ είναι ανθεκτικό σε μεγάλο εύρος επιθέσεων.
- Τελική Σταθερότητα: Λόγω του τρόπου λειτουργίας του blockchain, υπάρχουν μερικές περιπτώσεις όπου οι απαντήσεις που δίνει το σύστημα δεν είναι σταθερές, αλλά με τη σύντομη πάροδο του χρόνου τελικά όλο το σύστημα επιστρέφει σταθερές απαντήσεις.
- Ακεραιότητα: Η συμπεριφορά του συστήματος δεν περιλαμβάνει λογικά λάθη. Το blockchain διατηρεί την ακεραιότητα των δεδομένων και βεβαιώνει την ασφάλεια των συναλλαγών, όπως και το ιστορικό τους.

Για την αύξηση της ασφάλειας και της εμπιστοσύνης στο δίκτυο, το blockchain διαθέτει διάφορους μηχανισμούς, μέσω των οποίων μπορεί να διασφαλιστεί μία συναλλαγή, η κατάσταση ενός block, αλλά και η κατάσταση ολόκληρου του συστήματος. Οι μηχανισμοί αυτοί είναι οι εξής:

- Απόδειξη ύπαρξης και μη ύπαρξης: Μπορεί να εξακριβωθεί εύκολα και σίγουρα αν ένα στοιχείο υπάρχει στο σύστημα.
- Απόδειξη χρόνου: Όταν αποθηκεύονται πληροφορίες στο blockchain, αποθηκεύεται και η ώρα κατά την οποία προστέθηκαν. Συνεπώς, είναι δυνατή η δημιουργία εφαρμογών που παρακολουθούν τη συχνότητα συμβάντων και διατηρούν την ιστορικότητά τους.
- Απόδειξη σειράς: Λόγω της απόδειξης χρόνου, σε περιπτώσεις συμφόρησης του δικτύου, μπορεί να φαίνεται η σειρά με την οποία πραγματοποιήθηκαν κάποιες αιτήσεις / συναλλαγές.
- Απόδειξη συγγραφής: Η εισαγωγή δεδομένων στο blockchain περιλαμβάνει και τα ψηφιακά στοιχεία του χρήστη που τα προσέθεσε. Ο μηχανισμός αυτός χρησιμεύει και για την ανίχνευση κακόβουλων επιθέσεων.
- Απόδειξη ιδιοκτησίας: Βασιζόμενο σε όλες τις υπόλοιπες αποδείξεις, φαίνεται πάντα με βεβαιότητα σε ποιόν ανήκει κάποιο στοιχείο μέσα στο blockchain.

### 2.1.5 Πεδίο Εφαρμογής

Υπάρχουν πολλές εφαρμογές που μπορούν να επωφεληθούν από διάφορες δυνατότητες της τεχνολογίας blockchain. Αυτές οι εφαρμογές περιλαμβάνουν:

Πνευματικά Δικαιώματα

Η βιομηχανία πνευματικών δικαιωμάτων ιδιοκτησίας όπως η μουσική βιομηχανία μπορεί να αποκομίσει τεράστια οφέλη από την τεχνολογία blockchain. Η μουσική βιομηχανία περιλαμβάνει μια ποικιλία οντοτήτων όπως εκδότες, συγγραφείς, καλλιτέχνες, ετικέτες και παρόχους υπηρεσιών ροής. Η ιδιοκτησία της μουσικής άλλαξε και έγινε πιο δύσκολη λόγω της εξέλιξης του διαδικτύου και της ευκολίας πρόσβασης σε διάφορα εφαρμογές streaming μέσω του Διαδικτύου. Υπάρχει ανάγκη διαφάνειας στα πνευματικά δικαιώματα και στις πληρωμές ιδιοκτησίας για συγγραφείς και καλλιτέχνες.

Η ενοποίηση της μουσικής βιομηχανίας με την τεχνολογία blockchain μπορεί να λύσει πολλά ζητήματα σχετικά με τη διαφάνεια και την πληρωμή ιδιοκτησίας. Το blockchain μπορεί να χρησιμοποιηθεί, για παράδειγμα, για τη δημιουργία μιας ακριβούς κατανεμημένης βάσης δεδομένων για την προστασία πληροφοριών σχετικών με τα δικαιώματα μουσικής. Επίσης, μπορούν να χρησιμοποιηθούν έξυπνα συμβόλαια ώστε να παρέχουν διάφορες ψηφιακές και ασφαλείς συμβάσεις και συναλλαγές απαραίτητες για τη μουσική βιομηχανία.

Εκπαίδευση

Η εκπαίδευση ένας από τους τομείς που ξεκίνησαν να υιοθετούν το blockchain κυρίως για λειτουργίες όπως η διαχείριση διαπιστευτηρίων και πιστοποιητικών μάθησης, η διαχείριση της φήμης και η διαχείριση των αρχείων των μαθητών. Το blockchain μπορεί να χρησιμοποιηθεί ως αποκεντρωμένη βάση δεδομένων για τη μόνιμη αποθήκευση διαφόρων τύπων πληροφοριών εκπαίδευσης. Κατ' επέκταση, τα πανεπιστήμια μπορούν να διατηρούν κρυπτογραφικά υπογεγραμμένα και επιβεβαιώσιμα πιστοποιητικά στο blockchain, ώστε να παρέχεται εύκολη πρόσβαση σε εαυτά από όλα τα ενδιαφερόμενα μέρη (εργοδότες, ιδρύματα υποτροφιών, φοιτητές κτλ). Η ενοποίηση του blockchain με τις κοινωνίες μάθησης μπορεί να δημιουργήσει καινοτόμες εκπαιδευτικές εφαρμογές που εφαρμόζουν ένα νέο μοντέλο μάθησης που βασίζεται στην ανταλλαγή ιδεών και εννοιών σε συνδυασμό με ένα σύστημα παρακολούθησης για την αξιολόγηση των μαθησιακών αποτελεσμάτων. Το blockchain μπορεί να χρησιμοποιηθεί στη ρύθμιση συμβάσεων και πληρωμών για την αξιολόγηση της μάθησης και την καταγραφή της ακαδημαϊκής προόδου όπως και για την πληρωμή διδάκτρων μέσω ομότιμης διδασκαλίας με άλλους μαθητές.

Δημόσιες υπηρεσίες

Τα δεδομένα που δημιουργούνται από κυβερνητικούς οργανισμούς είναι εσωτερικά κατακερματισμένα και αδιαφανή για τους πολίτες και τις επιχειρήσεις. Με την χρήση της τεχνολογίας blockchain, οι εγγραφές δεδομένων μπορούν να δημιουργηθούν και να επαληθευτούν γρήγορα, διασφαλίζοντας την ασφάλεια και τη διαφάνεια των δεδομένων. Τα χαρακτηριστικά των αλυσίδων Blockchain όπως οι ψηφιακές υπογραφές και η χρονική σήμανση παρέχουν αμέτρητα πλεονεκτήματα στο κοινό. Εμφανίζονται, πλέον, υπηρεσίες που επιτρέπουν στους πολίτες να χειρίζονται συναλλαγές και να δημιουργούν λογαριασμούς χωρίς την ανάγκη δικηγόρων, κυβερνητικών υπαλλήλων και άλλων τρίτων προσώπων η οργανισμών.

Αρκετές κυβερνήσεις άρχισαν να υιοθετούν τεχνολογία blockchain για την υποστήριξη και την διάθεση διάφορων δημόσιων υπηρεσιών στους πολίτες τους. Για παράδειγμα, η εσθονική κυβέρνηση έχει χρησιμοποιήσει τεχνολογία blockchain για να επιτρέψει στους πολίτες να εκτελούν πολλές εργασίες χρησιμοποιώντας τα δελτία ταυτότητάς τους, όπως ψηφοφορία,

εγγραφή για τις επιχειρήσεις τους, παραγγελία ιατρικών συνταγών και πληρωμή φόρων. Επιπλέον, το Ηνωμένο Βασίλειο έχειο συντάξει τμήμα το οποίο αρχίσει να υιοθετεί το blockchain στις πληρωμές πρόνοιας. Επίσης, η Σουηδία έχει πραγματοποιήσει δοκιμές για να θέσει τις συναλλαγές ακινήτων στο blockchain. Η Ε.Ε. έχει αποδεχθεί την χρησιμότητα του blockchain ως υπηρεσία απαραίτητη για την ολοκληρωμένη παροχή υπηρεσιών προς τους πολίτες και σχεδιάζει το δικό της blockchain, το EUblockchain, ενώ μάλιστα βρίσκεται στον σχεδιασμό ενός συστήματος αυτοδύναμης ταυτότητας SSI, σύμφωνα με το οποίο κάθε χρήστης μπορεί να ταυτοποιηθεί χωρίς την ανάγκης κάποιας κεντρικής αρχής.

Υγειονομική περίθαλψη

Το Blockchain έχει μεγάλες δυνατότητες για την επίλυση προβλημάτων διαλειτουργικότητας των υφιστάμενων συστημάτων υγειονομικής περίθαλψης. Μπορεί να χρησιμοποιηθεί για την ενεργοποίηση αντικειμένων υγειονομικής περίθαλψης ούτως ώστε οι ερευνητές να μπορούν να μοιραστούν το Ηλεκτρονικό Αρχείο Υγείας (EHR) με ασφαλείς τρόπους.

Η διαχείριση των δεδομένων υγειονομικής περίθαλψης είτε με αποθήκευση ή ανάλυση δεν είναι εύκολη λειτουργία, ιδίως όσον αφορά το απόρρητο των δεδομένων. Με στόχο την διατήρηση ενός ασφαλούς περιβάλλοντος αποθήκευσης και διαμοιρασμού δεδομένων στον τομέα της υγείας, έχουν εμφανιστεί λύσεις βασιζόμενες στην τεχνολογία του blockchain, όπως το Healthcare Data Gateway (HDG). Επίσης, η προστασία των δεδομένων αυτών που χαρακτηρίζονται όχι απλώς προσωπικά αλλά ευαίσθητα όπως θα δούμε στην επόμενη ενότητα, μπορεί να διασφαλιστεί υιοθετώντας το ιδιωτικό blockchain που επιτρέπει σε συγκεκριμένα άτομα να αποθηκεύουν ή να τροποποιούν τις ιατρικές πληροφορίες [26]

Ο παρακάτω πίνακας παρουσιάζει τους τομείς εφαρμογής του blockchain ανά κατηγορία.


Σχήμα 6: Περιπτώσεις εφαρμογής blockchain

## 2.2 Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων

Ο Γενικός Κανονισμός για την Προστασία των Δεδομένων (GDPR - General Data Protection Regulation) [3] 2016/679 είναι μια ρύθμιση στη νομοθεσία της Ευρωπαϊκής Ένωσης (ΕΕ) περί προστασίας των δεδομένων και της ιδιωτικής ζωής για όλα τα άτομα εντός της Ευρωπαϊκής

Ένωσης και του Ευρωπαϊκού Οικονομικού Χώρου (ΕΟΧ). Στόχος του GDPR είναι να δώσει στους ιδιώτες τον έλεγχο των προσωπικών τους δεδομένων και να απλοποιήσει τους κανονισμούς για τις διεθνείς επιχειρήσεις, ενοποιώντας τις ρυθμίσεις εντός της ΕΕ (Council of the European Union 6/11/2015). Ο GDPR τέθηκε σε ισχύ στις 25 Μαΐου 2018.

### 2.2.1 Προσωπικά Δεδομένα

Ως προσωπικά δεδομένα ορίζονται οι πληροφορίες οι οποίες περιγράφουν ένα άτομο, όπως στοιχεία αναγνώρισης (ονοματεπώνυμο, ηλικία, κατοικία, επάγγελμα, οικογενειακή κατάσταση), φυσικά χαρακτηριστικά, εκπαίδευση, εργασία (προϋπηρεσία, εργασιακή συμπεριφορά), οικονομική κατάσταση (έσοδα, περιουσιακά στοιχεία, οικονομική συμπεριφορά), ενδιαφέροντα, δραστηριότητες, συνήθειες.

Ως ευαίσθητα προσωπικά δεδομένα χαρακτηρίζονται τα προσωπικά δεδομένα ενός ατόμου που αναφέρονται στη φυλετική ή εθνική του προέλευση, στα πολιτικά του φρονήματα, στις θρησκευτικές ή φιλοσοφικές του πεποιθήσεις, στη συμμετοχή του σε συνδικαλιστική οργάνωση, στην υγεία του, στην κοινωνική του πρόνοια, στην ερωτική του ζωή, τις ποινικές διώξεις και καταδίκες του, καθώς και στη συμμετοχή του σε συναφείς με τα ανωτέρω ενώσεις προσώπων. Τα ευαίσθητα δεδομένα προστατεύονται από τον Νόμο με αυστηρότερες ρυθμίσεις από ότι τα απλά προσωπικά δεδομένα.

### 2.2.2 Δικαιώματα ατόμων ως προς τα προσωπικά δεδομένα

Σύμφωνα με τον GDPR, τα άτομα έχουν έναν αριθμό από δικαιώματα όσον αφορά τα προσωπικά τους δεδομένα, τα κυριότερα από τα οποία παρουσιάζονται παρακάτω:

- Δικαίωμα ενημέρωσης: Κάθε άτομο πρέπει να ενημερώνεται με σαφήνεια όσον αφορά τη μεταποίηση των δεδομένων του. Αυτό περιλαμβάνει το όνομα και τα στοιχεία επικοινωνίας του οργανισμού που τα επεξεργάζεται, το σκοπό της επεξεργασίας των δεδομένων, τη νομική βάση για την επεξεργασία, την προβλεπόμενη χρονική περίοδο που θα διατηρούνται τα δεδομένα του ατόμου, τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων.
- Δικαίωμα πρόσβασης: Κάθε άτομο πρέπει να έχει πρόσβαση στις διαδικασίες που σχετίζονται με τα προσωπικά του δεδομένα.
- Δικαίωμα διόρθωσης: Εάν τα δεδομένα είναι ανακριβή, τα άτομα μπορούν να ζητήσουν διόρθωση αυτών, την οποία ο οργανισμός οφείλει να ακολουθήσει.
- Δικαίωμα διαγραφής: Κάθε άτομο μπορεί να απαιτήσει διαγραφή των δεδομένων του όποτε το επιθυμεί.
- Δικαίωμα αντίρρησης: Ένα άτομο έχει το δικαίωμα να ζητήσει από έναν οργανισμό να περιορίσει την επεξεργασία των προσωπικών του δεδομένων.
- Δικαίωμα κοινοποίησης: Κάθε άτομο πρέπει να ενημερώνεται όσον αφορά την κοινοποίηση των δεδομένων του σε τρίτους.
- Δικαίωμα αυτοματοποιημένης λήψης αποφάσεων και δημιουργίας προφίλ: Κάθε άτομο πρέπει να ενημερώνεται όσον αφορά τη λογική της αυτοματοποιημένης επεξεργασίας των δεδομένων του.
- Δικαίωμα φορητότητας των δεδομένων: Ένα άτομο έχει το δικαίωμα να διασφαλίσει ότι τα προσωπικά του δεδομένα αποθηκεύονται σε δομημένη, ευρέως χρησιμοποιούμενη και μηχανικά αναγνώσιμη μορφή. Όταν είναι τεχνικά εφικτό, ένα άτομο μπορεί να ζητήσει να μεταφέρει απευθείας τα προσωπικά του δεδομένα από έναν οργανισμό σε έναν άλλο.

### 2.2.3 Προστασία των προσωπικών δεδομένων

Ο ΓΚΠΔ δίνει ιδιαίτερη έμφαση στην προληπτική προστασία των δεδομένων. Η προστασία δεδομένων εκ σχεδιασμού (by Design) και προεπιλογής ή εξ' ορισμού (by Default) περιλαμβάνεται στον Κανονισμό για να επηρεάσει τον υπεύθυνο ανάπτυξης βάσεων δεδομένων ώστε να ενσωματωθούν στο σύστημα τους τεχνικά και οργανωτικά μέτρα για να διασφαλιστεί η προστασία των προσωπικών δεδομένων των υποκειμένων των δεδομένων. Αυτό συνεπάγεται την υποχρέωση των Υπευθύνων να επιδιώκουν την προστασία δεδομένων εξαρχής κατά το σχεδιασμό των συστημάτων τους (Intersoft Consulting, 2018).

Η έννοια της Προστασίας εκ Σχεδιασμού βασίζεται στη συνειδητοποίηση ότι οι συνθήκες για την επεξεργασία των δεδομένων εδράζονται κυρίως στο υλικο-λογισμικό που χρησιμοποιείται για το έργο.

Η αλματώδης ανάπτυξη της τεχνολογίας, καθιστά επιβεβλημένη την προστασία δεδομένων μέσω αυτής ενώ οι τεχνολογικές έννοιες για προληπτική προστασία χρησιμεύουν ως βάση για την ελαχιστοποίηση της επεμβατικότητας της επεξεργασίας αυτής. Κατά την εφεύρεση νέας τεχνολογίας, οι προγραμματιστές και παραγωγοί οφείλουν να τηρούν *την αρχή της ελαχιστοποίησης και της ανωνυμίας ή ψευδωνυμίας των δεδομένων*. Όταν δημιουργούνται νέα προϊόντα, η διαχείριση της αντίστοιχης οντότητας θα πρέπει να ενεργεί σε πρώιμο στάδιο του έργου για να ευαισθητοποιεί τους προγραμματιστές και τους σχεδιαστές για την υποχρέωση αυτή.

Η έννοια της προστασίας από προεπιλογή προστατεύει τους καταναλωτές από την εκτεταμένη τάση των εταιρειών να λαμβάνουν όσο το δυνατόν περισσότερα προσωπικά δεδομένα. Στόχος είναι, από προεπιλογή, να λαμβάνονται μόνο τα απολύτως απαραίτητα προσωπικά δεδομένα για τον συγκεκριμένο σκοπό επεξεργασίας. Η έννοια αυτή αφορά στο μέγεθος των συλλεγόμενων δεδομένων, την έκταση της επεξεργασίας τους, την περίοδο αποθήκευσής τους και την προσβασιμότητα τους. Για το σκοπό αυτό, ο Υπεύθυνος πρέπει να εφαρμόσει τα κατάλληλα τεχνικά και οργανωτικά μέτρα, ενώ όταν υφίσταται Εκτελών, ο τελευταίος πρέπει να δώσει στον Υπεύθυνο τη δυνατότητα να επιτύχει την προστασία από προεπιλογή. Οι φιλικές προς το απόρρητο προεπιλεγμένες ρυθμίσεις συνήθως προβλέπουν ένα βαθμό προστασίας τέτοιο, που οι χρήστες να μην απαιτείται να αλλάξουν τις ρυθμίσεις μιας υπηρεσίας ή ενός προϊόντος κατά την πρώτη χρήση ή πρόσβαση για να προστατευτούν. Όταν οι χρήστες επιθυμούν να αλλάξουν αυτές τις ρυθμίσεις, θα πρέπει να επιλέξουν και να τροποποιήσουν τις ρυθμίσεις από μόνοι τους. Η έννοια της προστασίας από προεπιλογή θα βοηθήσει, πάνω από όλα, την προστασία των ατόμων που δεν έχουν τις τεχνικές γνώσεις ή το χρόνο να εφαρμόσουν τις απαιτούμενες ρυθμίσεις που είναι φιλικές για το απόρρητο τους. Επιπλέον, με την αυξανόμενη πολυπλοκότητα και ποικιλία των διαδικτυακών υπηρεσιών και της χρήσης δεδομένων, η αξιολόγηση των επιπτώσεων των τεχνικών ρυθμίσεων για την προστασία των δεδομένων καθίσταται όλο και δυσχερέστερη.

## 2.3 Blockchain και GDPR

Από τις 25 Μαΐου 2018 έχει τεθεί σε εφαρμογή ο Γενικός Κανονισμός Προστασίας Δεδομένων ΕΕ 679/2016 (GDPR), ο οποίος και ισχύει άμεσα σε όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης.

Τον τελευταίο καιρό, έχουν γίνει πολλές συζητήσεις σε πολιτικό, ακαδημαϊκό και ιδιωτικό επίπεδο σχετικά με τη σχέση ανάμεσα στο blockchain και τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR). Πράγματι, πολλά από τα "σημεία τριβής" μεταξύ blockchain και GDPR οφείλονται σε δύο γενικούς παράγοντες.

Πρώτον, ο GDPR βασίζεται στην υπόθεση ότι σε κάθε σημείο επεξεργασίας δεδομένων προσωπικού χαρακτήρα είναι τουλάχιστον ένα φυσικό ή νομικό πρόσωπο - ο υπεύθυνος

επεξεργασίας δεδομένων - στο οποίο τα πρόσωπα στα οποία αφορούν τα δεδομένα μπορούν να απευθύνονται για την ικανοποίηση των δικαιωμάτων τους βάσει της κείμενης νομοθεσίας. Αυτοί οι υπεύθυνοι επεξεργασίας δεδομένων πρέπει να συμμορφώνονται με τις υποχρεώσεις που προκύπτουν από τον GDPR. Το blockchain, ωστόσο, είναι κατανεμημένες βάσεις δεδομένων που συχνά επιδιώκουν την αποκέντρωση, αντικαθιστώντας έναν ενιαίο παράγοντα με πολλούς διαφορετικούς παίκτες. Η έλλειψη συναίνεσης ως προς τον τρόπο με τον οποίο θα πρέπει να κατανέμεται η ευθύνη για την επεξεργασία δεδομένων δυσχεραίνει την κατανομή της ευθύνης και της λογοδοσίας.

Δεύτερον, ο GDPR βασίζεται στην υπόθεση ότι τα δεδομένα μπορούν να τροποποιηθούν ή να διαγραφούν όπου απαιτείται και σε συμμόρφωση με τις νομικές απαιτήσεις, όπως τα άρθρα 16 και 17 του Κανονισμού. Το blockchain, ωστόσο, δυσχεραίνει τη μονομερή τροποποίηση των δεδομένων, με σκοπό την διασφάλιση της ακεραιότητας των δεδομένων και την αύξηση της εμπιστοσύνης στο δίκτυο. Επιπλέον, το blockchain φέρνει στο προσκήνιο τις προκλήσεις της συμμόρφωσης με τις απαιτήσεις για ελαχιστοποίηση των δεδομένων και του περιορισμού του σκοπού στην τρέχουσα μορφή της οικονομίας των δεδομένων.

Το 2019, εκπονήθηκε για λογαριασμό του Ευρωπαϊκού Κοινοβουλίου, μία ενδιαφέρουσα μελέτη σχετικά με την τεχνολογία “Blockchain” και τον Γενικό Κανονισμό Προστασίας Δεδομένων 2016/679 (GDPR). Όπως αναφέρεται στην έκθεση, το Blockchain είναι ένα πολυσυζητημένο εργαλείο που, σύμφωνα με μερικούς, υπόσχεται να εγκαινιάσει μια νέα εποχή στην αποθήκευση δεδομένων και την εκτέλεση κώδικα, γεγονός που θα μπορούσε, με τη σειρά του, να τονώσει νέα επιχειρηματικά μοντέλα και αγορές. Στη μελέτη παρουσιάζονται οι περιπτώσεις στις οποίες η τεχνολογία “Blockchain” προσκρούει σε διατάξεις του GDPR, ενώ περιλαμβάνονται βασικές συστάσεις για τη διευθέτησή τους.

### 2.3.1 Προσωπικά και Ψευδώνυμα Δεδομένα

Υπάρχουν δύο τύποι δεδομένων όσον αφορά το Blockchain, τα προσωπικά δεδομένα και για τα ψευδώνυμα δεδομένα. Τα προσωπικά δεδομένα είναι οποιαδήποτε πληροφορία σχετική με ένα προσδιορισμένο ή αναγνωρίσιμο φυσικό πρόσωπο - δηλαδή η δυνατότητα ταυτοποίησης κάποιου από τα δεδομένα. Όσον αφορά στα κρυπτογραφημένα δεδομένα, αυτά εξακολουθούν να είναι προσωπικά δεδομένα, ωστόσο εμπίπτουν σε μια νέα κατηγορία δεδομένων προσωπικού χαρακτήρα που δημιουργήθηκε από τον ΓΚΠΔ, τα ψευδώνυμα δεδομένα.

Προσωπικά Δεδομένα

Τα προσωπικά δεδομένα αποτελούν τον πυρήνα και την αυτή καθ’ εαυτή προστατευόμενη ιδιότητα του ΓΚΠΔ. Τα ‘δεδομένα’ αναφέρονται σε ηλεκτρονικά αποθηκευμένες πληροφορίες και, κατά τους Voigt και Busche, περιλαμβάνουν και κάθε λογής σημάδια ή ενδείξεις που υποδεικνύουν δεδομένα. Τα δεδομένα, από μόνα τους, δεν εμπίπτουν στο πεδίο εφαρμογής του κανονισμού, αν δεν είναι προσωπικής φύσεως, και για να το κάνουν αυτό, βάσει του ΓΚΠΔ, πρέπει να αφορούν ένα προσδιορισμένο ή αναγνωρίσιμο φυσικό πρόσωπο. Όπως είδαμε ήδη, τα δεδομένα είναι προσωπικά εάν είναι άμεσα ή έμμεσα δυνατή η αναγνώριση ενός φυσικού προσώπου με αναφορά σε ένα αναγνωριστικό όπως όνομα, αναγνωριστικός αριθμός, ή βάσει ενός ή περισσοτέρων παραγόντων που σχετίζονται με τη φυσική, φυσιολογική, γενετική, πνευματική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου. Δεδομένου ότι δύναται να συμπεριληφθούν πληροφορίες που από μόνες τους δεν θεωρούνται δεδομένα προσωπικού χαρακτήρα, δεν καθορίζεται σαφώς το ποιος μπορεί να είναι σε θέση να προσδιορίσει το φυσικό πρόσωπο από συνδυασμό αυτών των δεδομένων, πράγμα που σημαίνει ότι οι συμπληρωματικές πληροφορίες δεν απαιτείται να κατέχονται από το ίδιο νομικό πρόσωπο.

Ο ΓΚΠΔ δεν αποκλείει ότι τα φυσικά πρόσωπα μπορεί να αναγνωρίζονται μέσω της ηλεκτρονικής παρουσίας τους λόγω και της συνεχώς αυξανόμενης χρήσης του διαδικτύου. Αυτό μπορεί να επεκταθεί σχεδόν σε όλα τα μέσα που χρησιμοποιούμε στην καθημερινότητα μας από συσκευές και εφαρμογές, έως πρωτόκολλα όπως διευθύνσεις πρωτοκόλλου διαδικτύου (IP) ή αναγνωριστικά cookie, τα οποία μπορούν να αφήσουν ψηφιακά ίχνη και μπορούν να χρησιμοποιηθούν για τον εντοπισμό φυσικών προσώπων όταν συνδυάζονται με μοναδικά αναγνωριστικά στοιχεία και άλλες πληροφορίες. Τέλος, ο ΓΚΠΔ αποκλείει την επισήμανση των προσωπικών δεδομένων από τους αποβιώσαντες υπό την αίρεση αυτά να μπορούν να βοηθήσουν στην αναγνώριση φυσικού προσώπου που είναι εν ζωή.

Ψευδώνυμα Δεδομένα

Η απόδοση ψευδωνύμου είναι η επεξεργασία προσωπικών δεδομένων, ούτως ώστε να απαιτούνται πρόσθετες πληροφορίες για τον προσδιορισμό της ταυτότητας του υποκειμένου, δεδομένου, όμως, ότι οι πρόσθετες αυτές πληροφορίες διατηρούνται ξεχωριστά πίσω από ένα τεχνικό ή διοικητικό τείχος προστασίας. Η χρήση ψευδωνύμων δεν αφαιρεί την προσωπική πτυχή των δεδομένων, αλλά επιτρέπει μεγαλύτερα περιθώρια επεξεργασίας τους, λόγω των αντίστοιχα χαμηλότερων κινδύνων. Ο ΓΚΠΔ λαμβάνει υπόψη όλα τα μέσα που είναι πιθανόν να χρησιμοποιηθούν για να εξακριβωθεί ένα φυσικό πρόσωπο από τα ψευδώνυμα δεδομένα, με βάρος σε όλους τους αντικειμενικούς παράγοντες όπως το κόστος, ο απαιτούμενος χρόνος για ταυτοποίηση και η διαθέσιμη τεχνολογία. (Bygrave, 2017)[5]

Συνεπώς, κάθε μεμονωμένη διαδικασία ψευδωνυμίας πρέπει να αξιολογηθεί ως προς τη δυσκολία που παρέχει στο να μεταφραστούν τα ψευδώνυμα δεδομένα σε προσωπικά. Σε αντίθεση με τα ψευδώνυμα δεδομένα, τα ανώνυμα δεδομένα αποκλείονται εξ' ολοκλήρου από το ΓΚΠΔ. Σε αυτά περιλαμβάνονται δεδομένα που ουδέποτε ήταν προσωπικού χαρακτήρα, ή έχουν υποβληθεί σε τόσο εκτεταμένη τεχνική ανωνυμοποίηση, ώστε κανένα φυσικό πρόσωπο να μην μπορεί να αναγνωριστεί μέσω αυτών.

### 2.3.2 Συμμόρφωση της τεχνολογίας Blockchain με τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR).

Η συμμόρφωση της τεχνολογίας Blockchain με τον GDPR αποτελεί ένα φλέγον ζήτημα, που έχει απασχολήσει την αρμόδια Γαλλική Εποπτική Αρχή (CNIL) καθώς και την Ευρωπαϊκή Επιτροπή [6]. Η συμμόρφωση της τεχνολογίας Blockchain με τον GDPR δεν αφορά την τεχνολογία per se, αλλά τον τρόπο με τον οποίο χρησιμοποιείται η εν λόγω τεχνολογία σε διάφορες περιπτώσεις και εφαρμογές, όπως ακριβώς συμβαίνει και με το Διαδίκτυο και την Τεχνητή Νοημοσύνη (Artificial Intelligence).

Τα δεδομένα που σχετίζονται με συναλλαγές και είναι καταχωρημένα σε έναν κατάλογο Blockchain ή υπόκεινται σε επεξεργασία σε ένα «έξυπνο συμβόλαιο» (smart contracts) - ψηφιακό πρωτόκολλο, που εκτελεί αυτόματα προκαθορισμένες διαδικασίες για μία συναλλαγή χωρίς να απαιτείται η συμμετοχή ενός τρίτου μέρους (π.χ. τράπεζας), μπορούν να οδηγήσουν σε ταυτοποίηση φυσικών προσώπων και ως εκ τούτου θεωρούνται προσωπικά δεδομένα που προστατεύονται από τον GDPR καθώς και από την ισχύουσα νομοθεσία περί προστασίας προσωπικών δεδομένων. Τρία σημαντικά ζητήματα που ανακύπτουν σχετικά με την προστασία των προσωπικών δεδομένων σε έναν κατάλογο blockchain, στο πλαίσιο του GDPR. Η αναφορά γίνεται μόνο στον GDPR, δεδομένου ότι δεν έχει ακόμα ψηφιστεί από το Ελληνικό Κοινοβούλιο το σχέδιο νόμου για την προστασία προσωπικών δεδομένων, σε εφαρμογή του GDPR.

1) Ποιος είναι ο υπεύθυνος επεξεργασίας / εκτελών την επεξεργασία σε έναν κατάλογο blockchain?

Στον GDPR γίνεται σαφής διάκριση ανάμεσα στον υπεύθυνο επεξεργασίας (data controller), που αποτελεί το μέρος που καθορίζει τους σκοπούς και τον τρόπο της επεξεργασίας των προσωπικών δεδομένων και φέρει την πρωταρχική ευθύνη και στον εκτελούντα την επεξεργασία (data processor), ο οποίος επεξεργάζεται προσωπικά δεδομένα για λογαριασμό του υπευθύνου επεξεργασίας. Σε πολλές περιπτώσεις ο ως άνω διαχωρισμός σε έναν κατάλογο blockchain καθίσταται δύσκολος, ιδίως σε έναν δημόσιο κατάλογο blockchain, όπως είναι το Bitcoin, όπου δεν υπάρχει έλεγχος επί των δεδομένων που υπόκεινται σε επεξεργασία στο πλαίσιο μιας συναλλαγής. Για παράδειγμα, θα μπορούσε να θεωρηθεί ότι όλα τα μέρη που ανταλλάσσουν προσωπικά δεδομένα στο πλαίσιο μίας τέτοιας συναλλαγής, ενεργούν ως υπεύθυνοι επεξεργασίας. Αντίστοιχα εκτελούντες την επεξεργασία δύνανται να θεωρηθούν άλλοι συμμετέχοντες σε έναν κατάλογο blockchain, όπως π.χ. οι προγραμματιστές «έξυπνων συμβολαίων» (smart contracts), οι οποίοι επεξεργάζονται προσωπικά δεδομένα για λογαριασμό αντίστοιχα των συμμετεχόντων που ενεργούν ως υπεύθυνοι επεξεργασίας, καθώς και οι miners (όσοι επιβεβαιώνουν συναλλαγές για την είσπραξη ανταμοιβής), οι οποίοι δεν συμμετέχουν μεν σε μια συναλλαγή αλλά χειρίζονται τους κόμβους (nodes) και επικυρώνουν τις συναλλαγές για λογαριασμό των συμμετεχόντων.

2) Προστασία των προσωπικών δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού

Σύμφωνα με τον GDPR, ο υπεύθυνος επεξεργασίας οφείλει να εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα για να διασφαλίζει ότι, εξ ορισμού, υπόκεινται σε επεξεργασία μόνο τα προσωπικά δεδομένα που είναι απαραίτητα για τον εκάστοτε σκοπό της επεξεργασίας και δεν καθίστανται προσβάσιμα χωρίς την παρέμβαση του φυσικού προσώπου σε αόριστο αριθμό φυσικών προσώπων. Σε έναν κατάλογο blockchain υφίσταται πάντοτε το ζήτημα απουσίας ελέγχου επί των διαδικασιών που πραγματοποιούνται σε αυτόν και ως εκ τούτου καθίσταται κάθε φορά απαραίτητος ο έλεγχος εάν η τεχνολογία blockchain είναι η κατάλληλη τεχνολογία που πρέπει να χρησιμοποιηθεί για την πραγματοποίηση του επιδιωκόμενου σκοπού. Επίσης, συνιστάται η επιλογή ενός ιδιωτικού καταλόγου blockchain (αντί ενός δημοσίου), που παρέχει μεγαλύτερο έλεγχο επί των προσωπικών δεδομένων, τα οποία υπόκεινται σε επεξεργασία, ειδικότερα σε ό,τι αφορά την διαβίβαση αυτών εκτός ΕΕ, καθώς πολλοί miners ενδέχεται να μην είναι εγκατεστημένοι εντός ΕΕ. Για τον σκοπό της ασφαλούς διαβίβασης δεδομένων σε χώρες εκτός ΕΕ, η εφαρμογή εγγυητικών μηχανισμών (τυποποιημένες συμβατικές ρήτρες, Δεσμευτικοί Εταιρικοί Κανόνες κλπ.) καθίσταται περισσότερο εφικτή σε έναν ιδιωτικό blockchain παρά σε έναν δημόσιο. Επιπρόσθετα, συνιστάται η επεξεργασία και αποθήκευση μόνο κρυπτογραφημένων, ψευδωνυμοποιημένων ή ανωνυμοποιημένων δεδομένων, καθώς και η διενέργεια εκτίμησης των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία προσωπικών δεδομένων

3) Άσκηση των δικαιωμάτων των υποκειμένων των δεδομένων

Όσον αφορά την άσκηση των δικαιωμάτων, που διατηρούν τα υποκείμενα των δεδομένων σύμφωνα με τον GDPR, ας σημειωθεί ότι ενδέχεται πολλά εκ των βασικών αυτών δικαιωμάτων, όπως το δικαίωμα διόρθωσης και το δικαίωμα διαγραφής (δικαίωμα στη λήθη), να μην μπορούν να ασκηθούν λόγω του τρόπου δομής και αποθήκευσης των δεδομένων στους καταλόγους blockchain. Ειδικότερα, οι κατάλογοι blockchain έχουν σχεδιαστεί κατά τέτοιο τρόπο, ώστε να μην είναι δυνατή η διαγραφή και διόρθωση των δεδομένων άπαξ αυτά καταχωρηθούν στην αλυσίδα των μπλοκ. Η «μη μεταβλητότητα» (immutability) αποτελεί βασικό χαρακτηριστικό της τεχνολογίας Blockchain. Συνεπώς, ακόμα και αν δύναται να προσδιοριστεί ο υπεύθυνος επεξεργασίας σε ένα δίκτυο, όπως για παράδειγμα στο Bitcoin, καθίσταται αδύνατο ο εν λόγω υπεύθυνος επεξεργασίας να διαγράψει ή να επικαιροποιήσει το αρχείο μίας συναλλαγής χωρίς να καταστρέψει την αλυσίδα των μπλοκ.

Η τεχνολογία Blockchain έχει συνολικά οικοδομηθεί επί τη βάσει της διασφάλισης ότι οι συναλλαγές δεν πρόκειται ποτέ να λησμονηθούν ή να διαγραφούν, με σκοπό την δημιουργία αποκεντρωμένης εμπιστοσύνης καθώς και την ανάπτυξη και επέκταση του δικτύου των συμμετεχόντων. Θα πρέπει να σημειωθεί ότι στον GDPR δεν εξειδικεύεται η έννοια της διαγραφής. Σε αυτό το πλαίσιο, η αρμόδια Γαλλική Εποπτική Αρχή (CNIL) αναγνωρίζει ότι ορισμένες τεχνικές κρυπτογράφησης, που συνδυάζονται με την καταστροφή του κλειδιού, μπορούν ενδεχομένως να θεωρηθούν διαγραφή ακόμα και αν δεν συνιστούν διαγραφή εν τη στενή έννοια. Επισημαίνεται, επίσης, ότι ακόμα και η άσκηση του δικαιώματος πρόσβασης από πλευράς των υποκειμένων των δεδομένων καθίσταται δύσκολη, καθώς είναι δύσκολος ο προσδιορισμός του υπευθύνου επεξεργασίας. Αναφορικά με τους ιδιωτικούς καταλόγους blockchain, και πάλι η αρμόδια Γαλλική Εποπτική Αρχή (CNIL) προτείνει τον καθορισμό ενός ελάχιστου αριθμού miners προκειμένου να αποφευχθούν αντιπαραθέσεις μεταξύ των εμπλεκομένων μερών, την εφαρμογή των κατάλληλων τεχνικών και οργανωτικών μέτρων, προκειμένου να ελαχιστοποιηθεί ο αντίκτυπος από την αποτυχία ενός αλγορίθμου στην ασφάλεια των συναλλαγών, καθώς και την κατάρτιση ενός εναλλακτικού σχεδίου τροποποίησης αλγορίθμων σε περίπτωση εντοπισμού ενός ευάλωτου σημείου στον κώδικα. Επιπλέον, συνιστάται η καταγραφή του τρόπου διακυβέρνησης, η εξέλιξη του λογισμικού που χρησιμοποιείται, καθώς και η διασφάλιση της εμπιστευτικότητας, της ακεραιότητας, της νομιμότητας και της διαφάνειας της τεχνολογίας Blockchain μέσω της εφαρμογής των κατάλληλων μέτρων.

# 3. Διακυβέρνηση σε Δίκτυα Blockchain

Τι εννοούμε πραγματικά με τον όρο διακυβέρνηση; Σύμφωνα με έναν ορισμό (Bell, 2002) [7], διακυβέρνηση είναι η χρήση θεσμών, δομών αρχών και συνεργασιών για την κατανομή πόρων και τον συντονισμό της προσπάθειας και της δραστηριότητας στην κοινωνία ή στην οικονομία.

Η ανάπτυξη των αποκεντρωμένων δικτύων μπορεί να θεωρηθεί ως μία επιλογή των ανθρώπων να αντιδράσουν στην διαχείριση των προσωπικών δεδομένων που τους αφορούν από τρίτους (κράτος, επιχειρήσεις), η οποία έχει αποδειχθεί πολλές φορές παρεμβατική ή ανεπαρκής να παρέχει προστασία. Η τεχνολογία blockchain προσελκύει ενδιαφέρον ως το μέσο που θα εξασφαλίσει περισσότερη δικαιοσύνη και δημοκρατία. Το γεγονός ότι οι ίδιοι οι συμμετέχοντες του δικτύου (community) εξασφαλίζουν ότι τα αποκεντρωμένα δίκτυα ουσιαστικά ελέγχονται και κυβερνώνται από το τους ίδιους, καλύπτει την ανάγκη για έλεγχο της δικαιοσύνης και της δημοκρατίας.

Η διακυβέρνησή μέσω αποκεντρωμένων δικτύων είναι ένα θέμα που προσελκύει ολοένα και περισσότερο ενδιαφέρον και αυτό οφείλεται σε πολλούς παράγοντες. Ένας εκ των βασικών παραγόντων, είναι ο ιδεολογικός. Ζούμε σε μια περίοδο που συλλέγονται και διακινούνται λεπτομερείς πληροφορίες σχετικά με φυσικά πρόσωπα, πολλές φορές μάλιστα χωρίς την γνώση ή την συναίνεση των προσώπων αυτών. Η τεχνολογία των αποκεντρωμένων δικτύων αντιμετωπίζεται ως το εργαλείο που μπορεί να συμβάλλει στην προστασία από την παραβίαση των προσωπικών δεδομένων των προσώπων.

Στο κεφάλαιο αυτό, αναλύουμε τις δύο βασικές πτυχές του όρου διακυβέρνησης: διακυβέρνηση από την υποδομή και διακυβέρνηση της υποδομής σύμφωνα με την ορολογία των de Philippi και McMullen (2018). Εξετάζουμε, την διακυβέρνηση όπως εφαρμόζεται στο σχεδιασμό και τη συντήρηση των πρωτοκόλλων δικτύου (διακυβέρνηση της υποδομής). Αντίθετα, ένας μηχανισμός συναίνεσης που είναι εγγενής στις συναλλαγές blockchain αναφέρεται στην διακυβέρνηση από την υποδομή. Δεν θα ασχοληθούμε, με το ερώτημα εάν θα μπορούσε να είναι εφικτή η αποκεντρωμένη διακυβέρνηση, η συμβολή ή αντικατάσταση παραδοσιακών πολιτικών θεσμών (Atzori, 2017).[8]

Η συμμετοχή της κοινότητας στη διαμόρφωση των ιδεών, των σχολίων, των αναφορών σφαλμάτων και του συνεισφερόμενου κώδικα και οι μηχανισμοί της κοινότητας που εξυπηρετούν τα παραπάνω αφορούν την διακυβέρνηση της υποδομής.

## 3.1 Centralized vs Decentralized Networks

Καθώς η αποκέντρωση ή αποκεντροποίηση (decentralization) είναι ένα από τα βασικά ζητήματα, κρίνεται απαραίτητο να διευκρινιστεί ο όρος. Η ίδια η λέξη, η οποία βέλτιστα αποδίδεται στα ελληνικά με τον όρο «συγκεντρωτισμός» (centralization) χρησιμοποιήθηκε πρώτη φορά στην Γαλλία, την εποχή του Ναπολέοντα μετά την Επανάσταση στα τέλη του 18ου αιώνα. Το αντώνυμο, «αποκεντρωτισμός», (decentralization) εμφανίστηκε για πρώτη φορά στη δεκαετία του 1830 στη γερμανική γλώσσα. Σε ένα αποκεντρωμένο σύστημα, τα στοιχεία χαμηλότερου επιπέδου (local components), που ενεργούν βάσει τοπικών δεδομένων, αλληλεπιδρούν για την επίτευξη παγκόσμιων στόχων.

Στο σημείο αυτό, τονίζεται ότι, ένα αποκεντρωμένο ή αποκεντρωτικό σύστημα (decentralized system) διαφέρει από ένα κατανεμημένο σύστημα. Η επεξεργασία ή η αποθήκευση μπορεί να κατανεμηθεί ενώ ο έλεγχος να παραμένει κεντρικός και βασισμένος σε παγκόσμιες πληροφορίες. Ένα κατανεμημένο σύστημα μπορεί φυσικά να είναι και αποκεντρωμένο. Εάν το αποκεντρωμένο σύστημα παρουσιάζει πιο σύνθετη συμπεριφορά, αυτή η συμπεριφορά εφαρμόζεται με έναν αυτο-οργανωμένο τρόπο χωρίς παγκόσμιο έλεγχο. Δεν υπάρχει δηλαδή ανάγκη κεντρικής εξουσίας.

Η οικονομία της χρηματιστήριας αγοράς (στην καθαρή της μορφή) είναι ένα παράδειγμα αποκεντρωμένου συστήματος. Δεν υπάρχει αρχή ελέγχου για επιβολή ποσοστώσεων παραγωγής, διαχείριση της αλυσίδας εφοδιασμού, προγραμματισμό παραδόσεων και ούτω καθεξής. Πολλά βιολογικά συστήματα πραγματικής ζωής είναι αποκεντρωμένα και αυτο-οργανωμένα, και μπορεί να αποτελούνται από μεγάλο αριθμό αυτόνομων μελών που εργάζονται για το κοινό καλό χωρίς κάποιον κυβερνήτη ή γραφειοκρατία.

Αντίθετα, σε ένα συγκεντρωτικό σύστημα (centralized system), υπάρχει μια μεμονωμένη οντότητα που ελέγχει είτε άμεσα είτε έμμεσα - όλα τα στοιχεία χαμηλότερου επιπέδου για την επίτευξη παγκόσμιων στόχων. Η πρόσβαση στις πληροφορίες ελέγχεται από μία αρχή και οι πληροφορίες περνούν συνήθως μέσω ενός μόνο κόμβου. Οποιαδήποτε σύνθετη συμπεριφορά που εφαρμοζεται από το σύστημα προκύπτει από τον κεντρικό έλεγχο, την κατεύθυνση και την επίβλεψη της κεντρικής αυτής οντότητας.

Τα αποκεντρωμένα δίκτυα είναι ένα υποσύνολο αποκεντρωμένων συστημάτων. Αποτελούνται από διασυνδεδεμένους υπολογιστικούς κόμβους που διαμοιράζονται πόρους ή επικοινωνούν μεταξύ τους προκειμένου να επιτύχουν έναν κοινό στόχο. Δεν υπάρχει κεντρική αρχή ελέγχου ή συντονισμού των κόμβων ή της κατάστασης του δικτύου.

Οι κόμβοι σε ένα αποκεντρωμένο δίκτυο έχουν συνήθως την ίδια σχετική κατάσταση (αυτός είναι ο λόγος για τον οποίο συχνά καλούνται δίκτυα peer-to-peer ή P2P). Η συνολική συμπεριφορά προκύπτει από την αλληλεπίδραση κόμβων, καθένας από τους οποίους ακολουθεί σαφώς καθορισμένους κανόνες ή διαδικασίες (που δύναται, αλλά δεν είναι απαραίτητο να είναι πανομοιότυπες). Δεν υπάρχει κανένα σημείο αποτυχίας (single failure point), και το το δίκτυο θα διατηρήσει την λειτουργία του ακόμα και σε μία κατάσταση όπου ένα σημαντικό μέρος των κόμβων του τεθεί εκτός λειτουργίας. Το πρώιμο διαδίκτυο ήταν ουσιαστικά ένα αποκεντρωμένο δίκτυο. Το όραμα του Tim Berners-Lee για τον Παγκόσμιο Ιστό, δηλαδή ένας ιστός που αποτελείται από διασυνδεδεμένο περιεχόμενο, αντανακλά το ίδιο πνεύμα. Μετά τις πρώτες μέρες, τα αποκεντρωμένα δίκτυα άρχισαν να εμφανίζονται στην κορυφή του Διαδικτύου. Ένα από τα πρώτα ήταν το Napster, μια υπηρεσία κοινής χρήσης αρχείων που ξεκίνησε το 1999. Ακολούθησαν άλλες εφαρμογές, συμπεριλαμβανομένου του BitTorrent (ένα πρωτόκολλο για τη διανομή αρχείων μέσω του Διαδικτύου), το Tor (ένα δίκτυο για ανώνυμο επικοινωνίας), καθώς και πολλά άλλα πρωτόκολλα P2P για ροή ήχου και βίντεο. Υπάρχουν επίσης δίκτυα πλέγματος (όπου οι κόμβοι συνδέονται μεταξύ τους άμεσα, δυναμικά και συχνά ασύρματα) και η εμπορική αγορά αναπτύσσεται κατά την ανάπτυξη εφαρμογών IoT και AI.

Για να ανακεφαλαιώσουμε, τα αποκεντρωμένα δίκτυα είναι συστήματα που έχουν πολλά κοινά χαρακτηριστικά:

- Το σύστημα αποτελείται από πολλούς κόμβους, καθένας από τους οποίους είναι ικανός υπολογισμού και ακολουθεί συγκεκριμένους κανόνες ή διαδικασίες.
- Οι κόμβοι αποτελούν δίκτυο. Κάθε κόμβος συνδέεται με έναν ή περισσότερους κόμβους στους οποίους αλληλεπιδρά άμεσα ή επικοινωνεί και με άλλους κόμβους έμμεσα. Δεν χρειάζεται να συνδεθούν ή να λειτουργούν όλοι οι κόμβοι για το δίκτυο για να συνεχίσει να λειτουργεί · δεν υπάρχει κανένα σημείο αποτυχίας.
- Το δίκτυο έχει σκοπό ή χρήση. Μπορεί να λειτουργήσει προς έναν στόχο (ή ένα σύνολο στόχων), ή μπορεί να χρησιμοποιηθεί για κάποιον παραγωγικό και χρήσιμο στόχο.
- Το δίκτυο δεν υπάρχει μεμονωμένα. Μπορεί να ανταλλάσσει πληροφορίες ή ενέργεια με εξωτερικό περιβάλλον ή με άλλα συστήματα. Υπάρχουν οριακές συνθήκες (φυσικές, νομικές ή άλλες μορφές) που περιορίζουν τι το δίκτυο είναι ικανό ή επιτρέπεται να κάνει.

Υπάρχουν πολλά είδη αποκεντρωμένων δικτύων, αλλά ολόκληρος ο τομέας είναι ακόμα πολύ ευρύς για τους σκοπούς μας. Η εστίασή μας είναι δίκτυα που χρησιμοποιούν τεχνολογία blockchain στις λειτουργίες τους. Τα παραδείγματα περιλαμβάνουν Bitcoin, Ethereum, 0x, Filecoin, HyperLedger, Swarm, Polkadot, για να αναφέρουμε μόνο μερικά. Πολλά - αλλά όχι όλα - τέτοια δίκτυα χρησιμοποιούν κρυπτονομίσματα ή ψηφιακά κουπόνια.

## 3.2 Βαθμός αποκέντρωσης

Μπορεί να είναι ασήμαντο να εκτιμηθεί ο πραγματικός βαθμός αποκέντρωσης. Μερικές φορές η εκτίμηση αυτή προκύπτει εύκολα ως εξής: Εάν η τροφοδοσία είναι στα χέρια ενός ιδρύματος ή μιας εταιρείας, η διακυβέρνηση είναι συγκεντρωτική. Αλλά τι γίνεται με μια τεχνοκρατία όπου ο πυρήνας ή η ομάδα κατέχει τη δύναμη; Είναι συγκεντρωτική επειδή υπάρχει μια ομάδα της οποίας η συμμετοχή σπάνια αλλάζει; Ή μήπως είναι αποκεντρωμένη επειδή υπάρχουν, για παράδειγμα, δώδεκα υπεύθυνοι λήψης αποφάσεων;

Αντίστοιχα ας αναλογιστούμε ένα blockchain με κατ' εξουσιοδότηση μηχανισμό απόδειξης πονταρίσματος (delegated proof of stake). Μπορεί να φαίνεται ότι είναι μια αποκεντρωμένη λύση, όμως στην πράξη οι αποφάσεις μπορεί να βασίζονται σε μικρό αριθμό πλούσιων κάτοχων διακριτικών. Κατ' επέκταση αυτής της σκέψης, ποιος θα κρίνει ότι μια ολιγαρχία ή πλουτοκρατία είναι συγκεντρωτική; Αν έπρεπε να σκεφτούμε έναν τεχνικό ορισμό για την αποκέντρωση, είναι προφανές ότι θα ισοδυναμούσε με την απουσία οποιουδήποτε ρόλου που μπορεί να υπαγορεύει αποφάσεις. Είναι λοιπόν ένα σύστημα με δύο ή τρεις ή περισσότερους υπεύθυνους, με πραγματική ισχύ λήψης αποφάσεων, αποκεντρωμένο; Ή είναι ίσως μια ευρύτερη συμμετοχή της κοινότητας που έχουμε πραγματικά στο μυαλό μας όταν μιλάμε για αποκέντρωση;

Η πραγματικότητα είναι ότι όταν μιλάμε για αποκέντρωση σε δίκτυα blochchain υπάρχουν πολλές διαστάσεις που πρέπει να εξετάσουμε, όπως :

- η κατανομή της εξορυκτικής δραστηριότητας,
- οι συνεισφορές στην ανάπτυξη κώδικα,
- η δραστηριότητα σε κρυπτογραφικές συναλλαγές,
- η ιδιοκτησία και η γεωγραφική κατανομή των κόμβων του δικτύου
- η συγκέντρωση της κατοχής των διακριτικών.

Μια πιθανή μέθοδος μέτρησης του βαθμού αποκέντρωσης έγκειται στον υπολογισμό του συντελεστή Gini σε οποιαδήποτε από αυτές τις διαστάσεις. Οι Srinivasan και Lee (2017) πρότειναν ένα δείκτη Nakamoto, υπολογιζόμενο ως ο ελάχιστος αριθμός οντοτήτων που απαιτείται για την επίτευξη άνω του 50% του συνόλου των ενδιαφερομένων (ο δείκτης Satoshi είναι η κανονικοποιημένη έκδοση εκφρασμένη ως ποσοστό).[9]

Πολλοί άλλοι δείκτες είναι δυνατοί και η σωστή μέτρηση της αποκέντρωσης αποτελεί θέμα έρευνας. Υπάρχει ένα μεγάλο μέρος της υπάρχουσας έρευνας στη θεωρία γραφημάτων που θα αποδειχθεί χρήσιμη. Υπάρχουν δείκτες όπως βαθμός, στενότητα, ενδιάμεσος, κεντρικός χαρακτήρας του ιδιοκτήτη κλπ. Τέτοιες αναλύσεις αναπτύχθηκαν αρχικά για τα κοινωνικά δίκτυα, όμως παρόμοιες μέθοδοι έχουν εφαρμοστεί με επιτυχία στην ανάλυση δικτύων υπολογιστών ή μεταφορών και εξάπλωσης ασθενειών. Οι δείκτες κεντρικότητας μπορούν να προσδιορίσουν τις πιο σημαντικές κορυφές σε ένα γράφημα, αλλά η ακρίβειά τους μπορεί να εξαρτάται σε μεγάλο βαθμό από την τοπολογία του δικτύου. Υπάρχει μια ενδιαφέρουσα διπλή προσέγγιση που επιδιώκει να ποσοτικοποιήσει τον ρόλο του μεμονωμένου κόμβου με διάφορα είδη μετρήσεων επιρροής.

Οι Kwon et al. (2019) δείχνουν ότι η πλήρης αποκέντρωση είναι θεωρητικά αδύνατη χωρίς αξιόπιστο τρίτο μέρος και αξιόπιστη διαχείριση ταυτότητας, εκτός εάν το πρωτόκολλο μπορεί

να επιβάλει κόστος Sybil (δηλαδή την προϋπόθεση όπου το κόστος για έναν συμμετέχοντα η εκτέλεση πολλαπλών κόμβων είναι μεγαλύτερη από το συνολικό κόστος για πολλούς συμμετέχοντες, ο καθένας εκτελεί έναν κόμβο). Η ανάλυσή τους περιλαμβάνει μηχανισμούς συναίνεσης, αλλά τα αποτελέσματα ενδέχεται να ισχύουν και για τα μοντέλα διακυβέρνησης.[10]

Υπάρχουν πολύ λίγες μελέτες σχετικά με τον πραγματικό βαθμό αποκέντρωσης στη διαχείριση των συστημάτων blockchain, πιθανώς επειδή είναι δύσκολο να βρεθούν συμπαγή δεδομένα. Στην περίπτωση των Bitcoin και Ethereum, οι Azouvi et al. (2019) εκτίμησαν τον αριθμό των προγραμματιστών που συμβάλλουν στη βάση κώδικα στο Github και τον αριθμό των ατόμων που συμμετέχουν στις συζητήσεις.[11]

Οι μετρήσεις Centrality υποδηλώνουν ότι τόσο το Bitcoin όσο και το Ethereum είναι αρκετά συγκεντρωμένα αναφορικά με τις συμβολές στον κώδικα και γενικά μόνο λίγοι άνθρωποι έχουν τη συνήθεια να συμμετέχουν σε συζητήσεις στο Διαδίκτυο.

Εργαλεία όπως το Alethio και το Ethercan μπορούν να είναι χρήσιμα για την ποσοτικοποίηση και την οπτικοποίηση της συγκέντρωσης σε αποκεντρωμένα δίκτυα. Στο Ethereum, υπάρχει διερευνητική έρευνα από την ConsenSys σε θέματα όπως η διασπορά των διακριτικών ιδιοκτησίας, η συγκέντρωση του πλούτου και η επιρροή των ορυχείων εξόρυξης. Οι Muzzy και Anderson (2019), εκτίμησαν ότι το 2019 τέσσερις κύριες ομάδες αποτελούσαν πάνω από το 72% της τριμηνιαίας παραγωγής μπλοκ και υπήρχαν μόνο δύο ομάδες που μαζί πλήρωσαν σχεδόν το 70% των εξορυκτών . Ωστόσο από γεωγραφικής άποψης, οι κόμβοι στο Ethereum φαίνεται να είναι καλά κατανεμημένοι.[12]

### 3.3 Επίπεδα Διακυβέρνησης σε Αποκεντρωμένες Εφαρμογές Blockchain (Governance in Blockchain D-Apps)

Η διακυβέρνηση είναι απαραίτητη εντός και μεταξύ κρατών, επιχειρήσεων, μη κερδοσκοπικών οργανισμών, κοινωνιών, οικογενειών, ομάδων εργασίας η ομάδων ανθρώπων οποιουδήποτε άλλου σκοπού που συμμετέχουν σε κάποιο αποκεντρωμένο δίκτυο. Θα κάνουμε μια σύντομη αναφορά στην κοινωνία στο παρελθόν και στο σήμερα για να ορίσουμε τον όρο της διακυβέρνησης σε αποκεντρωμένα δίκτυα καθώς μέχρι σήμερα δεν υπάρχουν καθολικά αποδεκτές και κοινές πρακτικές για την άσκηση διακυβέρνησης σε αποκεντρωμένα συστήματα και πρωτόκολλα blockchain.

Η έλλειψη σαφώς ορισμένων διαδικασιών αποφάσεων αποτελεί πρακτική πρόκληση για τους developers αποκεντρωμένων δικτύων. Το γεγονός ότι δεν υπάρχει κάποιο ορισμένο μοντέλο διακυβέρνησης αποδεδειγμένο ότι λειτουργεί καλά, αποτελεί τροχοπέδη σε όποιες αναβαθμίσεις των πρωτοκόλλων ή/και τεχνικές βελτιώσεις. Έτσι μια πιθανή διαφωνία μεταξύ ενδιαφερομένων μπορεί να προκαλέσει το φαινόμενο «protocol fork» και ουσιαστικά την διάσπαση της κοινότητας.

Στην ενότητα αυτή θα γίνει μια επισκόπηση των πολλαπλών επιπέδων διακυβέρνησης που ενδέχεται να επηρεάσουν τη λειτουργία ενός συστήματος blockchain. Η διακυβέρνηση των περισσότερων αποκεντρωμένων εφαρμογών blockchain (Dapps) χωρίζεται σε διαφορετικά επίπεδα που αλληλεπιδρούν μεταξύ τους:

- Το επίπεδο πρωτοκόλλων Διαδικτύου (π.χ. το πρωτόκολλο TCP / IP)
- Το επίπεδο δικτύου blockchain (π.χ. το πρωτόκολλο Ethereum)
- Το επίπεδο framework Dapp (π.χ. Aragon)
- Το επίπεδο Dapp (π.χ. District0x)

Κάθε ένα από αυτά τα επίπεδα έχει σχεδιαστεί και υλοποιηθεί από διαφορετικούς ανθρώπους, με διαφορετικούς σκοπούς, και από ξεχωριστές κοινότητες που ενδέχεται να μην επικοινωνούν η μία με την άλλη. Οι κοινότητες από το κάτω στρώμα της στοίβας συχνά εφαρμόζουν τη δική τους δομή διακυβέρνησης χωρίς να απασχολούνται για τα συστήματα διακυβέρνησης που εφαρμόζονται στα παραπάνω επίπεδα. Παρά την όποια έλλειψη συνέπειας, κάθε ένα από αυτά τα στρώματα εφαρμόζει τη δική του ξεχωριστή δομή διακυβέρνησης, η οποία παραμένει αλληλένδετη με τις δομές διακυβέρνησης των άλλων στρωμάτων. Τα κάτω στρώματα διαδραματίζουν έναν ιδιαίτερα σημαντικό ρόλο, καθώς αποτελούν τη βάση πάνω στην οποία χτίζονται όλα τα άλλα. Επιβάλλουν πώς θα λειτουργούν οι εφαρμογές που αναπτύσσονται στα ανώτερα στρώματα της στοίβας και ορίζουν τι είναι δυνατό να δημιουργηθεί στα υψηλότερα επίπεδα. Για παράδειγμα, το Aragon και το DAOstack είναι Dapps που έχουν κατασκευαστεί πάνω από το Ethereum blockchain και επομένως υπόκεινται στους κανόνες διακυβέρνησης του. Είναι από μόνα τους Dapp frameworks που εφαρμόζουν το δικό τους σύστημα πρωτοκόλλων και κανόνων για το πώς οι άνθρωποι μπορούν να αλληλεπιδράσουν με το Dapp τους ή να δημιουργήσουν νέα Dapps με βάση αυτά. Οι αποκεντρωμένες εφαρμογές (D-Apps) που αναπτύσσονται σε αυτά τα πλαίσια, με τη σειρά τους, θα δημιουργήσουν τα δικά τους πρωτόκολλα και κανόνες για να εξασφαλίσουν τη σωστή λειτουργία και διαχείριση τους. Τελικά, ένα Dapp υπόκειται άμεσα στους δικούς του κανόνες διακυβέρνησης και επηρεάζεται έμμεσα από τους κανόνες του δικτύου blockchain στο οποίο λειτουργεί, τους κανόνες του Ethereum blockchain που διασφαλίζουν την ορθή εκτέλεση των έξυπνων συμβολαίων και τους κανόνες του δικτύου Internet που κάνει τα πάντα να τρέχουν.

## 3.4 On-Chain & Off-Chain Governance

. Διακρίνονται δύο διαφορετικές πτυχές του όρου διακυβέρνησης:

- «Διακυβέρνηση από την υποδομή» και
- «Διακυβέρνηση της υποδομής».

Ανάλογα με την σκοπιά της ανάλυσης, μπορούμε να θεωρήσουμε δύο είδη κανόνων: ενδογενείς για μια συγκεκριμένη κοινότητα και εξωγενείς ως προς αυτήν την κοινότητα. Οι ενδογενείς κανόνες καταρτίζονται από την κοινότητα και για την κοινότητα και ουσιαστικά αποτελούν μια προσπάθεια της κοινότητας για αυτοδιοίκηση. Οι εξωγενείς κανόνες θεσπίζονται ή επιβάλλονται από τρίτο μέρος που είναι εξωτερικό της κοινότητας, αλλά έχει τη δυνατότητα να την επηρεάζει. Θα διερευνήσουμε καθέναν από αυτούς τους παράγοντες.

### 3.4.1 Διακυβέρνηση από την υποδομή

Η διακυβέρνηση από την υποδομή αναφέρεται στη διακυβέρνηση με κωδικοποιημένους κανόνες ενσωματωμένους σε ένα τεχνολογικό σύστημα - στην περίπτωσή μας, ένα σύστημα blockchain. Αυτό συνεπάγεται μια στενή κατανόηση της διαδικασίας λήψης αποφάσεων αναφορικά με την διαδικασία επιβολής των κανόνων, σε αντίθεση με την επεξεργασία και την ανάπτυξη αυτών των κανόνων.

Η διακυβέρνηση από την υποδομή μπορεί να περιλαμβάνει τόσο ενδογενείς κανόνες που προέρχονται από την κοινότητα όσο και εξωγενείς κανόνες που επιβάλλονται εκτός της κοινότητας. Δεδομένου ότι ο ορισμός εξαρτάται από την συγκεκριμένη κοινότητα, η διάκριση του αν ένας συγκεκριμένος κανόνας είναι ενδογενής ή εξωγενής εξαρτάται από την προοπτική της κοινότητας εξέτασης. Αυτό σημαίνει ότι ένας κανόνας μπορεί να είναι ενδογενής από τη μια προοπτική αλλά εξωγενής από την άλλη.

Σε ένα συγκεκριμένο δίκτυο blockchain όπως το Ethereum, οι ενδογενείς κανόνες είναι εκείνοι που κωδικοποιούνται απευθείας στο δίκτυο, όπως το πρωτόκολλο blockchain και ο αλγόριθμος συναίνεσης. Από την προοπτική μιας αποκεντρωμένης εφαρμογής D-App που

αναπτύσσεται πάνω στο δίκτυο Ethereum, οι ενδογενείς κανόνες περιλαμβάνουν όλες τις διαδικασίες λήψης αποφάσεων και τους τεχνικούς κανόνες που ενσωματώνονται στα έξυπνα συμβόλαια που διέπουν την εφαρμογή Dapp - ενώ το υποκείμενο πρωτόκολλο του δικτύου Ethereum θα μπορούσε να θεωρηθεί εξωγενές. Τόσο το δίκτυο blockchain όσο και το Dapp επηρεάζονται από κανόνες κωδικοποιημένους σε ένα σύστημα που είναι εξωγενές με τη δομή διακυβέρνησης του δικτύου ή του Dapp. Για παράδειγμα, τα πρωτόκολλα Internet TCP / IP και άλλα πρωτόκολλα δικτύου επιτρέπουν στους χρήστες να εντοπίζουν και να συνδέονται στο δίκτυο blockchain.

Όταν αυτοί οι κανόνες είναι ενδογενείς σε ένα δίκτυο blockchain, η διακυβέρνηση από την υποδομή αναφέρεται ως «on-chain governance» επειδή οι κανόνες διακυβέρνησης έχουν κωδικοποιηθεί απευθείας στο ίδιο το blockchain. Ως εκ τούτου, αυτοί οι κανόνες θεωρούνται γενικά αμετάβλητοι και αυτο-εκτελέσιμοι, καθώς η κανονική λειτουργία του δικτύου blockchain θα εγγυηθεί την εκτέλεσή τους με ασφαλή και αποκεντρωμένο τρόπο. Φυσικά, οι κανόνες διακυβέρνησης της αλυσίδας μπορούν επίσης να καθορίζουν διαδικασίες για την τροποποίησή τους. Ακριβώς όπως μπορούμε να δημιουργήσουμε νόμους που ορίζουν πώς να φτιάχνουμε, να τροποποιούμε ή να καταργούμε νόμους, μπορούμε να σχεδιάσουμε κανόνες πρωτοκόλλου που ορίζουν διαδικασίες για τη δημιουργία, την τροποποίηση ή την κατάργηση άλλων κανόνων πρωτοκόλλου. Η Tezos, για παράδειγμα, υπόσχεται να δημιουργήσει ένα αυτο-τροποποιημένο blockchain και να δώσει στους συμμετέχοντες τη δυνατότητα να αλλάξουν τους κανόνες του πρωτοκόλλου, συμπεριλαμβανομένων των κανόνων για την αλλαγή των κανόνων.

Η on-chain διακυβέρνηση παρουσιάζει τόσο πλεονεκτήματα όσο και μειονεκτήματα. Στην καλύτερη περίπτωση, η on-chain διακυβέρνηση είναι προβλέψιμη και δίκαιη κατά την εκτέλεσή της. Επειδή η αλλαγή της διαδικασίας ή του αποτελέσματος της υπάρχουσας διακυβέρνησης είναι εξαιρετικά δύσκολη υπόθεση, ολόκληρο το σύστημα είναι απόλυτα διαφανές και ελεγχόμενο. Όλοι μπορούν να δουν γιατί ελήφθη μια συγκεκριμένη απόφαση. Οι «ιδιοτροπίες» των υπευθύνων για τη λήψη αποφάσεων δεν μπορούν εύκολα να επηρεάσουν ή να αλλάξουν τις λειτουργίες του συστήματος. Ωστόσο, δεδομένης της δυσκολίας αλλαγής της on-chain διακυβέρνησης, είναι πιθανόν να παρουσιαστούν νέες και απροσδόκητες καταστάσεις, για τις οποίες δεν υπάρχουν επαρκώς και σαφώς ορισμένες διαδικασίες διαχείρισης. Η ευελιξία μπορεί να βοηθήσει ένα σύστημα να αντιμετωπίσει μοναδικές συνθήκες για τις οποίες δεν είχε κατασκευαστεί, αποφεύγοντας την εκτέλεση προκαθορισμένων διαδικασιών που μπορεί μεν να είναι δίκαιες κατά την εκτέλεσή τους αλλά άδικες στα αποτελέσματά τους. Επομένως, όπου είναι δυνατόν, οι προγραμματιστές θα πρέπει να παρέχουν on-chain διακυβέρνηση με μηχανισμούς που επιτρέπουν αλλαγές στους κανόνες πρωτοκόλλου που υποστηρίζουν το δίκτυο (όπως οι μηχανισμοί Tezos).

### 3.4.2 Διακυβέρνηση της υποδομής

Η «διακυβέρνηση της υποδομής» αναφέρεται σε όλους τους κανόνες που υπάρχουν εκτός μιας τεχνολογικής πλατφόρμας, ωστόσο επηρεάζουν την ανάπτυξη και τη λειτουργία της. Αυτοί οι κανόνες λειτουργούν σε κοινωνικό ή θεσμικό επίπεδο και όχι σε τεχνικό επίπεδο. Στα συστήματα blockchain, η διακυβέρνηση της υποδομής αναφέρεται συχνά ως «διακυβέρνηση εκτός αλυσίδας» επειδή οι κανόνες διακυβέρνησης ισχύουν και λειτουργούν εκτός της υποδομής blockchain. Αυτοί οι κανόνες και οι διαδικασίες δεν εκτελούνται αυτόματα και επομένως ενδέχεται να απαιτείται μια τρίτη αρχή για την επιβολή ή την εποπτεία. Η διακυβέρνηση της υποδομής περιλαμβάνει τόσο ενδογενείς όσο και εξωγενείς κανόνες.

#### *3.4.2.1 Ενδογενείς κανόνες*

Οι ενδογενείς κανόνες αποτελούνται από όλους τους κανόνες, τους κοινωνικούς κανόνες, τα έθιμα και άλλες δομές διακυβέρνησης που αναπτύχθηκαν ή εγκρίθηκαν από μια συγκεκριμένη κοινότητα με σκοπό τη διευκόλυνση του συντονισμού εντός αυτής της κοινότητας. Για παράδειγμα, οι προγραμματιστές στις κοινότητες ανοιχτού κώδικα έχουν επεξεργαστεί και ορίσει διαδικασίες που κωδικοποιούν τους κανόνες και τις διαδικασίες που χρησιμοποιούνται για να αποφασίσουν για τη μελλοντική ανάπτυξη και εξέλιξη ενός έργου λογισμικού ανοιχτού κώδικα. Αυτοί οι κανόνες είναι συνήθως κανόνες ή έθιμα που επιβάλλονται μέσω πίεσης από ομότιμους, αν και η κοινότητα μπορεί επίσης να εφαρμόσει επίσημους μηχανισμούς επιβολής και εποπτείας. Η μη τήρηση αυτών των κανόνων μπορεί να οδηγήσει σε αποκλεισμό από την κοινότητα ή άλλες μορφές κοινωνικής τιμωρίας.

Στο πλαίσιο μιας συγκεκριμένης κοινότητας blockchain, οι ενδογενείς κανόνες περιλαμβάνουν τους κανόνες και τις διαδικασίες που χρησιμοποιούνται για να αποφασίσουν για αλλαγές που θα εφαρμοστούν στο πρωτόκολλο, συμπεριλαμβανομένης της απόφασης για διακλάδωση. Στο Bitcoin, αυτές οι αποφάσεις λαμβάνονται κυρίως μέσω προτάσεων βελτίωσης Bitcoin (BIP) - ενός ανεπίσημου μηχανισμού μέσω του οποίου οι άνθρωποι μπορούν να προτείνουν νέες δυνατότητες και βελτιώσεις στο πρωτόκολλο Bitcoin. Το Ethereum εφάρμοσε ένα παρόμοιο σύστημα για τους ανθρώπους να υποβάλουν προτάσεις βελτίωσης Ethereum (EIPs), μια άτυπη διαδικασία με την οποία οι άνθρωποι μπορούν να προτείνουν ή να ζητήσουν αλλαγές στο πρωτόκολλο ή τον κώδικα Ethereum.

Με την πάροδο του χρόνου, οι άτυπες πρακτικές έχουν γίνει κανόνες στις αναπτυξιακές κοινότητες, αν και αυτές οι πρακτικές δεν είναι καλά τεκμηριωμένες ή ευρέως γνωστές. Για παράδειγμα, τα EIP πρέπει να πληρούν ένα συγκεκριμένο τεχνικό πρότυπο και να υποβάλλονται σε ομότιμους ελέγχους στο διαδίκτυο πριν προχωρήσουν στην ομάδα ανάπτυξης. Από εκεί, τα EIP πρέπει να γίνονται αποδεκτά ομόφωνα από τους βασικούς προγραμματιστές προτού προστεθούν στον χάρτη ανάπτυξης. Ωστόσο, δεν υπάρχει κάποια επίσημη δομή και καμία από αυτές τις συμβάσεις δεν είναι δεσμευτική. Οι αβεβαιότητες σχετικά με τη διαδικασία EIP και ο ρόλος που διαδραματίζει η αναπτυξιακή κοινότητα είναι συχνό σημείο αντιπαράθεσης.

Αφού οι προγραμματιστές ενός συστήματος blockchain υποβάλλουν μια πρόταση, υπάρχει συνήθως ένα σύστημα ψηφοφορίας για να καθοριστεί εάν η κοινότητα την υιοθετεί στο σύνολο της. Για το Bitcoin, οι εξορύκτες ψηφίζουν εκτελώντας νέο λογισμικό με ορισμένες ρυθμίσεις ενεργοποιημένες ή απενεργοποιημένες, υποδεικνύοντας έτσι υποστήριξη ή έλλειψη αυτού. Η σύσταση των κορυφαίων προγραμματιστών είναι συχνά πολύ σημαντική, αλλά δεν είναι καθοριστική. Στο βαθμό που αυτές οι προτάσεις γίνονται αποδεκτές και εφαρμόζονται σε κώδικα, η διακυβέρνηση της υποδομής έχει τη δυνατότητα να επηρεάζει τη διακυβέρνηση από την υποδομή. Με άλλα λόγια, η διακυβέρνηση εκτός αλυσίδας μπορεί να διαμορφώσει ή να επηρεάσει την διακυβέρνηση εντός αλυσίδας ενός συγκεκριμένου δικτύου που βασίζεται σε blockchain. Πράγματι, επειδή η διακυβέρνηση εκτός αλυσίδας προσανατολίζεται γενικά στην επεξεργασία ή την αλλαγή των κανόνων ενός δεδομένου πρωτοκόλλου blockchain, έχει τη δύναμη να τροποποιήσει τη δομή διακυβέρνησης on-chain.

#### *3.4.2.2 Εξωγενείς κανόνες*

Οι εξωγενείς κανόνες είναι όλοι οι άλλοι κανόνες που προέρχονται εκτός κοινότητας αλλά επηρεάζουν τις δραστηριότητες της. Ένα εξέχον παράδειγμα εξωγενούς κανόνα είναι ο νόμος. Παρόλο που ενδέχεται να μην ισχύουν απευθείας σε ένα δίκτυο blockchain, οι εθνικοί νόμοι σίγουρα ισχύουν για τους συμμετέχοντες ενός δικτύου και θα μπορούσαν να επηρεάσουν τη λειτουργία του. Αυτοί οι νόμοι δεν προέρχονται από την κοινότητα, ούτε επιλέγονται από

αυτήν. Επιβάλλονται από μια τρίτη αρχή, συνήθως από μια κυβέρνηση, για τη διασφάλιση της δημόσιας τάξης και της ηθικής και για την προώθηση των συμφερόντων του κοινού γενικά. Επειδή εφαρμόζονται μόνο από μια δεδομένη αρχή, τυχόν παραβιάσεις μπορούν να αποκατασταθούν μόνο από το εθνικό νομικό σύστημα μέσω της επιβολής του νόμου ή των δικαστικών διαδικασιών.

Συμπέρασμα: Η διακυβέρνηση από την υποδομή και η διακυβέρνηση της υποδομής - συνυπάρχουν περισσότερο ή λιγότερο ειρηνικά στο πλαίσιο ενός συστήματος blockchain. Μαζί, συμβάλλουν στη ρύθμιση μιας συγκεκριμένης πλατφόρμας ή υποδομής σύμφωνα με τη δική τους σειρά από μερικές φορές διαφορετικούς ή αντιφατικούς κανόνες. Και οι δύο μηχανισμοί παρουσιάζουν μια σειρά πλεονεκτημάτων και μειονεκτημάτων, τα οποία τα καθιστούν ιδιαίτερα κατάλληλα για συγκεκριμένες καταστάσεις, αλλά όχι για άλλες. Η αλυσίδα διακυβέρνησης εφαρμόζεται γενικά μέσω ενός συστήματος κανόνων, διαδικασιών και κοινωνικών κανόνων που δεν είναι τόσο άκαμπτα και τυποποιημένα όπως αυτά ενός συστήματος που βασίζεται σε κώδικα. Αυτά τα συστήματα είναι πιο ανεπίσημα και μη δομημένα από το αντίστοιχο με βάση τον κώδικα και επομένως είναι πιο περίπλοκα για την επίβλεψη και τον έλεγχο. Ως εκ τούτου, οι χρήστες μπορούν εύκολα να τους παρακάμψουν επειδή δεν υπάρχει αυτόματη επιβολή κανόνων. Τα συστήματα διακυβέρνησης On-chain, αντιθέτως, δεν μπορούν εύκολα να αποφευχθούν ή να παρακαμφθούν, επειδή λειτουργούν σύμφωνα με ένα σύστημα κανόνων που έχουν κωδικοποιηθεί άμεσα στο τεχνολογικό πλαίσιο που είναι υπεύθυνο για την επιβολή τους. Αυτά τα συστήματα είναι επίσης πιο ελεγχόμενα και επαληθεύσιμα από το αντίστοιχο εκτός αλυσίδας, επειδή κάθε συναλλαγή σε ένα blockchain συνοδεύεται από αμετάκλητη και μη αμφισβητήσιμη απόδειξη.

Ωστόσο, το κύριο μειονέκτημα κάθε συστήματος αποτελεί ταυτόχρονα και το πιο ισχυρό πλεονέκτημά του και το αντίστροφο. Ενώ η διακυβέρνηση εκτός αλυσίδας είναι δύσκολο να επιβληθεί λόγω της κοινωνικής της συνιστώσας, έρχεται επίσης με μεγάλη ευελιξία, επιτρέποντας στο σύστημα να αντιδρά γρήγορα και ομαλά σε απρόβλεπτες περιστάσεις και να προσαρμόζεται εύκολα στις αλλαγές στο περιβάλλον. Αντιθέτως, η διακυβέρνηση εντός αλυσίδας μπορεί να υπερέχει να κάνει ό,τι είχε σχεδιαστεί ρητά να κάνει. Αυτοί οι δύο μηχανισμοί - διακυβέρνηση από την υποδομή και διακυβέρνηση της υποδομής - συνυπάρχουν περισσότερο ή λιγότερο ειρηνικά στο πλαίσιο ενός συστήματος blockchain.

### 3.4.3 Διακυβέρνηση εντός αλυσίδας εναντίον Διακυβέρνησης εκτός αλυσίδας

Η τεχνολογία Blockchain, όπως τα έξυπνα συμβόλαια και τα μητρώα καταχωρημένων token, ανοίγουν νέες δυνατότητες στην διακυβέρνηση. Κατ 'αρχήν, πλέον είναι εφικτό να εφαρμοστούν διάφορες διαδικασίες λήψης αποφάσεων σε, on-chain κώδικα υπολογιστή. Το Tezos είναι ένα παράδειγμα blockchain με διακυβέρνηση on-chain. Στην Tezos, οποιοσδήποτε μπορεί να προτείνει αλλαγή παραμέτρων δικτύου με τη μορφή ενημέρωσης κώδικα. Εάν η πρόταση γίνει δεκτή σε ψηφοφορία μέσω αλυσίδας από τους εξορύκτες (καλούνται «bakers» στο Tezos), ο κώδικας ενεργοποιείται σε ένα δοκιμαστικό δίκτυο. Ο νέος κώδικας εκτελείται για μια χρονική περίοδο. Εάν δεν υπάρχουν προβλήματα, και η αποδοχή της πρόταση επιβεβαιωθεί σε δεύτερη ψηφοφορία, ο κώδικας εφαρμόζεται αυτόματα στο κύριο δίκτυο.

Με την on-chain διακυβέρνηση, είναι δυνατές πλέον δομές όπως οι αποκεντρωμένες αυτόνομες οργανώσεις (Decentralised Autonomous Oorganisation). Ο όρος DAO αναφέρεται σε μια οντότητα όπου οι κανόνες διακυβέρνησης είναι κωδικοποιημένοι ως συλλογή έξυπνων συμβολαίων και εκτελούνται όταν απαιτείται. Με άλλα λόγια, ένας DAO είναι ένας οργανισμός όπου οι άνθρωποι ή άλλες οντότητες αλληλεπιδρούν μέσω ενός πρωτοκόλλου που κωδικοποιείται ως ένα πρόγραμμα υπολογιστή. Είναι σπάνιο να βρει κάνεις αμιγείς DAOs.

Συχνά εμφανίζεται κάποια τρίτη οντότητα η οποία συγκεντρώνει όλη την εξουσία ή έχει το αποκλειστικό δικαίωμα του βέτο. Τα blockchains που αναφέρονται ως DAOs περιλαμβάνουν τους οργανισμούς Dash, Decred και MakerDAO.

Ως παράδειγμα του τι λειτουργίες μπορεί να επιτύχει η αλυσίδα, ας υπενθυμίσουμε ότι πολλά αποκεντρωμένα συστήματα μπορούν να θεωρηθούν ως ψηφιακοί κοινοί πόροι. Τα blockchains έχουν ένα πλεονέκτημα σε σύγκριση με άλλα συστήματα κοινών πόρων. Επιτρέπουν την επιβολή κανόνων δικτύου με ελάχιστο κόστος. Η κρυπτογραφία είναι το κλειδί για αυτήν την ικανότητα, επειδή καθιστά πολύ πιο εύκολο για τους υπερασπιστές να επαληθεύουν την αυθεντικότητα των πληροφοριών από ό, τι για τους επιτιθέμενους να εισάγουν διεφθαρμένες πληροφορίες. Για παράδειγμα, μπορεί να υπάρχει ένας συμφωνημένος κανόνας για τον περιορισμό του εύρους ζώνης που καταναλώνεται από οποιονδήποτε συμμετέχοντα στο δίκτυο. Η χρήση του εύρους ζώνης θα μπορούσε να μετρηθεί και η υπερβολική χρήση να τιμωρείται αυτόματα από ένα έξυπνο συμβόλαιο. Η εφαρμογή των αποφάσεων από έναν DAO απαιτεί συχνά κάποια δράση εκτός αλυσίδας. Για παράδειγμα, ένα συμφωνημένο ψήφισμα μπορεί να απαιτήσει αναβάθμιση λογισμικού από κάθε κόμβο σε ένα δίκτυο και αυτοί οι κόμβοι λειτουργούν από άτομα. Ένας DAO μπορεί να χρειάζεται επιπλέον άλλες υπηρεσίες. Ενώ ορισμένες υπηρεσίες μπορούν να αντιμετωπιστούν από αποκεντρωμένες εφαρμογές, η εργασία μπορεί επίσης να πραγματοποιηθεί από μέλη της κοινότητας, άλλους επαγγελματίες ή εταιρείες τρίτων. Οι ψηφιακές πληρωμές για τις υπηρεσίες αποδεσμεύονται από τα έξυπνα συμβόλαια όταν πληρούνται οι προϋποθέσεις για κάτι τέτοιο.

Δεδομένου ότι το βασικό πλεονεκτήματα της τεχνολογίας blockchain είναι η ικανότητα να αποδεικνύεται η κυριότητα των περιουσιακών στοιχείων και να πραγματοποιούνται ασφαλείς ψηφιακές μεταφορές, ένα αποκεντρωμένο ledger είναι το περιβάλλον για ένα DAO. Ωστόσο, το γεγονός, ότι τα κεφάλαια ελέγχονται από κώδικα, κάνει ένα DAO ευάλωτο. Εάν για παράδειγμα, οι αλλαγές του κώδικα ισχύουν αυτόματα μετά την ψηφοφορία μέσω διαδικτύου, ένας συνασπισμός “φαλαινών” (ιδιώτες που κατέχουν μεγάλα αποθέματα του ψηφιακού νομίσματος) με κακόβουλα κίνητρα θα μπορούσαν, καταρχήν, να εγκρίνουν την ανάληψη κεφαλαίων σε ένα DAO.

Υπάρχουν πλατφόρμες που διευκολύνουν τη δημιουργία ενός DAO, συμπεριλαμβανομένων των Aragon, DAOstack, Colony και MetaCartel. Κάθε μία από αυτές τις πλατφόρμες διαθέτει διαφορετικά χαρακτηριστικά και μια κάπως ξεχωριστή φιλοσοφία. Το Aragon για παράδειγμα, είναι αγνωστικό ως προς το μοντέλο λήψης αποφάσεων και προσφέρει ένα σύστημα αδειοδότησης και μια γλώσσα δέσμης ενεργειών το οποίο μπορεί να χρησιμοποιηθεί για τη δημιουργία ενός νέου οργανισμού συνδέοντας διαφορετικές ενότητες μεταξύ τους. Στον οργανισμό Colony, μια πρόταση χρηματοδοτείται γρηγορότερα αν υποστηρίζεται από καλύτερη φήμη. Το DAOstack ενσωματώνει μια αγορά προβλέψεων όπου τα στοιχήματα μπορούν να τοποθετηθούν σε μια πρόταση που γίνεται αποδεκτή ή όχι (αυτό αναγκάζει τους συμμετέχοντες να εστιάσουν την προσοχή τους). Στον Moloch (μια πρωτοβουλία χρηματοδότησης από την κοινότητα Ethereum), οι προτάσεις εξετάζονται διαδοχικά με μία πρόταση ανά πεδίο εφαρμογής την κάθε φορά. Κάθε μελλοντικό μέλος πρέπει να προσφέρει μια θυσία στον Moloch με τη μορφή κάποιας χρήσιμης εργασία ή πρόσθετου κεφαλαίου, και τα υπάρχοντα μέλη ψηφίζουν, στην αλυσίδα, για τη μοίρα του (η μοίρα ως παραδεκτό, ότι είναι).

Η υιοθέτηση της on-chain διακυβέρνησης ή η ανάπτυξη ενός DAO δεν καθιστά απαραίτητα τη διακυβέρνηση ευκολότερη. Με μια σύντομη ανάλυση, αυτά είναι μερικά από τα ζητήματα που θα προκύψουν.

- Ποιος μπορεί να συμμετέχει στη λήψη αποφάσεων και να αναλαμβάνει πρωτοβουλίες;

- Ποια είναι η διαδικασία δημιουργίας νέων πρωτοβουλιών;
- Πώς συνδυάζονται οι προτιμήσεις και διαφορετικές οπτικές γωνίες;
- Εάν χρησιμοποιείται ψηφοφορία, ποια είναι η διαδικασία, η απαρτία και το όριο αποδοχής;
- Ποια είναι τα διοικητικά όργανα;
- Υπάρχει κάποιος διαχωρισμός εξουσιών;
- Ποιος είναι ο μηχανισμός επίλυσης διαφορών;
- Το DAO εφαρμόζει μια νομικά δεσμευτική σύμβαση;
- Ποια είναι τα κίνητρα για συμμετοχή στη διακυβέρνηση;
- Ποια είναι η διαδικασία για την τροποποίηση του κώδικα εάν το DAO πρέπει να προσαρμοστεί;

Η on-chain διακυβέρνηση δεν συνεπάγεται αποκέντρωση. Ένας DAO μπορεί να εφαρμόσει σχεδόν οποιοδήποτε μοντέλο διακυβέρνησης, συμπεριλαμβανομένης της αυτοδυναμίας, της ολιγαρχίας, της αξιοκρατίας ή κάποιου κοινοτικού συστήματος. Με άλλα λόγια, ο βαθμός αποκέντρωσης και ο βαθμός εμπλοκής του ανθρώπου (δηλ. στην αλυσίδα έναντι της αλυσίδας) είναι δύο διαφορετικές διαστάσεις.

### 3.4.4 Νομικά ζητήματα

Τα αποκεντρωμένα δίκτυα δεν υπάρχουν μεμονωμένα. Ανεξάρτητα από το μοντέλο διακυβέρνησης, είναι πιθανό να υπάγονται στην δικαιοδοσία ενός ή περισσότερων κρατών και υπάρχουν ενδιαφερόμενα μέρη όπως οι νομοθέτες, οι ρυθμιστικές αρχές και οι φορολογικές αρχές. Ακόμα κι αν ένα σύστημα ήταν σε πλήρη συμφωνία με τους νόμους ενός έθνους, υπάρχουν και άλλα έθνη όπου οι νόμοι θα είναι διαφορετικοί. Στην πράξη είναι αδύνατο ένα σύστημα να ευθυγραμμιστεί με έως και 200 ή περισσότερα διαφορετικά σύνολα συχνά αντιφατικών νόμων.

Υπάρχει ένας βαθμός αυθαιρεσίας σχετικά με τη σχετική δικαιοδοσία. Μια ελεγκτική οντότητα μπορεί να εδρεύει σε μία χώρα, αλλά κόμβοι δικτύου και χρήστες μπορεί να βρεθούν σε πολλές διαφορετικές χώρες. Εάν χρειαστεί σε κάποια υποπερίπτωση, τα δικαστήρια ή οι ελεγκτικές αρχές μπορούν να εφαρμόσουν κάποιο δίκαιο, απλώς θα πρέπει να καθοριστεί σαφώς σε ποιο εφαρμοστέο δίκαιο υπάγεται η συγκεκριμένη περίπτωση. Από την άλλη πλευρά, εάν οι χρήστες και τα συμβαλλόμενα μέρη κάνουν σαφή ορισμό του ισχύοντος νόμου, τα περισσότερα δικαστήρια θα σεβαστούν αυτήν την επιλογή, υποθέτοντας ότι είναι σωστά διατυπωμένη και καταγεγραμμένη. Οι ενδιαφερόμενοι επενδυτές, πιθανότατα, θα επιλέξουν μια δικαιοδοσία και ένα νομικό σύστημα που θα παρεμβαίνει ελάχιστα στις επιχειρήσεις αποκεντρωμένων δικτύων.

Στην on-chain διακυβέρνηση ή σε DAO, οι διαδικασίες και οι κανόνες αποφάσεων γράφονται σε κώδικα υπολογιστή. Το πλεονέκτημα των έξυπνων συμβολαίων είναι η σαφήνεια, η ντετερμινιστικότητα και η διαφάνεια ενώ δεν υπάρχει περιθώριο παρερμηνείας.

Η εκτεταμένη ανάπτυξη αυτο-εκτελούμενου, αυτόνομου συμβατικού κώδικα μπορεί ακόμη και να οδηγήσει σε νόμο blockchain, ένα υποσύνολο του νόμου που ονομάστηκε lex cryptographia από τους Wright και de Filippi (2015).[13]

Το πρόβλημα είναι το γεγονός ότι τυχόν επίσημοι κανόνες θα είναι ελλιπείς. Ένα έξυπνο συμβόλαιο προϋποθέτει ότι τα κίνητρα είναι οικονομικά και οι αντισυμβαλλόμενοι είναι λογικοί. Αυτές οι υποθέσεις μπορεί να μην ισχύουν πάντα. Θα παρουσιαστούν καταστάσεις που δεν καλύπτονται από τον κώδικα. Σε μια τέτοια περίπτωση, το ζήτημα διευθέτησης, σε κώδικα,

αξιώσεων μεταξύ των μερών που έχουν ισχύ επιχειρήματα που βασίζονται στην ηθική και τη φυσική δικαιοσύνη δεν είναι μια απλή κατάσταση.

Αυτού του είδους οι εκτιμήσεις οδηγούν στο ερώτημα εάν ένα μοντέλο διακυβέρνησης μέσω αλυσίδας πρέπει στην πραγματικότητα να στοχεύει σε μία νομική σύμβαση. Δεν είναι ακόμη σαφές εάν τα έξυπνα συμβόλαια, οι DAO και άλλες αποκεντρωμένες εφαρμογές είναι έτοιμες να λάβουν αναγνώριση από το νόμο (Herian, 2018). [14] Μια δεσμευτική σύμβαση με επιλογή του εφαρμοστέου νόμου θα βοηθούσε στην ελαχιστοποίηση συγκρούσεων μεταξύ των διαφορετικών εθνικών νόμων και μια ρήτρα διαιτησίας θα ήταν χρήσιμος μηχανισμός για την επίλυση διαφορών.

Προς το παρόν, οι DAO δεν είναι νομικά πρόσωπα. Φυσικά, μπορεί κάποια εταιρεία να εγγραφεί σε κάποιον DAO και έτσι να απολαμβάνει την προστασία που προσφέρει μια καθιερωμένη νομική δομή, μαζί με όλα τα αντίστοιχα καθήκοντα και υποχρεώσεις. Αλλά είναι ένας DAO, που ελέγχεται από μια ανώνυμη εταιρεία, ένας πραγματικός αποκεντρωμένος οργανισμός;

Υπάρχει επίσης μια ενδιαφέρουσα ερώτηση για το ποιος κατέχει ένα DAO. Όταν δημιουργείται ένας DAO, τα ψηφιακά νομίσματα που μπορεί να εκδοθούν ενδέχεται να επιτρέπουν στον κάτοχό τους κάποια δυνατότητα ψήφου. Ωστόσο, μόνο τα διακριτικά των ψηφιακών νομισμάτων, που δημιουργούνται σε μια προσφορά διακριτικών ασφαλείας (STO) ή σε παρόμοιο πλαίσιο, δίνουν στον κάτοχο τους νομική κατοχύρωση ιδιοκτησίας. Ειδάλλως, οι κάτοχοι διακριτικών που προέκυψαν από οποιαδήποτε άλλη διαδικασία δεν έχουν κάποια νομική αξίωση ιδιοκτησίας.

Κατά κάποιο τρόπο, οι DAO είναι παρόμοιοι με τις εταιρείες που διαχειρίζονται την εργασία (LMFs). Σε ένα LMF, οι προμηθευτές εργασίας -αντί για τους προμηθευτές κεφαλαίου - κατέχουν την απόλυτη εξουσία, συμπεριλαμβανομένου του δικαιώματος μίσθωσης ή απόλυσης στελεχών. Υπάρχει μια σχετική έννοια της ιδιοκτησίας του διαχειριστή και η εταιρεία ελέγχεται από τους υπαλλήλους και τα άτομα που έχουν ενεργό ρόλο σε αυτήν. Υπάρχουν γιγαντιαίες εταιρείες όπως οι John Lewis, Zeiss και Bosch οι οποίες λειτουργούν με αυτόν τον τρόπο.

Η διαιτησία, από μόνη της, είναι μια ευρέως αποδεκτή και ώριμη μορφή επίλυσης διαφορών εκτός του δικαστικού συστήματος με στόχο την παράκαμψη των αδυναμιών ενός μοντέλου διακυβέρνησης. Υπάρχουν πρωτόκολλα που εμφανίζονται ως πιθανά φόρουμ για διαιτησία blockchain, συμπεριλαμβανομένων των Aragon, Jur, Kleros, Mattereum και Oath.

Για να δημιουργηθεί ένα έξυπνο συμβόλαιο, το έγγραφο με τους συμφωνημένους κανόνες μπορεί να κατακερματιστεί και να αποθηκευτεί σε ένα blockchain με το hash του να περιλαμβάνεται σε οποιαδήποτε μεταγενέστερη συναλλαγή. Εάν προχωρήσουμε περαιτέρω αυτή τη σκέψη, μπορεί να ενσωματώθεί ολόκληρη σύνταξη όρων παροχής υπηρεσιών του δικτύου. Εάν ένας χρήστης υπογράψει κρυπτογραφικά τους όρους, το συμβόλαιο θα έχει καλές πιθανότητες αν χρειαστεί να παραστεί σε δικαστήριο.

### 3.4.5 Συντονισμός

Ένας μηχανισμός συντονισμού αποτελεί ουσιαστικό μέρος της διακυβέρνησης. Χωρίς συνεργασία και συντονισμό καθίσταται αδύνατον να επιλυθούν συγκρούσεις, διαφορές και να γίνει κατανομή των πόρων σε μια κοινότητα ή μια κοινωνία.

Εάν υπάρχει περιορισμένος αριθμός υπευθύνων λήψης αποφάσεων ή σχετικά μικρή ομάδα βασικών προγραμματιστών αρκεί απλά η επικοινωνία μεταξύ των ατόμων ώστε να επιτευχθεί

συναίνεση. Δύναται να υπάρχουν επίσημα βήματα σε αυτήν τη διαδικασία, όπως φόρουμ και λίστες αλληλογραφίας και απομακρυσμένες ή προσωπικές συναντήσεις.

Υπάρχουν γνωστά δίκτυα (συμπεριλαμβανομένων των Bitcoin και Ethereum) όπου ο συντονισμός βασίζεται στην επίτευξη της συναίνεσης εντός μιας ομάδας βασικών προγραμματιστών ή κάποιου άλλου εσωτερικού κύκλου. Υπάρχει συνήθως μια καλά καθορισμένη διαδικασία για τον χειρισμό προτάσεων βελτίωσης, δηλαδή με προτεινόμενες αλλαγές στη βάση κώδικα ή στις παραμέτρους δικτύου. Παρακάτω παρουσιάζονται τα βασικά βήματα που επιτελούνται σε μια τέτοια διαδικασία:

1. Ένας συνεργάτης έρχεται με μια ιδέα για τον τρόπο τροποποίησης ή αναβάθμισης του δικτύου. Αυτός ή αυτή γράφει μια πρόταση και τη δημοσιεύει στο GitHub ή σε κάποιο άλλο συμφωνημένο αποθετήριο.

2. Διενεργείται συζήτηση σε συναντήσεις προγραμματιστών, μέσω τηλεδιάσκεψης, σε κοινοτικά κανάλια, διαδικτυακά φόρουμ ή λίστες αλληλογραφίας.

3. Οι βασικοί προγραμματιστές εξετάζουν την πρόταση, παρέχουν σχόλια, συζητούν τα πλεονεκτήματα και τα μειονεκτήματα, εξετάζουν τους κινδύνους και στοχεύουν στην συναίνεση εκτός αλυσίδας.

4. Λαμβάνεται απόφαση. Η πρόταση ενδέχεται να εγκριθεί εάν η πρόταση είναι τεχνικά βιώσιμη, διατίθεται σχετική χρηματόδοτησηγαι την πρόταση και επιτυγχάνεται συναίνεση.

5. Η αλλαγή εφαρμόζεται. Σε ορισμένα δίκτυα, οι βασικοί προγραμματιστές θα εφαρμόσουν την αναβάθμιση. σε άλλους (όπως το Bitcoin), η αναβάθμιση χρειάζεται εφαρμογή από την πλειονότητα των εξορρυκτών.

## 3.5 Decentralized Governance Models Principles

Δεδομένου του πλήθους των πιθανών μοντέλων διακυβέρνησης, προκύπτει το ερώτημα πως ορίζεται η σωστή διακυβέρνηση. Η απάντηση εξαρτάται προφανώς από το δίκτυο, τον σκοπό του και την κουλτούρα της κοινότητας. Η καλή διακυβέρνηση μπορεί να είναι κατανοητή ως ένα μοντέλο αποτελούμενο από κανόνες, διαδικασίες και θεσμούς που εκπληρώνει τα συμφέροντα και ικανοποιεί τις προτιμήσεις των ενδιαφερομένων μερών.

Κάποιοι έχουν την τάση να πιστεύουν ότι η διακυβέρνηση θα λειτουργήσει από μόνη της χωρίς βασικούς κανόνες, και ότι σε κάθε περίπτωση λίγη αναρχία στο παχνίδι δεν είναι τόσο άσχημη συνθήκη. Ωστόσο, μια συγκεκριμένη δομή είναι απαραίτητη για την ορθή διακυβέρνηση.

Ένα σημαντικό ερώτημα σχετικά με τη δομή της διακυβέρνησης είναι αν είναι συγκεντρωτική, αποκεντρωμένη ή κάτι ενδιάμεσο. Οι αποκεντρωμένες δομές προσφέρουν δυνατότητες μεγαλύτερης ποικιλομορφίας με διαφορετικές απόψεις που καλύπτονται από τοπικές μονάδες ή τα ίδια τα άτομα. Η διακυβέρνηση μπορεί να γίνει πιο αποτελεσματική εάν επιτρέπεται σε τέτοιες οντότητες να ανταποκρίνονται σε προβλήματα ή απρόβλεπτες καταστάσεις εγκαίρως και βάσει τοπικών πληροφοριών. Η αποκεντρωμένη διακυβέρνηση μπορεί επίσης να θεωρηθεί ως υψηλού βαθμού εάν η εξουσία ασκείται από φορείς γνωστούς στην κοινότητα.

Η αποκέντρωση μπορεί να αναλυθεί σε τρεις άξονες:.

- Η πολιτική αποκέντρωση είναι η μεταφορά εξουσίας και πόρων από την κεντρική κυβέρνηση σε χαμηλότερο επίπεδο. Σε εθνικά κράτη, η αποκέντρωση μπορεί να περιλαμβάνει τη δημιουργία νέων υπο-εθνικών ή περιφερειακών δικαιοδοσιών, θέλοντας να διεξάγει τοπικές εκλογές και να επιτρέπει στους τοπικούς αξιωματούχους να λαμβάνουν αποφάσεις χωρίς προηγούμενη έγκριση από ψηλά. Στις περισσότερες περιπτώσεις, η εκ των υστέρων παρακολούθηση αναμένεται να παραμείνει.

- Απαιτείται δημοσιονομική αποκέντρωση για να υπάρξει ουσιαστική πολιτική αποκέντρωση. Τοπικά όργανα λήψης αποφάσεων χρειάζονται επαρκείς οικονομικούς πόρους για την αποτελεσματική εκτέλεση των καθηκόντων τους. Πιθανές πηγές χρηματοδότησης αποτελούν οι φόροι, ή χρεώσεις ανά χρήση υπηρεσιών ή μεταφορά εσόδων από την κεντρική αρχή.

- Η οικονομική αποκέντρωση μεταφράζεται στην ανάθεση δημόσιων λειτουργιών μέσω της ιδιωτικοποίησης των δημοσίων υπηρεσιών κοινής ωφέλειας. Εταιρείες, συνεταιρισμοί, εθελοντικές ομάδες και άλλες μη κυβερνητικές οργανώσεις θα πρέπει να μπορούν να πραγματοποιούν και να χρεώνουν υπηρεσίες που προηγουμένως μονοπωλούνταν από την κυβέρνηση.

Ενώ υπάρχουν σαφή επιχειρήματα υπέρ των συστημάτων αποκεντρωμένης διακυβέρνησης, δεν λείπει και η αντίθετη κριτική. Η αποκέντρωση μπορεί να οδηγήσει σε απώλεια οικονομιών κλίμακας, αργή λήψη αποφάσεων, αδυναμία συντονισμού του συνολικού σύστηματος και την απώλεια ελέγχου των σπάνιων πόρων.

Όπως συζητήθηκε, η ύπαρξη μιας καλά καθορισμένης δομής είναι σημαντική. Εάν δεν υπάρχουν θεσμοί και δεν υπάρχει διαφάνεια και σαφώς ορισμένες διαδικασίες διακυβέρνησης, κάποιοι μπορεί να μπουν στον πειρασμό να χρησιμοποιήσουν το σύστημα προς όφελός τους. Η επίλυση των διαφορών θα χρειαστεί αργά ή γρήγορα καθώς η σύγκρουση μεταξύ των ενδιαφερομένων είναι αναπόφευκτη. Ένα καλό μοντέλο διακυβέρνησης παρέχει ένα πλαίσιο για την ειρηνική επίλυση των διαφορών και μειώνει τον κίνδυνο διάσπασης της κοινότητας. Είναι συνετό να έχει προσυμφωνηθεί και οριστεί μια διαδικασία συνδυασμού διαφορετικών απόψεων προς επίλυση πιθανών διαφορών που ενδέχεται να προκύψουν. Για παράδειγμα, ο μηχανισμός συναίνεσης μπορεί να επιτρέψει στην κοινότητα να διαλύσει την εκτελεστική εξουσία και να προκαλέσει επανεκλογή, παρόμοια με μια αρνητική ψήφο εμπιστοσύνης στα πολιτικά συστήματα.

Απαιτείται η συμμόρφωση των ενδιαφερομένων με τους κανόνες. Ένα unpermissioned αποκεντρωμένο δίκτυο αποτελεί έναν δημόσιο πόρο και απαιτείται η παρακολούθηση του τόσο για την πρόληψη της κατάχρησης όσο και για την κοινή χρήση ανταμοιβών με δίκαιο τρόπο. Η κρυπτογραφία και οι μηχανισμοί της αλυσίδας μπορούν να χρησιμοποιηθούν για την αυτοματοποίηση αυτής της λειτουργίας π.χ. τιμωρία της υπερβολικής κατανάλωσης του πόρου ή με διανομή μικρο-πληρωμών έναντι επαληθευμένης εργασίας. Τα κίνητρα είναι σημαντικά για τις λειτουργίες δικτύου καθώς και για τη διακυβέρνησή του. Υπάρχουν οικονομικά, κοινωνικά, ηθικά και ψυχολογικά κίνητρα. Τα κοινωνικά κίνητρα λειτουργούν καλά σε μικρότερες ομάδες ατόμων (όπως οι βασικοί προγραμματιστές) στις οποίες είναι μέλη και βρίσκονται σε συχνές φυσικές συναντήσεις. Οι προγραμματιστές μπορούν επίσης να παρακινηθούν από την κοινωνική αναγνώριση για τις συνεισφορές τους και από καθαρή απόλαυση από την εργασία στο έργο. Αλλά οι προγραμματιστές δεν επιβιώνουν μόνο με αναγνώριση: πρέπει επίσης να απολαμβάνουν οικονομικές ανταμοιβές. Ο συντονισμός είναι, λοιπόν, ουσιαστικό μέρος της λειτουργικής διακυβέρνησης καθώς θα πρέπει να περιλαμβάνει τη συγκέντρωση διαφορετικών απόψεων και αποτελεσματική κατανομή των πόρων είτε μέσω μιας διαδικασίας αναζήτησης συναίνεσης είτε με άλλα μέσα. Οι διαδικασίες αναζήτησης συναίνεσης μπορεί να λειτουργούν καλά όταν η πραγματική ομάδα λήψης αποφάσεων είναι μικρή. Για να είναι οι απόψεις της ευρύτερης κοινότητας ταυτισμένες και συμφιλιωμένες, η διεξαγωγή ψηφοφορίας είναι μια πρακτική εναλλακτική λύση.

Η ύπαρξη ενός συντάγματος ως βάση διακυβέρνησης είναι εξίσου καλή ιδέα στον αποκεντρωμένο χώρο ως ένα διαφανές θεμέλιο οργανώσεων και πολιτικών οντοτήτων. Η κοινότητα, ως αποτέλεσμα, αυτο-επιλέγει μια ομάδα ανθρώπων. Το πολιτιστικό στοιχείο του συντάγματος μπορεί επομένως να αναδυθεί φυσικά σε αποκεντρωμένα δίκτυα και να

ενσωματώνει αξίες όπως η ιδιωτικότητα, η ελευθερία, η αυτονομία, η διαφάνεια και η δημοκρατία. Υπάρχουν ήδη δίκτυα με σύνταγμα, χάρτη, μανιφέστο ήδη είτε σε ισχύ είτε σε ανάπτυξη. Σε αυτά περιλαμβάνονται έργα όπως το Aragon (2018), το Civil (2018), το Decred (2019) και το Saga (2020) ενώ αναμένεται να ακολουθήσουν περισσότερα νέα ανάλογα έργα.

Είναι καλή ιδέα για την κοινότητα να βρίσκεται σε τακτική αλληλεπίδραση στο διαδίκτυο ως προς τη διαχείριση του έργου. Τα φόρουμ και οι εκδηλώσεις εκτός σύνδεσης βοηθούν προφανώς, αλλά και οι επίσημες έρευνες μπορούν να είναι χρήσιμες όπως η πρόσφατη έρευνα διακυβέρνησης στην κοινότητα Ethereum (Beylin, 2019). [15]

# 4. Ερευνητικές Προσεγγίσεις σχετικά με Blockchain Voting

## 4.1 Ψηφιακή ψηφοφορία

Οι περισσότερες εκλογές στον φυσικό κόσμο χρησιμοποιούν χάρτινα ψηφοδέλτια, ακόμα κι αν ο υπολογισμός γίνεται συχνά με υπολογιστές. Από την δεκαετία του 1960, η ηλεκτρονική ψηφοφορία επί τόπου έχει χρησιμοποιηθεί σε πολλές χώρες. Το επόμενο βήμα είναι η απομακρυσμένη ηλεκτρονική ψηφοφορία (μέσω του Διαδικτύου), και χρησιμοποιείται στην Εσθονία και σε πολλά καντόνια στην Ελβετία. Ένα σύστημα βασισμένο σε blockchain δοκιμάστηκε στο Zug (Allen, 2018). [16]

Η απομακρυσμένη ψηφοφορία φέρνει πιθανά πλεονεκτήματα με τη μορφή χαμηλότερου κόστους, ταχύτερης μέτρησης, περισσότερης ευκολίας (και ως εκ τούτου καλύτερη συμμετοχής) και ευκολία πρόσβασης από εκείνους που ζουν στο εξωτερικό. Από την άλλη πλευρά, η ηλεκτρονική ψηφοφορία μπορεί να επιδεινώσει το ενδεχόμενο απάτης στις εκλογές. Τα μέτρα αποτροπής που λειτουργούν στον φυσικό κόσμο δεν μεταφέρονται εύκολα στο διαδίκτυο. Η αδύναμη κρυπτογράφηση ή τα σφάλματα λογισμικού μπορούν να κάνουν το σύστημα ευάλωτο σε χειρισμούς από απόσταση και μάλιστα σε τεράστια κλίμακα.

Η χειραγώγηση των ψηφοφόρων μπορεί να έχει πολλές μορφές, όπως επιρροή από τρίτα μέρη, αγορά ψήφων, αντίποινα ψηφοφόρων κ.λπ. Απαιτούνται δύο στοιχεία για την ψηφιακή μεταφορά και αναπαραγωγή των εκτός αλυσίδας ιδανικών μιας δίκαιης ψηφοφορίας: Επαλήθευση και εμπιστευτικότητα. Η επαλήθευση καλύπτει ζητήματα όπως ο αξιόπιστος έλεγχος της καταλληλότητας των ψηφοφόρων, αποδεικνύοντας ότι οι ψήφοι καταγράφονται πιστά και τα αποτελέσματα προκύπτουν επίσης σωστά. Η εμπιστευτικότητα μεταφράζεται στη μυστικότητα της ψηφοφορίας, έτσι ώστε η ψήφος να μην μπορεί να συσχετιστεί με την πραγματική ταυτότητα του ψηφοφόρου,την διεύθυνση πορτοφολιού ή κάποιο άλλο αναγνωρίσιμο χαρακτηριστικό.

Η κρυπτογραφία μπορεί να βοηθήσει στην επίτευξη της εμπιστευτικότητας στα ψηφιακά ψηφοδέλτια (Chaum et al., 2010). [17] Μία πιθανή τεχνική αποτελούν τα μικτά δίκτυα (mixed networks) (ένα σύνολο διακομιστών διαλογής που τρέχουν ένα mixnet πάνω από κρυπτογραφημένες ψήφους, με αποτέλεσμα την τυχαία παραλλαγή των ψήφων πριν από τη μέτρηση.
Εναλλακτική αποτελεί η ομοιομορφική κρυπτογράφηση (όπου ένας διακομιστής προσθέτει όλες τις κρυπτογραφημένες ψήφους και αποκρυπτογραφεί το αποτέλεσμα, έτσι ώστε οι μεμονωμένες ψήφοι να μην αποκρυπτογραφούνται ποτέ). Επίσης, είναι διαδεδομένη και η τεχνική των τυφλών υπογραφών, μια μυστική ανταλλακτική λειτουργία όπου ο διακομιστής εξουσιοδότησης δεν γνωρίζει τι υπέγραψαν ψηφιακά οι ψηφοφόροι.

Οι αλυσίδες blockchain με τα αμετάβλητα ίχνη ελέγχου τους μπορεί να φαίνονται σαν μια προφανής επιλογή για μια πλατφόρμα ψηφιακών εκλογών. Ωστόσο, η τεχνολογία blockchain μπορεί να κάνει τη ζωή ευκολότερη για όσους έχουν την τάση να χειραγωγούν ψηφοδέλτια. Με κάποια ευχέρεια στο προγραμματισμό και την κρυπτογραφία, μπορεί κανείς να δημιουργήσει μια αυτοματοποιημένη αγορά ψήφων και ένα έξυπνο συμβόλαιο μπορεί επαληθεύσει ότι λάβατε αυτό που πληρώσατε πριν αποζημιώσετε τους πωλητές. Σε αντίθεση με τον φυσικό κόσμο, ο καθένας εμπλεκόμενος έχει πολύ μικρότερο κίνδυνο να συλληφθεί.

Προκειμένου να αποφευχθεί η αγορά ψηφοφορίας, ένα ψηφιακό σύστημα ψηφοφορίας δεν πρέπει να παρέχει αποδείξεις (κρυπτογραφικά ή διαφορετικά) για τα περιεχόμενα της ψήφου. Εάν δεν μπορείτε να αποδειχθεί ποιο πλαίσιο έχει επιλεχθεί, τότε ένας εισβολέας δεν μπορεί να υπαγορεύσει αξιόπιστα τις επιλογές. Στην ρευστή δημοκρατία, ωστόσο, είναι αναγκαία αυτή η ιδιότητα: Ένας εκπρόσωπος χρειάζεται τη δυνατότητα να αποδείξει στους πρωταρχικούς κατόχους ψήφων πώς ψήφισαν.

Τα κατ 'εξουσιοδότηση συστήματα ψηφοφορίας - όπως χρησιμοποιούνται στις περισσότερες DPoS αλυσίδες blockchain - είναι ευάλωτα σε αναταραχές αλλά με άλλους τρόπους. Για παράδειγμα, ένα καρτέλ παραγωγών μπλοκ μπορεί να συνεργαστεί με σκοπό να θέσουν λογαριασμούς που απειλούν τις κερδοφόρες θέσεις τους σε μαύρη λίστα. Ή ο συνασπισμός κόμβων μπορεί να ψηφίσει έναν άλλο για να διατηρήσει την εξουσία του. Μια πλουτοκρατία μπορεί να προκαλέσει προκατάληψη των ψηφοφοριών. Ως πραγματικό παράδειγμα, όταν τέθηκε τον Οκτώβριο του 2019 σε ψηφοφορία επί της αλυσίδας μια παράμετρος συστήματος στο MakerDAO (τέλος σταθερότητας DAI). Το αποτέλεσμα δεν μπορεί να περιγραφεί ως αποτέλεσμα κοινής συναίνεσης. Ένα μεμονωμένο άτομο (το οποίο είχε τότε το 7,5% της προσφοράς μάρκας) χειραγώγησε τις εκλογές με 94% των ψήφων (Onggunhao, 2019).[18]

Είναι δύσκολο να βρεθούν αναλυτικά στοιχεία σχετικά με τη συμμετοχή σε ψηφοφορίες εντός της αλυσίδας, αλλά τα στοιχεία δείχνουν ότι μόνο λίγοι κάτοχοι διακριτικών λαμβάνουν μέρος (Learner, 2019). [19] Στις περισσότερες περιπτώσεις, η προσέλευση έχει πέσει κάτω από το 10%, αν και υπήρξαν θετικές εξαιρέσεις (π.χ. Decred Politeia # Pi4 στο 32%, Cosmos Proposal 1 στο 38%, Tezos Athens στο 50% ή παραπάνω και Decred Lightning στο 54%). Η παρουσία φαλαινών μπορεί να παρακάμψει σημαντικά αυτούς τους αριθμούς, και η προσέλευση μπορεί να μειωθεί δραματικά εάν μετρηθεί σε όρους διευθύνσεων πορτοφολιών που συμμετέχουν. Υπάρχουν τρόποι για να προαχθεί η συμμετοχή της κοινότητας. Για παράδειγμα, ένα δίκτυο μπορεί να διατηρήσει αυτόματα μια βαθμολογία φήμης για κάθε χρήστη και να προσαρμόζεται η επιρροής των χρηστών στη διακυβέρνηση σύμφωνα με τη βαθμολογία τους. Ο διαμοιρασμός tokens μπορεί να είναι κίνητρο για ψηφοφορία μέσω πονταρίσματος ή με ανακατανομή των tokens μεταξύ αυτών που συμμετείχαν. Σαν αντεπιχείρημα, οι άνθρωποι δεν πληρώνονται για να ψηφίσουν στις πολιτικές εκλογές. Όσοι ενδιαφέρονται πραγματικά για το τι συμβαίνει στην χώρα ή την κοινωνία τους θα λάβουν μέρος στη συζήτηση, θα ψηφίσουν και θα συμμετάσχουν με άλλους τρόπους.

Σε συστήματα ενός ατόμου με μία ψήφο, η ίδια η ανωνυμία των μπλοκ αλυσίδων μπορεί να αποτελέσει εμπόδιο για τη δίκαιη ψηφοφορία. Σε μια επίθεση του Sybil, ένα κακόβουλο μέρος μπορεί να αποκτήσει δυσανάλογη επιρροή δημιουργώντας μεγάλο αριθμό ψεύτικων ταυτοτήτων ή διευθύνσεων που φαίνεται να είναι γνήσια. Αυτό δημιουργεί ένα δίλημμα. Επειδή θέλουμε να διατηρήσουμε μυστική την ψηφοφορία, δεν θέλουμε να γνωρίζουμε τις ταυτότητες των ψηφοφόρων. Από την άλλη πλευρά, θέλουμε επίσης να βεβαιωθούμε ότι κανείς δεν μπορεί να ψηφίσει περισσότερες από μία φορές. Ένας τρόπος για να δημιουργήσουμε έναν μηχανισμό ψηφοφορίας ανθεκτικό στον εξαναγκασμό είναι ο έλεγχος ταυτότητας κάθε ψηφοφόρου αλλά η διατήρηση του ελέγχου μηχανισμού ταυτότητας ξεχωριστά από το πραγματικό (ψηφιακό) εισιτήριο ψηφοφορίας. Μόλις επικυρωθεί, στον ψηφοφόρο δίνεται ένα μοναδικό ψηφιακό διακριτικό (ένα ζευγάρι ιδιωτικών και δημόσιων κρυπτογραφικών κλειδιών) καθώς και μια λίστα διευθύνσεων που αντιπροσωπεύουν τις εναλλακτικές λύσεις στην ψηφοφορία.

Τα κουπόνια δημιουργούνται από ένα αξιόπιστο τρίτο μέρος ή από έναν ασφαλή αποκεντρωμένο μηχανισμό, έτσι ώστε να μην είναι ανιχνεύεται στην ταυτότητα των ψηφοφόρων. Στη φάση καταμέτρησης, τα διακριτικά επικυρώνονται τυφλά (χρησιμοποιώντας ένα mixnet, για παράδειγμα) έναντι του αρχική λίστα ψηφοφόρων. Αυτή είναι η ουσία συστημάτων απομακρυσμένης ψηφοφορίας ανθεκτικά στον εξαναγκασμό, όπως το Civitas (Clarkson et al., 2008) [20].

## 4.2 Θεμελιώδεις Αρχές Ψηφοφοριών

Η ψηφοφορία δεσμευτικού χαρακτήρα διέπεται από συνταγματικά κατοχυρωμένες καταστατικές αρχές.[21] Το 2002, το Συμβούλιο της Ευρώπης υιοθέτησε έναν κώδικα καλής πρακτικής για εκλογικά θέματα ο οποίος αναγνωρίζει πέντε θεμελιώδεις αρχές για τη διενέργεια δημοκρατικών εκλογών:

- Καθολική ψηφοφορία (universal suffrage): Κάθε πολίτης έχει το δικαίωμα ψήφου και εκλογής εφόσον πληροί τις προϋποθέσεις που ορίζει ο νόμος πχ ηλικία και εθνικότητα).
- *Ισότητα της ψήφου και των ψηφοφόρων (equal suffrage)*: Κάθε πολίτης δικαιούνται μια ψήφο και όλες οι ψήφοι είναι μεταξύ τους ισοδύναμες.
- *Ελευθερία της ψήφου και της ψηφοφορίας (free suffrage)*: Ο ψηφοφόρος έχει το δικαίωμα να εκφράσει τη βούλησή του ελεύθερα και χωρίς κανένα εξαναγκασμό ή άσκηση πίεσης.
- *Μυστικότητα της ψήφου (secret suffrage)*: Ο ψηφοφόρος έχει το δικαίωμα να ψηφίσει μυστικά.
- *Αμεσότητα της ψήφου και της ψηφοφορίας (direct suffrage)*: Οι ψήφοι που έχουν υποβληθεί από τους ψηφοφόρους καθορίζουν απευθείας το εκλογικό αποτέλεσμα.

Σε ένα σύστημα ηλεκτρονικής ψηφοφορίας, η εφαρμογή των πέντε καταστατικών αρχών προσδιορίζει ένα σύνολο θεμελιωδών απαιτήσεων ασφάλειας που πρέπει να ικανοποιούνται. Οι απαιτήσεις αυτές είναι οι εξής:

- *Δημοκρατικότητα*: Ένα σύστημα χαρακτηρίζεται δημοκρατικό αν και μόνο αν νόμιμοι ψηφοφόροι δικαιούνται να ψηφίσουν.
- *Ορθότητα – Ακρίβεια*: Η ορθότητα απαιτεί ότι το αποτέλεσμα της ψηφοφορίας που ανακοινώνεται είναι το πραγματικό αποτέλεσμα των εκλογών.
- *Μυστικότητα*: Σχετίζεται με το γεγονός ότι όλες οι ψήφοι παραμένουν μυστικές σε όλη τη διάρκεια της ψηφοφορίας αλλά και μετά τη λήξη της.
- *Μη αναγκαιότητα έκδοσης απόδειξης*: Το κρυπτογραφικό πρωτόκολλο που χρησιμοποιεί το σύστημα είναι σε θέση να πείθει τον ψηφοφόρο ότι η ψήφος του καταμετρήθηκε στο τελικό αποτέλεσμα χωρίς όμως να μπορεί να παρέχει απόδειξη γι' αυτό.
- *Προστασία από εξαναγκασμό*: Κανένας ψηφοφόρος δεν κατέχει ούτε είναι σε θέση να δημιουργήσει μία απόδειξη που να δείχνει το περιεχόμενο της ψήφου του.
- *Δικαιοσύνη*: Η απαίτηση αυτή διασφαλίζει ότι κανείς δεν μπορεί να μάθει το αποτέλεσμα της ψηφοφορίας πριν από την τελική καταμέτρηση των ψήφων και την επικύρωση του αποτελέσματος.
- *Επαληθευσιμότητα* : Σχετίζεται με την ύπαρξη μηχανισμών ελέγχου της διαδικασίας ψηφοφορίας προκειμένου αυτοί να εξασφαλίσουν ότι όλες οι ψήφοι παραλήφθηκαν κανονικά και καταμετρήθηκαν σωστά.
- *Επαληθεύσιμη συμμετοχή*: Διασφαλίζει ότι υπάρχει δυνατότητα να βρεθεί αν ένας συγκεκριμένος συμμετείχε ή όχι στην ψηφοφορία.
- *Ανθεκτικότητα*: Εγγυάται ότι δεν μπορεί να λάβει χώρα μια προσωρινή συνεργασία είτε ψηφοφόρων είτε αρχών η οποία θα μπορούσε να διακόψει τη διαδικασία ψηφοφορίας.

## 4.3 On Chain Μηχανισμοί ελέγχου ταυτότητας των ψηφοφόρων

Υπάρχουν διαφορετικοί τρόποι ελέγχου ταυτότητας των ψηφοφόρων. Για παράδειγμα, μπορεί να επαληθευτεί η πραγματική ταυτότητα με λογισμικό αναγνώρισης προσώπου που συγκρίνει έγγραφα ταυτότητας με μια φωτογραφία ή βίντεο του προσώπου. Ωστόσο, η τεχνολογία μπορεί να είναι ακριβή και αναξιόπιστη και θα πρέπει κανείς στην περίπτωση αυτή να εμπιστευτεί όποιον παρέχει την υπηρεσία επαλήθευσης, όπως για παράδειγμα η εφαρμογή Voatz. Η Voatz έχει συνάψει σύμβαση με την εταιρεία ελέγχου ταυτότητας Jumio με έδρα το Palo Alto, για την εκτέλεση απομακρυσμένου ελέγχου ταυτότητας. Η διαδικασία ελέγχου ταυτότητας απαιτεί από έναν ψηφοφόρο που χρησιμοποιεί την εφαρμογή Voatz αποκλειστικά στο iPhone να στείλει στον Jumio μια φωτογραφία της άδειας οδήγησης ή της σελίδας φωτογραφίας διαβατηρίου μαζί με ένα σύντομο, ζωντανό selfie βίντεο του προσώπου τους. Το Jumio χρησιμοποιεί λογισμικό σύγκρισης προσώπου με μηχανική εκμάθηση για να προσδιορίσει εάν το πρόσωπο στο αναγνωριστικό ταιριάζει με αυτό του βίντεο. Εάν ταυτοποιηθεί, ο ψηφοφόρος πιστοποιείται. Οι ερευνητές αμφισβήτησαν την αποτελεσματικότητα της χρήσης μιας μικρής φωτογραφίας άδειας οδήγησης ή μιας διαβατηρίου για έλεγχο ταυτότητας και σημείωσαν ότι αυτές οι φωτογραφίες μπορούν να είναι έως και 10 ετών. Μεταξύ άλλων προβλημάτων, σημείωσαν επίσης ότι τα συστήματα σύγκρισης προσώπου έχουν ανακαλυφθεί ότι έχουν υψηλά ποσοστά σφάλματος, ειδικά για μειονότητες.

Μια άλλη δυνατότητα είναι να χρησιμοποιηθεί η διεύθυνση ενός διακριτικού ενός πορτοφολιού ως ταυτότητα. Αυτή η επιλογή δεν είναι ανθεκτική: Εξαρτάται από την ασφαλή αποθήκευση ενός μεμονωμένου κομματιού πληροφοριών (το ιδιωτικό κλειδί) και δεν υπάρχει μυστική ψηφοφορία (ο καθένας μπορεί να μάθει πώς ψήφισαν όλοι οι άλλοι). Το απόρρητο μπορεί να είναι αόριστο επειδή η διεύθυνση πορτοφολιού και το υπόλοιπο των διακριτικών είναι ορατά στο blockchain. Εάν το πορτοφόλι μπορεί να συνδεθεί με μια διεύθυνση IP, μια διεύθυνση email ή έναν αριθμό τηλεφώνου, μπορεί να είναι αρκετά εύκολα να αποδοθεί σε ένα άτομο.

Μια ψηφιακή ταυτότητα (DID) αναδύεται ως πιθανή λύση σε θέματα απορρήτου. Στην Εσθονία, για παράδειγμα, κάθε πολίτης έχει ένα κρατικό DID που μπορεί να χρησιμοποιηθεί για πρόσβαση σε κυβερνητικές υπηρεσίες μέσω ψηφιακής υπογραφής. Στις εκλογές, η ταυτότητα πιστοποιείται από απόσταση χρησιμοποιώντας μια ταυτότητα με ηλεκτρονικό τσιπ. Ωστόσο, η ασφάλεια του συστήματος έχει επικριθει δίκαια (Heiberg and Willemson, 2014). [22]

Η αυτοδύναμη ταυτότητα (Self-sovereign identity, SSI) συνδυάζει μια ψηφιακή ταυτότητα με την τεχνολογία blockchain. Η ιδέα είναι ότι κάθε άτομο μπορεί επιλεκτικά να αποκαλύψει μόνο τα απαιτούμενα χαρακτηριστικά για το πρόσωπο και την ταυτότητά του, όπως και όταν χρειαστεί. Ένας αξιόπιστος επαληθευτής ελέγχει κρυπτογραφικά με την αρχή έκδοσης (όπως η κυβέρνηση) ότι οι αποκαλυφθείσες πληροφορίες είναι έγκυρες και ισχύουν. Αυτό γίνεται με μηδενική απόδειξη γνώσης, ώστε ο επαληθευτής να μην βλέπει ποτέ τα πρωτότυπα έγγραφα (π.χ. ένα ePassport) ή άλλες άσχετες πληροφορίες (δηλ. χαρακτηριστικά που δεν σχετίζονται με τον συγκεκριμένο σκοπό).

Ο στόχος του SSI είναι να έχει κάθε άτομο την δική του ταυτότητα του και να μπορεί να την ελέγχει. Ωστόσο, η τεχνολογία δεν έχει φτάσει ακόμα εκεί καθώς τα βιομηχανικά πρότυπα εξακολουθούν να εξελίσσονται και λείπουν οι υποδομές ενσωμάτωσης τους σε τεχνολογίες blockcain. Ο τομέας αυτός είναι ένας ενεργός τομέας πειραματισμού και πιθανών λύσεων όπως το Blockpass, το Circles, το Civic, το HumanityDAO, το Sovrin, το uPort και άλλα βρίσκονται σε στενό ανταγωνισμό για μερίδιο αγοράς.

## 4.4 Μηχανισμοί Ψηφοφορίας

Η ψηφοφορία είναι μια ευρέως χρησιμοποιούμενη μέθοδος συγκέντρωσης προτιμήσεων. Ανεξάρτητα από το αν η ψηφοφορία διεξάγεται στην αλυσίδα ή εκτός αλυσίδας, υπάρχουν πολλές επιλογές και παράμετροι. Σε ένα αποκεντρωμένο δίκτυο, οι κάτοχοι διακριτικών, οι χρήστες δικτύου ή οι χειριστές των κόμβων δικτύου είναι πιθανά μέλη του εκλογικού σώματος. Αυτές είναι μερικές από τις δυνατότητες για το εκλογικό σύστημα:

- Ισοσταθμισμένη ψηφοφορία χρησιμοποιείται σχεδόν σε όλες τις εθνικές και τοπικές πολιτικές εκλογές. Στα αποκεντρωμένα δίκτυα, αυτή η αρχή μεταφράζεται σε μία ψήφο ανά κάτοχο διακριτικού ή μία ψήφο ανά φορέα εκμετάλλευσης υποδομής,αναλόγως την περίπτωση
- Η σταθμισμένη ψηφοφορία είναι ένα σύστημα όπου ο αριθμός των ψήφων που κατέχονται από ένα άτομο ή οντότητα εξαρτάται από ορισμένες ποσοτικοποιήσιμες μετρήσεις.
  (α) Σε μια πλουτοκρατία, το βάρος είναι ανάλογο με τον αριθμό των tokens που διακυβεύονται από κάθε ψηφοφόρο. Κάθε μονοτονική και αυξανόμενη λειτουργία του πονταρίσματος έχει αντίστοιχα αποτελέσματα.
  (β) Ωστόσο, το σχέδιο στάθμισης μπορεί να είναι οπισθοδρομικό, έτσι ώστε η δύναμη ψήφου να μπορεί να κορεστεί σε υψηλότερα επίπεδα πλούτου. Ως παράδειγμα ενός συστήματος οπισθοδρομικής στάθμισης, η Saga χρησιμοποιεί ένα ισορροπημένο σύστημα ψηφοφορίας (Man et al.,2019). [23] Ο στόχος είναι να ληφθούν εξίσου υπόψη τα συμφέροντα εκείνων με μεγάλες ποσότητες token με εκείνους με λιγότερες συμμετοχές αλλά που προσθέτουν αξία ως μέλη μιας μεγαλύτερης κοινότητας. Η δύναμη ψήφου είναι ένας σταθμισμένος μέσος όρος ψηφοφορίας βάσει πονταρίσματος και ισοδύναμης ψήφου, με τον συντελεστή Gini να χρησιμοποιείται ως συντελεστής στάθμισης. Για παράδειγμα, εάν υπάρχουν 1 εκατομμύριο χρήστες με 100 μάρκες (tokens) το καθένα και 12 φάλαινες με 100 εκατομμύρια μάρκες το καθένα, ένα σύστημα βασισμένο στο ποντάρισμα θα μεταφράζεται σε πλουτοκρατία με τις φάλαινες (ως ομάδα) να κατέχουν το 55% της ψήφου. Στην ψηφοφορία ίσης στάθμισης, οι φάλαινες θα κρατούσαν μια ελάχιστη ποσότητα ισχύος. Στην ισορροπημένη ψηφοφορία, οι φάλαινες (ως ομάδα) θα κατέχουν το 25% του δύναμη ψήφου. Οι απόψεις τους θα υπολογίζονταν, αλλά δεν θα μπορούσαν να υπαγορεύσουν αποφάσεις.
  (γ) Το βάρος μπορεί να είναι ανάλογο με το συσσωρευμένο gas που ξοδεύεται από κάθε ψηφοφόρο. Αυτό το είδος στάθμισης ευνοεί τους καθιερωμένους, μακροχρόνιους χρήστες σε βάρος των νεοεισερχόμενων. Η μακροζωία ενός κόμβου ή του χρήστη του δικτύου είναι πιθανές εναλλακτικές μετρήσεις. Μπορεί να εφαρμόζεται ένα σύστημα διαχείρισης φήμης για την ενημέρωση της ψήφου, την επιβράβευση χρηστών ή κόμβων σε καλή κατάσταση και την τιμωρία της κακής συμπεριφοράς.
- Κατά την εξουσιοδοτημένη ψηφοφορία (delegated voting) και στην ρευστή δημοκρατία (liquid democracy), το εκλογικό σώμα (π.χ. όλοι οι κάτοχοι διακριτικών) επιλέγει πολύ μικρότερο αριθμό αντιπροσώπων που λαμβάνουν αποφάσεις για λογαριασμό τους. Εάν η ιδέα είναι ότι οι εκπρόσωποι είναι που κατανοούν καλύτερα την τεχνολογία, τότε το μοντέλο διακυβέρνησης γίνεται πρότυπο αξιοκρατίας ή μια τεχνοκρατία. Σε πολλά πρωτόκολλα PoS και DPoS, οι στοιχειοθετημένοι κόμβοι μπορούν να ψηφίσουν για αποφάσεις διακυβέρνησης.
- Στην τετραγωνική ψηφοφορία (Lalley and Weyl, 2018) [24], ένας ψηφοφόρος μπορεί να υποβάλει περισσότερες από μία ψήφους σε μια εναλλακτική, αλλά με το οριακό κόστος να αυξάνεται σε κάθε βήμα (έτσι ώστε η δεύτερη ψηφοφορία θα απαιτούσε 4 μονάδες, η τρίτη 9 μονάδες κ.ο.κ σύντομα). Η διαίσθηση είναι ότι όσο περισσότερης εκτίμησης χαίρει κάτι, τόσο περισσότερο θα πρέπει να είμαστε διατεθειμένοι να

ξοδέψουμε για την οριακή ψήφο. Το αποτέλεσμα της τετραγωνικής ψηφοφορίας μπορεί να είναι παρόμοιο με την ισορροπημένη ψηφοφορία (όπως παραπάνω με την χρήση των συντελεστών προσαρμογής της επιρροής των ψηφοφόρων Gini). Ευρέως υποστηριζόμενες πρωτοβουλίες ευνοούνται και τα πλούσια άτομα δεν μπορούν να κυριαρχήσουν εύκολα στο αποτέλεσμα. Η ιδέα επεκτάθηκε σε τετραγωνική χρηματοδότηση (Buterin et al., 2018) όπου διατέθηκε η χρηματοδότηση σε ένα έργο δημοσίων αγαθών ως το ανάλογο με το τετράγωνο του αθροίσματος των τετραγωνικών ριζών όλων των εισφορές που ελήφθησαν. Η τετραγωνική χρηματοδότηση χρησιμοποιείται στο GitCoin, μια πλατφόρμα ανταποδοτικότητας για κώδικα ανοιχτού κώδικα στο blockchain Ethereum.[25]

- Η ψηφοφορία με σκορ είναι ένας μηχανισμός όπου κάθε ψηφοφόρος προσδίδει μια αριθμητική βαθμολογία σε ορισμένες (αλλά όχι απαραίτητα σε όλες) εναλλακτικές λύσεις. Μπορεί να υπάρχει περιορισμός του προϋπολογισμού, δηλαδή ένας σταθερός αριθμός πιστώσεων που μπορεί να διανείμει κάθε ψηφοφόρος. Το Eximchain είναι ένα παράδειγμα ενός ledger που συνδυάζει ψηφοφορία με σκορ και τετραγωνική ψηφοφορία.
- Η ομοσπονδιακή ψηφοφορία είναι ένας ενδιαφέρων μηχανισμός ψηφοφορίας που μπορεί επίσης να χρησιμοποιηθεί ως αλγόριθμος συναίνεσης. Σε ένα γύρο ομοσπονδιακής ψηφοφορίας, οι κόμβοι ανταλλάσσουν μηνύματα έως ότου κάθε κόμβος μπορεί να επιβεβαιώσει ότι υπάρχει τοπική απαρτία που είναι ικανοποιημένη με την ίδια εναλλακτική. Εάν οι κόμβοι ακολουθούν το πρωτόκολλο για διαδοχικούς γύρους, η απαρτία (με την προϋπόθεση ότι ισχύουν ορισμένες τεχνικές προϋποθέσεις) συνεχίζει να επεκτείνεται έως ότου συμφωνήσουν όλοι οι κόμβοι. Αυτή η διαδικασία ονομάζεται Ομοσπονδιακή Βυζαντινή Συμφωνία (FBA), και αποτελεί βασικό στο πρωτόκολλο συναίνεσης των Ripple, Stellar και Tixl., ενώ δεν διαφαίνεται κανένα εμπόδιο, καταρχήν, για ευρύτερη εφαρμογή.

## 4.5 Προτεινόμενες Ερευνητικές Εφαρμογές Φηφοφορίας στο Δημόσιο Blockchain

Η ιδέα πίσω από την ψηφοφορία στο blockchain προέρχεται από την εννοιολογική ομοιότητα του blockchain με το Bulletin Board. Πράγματι, και στις δύο περιπτώσεις, οι συναλλαγές πρέπει να καταγράφονται ακαριαία και οι συμμετέχοντες καταλήγουν σε συναίνεση σχετικά με το ποιες συναλλαγές είναι έγκυρες και ποιες όχι. Στην περίπτωση των κρυπτονομισμάτων, αυτές οι συναλλαγές αντιπροσωπεύουν τη μεταβίβαση της αξίας, ενώ στην περίπτωση των εκλογών αυτές οι συναλλαγές αντιπροσωπεύουν την καταγραφή της προτί Bitcoin μησης.

Μια ψηφοφορία στο blockchain εξαλείφει την ανάγκη για ένα αξιόπιστο τρίτο μέρος επεύθυνο να διατηρήσει τα δεδομένα που απαιτούνται για την έγκριση και τον έλεγχο των εκλογών. Μπορεί επίσης, θεωρητικά, να οδηγήσει σε πραγματικά αποκεντρωμένες εκλογές όπου οι ίδιοι οι ψηφοφόροι διεξάγουν τις εκλογές χωρίς κανένα αξιόπιστο κόμμα να καταγράφει, να μετρά και να επαληθεύει τις ψήφους. Όλα τα μέρη αποδέχονται τα περιεχόμενα του Bulletin Board όπου θα πραγματοποιηθεί ο έλεγχος, καθώς αποδέχονται τις καταγεγραμμένες συναλλαγές στο blockchain. Ως αποτέλεσμα, πολλοί πρότειναν διάφορα σύστημα ψηφοφορίας με τεχνολογία κατανεμημένου καθολικού όπως το blockchain. Εκτός από ακαδημαϊκές έρευνες που θα παρουσιαστούν παρακάτω, υπάρχουν και εμπορικές εφαρμογές ψηφοφορίας στο blockchain  όπως οι VOLT,Voatz, Democracy.Earth, FollowMyVote και άλλα.

Παρακάτω παρουσιάζουμε τις βασικές ακαδημαϊκές έρευνες σχετικές με διαδικασίες ψηφοφορίας στο blockchain.

α) Στο έγγραφο με τίτλο «Προς την ασφαλή ηλεκτρονική ψηφοφορία χρησιμοποιώντας Ethereum Blockchain» [26] , ο Ali Kaan Ko et al. παρουσίασε μια αποκεντρωμένη λύση ψηφοφορίας με βάση το Ethereum Blockchain. Στην παραπάνω δημοσίευση, επισημαίνεται

ότι ένα σύστημα ηλεκτρονικής ψηφοφορίας πρέπει να είναι ασφαλές με πλήρη διαφάνεια (προστασία της ιδιωτικής ζωής) και να μην επιτρέπει στους ψηφοφόρους διπλές ή πολλαπλές ψήφους. Προτείνεται η ανάπτυξη εφαρμογής ηλεκτρονικής ψηφοφορίας ως έξυπνο συμβόλαιο που επιτρέπει σε χρήστες με έγκυρες διευθύνσεις λογαριασμού (External Owned Accounts) να ψηφίσουν για το συμβόλαιο (μία ψήφος ανά διεύθυνση σε ένα μόνο ερώτημα). Παρ 'όλα αυτά, αυτή η λύση δεν προσφέρει αυτοματοποιημένο πρωτόκολλο επαλήθευσης διεύθυνσης, δεδομένου ότι οι EOA αποκτούν το δικαίωμά της ψήφου τους από μια Κεντρική Αρχή που εγκρίνει ή απορρίπτει τους ψηφοφόρους. Τα κύρια πλεονεκτήματα που προσφέρει είναι επιχειρηματικοί κανόνες, διαφάνεια και περιορισμός μίας ψήφου ανά EOA διεύθυνση.

β) Στην δημοσίευση με τίτλο «Το μέλλον της ηλεκτρονικής ψηφοφορίας »,ο Tarasov et. [27] ερεύνησε την ηλεκτρονική ψηφοφορία και την πιθανή διεξαγωγή της στο Blockchain. Εκτός των ιδιοτήτων της διαφάνειας, ιδιωτικότητας και ακεραιότητας που αποτελούν εγγενείς ιδιότητες των αποκεντρωμένων εφαρμογών Blockchain, η προτεινόμενη αυτή λύση προτείνει μια φάση εγγραφής για την επαλήθευση της ταυτότητας των ψηφοφόρων.

Η εγγραφή είναι το πρώτο βήμα του πρωτοκόλλου και απαιτείται ως μέρος της επαλήθευσης ταυτότητας για σκοπούς ελέγχου. Βοηθά στην καταγραφή και παρακολούθηση των ψηφοφόρων που έχουν συμμετάσχει στην ψηφοφορία. Παρόλο που η διαδικασία επαλήθευσης γίνεται χρησιμοποιώντας ένα Πρωτόκολλο χειραψίας πρόκλησης-απόκρισης, περιλαμβάνει και πάλι έναν κεντρικό διακομιστή (Κεντρική Αρχή) για τη διαχείριση της επαλήθευσης και της προσθήκης των δεδομένων των χρηστών (διευθύνσεις email) στη βάση δεδομένων. Αξίζει να σημειωθεί ότι είναι οι διευθύνσεις ηλεκτρονικού ταχυδρομείου σχετικά εύκολο να χακαριστούν σήμερα.

γ) Αποκεντρωμένη, διαφανής, χωρίς εμπιστοσύνη ψηφοφορία στο Ethereum Blockchain:

Ο Fernando Lobato Meeser [28], στο άρθρο του με τίτλο «Αποκεντρωμένη, διαφανής, χωρίς εμπιστοσύνη ψηφοφορία στο Ethereum Blockchain » ασχολείται με δύο τύπους ζητημάτων με λύσεις E-Voting. Πρώτον, η ικανότητα από οποιονδήποτε να μετρήσει τα αποτελέσματα από το έξυπνο συμβόλαιο πριν ολοκληρωθεί η υποβολή όλων των ψήφων, και δεύτερον, την ανωνυμία των ψήφων δεδομένου ότι τα δημόσια κλειδιά μπορούν να συσχετιστούν με τις καταγεγραμμένες ψήφους. Σε αυτό το άρθρο, ο συγγραφέας παρουσιάζει την εφαρμογή ενός συστήματος ψηφοφορίας ως έξυπνο συμβόλαιο που λειτουργεί στο Ethereum που χρησιμοποιεί threshold keys και υπογραφές συνδεσιμότητας (linkable ring signatures). Ωστόσο, αυτή η λύση περιλαμβάνει και πάλι μια φάση εγγραφής, στην οποία οι ψηφοφόροι βασίζονται σε μια Κεντρική Αρχή για να εγγράψουν το δημόσιο κλειδί τους για την ψηφοφορία.

Όλες οι παραπάνω έρευνες βασίζονται στο ίδιο σενάριο όπου κάθε υποψήφιος αντιπροσωπεύεται από μια διεύθυνση Ethereum (λογαριασμός). Όταν ένας ψηφοφόρος θέλει να ψηφίσει έναν συγκεκριμένο υποψήφιο, στέλνει μια σταθερή μικρή πληρωμή στη διεύθυνση του υποψηφίου ή στην διεύθυνση του smart contract. Αυτή η συναλλαγή καταγράφεται στο blockchain. Κατά συνέπεια, οι ίδιοι οι ψηφοφόροι πρέπει να εκπροσωπούνται χρησιμοποιώντας διευθύνσεις που λειτουργούν ως ψευδώνυμα. Όταν τελειώσουν οι εκλογές, όλοι μπορούν να ελέγξουν το blockchain και να αθροίσουν το ποσό των ψήφων που έλαβε κάθε διεύθυνση υποψηφίου ή κάθε έξυπνο συμβόλαιο και να δηλώσουν τον νικητή.

δ) «Αφαίρεση αξιόπιστων αρχών συσκέψεων αυτο-επιβολής μέσω του Ethereum»: Στο έγγραφο που δημοσίευσε ο Patrick McCorry [29], ισχυρίζεται ότι το προτεινόμενο πρωτόκολλο επιτρέπει σε οποιονδήποτε, συμπεριλαμβανομένων των παρατηρητών, να επαληθεύει την ακεραιότητα των εκλογών χωρίς να χρειάζεται να εμπιστευόμαστε κάποιες αρχές ενώ παράλληλα διατηρείται η ιδιωτική ζωή των ψηφοφόρων, Επιτυγχάνεται δηλαδή το

Open Vote Network (OV-net) και το Direct Recording Electronic με ακεραιότητα (DRE-i), και DRE-i με ενισχυμένο απόρρητο (DREip). Παρ 'όλα αυτά, το σύστημά τους απαιτεί μια αρχή για τη δημιουργία μιας λίστας επιλέξιμων ψηφοφόρων και να τους μεταφέρει στο Ethereum Blockchain πριν ξεκινήσει η διαδικασία των εκλογών. Οι ψηφοφόροι μπορούν να επαληθεύσουν μόνοι τους τους εαυτούς τους χρησιμοποιώντας τα καταγεγραμμένα δεδομένα. Για τον σκοπό αυτό πρέπει να χρησιμοποιηθεί ένα blockchain που υποστηρίζει έξυπνα συμβόλαια. Αυτό υλοποιείται στο Open Vote Network (McCorry et al., 2017). Η αντίσταση στον εξαναγκασμό είναι προβληματική σε αυτό το βασικό σχήμα, καθώς ένας εισβολέας μπορεί εύκολα να εξακριβώσει αν ο στόχος του ακολούθησε τις οδηγίες του, απλώς εξετάζοντας το blockchain. Παρόλο που μια προκαθορισμένη λίστα ψηφοφόρων είναι μια καλή επιλογή για ορισμένες περιπτώσεις χρήσης, παραμένει η πρόκληση αναφορικά με την πλήρη αποκέντρωση της διαδικασίας ψηφοφορίας

## 4.6 Ζητήματα Σχετικά με Blockchain Voting και Πιθανές Λύσεις

Πρώτον, για να καταστεί δυνατή η εξακρίβωση της εγκυρότητας των ψηφοφόρων, πρέπει να υπάρχει ένα πρωτόκολλο που καθορίζει τη χαρτογράφηση (mapping) μεταξύ διευθύνσεων ψηφοφόρων και των πραγματικών τους ταυτοτήτων. Εάν εκτελείται από μια αρχή εγγραφής, τότε ένα αξιόπιστο τρίτο μέρος εισάγεται στο σύστημα ψηφοφορίας και η χρήση του blockchain μοιάζει με την περίπτωση permissioned blockchain. Εάν οι εκλογές διεξάγονται σε μικρή κλίμακα, τότε είναι λογικό να υποθέσουμε ότι οι ψηφοφόροι μπορούν από κοινού να συμφωνήσουν για την επιλεξιμότητά τους, χρησιμοποιώντας πραγματικές πληροφορίες. Στην περίπτωσή μας, η επαλήθευση ταυτότητας απαιτεί έναν πάροχο ταυτότητας που πρέπει να δεσμεύει τις πραγματικές ταυτότητες με τα διαπιστευτήρια ψήφου που χορηγούνται μόνο σε εκείνους με δικαίωμα ψήφου. Αυτό σημαίνει ότι απαιτείται μια αρχή εγγραφής, αλλά πρέπει να αποτραπεί η σύνδεση των ψηφοφόρων με διευθύνσεις Ethereum. Αυτό μπορεί να γίνει χρησιμοποιώντας αρχές κρυπτογραφικής ανωνυμίας όπως τυφλές υπογραφές και mixnets. Ενώ αυτή η δέσμευση μπορεί να γίνει επαληθεύσιμη με εργαλεία όπως το PACBS, οι ταυτότητες εξακολουθούν να διατηρούνται σε μια κεντρική βάση δεδομένων που λειτουργεί από ένα εθνικό κράτος - ένα αξιόπιστο τρίτο μέρος.

Ένα δεύτερο μειονέκτημα είναι ότι το βασικό σύστημα ψηφοφορίας Ethereum δεν ικανοποιεί ούτε την έννοια του απορρήτου της ψηφοφορίας. Η χρήση ψευδωνύμων παρέχει ελάχιστη προστασία, αλλά οι πραγματικές ταυτότητες ενδέχεται να διαρρεύσουν ή ενδέχεται να απονομηθούν χρησιμοποιώντας προηγμένες τεχνικές ανάλυσης (Meiklejohn et al., 2013) [30]. Μια πιθανή λύση χρησιμοποιεί τεχνικές που χρησιμοποιούνται σε ομομορφικά συστήματα ψηφοφορίας. Οι ψηφοφόροι κρυπτογραφούν την επιλογή του υποψηφίου τους και αντί να στέλνουν συναλλαγές σε κάθε υποψήφιο στέλνουν συναλλαγές σε μία μόνο διεύθυνση που ανήκει σε έναν επαληθευτή. Υπάρχουν εναλλακτικοί τρόποι για να καταχωρηθεί κάποιο κρυπτογραφημένο ψηφοδέλτιο μέσα στη συναλλαγή, ανάλογα με τον τύπο του blockchain που χρησιμοποιείται: Στην περίπτωση του Bitcoin, η κρυπτογράφηση θα γίνει έξω από το σύστημα και θα πρέπει να υπάρχουν αποδείξεις εγκυρότητας μηδενικής γνώσης που αποθηκεύονται σε ξεχωριστή πηγή δεδομένων και συνδέονται με τη συναλλαγή με μια κατασκευή όπως η δήλωση OP_RETURN. Αυτή η προσέγγιση έχει το μειονέκτημα ότι η εξωτερική πηγή δεδομένων γίνεται αξιόπιστο τρίτο μέρος που έχει τον έλεγχο των πραγματικών δεδομένων.

Τρίτον, όλα τα δημόσια blockchain έχουν προβλήματα απόδοσης, τόσο στον αριθμό των συναλλαγών που εκκαθαρίζονται ανά δευτερόλεπτο όσο και στο χρόνο αναμονής για επιβεβαίωση μιας συναλλαγής. Αυτά τα καθιστούν δύσκολα για χρήση σε εκλογές μεγάλης κλίμακας.

Τέταρτον, για την επίλυση των προβλημάτων εξαναγκασμού, απαιτούνται περισσότερες κεντρικές αρχές. Στο τέλος της ψηφοφορίας, θα πρέπει να υπάρχει μια αρχή που παρέχει ανώνυμα διαπιστευτήρια (διευθύνσεις) στους ψηφοφόρους, προκειμένου να στερήσει από τον εκβιαστή τη δυνατότητα να μάθει αν ο στόχος τους έλαβε πραγματικά μέρος στις εκλογές και ποια ήταν η επιλογή τους. Επιπλέον, μια άλλη κεντρική αρχή πρέπει να λειτουργεί από την πλευρά της καταμέτρησης και να φιλτράρει τις εξαναγκασμένες ψήφους βάσει των πλαστών διαπιστευτηρίων.

Επίσης, η δημόσια διαθεσιμότητα δεδομένων συλλογής καθιστά την ιδιωτικότητα ακόμη πιο δύσκολη. Εκτός από το απόρρητο, το βασικό σχέδιο ψηφοφορίας blockchain δεν υποστηρίζει τη δικαιοσύνη, καθώς οποιοσδήποτε μπορεί να υπολογίσει τα ενδιάμεσα αποτελέσματα παρακολουθώντας τις συναλλαγές που μεταδίδονται στο blockchain. Αυτό μπορεί να επηρεάσει την επιλογή των ψηφοφόρων που έχουν καθυστερήσει (Nasser et al., 2018).[31]

Οι προτεινόμενες λύσεις blockchain μπορούν να εξεταστούν ως προς τον βαθμό αποκέντρωσης τους. Εάν είναι πραγματικά μη συγκεντρωτικές ή αν υποστηρίζουν εκλογές μεγάλης κλίμακας. Μια ανάλυση του (Dricot & Pereira, 2018)[32] διαπιστώνει ότι μόνο το δίκτυο OpenVote (McCorry et al., 2017), είναι μια λειτουργικά αποκεντρωμένη πλατφόρμα. Ωστόσο, έχει προβλήματα κλιμάκωσης, καθώς προορίζεται να χρησιμοποιηθεί μόνο για εκλογές μικρής κλίμακας ή αίθουσα συνεδριάσεων (για μέγιστο αριθμό 50 ψηφοφόρων όπως ισχυρίζονται οι ίδιοι οι συγγραφείς).

Πρέπει επίσης να τονιστεί ότι, τα επιχειρήματα αποκέντρωσης ισχύουν μόνο για το επίπεδο εφαρμογής, δηλαδή το ίδιο το πρωτόκολλο ψηφοφορίας. Ενώ το επίπεδο δικτύου - το blockchain - θεωρείται αποκεντρωμένο, μια πιο προσεκτική ματιά αποκαλύπτει ότι υπάρχει συγκέντρωση στην εξορυκτική ισχύ. Για παράδειγμα, μια πρόσφατη εργασία του (Gencer, 2018) [33]διαπιστώνει ότι το 90% της εξορυκτικής δύναμης βρίσκεται στα χέρια 16 ανθρακωρύχων στο Bitcoin και 11 ανθρακωρύχων στο Ethereum.

Τέλος, η ψηφοφορία blockchain επιδεινώνει ένα μεγάλο πρόβλημα που αντιμετωπίζουν όλα τα ηλεκτρονικά συστήματα ψηφοφορίας, ειδικά τα κρυπτογραφικά. Το Enfranchisement απαιτεί ότι ο ψηφοφόρος κατανοεί τη διαδικασία στην οποία συμμετέχει. Αυτό είναι δύσκολο να γίνει όταν το σύστημα είναι χτισμένο πάνω από σύνθετες μαθηματικές έννοιες που δεν μπορούν να εξηγηθούν εύκολα. Αυτή η κατάσταση επιδεινώνεται λόγω της πιθανότητας και του χαρακτήρα κινήτρων της ασφάλειας πολλών από τα σχέδια που αντιμετωπίζαμε. Αυτό ισχύει ειδικά για την ψηφοφορία blockchain. Αν και η επιστημονική τους ανάλυση είναι καλή, ο μέσος ψηφοφόρος μπορεί να μην είναι σίγουρος με λιγότερο από τέλειες λύσεις.

# 5 Ethereum Blockchain

## 5.1 Ethereum

Το Ethereum είναι το δεύτερο κρυπτονόμισμα που εμφανίστηκε στις αγορές μετά το Bitcoin. Αν και η ιδέα προήρθε από τον Vitalik Buterin, ανακοινώθηκε επίσημα με μια μεγάλη λίστα δημιουργών (Antonio Di Iorio,Charles Hoskinson, Mihai Alisie,Amir Chetrit, Joseph Joseph Lublin, Gavin Wood και Jeffrey Wilke).

Η ανάπτυξή του ξεκίνησε στις αρχές του 2014, από μια ελβετική εταιρεία, την Ethereum Switzerland GmbH (EthSuisse). Ο κύκλος ζωής και τα βασικά οικονομικά χαρακτηριστικά, όπως αυτά ισχύουν στο δεύτερο τετράμηνο του έτους 2020 παρουσιάζονται στην παρακάτω εικόνα:


Εικόνα 7 : Βασικά οικονομικά χαρακτηριστικά Ethereum

Η βασική ιδέα ήταν το Ethereum, να μην αποτελεί μια απλή πλατφόρμα ανταλλαγής κρυπτονομισμάτων, αλλά στην ουσία να αποτελεί πλατφόρμα, μέσω της οποίας να μπορούν να δημιουργούνται διάφορες εφαρμογές με βάση το blockchain (αποκεντρωμένες εφαρμογές). Αρχικά η ιδέα αυτή είχε προταθεί για εφαρμογή στο blockchain του Bitcoin. Ωστόσο, η γλώσσα του Bitcoin είναι Turing-incomplete. Η υποστήριξη της ιδέας απαιτούσε μια Turing-complete γλώσσα. Έτσι, επικράτησε η ιδέα να χρησιμοποιούνται έξυπνα συμβόλαια και κατόπιν ξεκίνησε η ανάπτυξη του λογισμικού μέσω του οποίου θα υλοποιούταν. Το έργο αυτό ανέλαβε ο Gavin Wood, επικεφαλής της εταιρείας, ο οποίος παρουσίασε το 'yellow paper', που καθόριζε την εικονική μηχανή (virtual machine) του Ethereum (EVM). Έπειτα, δημιουργήθηκε ένα ελβετικό μη κερδοσκοπικό ίδρυμα για το Ethereum, το Stiftung Ethereum. Η ανάπτυξη του ιδρύματος αυτού χρηματοδοτήθηκε από το κοινό στην πρώτη ICO (Initial Coin Offering) που πραγματοποιήθηκε την περίοδο Ιουλίου Αυγούστου του 2014, όπου οι επενδυτές μπορούσαν να αγοράσουν ether, δηλαδή το νόμισμα του Ethereum, χρησιμοποιώντας, όμως, Bitcoins για την αγορά του. Συνολικά, δόθηκαν 72 εκατομμύρια ether, τα οποία είχαν γίνει pre-mined, δηλαδή δε γεννήθηκαν από το mining κάποιου block. Τον Μάρτιο του 2017, ανακοινώθηκε η δημιουργία του M.K.O. Enterprise Ethereum Alliance (EOX), που περιείχε 30 ιδρυτικά μέλη που χρησιμοποιούσαν το blockchain, ενώ σήμερα περιέχει πάνω από 150 εταιρείες-μέλη. Συνοψίζοντας, η δημιουργία του Ethereum, αποτέλεσε βάση για την ανάπτυξη χιλιάδων αποκεντρωμένων εφαρμογών, καθώς χρησιμοποιεί τα έξυπνα συμβόλαια (smart contracts), τα οποία γράφονται σε γλώσσα Turing-Complete.

## 5.2 Βασικά Χαρακτηριστικά Ethereum

Ο τρόπος, με τον οποίο το blockchain του Ethereum έχει κατασκευαστεί, διαφέρει πολύ από το κλασσικό πρότυπο ενός κρυπτονομίσματος, ώστε να μπορεί να αποτελέσει πλατφόρμα, μέσω της οποίας να δημιουργούνται όλων των ειδών projects με βάση το blockchain. Μάλιστα, πολλά από τα δεδομένα δεν είναι αποθηκευμένα στο ίδιο το blockchain, αλλά Modified Merkle Patricia Tries εξωτερικά αυτού. Το μόνο που αποθηκεύεται στο blockchain είναι η ρίζα (root) αυτού του δέντρου, με τρόπο ώστε να μην επηρεάζεται από την αλλαγή των δεδομένων. Το project του, όμως, έχει διαφορές ακόμα και στην πληρωμή των miners. Πάμε, πρώτα, να δούμε από τι αποτελείται ένα block στο Ethereum blockchain.

### 5.2.1 Blocks

Τα blocks στο Ethereum είναι τελείως διαφορετικά από τα blocks των τεσσάρων πεδίων ενός κλασσικού κρυπτονομίσματος. Στην πραγματικότητα, περιέχουν 15 πεδία τα οποία είναι:

- Previous hash
  Το hash value του προηγούμενου block, μέσω του οποίου ενώνονται και δημιουργείται η αλυσίδα.
- Nonce
  Ένας τυχαίος αριθμός 64-bits, ο οποίος χρησιμοποιήθηκε για το mining του block, και συγκεκριμένα, αυτός που ταίριαξε, ώστε να δοθεί έξοδος που συναντά τα κριτήρια που είχαν τεθεί. Αποδεικνύει, σε συνδυασμό με το mix hash που θα δούμε, ότι ένα επαρκές σύνολο υπολογιστικής ισχύος χρησιμοποιήθηκε για τη δημιουργία του συγκεκριμένου block.
- Timestamp
  Μια βαθμωτή τιμή ίση με την έξοδο της εντολής time του Unix, κατά τη γέννηση του block.
- Uncle's hash To hash value ενός uncle block.
- Beneficiary
  Η διεύθυνση 160-bit στην οποία έχουν καταβληθεί όλα τα τέλη που συλλέγονται από την επιτυχημένη εξόρυξη αυτού του μπλοκ. Με λίγα λόγια, η διεύθυνση του miner, ο οποίος δημιούργησε το block.
- Logs bloom
  Ένα φίλτρο, ονομαζόμενο Bloom, το οποίο αποτελείται από πληροφορίες ευρετηρίου (διεύθυνση καταγραφής και θέματα καταγραφής), από τις οποίες αποτελούνται οι διάφορες συναλλαγές του συγκεκριμένου block.
- Difficulty
  Μια βαθμωτή τιμή που αντιστοιχεί στο επίπεδο δυσκολίας εύρεσης του συγκεκριμένου block. Προκύπτει από το επίπεδο δυσκολίας του προηγούμενου block και το timestamp αυτού του block.
- Extra Data
  Ένας αυθαίρετος πίνακας bytes, ο οποίος περιέχει δεδομένα σχετικά με αυτό το block. Πρέπει να αποτελείται από 32 bytes ή λιγότερα.
- Block Number
  Μία βαθμωτή τιμή ίση με τον αριθμό των προηγούμενων block στην αλυσίδα. Το genesis block, δηλαδή το πρώτο block έχει την τιμή αυτή ίση με 0.
- Gas Limit
  Μια βαθμωτή τιμή ίση με το συγκεκριμένο όριο δαπάνης gas ανά block. Για το gas θα μιλήσουμε εκτενώς σε επόμενη ενότητα, αλλά αποτελεί τη μονάδα μέτρησης υπολογιστικής ισχύος για την εκτέλεση των έξυπνων συμβολαίων (smart contracts).
- Gas Used
  Μια βαθμωτή τιμή ίση με το σύνολο του gas, που δαπανήθηκε για την εκτέλεση όλων των συναλλαγών, που περιέχονται στο συγκεκριμένο block.
- Mix hash
  Μια τιμή κατακερματισμού (hash value) 64-bits, η οποία σε συνδυασμό με το nonce, αποδεικνύει ότι έχει πραγματοποιηθεί επαρκής υπολογισμός για τη δημιουργία του συγκεκριμένου block.
- State Root
  Αποτελεί την τιμή κατακερματισμού (hash value), με χρησιμοποίηση του Keccak-256-bits, της ρίζας ενός δέντρου, ονόματι state trie, αφού όλες οι συναλλαγές έχουν εκτελεστεί και έχει έρθει σε τελική μορφή. Για το δέντρο αυτό, όπως και τα υπόλοιπα δύο θα μιλήσουμε στη συνέχεια.
- Transaction Root
  Αποτελεί την τιμή κατακερματισμού (hash value), με χρησιμοποίηση του Keccak-256-bits, της ρίζας ενός δέντρου, ονόματι transaction trie, το οποίο περιέχει κάθε συναλλαγή η οποία συμπεριλήφθηκε στο συγκεκριμένο block.

- Receipt Root
  Αποτελεί την τιμή κατακερματισμού (hash value), με χρησιμοποίηση του Keccak-256-bits, της ρίζας ενός δέντρου, ονόματι receipt trie, το οποίο περιέχει όλες τις αποδείξεις των συναλλαγών που συμπεριλήφθηκαν στο συγκεκριμένο block.

Παρακάτω θα αναλύσουμε την έννοια και τη σχέση μεταξύ των nonce και difficulty.

Στο Ethereum blockchain υπάρχει ένας συγκεκριμένος τεχνητός χρόνος από τη δημιουργία ενός block, μέχρι τη δημιουργία του επόμενου. Ο χρόνος αυτός είναι πάντα περίπου 15 δευτερόλεπτα και ο λόγος ύπαρξης του σχετίζεται με την σταθερότητα του συστήματος. Για τη διατήρηση του χρόνου αυτού στα ίδια επίπεδα ακόμη και όταν η υπολογιστική ισχύς που χρησιμοποιείται αλλάζει, χρησιμοποιείται το difficulty και το nonce. Συγκεκριμένα, χρησιμοποιείται ένας αλγόριθμος, ο οποίος αναλόγως με την κινητικότητα, δημιουργεί ένα στόχο για τους miners που ασχολούνται με την εύρεση του νέου block. Θέτει μια τιμή 256-bits, κάτω από την οποία πρέπει να βρίσκεται η τιμή κατακερματισμού (hash value) του συγκεκριμένου block.

Η τιμή κατακερματισμού του block προκύπτει από τα data του block, το hash value του προηγούμενου block και το nonce. Τα δύο πρώτα είναι σταθερά, ενώ το τρίτο αλλάζει ώστε να φτάσει ένας miner να βρει μια τιμή μικρότερη της τιμής-στόχου. Δηλαδή, όσο μεγαλύτερο είναι το difficulty, τόσο περισσότερες δοκιμές nonce πρέπει να γίνουν, ώστε να φτάσει ένας miner στο επιθυμητό αποτέλεσμα.

Διαχείριση Συγκρούσεων

Υπάρχουν ορισμένες περιπτώσεις που δύο blocks, μπορεί να είναι έγκυρα και να δημιουργηθούν ακριβώς στον ίδιο χρόνο, γεγονός που ονομάζεται σύγκρουση block ή αλλιώς block clash. Όμως, μόνο το ένα από αυτά θα καταφέρει τελικά να γίνει μέρος του blockchain, ακόμα και αν τα δεδομένα στο άλλο block είναι τεχνικά έγκυρα. Στο Ethereum τα blocks που ‘χάνουν’ ονομάζονται Uncle’s blocks. Σε αντίθεση με τα περισσότερα κρυπτονομίσματα, που τα block αυτά απλά χάνονται και δε γίνεται κανείς να αναφερθεί σε αυτά, στο Ethereum μπορεί να γίνει αναφορά σε αυτά από μερικά από τα επόμενα blocks, και μάλιστα, παρ’ ότι τα δεδομένα τους δε χρησιμοποιούνται, δίνεται μια μικρότερη ανταμοιβή για τον miner των συγκεκριμένων blocks. Αυτό συμβαίνει συχνά στο δίκτυο του Ethereum, καθώς ο χρόνος μεταξύ δύο block είναι πολύ μικρός. Με γνώμονα την ενθάρρυνση των miners να συνεχίσουν να προσδίδουν αξία στο δίκτυο Ethereum, το σύστημα αναγνωρίζει την εργασία που έγινε για τη δημιουργία τέτοιου κανονικού ή uncle block και επιβραβεύει αναλόγως τον miner.

### 5.2.2 Συναρτήσεις Κατακερματισμού (Hash Functions)

Μία συνάρτηση κατακερματισμού (hash function), είναι μια συνάρτηση, η οποία χρησιμοποιείται για να μετατρέψει (κρυπτογραφήσει) μία οποιουδήποτε μήκους συμβολοσειρά, την οποία δέχεται ως είσοδο (input), σε μία νέα, σταθερού μήκους συμβολοσειρά, την οποία προσδίδει ως έξοδο (hash value). Πολλές συναρτήσεις που κάνουν τη συγκεκριμένη δουλειά υπάρχουν στις μέρες μας, όμως κάποιοι παράγοντες πρέπει να ληφθούν υπόψιν, ώστε να αποφασίσουμε ποια από όλες θα διαλέξουμε, για να κάνουμε μια συγκεκριμένη εργασία. Αρχικά, κάθε είσοδος, οποιαδήποτε και αν είναι αυτή, πρέπει να μετατρέπεται από τη συνάρτηση σε μοναδική έξοδο και το αντίθετο, δηλαδή από κάθε έξοδο πρέπει να είναι δυνατό να προκύψει μόνο μία είσοδος. Πρέπει, μάλιστα, να είναι αδύνατο να προκύψει ίδια έξοδος από δύο διαφορετικές εισόδους, ή το αντίθετο. Η ταχύτητα υπολογισμού της εξόδου (hash value) αποτελεί, επιπλέον πολύ σημαντικό παράγοντα. Πρέπει να είναι σχετικά εύκολο και γρήγορο να υπολογιστεί η συγκεκριμένη τιμή, δεδομένης της εισόδου. Τέλος, η ασφάλεια αποτελεί το σημαντικότερο παράγοντα. Η επιστροφή δεδομένης της εξόδου στην είσοδο, πρέπει να είναι υπερβολικά δύσκολη, έως και αδύνατη, ώστε να μην μπορεί

κάποιος σε μικρό χρόνο να μάθει το από-κρυπτογραφημένο μήνυμα. Επίσης, μια μικρή αλλαγή στην είσοδο πρέπει να επιφέρει τεράστιες αλλαγές στην έξοδο.

Το blockchain, λόγω της ασφάλειας και της μη μεταβλητότητας των δεδομένων που είναι αποθηκευμένα σε αυτό, μπορεί να λειτουργήσει αποτελεσματικά ως ένας χώρος για την αποθήκευση των hashes δεδομένων που έχουν αποθηκευτεί εκτός αυτού. Στο blockchain οι συναρτήσεις κατακερματισμού προσδιορίζουν τη μοναδική κατάσταση της αλυσίδας κάθε χρονική στιγμή. Ουσιαστικά τα blocks είναι συνδεδεμένοι κατάλογοι δεδομένων, αφού όπως προαναφέρθηκε η επικεφαλίδα κάθε block περιέχει το hash του προηγούμενου block. Συνεπώς, οποιαδήποτε αλλαγή γίνει στα δεδομένα προκαλεί αναντοιστοιχία με το hash που είναι αποθηκευμένο στο blockchain και άρα για να τροποποιηθεί οποιοδήποτε δεδομένο ενός block πρέπει να τροποποιηθεί το hash του block και άρα και τα hashes όλων των επόμενων blocks του blockchain, κάτι που είναι πρακτικά αδύνατο.

Οι πιο γνωστές κρυπτογραφικές συναρτήσεις είναι η SHA-1, SHA-2 (ή αλλιώς SHA-256), SHA-3, MD5 και Blake2.

Η SHA-256 είναι η συνάρτηση κατακερματισμού που χρησιμοποιείται από το Bitcoin blockchain, ενώ το Ethereum blockchain χρησιμοποιεί την Keccak-256.

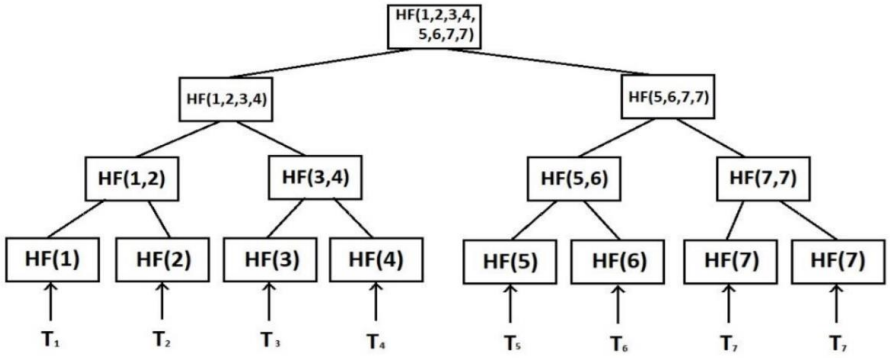
### 5.2.3 Αποθήκευση Δεδομένων στο Blockchain

#### *5.2.3.1 Merkle Trees*

Το Merkle Tree είναι μία δομή δεδομένων (data structure), η οποία αναπαρίσταται ως ένα δέντρο. Κάθε φύλλο (leaf) του δέντρου αναπαριστά ένα κρυπτογραφημένο μήνυμα, κάθε κλαδί (branch) του αναπαριστά τη συνδυασμένη τιμή κατακερματισμού εξόδου (hash value) των παιδιών της, βάσει ενός αλγορίθμου κατακερματισμού (hash algorithm), ενώ η ρίζα του αποτελείται από μία μόνο τιμή, η οποία αναπαριστά τη συνολική συνδυαστική τιμή κατακερματισμού όλου του δέντρου.

Το blockchain ενός κρυπτονομίσματος αποτελείται από χιλιάδες block, ενώ κάθε block αποτελείται από μερικές χιλιάδες συναλλαγές. Κάθε block χρησιμοποιεί ως μέσο αναπαράστασης όλων των συναλλαγών που βρίσκονται σε αυτό, ένα μόνο Merkle Tree και μάλιστα μόνο τη ρίζα του (Merkle Root). Τα Merkle Trees χρησιμοποιούν πάντα ζευγάρια μηνυμάτων-συναλλαγών. Αν ο αριθμός τους είναι περιττός (odd), τότε δημιουργείται ένα αντίγραφο της τελευταίας συναλλαγής και γίνεται ζευγάρι με τον εαυτό της, καθώς και όταν κατά πλάτος ενός βήματος, το σύνολο των κλαδιών που προκύπτουν είναι περιττός, τότε και πάλι δημιουργείται αντίγραφο του τελευταίου κλαδιού και ζευγαρώνει με τον εαυτό του. Σε κάθε γύρο το σύνολο των νέων κλαδιών ή φύλλων περνάει σε ζευγάρια από μια συνάρτηση κατακερματισμού (hash function), από την οποία προκύπτει το επόμενο επίπεδο, το οποίο περιέχει τη συνδυασμένη τιμή κατακερματισμού των δύο και η διαδικασία συνεχίζεται, έως ότου προκύψει η ρίζα του δέντρου.

Για να αντιληφθούμε καλύτερα τη λειτουργία των Merkle Trees, ας αναφέρουμε ένα παράδειγμα. Έστω ότι έχουμε 7 συναλλαγές που πρέπει να μπούνε σε ένα block (T1, T2, …, T7) και ότι απλά χρησιμοποιούμε μια hash function (HF). Το δέντρο που θα προκύψει είναι το εξής:




Σχήμα 8: Παράδειγμα Merkle Tree

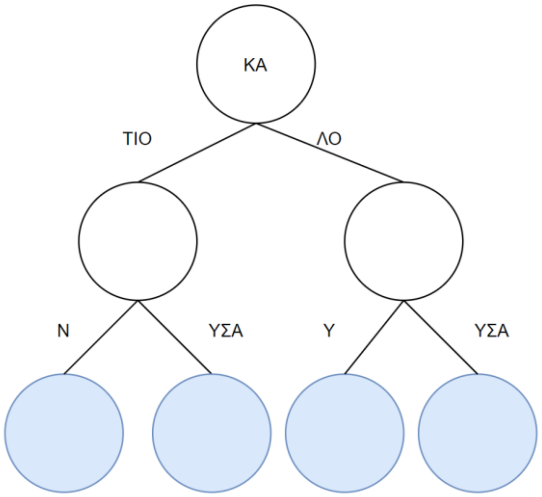
Οπότε, όλα τα δεδομένα όλων των συναλλαγών είναι αποθηκευμένα μέσα στην τιμή κατακερματισμού της ρίζας του δέντρου. Όμως, το Merkle Tree δεν είναι δέντρο αναζήτησης, δηλαδή για να αποδείξει κάποιος ότι μία συναλλαγή περιέχεται σε αυτό πρέπει να ψάξει όλο το δέντρο. Επίσης, για να αποδειχτεί ότι κάθε συναλλαγή δεν είναι ψεύτικη, πάλι πρέπει να ψαχτεί όλο το δέντρο. Ωστόσο, αν κάποιος θέλει να αλλάξει σκοπίμως μια συναλλαγή, ώστε να προκαλέσει πρόβλημα στο blockchain, αυτό γίνεται αμέσως αντιληπτό, καθώς η ρίζα του δέντρου αλλάζει τελείως. Οπότε, τα Merkle Trees προσφέρουν ασφάλεια, αλλά έχουν πολύ μεγάλο χρόνο αναζήτησης. Για το λόγο αυτό χρησιμοποιείται ένα τέχνασμα, ώστε κάποιος που απλά θέλει να ελέγξει μόνο αν μια συναλλαγή που τον αφορά περιέχεται στο συγκεκριμένο block και όχι όλες τις συναλλαγές, να μπορεί να το κάνει με μικρό κόστος σε χρόνο και χώρο. Συγκεκριμένα, δίνονται μόνο οι απαραίτητες πληροφορίες που θα χρειαστεί σε κάθε επίπεδο του δέντρου, ώστε βάζοντας τη συναλλαγή να μπορεί να σχηματίσει τη ρίζα του δέντρου και να δει αν αυτή ταυτίζεται με την πραγματική. Αν ναι, η συναλλαγή περιέχεται όντως στο block.

Για παράδειγμα, αν κάποιος θέλει να ελέγξει αν περιέχεται στη συναλλαγή T6, μια συναλλαγή που τον αφορά, ή αν η συναλλαγή T6 είναι έγκυρη, αρκεί να του δοθούν οι κόμβοι HF(5) , HF(7,7) , HF(1,2,3,4), του παραπάνω σχήματος. Έπειτα, μέσω του HF(6) που ήδη έχει βρίσκει τον HF(5,6), μέσω του HF(5,6) και του HF(7,7) βρίσκει τον HF(5,6,7,7) και, τέλος, μέσω του HF(1,2,3,4) και του HF(5,6,7,7) βρίσκει τη ρίζα και τη συγκρίνει με την πραγματική.

### 5.2.2 Modified Merkle-Patricia Tree

Το block, όπως είδαμε, περιέχει τις ρίζες τριών δέντρων ως πεδία του. Όλα, αυτά τα δέντρα, είναι ίδιου είδους, Modified Merkle-Patricia Trees. Το Modified Merkle-Patricia Tree αποτελεί δομή δεδομένων, η οποία πρωτοχρησιμοποιήθηκε στο Ethereum. Είναι ένας συνδυασμός Merkle-Tree, που παρουσιάστηκε στην προηγούμενη ενότητα και Patricia-Tree. Το Merkle Tree, όπως είδαμε, προσφέρει ασφάλεια στις συναλλαγές, καθώς, αν έστω ένα τμήμα του αλλάξει, αλλάζει και το hash value της ρίζας του, οπότε γίνεται αμέσως αντιληπτό. Είναι, όμως, αρκετά αργό στην εύρεση ενός φύλλου του, καθώς πρέπει κανείς να διασχίσει ολόκληρη τη διαδρομή που πάει προς το φύλλο αυτό ή να δοθούν σε κάποιον έτοιμοι κάποιοι κόμβοι του δέντρου. Όταν περιέχονται συναλλαγές μόνο ενός συγκεκριμένου block, ο μεγάλος αυτός χρόνος δε γίνεται αισθητός, καθώς είναι λίγα τα δεδομένα. Το Ethereum, όμως, για να μπορέσει να εκλπηρώσει το σκοπό του χρειάζεται μεγάλο όγκο δεδομένων. Το Patricia Trie έχει το πλεονέκτημα ότι είναι πολύ πιο γρήγορο στην εύρεση δεδομένων, αλλά λιγότερο ασφαλές. Το Patricia Trie (trie από retrieval) είναι μια δομή δεδομένων, η οποία χρησιμοποιεί προθέματα, ώστε να κάνει την ανάκτηση των δεδομένων πολύ πιο γρήγορη. Συγκεκριμένα,

παίρνει τις συμβολοσειρές ως εισόδους και ελέγχει αν κάποιες εξ' αυτών έχουν κοινά προθέματα, αρχίζουν δηλαδή από ίδια σύμβολα. Αρχίζει, σιγά σιγά να δημιουργείται ένα δέντρο, το οποίο ξεκινά από έναν κόμβο, ο οποίος πηγαίνει με το κοινό πρόθεμα στους επόμενους κόμβους και αυτοί με το επόμενο κοινό πρόθεμα στους επόμενους και ούτω καθεξής. Όταν φτάσει μια συμβολοσειρά στο τέλος της, πηγαίνει σε έναν τελικό κόμβο, που σημαίνει τέλος συμβολοσειράς. Η διαδικασία συνεχίζεται μέχρι όλες οι συμβολοσειρές να τερματίσουν (μπλε κόμβοι). Για να γίνει καλύτερα αντιληπτή η όλη διαδικασία, ας πάμε σε ένα παράδειγμα. Έστω ότι έχουμε τις συμβολοσειρές ΚΑΤΙΟΝ,ΚΑΤΙΟΥΣΑ,ΚΑΛΟΥ, ΚΑΛΟΥΣΑ. Τότε σχηματίζεται το παρακάτω δέντρο:




Σχήμα 9: Παράδειγμα Modified Merkle-Patricia Tree

Όπως γίνεται αντιληπτό, στα δέντρα αυτά είναι πολύ γρήγορη η διαδικασία εύρεσης κάποιας συμβολοσειράς, καθώς γνωρίζοντας τη συμβολοσειρά, μπορεί κανείς να επισκέπτεται μόνο τους κόμβους που οδηγούνται προς αυτή και έτσι να βρει εύκολα, αν η συγκεκριμένη συμβολοσειρά βρίσκεται στο δέντρο.

Το Modified Merkle Patricia Trie του Ethereum χρησιμοποιεί αυτά ακριβώς τα πλεονεκτήματα των Merkle Trees και των Patricia Tries, χωρίς τα μειονεκτήματά τους, ώστε να φτάσει στο επιθυμητό αποτέλεσμα. Το δέντρο αυτό παίρνει ως είσοδο ζευγάρια κλειδιών-τιμών (key-value pairs) στο δεκαεξαδικό (hex) σύστημα, δηλαδή ένα mapping.

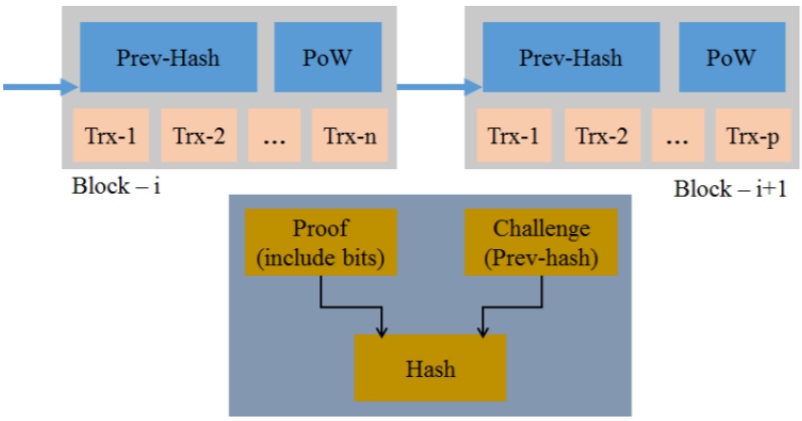
### 5.2.3 Αλγόριθμοι Συναίνεσης

Ένας αλγόριθμος συναίνεσης (consensus algorithm) είναι μία διαδικασία μέσω της οποίας όλοι οι κόμβοι ενός δικτύου καταλήγουν σε μία συμφωνία για την παρούσα κατάσταση του κατανεμημένου blockchain. Δηλαδή οι μηχανισμοί συναίνεσης εξασφαλίζουν ότι όλοι οι μη-ελαττωματικοί χρήστες του δικτύου εκτελούν τις ίδιες ανανεώσεις κατάστασης του συστήματος με τη σειρά που συνέβησαν τα γεγονότα που άλλαξαν την κατάστασή του. Οι πιο γνωστοί αλγόριθμοι συναίνεσης είναι οι Proof of Work (PoW) και Proof of Stake (PoS). Τον τελευταίο, ωστόσο καιρό έχουν εμφανιστεί εναλλακτικοί νέοι αλγόριθμοι συναίνεσης όπως οι Proof of Activity (PoAct) και Proof of Authority(PoA)

#### *5.2.3.1 Proof of Work*

Οι Cynthia Dwork και Moni Naor, σε μία δημοσίευσή τουςτο 1993, παρουσίασαν αυτόν τον αλγόριθμο του αλγορίθμου Proof of Work (PoW) και ανέφεραν συγκεκριμένα: Η βασική ιδέα είναι να ζητηθεί από τον χρήστη να υπολογίσει μια μέτριας δυσκολίας, αλλά όχι δύσχρηστη συνάρτηση, προκειμένου να αποκτήσει πρόσβαση σε έναν πόρο, αποτρέποντας έτσι την

επιπόλαιη χρήση του. Το 2006, ο Harold Thomas Finney, δημιούργησε τον αλγόριθμο RPoW (Reusable Proof of Work) με στόχο να λύσει το πρόβλημα της διπλής σπατάλης (double spending problem). Ο αλγόριθμος αυτός μετά χρησιμοποιήθηκε στο Bitcoin, για να λύσει το ίδιο πρόβλημα, ενώ συνεχίζει να χρησιμοποιείται ευρέως μέχρι σήμερα στην πλειοψηφία των κρυπτονομισμάτων. Στην ουσία, ο Reusable Proof of Work δεν είναι αλγόριθμος, αλλά ιδέα, η οποία βασίζεται σε κάποιον αλγόριθμο υπολογισμού συνάρτησης. Proof of Work, σε γενικά πλαίσια, σημαίνει ότι για να ανταμειφθεί κανείς με το να έχει πρόσβαση σε έναν πόρο, πρέπει να υπολογίσει την αποκρυπτογράφηση του κρυπτογραφημένου στίγματός του. Μάλιστα, για να έχει κανείς πρόσβαση και σε άλλον πόρο πρέπει πάλι να κάνει το ίδιο. Οπότε, έτσι, αποφεύγεται το double spending problem, διότι, αν σπαταλήσει κανείς ένα αντικείμενο αξίας, για να αποκτήσει πρόσβαση σε έναν πόρο, θα χρειαστεί κάποιος χρόνος ώσπου να μπορέσει να το κάνει, οπότε αν προσπαθήσει κανείς με το ίδιο αντικείμενο αξίας να αποκτήσει πρόσβαση και σε άλλον πόρο, θα χρειαστεί πάλι να υπολογίσει, και ο χρόνος είναι αρκετά μεγαλύτερος, από αυτόν που χρειάζεται, ώστε το αντικείμενο αξίας να έχει φύγει ήδη από την κατοχή του. Στα κρυπτονομίσματα η ιδέα αυτή χρησιμοποιείται για την ασφάλεια των συναλλαγών και μάλιστα, υπάρχει μηχανισμός ρύθμισης, ώστε ο χρόνος από την δημιουργία ενός block μέχρι τη δημιουργία του επόμενου block, να διατηρείται μεγάλος. Οι εξορύκτες έχουν δύο σημαντικούς ρόλους: να επικυρώνουν τις συναλλαγές αποφεύγοντας τις πιθανές απειλές δικτύου, και να υπολογίζουν τα σημεία λέξης-κλειδιού. Το μπλοκ περιέχει αριθμούς συναλλαγών, όπου ο miner εφαρμόζει απόδειξη εργασίας για την αξιολόγηση μεμονωμένων συναλλαγών όπως φαίνεται στο παρακάτω σχήμα, προκειμένου να λάβει κάποια ανταμοιβή.




Σχήμα 10: Συναλλαγές απόδειξης εργασίας.

Προκειμένου να επιτευχθούν οι πόντοι ανταμοιβής, όλοι οι miners ανταγωνίζονται μεταξύ τους για να λύσουν το μαθηματικό πρόβλημα. Μετά την εξεύρεση λύσης, ο miner τη μεταδίδει σε όλους τους συμμετέχοντες του δικτύου για να ενημερώσουν το blockchain και να λάβει την ανταμοιβή της εργασίας σε κρυπτονομίσματα. Σε ένα πραγματικό πρόβλημα, η διαδικασία εξόρυξης είναι ουσιαστικά μια αντίστροφη συνάρτηση κατακερματισμού. Στο τυπικό blockchain, οι παράμετροι ενημερώνονται κάθε δεκαπενθήμερο και το νέο μπλοκ δημιουργείται κάθε 10 λεπτά.

Το πρωτόκολλο PoW λειτουργεί με κατανεμημένη συναίνεση, όπου ο miner χρειάζεται πολλή ενέργεια. Οι ετήσιες συναλλαγές καταναλώνουν περίπου όση ηλεκτρική ενέργεια καταναλώνεται ετησίως στη Δανία. Αυτό είναι και το μεγαλύτερο μειονέκτημα αυτού του αλγρίθμου και ο βασικός λόγος που το Ethereum Blockchain αναμένεται να υιοθετήσει ολοκληρωτικά τον εναλλακτικό αλγόριθμο PoS που θα περιγραφεί παρακάτω :

#### *5.2.3.2 Proof of Stake*

Αρχικά, η ιδέα αυτού του αλγορίθμου δημιουργήθηκε για για να βοηθήσει στην διαχείριση προτεραιότητας εκτέλεσης των συναλλαγών του bitcoin. Η βασική έννοια της απόδειξης-πονταρίσματος είναι η απόδειξη της ιδιοκτησίας του ψηφιακού νομίσματος από την απόδειξη της εργασίας. Σε αυτόν τον αλγόριθμο συναίνεσης, οι επικυρωτές (validators) των νέων blocks επενδύουν τα κρυπτονομίσματά τους στο σύστημα ως απόδειξη επικύρωσης των συναλλαγών. Πιο συγκεκριμένα, κάθε validator ψηφίζει τα blocks που θεωρεί ότι μπορούν να προστεθούν στο blockchain κλειδώνοντας έναν αριθμό από τα κρυπτονομίσματα που διαθέτει σαν “στοίχημα”. Συνεπώς, η ψήφος του κάθε validator είναι ανάλογη του ποσού που κλείδωσε. Το block που θα συγκεντρώσει τις περισσότερες ψήφους, θα προστεθεί τελικά στο blockchain και θα δοθεί η ανάλογη ανταμοιβή στους validators προκειμένου να έχουν κίνητρο να δρούν καλόβουλα. Όσοι validators ψήφισαν το προστιθέμενο block λαμβάνουν οικονομική αμοιβή ανάλογη της ψήφου τους. Στην περίπτωση που κάποιος validator ψηφίσει δόλια ένα block που δεν είναι έγκυρο, κρατείται από το σύστημα το ποσό που κλείδωσε. Καθώς το κόστος ενέργειας και υλικού αυξάνεται με αυξανόμενη δυσκολία εξόρυξης στα δίκτυα POW, το POS εμφανίστηκε ως εναλλακτική λύση. Δίνει μεγαλύτερο βάρος στον συμμετέχοντα για να πραγματοποιήσει εξόρυξη ή έλεγχο ταυτότητας αποκλεισμού συναλλαγών ανάλογα με τον αριθμό των κρυπτονομισμάτων που κατέχει. Παρόλο που το POS επιτυγχάνει τον σκοπό της μείωσης των λογαριασμών ηλεκτρικής ενέργειας και χρησιμοποιεί υλικό χαμηλού κόστους, προωθεί την συσσώρευση κρυπτονομισμάτων αντί της κατανάλωσης.

Τόσο το POW όσο και το POS αποτρέπουν τις πιθανότητες επίθεσης 51% - μια υποθετική κατάσταση όπου μια ομάδα συμμετεχόντων μπορεί να κερδίσει περισσότερο από το ήμισυ της υπολογιστικής ισχύος του δικτύου. Η κατοχή του 51% της ισχύος του δικτύου θα σήμαινε τον πλήρη έλεγχο του δικτύου, συμπεριλαμβανομένης της δυνατότητας να σταματήσει η επιβεβαίωση νέων συναλλαγών, να σταματήσουν οι πληρωμές μεταξύ διαφόρων χρηστών blockchain και ακόμη και να αντιστραφούν οι συναλλαγές που είχαν ολοκληρωθεί στο παρελθόν κατά τον έλεγχο του δικτύου.

#### *5.2.3.3 Proof of Action*

Ο αλγόριθμος Απόδειξη δραστηριότητας (POA), ο οποία είναι ένα υβριδικό μοντέλο POW και POS, προσπαθεί να συνδυάσει τα πλεονεκτήματα και των δύο. Στο POA, η διαδικασία εξόρυξης ξεκινά ως μια τυπική διαδικασία POW με διάφορους miners που προσπαθούν να ξεπεράσουν ο ένας τον άλλον με μεγαλύτερη υπολογιστική ισχύ για να βρουν ένα νέο μπλοκ. Όταν βρεθεί ένα νέο μπλοκ (mined), το σύστημα αλλάζει σε POS, με το μπλοκ που μόλις βρέθηκε να περιέχει μόνο μια κεφαλίδα και τη διεύθυνση ανταμοιβής του miner.

Με βάση τις λεπτομέρειες της κεφαλίδας, επιλέγεται μια νέα τυχαία ομάδα επικυρωτών από το δίκτυο blockchain που απαιτείται να επικυρώσουν ή να υπογράψουν το νέο μπλοκ. Όσο περισσότερα κρυπτονομίσματα κατέχει ένας επικυρωτής, τόσο περισσότερες πιθανότητες έχει να επιλεγεί ως υπογράφων. Μόλις όλοι οι επικυρωτές υπογράψουν το μπλοκ που βρέθηκε πρόσφατα, εντοπίζεται και προστίθεται στο δίκτυο blockchain και οι συναλλαγές αρχίζουν να καταγράφονται σε αυτό. Σε περίπτωση που ορισμένοι από τους επιλεγμένους υπογράφοντες δεν είναι διαθέσιμοι για να υπογράψουν το μπλοκ στην ολοκλήρωση, η διαδικασία μετακινείται στο επόμενο μπλοκ νίκης με ένα νέο σετ επικυρωτών να επιλέγεται τυχαία ανάλογα με το ποντάρισμα του νομίσματος και η διαδικασία συνεχίζεται έως ότου ένα νικητήριο μπλοκ λάβει τον απαιτούμενο αριθμό υπογραφόντων και γίνεται πλήρες μπλοκ. Τα έξοδα εξόρυξης / ανταμοιβές κατανέμονται μεταξύ του miner και των διαφόρων επικυρωτών που συνέβαλαν στους αντίστοιχους ρόλους τους για να εγγραφεί το μπλοκ.

Δεδομένου ότι ο αλγόριθμος POA παντρεύει στοιχεία των POW και την POS, έχει δεχθεί κριτική για τη μερική χρήση και των δύο. Απαιτείται πάρα πολύ ισχύς για την εξόρυξη μπλοκ

κατά τη φάση POW και οι συλλέκτες κρυπτονομισμάτων εξακολουθούν να έχουν περισσότερες πιθανότητες να μπουν στη λίστα των υπογραφόντων και να συγκεντρώσουν περισσότερες ανταμοιβές κρυπτονομισμάτων.

Τέλος ο αλγόριθμος POA αποτρέπει επίσης την πιθανότητα επίθεσης 51% όπως στο POW και στο POS, καθώς είναι αδύνατο να προβλεφθεί ποιος θα είναι ο υποψήφιος παίκτης στο μέλλον, και ο ανταγωνισμός εξοικονόμησης νομισμάτων μεταξύ των υπογραφόντων δεν επιτρέπει τη συσσώρευση υπολογιστικής ισχύος μέσα σε μια ομάδα.

#### *5.2.3.4 Proof of Authority*

Ο αλγόριθμος Proof of Authority (PoA) είναι ένας αλγόριθμος συναίνεσης που βασίζεται στη φήμη και αποτελεί μια πρακτική και αποτελεσματική λύση για δίκτυα blockchain (ειδικά τα ιδιωτικά). Ο όρος προτάθηκε το 2017 από τον συνιδρυτή της Ethereum και τον πρώην CTO Gavin Wood. Ο αλγόριθμος συναίνεσης PoA αξιοποιεί την αξία των ταυτοτήτων, πράγμα που σημαίνει ότι οι επικυρωτές μπλοκ δεν ποντάρουν κρυπτονομίσματα αλλά αντ 'αυτού τη φήμη τους. Επομένως, τα PoA blocks προστατεύονται από τους κόμβους επικύρωσης που επιλέγονται αυθαίρετα ως αξιόπιστες οντότητες. Η λειτουργία του μοντέλου PoA βασίζεται σε περιορισμένο αριθμό επικυρωτών και αυτό το καθιστά ένα εξαιρετικά επεκτάσιμο σύστημα. Τα μπλοκ και οι συναλλαγές επαληθεύονται από προ-εγκεκριμένους συμμετέχοντες, οι οποίοι ενεργούν ως συντονιστές του συστήματος.

Ο αλγόριθμος συναίνεσης PoA μπορεί να εφαρμοστεί σε μια ποικιλία σεναρίων και θεωρείται μια επιλογή υψηλής αξίας για εφοδιαστικές εφαρμογές. Όσον αφορά τις αλυσίδες εφοδιασμού, για παράδειγμα, το PoA θεωρείται μια αποτελεσματική και λογική λύση καθώς επιτρέπει στις εταιρείες να διατηρήσουν το απόρρητό τους, αξιοποιώντας ταυτόχρονα τα οφέλη της τεχνολογίας blockchain. Το Microsoft Azure είναι ένα άλλο παράδειγμα όπου εφαρμόζεται ο αλγόριθμος PoA. Με λίγα λόγια, η πλατφόρμα Azure παρέχει λύσεις για ιδιωτικά δίκτυα, με ένα σύστημα που δεν απαιτεί εγγενές νόμισμα όπως τα Ethereum gas, καθώς δεν υπάρχει ανάγκη εξόρυξης.

Μερικοί θεωρούν ότι το PoA είναι ένα τροποποιημένο PoS, το οποίο αξιοποιεί την ταυτότητα αντί για τα κρυπτονομίσματα. Λόγω της αποκεντρωμένης φύσης των περισσότερων δικτύων blockchain, το PoS δεν είναι πάντα κατάλληλο για ορισμένες επιχειρήσεις και εταιρείες. Αντίθετα, τα συστήματα PoA μπορεί να αντιπροσωπεύουν μια καλύτερη λύση για ιδιωτικές μπλοκ αλυσίδες επειδή η απόδοσή του είναι σημαντικά υψηλότερη.

Προϋποθέσεις συναίνεσης της απόδειξης της αρχής

Αν και οι συνθήκες μπορεί να διαφέρουν από σύστημα σε σύστημα, ο αλγόριθμος συναίνεσης PoA συνήθως βασίζεται σε:

- έγκυρες και αξιόπιστες ταυτότητες: οι επικυρωτές πρέπει να επιβεβαιώσουν τις πραγματικές τους ταυτότητες.
- δυσκολία να γίνει κανείς επικυρωτής: ένας υποψήφιος πρέπει να είναι πρόθυμος να επενδύσει χρήματα και να διακυβεύσει τη φήμη του. Υπάρχει μια πολύπλοκη διαδικασία που μειώνει τους κινδύνους επιλογής αμφισβητήσιμων επικυρωτών και ενθαρρύνει μια μακροπρόθεσμη δέσμευση.
- ένα πρότυπο για έγκριση επικυρωτή: η μέθοδος επιλογής επικυρωτών πρέπει να είναι ίση με όλους τους υποψηφίους.

Η ουσία πίσω από τον μηχανισμό φήμης είναι η βεβαιότητα πίσω από την ταυτότητα του επικυρωτή. Αυτή δεν μπορεί να είναι μια εύκολη διαδικασία. Ένα ασφαλές PoA θα πρέπει να είναι ικανό να αποβάλλει κακούς παίκτες Τέλος, η διασφάλιση ότι όλοι οι επικυρωτές ακολουθούν την ίδια διαδικασία εγγυάται την ακεραιότητα και την αξιοπιστία του συστήματος.

Περιορισμοί

Η αντίληψη του μηχανισμού PoA είναι ότι ξεπερνά την έννοια της αποκέντρωση. Έτσι θα μπορούσε κανείς να πει ότι αυτό το μοντέλο αλγόριθμου συναίνεσης είναι απλώς μια προσπάθεια να καταστούν τα κεντρικά συστήματα πιο αποτελεσματικά. Ενώ ο αλγόριθμος PoA αποτελεί μια ελκυστική λύση για μεγάλες εταιρείες με υλικοτεχνικές ανάγκες, φέρνει κάποιο δισταγμό - ειδικά εντός του πεδίου της κρυπτογράφησης. Τα συστήματα PoA έχουν υψηλή απόδοση, αλλά οι πτυχές του αμετάβλητου τίθενται υπό αμφισβήτηση όταν συμπεριφορές όπως η λογοκρισία και η μαύρη λίστα μπορούν εύκολα να επιτευχθούν.

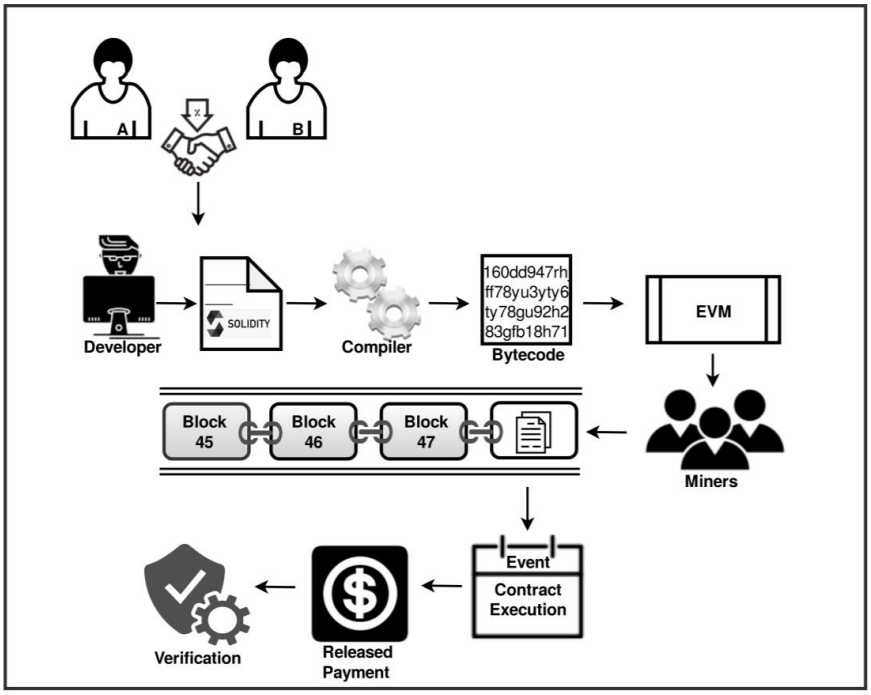
Μια άλλη κοινή κριτική είναι ότι οι ταυτότητες των επικυρωτών PoA είναι ορατές σε όλους. Το επιχείρημα εναντίον αυτού είναι ότι μόνο οι καθιερωμένοι παίκτες που είναι σε θέση να κατέχουν αυτή τη θέση θα επιδιώκουν να γίνουν επικυρωτές (ως γνωστά στο κοινό συμμετέχοντες). Ωστόσο, γνωρίζοντας τις ταυτότητες των επικυρωτών θα μπορούσε ενδεχομένως να οδηγήσει σε χειραγώγηση τρίτων. Για παράδειγμα, εάν ένας ανταγωνιστής θέλει να διαταράξει ένα δίκτυο που βασίζεται σε PoA, μπορεί να προσπαθήσει να επηρεάσει τους γνωστούς στο κοινό επικυρωτές να ενεργήσουν ανέντιμα προκειμένου να θέσουν σε κίνδυνο το σύστημα από μέσα.

Τα PoW, PoS ή PoA έχουν όλα τα δικά τους μοναδικά πλεονεκτήματα και μειονεκτήματα. Είναι γνωστό ότι η αποκέντρωση εκτιμάται ιδιαίτερα στην κοινότητα κρυπτογράφησης και το PoA, ως μηχανισμός συναίνεσης, θυσιάζει την αποκέντρωση προκειμένου να επιτευχθεί υψηλή απόδοση και κλιμάκωση. Τα εγγενή χαρακτηριστικά των συστημάτων PoA είναι μια έντονη αντίθεση με τον τρόπο λειτουργίας των blockchains μέχρι τώρα. Ωστόσο, το PoA παρουσιάζει μια ενδιαφέρουσα προσέγγιση και δεν μπορεί να αγνοηθεί ως μια αναδυόμενη λύση blockchain, η οποία μπορεί να ταιριάζει καλά σε ιδιωτικές εφαρμογές blockchain.

## 5.3 Smart Contracts

Τα έξυπνα συμβόλαια έχουν δύο χαρακτηριστικά, τα οποία τα καταστούν κατάλληλα για να εκπληρώσουν το συγκεκριμένο σκοπό. Το πρώτο είναι ότι είναι αμετάβλητα (immutable), δηλαδή αν ένα έξυπνο συμβόλαιο εκτελεστεί, ο κώδικάς του ποτέ δεν μπορεί να αλλάξει. Το δεύτερο χαρακτηριστικό είναι ότι είναι αποκεντρωμένα (decentralized), δηλαδή όταν κάποιος θέλει να εκτελέσει μια συνάρτηση ενός έξυπνου συμβολαίου, θα πρέπει, για να γίνουν αλλαγές, όντως, στην κατάστασή του, η πλειοψηφία των miners του Ethereum, να εγκρίνει τη συναλλαγή. Αυτά τα δύο χαρακτηριστικά προσφέρουν ασφάλεια, καθώς αν συμφωνηθεί κάτι, ούτε αλλάζει ποτέ, ούτε τα κριτήρια που έχουν οριστεί, μπορούν να προσπεραστούν, καθώς δε θα υπάρξει έγκριση. Το πρότυπο που χρησιμοποιεί το Ethereum για να προσεγγίσει τη χρήση μια TuringComplete γλώσσας μοιάζει με αυτό μιας εικονικής μηχανής (virtual machine). Για το λόγο αυτό, η γλώσσα στην οποία γράφονται τα έξυπνα συμβόλαια στο Ethereum ονομάζεται EVM (Ethereum Virtual Machine). Η γλώσσα αυτή μοιάζει με κώδικα μηχανής (assembly).

Στην παρακάτω εικόνα παρουσιάζονται τα στάδια εκτέλεσης ενός smart contract που αποτελεί την συμφωνία δύο ενδιαφερόμενων μερών. Ο κώδικας του smart contract γράφεται από κάποιον developer σε κώδικα Solidity. Ο κώδικας αυτό μεταγλωττίζεται σε bytecode ούτως ώστε να μπορεί να διαβαστεί από την εικονική μηχανή του Ethereum. Στη συνέχεια απαιτείται η συμμετοχή των miners ώστε να προστεθεί το block στην αλυσία. Όταν εισαχθεί, μπορούν να ξεκινήσουν οι ορισμένες από τον κώδικα λειτουργίες του έξυπνου συμβολαίου και να προκύψουν τα επιθυμητά events. Η εκτέλεση του συμβολαίου απελευθερώνει και τις πληρωμές στις κατάλληλες διευθύνσεις, τις οποίες στη συνέχεια μπορεί να επαληθεύσει κάθε συμμετέχων στο δίκτυο.




Σχήμα 11: Στάδια Εκτέλεσης Smart Contract στο δίκτυο Ethereum

## 5.4 Ethereum Virtual Machine (EVM)

Το Ethereum ουσιαστικά αναφέρεται σε μία σειρά πρωτοκόλλων που ορίζουν μια πλατφόρμα για αποκεντρωμένες εφαρμογές. Στην καρδιά αυτής της πλατφόρμας βρίσκεται η Εικονική Μηχανή Ethereum (Ethereum Virtual Machine - EVM), η οποία μπορεί να εκτελέσει κώδικα αυθαίρετης αλγοριθμικής πολυπλοκότητας. Η Εικονική Μηχανή του Ethereum αποτελεί το περιβάλλον εκτέλεσης των έξυπνων συμβολαίων στο Ethereum. Είναι πλήρως απομονωμένη από το δίκτυο, γεγονός που σημαίνει ότι ο κώδικας που τρέχει εντός της εικονικής μηχανής δεν έχει καμία πρόσβαση στο δίκτυο, το σύστημα αρχείων ή άλλες διαδικασίες. Μάλιστα τα έξυπνα συμβόλαια έχουν περιορισμένη πρόσβαση ακόμα και όσον αφορά άλλα έξυπνα συμβόλαια. Οι προγραμματιστές μπορούν να δημιουργήσουν έξυπνα συμβόλαια με τη χρήση φιλικών γλωσσών προγραμματισμού, οι οποίες βασίζονται σε υφιστάμενες γλώσσες όπως JavaScript και Python.

Όπως κάθε blockchain, έτσι και το Ethereum στηρίζεται σε ένα peer-to-peer δίκτυο. Η βάση δεδομένων του Ethereum blockchain συντηρείται και ενημερώνεται από πολλούς κόμβους που συνδέονται στο δίκτυο. Κάθε κόμβος του δικτύου τρέχει την Εικονικής Μηχανή Ethereum και εκτελεί τις ίδιες οδηγίες. Αυτή η μέθοδος καθιστά τους υπολογισμούς στο Ethereum πολύ πιο αργούς και ακριβούς από ότι σε έναν παραδοσιακό υπολογιστή. Ωστόσο, έτσι εξασφαλίζεται η ύπαρξη συναίνεσης σε ολόκληρο το blockchain, χωρίς να είναι αναγκαία η ύπαρξη μιας τρίτης έμπιστης αρχής (trusted third party).

Η εικονική μηχανή του Ethereum (Ethereum Virtual Machine) δίνει τη δυνατότητα στους προγραμματιστές να γράφουν έξυπνα συμβόλαιο σε κανονική γλώσσα (Solidity) και όχι σε τύπου assembly γλώσσα. Οι διάφορες εντολές της Solidity μεταφράζονται σε κώδικα που μπορεί να τρέξει η EVM, με αποτέλεσμα να μπορούν να τρέχουν τα έξυπνα συμβόλαια. Είναι μια στατική scripting γλώσσα, η οποία διεξάγει τη διαδικασία της επαλήθευσης και επιβολής των περιορισμών κατά το χρόνο σύνταξης (compile time) και όχι κατά το χρόνο εκτέλεσης (run time). Έχει και τις δυνατότητες του αντικειμενοστραφή προγραμματισμού, όπως η αφαιρετικότητα (abstraction), η κληρονομιά (inheritance), ο πολυμορφισμός (polymorphish), η

κλάση (class), η διεπαφή (interface) και η ενθυλάκωση (encapsulation). Γενικά, είναι μια γλώσσα με πολλές δυνατότητες που συνδυάζει τον αντικειμενοστραφή προγραμματισμό, το scripting, αλλά και όσες λειτουργίες κρίνονται απαραίτητες για ένα συμβόλαιο που τρέχει στο Ethereum.

## 5.5 Τύποι Λογαριασμών στο Ethereum

Στο Ethereum υπάρχουν δύο είδη λογαριασμών (accounts), οι εξωτερικοί λογαριασμοί ή Externally Owned Accounts (EOA) και οι λογαριασμοί συμβολαίων ή Contract Accounts.

Οι εξωτερικοί λογαριασμοί είναι αυτοί τους οποίους διαθέτουν τα άτομα και οι οποίοι χρησιμοποιούνται για να στέλνουν και να λαμβάνουν Ether σε και από άλλους εξωτερικούς λογαριασμούς, καθώς και για να εκτελούν έξυπνα συμβόλαια (smart contracts). Κάθε έξυπνο συμβόλαιο έχει και αυτό το δικό του λογαριασμό, ο οποίος είναι ο λογαριασμός συμβολαίου.

### 5.5.1 Account State

Ένα Ethereum account περιέχει τέσσερα πεδία:

1) Nonce Είναι ένας αριθμός, ίσος με τον αριθμό των συναλλαγών ή των δημιουργιών συμβολαίων που έχουν πραγματοποιηθεί από τον συγκεκριμένο λογαριασμό.

2) Balance Το σύνολο των Ether που περιέχει ο συγκεκριμένος λογαριασμός, μετρημένο σε Wei (1 Ether = 1000000000000000 Wei).

3) storageRoot Η τιμή κατακερματισμού της ρίζας του account storage trie

4) codeHash Η τιμή κατακερματισμού που οδηγεί στον κώδικα EVM του λογαριασμού.

Όλα τα παραπάνω πεδία, εκτός του codeHash, μπορούν να αλλάξουν, καθώς με νέες συναλλαγές δημιουργούνται νέα δεδομένα για τον λογαριασμό. Στους εξωτερικούς λογαριασμούς, το storageRoot είναι άδειο και το codeHash είναι τιμή κατακερματισμού για μία άδεια συμβολοσειρά. Στους λογαριασμούς συμβολαίων, όλα τα δεδομένα είναι αποθηκευμένα μέσα στο Account Storage Trie, το οποίο είναι ένα Merkle Patricia Trie, με κλειδιά τους λογαριασμούς συμβολαίων και τιμές τα δεδομένα του κώδικα. Η τιμή κατακερματισμού της ρίζας αυτού του δέντρου αποτελεί το πεδίο storageRoot, ενώ ο κώδικας του συμβολαίου αυτού είναι το πεδίο codeHash, αφου κρυπτογραφηθεί.

Όπως γίνεται αντιληπτό, απόρροια του γεγονότος ότι το codeHash δεν αλλάζει, είναι ότι ένα έξυπνο συμβόλαιο το οποίο περιέχει λάθη και έχει ήδη εκτελεστεί, δεν μπορεί να αντικατασταθεί από κάποιο νέο, καθώς τότε θα άλλαζε και το codeHash του λογαριασμού του. Αυτός είναι και ο λόγος που τα smart contracts πρέπει να τεστάρονται για τη λειτουργία τους εξονυχιστικά, πριν εκτελεστούν.

### 5.5.2 World State

Το World State είναι ένα mapping με κλειδί κάποιον λογαριασμό και τιμή το account state του λογαριασμού. Δηλαδή, δεδομένου ενός συγκεκριμένου λογαριασμού, δίνει τις πληροφορίες που αναφέραμε στο account state. Αναπαρίσταται ως ένα Merkle Patricia Trie, το οποίο, εκτός της ρίζας του, δεν αποτελεί μέρος του blockchain και ονομάζεται state trie. Για όλο το δίκτυο του Ethereum υπάρχει μόνο ένα state trie. Προφανώς, καθώς αλλάζουν τα δεδομένα των λογαριασμών μέσω των συναλλαγών, αλλάζει και το world state. Αν μπορούσαμε να φανταστούμε το δίκτυο του Ethereum ως έναν αποκεντρωμένο υπολογιστή, το world state θα αποτελούσε τον σκληρό του δίσκο. Οπότε, στο Ethereum δεν έχουμε όλα τα δεδομένα αποθηκευμένα μέσα στο blockchain, αλλά πολλά είναι εξωτερικά, που, όμως, οι αλλαγές σε αυτά πραγματοποιούνται μόνο αν μια συναλλαγή που τα επηρεάζει, μπει στο blockchain.

## 5.6 Συναλλαγές και Δέντρα Συναλλαγών

Υπάρχουν δύο κατηγορίες συναλλαγών, οι οποίες μπορούν να πραγματοποιηθούν στην πλατφόρμα του Ethereum, εκ των οποίων η μία περιέχει δύο υποκατηγορίες.

Οι κατηγορίες αυτές είναι:

1. Συναλλαγές μεταξύ ήδη υπαρχόντων λογαριασμών. Χωρίζεται σε δύο κατηγορίες:

   - Συναλλαγές μεταξύ δύο εξωτερικών λογαριασμών, δηλαδή μεταφορά αξίας από έναν κανονικό λογαριασμό σε έναν άλλο
   - Συναλλαγές μεταξύ ενός εξωτερικού λογαριασμού και ενός λογαριασμού συμβολαίου

2. Δημιουργία ενός νέου λογαριασμού συμβολαίου, δηλαδή εκτέλεση ενός νέου smart contract

Μια συναλλαγή (Transaction) περιέχει τα εξής πεδία:

1. Nonce Αριθμός συναλλαγών που έχουν σταλεί από τον λογαριασμό που δημιούργησε τη συγκεκριμένη συναλλαγή.

2. gasPrice Αξία σε Wei του gas που σπαταλήθηκε για να πληρωθούν τα υπολογιστικά κόστη εκτέλεσης της συναλλαγής.

3. gasLimit Η μέγιστη ποσότητα gas, που είναι δυνατό να χρησιμοποιηθεί για την εκτέλεση της συναλλαγής.

4. to Αν αφορά συναλλαγή μεταξύ εξωτερικών λογαριασμών, το πεδίο αυτό είναι ο λογαριασμός στον οποίο θα μεταφερθούν τα χρήματα. Αν αφορά συναλλαγή μεταξύ εξωτερικού λογαριασμού και λογαριασμού συμβολαίου, δηλαδή συναλλαγή, όπου κάποιος εξωτερικός λογαριασμός κάλεσε κάποια συνάρτηση από το συμβόλαιο, το πεδίο αυτό είναι ο λογαριασμός του συμβολαίου. Αν αφορά τη δημιουργία ενός νέου συμβολαίου, το πεδίο αυτό είναι πάντα κενό.

5. Value Αν η συναλλαγή αυτή αφορά τη μεταφορά χρημάτων από ένα εξωτερικό λογαριασμό σε έναν άλλο, τότε το πεδίο αυτό είναι το ποσό σε Wei, που πρόκειται να μεταφερθεί. Αν η συναλλαγή αυτή αφορά την κλίση ενός συμβολαίου, τότε το πεδίο αυτό είναι το ποσό σε Wei, που θα πληρωθεί από τον λογαριασμό συμβολαίου, που λαμβάνει το μήνυμα. Αν η συναλλαγή αυτή αφορά τη δημιουργία ενός νέου συμβολαίου, τότε το πεδίο αυτό είναι το ποσό σε Wei που θα προστεθεί στο υπόλοιπο του νεοδημιουργηθέντος συμβολαίου.

6. v,r,s Τιμές οι οποίες χρησιμοποιούνται στην κρυπτογραφημένη υπογραφή της συναλλαγής, ώστε να μπορεί να προσδιοριστεί ο λογαριασμός που έστειλε τη συναλλαγή.

7. Data Το πεδίο αυτό χρησιμοποιείται μόνο στην πρώτη κατηγορία συναλλαγών. Περιέχει τα δεδομένα εισόδου της συναλλαγής.

8. init Το πεδίο αυτό χρησιμοποιείται μόνο στη δεύτερη κατηγορία συναλλαγών. Περιέχει τον κώδικα EVM που χρησιμοποιήθηκε για την αρχικοποίηση του έξυπνου συμβολαίου.

Όταν μια συναλλαγή εκτελεστεί και το block, στο οποίο περιέχεται γίνει μέρος του Ethereum blockchain, δημιουργείται μία απόδειξη συναλλαγής (transaction receipt), η οποία περιέχει λεπτομέρειες για την εκτέλεση της συναλλαγής. Αυτό αναφέρεται, διότι υπάρχουν δύο Modified Merkle Patricia Tries, τα οποία δημιουργούνται για τις συναλλαγές.

Τα δέντρα αυτά είναι το transaction trie και το transaction receipt trie.

Υπάρχει ένα transaction trie για κάθε block που γίνεται μέρος της αλυσίδας. Περιέχει όλες τις πληροφορίες για τις συναλλαγές του συγκεκριμένου block που αναφέρθηκαν παραπάνω. Η τιμή κατακερματισμού της ρίζας του δέντρου αυτού αποτελεί πεδίο του block, όπως είδαμε.

Υπάρχει ένα transaction receipt trie για κάθε block που γίνεται μέρος της αλυσίδας. Περιέχει αποδείξεις των συναλλαγών που συμπεριλήφθηκαν στο συγκεκριμένο block. Η τιμή κατακερματισμού της ρίζας του δέντρου αυτού αποτελεί, επίσης, πεδίο του block.

## 5.7 Ether και κόστος συναλλαγών

Για να μπορέσει κάποιος να εκτελέσει ή να καλέσει ένα έξυπνο συμβόλαιο θα πρέπει, να πληρώσει ένα ποσό, ανάλογο της υπολογιστική ενέργειας από τους miners για την πραγματοποίηση του συγκεκριμένου σκοπού. Η μονάδα μέτρησης της ενέργειας αυτής ονομάζεται gas και η ποσότητα του gas, η οποία σπαταλάται για τη χρήση κάθε εντολής της EVM είναι καθορισμένη από τους δημιουργούς του Ethereum. Το gas που χρησιμοποιείται μεταφράζεται σε Ether και τα χρήματα αυτά πηγαίνουν στον miner, ο οποίος εισήγαγε τη συναλλαγή αυτή στο block του. Η τιμή του gas, όμως δεν είναι προκαθορισμένη. Κάθε χρήστης, ο οποίος δημιουργεί ή εκτελεί ένα έξυπνο συμβόλαιο αποφασίζει τι ποσό θα πληρώσει ανά gas (gas price) που θα χρησιμοποιηθεί για τη συναλλαγή αυτή, αναλόγως με το πόσο γρήγορα θέλει να εκτελεστεί. Όπως αναφέρθηκε, οι miners επιδιώκουν το μεγαλύτερο κέρδος για την υπολογιστική ενέργεια που σπαταλούν, οπότε προφανώς θα εισάγουν ευκολότερα στο block τους συναλλαγές-εκτελέσεις συμβολαίων με μεγάλη τιμή gas. Επίσης, ο χρήστης καθορίζει και τη μέγιστη ποσότητα gas (gas limit), την οποία είναι διατεθειμένος να σπαταλήσει για την εκτέλεση μιας τέτοιας συναλλαγής. Ο χρήστης πληρώνει ποσό σε Wei (1 Ether = 1015 Wei) ίσο με το γινόμενο gas price x gas limit. Αν το αίτημα εκτελεστεί επιτυχώς, δηλαδή συναντώνται τα κριτήρια που το συμβόλαιο ορίζει και ο miner το ‘εξορύξει’, τότε, αν δε χρησιμοποιηθεί όλο το gas, που ορίζεται από το gas limit, τα υπόλοιπα χρήματα επιστρέφονται στον χρήστη. Αν, όμως, το αίτημα δεν εκτελεστεί επιτυχώς, καθώς δε συναντώνται τα προ-απαιτούμενα κριτήρια, σπαταλάται όλο το ποσό, ως φόρος, στον χρήστη που έκανε εσφαλμένη κλήση συμβολαίου. Αυτό είναι και άλλο ένα χαρακτηριστικό που προσφέρει ασφάλεια, καθώς οι χρήστες πρέπει να είναι σίγουροι για την συναλλαγή που εκτελούν.

Το Ethereum παρέχει τη δυνατότητα δημιουργίας ενός κρυπτονομίσματος που ονομάζεται “Ether”. Το Ether μπορεί να μεταφερθεί μεταξύ λογαριασμών και χρησιμοποιείται ως εξής:

- για συναλλαγές ανάμεσα σε χρήστες του Ethereum blockchain.
- για την πληρωμή των υπολογισμών που γίνονται εντός της Εικονικής Μηχανής του Ethereum (EVM). Δηλαδή χρησιμοποιείται ως μέσο κοστολόγησης της υπολογιστικής ισχύος που καταναλώνει η πλατφόρμα Ethereum.

  Όπως περιγράφηκε παραπάνω, το Ethereum υλοποιεί ένα περιβάλλον εκτέλεσης έξυπνων συμβολαίων μέσω της Εικονικής Μηχανής του Ethereum. Κάθε κόμβος που συμμετέχει στο δίκτυο εκτελεί τους ίδιους υπολογισμούς προκειμένου να επικυρώσει ένα νέο block. Το γεγονός ότι τα έξυπνα συμβόλαια εκτελούνται πολλές φορές, τα καθιστά δαπανηρά και άρα πρέπει να υπάρχει ένα κίνητρο ώστε να μη χρησιμοποιείται η πλατφόρμα για υπολογισμούς που μπορούν να γίνουν εκτός αυτής. Το κίνητρο είναι το κόστος σε Ether που έχει κάθε λειτουργία που πραγματοποιείται στο Ethereum blockchain.

## 5.8 D-Apps και DAOs

Οι αποκεντρωμένες εφαρμογές αποτελούν ένα από τα πολλά επαναστατικά μοντέλα που έφερε μαζί της η έλευση της τεχνολογίας του blockchain. Μέσω των εφαρμογών αυτών, πολλές από τις σχέσεις εξουσίας που διέπουν την καθημερινότητά μας τείνουν να αλλάξουν. Ειδικότερα, η ανάγκη για μεσάζοντες στις διάφορες συναλλαγές, όποιας μορφής και αν είναι αυτές, καταργείται και έτσι δίνεται η δυνατότητα στους χρήστες να εμπορευτούν ο ένας από τον άλλον άμεσα κάποιο προϊόν ή υπηρεσία. Εδώ να αναφερθεί, ότι αποκεντρωμένες εφαρμογές αποτελούν και τα ίδια τα κρυπτονομίσματα, γεγονός που θα γίνει αντιληπτό στη συνέχεια. Αν και δεν υπάρχει μια γενική τομή στην οποία να συμφωνούν όλοι, όσον αφορά τον ορισμό των αποκεντρωμένων εφαρμογών, μια δημοσίευση του 2014, από τον David A. Johnston, ονόματι 'The General Theory of Decentralized Applications, Dapps' περιέχει τον πιο αποδεκτό ορισμό για τις εφαρμογές αυτές.

Ο ορισμός αυτός βασίζεται σε τρεις τομές:

1. Οι εφαρμογές αυτές πρέπει να είναι ανοιχτού κώδικα και να μην υπάρχει κάποια κεντρική εξουσία πάνω τους. Επίσης, τα δεδομένα δραστηριοτήτων τους πρέπει να παρέχονται δημόσια σε μέρος που οποιοσδήποτε αλληλεπιδρά με αυτές μπορεί να τα ελέγξει.

2. Οι εφαρμογές μπορούν να εκδίδουν κάποιο token, η διανομή του οποίου πρέπει να καθίσταται με σαφή τρόπο. Επίσης, τα tokens πρέπει να αποτελούν αναπόσπαστο και απαραίτητο κομμάτι της εφαρμογής.

3. Οι εφαρμογές αυτές μπορούν να αλλάξουν, ώστε να βελτιωθούν, αλλά αυτό πρέπει να προκύψει μέσω της συναινετικής πλειοψηφίας των χρηστών. Οι αποκεντρωμένες εφαρμογές έκαναν την εμφάνισή τους, μαζί με το blockchain. Μάλιστα, το Bitcoin είναι και το ίδιο μια αποκεντρωμένη εφαρμογή, όπως και όλα τα κρυπτονομίσματα που ακολούθησαν. Πλέον, η αξιοπιστία και η ασφάλεια που παρέχουν οι εφαρμογές αυτές τις κάνουν ολοένα και δημοφιλέστερες μεταξύ των χρηστών. Στο γεγονός αυτό συντέλεσαν, βέβαια, η ανικανότητα πολλών 'μεσαζόντων' εφαρμογών να δημιουργήσουν ένα αίσθημα ασφάλειας στους χρήστες τους, καθώς και η κατάργηση των επιπρόσθετων εξόδων από τις αποκεντρωμένες εφαρμογές σε τρίτα πρόσωπα μιας συναλλαγής.

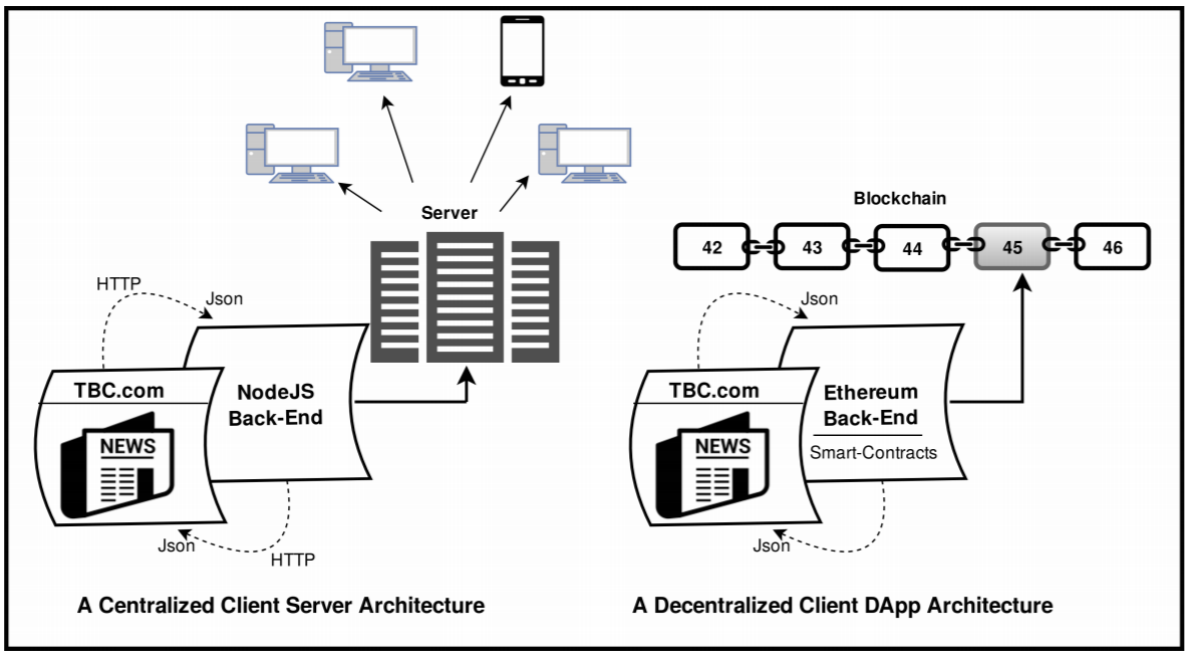
Ο όρος DAO αναφέρεται σε μια οντότητα όπου οι κανόνες διακυβέρνησης είναι κωδικοποιημένοι ως συλλογή έξυπνων συμβολαίων και εκτελούνται όταν απαιτείται. Με άλλα λόγια, ένας DAO είναι ένας οργανισμός όπου οι άνθρωποι ή άλλες οντότητες αλληλεπιδρούν μέσω ενός πρωτοκόλλου που κωδικοποιείται ως ένα πρόγραμμα υπολογιστή. Είναι σπάνιο να βρει κάνεις αμιγείς DAOs. Συχνά εμφανίζεται κάποια τρίτη οντότητα η οποία συγκεντρώνει όλη την εξουσία ή έχει το αποκλειστικό δικαίωμα του βέτο. Τα blockchains που αναφέρονται ως DAOs περιλαμβάνουν τους οργανισμούς Dash, Decred και MakerDAO.

### 5.8.1 Αρχιτεκτονική Αποκεντρωμένων Εφαρμογών D-Apps

Η τεχνολογία Blockchain εισήγαγε μια εντελώς νέα κουλτούρα στην ανάπτυξη και διαχείριση λογισμικού και συστημάτων. Με την τεχνολογία blockchain, οι προγραμματιστές δεν είναι μόνο συνεισφέροντες στο λογισμικό, πολλοί από αυτούς βοηθούν στη λειτουργία του δικτύου με συμμετοχή κόμβων, υποστήριξη εξόρυξης κ.λπ.

Οι αποκεντρωμένες εφαρμογές D-Apps είναι εφαρμογές που τρέχουν από άκρη σε άκρη στο blockchain και παρέχουν στον εξωτερικό κόσμο του blockchain τα χαρακτηριστικά και τις υπηρεσίες προκειμένου να μπορεί να παρακολουθεί και να αλληλεπιδρά με το blockchain. Μέσω τέτοιων εφαρμογών, καθίσταται δυνατό να συναλλάσονται απευθείας άνθρωποι, εφαρμογές και ολόκληρα συστήματα εφαρμογών χωρίς κάποια κεντρική αρχή διαχείρισης κι ελέγχου και συχνά χωρίς την ανάγκη να γνωρίζονται μεταξύ τους.

Στην πιο απλή μορφή της, μια εφαρμογή D-App περιλαμβάνει front-end λογισμικό (client interface) και back-end λογισμικό το οποίο περιλαμβάνει κάποιο έξυπνο συμβόλαιο και τον κώδικα του blockchain. Ένα παράδειγμα τέτοιας εφαρμογής αποτελεί κάποιο πορτοφόλι ηλεκτρονικών κρυπτονομισμάτων που περιλαμβάνει κάποια διεπαφή για τον χρήστη (client interface) και την αποκεντρωμένη υποδομή του blockchain (blockchain decentralized infrastructure). Η αρχιτεκτονική μια τέτοιας εφαρμογής είναι παρεμφερής με την αρχιτεκτονική web-browser και web server με την ειδοποιό διαφορά ότι το blockchain επιτρέπει την αποκεντρωμένη υποδομή καθώς το blockchain δεν βρίσκεται σε έναν κεντρικό κόμβο αλλά στους υπολογιστικούς κόμβους (computing nodes) που συμμετέχουν στο δίκτυο.




Σχήμα 12: Σύγκριση Client-Server και Αποκεντρωμένης Αρχιτεκτονικής

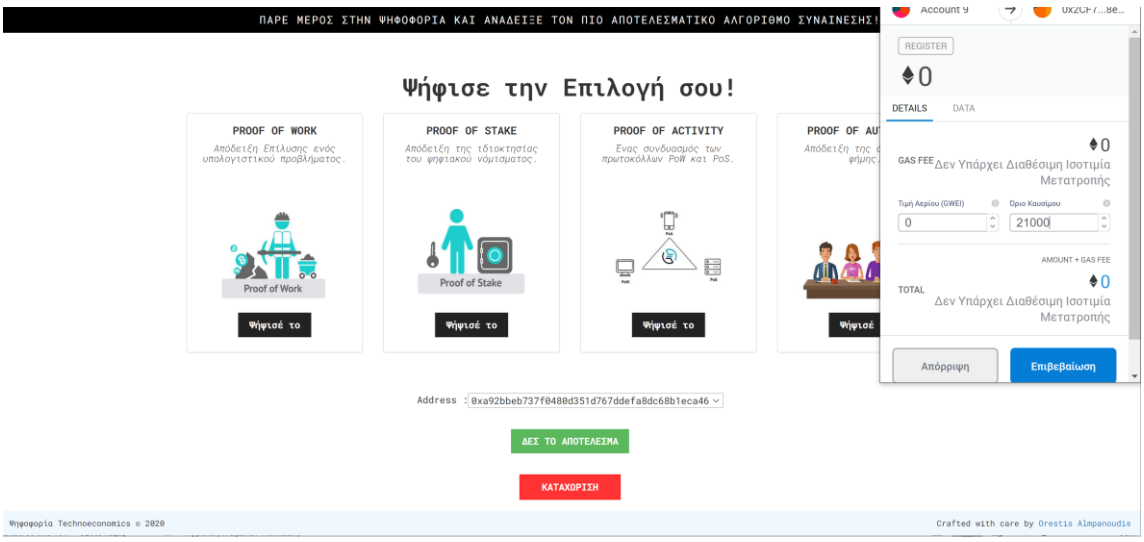
# 6. Ανάπτυξη Αποκεντρωμένης Εφαρμογής Ψηφοφορίας στο Ethereum Blockchain

Σε αυτήν την ενότητα παρουσιάζουμε μια αποκεντρωμένη εφαρμογή Ψηφοφορίας στο blockchain με στόχο να αναδείξουμε αφενός μεν τα κύρια οφέλη που μπορεί να παρέχει το blockchain σε μια διαδικασία, αφ' ετέρου τον τρόπο με τον οποίο θα μπορούσε να αναπτυχθεί μια διαδικτυακή εφαρμογή που βασίζει την λειτουργία της στο blockchain. Δεν θα ασχοληθούμε με τους μηχανισμούς της ταυτοποίησης των ψηφοφόρων και εγγραφής, όπως παρουσιάστηκε στις προηγούμενες ενότητες. Ο προσωπικός έλεγχος ταυτότητας θεωρείται διαφορετικό υπο-πρόβλημα και έμεινε εκτός του πεδίου εφαρμογής αυτής της μελέτης, όπως και οι νομικοί κανονισμοί.

Η εφαρμογή στοχεύει ψηφοφορίες μικρής κλίμακας όπως κάποια ψηφοφορία στο ΔΣ μιας επιχείρησης, όπου οι υποψήφιοι ορίζονται με off-chain συντονισμό όπως παρουσιάστηκε στην ενότητα 4.5.

Στοχεύουμε να αναδείξουμε τις κύριες συνεισφορές του Blockchain σε μια τέτοια διαδικασία και συγκεκριμένα την διατήρηση της ακεραιότητας και της αμεταβλητότητας της ψηφοφορίας και των δεδομένων εξασφαλίζοντας ευρωστία και αξιοπιστία του συστήματος ψηφοφορίας. Παράλληλα το σύστημα μας χαρακτηρίζεται από διαφάνεια, σαφήνεια και ντετερμινισμό της ψηφοφορίας, δημόσια απεικόνιση των έξυπνων συμβολαίων, και διασφάλιση ότι διατίθεται ακριβώς μία έγκυρη απόρρητη ψήφος ανά ψηφοφόρο. Οποιοσδήποτε συμμετέχοντας στο δίκτυο μπορεί να ελέγξει μόνος του την διαδικασία και δεν χρειάζεται κάποια κεντρική αρχή για την επαλήθευση του αποτελέσματος της διαδικασίας.

Στην περίπτωση μας και για λόγους ανάπτυξης και δοκιμών, προσομοιάζουμε την λειτουργία ενός private blockchain με το IDE Ganache, που θα περιγραφεί παρακάτω. Όταν ολοκληρωθεί και ελεγχθεί η εφαρμογή, μπορεί να γίνει deployed σε κάποιο δοκιμαστικό δίκτυο όπως το ropsten network ή ακόμα και το main net με κάποιες μικρές προσαρμογές που σχετίζονται με τους παρεχόμενους λογαριασμούς του κάθε δικτύου και τις παραμέτρους δικτύου αναφορικά με τον server-side κώδικα.




Σχήμα 13: Η διαδικτυακή αποκεντρωμένη εφαρμογή που σχεδιάζουμε

## 6.1 Συστατικά Συστήματος

Η προτεινόμενη εφαρμογή αποτελείται από τα ακόλουθα συστατικά:

1) Εφαρμογή Ιστού: Η εφαρμογή Ιστού επιτρέπει στους ψηφοφόρους και στον διαχειριστή για έλεγχο ταυτότητας για περαιτέρω επεξεργάζομαι, διαδικασία. Ο διαχειριστής προσθέτει τη λίστα υποψηφίων και στη συνέχεια εκκινήστε ένα αίτημα HTTP στο διακομιστή διαχείρισης συμβάντων που περιέχει τα εισαγόμενα δεδομένα. Ο στόχος αυτής της εφαρμογής Ιστού θα είναι διαθέσιμο ως διεπαφή προγραμματισμού εφαρμογών επιτρέποντας στον διαχειριστή να προσθέσει τη λίστα υποψηφίων και επιτρέψτε στις επιλεγμένες ψήφους να ψηφίσουν (μέσω ελέγχου ταυτότητας μέσω βάση δεδομένων). Καθώς η διαδικασία ψηφοφορίας πραγματοποιείται στο δίκτυο Ethereum, είναι υποχρεωτικό να υπάρχει διασύνδεση που να συνδέει την εφαρμογή ιστού με το εικονικό δίκτυο Blockchain. Επομένως, μια εφαρμογή Metamask είναι ενσωματωμένη εντός της εφαρμογής ιστού. Όλες οι συναλλαγές που μεταδίδονται από την εφαρμογή Ιστού αποστέλλονται στο δίκτυο Blockchain μέσω αυτού του πελάτη.

2) Διακομιστής διαχείρισης συμβάντων: Ο κύριος στόχος του συμβάντος

Ο Διαχειριστής διαχείρισης πρέπει να αναπτύξει το Έξυπνο συμβόλαιο στο δίκτυο με τα δεδομένα (ερωτήσεις και απαντήσεις) που λαμβάνονται από την εφαρμογή Ιστού. Επομένως, περιέχει Ethereum Πορτοφόλι (διεύθυνση) που απαιτείται για την ανάπτυξη της σύμβασης, και μιας βάσης δεδομένων για να αποθηκεύεται η λίστα των διευθύνσεων σύμβασης που θα ληφθούν αργότερα από την εφαρμογή Ιστού.

3) Έξυπνα συμβόλαια: Η λογική της διαδικασίας της ψηφοφορίας που περιγράφεται στην επόμενη ενότητα, μεταφράζεται εξ ολοκλήρου σε κώδικα έξυπνου συμβολαίου, με το οποίο μπορούν να αλληλεπιδρούν οι συμμετέχοντες του ιδιωτικού δικτύου Blockchain.

Το έξυπνο συμβόλαιο εξυπηρετεί την προσθήκη των υποψηφίων και να ξεκινήσει το ψηφοφορία περιορίζοντας μία ψήφο χρήστη μόνο μία φορά. Το έξυπνο συμβόλαιο επικυρώνει τους ψηφοφόρους και ξεκινά την ψηφοφορία, επεξεργάζεται και αυξάνει τον αριθμό των ψήφων κατά την ψηφοφορία και επιστρέφει τις συνολικές ψήφους.

4) Infura - IPFS: Παίζει σημαντικό ρόλο στη φιλοξενία της αποκεντρωμένη διαδικτυακή εφαρμογή μέσω της οποίας μπορούν οι ψηφοφόροι να ψηφίσουν μέσω Διαδικτύου από οποιοδήποτε μέρος του κόσμου.

5) Metamask: Είναι μια επέκταση για πρόσβαση στο Ethereum ενεργοποιημένες κατανεμημένες εφαρμογές ή "Dapps" στο δικό σας πρόγραμμα περιήγησης. Η επέκταση εισάγει το Ethereum web3 API και το περιβάλλον javascript κάθε ιστότοπου, έτσι ώστε τα dapps να μπορούν να διαβάσουν από το blockchain. Το MetaMask επιτρέπει επίσης στο χρήστη να δημιουργήσει και διαχειρίζονται τις δικές τους ταυτότητες μέσω ιδιωτικών κλειδιών, οπότε όταν Ο Dapp θέλει να πραγματοποιήσει μια συναλλαγή και να γράψει στο blockchain, ο χρήστης λαμβάνει μια ασφαλή διεπαφή για να ελέγξει το πριν από την έγκριση ή την απόρριψη. Οι λογαριασμοί που θα χρησιμοποιηθούν στο Metamask παρέχονται από

Όλα τα συστατικά του συστήματος θα αναλυθούν στο κεφάλαιο 7.

## 6.2 Διαδικασία Ψηφοφορίας

Η ψηφοφορία ως δημοκρατική διαδικασία αντιπροσωπεύει το παγκόσμιο πρόβλημα της επιλογής νικητή ή ηγέτη μέσω διαδικασία ψηφοφορίας. Στόχος μας είναι να σχεδιάσουμε και να αναπτύξουμε ένα Dapp για ψηφοφορία που επιλέγει ανάμεσα σε αριθμό αντικειμένων, όπως ένα σύνολο προτάσεων ή προϊόντων. Στην περίπτωσή μας, θα επιλέξουμε τη δημοτικότητα τεσσάρων διαφορετικών προτάσεων.

Εδώ είναι η λογική ή οι κανόνες που πρέπει να εφαρμοστούν.

- Ο πρόεδρος οργανώνει την ψηφοφορία και θέτει σε εφαρμογή το smart contract
- Οι ψηφοφόροι προσδιορίζονται από τις διευθύνσεις του λογαριασμού τους.
- Μόνο ο πρόεδρος μπορεί να εγγράψει άλλους ψηφοφόρους.
  (κεντρική διαχείριση όπως παρατηρήθηκε
- Ένας ψηφοφόρος μπορεί να εγγραφεί μόνο μία φορά.
- Μόνο οι εγγεγραμμένοι ψηφοφόροι μπορούν να ψηφίσουν.
- Οι ψηφοφόροι μπορούν να ψηφίσουν μόνο μία φορά.
- Οι ψηφοφόροι μπορούν να ψηφίσουν μόνο για τα αντικείμενα που παρουσιάζονται.
- Η ψηφοφορία έχει τέσσετα στάδια που εκτελούνται με χρονική σειρά (Αρχικοποίηση, εγγραφή, κατάθεση ψήφου, Ολοκλήρωση)
- Μόνο ο πρόεδρος μπορεί να ολοκληρώσει την διαδικασίατης ψηφοφορίας. Ένα έξυπνο συμβόλαιο μπορεί να γίνει self-distruct από τον δημιουργό του ή να ολοκληρωθεί μετά από χ διάστημα ή μετά απο ικανοποίηση κάποιας συνθήκης(πχ ψήφισαν όλοι) που θα ορίσει ο δημιουργός του. Δεν θα ασχοληθούμε περαιτέρω με την συνθήκη τερματισμού του συμβολαίου.

Στάδια Ψηφοφορίας

Μια τυπική διαδικασία εκλογής περιλαμβάνει κατ΄ελάχιστον τα εξής στάδια:

- Registration (Εγγραφή).
  Η εκλογική αρχή δημιουργεί την εκλογική λίστα και την δημοσιεύει στο δίκτυο. Ακολουθεί μια περίοδος παραπόνων στην διάρκεια της οποίας οι ψηφοφόροι πρέπει να εκθέσουν τις αντιρρήσεις τους. Ακολούθως η τελική λίστα δημοσιεύεται από την εκλογική αρχή.
- Voting (Ψηφοφορία). Η ψηφοφορία χωρίζεται σε δύο φάσεις:
  (α) Validation (Επιβεβαίωση). Περιλαμβάνει τον έλεγχο της εγκυρότητας αυτών που επιχειρούν να ψηφίσουν και επιτρέπει μόνο στους νόμιμους ψηφοφόρους που δεν έχουν ακόμη ψηφίσει να προχωρήσουν στη διαδικασία.
  (β) Collection (Συλλογή). Διαδικασία συλλογής των έγκυρων ψήφων.
- Tallying (Καταμέτρηση). Η αρχή συλλογής ψήφων σταματά να δέχεται ψήφους και αρχίζει την καταμέτρηση. Τα τελικά αποτελέσματα δίνονται στη δημοσιότητα.

Στην ενότητα 6.7 θα δούμε πως όλες αυτές οι απαιτήσεις μεταφράζονται στον κώδιακ του έξυπνου συμβολαίου. Παράλληλα στην ενότητα 7.4 παρουσιάζονται τα scripts που αναπτύχθηκαν προκειμένου να διαπιστωθεί ότι ολοι οι παραπάνω κανόνες εφαρμόζονται καλώς στον κώδικα του έξυπνου συμβολαίου

## 6.3 Δομή των μπλοκ

Δεδομένου ότι τα μπλοκς του Ethereum περιέχουν συναλλαγές και δεδομένου ότι το registration και το voting της εφαρμογής μας αποτελούν συναλλαγές στο Ethereum Blockchain, η δομή των συναλλαγών θα είναι ίδια με τη δομή που παρουσιάστηκε στην ενότητα 5.6 ενώ η δομή των μπλοκ θα είναι ίδια με αυτή που παρουσιάστηκε στην ενότητα 5.2.1.

Ουσιαστικά το μόνο δεδομένο που θα έχει μέσα κάποιο transaction θα είναι η επιλογή vote του ψηφοφόρου. Η συναλλαγή θα φέρει χρονοσφραγίδα και θα κοστίζει συγκεκριμένα gas όπως παρουσιάστηκε , το πεδίο from θα είναι η διεύθυνση του ψηφοφόρου, το πεδίο to θα ειναι η διεύθυνση του smart contract. Οι miners του συστήματος συμπεριλαμβάνουν στα blocks τους τις συναλλαγές ανάλογα με τα gas που κοστίζουν και έτσι οι διάφορες ψήφοι κατατίθενται στο blockchain.

## 6.4 Διαχείριση Κλειδιών

Η κρυπτογράφηση δημοσίου κλειδιού (Public Key Cryptography) ή αλλιώς ασύμμετρου κλειδιού (Asymmetric Key Cryptography) επινοήθηκε στο τέλος της δεκαετίας του 1970 από τους Whitfield Diffie και Martin Hellman[36]. Σε αντίθεση με την κρυπτογράφηση συμμετρικού κλειδιού (Symmetric Key Cryptography) όπου αποστολέας και παραλήπτης μοιράζονται ένα κοινό μυστικό κλειδί, η κρυπτογράφηση ασύμμετρου κλειδιού βασίζεται στην ιδέα οτι ο αποστολέας και ο παραλήπτης διαθέτουν διαφορετικά κλειδιά για διαφορετικές λειτουργίες.

Πιο συγκεκριμένα κάθε χρήστης διαθέτει δύο κλειδιά κρυπτογράφησης: το ιδιωτικό (private key) και το δημόσιο (public key). Το δημόσιο κλειδί είναι φανερό είτε σε όλη τη διαδικτυακή κοινότητα, είτε σε συγκεκριμένους παραλήπτες. Αντίθετα, κάθε χρήστης θα πρέπει να προφυλάσσει το ιδιωτικό του κλειδί και να το κρατάει κρυφό από τους υπόλοιπους χρήστες. Τα δύο αυτά κλειδιά έχουν μαθηματική σχέση μεταξύ τους. Δηλαδή, αν το ένα έχει χρησιμοποιηθεί για την κρυπτογράφηση κάποιου μηνύματος, το άλλο θα χρησιμοποιηθεί για την αποκρυπτογράφηση αυτού. Απαραίτητος παράγοντας για την επιτυχία αυτού του είδους κρυπτογραφικού αλγορίθμου είναι το γεγονός ότι η γνώση του δημοσίου κλειδιού δεν επιτρέπει με κανέναν τρόπο τον υπολογισμό του ιδιωτικού κλειδιού.

Πέρα από το ζευγάρι δημόσιου - ιδιωτικού κλειδιού κάθε χρήστης του blockchain έχει και μία διεύθυνση πορτοφολιού (wallet address), η οποία προκύπτει ως το Keecak-hash των τελευταίων 20 ψηφίων του δημοσίου κλειδιού. Η διεύθυνση αυτή ουσιαστικά αποτελεί την εικονική τοποθεσία του χρήστη. Στην εφαρμογή μας θα χρησιμοποιήσουμε την πλατφόρμα Ganache για την δημιουργία εικονικού ιδιωτικού δικτύου blockchain με συμμετέχοντες λογαριασμούς και το plug-in της πλατφόρμας διαχείρισης πορτοφολιών Metamask.Η ύπαρξη κρυπτογραφίας δημόσιου κλειδιού είναι απαραίτητη προϋπόθεση για το μοντέλο ασφαλείας του blockchain.

## 6.5 Πολιτική πρόσβασης στο δίκτυο του blockchain

Όπως είδαμε στην ενότητα 2.1.3 υπάρχουν δύο επιλογές ως προς τον τύπο blockchain των εφαρμογών:

Permission-less δίκτυο Ethereum

Δεν υπάρχει συγκεκριμένη λίστα από κόμβους, αλλά οποιοσδήποτε θέλει θα μπορεί να συμβάλει στην επικύρωση. Σε αυτή την περίπτωση, το blockchain θα μπορεί να χρησιμοποιηθεί πιο εύκολα και για άλλες εφαρμογές, καθώς τα περισσότερα blockchains χρησιμοποιούν αυτό το είδος δικτύου.

Permissioned δίκτυο

Οι κόμβοι που θα επικυρώνουν τα block και τις συναλλαγές θα είναι συγκεκριμένοι επιλεγμένοι κόμβοι. Σε αυτή την περίπτωση, ουσιαστικά βέβαια δεν μιλάμε για πλήρως αποκεντρωμένη εφαρμογή.

Ένα δίκτυο blockchain είναι χωρίς άδεια (permission-less) όταν δεν απαιτείται άδεια για να γίνει κάποιος μέλος του δικτύου και να συμβάλει στη συντήρησή του, δηλαδή την επικύρωση των συναλλαγών και τη δημιουργία νέων block. Ένα δίκτυο blockchain είναι με άδεια (permissioned) όταν υπάρχει λίστα με τους κόμβους που μπορούν να έχουν πρόσβαση σε αυτό και αυτοί οι κόμβοι έχουν μοναδικό αναγνωριστικό.

Χρειαζόμαστε διαφάνεια, έλεγχο ταυτότητας και αποδεδειγμένη ικανότητα συμμετοχής στην πλατφόρμα ψηφοφορίας. Από την άλλη, πρέπει να διασφαλίσουμε ότι οι άνθρωποι που συμμετέχουν στις εκλογές είναι πραγματικοί άνθρωποι και χρησιμοποιούν σωστά διαπιστευτήρια. Το σύστημα μας θα πρέπει αν είναι σε θέση ανά πάσα στιγμή να αποδείξει τα παραπάνω.

Στο πλαίσιο μελέτης αποκεντρωμένων εφαρμογών ψηφοφορίας, θα επιλέξουμε να αναπτύξουμε μια εφαρμογή ψηφοφορίας στο ιδιωτικό δίκτυο blockchain καθώς όπως παρατηρήθηκε στην ενότητα 2.1.3 μια λύση ψηφοφορίας στο ιδιωτικό blockchain είναι πολύ πιο ασφαλής (μόνο οι συμμετέχοντες στο δίκτυο μπορούν να αλληλεπιδρούν με το έξυπνο συμβόλαιο).Επίσης όπως παρατηρήθηκε στην ενότητα 2.3.2 η επιλογή ενός private blockchain συνίσταται και για λόγους συμμόρωσης με τον GDPR.

## 6.6 Αλγόριθμος Συναίνεσης

Ο αλγόριθμος συναίνεσης που χρησιμοποιείται αυτή την στιγμή στο Ethereum Blockchai είναι ο PoW, όπως παρουσιάστηκε αναλυτικά στην ενότητα 5.2.2.1.

## 6.7 Smart Contracts

Στην ενότητα αυτή θα παρουσιάσουμε αναλυτικά το smart contract που χρησιμοποιείται στην αποκεντρωμένη εφαρμογή ψηφοφοριας. Κάθε smart contract ξεκινάει με την δήλωση της έκδοσης Solidity, στην οποία έχει γραφτεί:

pragma solidity ^χ.χ.χ.

Κατόπιν ξεκινάει ο κώδικας του έξυπνου συμβολαίου με την ονομασία Ballot.

### 6.7.1 Μεταβλητές Συστήματος

Το έξυπνο συμβόλαιο περιέχει δύο δομές struct με το όνομα Voter και Proposal.

Η δομή Voter περιλαμβάνει τις μεταβλητές weight (τύπου uint8, vote και voted (τύπου boolen). Η πρώτη σχετίζεται με το βάρο του ψηφοφόρου, η δεύτερη με την επιλογή του ψηφοφόρου ενώ η τρίτη λογική μεταβλητή σχετίζεται με το αν έχει ψηφίσει ο ψηφοφόρος η όχι Στην δομή αυτή θα μπορούσαν να προστεθούν και άλλες μεταβλητές όπως κάποια μεταβλητή τύπου διεύθυνσης που θα υποδεικνύει την ανάθεση της ψήφου σε μια άλλη διεύθυνση.

Η δομή Proposal αναφέρεται στις υποψήφιες εναλλακτικές επιλογές της ψηφοφορίας περιλαμβάνει την μεταβλητή Votecount τύπου uint.

Χρησιμοποιείταιε ένα mapping για τους ψηφοφόρους με βάση την διεύθυνση, μια μεταβλητή τύπου address για την αποθήκευση του προέδρου της ψηφοφορίας (chairperson) ενώ χρησιμοποιείται κι ένας πίνακας για την αποθήκευση των εναλλακτικών την ψηφοφορίας (proposals).

Χρησιμοποιείται μία μεταβλητή τύπου uint για την καταγραφή και διαχείρση του χρόνου εκτέλεσης των συναρτήσεων register,vote,winning proposal.

Τέλος, από άποψη μεταβλητών χρησιμοποιέιται και μια μεταβλητή τύπου state( enum) που υποδηλώνει τα στάδια της ψηφοφορίας για κάθε ψηφοφόρο και παίρνει αποκλειστικά τις τιμές (Init,Reg,Vote,Done).Τα διάφορα αυτά στάδια μπορούν να αλλάξουν και να σημειωθούν στην αντίστοιχη μεταβλητή e-num με την ολοκλήρωση εκτέλεσης κάποιας συνάρτησης, όπως για παράδειγμα register, όπου η μεταβλητή θα αλλάξει από state ‘Reg’ σε state ‘Vote’.

### 6.7.2 Λειτουργίες Συστήματος

Κατά το πρώτο deployment του smart contract, εκτελούνται αποκλειστικά για μία φόρα οι συναρτήσεις τύπου constructor. Οι συναρτήσεις αυτές ειναι δημόσιες, ωστόσο μπορούν να εκτελεστούν μόνο από την διεύθυνση που έκανε deploy το smart contract. Συνήθως σε αυτές περιλαμβάνεται αρχικοποίηση κάποιων μεταβλητών που θα χρησιμοποιηθούν στον κώδικα του έξυπνου συμβολαίου. Στην περίπτωση μας η συνάρτηση constructor αρχικοποιεί τις τιμές των μεταβλητών που υποδηλώνουν τον διοργανωτή τον εκλογών (chairperson), τον αριθμό των υποψηφίων, την κατάσταση του συστήματος και τον

χρόνο έναρξης της κάθε κατάστασης. Είναι το στάδιο όπου ο διοργανωτής των εκλογών αρχικοποιεί την διαδικασία της ψηφοφορίας ορίζοντας το θέμα και τις εναλλακτικές της ψηφοφορίας. Η τιμή της μεταβλητής state παίρνει την πρώτη δυνατή τιμή Init.

Η δεύτερη συνάρτηση που χρησιμοποιείται είναι η δημόσια συνάρτηση register που παίρνει ως όρισμα μια διεύθυνση με το όνομα toProposal. Η συνάρτηση αυτή ελέγχει :

- Αν η μεταβλητοί που δηλώνει την κατάσταση του συστήματος έχει την τιμή Reg.
- Αν η συνάρτηση καλείται από τον διοργανωτή της ψηφοφορίας (καθώς μόνο ο διοργανωτής μπορεί να εγκρίνει νέους ψηφοφόρους)
- Αν η διεύθυνση του υποψηφίου έχει ψηφίσει.

Α κάποιος από τους παραπάνω ελέγχους δεν ικανοποιείται, τότε απορρίπτεται η κλήση της συνάρτησης. Αν οι έλεγχοι ικανοποιούνται, τότε δίνεται το ανάλογο βάρος στον ψηφοφόρο και θέτει την τιμή της μεταβλητής voted σε false για λόγους ασφαλείας. Επίσης στον τελευταίο εμφωλευμένο έλεγχο, ελέγχεται αν έχει ολοκληρωθεί το προηγούμενο στάδιο. Στην συγκεκριμένη υλοποίηση όλοι οι ψηφοφόροι έχουν βάρος 1. Αν θέλαμε να χρησιμοποιήσουμε βάρη στο παρόν σύστημα θα έπρεπε να έχουμε ορίσει ένα ακόμα mapping για τους ψηφοφόρους με τα αντίστοιχα βάρη τους.

Η τρίτη συνάρτηση είναι ο πυρήνας του smart contract μας καθώς με την κλήση αυτή της δημόσιας συνάρτησης, ο ψηφοφόρος θα καταθέσει οριστικά την ψήφο του στο smart contract. Ονομάζεται vote και παίρνει ως όρισμα μια μεταβλητή τύπου uint8 με όνομα toProposal, που ουσιαστικά θα εμπεριέχει την επιλογή του ψηφοφόρου. Για να είναι εφικτό για έναν ψηφοφόρο να καλέσει επιτυχώς αυτή τη συνάρτηση, ελέγχεται αν :

- Η τιμη της μεταβλητής stage είναι “Vote”, που σημαίνει ότι ο διοργανωτής της ψηφοφορίας έχει εγκρίνει την συγκεκριμένη διεύθυνση να ψηφίσει.
- Η επιλογή του ψηφοφόρου ανήκει στις δυνατές επιλογές
- Αν ο ψηφοφόρος έχει ψηφίσει

Αν κάποιος από τους παραπάνω ελέγχους δεν ικανοποιείται, τότε απορρίπτεται η κλήση της συνάρτησης. Αν οι έλεγχοι ικανοποιούνται τότε εκτελούνται με την ακόλουθη σειρά οι εξής ενέργειες:

- Τίθεται η Boolean μεταβλητή voted σε ‘True’
- Σώνεται το όρισμα της συνάρτησης στη μεταβλητή vote
- Αυξάνεται η μεταβλητή Votecount της αντίστοιχης επιλογής Proposal κατά το βάρος του ψηφοφόρου (εδώ το βάρος είναι 1)

Η τελευταία συνάρτηση του συμβολαίου μας είναι μια συνάρτηση view, δηλαδή που δεν παίρνει κάποιο όρισμα. Επιστρέφει τον νικητή της ψηφοφορίας αφού διεξάγει την σύγκριση των ψήφων για κάθε υποψήφιο.

```
pragma solidity ^0.7.0;
UnitTest stub | dependencies | uml
contract Ballot {

    struct Voter {
        uint weight;
        bool voted;
        uint8 vote;
        // address delegate;
    }
    struct Proposal {
        uint voteCount;
    }
    enum Stage {Init,Reg, Vote, Done}
    Stage public stage = Stage.Init;

    address chairperson;
    mapping(address => Voter) voters;
    Proposal[] proposals;


    uint startTime;

    /// Create a new ballot with $(_numProposals) different proposals.
    ftrace | funcSig
    constructor (uint8 _numProposals!) public  {
        chairperson = msg.sender;
        proposals.length = _numProposals!;
        stage = Stage.Reg;
        startTime = now;
    }
```

```
    /// Give $(toVoter) the right to vote on this ballot.
    /// May only be called by $(chairperson).
    ftrace | funcSig
    function register(address toVoter!) public {
        if (stage != Stage.Reg) {return;}
        if (msg.sender != chairperson || voters[toVoter!].voted) return;
        voters[toVoter!].weight = 1;
        voters[toVoter!].voted = false;
        if (now > (startTime+ 10 seconds)) {
            stage = Stage.Vote;
            startTime = now;
        }
    }

    /// Give a single vote to proposal $(toProposal).
    ftrace | funcSig
    function vote(uint8 toProposal!) public  {
        if (stage != Stage.Vote) {return;}
        Voter storage sender = voters[msg.sender];
        if (sender.voted || toProposal! >= proposals.length) return;
        sender.voted = true;
        sender.vote = toProposal!;
        proposals[toProposal!].voteCount += sender.weight;
        if (now > (startTime+ 10 seconds)) {stage = Stage.Done;}

    }

    ftrace | funcSig
    function winningProposal() public view returns (uint8 _winningProposal!) {
       if(stage != Stage.Done) {return;}
        uint256 winningVoteCount = 0;
        for (uint8 prop = 0; prop < proposals.length; prop++)
            if (proposals[prop].voteCount > winningVoteCount) {
                winningVoteCount = proposals[prop].voteCount;
                _winningProposal! = prop;
            }
    }
```

# 7. Υλοποίηση Εφαρμογής

## 7.1 Blockchain server

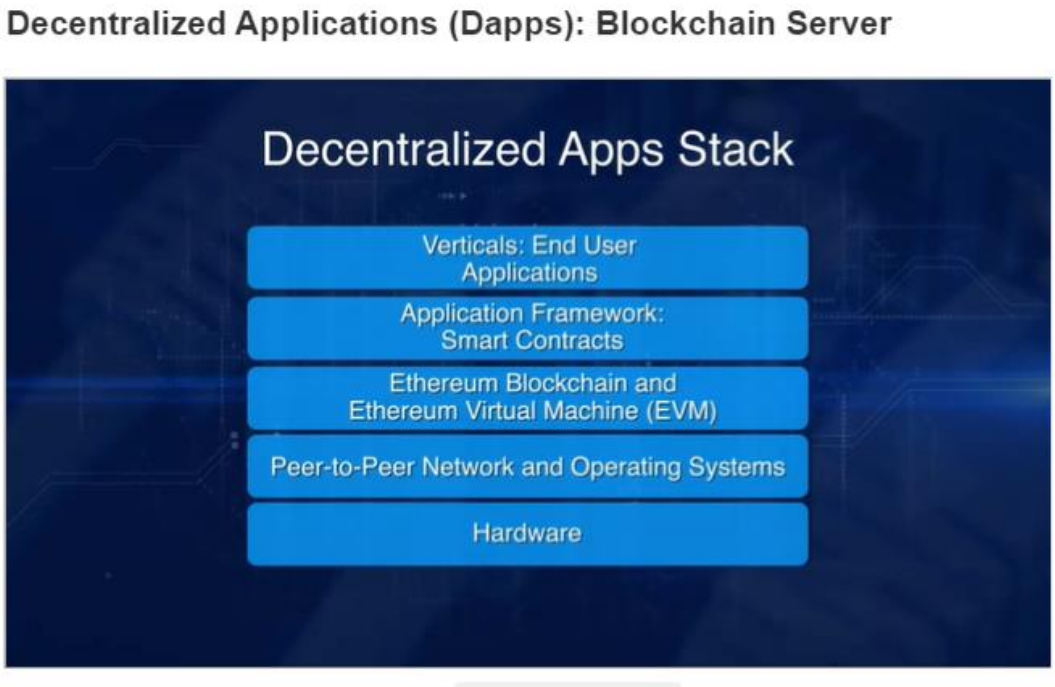
Όπως περιγράφηκε στην ενότητα 5.8, οι αποκεντρωμένες εφαρμογές D-Apps είναι εφαρμογές που τρέχουν από άκρη σε άκρη στο blockchain και παρέχουν στον εξωτερικό κόσμο του blockchain τα χαρακτηριστικά και τις υπηρεσίες προκειμένου να μπορεί να παρακολουθεί και να αλληλεπιδρά με το blockchain.

Συνολικά, η αρχιτεκτονική μιας εφαρμογής DApp περιλαμβάνει το δίκτυο peer-to-peer στο οποίο λειτουργεί αυτό το blockchain. Ο κόμβος ενός blockchain φιλοξενεί το EVM (Ethereum Virtual Machine) και το έξυπνο συμβόλαιο εκτελείται στο EVM. Οι διεπαφές χρήστη της εφαρμογής DApp που τρέχουν πάνω από αυτό το επίπεδο, χρησιμοποιούν το έξυπνο συμβόλαιο για τη λογική τους.

Η διεπαφή πελάτη (client interface) μπορεί να είναι:

- μια διεπαφή γραμμή εντολών CLI (Command Line Interface)
- κάποια δομή HTML/Javascript (HTML/Javascript framework)
- κάποια τοπική εφαρμογή υπολογιστή (desktop app)
- κάποια διαδικτυακή εφαρμογή (web-app)
- κάποια εφαρμογή κινητής συσκευής (mobile app)
- διαδίκτυο των πραγμάτων (IoT)

Σε κάθε περίπτωση, το front-end κομμάτι της εφαρμογής βρίσκεται εκτός του πρωτοκόλλου blockchain και μπορεί να συνδεθεί μόνο με το έξυπνο συμβόλαιο blockchain, χρησιμοποιώντας αντικείμενα (artifacts) που δημιουργούνται από τη διαδικασία μεταγλώττισης (compile) έξυπνων συμβολαίων.




Σχήμα 14: Αρχιτεκτονική Blockchain Server Αποκεντρωμένων Εφαρμογών

Η ονοματολογία blockchain server προέρχεται από την ομοιότητα με εφαρμογές ιστού-διακομιστή ιστού. Διακομιστής κινητής τηλεφωνίας, εφαρμογές πελάτη για κινητά, διακομιστής

βάσης δεδομένων, πελάτες βάσης δεδομένων, κ.λπ. Έτσι, ο όρος, διακομιστής blockchain χρησιμοποιείται για να περιγράψει όλες τις λειτουργίες που παρέχει.

Το API, ή η διεπαφή προγραμματισμού εφαρμογών, είναι ένας βολικός και τυπικός τρόπος για να υποστηριχθεί ένα σύνολο λειτουργιών που σχετίζονται με ένα συγκεκριμένο σύνολο δεδομένων και υπηρεσιών. Τα API προσφέρονται επίσης για επαναχρησιμοποίηση του κώδικα.

Ένα API δημοσιεύει ένα σύνολο λειτουργιών ή μεθόδων που μπορούν να χρησιμοποιηθούν μέσω προγραμματισμού για την επίκληση λειτουργιών, την πρόσβαση σε δεδομένα και την αποθήκευση δεδομένων.Η πρόσβαση σε ένα API μπορεί να ελεγχθεί με συγκεκριμένη μέθοδο πρόσβασης, για παράδειγμα, δημόσια κλειδιά, εάν αυτό απαιτείται από την εφαρμογή. Σε ένα πραγματικό δίκτυο Blockchain υπάρχουν δύο μεγάλες κατηγορίες API.

- **Admin API**

  Περιλαμβάνει API για διαχείριση, εντοπισμό σφαλμάτων, mining , personal και txpool. Υποστηρίζουν μεθόδους για τη διαχείριση του κόμβου geth.

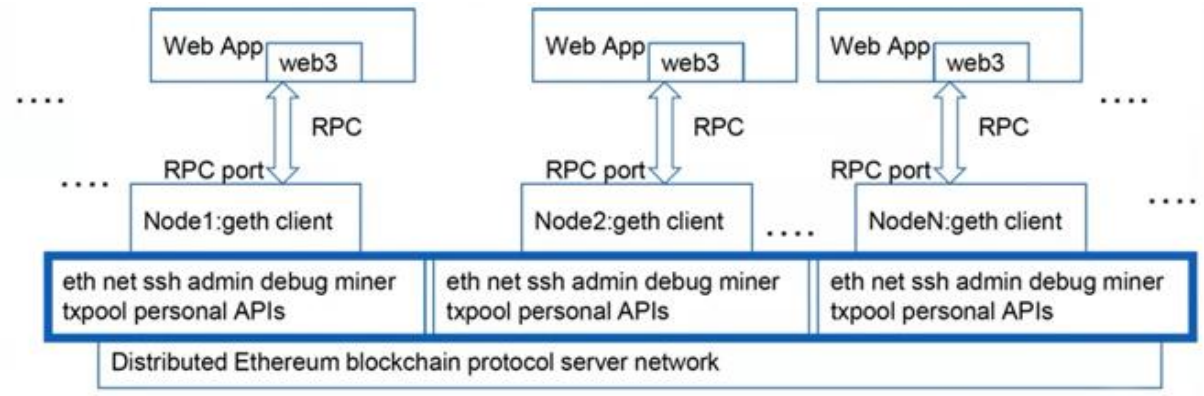
  - **Admin API**, το API Admin επιτρέπει να χρησιμοποιήσουμε συναρτήσεις για να εργαστούμε ως κόμβος του Ethereum με την παρουσία Geth, συμπεριλαμβανομένου του ομότιμου δικτύου και της διαχείρισης του τελικού σημείου RPC. το Admin API υποστηρίζει λειτουργίες για τη διαχείριση του κόμβου. Παραδείγματα εντολών, admin.addPeer (), admin.nodeInfo (). Σε αυτήν την περίπτωση, το «Admin» είναι το API και το «addPeer» και το «nodeInfo» είναι συναρτήσεις του Admin API.
  - **Debug API**, για παράδειγμα, Debug.dumpBlock (16). Αυτό θα εμφανίσει τις λεπτομέρειες της κεφαλίδας μπλοκ του μπλοκ 16. Μπορείτε να παρατηρήσετε ότι το Debug API εντοπισμού σφαλμάτων σάς παρέχει τη δυνατότητα να κοιτάμε, να μελετάμε και να εντοπίζουμε τυχόν ζητήματα κοιτάζοντας το μπλοκ.
  - **Miner API**, το miner API μας επιτρέπει να ελέγχεουμε τη λειτουργία εξόρυξης κόμβων και να ορίζετε διάφορες συγκεκριμένες ρυθμίσεις εξόρυξης. Παράδειγμα, miner.start (), miner.stop () είναι δείγματα συναρτήσεων που θα ξεκινήσουν και θα σταματήσουν το miner.
  - **Personal API** ασχολείται με τη δημιουργία και τη διαχείριση λογαριασμών σε έναν κόμβο. Διαχειρίζεται επίσης ιδιωτικά κλειδιά στο κατάστημα κλειδιών, γι 'αυτό ονομάζεται προσωπικό API. Παράδειγμα, το personal.newAccount () θα δημιουργήσει έναν νέο λογαριασμό μέσα σε έναν κόμβο.
  - **Txpool API**, το Txpool, ή το API συγκέντρωσης συναλλαγών, μας δίνει πρόσβαση σε πολλές μη τυπικές μεθόδους RPC για να ελέγξουμε το όλων των εκκρεμών συναλλαγώνς, καθώς και αυτών που βρίσκονται σε ουρά για μελλοντική επεξεργασία. Παράδειγμα, η ενολή txpool.inspect () μας απαριθμεί όλες τις εκκρεμείς συναλλαγές για να τις κατανοήσετε και να συλλέξετε για τη δημιουργία ενός μπλοκ συναλλαγών.
- **Web3 API, web3, eth και net**.

  Υποστηρίζουν μεθόδους για ανάπτυξη Dapps.

Όταν ένα αίτημα ιστού ξεκινά από έναν χρήστη και εάν είναι ένα κανονικό αίτημα εφαρμογής ιστού, κατευθύνεται στο τελικό σημείο HTTP, στο παράδειγμα μας στη θύρα 8080 και στον διακομιστή ιστού που το εκτελεστεί.

Ο πελάτης geth πρέπει να εκθέσει ένα τελικό σημείο RPC χρησιμοποιώντας την εντολή θύρας RPC. Ένα web3 artifact δημιουργείται στο script της ιστοσελίδας. (το web3.js είναι βιβλιοθήκη JavaScript) για την επικοινωνία του web-app με το blockchain μέσω κάποιου σημείου RPC.

Τα αιτήματα (requests) ή οι κλήσεις (calls) πραγματοποιούνται στο αντικείμενο web3, μεταδίδονται ως αγωγός (pipeline) JSON ή RPC μεταξύ του web-App και του πελάτη geth, όπως παρουσιάζεται παρακάτω:




Σχήμα 15: Μετάδοση αιτημάτων από το web3 στον κόμβο geth

Για τους χρήστες ενός D-app δεν είναι απαραίτητο να αποτελούν πλήρεις κόμβους (full nodes) της αλυσίδας blockchain και να διαθέτουν αντίγραφο όλων των συναλλαγών και των λειτουργιών του blockchain, όπως συμβαίνει με έναν geth-client. Η ζητούμενη κλήση (call) και λειτουργία (function) εκτελούνται χρησιμοποιώντας το κατάλληλο API και τον κώδικα του έξυπνου συμβολαίου (smart contract) και το αποτέλεσμα, επιστρέφεται στον client.

## 7.2 Εργαλεία για τη δημιουργία αποκεντρωμένων εφαρμογών στο Ethereum

Το blockchain του Ethereum αποτελεί στην ουσία το περιβάλλον στο οποίο ζουν οι εφαρμογές αυτές. Μάλιστα, οι αποκεντρωμένες εφαρμογές το χρησιμοποιούν ως βάση δεδομένων και συνήθως δε χρησιμοποιούν καν κανονικές βάσεις. Αυτός είναι και ο κύριος λόγος που είναι αποκεντρωμένες. Τα συμβόλαια των αποκεντρωμένων εφαρμογών στο Ethereum, γράφονται σε Solidity και μεταφράζονται κατά το compile σε bytecode EVM. Σκοπός όλων των υπόλοιπων εργαλείων είναι κάποια στιγμή η εφαρμογή να γίνει μέρος του Ethereum δικτύου.

Για την ανάπτυξη και τη σωστή χρήση αποκεντρωμένων εφαρμογών (Dapps) στο Ethereum έχουν προταθεί πάμπολλα εργαλεία, τα οποία συνεχώς εξελίσσονται και αυξάνονται. Στα πλαίσια της συγκεκριμένης εργασίας θα αναφερθούν μόνο αυτά που χρησιμοποιήθηκαν για την εκπόνησή της. Ethereum Blockchain

Node.js and Web3

Το node.js είναι ένα περιβάλλον ανοιχτού κώδικα, το οποίο παρέχει διάφορες βιβλιοθήκες στους χρήστες του, με μία από αυτές να είναι το web3. Το web3 είναι μια συλλογή από βιβλιοθήκες, η οποία επιτρέπει στους χρήστες να αλληλεπιδράσουν με έναν τοπικό ή και απομακρυσμένο κόμβο του Ethereum, χρησιμοποιώντας σύνδεση HTTP, WebSocket ή IPC. Έχει όλες τις δυνατότητες επικοινωνίας και με το πραγματικό blockchain. Μέσω αυτού, μπορεί κάποιος να εντοπίσει ένα συμβόλαιο, δίνοντας δύο πληροφορίες, το Abi του συμβολαίου και την διεύθυνση του λογαριασμού του και έπειτα να επικοινωνήσει μαζί του. Το web3 χρησιμοποιεί τη γλώσσα Javascript για τη χρήση του και τις εντολές του.

Ganache

Το ganache είναι ένα εργαλείο, μέσω του οποίου ο χρήστης μπορεί να δημιουργήσει το δικό του προσωπικό τοπικό blockchain, το οποίο λειτουργεί με τον ίδιο ακριβώς τρόπο που λειτουργεί το πραγματικό Ethereum blockchain, με τη διαφορά ότι δε χρησιμοποιεί miners, αλλά ο χρήστης μπορεί να εισάγει πόσος χρόνος θέλει να μεσολαβεί από τη δημιουργία ενός block, μέχρι τη δημιουργία ενός άλλου. Χρησιμοποιείται ώστε να δοκιμαστεί η λειτουργία των έξυπνων συμβολαίων ή της εφαρμογής που είναι χτισμένα πάνω στο Ethereum, πριν αυτά πυροδοτηθούν στο πραγματικό blockchain. Δίνει τη δυνατότητα στον χρήστη να εισάγει όποιες επιλογές θέλει, ώστε να προσομοιώσει όπως ακριβώς θέλει τις εφαρμογές του.

Truffle

Το Truffle είναι ένα αναπτυξιακό περιβάλλον, δοκιμαστικό πλαίσιο (testing framework) και μέσο επικοινωνίας με το Ethereum, που έχει σκοπό να βελτιώσει και να διευκολύνει τον τρόπο με τον οποίο ένας προγραμματιστής αλληλεπιδρά με αυτό. Συγκεκριμένα, είναι ένα μέσο το οποίο επικοινωνεί με το ganache και μέσω του οποίου καθίσταται δυνατή η μετατροπή των έξυπνων συμβολαίων, τα οποία είναι γραμμένα σε solidity, στη γλώσσα που αντιλαμβάνεται το blockchain. Τα κάνει compile, τα συνδέει, τα αναπτύσσει και διαχειρίζεται τον δυαδικό τους κώδικα. Μέσω του truffle, δίνεται η δυνατότητα στον προγραμματιστή να εκτελέσει όλα του τα συμβόλαια μαζί και να φτιάξει ξεχωριστά tests για το καθένα, που με μία εντολή αυτόματα θα εκτελεστούν όλα. Επίσης, μπορεί κάποιος να επικοινωνήσει άμεσα με ένα έξυπνο συμβόλαιο ενός τοπικού blockchain, δηλαδή να του αλλάξει την κατάσταση. Το truffle χρησιμοποιεί ως γλώσσα την Javascript, και κυρίως το κομμάτι των υποσχέσεων (promises). Τέλος, να αναφερθεί ότι το truffle δε χρησιμοποιείται στο πραγματικό blockchain, αλλά αν συνδυαστεί με το ganache και το web3 που θα εξεταστεί αμέσως μετά, δίνει τη δυνατότητα ακριβούς προσομοίωσης για δοκιμή στον κώδικα ενός έξυπνου συμβολαίου.

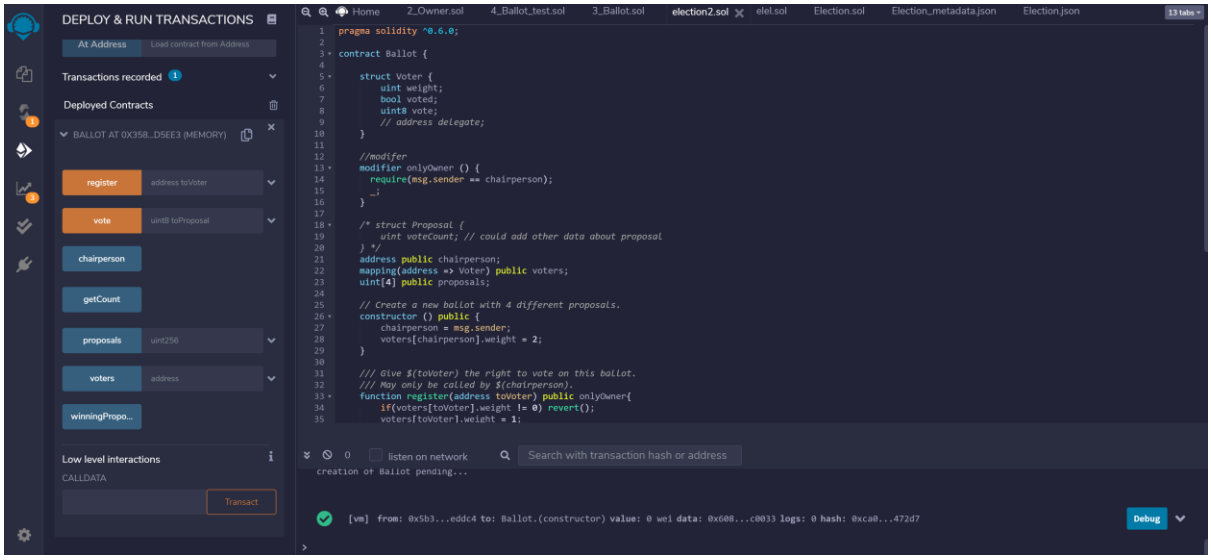
Metamask

Η εφαρμογή Metamask είναι η κύρια εφαρμογή, μέσω της οποίας οι χρήστες διαχειρίζονται τους λογαριασμούς τους στο Ethereum Blockchain, δηλαδή είναι μια frontend εφαρμογή. Δίνει δυνατότητα επιλογής και τοπικού δικτύου, οπότε ο προγραμματιστής μπορεί να εξετάζει πώς το site του επικοινωνεί με τον χρήστη, ώστε να έχει σφαιρική άποψη για την αποκεντρωμένη εφαρμογή του.

## 7.3 Tutorial Εφαρμογής

### 7.3.1 Εγκατάσταση Πακέτων και Frameworks

Αρχικά θα χρειαστούμε κάποιο IDE όπως το Visual ή το Sublime,στα οποία μπορεί κανείς να γράψει σε γλώσσα Solidity και να κατεβάσει χρήσιμα extensions όπως πακέτα μεταγλώττισης, πακέτα debug και πακέτα mark-up/highlight για κάθε γλώσσα προγραμματισμού. Προτείνεται, τουλάχιστον στο αρχικό στάδιο η ανάπτυξη smart contracts στην open-source διαδικτυακή πλατφόρμα Remix, όπου μπορεί κανείς να αναπτύξει scripts και να χρησιμοποιήσει κάποιον από τους προσφερόμενους virtual compilers. Παρέχεται επίσης κάποιο στοιχειώδες front-end περιβάλλον για την αλληλεπίδραση με τις συναρτήσεις του κώδικα, όπως φαίνεται παρακάτω :




Σχήμα 16: Η πλατφόρμα Remix

### *7.3.1.1 Εγκατάσταση npm και node.js*

Αρχικά θα πρέπει να ελέγψουμε αν έχουμε εγκατεστημένα τα node package management και την γλώσσα node.js. Αυτό μπορούμε να το δούμε ανοίγοντας ένα τερματικό και πληκτρολογώντας npm –v και node—v. Σε περίπτωση που είναι εγκατεστημένα , το τερματικό θα μας επιστρέψει τις εκδόσεις που ειναι εγκατεστημένες στον υπολογιστή μας.

Αλλιώς για να τα εγκαταστήσουμε θα πρέπει να ανοίξουμε ένα τερματικό PowerShell και να πληκτρολογήσουμε :

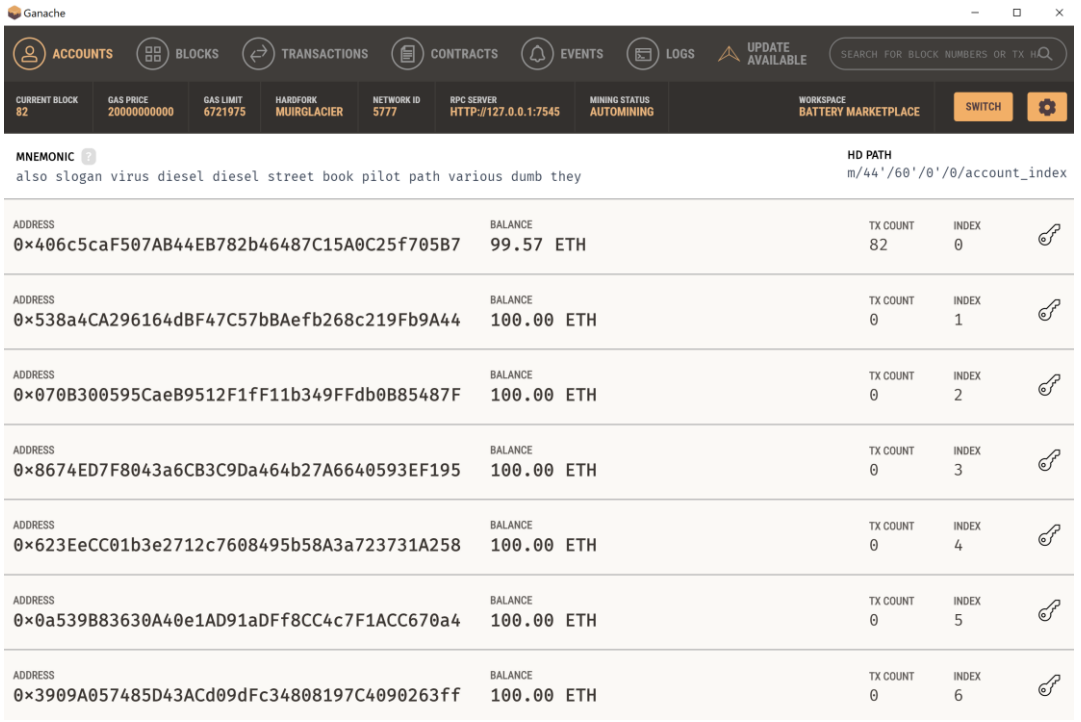
npm install npm και

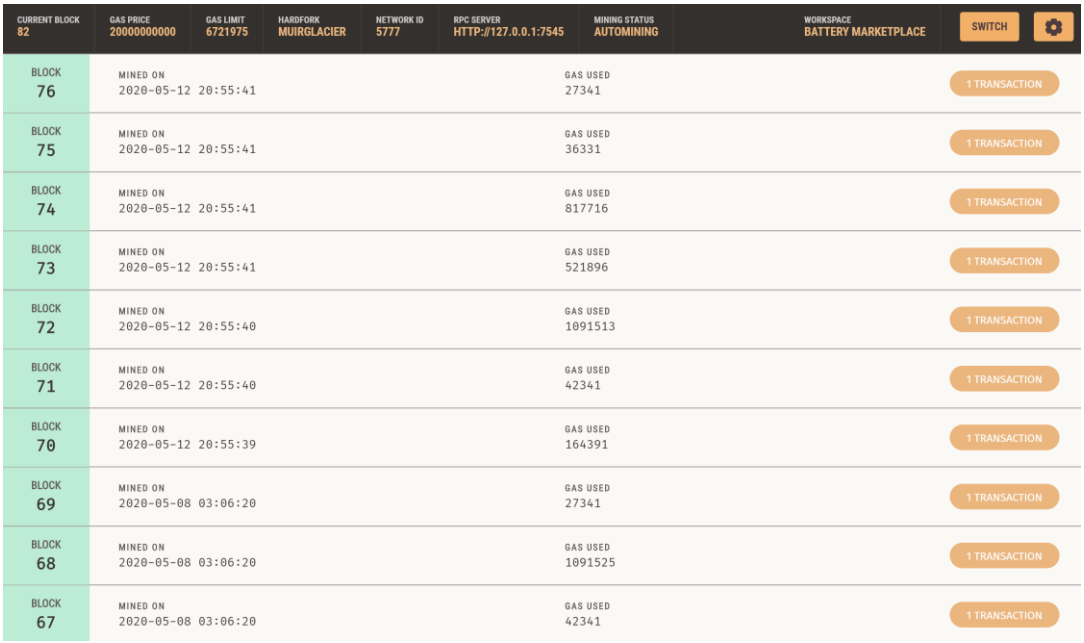
npm install- g @0.x.y (global install of node's version x.y)

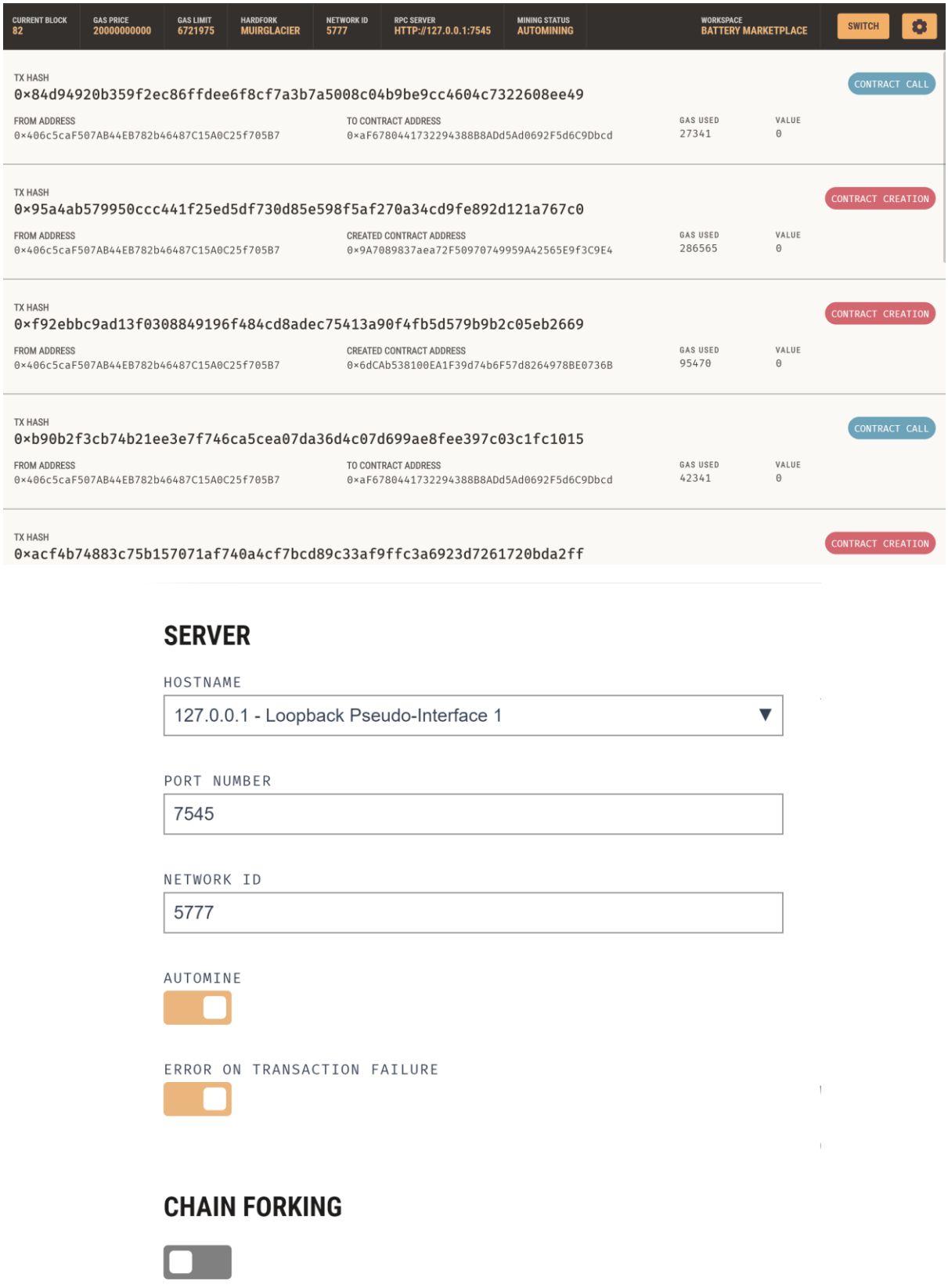
Εναλλακτικά μπορούμε να εγκαταστήσουμε την node από την ιστοσελίδα nodejs.org, και η εγκατάσταση της θα περιλαμβάνει και όποια dependencies λείπουν, όπως το πακέτο npm .

### *7.3.1.2 Εγκατάσταση Ganache*

Μπορούμε να κατεβάσουμε το Ganache είτε από το τερματικό (npm install ganache-cli) ή από την επίσημη ιστοσελίδα. Ο Ganache μας επιτρέπει να στήσουμε ένα προσωπικό δίκτυο Ethereum blockchain και μας παρέχει και κάποιους λογαριασμούς για να μπορούμε να κάνουμε δοκιμές. Όταν ολοκληρωθεί η εγκατάσταση και ανοίξει ένα νέο 'workplace' βλέπουμε τα βασικά στοιχεία του personal blockchain, όπως παρουσιάζεται παρακάτω. Διαθέτει πολλές επιλογές παραμετροποίησης και μπορεί να συνδεθεί με συγκεκριμένα project ώστε να μπορεί να παρέχει πληροφόρηση για blocks,transactions,events,contracts που έχουν γίνει deployed.


Ganache
ACCOUNTS
BLOCKS
TRANSACTIONS
CONTRACTS
EVENTS
LOGS
UPDATE AVAILABLE
SEARCH FOR BLOCK NUMBERS OR TX H
CURRENT BLOCK 82
GAS PRICE 20000000000
GAS LIMIT 6721975
HARDFORK MUIRGLACIER
NETWORK ID 5777
RPC SERVER HTTP://127.0.0.1:7545
MINING STATUS AUTOMINING
WORKSPACE BATTERY MARKETPLACE
SWITCH
MNEMONIC
also slogan virus diesel diesel street book pilot path various dumb they
HD PATH
m/44'/60'/0'/0/account_index
ADDRESS 0x406c5caF507AB44EB782b46487C15A0C25f705B7 BALANCE 99.57 ETH TX COUNT 82 INDEX 0
ADDRESS 0x538a4CA296164dBF47C57bBAefb268c219Fb9A44 BALANCE 100.00 ETH TX COUNT 0 INDEX 1
ADDRESS 0x070B300595CaeB9512F1fF11b349FFdb0B85487F BALANCE 100.00 ETH TX COUNT 0 INDEX 2
ADDRESS 0x8674ED7F8043a6CB3C9Da464b27A6640593EF195 BALANCE 100.00 ETH TX COUNT 0 INDEX 3
ADDRESS 0x623EeCC01b3e2712c7608495b58A3a723731A258 BALANCE 100.00 ETH TX COUNT 0 INDEX 4
ADDRESS 0x0a539B83630A40e1AD91aDFf8CC4c7F1ACC670a4 BALANCE 100.00 ETH TX COUNT 0 INDEX 5
ADDRESS 0x3909A057485D43ACd09dFc34808197C4090263ff BALANCE 100.00 ETH TX COUNT 0 INDEX 6

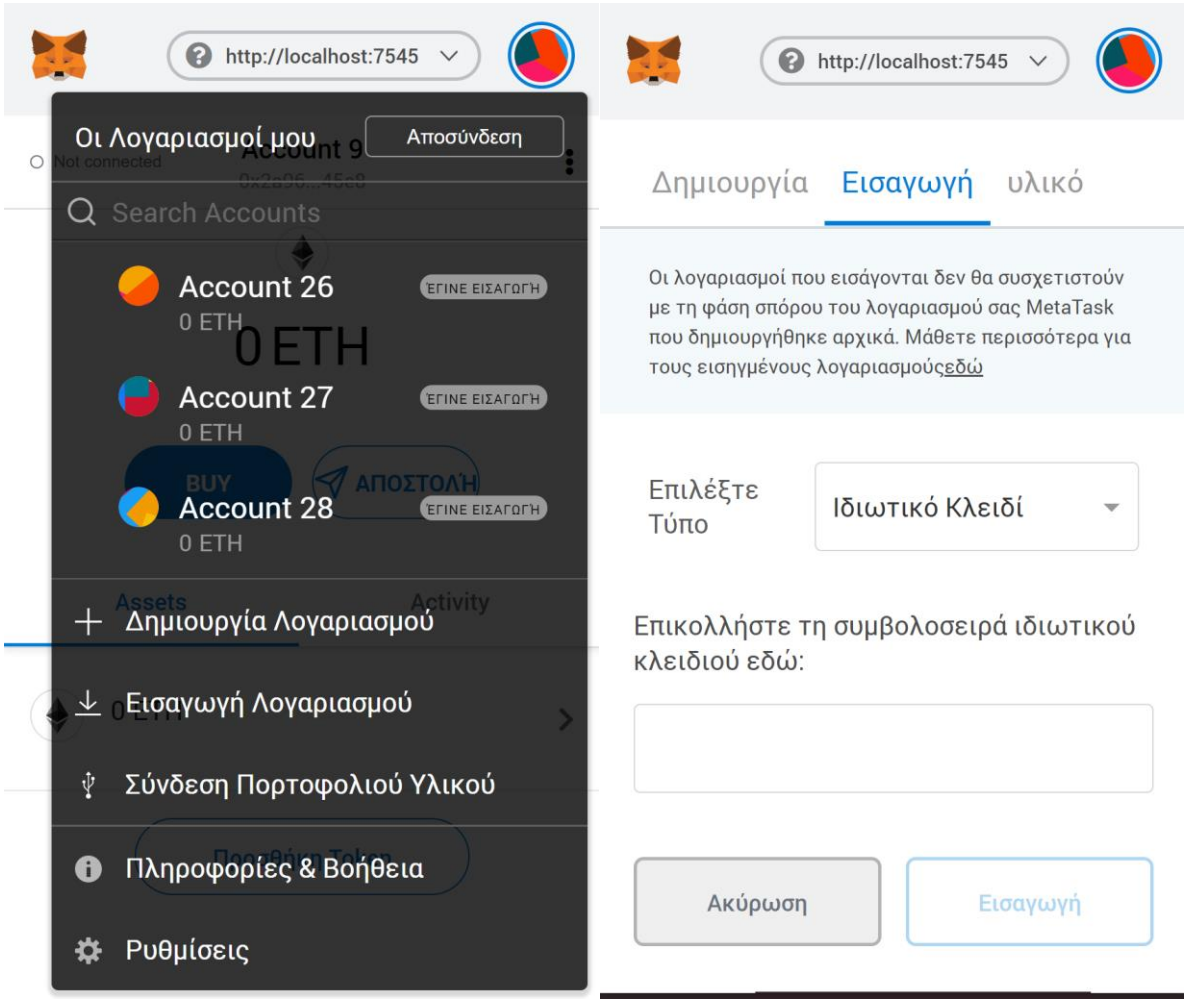

CURRENT BLOCK 82
GAS PRICE 20000000000
GAS LIMIT 6721975
HARDFORK MUIRGLACIER
NETWORK ID 5777
RPC SERVER HTTP://127.0.0.1:7545
MINING STATUS AUTOMINING
WORKSPACE BATTERY MARKETPLACE
SWITCH
BLOCK 76 MINED ON 2020-05-12 20:55:41 GAS USED 27341 1 TRANSACTION
BLOCK 75 MINED ON 2020-05-12 20:55:41 GAS USED 36331 1 TRANSACTION
BLOCK 74 MINED ON 2020-05-12 20:55:41 GAS USED 817716 1 TRANSACTION
BLOCK 73 MINED ON 2020-05-12 20:55:41 GAS USED 521896 1 TRANSACTION
BLOCK 72 MINED ON 2020-05-12 20:55:40 GAS USED 1091513 1 TRANSACTION
BLOCK 71 MINED ON 2020-05-12 20:55:40 GAS USED 42341 1 TRANSACTION
BLOCK 70 MINED ON 2020-05-12 20:55:39 GAS USED 164391 1 TRANSACTION
BLOCK 69 MINED ON 2020-05-08 03:06:20 GAS USED 27341 1 TRANSACTION
BLOCK 68 MINED ON 2020-05-08 03:06:20 GAS USED 1091525 1 TRANSACTION
BLOCK 67 MINED ON 2020-05-08 03:06:20 GAS USED 42341 1 TRANSACTION




Σχήμα 17: Οι Λειτουργίες του Ganache

### *7.3.1.3 Εγκατάσταση Metamask plugin*

Μπορούμε να το εγκαταστήσουμε από το επίσημο site της Metamask. Ουσιαστικά είναι ένα πορτοφόλι με πολλές δυνατότητες και επιλογές για λόγους Development, όπως η σύνδεση RPC σε localhost δίκτυο. Μπορεί κανείς να εισάγει το ιδιωτικό του κλειδί και ουσιαστικά να συνδεθεί με κάποιον λογαριασμό, Εισάγοντας ιδιωτικά κλειδιά λογαριασμών του Ganache θα μπορέσουμε να αναπαραστήσουμε τους διάφορους ρόλους στην εφαρμογή μας.

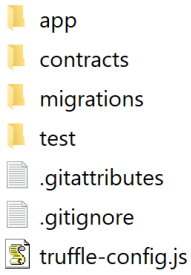



Σχήμα 18: Το πορτοφόλι Metamask

### *7.3.1.4 Εγκατάσταση σουίτας Truffle*

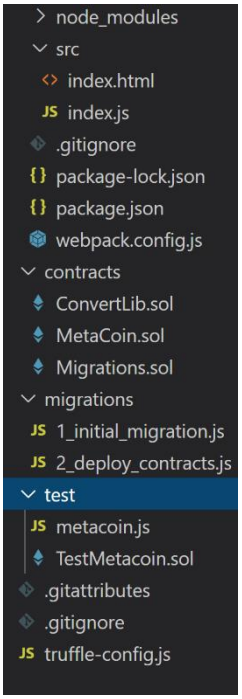
Για την εγκατάσταση του Truffle,δημιουργούμε ένα νέο φάκλεο και μέσα σε αυτόν εγκαθιστούμε το truffle μέσω της εντολής npm install truffle . Στην παραπάνω εντολή μπορούμε να συμπληρώσουμε @x.y για να επιλέξουμε να κατεβάσουμε κάποια συγκεκριμένη έκδοση π.χ. 5.1. Καλό θα ήταν, πριν ξεκινήσουμε την εγκατάσταση να ελέγξουμε την συμβατότητα των εκδόσεων της node με την σουίτα truffle από το επίσημο site της truffle. Στην ιστοσελίδα https://www.trufflesuite.com/, υπάρχει το πλήρες documentation της πλατφόρμας για την χρήση της πλατφόρμας. Η πλατφόρμα παρέχει κάποια 'boxes' που παρέχουν κάποια βασικά πακέτα εργαλείων και βιβλιοθηκών για την ανάπτυξη αποκεντρωμένων εφαρογών. Τα πιο δημοφιλή και αναπτυσσόμενα πακέτα είναι το react-box και το webpack. Στην περίπτωση μας θα χρησιμοποιήσουμε το webpack, το οποίο θα εγκαταστήσουμε με την εντολή *truffle unbox web-pack*.

Μόλις ολοκληρωθεί το un-boxing του πακέτου, αν περιηγηθούμε στον φάκελο θα δούμε ότι έχει εγκατασταθεί το εξής directory:




Πηγαίνουμε στο Visual και βλέπουμε ότι υπάρχει

- ο φάκελος contracts με τρία demo contracts,
- ο φάκελος migrations που περιλαμβάνει δύο scripts που περιγράφουν τον τρόπο που θα γίνουν deploy τα contracts,
- ο φάκελος test με δυο script ελέγχου.
- ο φάκελος src που περιλαμβάνει όλο το server-side κομμάτι της εφαρμογής αποτελούμενο κατά βάση από τα αρχεία index.html και index.js
- ο φάκελος node modules, που περιλαμβάνει όλες τις βιβλιοθήκες που απαιτούνται για να επιτραπεί στην πλατφόρμα να στήσει ένα τοπικό περιβάλλον blockchain και να επικοινωνεί με αυτό μέσω μιας διαδικτυακής εφαρμογής
- το αρχείο truffle-config.js που περιλαμβάνει πληροφοριες δικτύου για το hosting της εφαρμογής.




*Κάνουμε τις απαραίτητες ρυθμίσεις δικτύου στο αρχείο* truffle-config.js και στο ganache όσον αφορά την διεύθυνση του hosting και την πόρτα (απο προεπιλογή localhos:8080 και πόρτα 8545) και συνδεόμαστε με κάποιο λογαριασμό στο metamask *Κάνουμε compile και migrate την demo αυτή την εφαρμογή.*

Σχήμα 19: directory sample εφαρμογής

```
Compiling your contracts...
===========================
> Compiling .\contracts\ConvertLib.sol
> Artifacts written to C:\Users\orest\demo\build\contracts
> Compiled successfully using:
   - solc: 0.5.12+commit.7709ece9.Emscripten.clang



Starting migrations...
======================
> Network name:    'ganache'
> Network id:      5777
> Block gas limit: 0x6691b7


1_initial_migration.js
======================

   Deploying 'Migrations'
   ----------------------
   > transaction hash:    0xacf4b74883c75b157071af740a4cf7bcd89c33af9ffc3a6923d7261720bda2ff
   > Blocks: 0            Seconds: 0
   > contract address:    0xaF6780441732294388B8ADd5Ad0692F5d6C9Dbcd
   > block number:        78
   > block timestamp:     1602610031
   > account:             0x406c5caF507AB44EB782b46487C15A0C25f705B7
   > balance:             99.57497022
   > gas used:            164175
   > gas price:           20 gwei
   > value sent:          0 ETH
   > total cost:          0.0032835 ETH


   > Saving migration to chain.
   > Saving artifacts
   -------------------------------------
   > Total cost:           0.0032835 ETH
```

```
2_deploy_contracts.js
=====================

   Deploying 'ConvertLib'
   ----------------------
   > transaction hash:    0xf92ebbc9ad13f0308849196f484cd8adec75413a90f4fb5d579b9b2c05eb2669
   > Blocks: 0            Seconds: 0
   > contract address:    0x6dCAb53810OEA1F39d74b6F57d8264978BE0736B
   > block number:        80
   > block timestamp:     1602610031
   > account:             0x406c5caF507AB44EB782b46487C15A0C25f705B7
   > balance:             99.572214
   > gas used:            95470
   > gas price:           20 gwei
   > value sent:          0 ETH
   > total cost:          0.0019094 ETH


   Linking
   -------
   * Contract: MetaCoin <--> Library: ConvertLib (at address: 0x6dCAb53810OEA1F39d74b6F57d8264978BE0736B)

   Deploying 'MetaCoin'
   --------------------
   > transaction hash:    0x95a4ab579950ccc441f25ed5df730d85e598f5af270a34cd9fe892d121a767c0
   > Blocks: 0            Seconds: 0
   > contract address:    0x9A7089837aea72F50970749959A42565E9f3C9E4
   > block number:        81
   > block timestamp:     1602610031
   > account:             0x406c5caF507AB44EB782b46487C15A0C25f705B7
   > balance:             99.5664827
   > gas used:            286565
   > gas price:           20 gwei
   > value sent:          0 ETH
   > total cost:          0.0057313 ETH


   > Saving migration to chain.
   > Saving artifacts
   -------------------------------------
   > Total cost:           0.0076407 ETH


Summary
=======
> Total deployments:   3
> Final cost:          0.0109242 ETH
```

Σχήμα 20: Το deployment των smart contracts

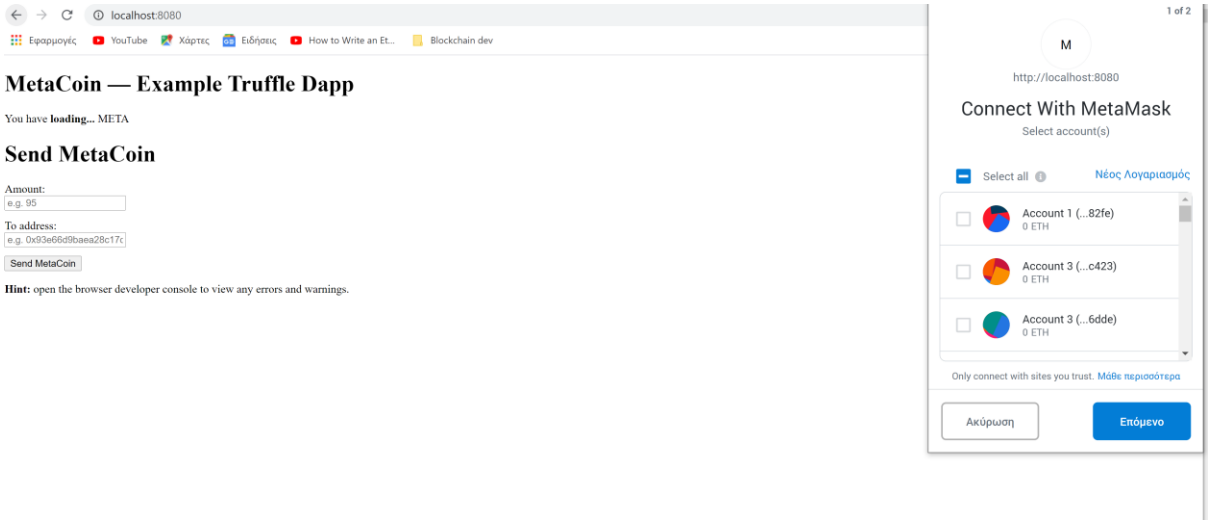
*Στη συνέχεια μπαίνουμε στο τεστ περιβάλλον της truflle πληκτρολογόντας truffle development όπου μπορούμε να αλληλοεπιδρούμε με τα deployed συμβόλαια μας και γενικότερα με τα δεδομένα της αλυσίδας.* Αμέσως εμφανίζονται 10 λογαριασμοί με τα αντίστοιχα κλειδιά τους. Μπορούμε να ελέγξουμε ότι αυτοί οι λογαριασμοί αντιπροσωπεύονται από τα αντίστοιχα δημόσια κλειδιά τους που εμφανίζονται στο ganache, είναι και αυτοί που είναι συνδεδεμένοι στο δίκτυο.

```
truffle(develop)> accounts[0].balance
undefined
truffle(develop)> accounts[0]
'0x406c5caF507AB44EB782b46487C15A0C25f705B7'
truffle(develop)> web3.eth.getAccounts().then( function(s){FirstAccount=s[0]; return FirstAccount})
'0x406c5caF507AB44EB782b46487C15A0C25f705B7'
truffle(develop)>
```

Σχήμα 21: Κονσόλα Truffle Development

Παρουσιάζονται τα στοιχεία των 3 deployments καθώς και τα στοιχεία του δικτύου. Πλοηγούμαστε στον φάκελο app και τρέχουμε την εντολή npm run dev.

Κατόπιν ανοίγουμε έναν browser με συνδεδεμένο πορτοφόλι metamask και είμαστε σε θέση πλέον να αλληλεπιδράσουμε με την demo αυτή εφαρμογή:

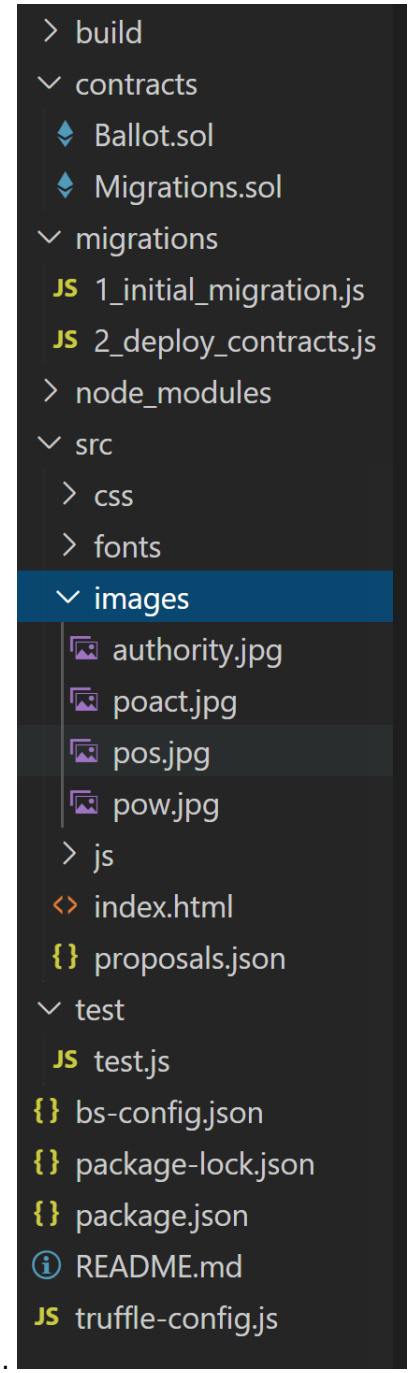



Σχήμα 22 : Sample Εφαρμογή

Βασιζόμενοι στο pre-installed αυτό πακέτο και διατηρώντας τον φάκελο node modules, που περιλαμβάνει όλες τις βιβλιοθήκες, μπορούμε να γράψουμε τη δική μας αποκεντρωμένη εφαρμογή με περιεχόμενα:

- το συμβόλαιο ballot.sol
- τα migrations scripts που περιγράφουν τον τρόπο που θα γίνουν deploy ta contracts,
- τα test scripts
- το server-side κομμάτι της εφαρμογής αποτελούμενο κατά βάση από τα αρχεία index.html και index.js
- το αρχείο truffle-config.js που περιλαμβάνει πληροφορίες δικτύου για το hosting της εφαρμογής.

Χρησιμοποιούμε τον κώδικα που αναπτύξαμε και παρουσιάζεται στην επόμενη ενότητα για όλα τα μέρη της εφαρμογής όπως περιγράφηκε προηγουμένως. Έτσι προκύπτει το εξής directory:

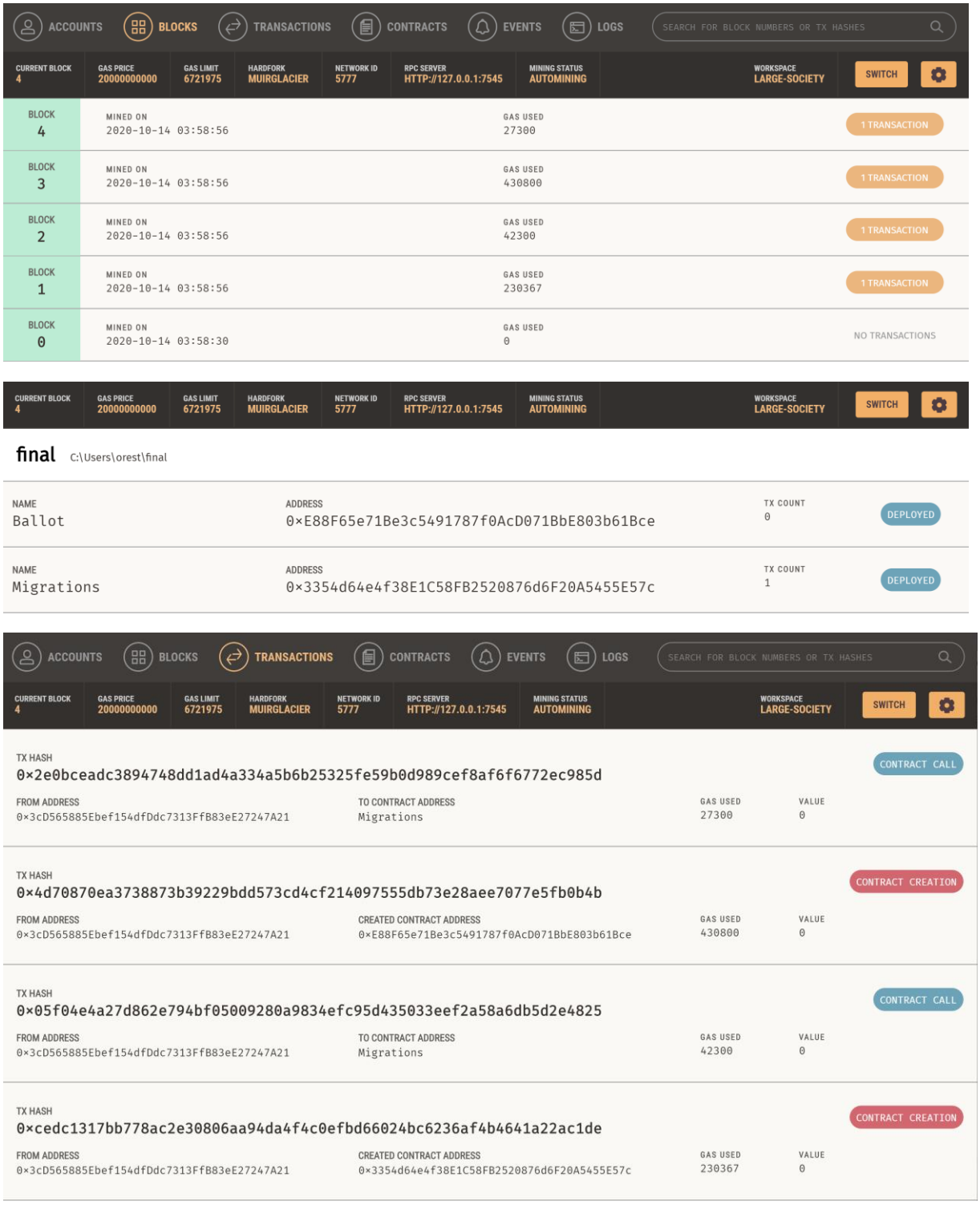



Σχήμα 23: Directory εφαρμογής

Κάνουμε compile και migrate τα smart contracts. Όλα τα στοιχεία των transactions παρουσιάζονται παρακάτω και μπορούν να ιχνηλατηθούν στο Ganache (παρόμοια λειτουργία με το Etherscan)

```
Compiling your contracts...
===========================
> Everything is up to date, there is nothing to compile.


Starting migrations...
======================
> Network name:    'development'
> Network id:      5777
> Block gas limit: 0x6691b7


1_initial_migration.js
======================

   Replacing 'Migrations'
   ----------------------
   > transaction hash:    0x456c936ce50cc9357b096b52863be9b3fe3ed30a4c2ab33761f834f58b8fb7fc
   > Blocks: 0            Seconds: 0
   > contract address:    0xEa8C09DFC02F22fA8904e812564cb322b38e1660
   > block number:        1
   > block timestamp:     1602089314
   > account:             0x605f22899BEdf068C5e60b95D9F7C616AF0deb0A
   > balance:             99.99539266
   > gas used:            230367
   > gas price:           20 gwei
   > value sent:          0 ETH
   > total cost:          0.00460734 ETH


   > Saving migration to chain.
   > Saving artifacts
   -------------------------------------
   > Total cost:          0.00460734 ETH


2_deploy_contracts.js
=====================

   Replacing 'Ballot'
   ------------------
   > transaction hash:    0x4ee17fe756b3db85b3ebdb9f32599faaddf142fc46b70027c8e7ea91e5e18698
   > Blocks: 0            Seconds: 0
   > contract address:    0x27b6ea0866c568e5256e455CD8d80123e3ED8848
   > block number:        3
   > block timestamp:     1602089315
   > account:             0x605f22899BEdf068C5e60b95D9F7C616AF0deb0A
   > balance:             99.9859309
   > gas used:            430788
   > gas price:           20 gwei
   > value sent:          0 ETH
   > total cost:          0.00861576 ETH
```

Σχήμα 24: Compile και deploy των smart contracts

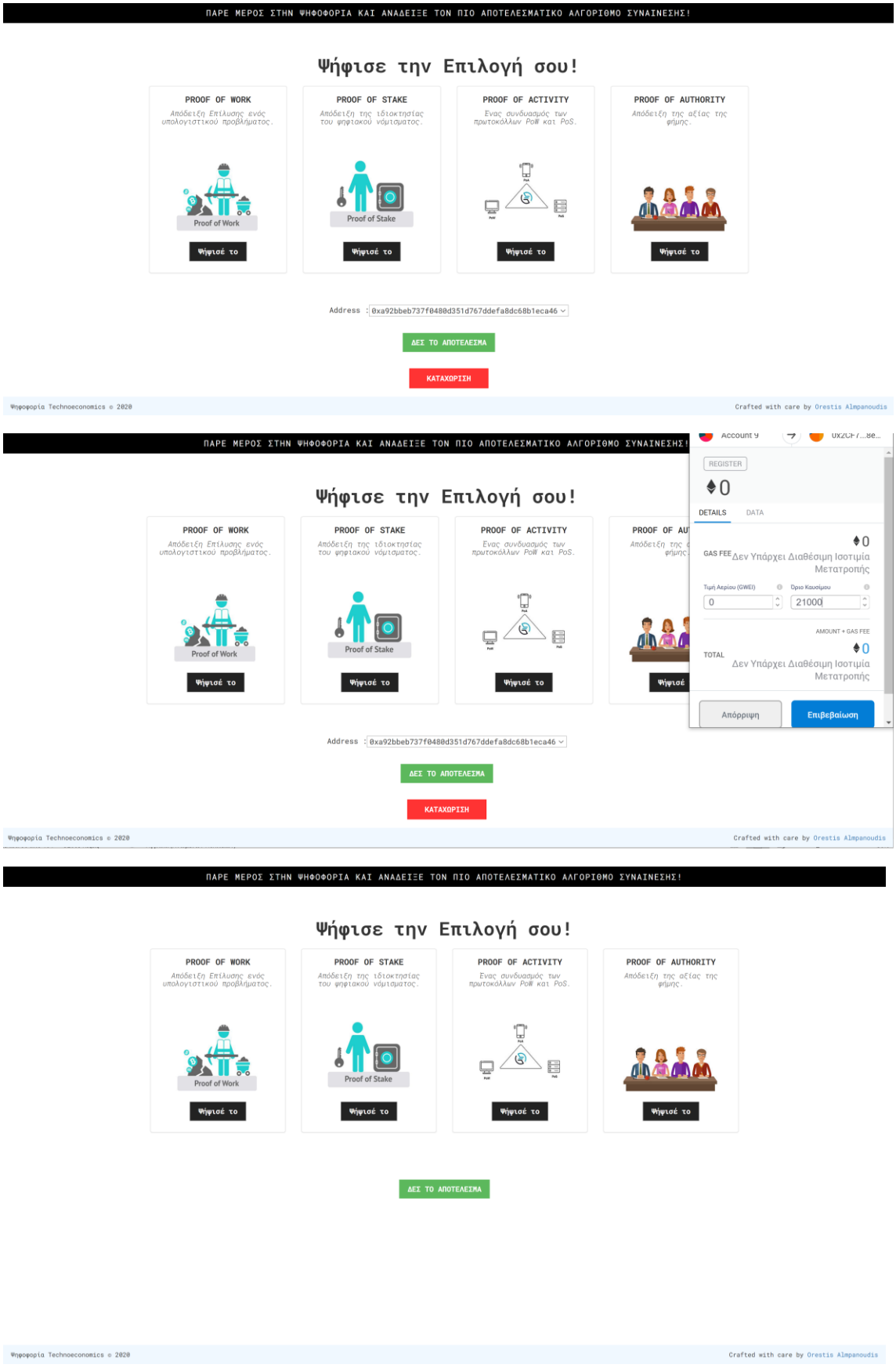



Σχήμα 25: Ιχνηλάτηση Συναλλαγών στο Ganache

Στη συνέχεια τρέχουμε την εντολή npm run dev και βλέπουμε τον συγχρονισμό του sever που κάνει get τα αντίστοιχα αρχεία και artifacts που χρειάζεται για να τρέξει η εφαρμογή.

```
C:\Users\orest\final>npm run dev

> Ballot@1.0.0 dev C:\Users\orest\final
> lite-server

** browser-sync config **
{
  injectChanges: false,
  files: [ './**/*.{html,htm,css,js}' ],
  watchOptions: { ignored: 'node_modules' },
  server: {
    baseDir: [ './src', './build/contracts' ],
    middleware: [ [Function], [Function] ]
  }
}
[Browsersync] Access URLs:
 ------------------------------------
       Local: http://localhost:3000
    External: http://192.168.1.4:3000
 ------------------------------------
          UI: http://localhost:3001
 UI External: http://localhost:3001
 ------------------------------------
[Browsersync] Serving files from: ./src
[Browsersync] Serving files from: ./build/contracts
[Browsersync] Watching files...
20.10.07 19:53:04 304 GET /index.html
20.10.07 19:53:04 304 GET /css/bootstrap.min.css
20.10.07 19:53:04 304 GET /css/style.css
20.10.07 19:53:04 304 GET /js/web3.min.js
20.10.07 19:53:04 304 GET /js/truffle-contract.js
20.10.07 19:53:04 304 GET /js/app.js
20.10.07 19:53:04 404 GET /images/apple.jpg
20.10.07 19:53:04 304 GET /proposals.json
20.10.07 19:53:04 304 GET /images/pow.jpg
20.10.07 19:53:04 304 GET /images/pos.jpg
20.10.07 19:53:04 304 GET /images/authority.jpg
20.10.07 19:53:04 304 GET /images/poact.jpg
20.10.07 19:53:04 200 GET /Ballot.json
```

Σχήμα 26: Άνοιγμα Διαδικτυακής Εφαρμογής




Σχήμα 27: Είσοδος Διοργανωτή, Καταχώρηση ενός Ψηφοφόρου, Είσοδος ενός Ψηφοφόρου

## 7.4 Κώδικας Testing

Όπως ειπώθηκε πορηγουμένως, το περιβάλλον Truffle δίνει τη δυνατότητα στον Developer να αναπτύξει δοκιμαστικά script για να διασφαλιστεί η ομαλή και ασφαλης λειτουργία των smart contracts. Για την παρούσα υλοποίηση θα αναπτύξουμε 10 διαφορετικές περιπτώσεις ελέγχου (6 θετικές και 4 αρνητικές), οι οποίες παρουσιάζονται παρακάτω :

1. Έλεγχος ότι το smart contract έγινε deployed και μάλιστα από την διεύθυνση 0 (chairperson)

```
let Ballot = artifacts.require("./Ballot.sol");

let ballotInstance;

let _voting = {
  "winner": 0,
  "one": 1,
  "two": 2,
  "three": 3
}

contract('Ballot Contract', function (accounts) {
  //accounts[0] is the default account
  //Test case 1
  Run Test | Debug Test
  it("Contract deployment", function() {
    return Ballot.deployed().then(function (instance) {
      ballotInstance = instance;
      assert(ballotInstance !== undefined, 'Ballot contract should be defined');
    });
  });
```

2. Έλεγχος συνάρτησης Registration. Χρησιμοποιούμε την αποδειξη συναλλαγής για τον έλεγχο αυτό. Ουσιαστικά ελέγχουμε αν η συναλλαγή-κλήση της συνάρτησης Register ήταν επιτυχής, καθώς η απόδειξη κάθε επιτυχημένης συναλλαγής έχει στάτους που ισούται με την τιμή ‘0x01’.

```
//Test case 2
Run Test | Debug Test
it("Valid user registration", function() {
  return ballotInstance.register(accounts[1], { from: accounts[0]}).then(function (result) {
    assert.equal('0x01', result.receipt.status, 'Registration is valid');
    return ballotInstance.register(accounts[2], { from: accounts[0]});
  }).then(function (result) {
    assert.equal('0x01', result.receipt.status, 'Registration is valid');
    return ballotInstance.register(accounts[3], { from: accounts[0]});
  }).then(function(result) {
    assert.equal('0x01', result.receipt.status, 'Registration is valid');
    return ballotInstance.register(accounts[4], { from: accounts[0]});
  }).then(function(result) {
    assert.equal('0x01', result.receipt.status, 'Registration is valid');
    return ballotInstance.register(accounts[5], { from: accounts[0]});
  }).then(function(result) {
    assert.equal('0x01', result.receipt.status, 'Registration is valid');
  });
});
```

3.Έλεγχος ότι καταχωρήθηκε μια έγκυρη ψήφος. Παρομοίως, χρησιμοποιούμε την απόδειξη συναλλαγής για τον έλεγχο αυτό.

```
//Test case 3
Run Test | Debug Test
it("Valid voting", function() {
  return ballotInstance.vote(_voting.winner, {from: accounts[0]}).then(function (result) {
    assert.equal('0x01', result.receipt.status, 'Voting is done');
    return ballotInstance.vote(_voting.one, {from: accounts[1]});
  }).then(function (result) {
    assert.equal('0x01', result.receipt.status, 'Voting is done');
    return ballotInstance.vote(_voting.two, {from: accounts[2]});
  }).then(function (result) {
    assert.equal('0x01', result.receipt.status, 'Voting is done');
    return ballotInstance.vote(_voting.three, {from: accounts[3]});
  }).then(function (result) {
    assert.equal('0x01', result.receipt.status, 'Voting is done');
    return ballotInstance.vote(_voting.winner, {from: accounts[4]});
  }).then(function (result) {
    assert.equal('0x01', result.receipt.status, 'Voting is done');
  });
});
```

4.Έλεγχος Λειτουργίας Ανάδειξης Νικητή Winning-Proposal

```
//Test case 4
Run Test | Debug Test
it("Validate winner", function () {
  return ballotInstance.winningProposal.call().then(function (result) {
    assert.equal(_voting.winner, result.toNumber(), 'Winner is validated with the expected winner');
  });
});
```

5. Έλεγχος Λειτουργίας Καταμέτρησης Ψήφων get.Count

```
//Test case 5
Run Test | Debug Test
it("Valid individual votes", function () {
  return ballotInstance.getCount.call().then(function (result) {
    assert.equal(3, result[0].toNumber(), 'Individual vote is validated with expected vote count');
    assert.equal(1, result[1].toNumber(), 'Individual vote is validated with expected vote count');
    assert.equal(1, result[2].toNumber(), 'Individual vote is validated with expected vote count');
    assert.equal(1, result[3].toNumber(), 'Individual vote is validated with expected vote count');
  });
});
```

6. Έλεγχος ότι η κλήση της συνάρτησης Register στο συμβόλαιο μπορεί να γίνει από τον διοργανωτή αποκλειστικά. Στον πρώτο αυτό αρνητικό έλεγχο, ελέγχουμε το ενδεχόμενο να μπορεί κάποιος άλλος λογαριασμός (ο 2$^{ος}$ συγκεκριμένα) να χορηγήσει δικαίωμα ψήφου σε κάποιον ψηφοφόρο. Όταν η κλήση της συνάρτησης γίνει από εσφαλμένο λογαριασμό, ο έλεγχος επιβεβαιώνεται.

```
//Test case 6
  Run Test | Debug Test
it("Should NOT accept unauthorized registration", function () {
return ballotInstance.register(accounts[6], { from: accounts[1]})
  .then(function (result) {
      throw("Condition not implemented in Smart Contract");
  }).catch(function (e) {
    if(e === "Condition not implemented in Smart Contract") {
      assert(false);
    } else {
      assert(true);
    }
  })
});
```

7. Έλεγχος ότι η κλήση της συνάρτησης Register στο συμβόλαιο μπορεί να γίνει μία φορά αποκλειστικά για κάθε ψηφοφόρο. Στον δεύτερο αυτό αρνητικό έλεγχο, ελέγχουμε το ενδεχόμενο να μπορεί να χορηγηθεί δικαίωμα ψήφου περισσότερες από μία φορές σε κάποιον ψηφοφόρο. Όταν η κλήση της συνάρτησης γίνεται για δεύτερη φορά, ο έλεγχος επιβεβαιώνεται.

```
//Test case 7
  Run Test | Debug Test
it("Should NOT register already registered user", function () {
return ballotInstance.register(accounts[1], { from: accounts[0]})
  .then(function (result) {
    throw("Condition not implemented in Smart Contract");
}).catch(function (e) {
  if(e === "Condition not implemented in Smart Contract") {
    assert(false);
  } else {
    assert(true);
  }
})
});
```

8. Έλεγχος ότι μόνο οι registered users μπορούν να να ψηφίσουν

```
//Test case 8
Run Test | Debug Test
it("Should NOT accept unregistered user vote", function () {
return ballotInstance.vote(1, {from: accounts[7]})
  .then(function (result) {
      throw("Condition not implemented in Smart Contract");
  }).catch(function (e) {
    if(e === "Condition not implemented in Smart Contract") {
      assert(false);
    } else {
      assert(true);
    }
  })
});
```

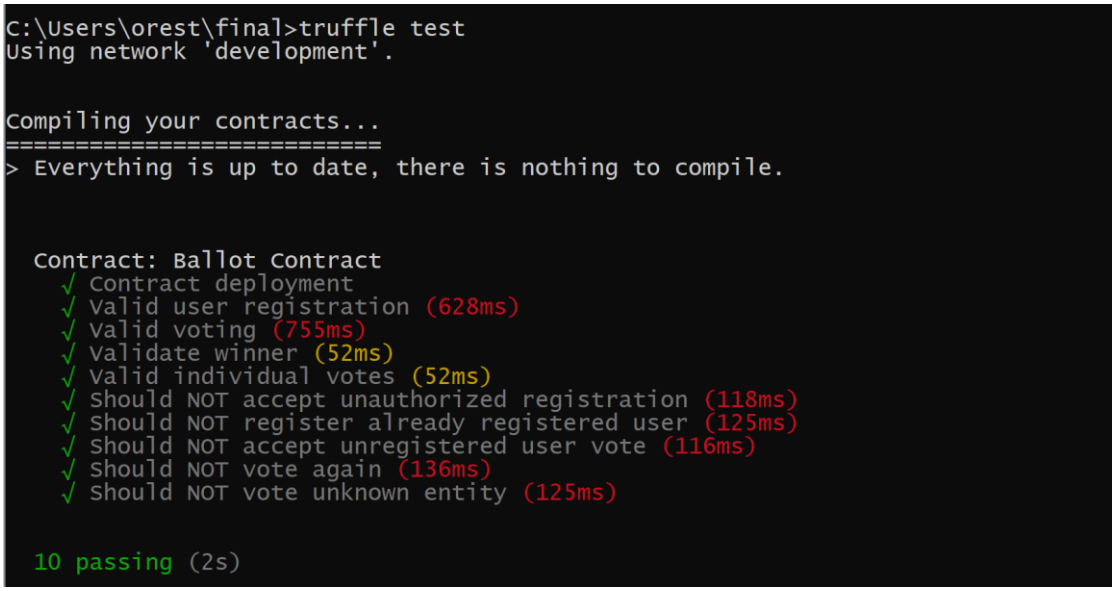
9. Έλεγχος ότι η κλήση της συνάρτησης Vote στο συμβόλαιο μπορεί να γίνει μία φορά αποκλειστικά για κάθε ψηφοφόρο. Στον τέταρτο αυτό αρνητικό έλεγχο, ελέγχουμε το ενδεχόμενο να μπορεί να κατατεθεί μία ψήφος περισσότερες από μία φορές σε κάποιον ψηφοφόρο. Όταν η κλήση της συνάρτησης γίνεται για δεύτερη φορά, ο έλεγχος επιβεβαιώνεται (voted='true').

```
//Test case 9
Run Test | Debug Test
it("Should NOT vote again", function () {
return ballotInstance.vote(1, {from: accounts[1]})
  .then(function (result) {
      throw("Condition not implemented in Smart Contract");
  }).catch(function (e) {
    if(e === "Condition not implemented in Smart Contract") {
      assert(false);
    } else {
      assert(true);
    }
  })
});
```

10. Στον τελευταίο αρνητικό έλεγχο, ελέγχουμε αν δίνεται το δικαίωμα σε κάποιον ψηφοφόρο να ψηφίσει μία επιλογή που δν υπάρχει. Ο έλεγχος επιβεβαιώνεται όταν κάποιος ψηφοφόρος επιλέξει να ψηφίσει κάποιο Proposal που δεν υφίσταται.

```
//Test case 10
Run Test | Debug Test
it("Should NOT vote unknown entity", function () {
  return ballotInstance.vote(4, {from: accounts[5]})
  .then(function (result) {
      throw("Condition not implemented in Smart Contract");
  }).catch(function (e) {
    if(e === "Condition not implemented in Smart Contract") {
      assert(false);
    } else {
      assert(true);
    }
  })
});
```

Μέσω της εντολής truffle test, κάνουμε compile τα smart contracts, και μπορούμε να εκτελέσουμε ελέγχους για τον κώδικα του smart contract με βάση τα scripts ελέγχου που περιέχονται στο test.js. Το αποτέλεσμα αυτής της διαδικασίας, θα πρέπει να προκύψει στο τερματικό με την ένδειξη passing ή not passing, όπως παρουσιάζεται παρακάτω:


C:\Users\orest\final>truffle test
Using network 'development'.
Compiling your contracts...
> Everything is up to date, there is nothing to compile.
Contract: Ballot Contract
√ Contract deployment
√ Valid user registration (628ms)
√ Valid voting (755ms)
√ Validate winner (52ms)
√ Valid individual votes (52ms)
√ Should NOT accept unauthorized registration (118ms)
√ Should NOT register already registered user (125ms)
√ Should NOT accept unregistered user vote (116ms)
√ Should NOT vote again (136ms)
√ Should NOT vote unknown entity (125ms)
10 passing (2s)

## 7.5 Κώδικας Server-side Application

Τα αιτήματα (requests) ή οι κλήσεις (calls) πραγματοποιούνται στο αντικείμενο web3, μεταδίδονται ως αγωγός (pipeline) JSON ή RPC μεταξύ του web-App και του πελάτη geth.

Λόγω της ασύγχρονης επικοινωνία, για την επικοινωνία με το blockchain χρησιμοποιούνται εντολές με την μορφή υπόσχεσης (promise) και λαμβάνονται στιγμιότυπα (instances). Παράδειγμα μιας τέτοιας εντολής ειναι στη συνάρτηση register, όπου αν ισχύει η υπόσχεη (app.contracts.vote.deployed), λαμβάνεται το αντίστοιχο στιγμιότυπο.

```
App.contracts.vote.deployed().then(function(instance)
```

Μάλιστα τον τελευταίο καιρό έχουν αναπτυχθεί βιβλιοθήκες για την διαχείριση τέτοιων εντολών και για την διευκόλυνση της ανάπτυξης κώδικα σε αποκεντρωμένες εφαρμογές. Μια τέτοια βιβλιοθήκη είναι η chai-as promised.

Αρχικά στον κώδικα της εφαρμογής θα πρέπει να αρχικοποιήσουμε όλα τα δεδομένα που σχετίζονται με την εφαρμογή και το δίκτυο. Εδώ ορίζεται το url της εφαρμογής και παρέχονται όλες οι πληροφορίες που απαιτούνται για την σωστή εμφάνιση των διάφορων objects της ιστοσελίδας (εικόνες, ονόματα, μεταβλητές).

Η συνάρτηση init function είναι υπεύθυνη για την σωστή εμφάνιση και αρχικοποίηση των proposals στην αποκεντρωμένη εφαρμογή καθώς συνδέει την back-end λογική με τον front-end κώδικα (html,css)

Η συνάρτηση init web3 εξασφαλίζει την σωστή επικοινωνία με το web3 παρέχοντας ένα σημείο RPC (εδώ 127.0.0.1:7545).

Η συνάρτηση initContract φέρνει τα απαραίτητα artifacts που δημιουργήθηκαν κατά το compile του συμβολαίου και ορίζει τον διοργανωτή της ψηφοφορίας.

Για κάθε συνάρτηση του smart contract υπάρχει μία αντίστοιχη συνάρτηση στην εφαρμογή του blockchain sever που επιτρέπει την επικοινωνία της διαδικτυακής εφαρμογής με το blockchain.

Η συνάρτηση getchairperson, ελέγχει ποιος λογαριασμός έχει συνδεθεί στο Metamask και παρέχει την κατάλληλη εικόνα στην διαδικτυακή εφαρμογή με τα ανάλογα jQueries, καθώς μόνο ο chairperson έχει την δυνατότητα να κάνει register και άρα «βλέπει» αυτή την λειτουργία όταν συνδέεται.

Οι συναρτήσεις handle register,handle winner kai handle vote επικοινωνούν με τις αντίστοιχες συναρτήσεις register, winningproposal και vote του smart contract προκειμένου να «φέρουν» στην διαδικτυακή εφαρμογή τις διάφορες λειτουργίες του συμβολαίου και να παρέχουν τα κατάλληλα μηνύματα στον χρήστη της ανάλογα με τις ενέργειες του.

Τέλος ορίζεται η λειτουργία των διαφόρων buttons με τις συναρτήσεις που καλούν. Παρακάτω παρουσιάζεται ο πλήρης κώδικας της web εφαρμογής.

```
App = {
  web3Provider: null,
  contracts: {},
  names: new Array(),
  url: 'http://127.0.0.1:7545',
  chairPerson:null,
  currentAccount:null,
  init: function() {
    $.getJSON('../proposals.json', function(data) {
      var proposalsRow = $('#proposalsRow');
      var proposalTemplate = $('#proposalTemplate');

      for (i = 0; i < data.length; i ++) {
        proposalTemplate.find('.panel-title').text(data[i].name);
        proposalTemplate.find('.panel-description').text(data[i].description);
        proposalTemplate.find('img').attr('src', data[i].picture);
        proposalTemplate.find('.btn-vote').attr('data-id', data[i].id);

        proposalsRow.append(proposalTemplate.html());
        App.names.push(data[i].name);
      }
    });
    return App.initWeb3();
  },

  initWeb3: function() {
        // Is there is an injected web3 instance?
    if (typeof web3 !== 'undefined') {
      App.web3Provider = web3.currentProvider;
    } else {
      // If no injected web3 instance is detected, fallback to the TestRPC
      App.web3Provider = new Web3.providers.HttpProvider(App.url);
    }
    web3 = new Web3(App.web3Provider);

    App.populateAddress();
    return App.initContract();
  },
```

```
initContract: function() {
    $.getJSON('Ballot.json', function(data) {
  // Get the necessary contract artifact file and instantiate it with truffle-contract
  var voteArtifact = data;
  App.contracts.vote = TruffleContract(voteArtifact);

  // Set the provider for our contract
  App.contracts.vote.setProvider(App.web3Provider);

  App.getChairperson();
  return App.bindEvents();
});
},

bindEvents: function() {
  $(document).on('click', '.btn-vote', App.handleVote);
  $(document).on('click', '#win-count', App.handleWinner);
  $(document).on('click', '#register', function(){ var ad = $('#enter_address').val(); App.handleRegister(ad); });
},

populateAddress : function(){
  new Web3(new Web3.providers.HttpProvider(App.url)).eth.getAccounts((err, accounts) => {
    jQuery.each(accounts,function(i){
      if(web3.eth.coinbase != accounts[i]){
        var optionElement = '<option value="'+accounts[i]+'">'+accounts[i]+'</option';
        jQuery('#enter_address').append(optionElement);
      }
    });
  });
},
```

```
getChairperson : function(){
  App.contracts.vote.deployed().then(function(instance) {
    return instance.chairperson();
  }).then(function(result) {
    App.chairPerson = result.toString();
    App.currentAccount = web3.eth.coinbase;
    if(App.chairPerson != App.currentAccount){
      jQuery('#address_div').css('display','none');
      jQuery('#register_div').css('display','none');
    }else{
      jQuery('#address_div').css('display','block');
      jQuery('#register_div').css('display','block');
    }
  })
},

handleRegister: function(addr){
  var voteInstance;
  App.contracts.vote.deployed().then(function(instance) {
    voteInstance = instance;
    return voteInstance.register(addr);
  }).then( function(result){
    if(result.receipt.status == '0x01')
      alert(addr + " is registered successfully")
    else
      alert(addr + " account registeration failed due to revert")
  }).catch( function(err){
    alert(addr + " account registeration failed")
  })
},
```

```
handleVote: function(event) {
  event.preventDefault();
  var proposalId = parseInt($(event.target).data('id'));
  var voteInstance;
  web3.eth.getAccounts(function(error, accounts) {
    var account = accounts[0];

    App.contracts.vote.deployed().then(function(instance) {
      voteInstance = instance;

      return voteInstance.vote(proposalId, {from: account});
    }).then(function(result){
          if(result.receipt.status == '0x01')
          alert(account + " Voting done successfully")
          else
          alert(account + " Voting not done successfully due to revert")
      }).catch(function(err){
        alert(account + " Voting failed")
  });
  });
},
handleWinner : function() {
  var voteInstance;
  App.contracts.vote.deployed().then(function(instance) {
    voteInstance = instance;
    return voteInstance.winningProposal();
  }).then(function(res){
    alert(App.names[res] + "  is the winner! Tally yourself for exact results!");
  }).catch(function(err){
    console.log(err.message);
  })
}
};
$(function() {
  $(window).load(function() {
    App.init();
  });
```

Migration Scripts

```
var Migrations = artifacts.require("Migrations");

module.exports = function(deployer) {
  deployer.deploy(Migrations);
};
```

```
var Ballot = artifacts.require("Ballot");

module.exports = function(deployer) {
  deployer.deploy(Ballot);
};
```

```
UnitTest stub | dependencies | uml
contract Migrations {
  address public owner;
  uint public last_completed_migration;

  modifier restricted() {
    if (msg.sender == owner) _;
  }

  ftrace | funcSig
  function Migrations() public {
    owner = msg.sender;
  }

  ftrace | funcSig
  function setCompleted(uint completed⬆) public restricted {
    last_completed_migration = completed⬆;
  }

  ftrace | funcSig
  function upgrade(address new_address⬆) public restricted {
    Migrations upgraded = Migrations(new_address⬆);
    upgraded.setCompleted(last_completed_migration);
  }
}
```

Διαχείριση έκδοσης compiler και δικτύου στο αρχείο Truffle config.js

```
// Configure your compilers
compilers: {
  solc: {
    version: "0.5.17",    // Fetch exact version from solc-bin (default: truffle's version)
    // version: "0.5.1",    // Fetch exact version from solc-bin (default: truffle's version)
    // docker: true,        // Use "0.5.1" you've installed locally with docker (default: false)
    // settings: {          // See the solidity docs for advice about optimization and evmVersion
    //  optimizer: {
    //    enabled: false,
    //    runs: 200
    //  },
    //  evmVersion: "byzantium"
    // }
  }
}
```

```
networks: {
  // Useful for testing. The `development` name is special - truffle uses it by default
  // if it's defined here and no other network is specified at the command line.
  // You should run a client (like ganache-cli, geth or parity) in a separate terminal
  // tab if you use this network and you must also set the `host`, `port` and `network_id`
  // options below to some value.
  //
   development: {
       host:"localhost",
       port:7545,
       network_id:"*" //Match any network id
   }
```

## 7.6 Κώδικας Front-end HTML και CSS

```
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <!-- The above 3 meta tags *must* come first in the head; any other head content must come *after* these tags -->
    <title>Ψήφισε την Επιλογή σου!</title>
    <link href="https://fonts.googleapis.com/css2?family=Roboto+Mono:ital,wght@0,400;0,700;1,300&display=swap" rel="sty
    <!-- Bootstrap -->
    <link href="css/bootstrap.min.css" rel="stylesheet">
    <link href="css/style.css" rel="stylesheet">

    <!-- HTML5 shim and Respond.js for IE8 support of HTML5 elements and media queries -->
    <!-- WARNING: Respond.js doesn't work if you view the page via file:// -->
<!--     [if lt IE 9]>
      <script src="https://oss.maxcdn.com/html5shiv/3.7.3/html5shiv.min.js"></script>
      <script src="https://oss.maxcdn.com/respond/1.4.2/respond.min.js"></script>
    <![endif] -->
  </head>
  <body>
    <div class="container-fluid top-bar">
      <p>ΠΑΡΕ ΜΕΡΟΣ ΣΤΗΝ ΨΗΦΟΦΟΡΙΑ ΚΑΙ ΑΝΑΔΕΙΞΕ ΤΟΝ ΠΙΟ ΑΠΟΤΕΛΕΣΜΑΤΙΚΟ ΑΛΓΟΡΙΘΜΟ ΣΥΝΑΙΝΕΣΗΣ!</p>
    </div>
    <div class="container heading-area">
      <div class="row">
        <div class="col-12">
          <h1 class="text-center">Ψήφισε την Επιλογή σου!</h1>
        </div>
      </div>

      <div id="proposalsRow" class="row">
      </div>
    </div>

    <div id="proposalTemplate" style="display: none;">
      <div class="col-sm-6 col-md-3">
        <div class="panel panel-default panel-proposal text-center">
          <div class="panel-heading">
            <h3 class="panel-title">PROOF OF WORK</h3>
            <h3 class="panel-description">Απόδειξη Επίλυσης ενός υπολογιστικού προβλήματος.</h3>
          </div>
          <div class="panel-body">
            <img alt="140x140" data-src="holder.js/140x140" class="img-rounded img-center" src="images/apple.jpg"
            <br/><br/>
            <button class="btn btn-default btn-vote" type="button" data-id="0">Ψήψισέ το</button>
          </div>
        </div>
      </div>
    </div>
    <div class="container">
      <div class="row row-center" id="address_div">
          <span> Address : </span>
          <select id="enter_address" value=""></select>
      </div>
      <div class="row winner row-center">
       <button class="btn btn-success" type="button" id="win-count">ΔΕΣ ΤΟ ΑΠΟΤΕΛΕΣΜΑ</button>
      </div>
      <div class="row row-center" id="register_div">
          <button class="btn btn-info" type="button" id="register">ΚΑΤΑΧΩΡΙΣΗ</button>
      </div>
    </div>
    <div class="container-fluid footer">
      <div class="row signature">
      <div class="col-xs-6 col-md-6">
        <p class="tiny pb-0 pb-md-1">Ψηφοφορία TechnoEconomics© 2020</p>
      </div>
      <div class="col-xs-6 col-md-6 text-right">
        <p class="tiny">Crafted with care by <a href="#">Orestis Almpanoudis</a>
        </p>
      </div>
      </div>
    </div>
```

```
    <!-- jQuery (necessary for Bootstrap's JavaScript plugins) -->
    <script src="https://ajax.googleapis.com/ajax/libs/jquery/1.12.4/jquery.min.js"></script>

    <!-- Include all compiled plugins (below), or include individual files as needed -->
    <script src="https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js" integrity="sha384-JZR6Spejh4U02d8
    <script src="js/web3.min.js"></script>
    <script src="js/truffle-contract.js"></script>
    <script src="js/app.js"></script>
    <script>

    var docElm = document.documentElement;
    if (docElm.requestFullscreen) {
        docElm.requestFullscreen(Element.ALLOW_KEYBOARD_INPUT);
    }
    else if (docElm.mozRequestFullScreen) {
    docElm.mozRequestFullScreen(Element.ALLOW_KEYBOARD_INPUT);
    }
    else if (docElm.webkitRequestFullScreen) {
        docElm.webkitRequestFullScreen(Element.ALLOW_KEYBOARD_INPUT);
    }
    </script>
  </body>
</html>
```

CSS

```
body {
    font-family: 'Roboto Mono', monospace;
}

h1 {
    font-weight: 600;
    line-height: 1em;
    margin: 0.6em 0;
}

.top-bar {
    background-color: #000;
    color: white;
    display: flex;
    justify-content: center;
    padding: 10px;
    text-align: center;
}

.top-bar p {
    font-size: 16px;
    letter-spacing: 1.5px;
    line-height: 1.2em;
    margin-bottom: 0;
}

.panel-proposal {
    padding: 6px 16px;
}

.heading-area {
    padding: 40px 16px;
}
```

```css
.panel-default>.panel-heading {
    padding: 10px 0px;
    background-color: #fff;
    border: none;
    height: 103px;
}

.panel-description {
    font-style: italic;
    font-weight: 300;
    font-size: 14px;
    margin-top: 10px;
}

.panel-title {
    font-weight: 600;
    text-transform: uppercase;
}


.btn {
    font-weight: 600;
    border-radius: 0;
    padding: 8px 16px;
}

.btn-vote {
    background-color: #222;
    color: #fff;
    font-weight: 600;
    border-radius: 0;
    padding: 8px 16px;
}
```

```css
.btn-info:hover {
    color: #fff;
    background-color: #ff1a1a;
    border-color: #ff1a1a;
}

.btn-success {
    border-color: inherit;
}

.panel-body img {
    height: 150px;
    object-fit: fill;
    max-width: 100%;
}

.winner {
    padding: 30px 0;
}

.row-center {
    display: flex;
    justify-content: center;
}

.footer {
    position: fixed;
    bottom: 0;
    width: 100%;
}

.signature {
    background-color: aliceblue;
    padding-top: 10px;
}

.text-right {
    text-align: right;
}
```

Proposals.jason

```
[
  {
    "id": 0,
    "name": "PROOF OF WORK",
    "description": "Απόδειξη Επίλυσης ενός υπολογιστικού προβλήματος.",
    "picture": "images/pow.jpg"
  },
  {
    "id": 1,
    "name": "PROOF OF STAKE",
    "description": "Απόδειξη της ιδιοκτησίας του ψηφιακού νόμισματος.",
    "picture": "images/pos.jpg"
  },
  {
    "id": 2,
    "name": "PROOF OF ACTIVITY",
    "description": "Ένας συνδυασμός των πρωτοκόλλων PoW και PoS.",
    "picture": "images/poact.jpg"
  },
  {
    "id": 3,
    "name": "PROOF OF AUTHORITY",
    "description": "Απόδειξη της αξίας της φήμης.",
    "picture": "images/authority.jpg"
  }
]
```

# 8. Συμπεράσματα και Μελλοντικές Προοπτικές

Συνοψίζοντας, σε αυτή τη μελέτη, προσπαθήσαμε να προσεγγίσουμε το ερώτημα εάν το blockchain είναι το μέλλον των ψηφοφοριών, όπως ισχυρίζονται πολλοί συγγραφείς συστημάτων ηλεκτρονικής ψηφοφορίας και αν μπορεί μια ψηφοφορία στο blockchain να καλύψει τις απαιτήσεις ασφαλείας που παρουσιάστηκαν στην ενότητα 4.2 . Αναπτύξαμε μια αποκεντρωμένη εφαρμογή για την διεξαγωγή ψηφοφορίας μικρής κλίμακας και αναδείξαμε ότι η ψηφοφορία στο blockchain λύνει το πρόβλημα της επίτευξης συναίνεσης μεταξύ μερών με αντικρουόμενα συμφέροντα. Η διατήρηση της ακεραιότητας και της α-μεταβλητότητας της ψηφοφορίας και των δεδομένων εξασφαλίζει ευρωστία και αξιοπιστία του συστήματος. Επίσης, η διαφάνεια, η σαφήνεια και ο ντετερμινισμός της ψηφοφορίας σε συνδυασμό με το γεγονός ότι ο οποιοσδήποτε συμμετέχοντας στο δίκτυο μπορεί να ελέγξει μόνος του την διαδικασία και δεν χρειάζεται κάποια κεντρική αρχή για την επαλήθευση του αποτελέσματος της διαδικασίας συμπληρώνουν τα θετικά στοιχεία της εφαρμογής μας.

Στα μειονεκτήματα της εφαρμογής συμπεριλαμβάνεται το γεγονός ότι η διαδικασία δεν είναι πλήρως αποκεντρωμένη και ανώνυμη αλλά ψευδώνυμη. Κατ'αρχήν, κάθε ψήφος μπορεί να συνδεθεί με το δημόσιο κλειδί κάθε λογαριασμού. Τόσο η υποβολή των υποψήφιων όσο και το registration ελέγχονται κεντρικά από τον διοργανωτή της διαδικασίας. Ακόμα και αν χρησιμοποιούσαμε μια λύση με mixed networks για την διανομή των κλειδιών, θα χρειαζόμασταν μια κεντρική βάση δεδομένων για την αποθήκευση τους. Υπάρχουν τρόποι να καταστεί ανώνυμη μια τέτοια εφαρμογή ακολουθώντας το πλήρως ανώνυμο σύστημα ψηφοφορίας Open Vote Network που προτάθηκε από τον Patrick McCorry. Εξασφαλίζεται από άκρη σε άκρη μυστικότητα της διαδικασίας, ωστόσο το σύστημα αυτό προορίζεται να χρησιμοποιηθεί μόνο για εκλογές μικρής κλίμακας. Το Open Vote αποτελεί ίσως την πιο ολοκληρωμένη λύση ψηφοφορίας στο blockchain ως σήμερα, ωστόσο έχει ακόμα πολλές αδυναμίες όπως για παράδειγμα η μηδενική αντίσταση στον εξαναγκασμό. Προκειμένου να είναι ένα πρωτόκολλο ψηφοφορίας σε θέση να πείσει τους ηττημένους υποψηφίους, καθώς και το εκλογικό σώμα και τους παρατηρητές, θα πρέπει να ικανοποιεί πολύ πιο αυστηρές απαιτήσεις ασφαλείας,

Η ηλεκτρονική ψηφοφορία είναι ακόμη στα σπάργανα και πρέπει να προσεγγιστεί με προσοχή καθώς μπορεί να βοηθήσει τους επιτιθέμενους να εξαπατήσουν σε μεγάλη κλίμακα με ευκολία. Η ίδια η τεχνολογία blockchain είναι αναπτύσσομενη. Ωστόσο, καθώς όλες οι ανθρώπινες δραστηριότητες πρόκειται να διεξαχθούν ηλεκτρονικά μακροπρόθεσμα και η ψηφοφορία δεν μπορεί να αποτελέσει εξαίρεση. Η κρυπτογραφία και άλλες τεχνικές θα εξελιχθούν για να υποστηρίξουν τις απαιτήσεις ασφαλείας και την προστασία των προσωπικών δεδομένων. Η ανάπτυξη σε τομείς όπως το διαδίκτυο των πραγμάτων μπορεί να επιφέρει διαφορετικούς on-chain τρόπους ταυτοποίησης όπως η αυτοδύναμη ταυτότητα που παρουσιάστηκε στην ενότητα 4.3. Επίσης, πολύ υποσχόμενος είναι ο τομέας των side-chains και η ανάπτυξη του αναμένεται να επιφέρει σημαντικές βελτιώσεις σε πληθώρα on-chain διαδικασιών.

Οι developers θα πρέπει να παρακινήσουν για μεγαλύτερη συμμετοχή και για καλύτερο συντονισμό στις διάφορες κοινότητες αποκεντρωμένων συστημάτων, ώστε να λαμβάνονται όσο το δυνατόν πιο δημοκρατικές αποφάσεις που ωφελούν την ίδια την κοινότητα και εξασφαλίζουν την μακροχρόνια εξυπηρέτηση της.

Ταυτόχρονα, το κοινό θα πρέπει σταδιακά να εξοικειωθεί με τις νέες διαδικασίες συμμετέχοντας σε εκλογές μικρής κλίμακας όπου τα διακυβεύματα δεν είναι τόσο υψηλά όσο στις εθνικές κυβερνητικές εκλογές. Αυτό σημαίνει ότι η εισαγωγή της ηλεκτρονικής ψηφοφορίας πρέπει να είναι από κάτω προς τα πάνω και σταδιακή, παρέχοντας εγγυήσεις ασφάλειας που θεωρητικά είναι αυστηρές, αλλά εύκολα κατανοητές από τον μέσο ψηφοφόρο.

# 9. Βιβλιογραφία

1. Hal Finney. Reusable Proofs of Work. Nakamoto Institute. https://nakamotoinstitute.org/finney/rpow/index.html. 25th June 2019

2. Ameer Rosic. What is Blockchain Technology? A Step-by-Step Guide For Beginners. Blockgeeks. https://blockgeeks.com/guides/what-is-blockchain-technology/. 25th June 2019.

3. Handbook on European data protection law, 2018 edition https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf

4. Blockchain and the General Data Protection Regulation, EPRS | European Parliamentary Research Service Scientific Foresight Unit (STOA), July 2019 https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf

5. Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements *Oslo Law Review, Volume 4, No. 2, 2017*

6. Solutions for a responsible use of the blockchain in the context of personal data, CNIL,September 2018 https://www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf

7. Bell, Stephen (2002): “Economic Governance and Institutional Dynamics”. Oxford University Press

8. Atzori, Marcella (2017): “Blockchain technology and decentralized governance: Is the state still necessary?”, Journal of Governance and Regulation, vol. 6(1), pp. 45-62

9. Srinivasan, Balaji S. and Leland Lee (2017): “Quantifying Decentralization”. Retrieved on May 15, 2020 from https://news.earn.com/quantifying-decentralization-e39db233c28e.

10. Kwon, Yujin, Liu Jian Li, Kim Minjeong, Song Dawn and KIm Yongdae (2019): “Impossibility of Full Decentralization in Permissionless Blockchains”, Proceedings of the 1st ACM Conference on Advances in Financial Technologies, October 21-23 2019, Zurich, pp. 110–123

11. Azouvi, Sarah, Mary Maller and Sarah Meiklejohn (2019): “Egalitarian Society or Benevolent Dictatorship: The State of Cryptocurrency Governance”, in: A. Zohar et al. (eds.), ”Financial Cryptography and Data Security”, FC 2018, Lecture Notes in Computer Science, vol 10958, pp. 127-143. Springer, Berlin, Heidelberg

12. Muzzy, Everett and Mally Anderson (2019): “Measuring Blockchain Decentralization”. Retrieved on May 16, 2020 from https://consensys.net/research/measuring-blockchain-decentralization/.

13. Wright, Aaron and Primavera de Filippi (2018): “Blockchain and the Law: The Rule of Code”. Harvard University Press

14. Herian, Robert (2018): “Legal Recognition of Blockchain Registries and Smart Contracts”, draft report prepared for a workshop on “Blockchains & smart contracts legal and regulatory framework”, Paris, France, 12th December. DOI 10.13140/RG.2.2.12449.86886.

15. Beylin, Eva (2019): “Ethereum Governance Survey Results” , https://medium.com/p/c67c11695f2a

16. Allen, Matthew (2018): “Swiss blockchain voting platform begins trial https://www.swissinfo.ch/eng/crypto-valley_swiss-blockchain-voting-platform-begins-trial/44215246.

17. Chaum, David, Markus Jakobsson, Ronald Rivest, Peter Ryan, Josh Benaloh, Miroslav Kutyłowski, and Ben Adida (2010, eds.): “Towards Trustworthy Elections: New Directions in Electronic Voting”. Springer

18. Onggunhao, Daniel (2019): “Wow. The @MakerDAO stability fee (interest rate) has dropped to 5.5%. A single whale (with 97% of voting power) made the decision. Went from 2,489 votes a few hours ago, to 44,539 votes.” October 28, 2019, 3:25 PM

19. Learner, Roy (2019): “Blockchain Voter Apathy”. https://medium.com/p/69a1570e2af3

Ethereum White paper,A Next-Generation Smart Contract and Decentralized Application Platform

20. Clarkson, Michael, Stephen Chong, and Andrew Myers (2008): “Civitas: Toward a Secure Voting System”, IEEE Symposium on Security and Privacy, pp. 354-368.

21. Λαμπρινουδάκης Κ., Μήτρου Λ., Γκρίτζαλης Σ., Κάτσικας Σ. “Προστασία της ιδιωτικότητας & τεχνολογίες πληροφορικής και επικοινωνιών”, Κεφ 18: “Προστασία της ιδιωτικότητας στην Ηλεκτρονική Ψηφοφορία”, Αθήνα 2010, ISBN 9607182707

22. Heiberg, Sven and Jan Willemson (2014): "Verifiable internet voting in Estonia", 6th IEEE International Conference on Electronic Voting (Lochau/Bregenz, Austria), pp. 1–8.

23. Man, Ido, Ron Sabo and Ehud Segal (2019): “Resolving the Stake-Based vs. Participant-Based Voting Dilemma”. https://blog.saga.org/resolving-the-stake-based-vs-participant-based-voting-dilemma-de0b50376f8f .

24. Lalley, Steven and E. Glen Weyl (2018): “Quadratic Voting: How Mechanism Design Can Radicalize Democracy”, American Economic Association Papers and Proceedings, 1(1), pp. 1-5. Available at https://ssrn.com/abstract=2003531.

25. Buterin, Vitalik, Zoë Hitzig, and E. Glen Weyl (2018): “Liberal Radicalism: A Flexible Design For Philanthropic Matching Funds“. Available at https://ssrn.com/abstract=3243656

26. Towards Secure E-Voting Using Ethereum Blockchain, International Symposium on Digital Forensic and Security (ISDFS), Ali Kaan Ko Antalya, Turkey

27. Internet Voting Using Zcash, Pavel Tarasov, 14th International Conference on Applied Computing

28. Decentralized , Transparent , Trustless Voting on the Ethereum Blockchain Fernando. Fernando Lobato Meeser; 2017.

29. A Smart Contract for Boardroom Voting with Maximum Voter Privacy,Patrick, McCorry, Siamak F. Shahandashti, Feng Hao, 2017

30. Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., & Savage, S. (2013). A fistful of bitcoins: characterizing payments among men with no names. In IMC ’13: Proceedings of the 2013 conference on Internet measurement conference.

31. Nasser, Y., Okoye, C., Clark, J., & Ryan, P. Y. A. (2018). Blockchains and voting: Somewhere between hype and a panacea.

33. Gencer, A. E. (2018). Decentralization in bitcoin and Ethereum networks.

34. —. Ethereum Explained: Merkle Trees, World State, Transactions, and More. PEGASYS. https://pegasys.tech/ethereum-explained-merkle-trees-world-statetransactions-and-more/. 4 th July 2019.

35. Hal Finney. Reusable Proofs of Work. Nakamoto Institute. https://nakamotoinstitute.org/finney/rpow/index.html. 25th June 2019.

36. https://en.wikipedia.org/wiki/Public-key_cryptography (2019)

37. https://remix.ethereum.org/

38. nodejs.org

39. trufflesuite.com

40.Personal blockchain for Ethereum Development. Github. https://github.com/trufflesuite/ganache, 8 th July 2019.