Πανεπιστήμιο Δυτικής Αττικής

Σχολή Μηχανικών

Τμήμα Μηχανικών Πληροφορικής και Υπολογιστών

Πτυχιακή εργασία

Εκλογικό σύστημα με τεχνολογία Blockchain

Σπανός Αχιλλέας
711161048

Επιβλέπων:

Ιωάννα Καντζάβελου
Επίκουρη Καθηγήτρια

Αιγάλεω - Αθήνα, Ιούλιος, 2023

Εγκρίθηκε από την εξεταστική επιτροπή την 12 / 07 / 2023.

Ioanna Kantzavelou
Digitally signed by Ioanna Kantzavelou
Date: 2023.07.25 13:06:42 +03'00'

Ιωάννα Καντζάβελου
Επίκουρη Καθηγήτρια

Antonios Bogris
Digitally signed by Antonios Bogris
Date: 2023.07.26 16:25:06 +02'00'

Αντώνιος Μπόγρης
Καθηγητής

Vasileios Mamalis
Digitally signed by Vasileios Mamalis
Date: 2023.07.27 13:39:19 +03'00'

Βασίλειος Μάμαλης
Καθηγητής

.....

Σπανός Αχιλλέας
Σχολή Μηχανικών, Τμήμα Μηχανικών πληροφορικής και Υπολογιστών
Πανεπιστήμιο Δυτικής Αττικής

Ευχαριστίες

Θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες, στην κυρία Ιωάννα Καντζάβελου για την αξιόλογη καθοδήγηση κατά τη διάρκεια της διπλωματικής εργασίας. Η συνεργασία μας αποτελεί πηγή έμπνευσης και αναπτυξιακής προόδου για μένα.

Οι συμβουλές σας, η προθυμία σας να μοιραστείτε τις γνώσεις σας και η ενθάρρυνσή σας με είχαν οδηγήσει σε μια εμπειρία μάθησης και ανάπτυξης που θα με συντροφεύει για πάντα. Η σαφής και προσεκτική σας ανάλυση των ιδεών μου, καθώς και οι προτάσεις σας για βελτίωση, με βοήθησαν να αναπτύξω τις ικανότητές μου και να προχωρήσω σε νέα επίπεδα.

Πραγματικά, εκτιμώ τον χρόνο και την προσοχή που αφιερώσατε για να με καθοδηγήσετε και να με ενθαρρύνετε καθ' όλη τη διάρκεια της διπλωματικής εργασίας. Η συνεισφορά σας έχει επηρεάσει θετικά την ακαδημαϊκή μου πορεία και την επαγγελματική μου ανάπτυξη.

Θέλω να σας ευχαριστήσω θερμά για την ευκαιρία που μου δώσατε να επεκτείνω τις γνώσεις μου, να εξερευνήσω νέες ιδέες και να αναπτύξω τις δεξιότητές μου. Η στήριξή σας και η προσφορά σας στο πεδίο της ασφάλειας θα παραμείνουν ανεκτίμητες.

Ευελπιστώ ότι θα έχουμε την ευκαιρία να συνεργαστούμε ξανά στο μέλλον και να συνεχίσω να αποκομίζω τα φρονήματά σας και τη σοφία σας. Σας εύχομαι ό,τι καλύτερο για το μέλλον σας και ευελπιστώ ότι θα συνεχίσετε να επηρεάζετε θετικά τους άλλους με την αφοσίωσή σας και την απόδοσή σας.

Σπανός Αχιλλέας

Περίληψη

Πλέον πολλές εφαρμογές, λειτουργούν χωρίς βάση δεδομένων, με ανοιχτό κώδικα που εκτελείται στο δίκτυο Blockchain εκμεταλλευόμενες όλα τα οφέλη του. Η αποκεντρωμένη τεχνολογία και η εγγύηση της διαλειτουργικότητας και ασφάλειας των δεδομένων χρησιμοποιείται ήδη σε πολλούς τομείς της καθημερινότητας, όπως εφαρμογές υγείας, μεταφοράς κ.ο.κ.. Σκοπός αυτής της διπλωματικής εργασίας είναι η δημιουργία μίας αποκεντρωμένης εφαρμογής εκλογών στο δίκτυο του Ethereum, με την ταυτοποίηση πολιτών, αλλά και την εκλογική διαδικασία να βασίζονται αποκλειστικά στην εκτέλεση ανοιχτού κώδικα αποθηκευμένου στο Blockchain. Θα ακολουθήσει μία μελέτη σχετικά με τις υπηρεσίες ασφάλειας που προσφέρει το Blockchain, κινδύνους και νέες επιθέσεις που μπορούν να πραγματοποιηθούν σε ένα τέτοιο δίκτυο αλλά και την ασφάλεια που παρέχει η προτεινόμενη εφαρμογή εκλογών.

Λέξεις Κλειδιά: Blockchain, Ψηφοφορία, Ethereum, Έξυπνο συμβόλαιο

Abstract

Many applications operate without a database, with open source running on the Blockchain network exploiting all its benefits. Decentralized technology and its guarantee interoperability and data security is already used in many areas in everyday life applications, such as health, transportation, etc. The purpose of this thesis is to create a decentralized election application on the Ethereum network, with the identification of citizens and the electoral process based solely on the execution of open source code stored in the Blockchain. This will be followed by a study on the security services offered by Blockchain, risks and new attacks that can be carried out in such a network and the security provided by the proposed application.

Keywords: Blockchain, Voting, Ethereum, Smart contract

Περιεχόμενα

Κατάλογος Σχημάτων

Κατάλογος Πινάκων

Κεφάλαιο 1

Εισαγωγή

Σε μία χώρα σαν την Ελλάδα όπου γεννήθηκε η δημοκρατία η ύπαρξη ασφαλούς πλατφόρμας ψηφοφορίας είναι πολύ σημαντική. Ανά τα χρόνια έχουν διεξαχθεί πολλές έρευνες με σκοπό την αντιμετώπιση των προβλημάτων που παρουσιάζονται σε συστήματα ψηφοφορίας. Έχει αναπτυχθεί ένα πλήθος ερευνητικών εργασιών ώστε να υλοποιηθεί ένα ασφαλές και αξιόπιστο σύστημα ψηφοφορίας. Κύριος στόχος είναι η αντιμετώπιση προβλημάτων που αφορούν ζητήματα ασφάλειας, ανωνυμίας, αλλά και γενικότερα απάτες που μπορεί να λάβουν χώρα σε τέτοια συστήματα. Η νέα και πολλά υποσχόμενη τεχνολογία του Blockchain, παρέχοντας τη δυνατότητα δημιουργίας ανοιχτού κώδικα, χρησιμοποιείται ήδη σε πολλές εφαρμογές της καθημερινότητας εκμεταλλευόμενες όλα τα οφέλη του.

1.1 Πλαίσιο, σκοπός και στόχοι της πτυχιακής εργασίας

Η παρούσα πτυχιακή εργασία εστιάζει στον σχεδιασμό και την υλοποίηση ενός συστήματος ψηφοφορίας με χρήση της τεχνολογίας blockchain, με έμφαση στην ασφαλή ταυτοποίηση των χρηστών. Ο κύριος σκοπός της εργασίας είναι να αντιμετωπίσει τα προβλήματα εμπιστοσύνης και ασφάλειας που σχετίζονται με τις παραδοσιακές μεθόδους ψηφοφορίας και να παρέχει ένα αξιόπιστο, αμετάβλητο και ανοιχτό σύστημα για τη διεξαγωγή ψηφοφοριών.

Οι στόχοι της πτυχιακής εργασίας είναι οι εξής:

1. Να αναπτυχθεί ένα σύστημα ψηφοφορίας με τη χρήση της τεχνολογίας blockchain, το οποίο θα είναι ανοιχτό, αμετάβλητο και ασφαλές.

2. Να προσφέρει έναν αξιόπιστο μηχανισμό ασφαλούς ταυτοποίησης των χρηστών, ώστε να αποτραπούν οι απάτες και οι παραποιήσεις των ψήφων.

3. Να επιτρέπει τη διατήρηση και την προστασία της ιδιωτικότητας των χρηστών κατά τη διάρκεια της διαδικασίας ψηφοφορίας.

4. Να αναλύσει τις αδυναμίες και τις πιθανές απειλές του συστήματος και να προτείνει λύσεις για την αντιμετώπισή τους.

Για την επίτευξη αυτών των στόχων, υλοποιήθηκε ένα σύστημα ψηφοφορίας που βασίζεται στην τεχνολογία του Ethereum και εξυπηρετείται από έξυπνα συμβόλαια. Οι χρήστες υποβάλλουν την ψήφο τους μέσω μιας ασφαλούς ταυτοποίησης, που συνδυάζει την κρυπτογραφία και την αποστολή ενός ενιαίου κωδικού OTP μέσω SMS. Επιπλέον, πραγματοποιήθηκε μια ανάλυση ασφάλειας για την αναγνώριση και αντιμετώπιση τυχόν ευπαθειών του συστήματος.

Με την παρούσα εργασία, προτείνονται λύσεις για τη βελτίωση της ασφάλειας, της εμπιστοσύνης και της αποτελεσματικότητας των συστημάτων ψηφοφορίας με τη χρήση τεχνολογίας blockchain.

1.2 Μεθοδολογία

Η μεθοδολογία που ακολουθήθηκε για την πραγματοποίηση αυτής της πτυχιακής εργασίας περιλαμβάνει τις εξής φάσεις:

1. Παρουσίαση του θεωρητικού υπόβαθρου: Στην αυτήν τη φάση, πραγματοποιήθηκε μια λεπτομερής μελέτη της τεχνολογίας blockchain και των κρυπτογραφικών αλγορίθμων που σχετίζονται με αυτήν. Μέσω αυτής της ανάλυσης, ο κάθε αναγνώστης αποκτά μια βαθύτερη γνώση και κατανόηση της διαφοροποίησης και της σοβαρότητας που προσφέρει το σύστημα ψηφοφορίας με βάση την τεχνολογία blockchain. Η εξέταση των κρυπτογραφικών αλγορίθμων παρέχει μια καλύτερη κατανόηση των μηχανισμών ασφαλείας που ενσωματώνονται στο σύστημα. Αυτή η γνώση και κατανόηση παρέχουν στους αναγνώστες τη δυνατότητα να αναγνωρίζουν τα πλεονεκτήματα και την αξιοπιστία του συστήματος ψηφοφορίας, καθώς και τη σοβαρότητα και την αξία της ασφάλειας που παρέχει.

2. Μελέτη και ανάλυση των υπαρχόντων συστημάτων ψηφοφορίας: Σε αυτήν τη φάση, διερευνήθηκαν και αναλύθηκαν τα προβλήματα και οι αδυναμίες των παραδοσιακών μεθόδων ψηφοφορίας. Μελετήθηκαν επίσης παρόμοια συστήματα ψηφοφορίας που βασίζονται στην τεχνολογία blockchain, προκειμένου να αναδειχθούν οι βέλτιστες πρακτικές και οι πιο ασφαλείς προσεγγίσεις.

3. Σχεδιασμός του συστήματος ψηφοφορίας: Με βάση την ανάλυση των απαιτήσεων και των περιορισμών, σχεδιάστηκε το σύστημα ψηφοφορίας στο δίκτυο Ethereum. Ο σχεδιασμός περιλαμβάνει καθορισμό της δομής του συστήματος, αλλά και διαχωρισμό της εκλογικής διαδικασίας σε 4 φάσεις. Σε κάθε φάση γίνεται ανάλυση των λειτουργιών που θα λαμβάνουν χώρα, καθορισμός της δομής του συστήματος, ταυτοποίηση των απαιτήσεων ασφάλειας και καθορισμός αλγορίθμων κρυπτογράφησης.

4. Υλοποίηση του συστήματος: Με βάση τον σχεδιασμό, υλοποιήθηκε το σύστημα ψηφοφορίας με τη χρήση της πλατφόρμας Ethereum και των έξυπνων συμβολαίων. Επίσης, έγινε και μια λεπτομερής παρουσίαση στη διεπαφή χρήστη, μέσω μιας προσομοίωσής ψηφοφορίας λαμβάνοντας υπόψη κάθε πιθανή έξοδο ή σφάλμα που μπορεί να κάνει ο χρήστης.

5. Ασφάλεια και απόδοση: Πραγματοποιήθηκε μια λεπτομερής ανάλυση ασφάλειας του συστήματος για τον εντοπισμό πιθανών ευπαθειών και απειλών. Αναφέρθηκαν οι κυριότερες μορφές επιθέσεων που θα μπορούσαν να βλάψουν το σύστημα που υλοποιήθηκε, αλλά και ο τρόπος αντιμετώπισης αυτών των κινδύνων από το σύστημα μας.

6. Αξιολόγηση και συμπεράσματα: Ολοκληρώθηκε η αξιολόγηση του συστήματος ψηφοφορίας, λαμβάνοντας υπόψη τους στόχους και τις απαιτήσεις που ορίστηκαν στο πλαίσιο της πτυχιακής εργασίας, με σημαντικότερα την ικανοποίηση των αρχών ψηφοφορίας και την ασφαλή ταυτοποίηση των έγκυρων ψηφοφόρων που θα τους επιτρέψει την καταβολή ψήφου. Επιπλέον αναφέρθηκαν όλες οι λειτουργικές ή τεχνικές αδυναμίες του συστήματος, καθώς και ο τρόπος αντιμετώπισης τους. Πραγματοποιώντας αυτή την αξιολόγηση του συστήματος αφήνουμε περιθώρια για περεταίρω μελέτη.

1.3 Περιορισμοί

Ο μόνος, αλλά αρκετά σημαντικός περιορισμός είναι ότι το σύστημα είναι σχεδιασμένο να λειτουργεί αποκλειστικά μέσω του Ethereum, χωρίς να χρησιμοποιείται κάποια άλλη βάση δεδομένων ή διακομιστής εκτός από το έξυπνο συμβόλαιο. Αυτό εξασφαλίζει ότι το σύστημα παραμένει εξαιρετικά αποκεντρωμένο, καθώς οι ψηφοφόροι συμμετέχουν απευθείας μέσω του Ethereum

blockchain χωρίς ενδιάμεσους. Αυτή η αποκεντρωμένη λειτουργία ενισχύει την αξιοπιστία, τη διαφάνεια και την ασφάλεια του συστήματος ψηφοφορίας που έχει υλοποιηθεί στο Ethereum.

1.4 Οργάνωση, κεφαλαίωση, διάρθρωση της εργασίας

Η παρούσα διπλωματική εργασία, αφορά την πρόταση και υλοποίηση ενός συστήματος ψηφοφορίας μέσω Blockchain. Παρακάτω παρουσιάζουμε σύντομα τα περιεχόμενα των κεφαλαίων:

- **Κεφάλαιο 2: Θεωρητικό υπόβαθρο**

  Σε αυτό το κεφάλαιο παρουσιάζεται το θεωρητικό υπόβαθρο που αφορά την τεχνολογία του Blockchain και την ηλεκτρονική ψηφοφορία. Εξηγούνται οι βασικές έννοιες του Blockchain, οι αρχές της λειτουργίας του και οι κρυπτογραφικές τεχνικές που χρησιμοποιούνται.

- **Κεφάλαιο 3: Ηλεκτρονική ψηφοφορία και ήδη υπάρχοντα συστήματα ψηφοφορίας μέσω Blockchain**

  Σε αυτό το κεφάλαιο παρουσιάζονται οι γενικές αρχές της ηλεκτρονικής ψηφοφορίας και εξετάζονται τα υπάρχοντα συστήματα ψηφοφορίας που βασίζονται στο Blockchain. Παρουσιάζονται παραδείγματα επιτυχημένων περιπτώσεων εφαρμογής της τεχνολογίας Blockchain στην ψηφοφορία και αναλύονται οι προκλήσεις που πρέπει να αντιμετωπίσουν αυτά τα συστήματα. Επίσης, γίνεται ανασκόπηση των συστημάτων ψηφοφορίας που χρησιμοποιούν το Blockchain και αναλύονται οι προκλήσεις και οι πλεονεκτήματα που σχετίζονται με αυτήν την τεχνολογία, καθώς και όλες οι μέθοδοι τις οποίες υιοθετούν.

- **Κεφάλαιο 4: Λειτουργία προτεινόμενου συστήματος**

  Σε αυτό το κεφάλαιο περιγράφεται η λειτουργία του προτεινόμενου συστήματος ψηφοφορίας με χρήση Blockchain. Αναλύονται τα βήματα και οι διαδικασίες που ακολουθούνται για την καταγραφή των ψήφων, την επιβεβαίωση της ταυτότητας των ψηφοφόρων και τον υπολογισμό των αποτελεσμάτων. Επίσης, αναλύεται η αρχιτεκτονική του συστήματος και οι τεχνολογίες που υιοθετήθηκαν από ήδη υπάρχοντα συστήματα.

- **Κεφάλαιο 5: Υλοποίηση προτεινόμενου συστήματος**

  Θα παρουσιαστεί η υλοποίηση του προτεινόμενου συστήματος ψηφοφορίας με χρήση Blockchain. Παρέχεται μια επισκόπηση του κώδικα έξυπνων συμβολαίων που χρησιμοποιείται και παρουσιάζονται στιγμιότυπα οθόνης από το χρήστη (UI), προκειμένου να γίνει κατανοητή η διαδικασία της ψηφοφορίας και η αλληλεπίδραση των χρηστών με το σύστημα.

- **Κεφάλαιο 6: Περιπτώσεις χρήσης και ανάλυση ασφάλειας του συστήματος που υλοποιήθηκε**

  Σε αυτό το κεφάλαιο παρουσιάζονται περιπτώσεις χρήσης του υλοποιημένου συστήματος ψηφοφορίας με χρήση Blockchain. Εξετάζονται οι προκλήσεις και οι απαιτήσεις ασφάλειας που πρέπει να αντιμετωπιστούν σε αυτές τις περιπτώσεις και γίνεται ανάλυση των μηχανισμών ασφάλειας που χρησιμοποιούνται στο σύστημα.

1.5 Δημοσιεύσεις

Στο πλαίσιο εκπόνησης της διπλωματικής αυτής εργασίας, πραγματοποιήθηκε μία παρουσίαση poster στο συνέδριο «5th Summit on Gender Equality in Computing» με τίτλο «A Blockchain-based Electronic Voting System: EtherVote» [SK23b], μία έκδοση του οποίου δημοσιεύθηκε στο arxiv [SK23a], όπως παρουσιάζονται παρακάτω:

- Achilleas Spanos and Ioanna Kantzavelou. A Blockchain-based Electronic Voting System: EtherVote. 2023. arXiv: 2307.10726 [cs.CR].
- Achilleas Spanos and Ioanna Kantzavelou. «Poster: A Blockchain-based Electronic Voting System: EtherVote». In: 5th Summit on Gender Equality in Computing (GEC), Greek ACM-W Chapter Event. GEC ’23. Athens, Greece, June 2023.

Κεφάλαιο 2

Θεωρητικό υπόβαθρο

Σε αυτό το κεφάλαιο θα οριστεί η τεχνολογία Blockchain, καθώς και κάθε τεχνολογική πτυχή της. Θα ξεκινήσουμε δίνοντας μια γενική εικόνα του τι είναι το Blockchain, και θα εμβαθύνουμε σε πιο ειδικές κατηγορίες και ορισμούς, απαραίτητους για να κατανοήσει κανείς τη συνέχεια της διπλωματικής εργασίας. Όλο το θεωρητικό υπόβαθρο, και οι τεχνολογίες που προσφέρει το Blockchain, πρέπει να γίνουν καλά κατανοητές, πριν προχωρήσουμε στα επόμενα κεφάλαια, και δούμε πως μπορεί μια τέτοια τεχνολογία να υιοθετηθεί σε καθημερινές εφαρμογές, αλλά πιο συγκεκριμένα σε εφαρμογή εθνικών εκλογών.

2.1 Τι είναι το Blockchain

Η τεχνολογία Blockchain, είναι μια νέας μορφής βάση δεδομένων, που προσφέρει διαφάνεια σε ανταλλαγές πληροφοριών εντός ενός δικτύου. Ένα blockchain αποθηκεύει δεδομένα σε μπλοκ που συνδέονται μεταξύ τους δημιουργώντας μια αλυσίδα. Τα δεδομένα αυτά είναι χρονικά συνδεδεμένα και συνεπή, που οφείλεται στο γεγονός ότι η διαγραφή ή τροποποίηση αυτής της αλυσίδας χωρίς συναίνεση από το δίκτυο είναι αδύνατη. Συνεπώς, η τεχνολογία Blockchain δημιουργεί ένα αμετάβλητο βιβλίο για την παρακολούθηση όλων των συναλλαγών που αποθηκεύονται σε αυτό. Η καινούρια αυτή τεχνολογία διαθέτει ενσωματωμένους μηχανισμούς που αποτρέπουν τις μη εξουσιοδοτημένες καταχωρίσεις συναλλαγών. [AWS-a]

2.1.1 Αρχιτεκτονική ενός Blockchain

Blocks

Με άλλα λόγια το Blockchain είναι μια συνεχώς αυξανόμενη λίστα εγγραφών, που ονομάζονται μπλοκ, τα οποία συνδέονται και ασφαλίζονται χρησιμοποιώντας κρυπτογραφία, δημιουργώντας μία αλυσίδα. Κάθε αλυσίδα αποτελείται από πολλαπλά μπλοκ, και κάθε μπλοκ έχει δύο βασικά στοιχεία:

- Τα δεδομένα (data) του block. Η πληροφορία δηλαδή που αποθηκεύεται σε κάθε block. Για την επικύρωση της ταυτότητας των συναλλαγών χρησιμοποιείται ασύμετρη κρυπτογραφία.
- Την κεφαλίδα του μπλοκ. Κάθε κεφαλίδα περιλαμβάνει μερικά βασικά στοιχεία [Zhe+17] :

Χαρακτηριστικά κεφαλίδας	Λειτουργία
Έκδοση μπλοκ	Υποδεικνύει το σύνολο κανόνων επικύρωσης μπλοκ που πρέπει να ακολουθηθεί.
Ρίζα δέντρου Markle	Η τιμή κατακερματισμού όλων των συναλλαγών στο μπλοκ.
Timestamp	Η τρέχουσα ώρα ως δευτερόλεπτα σε καθολική ώρα από τη 1η Ιανουαρίου 1970.
nBits	Όριο στόχου ενός έγκυρου κατακερματισμού μπλοκ.
Nonce	Το nonce είναι ένας ακέραιος αριθμός που δημιουργείται τυχαία, όταν δημιουργείται ένα block. Ένα πεδίο 4 byte, το οποίο συνήθως ξεκινά με 0 και αυξάνεται για κάθε υπολογισμό κατακερματισμού.
Κατακερματισμός γονικού μπλοκ	μια τιμή κατακερματισμού 256-bit που παραπέμπει στο προηγούμενο μπλοκ.

Πίνακας 1. Κεφαλίδα μπλοκ

2.1.2 Miner στο Blockchain

Μέσω μιας διαδικασίας που ονομάζεται εξόρυξη, γίνεται η δημιουργία νέων μπλοκ στο blockchain. Η διαδικασία της εξόρυξης είναι αρκετά απαιτητική σε πόρους, λόγω του μοναδικού nonce, τιμής κατακερματισμού, αλλά και τιμής κατακερματισμού του προηγούμενου μπλοκ.

Για τη δημιουργία ενός μπλοκ, οι miners, καλούνται να λύσουν ένα πολύπλοκο μαθηματικό πρόβλημα, με σκοπό την εύρεση του nonce, και συνεπώς τη δημιουργία μιας αποδεκτής τιμής κατακερματισμού. Το nonce είναι 32 bit και το hash είναι 256, επομένως υπάρχουν περίπου τέσσερα δισεκατομμύρια πιθανοί συνδυασμοί nonce-hash που πρέπει να εξορυχτούν πριν βρεθεί ο σωστός. Ο miner που θα καταφέρει να λύσει το γρίφο δηλαδή να βρει το ”χρυσό nonce” έχει τη δυνατότητα να προσθέσει το μπλοκ του στην αλυσίδα. Όλοι οι κόμβοι θα πρέπει να εγκρίνουν το block, με τη χρήση μηχανισμού συναίνεσης (θα αναφερθούν λεπτομερώς στη συνέχεια). Αν εγκριθεί από τη πλειοψηφία των κόμβων, το νέο block, θα προστεθεί στην αλυσίδα όλων των κόμβων ενός δικτύου blockchain.

Στην περίπτωση που τροποποιηθούν τα δεδομένα ενός μπλοκ εντός της αλυσίδας, απαιτείται εκ νέου εξόρυξη όλων των μπλοκ που το ακολουθούν σε αυτή τη χρονογραφημένη αλυσίδα. Επομένως, είναι εξαιρετικά δύσκολο να χειριστεί κανείς την τεχνολογία blockchain. Με την εξόρυξη ενός νέου μπλοκ, το οποίο θα πρέπει να γίνει αποδεχτό από όλους τους κόμβους του δικτύου, ο miner θα ανταμειφτεί οικονομικά. [DWB22]

2.1.3 Κρυπτογραφικές συναρτήσεις κατακερματισμού - Hash

Μια συνάρτηση κατακερματισμού είναι ένας μαθηματικός αλγόριθμος που λαμβάνει δεδομένα αυθαίρετου μήκους ως είσοδο και τα αντιστοιχίζει σε ένα κρυπτογραφημένο κείμενο σταθερού μήκους ως έξοδο. Αυτή η έξοδος ονομάζεται σύνοψη μηνύματος, ή τιμή κατακερματισμού (hash)[Mac21]

Ιδιότητες συναρτήσεων κατακερματισμού

Η διαδικασία κατακερματισμού όχι μόνο ασφαλίζει το μήνυμα αλλά κάνει και τον υπολογισμό εύκολο. Συμπιέζει το μήνυμα σε κατακερματισμό που είναι αποτελεσματικό τόσο για υπολο-

Σχήμα 1. Κρυπτογραφική συνάρτηση κατακερματισμού

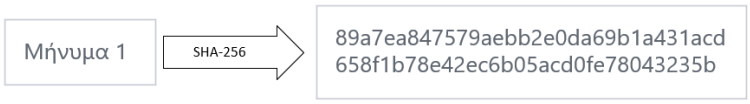
γισμούς όσο και για επικοινωνία. Οι συναρτήσεις κατακερματισμού έχουν τις παρακάτω ιδιότητες [ngr22]:

1. **Ντετερμινιστική**: Μια συνάρτηση κατακερματισμού πρέπει να είναι ντετερμινιστική, πράγμα που σημαίνει ότι για κάθε δεδομένη είσοδο μια συνάρτηση κατακερματισμού πρέπει πάντα να δίνει το ίδιο αποτέλεσμα - Hash.

2. **Εφέ Χιονοστιβάδας (Avalanche Effect)**: ακόμα και αν αλλάξει ένα μόνο γράμμα, ο κατακερματισμός αλλάζει δραματικά.

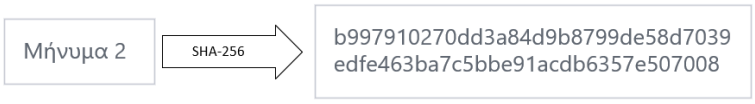
   Για παράδειγμα:

   - Όπως βλέπουμε στη συνέχεια η κρυπτογράφηση τη μηνύματος "Μήνυμα 1" με αλγόριθμο κατακερματισμού δίνει το παρακάτω Hash.



Σχήμα 2. Υπολογισμός Hash πρώτου μηνύματος

   - Όμως αν πραγματοποιηθεί μια μικρή αλλαγή στο μήνυμα που κρυπτογραφείται, δηλαδή αλλάξουμε τη φράση εισόδου σε "Μήνυμα 2", το Hash είναι σημαντικά διαφορετικό από το προηγούμενο μήνυμα.



Σχήμα 3. Υπολογισμός Hash δεύτερου μηνύματος

3. Οι συναρτήσεις κατακερματισμού είναι **μονόδρομες**. Για ένα δεδομένο μήνυμα εισόδου X, είναι εύκολο να υπολογιστεί η έξοδος H(X)=D. Αντιθέτως, χρησιμοποιώντας το D, δεν μπορεί κανείς να βρει το X. Υπάρχει μια μικρή πιθανότητα να λάβετε H(X)=H(Y). όπου το X δεν είναι ίσο με το Y. Ωστόσο, είναι δύσκολο να βρείτε τα X και Y χρησιμοποιώντας τον ίδιο κατακερματισμό.

   Για παράδειγμα, εάν μια συνάρτηση κατακερματισμού παράγει N bit εξόδου. Ένας εισβολέας πρέπει να υπολογίσει $2^{N/2}$ λειτουργίες κατακερματισμού σε τυχαία είσοδο για να αναζητήσει τη δεύτερη αντιστοίχιση της εξόδου.

   Ως εκ τούτου, για κάθε 256 συναρτήσεις κατακερματισμού, ο εισβολέας πρέπει να υπολογίσει 2^{128} λειτουργίες κατακερματισμού. Ακόμα κι αν ένας υπολογισμός διαρκεί 1μs, θα χρειαστούν περίπου 10^{25} χρόνια για να ταιριάζει με την έξοδο.

4. **Ανθεκτικό σε συγκρούσεις**: Γνωρίζοντας δύο μηνύματα μ1 και μ2, είναι σχεδόν αδύνατο να βρεθεί τιμή κατακερματισμού έτσι ώστε hash(μ1) = hash(μ2).

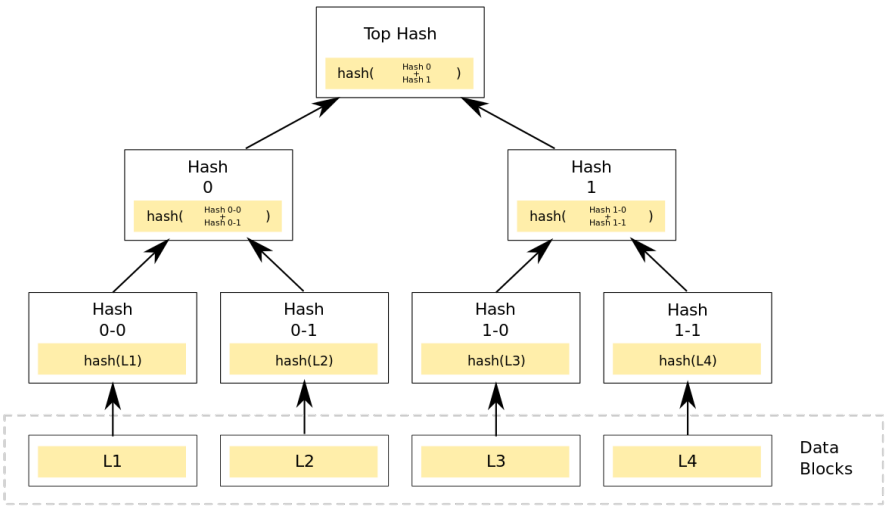
5. **Αντίσταση προ εικόνας**: Δεδομένης μιας τιμής κατακερματισμού X, είναι σχεδόν αδύνατο να βρεθεί μήνυμα μ έτσι ώστε X=hash(μ).

6. **Απόκρυψη πληροφοριών / Δεύτερη αντίσταση προ εικόνας**: Δεδομένου ότι η σύνοψη ενός μηνύματος είναι μη αναστρέψιμη, είναι σχεδόν αδύνατο να βρεθεί ο ίδιος κατακερματισμός για διαφορετικά μηνύματα. Επομένως, ο μόνος τρόπος να επαληθευτεί ένα κατακερματισμένο μήνυμα, είναι με το κατακερματισμό του πιθανού μηνύματος, και με τον έλεγχο ταιριάσματος των δύο Hash.

Merkle tree

Σύμφωνα με το [S22] το Merkle tree είναι ένα δέντρο κατακερματισμού, όπου κάθε κόμβος / φύλλο του δέντρου κρυπτογραφείται με τον κρυπτογραφικό κατακερματισμό ενός μπλοκ δεδομένων. Κάθε κόμβος που δεν είναι φύλλο του δέντρου κρυπτογραφείται με τον κρυπτογραφικό κατακερματισμό των κατακερματισμών των κόμβων-παιδιών τους. Η πλειοψηφία των εφαρμογών του Merkle tree είναι δυαδικές (κάθε κόμβος έχει δύο κόμβους - παιδιά), αλλά μπορούν επίσης να έχουν πολλούς περισσότερους θυγατρικούς κόμβους. Επιτρέπει τη γρήγορη και ασφαλή επαλήθευση των περιεχομένων σε μεγάλα σύνολα δεδομένων και επαληθεύει τη συνέπεια και το περιεχόμενο τους.

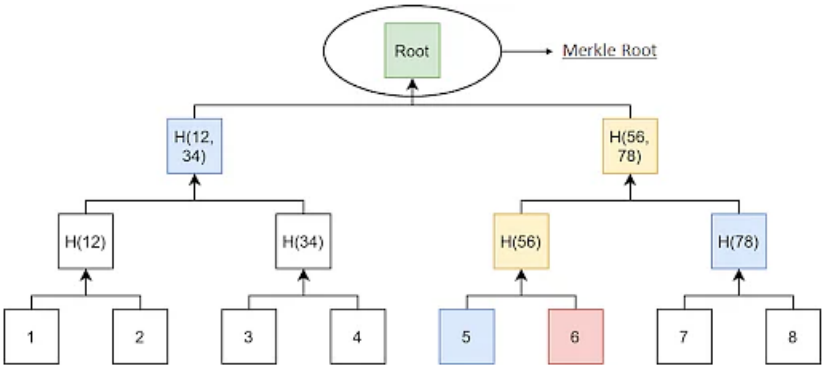
Συνοψίζοντας, το Merkle tree, είναι ένα δυαδικό δέντρο, με τη τιμή κατακερματισμού κάθε κόμβου να είναι η τιμή κατακερματισμού των κόμβων-παιδιών του.



Σχήμα 4. Merkle tree / Δέντρο κατακερματισμού

Ρίζα Merkle

Σύμφωνα με το [S22] η ρίζα Merkle είναι μια μαθηματική μέθοδος επιβεβαίωσης των ενεργειών σε ένα Merkle δέντρο. Συμμετέχει στη διασφάλιση της ακεραιότητας των δεδομένων των μπλοκ σε ένα κατανεμημένο δίκτυο.



Σχήμα 5. Ρίζα δέντρου

Κατακερματισμός στο Blockchain

Υπάρχουν πολλοί λόγοι για τους οποίους το Blockchain χρησιμοποιεί τις συναρτήσεις κατακερματισμού [ngr22]:

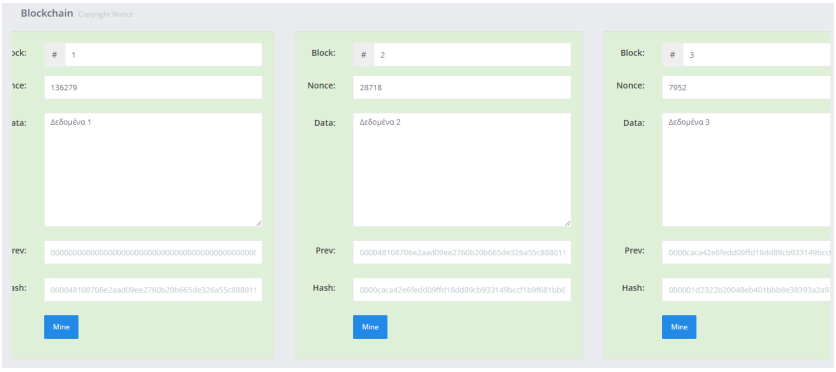
- Merkle Tree: Χρησιμοποιεί τις συναρτήσεις κατακερματισμού ώστε να αποφύγει τη δημιουργία δύο δέντρων Merkle, με την ίδια τιμή κατακερματισμού ρίζας του δέντρου.
- Συναίνεση απόδειξης εργασίας (Proof of Work) : Αυτός ο αλγόριθμος θα αναλυθεί στη συνέχεια του κεφαλαίου.
- Ψηφιακές υπογραφές: διασφαλίζουν την ακεραιότητα των δεδομένων και χρησιμοποιούνται για έλεγχο ταυτότητας για συναλλαγές blockchain.
- Η αλυσίδα των μπλοκ: Κάθε κεφαλίδα μπλοκ σε ένα μπλοκ στην αλυσίδα μπλοκ περιέχει τον κατακερματισμό της προηγούμενης κεφαλίδας μπλοκ.

2.1.4 Αμεταβλητότητα

Η ιδιότητα που καθιστά τη τεχνολογία Blockchain ως βάση δεδομένων, τόσο διαφορετική και πολλά υποσχόμενη, είναι η αμεταβλητότητα των δεδομένων που προσφέρει. Κάθε μπλοκ περιέχει τη τιμή κατακερματισμού του εαυτού του, αλλά και του προηγούμενου μπλοκ. Αυτό, με τη σειρά του, διασφαλίζει ότι τα μπλοκ είναι αναδρομικά συζευγμένα. Αυτή η λειτουργία είναι που διασφαλίζει ότι κανείς δεν μπορεί να παρέμβει στο σύστημα ή να αλλάξει τα ήδη αποθηκευμένα δεδομένα σε κάθε μπλοκ, καθώς θα άλλαζε η τιμή κατακερματισμού του μπλοκ, με αποτέλεσμα την αλλαγή δεδομένων εκατοντάδων κόμβων.

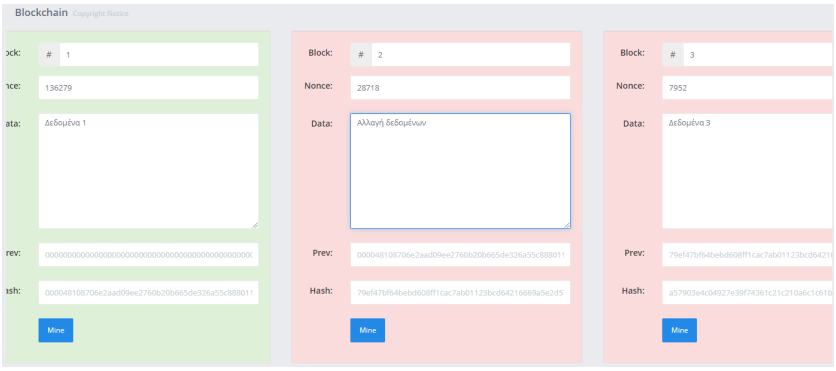
Στο Blockchain tools μπορεί κανείς να πειραματιστεί και να κατανοήσει καλύτερα τις λειτουργίες που προσφέρει το blockchain, αλλά και τα hashes του προηγούμενου κεφαλαίου, προσφέροντας ένα εξαιρετικό περιβάλλον προσομοίωσης. Με τη χρήση αυτού του εργαλείου έγιναν οι παρακάτω εικόνες.

Στην παρακάτω εικόνα βλέπουμε τα blocks ενός blockchain, και τις πληροφορίες που αυτά περιλαμβάνουν. Κάθε μπλοκ, περιλαμβάνει και το hash του προηγούμενου μπλοκ, δημιουργώντας μία αλυσίδα.



Σχήμα 6. Blockchain

Όπως αναφέρθηκε και παραπάνω η τροποποίηση των δεδομένων οποιουδήποτε μπλοκ, έχει ως αποτέλεσμα την αλλαγή της τιμής κατακερματισμού-hash του μπλοκ, άρα και την αλλαγή δεδομένων όλων των μετέπειτα κόμβων.

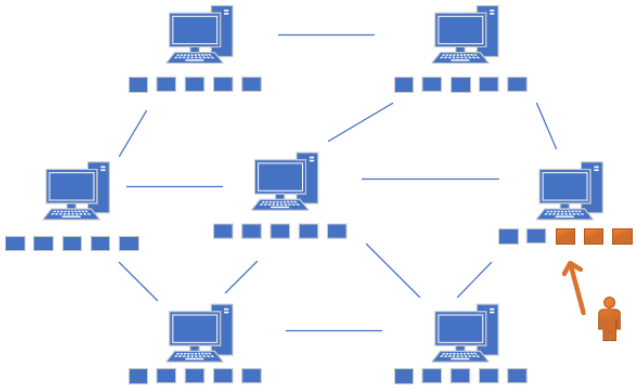


Σχήμα 7. Τροποποίηση δεδομένων δεύτερου μπλοκ

2.1.5 Κατανεμημένο δίκτυο

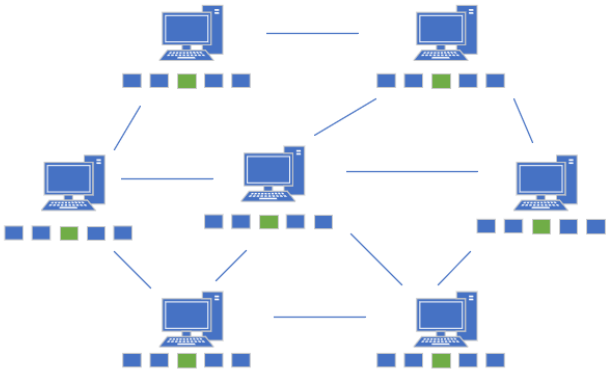
Το blockchain είναι ένα κατανεμημένο δίκτυο. Διαθέτει τεχνολογία peer-to-peer (P2P), η οποία επιτρέπει στους συμμετέχοντες στο δίκτυο να πραγματοποιούν συναλλαγές χωρίς να χρειάζονται μεσάζοντες, ή κεντρικό διακομιστή. Κάθε υπολογιστής - μέλος του δικτύου διατηρεί ένα πλήρες αντίγραφο του blockchain και επαληθεύει την αυθεντικότητά του με άλλους κόμβους για να εγγυηθεί ότι τα δεδομένα είναι ακριβή. Ένας κόμβος μπορεί να εκτελεί ταυτόχρονα τις λειτουργίες κοινής χρήσης και λήψης, γεγονός που εξηγεί την ταχύτητα, την ασφάλεια και την αποτελεσματικότητα του δικτύου [Sha22].

Στην περίπτωση τροποποίησης δεδομένων σε κάποιο μπλοκ, όπως προαναφέραμε αλλάζει το hash και των επόμενων μπλοκ.



Σχήμα 8. Τροποποίηση ενός μπλοκ σε έναν κόμβο

Μέσω του κατανεμημένου δικτύου, γίνεται συνεχώς έλεγχος μεταξύ των κόμβων του δικτύου. Επομένως, αμέσως η αλλαγή δεδομένων σε ένα κόμβο θα γίνει αισθητή στους υπόλοιπους κόμβους του δικτύου. Λόγω αυτής της συνεχής επικοινωνίας που παρέχεται στα κατανεμημένα συστήματα, γίνεται η αποκατάσταση των αλλαγμένων μπλοκ στον επιτιθέμενο κόμβο.



Σχήμα 9. Επαναφορά των μπλοκ σε ένα κόμβο

Προκλήσεις αμετάβλητης αλυσίδας Blockchain

Παρότι ο μηχανισμός που προσφέρει αυτή η τεχνολογία είναι αρκετά ισχυρός υπάρχουν μερικές προκλήσεις.

- **Επίθεση 51%**: Είναι μια επίθεση σε ένα blockchain από μια ομάδα από miners που ελέγχουν περισσότερο από το 50% του ποσοστού εξόρυξης του δικτύου. Η κατοχή του 51% των κόμβων στο δίκτυο δίνει στα μέρη που ελέγχουν τη δύναμη να αλλάξουν το blockchain, τροποποιώντας τα δεδομένα, διαγράφοντας μπλοκ, αντιστρέφοντας ολοκληρωμένες συναλλαγές κοκ. [Fra22a].

- **Κβαντική Υπολογιστική**: Μια άλλη σημαντική πρόκληση στον μηχανισμό blockchain είναι ο κβαντικός υπολογισμός. Απειλεί την αμετάβλητη φύση του blockchain. Αρκετές με-

λέτες έχουν αναφέρει, ότι ο κβαντικός υπολογισμός θα μπορέσει να ανατρέψει το δημόσιο κλειδί του δικτύου, το οποίο με τη σειρά του είναι σε θέση να βρει τα ιδιωτικά κλειδιά για την είσοδο στο σύστημα [Cha23].

2.1.6 Byzantine Fault Tolerance

Πρόβλημα βυζαντινών στρατηγών

Το πρόβλημα των βυζαντινών στρατηγών δημιουργήθηκε το 1982 από τους Leslie Lamport, Robert Shostak, και Marshall Pease. Είναι ένα άλυτο μέχρι σήμερα πρόβλημα το οποίο μας βοηθά να κατανοήσουμε τη σημαντικότητα του blockchain. Μπορεί να εξηγηθεί ως εξής:

" Φανταστείτε ότι πολλές μεραρχίες του βυζαντινού στρατού είναι στρατοπεδευμένες έξω από μια εχθρική πόλη, και κάθε τμήμα διοικείται από τον δικό της στρατηγό. Οι στρατηγοί μπορούν να επικοινωνούν μεταξύ τους μόνο μέσω αγγελιοφόρου. Αφού παρατηρήσουν τον εχθρό, πρέπει να αποφασίσουν για ένα κοινό σχέδιο δράσης. Ωστόσο, ορισμένοι από τους στρατηγούς μπορεί να είναι προδότες, προσπαθώντας να εμποδίσουν τους πιστούς στρατηγούς να καταλήξουν σε συμφωνία. Οι στρατηγοί πρέπει να αποφασίσουν πότε θα επιτεθούν στην πόλη, αλλά χρειάζονται μια ισχυρή πλειοψηφία του στρατού τους για να επιτεθούν ταυτόχρονα. Οι στρατηγοί πρέπει να έχουν έναν αλγόριθμο που να εγγυάται ότι (α) όλοι οι πιστοί στρατηγοί αποφασίζουν για το ίδιο σχέδιο δράσης και (β) ένας μικρός αριθμός προδοτών δεν μπορεί να κάνει τους πιστούς στρατηγούς να υιοθετήσουν ένα κακό σχέδιο. Οι πιστοί στρατηγοί θα κάνουν όλοι ότι λέει ο αλγόριθμος, αλλά οι προδότες μπορεί να κάνουν ότι θέλουν. Ο αλγόριθμος πρέπει να εγγυάται τη συνθήκη (α) ανεξάρτητα από το τι κάνουν οι προδότες. Οι πιστοί στρατηγοί δεν πρέπει μόνο να καταλήξουν σε συμφωνία, αλλά θα πρέπει να συμφωνήσουν σε ένα λογικό σχέδιο. " [LSP19]

Byzantine Fault Tolerance

Το Byzantine Fault Tolerance (BFT) είναι το χαρακτηριστικό ενός κατανεμημένου δικτύου για την επίτευξη συναίνεσης. Ο στόχος αυτού του μηχανισμού είναι η προστασία από αστοχίες του συστήματος, εφαρμόζοντάς συλλογική λήψη αποφάσεων. Μέσω αυτής της μεθόδου λήψης αποφάσεων μειώνεται η επιρροή των ελαττωματικών κόμβων [Hoo22]. Για να εξασφαλίσουν την επιτυχία της ομάδας των στρατηγών, χρειάζονται έναν αλγόριθμο που θα μπορούσε να συμμορφώνεται με τις ακόλουθες προϋποθέσεις [Him22]:

- Όλοι οι στρατηγοί πρέπει να συμφωνήσουν για την επόμενη δράση του σχεδίου.
- Οι στρατηγοί πρέπει να είναι αξιόπιστοι και πιστοί στο σύστημα.
- Οι στρατηγοί δεν πρέπει να επηρεαστούν για να γίνουν προδότες του δικτύου.
- Πρέπει να ακολουθήσουν τον αλγόριθμο του συστήματος.
- Η ομάδα των στρατηγών πρέπει να καταλήξει σε συναίνεση ή απόφαση, ανεξάρτητα από τις ενέργειες των προδοτών.
- Το σύστημα ή το δίκτυο δεν πρέπει να οδηγεί σε επίθεση κατά 51% σε οποιοδήποτε σημείο δράσης.

Πρακτική βυζαντινή ανοχή σφαλμάτων

Η πρακτική βυζαντινή ανοχή σφαλμάτων (Practical Byzantine Fault Tolerance) είναι ένα σύστημα που έχει έναν πρωτεύων και πολλούς δευτερεύοντες κόμβους. Η συνεργασία αυτών των κόμβων οδηγεί στη συναίνεση, λύνοντας το πρόβλημα των Βυζαντινών Στρατηγών.

Λειτουργεί ως εξής [Dal21]:

1. Γίνεται αίτημα στο πρωτεύοντα κόμβο.
2. Ο πρωτεύων κόμβος στέλνει το αίτημα στους υπόλοιπους (δευτερεύοντες κόμβους).
3. Γίνεται επεξεργασία του αιτήματος, παροχή της υπηρεσίας και απαντούν σε εκείνον που έστειλε το αίτημα.
4. Ο κόμβος που έστειλε το αίτημα περιμένει μέχρι να λάβει την ίδια απάντηση από μ+1 κόμβους, με το μ να είναι ο μέγιστος αριθμός κακόβουλων κόμβων που επιτρέπει το σύστημα.
5. Ο μέγιστος αριθμός κακόβουλων κόμβων είναι πάντα μικρότερος από το ένα τρίτο του συνόλου των κόμβων του συστήματος.

2.1.7 Μηχανισμοί συναίνεσης

Οι μηχανισμοί συναίνεσης στο blockchain χρησιμοποιούνται, έτσι ώστε όλοι οι κόμβοι του δικτύου, να συμφωνούν στη κατάσταση του blockchain, και να επιτρέπουν την ασφαλή ενημέρωση μιας κατανεμημένης κοινής κατάστασης. Η επίτευξη συναίνεσης σε ένα κατανεμημένο σύστημα παρουσιάζει πολλές προκλήσεις, διότι οι αλγόριθμοι συναίνεσης είναι ανθεκτικοί σε αστοχίες κόμβων, διαχωρισμούς δικτύου, καθυστερήσεις μηνυμάτων, μηνύματα που φτάνουν εκτός σειράς και κατεστραμμένα μηνύματα [BA17].

Proof of Work - PoW

Περισσότερο από το 90% του κεφαλαίου της αγοράς των κρυπτονομισμάτων, αντιπροσωπεύονται από blockchain, που υποστηρίζουν τον μηχανισμό συναίνεσης Proof of Work (PoW). Στον μηχανισμό συναίνεσης Proof-of-Work, οι miners ανταγωνίζονται για την ανταμοιβή μπλοκ προσπαθώντας να μαντέψουν την τιμή nonce του μπλοκ, μέχρι τη στιγμή που θα βρεθεί αυτή η τιμή και θα δώσει στον κατακερματισμό του μπλοκ τα απαραίτητα μηδενικά bit [Ga16].

Ο μηχανισμός αυτός λειτουργεί ως εξής. Για να δημιουργηθεί το επόμενο μπλοκ, κάθε κόμβος πρέπει να λύσει ένα κρυπτογραφικό πρόβλημα. Ο πρώτος miner που βρίσκει μια λύση σε αυτό το περίπλοκο πρόβλημα, γίνεται ο υπεύθυνος για το κλείσιμο και την παράδοση του μπλοκ. Επομένως, όσο πιο γρήγορα λύσει το πρόβλημα, τόσο περισσότερες ευκαιρίες έχει για τη δημιουργία του επόμενου μπλοκ. Ο ρόλος των miner είναι διπλός. Όταν οι υπολογιστές λύνουν το μαθηματικό πρόβλημα, παράγουν νέα νομίσματα και με αυτό το τρόπο η πληρωμή στο δίκτυο γίνεται αξιόπιστη, αφού επαληθευτούν οι πληροφορίες των συναλλαγών του. Ο δημιουργός του μπλοκ λαμβάνει μια ανταμοιβή. Αυτή η ανταμοιβή είναι το κίνητρο που παρέχει το δίκτυο για να κρατήσει τους κόμβους "πιστούς".

Αυτός ο μηχανισμός όμως παρουσιάζει μερικά σοβαρά μειονεκτήματα. Λόγω της ανταμοιβής του miner που θα βρει το επόμενο μπλοκ, οι miners θα μπορούσαν να ενώσουν την ισχύ τους, δημιουργώντας τα λεγόμενα mining pools. Με τον διαμοιρασμό της υπολογιστικής ισχύος μοιράζεται και το κέρδος από το μπλοκ που εξορύσσουν. Εάν μία από αυτές τις ομάδες εξόρυξης μπορούσε να φτάσει το 51% της συνολικής ισχύος του δικτύου, όλα όσα είπαμε για την αποκέντρωση του blockchain δε θα ισχύουν [Lep+20].

Proof of Stake - PoS

Ο όρος "Stake" ορίζεται τον αριθμό των tokens που στοιχηματίζει ένας χρήστης προκειμένου να συμμετάσχει στη διαδικασία επικύρωσης ενός νέου μπλοκ. Το πρωτόκολλο είναι απλό. Ένας κόμβος συμμετέχει στη διαδικασία συναίνεσης αναλογικά με τα πονταρίσματα που στοιχηματίζει. Όσο περισσότερο στοιχηματίζει, τόσο μεγαλύτερη επιρροή έχει στην επικύρωση του επόμενου μπλοκ. Οι κόμβοι δε χρειάζεται να ανταγωνίζονται μεταξύ τους για την επίλυση του δύσκολου

κρυπτογραφικού προβλήματος, κάνοντας τη διαδικασία εξόρυξης πιο αποτελεσματική. Ως κίνητρο για να κρατήσει τους κόμβους πιστούς, ο δημιουργός λαμβάνει μια ανταμοιβή για τη διάδοση του μπλοκ [Lep+20]. Σύμφωνα με το [BG17], υπάρχουν δύο τύποι σχεδιασμού PoS:

- Απόδειξη στοιχήματος με βάση το blockchain. Ανά περιόδους, εκλέγεται ένας δημιουργός και παραδίδει το επόμενο μπλοκ που θα προστεθεί στην αλυσίδα.
- "Consortium consensus—Byzantine Fault Tolerance (BFT)" πρωτόκολλο. Ένας κόμβος εκλέγεται και εκτελείται μια διαδικασία ψηφοφορίας για να βρεθεί η συναίνεση. Στη διαδικασία ψηφοφορίας, κάθε κόμβος μετράει αναλογικά με το ποντάρισμα που στοιχηματίζει.

Proof-of-Authority - PoA

Ο αλγόριθμος συναίνεσης Proof-of-Authority βασίζεται σε αξιόπιστους κόμβους που αναγνωρίζονται ως αρχές. Αυτοί οι κόμβοι διαθέτουν ένα μοναδικό αναγνωριστικό θεωρώντας τους μισούς ειλικρινείς. Η συναίνεση επιτυγχάνεται με την εναλλαγή εξόρυξης. Με αυτό το τρόπο κατανέμεται δίκαια η ευθύνη της δημιουργίας μπλοκ [Ang+18].

Proof-of-Activity - POA

Ο μηχανισμός συναίνεσης Proof-of-Activity είναι ένας υβριδικός μηχανισμός που συνδυάζει τους μηχανισμούς συναίνεσης Proof-of-Work και Proof-of-Stake. Οι miners προσπαθούν να βρουν το nonce, με σκοπό τη χρηματική ανταμοιβή. Όσο περισσότερη υπολογιστική ισχύ έχει ένας miner τόσο μεγαλύτερες πιθανότητες υπάρχουν για να βρει ένα μπλοκ. Η επικύρωση των συναλλαγών γίνεται με τη χρήση υπογραφών, με το PoS να αναλαμβάνει [Ben+14].

Έτσι ένας επιτιθέμενος για να ελέγχει το δίκτυο, θα πρέπει να έχει πάνω από το 51% των κόμβων του δικτύου, αλλά και ένα πολύ μεγάλο ποσό από tokens, συνδυάζοντας τους μηχανισμούς του PoW και PoS.

2.2 Είδη δικτύων Blockchain

Ένα blockchain μπορεί να ανήκει σε διάφορες κατηγορίες. Με βάση τη φύση της προσβασιμότητας των δεδομένων μπορεί να είναι δημόσιο, ιδιωτικό, δίκτυο κοινοπραξίας, ή επιτρεπόμενο (permitioned) δίκτυο [SY19].

2.2.1 Δημόσιο Δίκτυο

Ένα δημόσιο blockchain είναι προσβάσιμο από όλο το κόσμο. Κάθε ένας μπορεί να στείλει συναλλαγές και να συμμετέχει στη διαδικασία συναίνεσης, η οποία καθορίζει ποια μπλοκ προστίθενται στην αλυσίδα και ποια είναι η τρέχουσα κατάσταση. Λόγω της εύκολης πρόσβασης, τα δημόσια blockchain υιοθετούνται πό πολλούς οργανισμούς, καθώς δεν απαιτείται επαλήθευση από τρίτους [Coi].

2.2.2 Ιδιωτικό Δίκτυο

Οι ιδιωτικές αλυσίδες μπλοκ, γνωστές και ως διαχειριζόμενες αλυσίδες μπλοκ, είναι επιτρεπόμενες αλυσίδες μπλοκ που διαχειρίζονται από μία μόνο οντότητα. Αυτή η οντότητα λαμβάνει αποφάσεις, για το ποιος μπορεί να είναι ένας κόμβος.

Επιπλέον, η οντότητα αυτή εκχωρεί τα δικαιώματα κάθε κόμβου για την εκτέλεση συναρτήσεων, που μπορεί και να διαφέρουν. Λόγω της περιορισμένης πρόσβασης σε αυτές τις αλυσίδες, όπως είναι λογικό, είναι μόνο, εν μέρει αποκεντρωμένες.

Στο άρθρο [Coi] παρουσιάζεται π παρακάτω πίνακας σύγκρισης δημόσιου και ιδιωτικού δικτύου.

	Δημόσιο blockchain	**Ιδιωτικό** blockchain
Εξουσία	Αποκεντρωμένη	Δυνατότητα αποκεντρωμένης
Πρόσβαση	Δημόσια, προσβάσιμη από όλους	Είσοδος με πρόσκληση λόγω επιτρεπόμενου δικτύου
Συναλλαγές/s	Λιγότερες	Περισσότερες
Ταχύτητα	Αργό	Γρήγορο
Κατανάλωση ενέργειας	Υψηλή	Χαμηλή
Ρίσκα	Υψηλοί κίνδυνοι επιθέσεων, απάτης	Κακόβουλοι κόμβοι δε μπορούν να επιτεθούν
Κατανάλωση ενέργειας	Εξαιρετικά ασφαλής	Λιγότερο ασφαλής

Πίνακας 2. Δημόσιο - Ιδιωτικό δίκτυο

2.2.3 Δίκτυο κοινοπραξίας

Τα blockchains κοινοπραξίας, σε αντίθεση με τα ιδιωτικά blockchain, είναι επιτρεπόμενα blockchains που διαχειρίζονται μια κοινοπραξία οργανισμών και όχι από ένα μεμονωμένο ίδρυμα. Ως αποτέλεσμα, τα blockchain κοινοπραξιών έχουν μεγαλύτερη αποκέντρωση από τα ιδιωτικά blockchain, με αποτέλεσμα αυξημένη ασφάλεια.

Από την άλλη πλευρά, η σύσταση κοινοπραξιών μπορεί να είναι δύσκολη επειδή απαιτεί τη συνεργασία μεταξύ πολλών επιχειρήσεων. Επειδή οι πληροφορίες από τα ελεγμένα μπλοκ είναι κρυμμένα από το κοινό, η αλυσίδα μπλοκ της κοινοπραξίας έχει υψηλό επίπεδο απορρήτου. Όποιος είναι μέλος αυτού του blockchain, ωστόσο, μπορεί να έχει πρόσβαση. Το blockchain κοινοπραξίας, σε αντίθεση με ένα δημόσιο blockchain, δεν έχει τέλη συναλλαγών [Coi].

2.2.4 Επιτρεπόμενο δίκτυο

Ένα επιτρεπόμενο δίκτυο blockchain δημιουργείται συνήθως από επιχειρήσεις που δημιουργούν ένα ιδιωτικό blockchain. Αξίζει να σημειωθεί ότι τα δημόσια δίκτυα blockchain μπορούν επίσης να επιτρέπονται. Αυτό περιορίζει ποιος είναι εξουσιοδοτημένος να συμμετέχει στο δίκτυο και ποιες συναλλαγές μπορούν να κάνουν. Για να συμμετάσχουν κάθε κόμβος, πρέπει πρώτα να λάβει πρόσκληση ή εξουσιοδότηση.

Τα επιτρεπόμενα δίκτυα blockchain παρέχουν μια αποκεντρωμένη πλατφόρμα, η οποία σημαίνει ότι τα δεδομένα δεν αποθηκεύονται σε κεντρική βάση και ότι ο καθένας μπορεί να έχει πρόσβαση σε αυτά ανά πάσα στιγμή και από οποιαδήποτε τοποθεσία. Διασφαλίζει ότι όλες οι εγγραφές έχουν αμετάβλητες υπογραφές. Ολόκληρο το σύστημα είναι ασφαλές και τα δεδομένα είναι ασφαλή επειδή όλες οι ανταλλαγές πληροφοριών και οι συναλλαγές κρυπτογραφούνται.

Επιπλέον, οι miners και οι συμμετέχοντες του δικτύου παραμένουν ανώνυμοι. Ένα άλλο πλεονέκτημα του επιτρεπόμενου blockchain είναι η διαφάνεια. Όλοι μπορούν να δουν όλα τα δεδομένα και τις πληροφορίες. Ωστόσο, αυτό το όφελος απέτυχε, προκαλώντας ανησυχίες σχετικά με την ασφάλεια των δεδομένων στο blockchain χωρίς άδεια. Δε χρειάζεται να αποδείξει κανείς την ταυτότητά του στο επιτρεπόμενο blockchain [Coi].

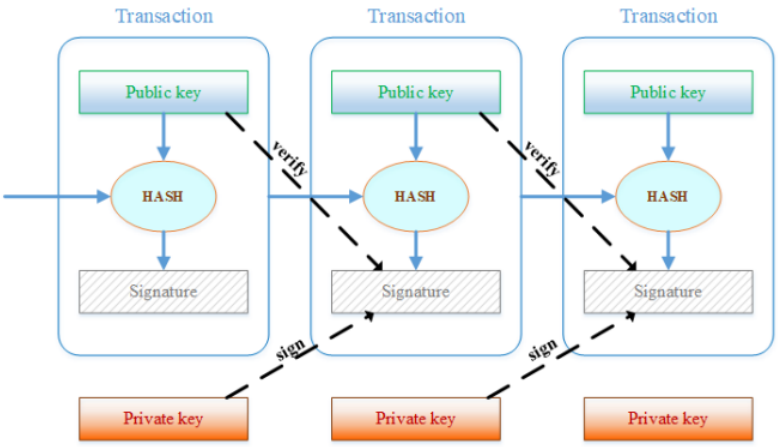
2.3 Δίκτυο Bitcoin

Σε αυτή την ενότητα,θα γίνει μια γενική επισκόπηση σχετικά με το δίκτυο Bitcoin. Εστιάζουμε στο σύστημα και το πρωτόκολλό του, και ιδίως για τον τρόπο διάδοσης των πληροφοριών στο δίκτυο. Η τεχνολογία blockchain αποκαλύφθηκε για πρώτη φορά από τον Satoshi Nakamoto στην εργασία του [Nak08].

2.3.1 Βασικά στοιχεία δικτύου Bitcoin

Ο Nakamoto πρότεινε ένα κατανεμημένο P2P σύστημα που χρησιμεύει ως γεννήτρια της υπολογιστικής απόδειξης της χρονολογικής σειρά συναλλαγών [Nak08]. Στο Bitcoin διαδίδονται δύο διαφορετικοί τύποι πληροφοριών: συναλλαγές και μπλοκ. Οι συναλλαγές είναι που επιτρέπουν τη μεταφορά του νομίσματος (αλυσίδα ψηφιακών υπογραφών), ενώ τα μπλοκ χρησιμοποιούνται για τον συγχρονισμό της κατάστασης σε όλους τους κόμβους του δικτύου[DW13]. Με τον όρο συναλλαγή εννοούμε το σύνολο ενός ψηφιακά υπογεγραμμένου κατακερματισμού της προηγούμενης συναλλαγής και του δημόσιου κλειδιού του επόμενου κατόχου. Η υπογραφή αυτής της συναλλαγής γίνεται με τη χρήση ιδιωτικού κλειδιού, ενώ η επαλήθευσή της με τη χρήση του δημοσίου.

Η παρακάτω εικόνα είναι από την ερευνητική εργασία [VJR18], και φαίνεται η δομή της συναλλαγής στο δίκτυο Bitcoin.



Σχήμα 10. Συναλλαγή στο δίκτυο Bitcoin

Το Bitcoin μπορεί να χαρακτηριστεί ως " σύστημα μετάβασης κατάστασης". Αποτελείτε από τη κατάσταση που βρίσκεται το δίκτυο και τη συνάρτηση μετάβασης κατάστασης. Με άλλα λόγια απεικονίζεται η κατάσταση ιδιοκτησίας όλων των υπαρχόντων bitcoin και περιέχει μια συνάρτηση μετάβασης κατάστασης, με τη μορφή συναλλαγής. Η έξοδος της συνάρτησης μετάβασης κατάστασης είναι μια νέα κατάσταση. Τα αποτελέσματα αυτής της διαδικασίας είναι αλλαγές κατάστασης του αποστολέα και του παραλήπτη εάν ο αποστολέας έχει αρκετά bitcoin για να κάνει μια συναλλαγή ή ένα σφάλμα στην αντίθετη περίπτωση [VJR18].

2.3.2 Πρωτόκολλο επικοινωνίας Bitcoin

Όλοι οι χρήστες-κάτοχοι Bitcoin ανήκουν σε ένα κατανεμημένο δίκτυο. Συνεπώς, δεν υπάρχει κάποιος κεντρικός κόμβος για τη λήψη αποφάσεων ολόκληρου του δικτύου. Κάθε κόμβος αποφασίζει μόνος του για την υπηρεσία θα παρέχει στο υπόλοιπο δίκτυο.

Ένας κόμβος που θέλει να συνδεθεί στο δίκτυο για πρώτη φορά πρέπει να συνδεθεί με κάποιους ειδικούς ομότιμους που ονομάζονται “seeds“. Αυτοί παρέχουν τη λίστα των ομότιμων τους. Όλοι οι πελάτες που περιλαμβάνονται επιλέγονται τυχαία και η λίστα μπορεί να περιέχει έως και χίλιους κόμβους. Μετά την ανάκτηση των λιστών των ομότιμων, ένας κόμβος επιλέγει μεταξύ τους μέχρι να φτάσει τον προεπιλεγμένο μέγιστο αριθμό συνδέσεων (συνήθως από 8 έως 126) [Pap+18].

2.3.3 Συναλλαγές στο Bitcoin

Κάθε συναλλαγή έχει τη μορφή μιας τιμής κατακερματισμού. Αυτή η τιμή κατακερματισμού, περιλαμβάνει το αναγνωριστικό της συναλλαγής και μερικές εισόδους και εξόδους. Η συναλλαγή στο Bitcoin μπορεί να έχει N αριθμό εισόδων, αλλά μόνο έως δύο εξόδους.

Η χρήση πολλών εισόδων ωφελεί στο συνδυασμό μικρότερων ποσοτήτων κερμάτων από έναν αποστολέα σε έναν παραλήπτη [Nak08]. Όλοι οι κόμβοι που είναι μέλη του δικτύου έχουν ένα πλήρες αντίγραφο του Blockchain, το οποίο απεικονίζει όλες τις συναλλαγές και ιδιοκτησίες στο δίκτυο. Οι συναλλαγές νομισμάτων από έναν λογαριασμό σε έναν άλλον, γίνονται δημόσια. Αφού γίνει η δήλωση αποστολής από τον αποστολέα, ακολουθεί ένας έλεγχος ορθότητας από το δίκτυο [VJR18].

2.3.4 Bitcoin και PoW

Το Bitcoin δίκτυο χρησιμοποιεί τον μηχανισμό συναίνεσης Proof of Work (PoW). Με αυτό το τρόπο αποφεύγονται στο δίκτυο, όποιες προσπάθειες χειραγώγησης κάποιας συναλλαγής, ή δεδομένων κάποιου μπλοκ. Κάθε κόμβος πρέπει να κάνει δύσκολους υπολογισμούς για να αποδειχθεί η γνησιότητα του. Όσο η υπολογιστική ισχύς των κόμβων του δικτύου είναι μεγαλύτερη από εκείνη ενός επιτιθέμενου, το δίκτυο παραμένει ασφαλές. Όπως και σε πολλά άλλα δίκτυο κάθε block αποτελείται από ένα σύνολο συναλλαγών (ή αλλιώς δεδομένων), από τη τιμή κατακερματισμού του προηγούμενου block και το nonce. Με τη προσθήκη του timestamp αποδεικνύεται ότι τα δεδομένα υπήρχαν τη στιγμή του κατακερματισμού.

Το PoW σύστημα κατακερματισμού του Bitcoin βασίζεται στην SHA-256 κρυπτογραφική συνάρτηση κατακερματισμού. Το PoW επιτυγχάνεται αυξάνοντας το nonce του block κατά 1 μέχρι να παραχθεί η τιμή κατακερματισμού με τον απαιτούμενο αριθμό από μηδενικά bit στην αρχή αυτού του κατακερματισμού. Αφού ολοκληρωθεί η διαδικασία δε μπορεί να αναιρεθεί χωρίς εκ νέου υπολογισμό. Αν με κάποιο τρόπο, αλλάξουν τα δεδομένα από έναν επιτιθέμενο, όπως αναφέραμε στο προηγούμενο κεφάλαιο, θα αλλάξει και η τιμή των επόμενων block. Σε γενικότερες γραμμές, ισχύει ότι η αλυσίδα που υπάρχει στην πλειοψηφία των κόμβων του δικτύου, είναι η σωστή [VJR18].

2.4 Δίκτυο Ethereum

Σε αυτή την ενότητα δίνουμε μια γενική επισκόπηση σχετικά με το δίκτυο Ethereum, δίνοντας βαρύτητα σε όλες τις υπηρεσίες που προσφέρει. Αυτές οι υπηρεσίες είναι πολύ σημαντικές, και θα μας βοηθήσουν στη συνέχεια, ώστε να καταλάβει κανείς το τρόπο λειτουργίας της εφαρμογής εκλογών, μιας και θα υλοποιηθεί στο δίκτυο αυτό.

2.4.1 Βασικά στοιχεία δικτύου Ethereum

Το δίκτυο Ethereum προτάθηκε από τον Vitalik στην επιστημονική εργασία [But+14], και αντιμετώπισε πολλά προβλήματα που εμφανίζονται το Bitcoin [VJR18]. Είναι μια αποκεντρωμένη

πλατφόρμα, που δημιουργεί ένα κατανεμημένο (P2P) δίκτυο που εκτελεί και επαληθεύει με ασφάλεια συναλλαγές και κώδικα(έξυπνα συμβόλαια). Τα έξυπνα συμβόλαια επιτρέπουν στους συμμετέχοντες να ανταλλάσουν μεταξύ τους πληροφορίες, δεδομένα και να κάνουν συναλλαγές χωρίς αξιόπιστη κεντρική αρχή. Όλες οι συναλλαγές διανέμονται με ασφάλεια στους κόμβους όλου του δικτύου. Κάθε κόμβος μπορεί να δει τη συναλλαγή και να την επαληθεύσει, ενώ παράλληλα είναι αδύνατη η τροποποίησή της. Οι συναλλαγές αποστέλλονται και λαμβάνονται από λογαριασμούς Ethereum που έχουν δημιουργηθεί από χρήστες. Για να ολοκληρωθεί μια συναλλαγή, θα πρέπει να την υπογράψει ο αποστολές, ο οποίος θα χρεωθεί και το κόστος επεξεργασίας πληρώνοντας ένα ποσό από Ethers, το κρυπτονόμισμα του Ethereum [AWS-b].

Πορτοφόλια

Όσοι έχουν Ethereum χρησιμοποιούν πορτοφόλια για να αποθηκεύσουν τα Ethers τους. Το πορτοφόλι είναι μια ψηφιακή διεπαφή που επιτρέπει την πρόσβαση στα Ethers που είναι αποθηκευμένος στο blockchain. Κάθε πορτοφόλι έχει μια διεύθυνση, μέσω της οποίας γίνονται συναλλαγές.

Τα Ethers, δεν αποθηκεύονται πραγματικά στο πορτοφόλι. Κάθε πορτοφόλι περιέχει ιδιωτικά κλειδιά. Ο χρήστης λαμβάνει ένα ιδιωτικό κλειδί για κάθε Ether που διαθέτει. Χωρίς το ιδιωτικό κλειδί η πρόσβαση δεν είναι εφικτή.

2.4.2 Συναλλαγές στο Ethereum

Στο δίκτυο του Ethereum, κάθε συναλλαγή έχει πεδία. Όπως και το Bitcoin έτσι και Ethereum για κάθε συναλλαγή απαιτούνται: η τιμή κατακερματισμού του προηγούμενου μπλοκ, το nonce, και λεπτομέρειές συναλλαγής. Επιπρόσθετα μπορεί να χρησιμοποιήσει και άλλα πεδία όπως φόρους κοκ. Όλες οι συναλλαγές θα επικυρωθούν ελέγχοντας το timestamp, το nonce και τη διαθεσιμότητα των φόρων για την εκτέλεση της συναλλαγής.

Για τη δημιουργία νέων μπλοκ το δίκτυο αυτό παρέχει κίνητρα στους miners. Για την οποιαδήποτε ενέργεια απαιτείται κόστος (**gas**). Αυτό το κόστος χρησιμοποιείται ως τέλη, αντί των Ethers, για ευκολία υπολογισμού. Ο κύριος λόγος είναι ότι τα Ethers, ποικίλλουν σε αξία, αναλόγως τις διακυμάνσεις της αγοράς, σε αντίθεση με το gas , που έχει σταθερή αξία. Αυτό το gas, για να πραγματοποιηθεί μία συναλλαγή, υπολογίζεται μέσω της διαδικασίας εξόρυξης.

Το Ethereum έχει ένα μοντέλο κινήτρων εξόρυξης όπου οι miners ανταγωνίζονται για τη δημιουργία μπλοκ. Ο miner που θα λύσει πρώτα το δύσκολο μαθηματικό πρόβλημα ονομάζεται νικητής, ενώ οι υπόλοιποι που το λύνουν μετά ονομάζονται omer. Το μπλοκ του νικητή προστίθεται στην κύρια αλυσίδα, και τα μπλοκ των omer, προστίθενται ως πλαϊνά μπλοκ στην κύρια αλυσίδα. Ο miner που βρήκε το νικητήριο μπλοκ ανταμείβεται με Ethers. [MSA19]

2.4.3 Έξυπνα συμβόλαια

Σύμφωνα με το [AWS-b] ένα έξυπνο συμβόλαιο είναι ο κώδικας εφαρμογής που βρίσκεται σε μια συγκεκριμένη διεύθυνση στο blockchain, γνωστή ως διεύθυνση συμβολαίου. Οι εφαρμογές μπορούν να καλούν τις λειτουργίες έξυπνων συμβολαίων, να αλλάζουν την κατάστασή τους και να ξεκινούν συναλλαγές. Τα έξυπνα συμβόλαια γράφονται σε γλώσσες προγραμματισμού όπως η Solidity και η Vyper, και μεταγλωττίζονται από την Εικονική Μηχανή Ethereum σε bytecode και εκτελούνται στο blockchain. Με άλλα λόγια μέσω των έξυπνων συμβολαίων μπορεί καθένας να αποθηκεύει δεδομένα και ανοιχτό κώδικα, ο οποίος μετά να καλείται για εκτέλεση σε εφαρμογές. Μόλις γίνει η δημοσίευση επιτυχώς και συμπεριληφθεί στο blockchain, επιστρέφεται μία διεύθυνση (Receipt), που είναι η διεύθυνση του συμβολαίου, και υπολογίζεται χρησιμοποιώντας μια συνάρτηση κατακερματισμού [AWS-b].

Κάθε έξυπνο συμβόλαιο είναι:

- **Πρόγραμμα:** Είναι απλά προγράμματα υπολογιστών.
- **Αμετάβλητο:** Μόλις αναπτυχθεί ο κώδικας ενός έξυπνου συμβολαίου, δε μπορεί να αλλάξει.
- **Ντετερμινιστικό:**Το αποτέλεσμα της εκτέλεσης ενός έξυπνου συμβολαίου είναι το ίδιο για όλους όσους το εκτελούν, δεδομένου του πλαισίου της συναλλαγής που ξεκίνησε την εκτέλεσή του και της κατάστασης του Ethereum blockchain τη στιγμή της εκτέλεσής του.

Ethereum Virtual Machine

Πολύ σημαντικό για την ανάπτυξη έξυπνων συμβολαίων είναι το **Ethereum Virtual Machine (EVM)**. Το EVM προσφέρει το περιβάλλον για τη δημιουργία και την ανάπτυξη έξυπνων συμβολαίων στη γλώσσα προγραμματισμού Solidity. Η εικονική μηχανή Ethereum, ή EVM, χρησιμεύει ως «εικονικός υπολογιστής» ή πλατφόρμα λογισμικού που χρησιμοποιείται από προγραμματιστές για τη δημιουργία αποκεντρωμένων εφαρμογών.

Εκτέλεση έξυπνων συμβολαίων

Τα έξυπνα συμβόλαια, απαιτούν συνήθως μια γλώσσα high-level, όπως η Solidity. Πριν την εκτέλεσή'η τους μεταγλωττίζονται σε bytecode χαμηλού επιπέδου. Με την ολοκλήρωση της μεταγλώττισης τους, αναπτύσσονται στη πλατφόρμα Ethereum, με τη χρήση μιας ειδικής συναλλαγής δημιουργίας συμβολαίου. Κάθε συμβόλαιο αναγνωρίζεται από μια διεύθυνση Ethereum, που δημιουργήθηκε με την ολοκλήρωση της συναλλαγής, γνωστό και ως ABI. Αυτή η διεύθυνση μπορεί να χρησιμοποιηθεί ως παραλήπτης σε μια συναλλαγή, προκειμένου να στείλει κάποιος χρήματα στο συμβόλαιο, ή για να καλέσει τις συναρτήσεις του.

Είναι σημαντικό ότι τα συμβόλαια τρέχουν μόνο εάν καλούνται από μια συναλλαγή. Τα συμβόλαια δεν τρέχουν ποτέ "στο παρασκήνιο". Ουσιαστικά παραμένουν αδρανείς έως ότου μια συναλλαγή ενεργοποιήσει την εκτέλεση, είτε άμεσα είτε έμμεσα ως μέρος μιας αλυσίδας κλήσεων συμβολαίων.

2.4.4 Αποκεντρωμένες εφαρμογές - dApps

Οι αποκεντρωμένες εφαρμογές (Decentralized Applications ή dApps) είναι ψηφιακές εφαρμογές ή προγράμματα που εκτελούνται σε ένα blockchain, ή γενικότερα ένα κατανεμημένο δίκτυο υπολογιστών [Fra22b]. Ένα dApp χρησιμοποιεί το blockchain για αποθήκευση και επεξεργασία των δεδομένων του, λειτουργία η οποία επιτυγχάνεται με τη χρήση των έξυπνων συμβολαίων. Το περιβάλλον διεπαφής με το χρήστη, δημιουργείται με το παραδοσιακό τρόπο, ενός απλού ιστότοπου. Έτσι μπορεί κανείς να σκεφτεί τα dApps ως έναν ιστότοπο, με ένα η περισσότερα έξυπνα συμβόλαια. Η μόνη διαφορά είναι ότι τα δεδομένα και οι υπολογισμοί παρέχονται από το blockchain.

Χαρακτηριστικά

Κάθε αποκεντρωμένη εφαρμογή, περιλαμβάνει μερικά χαρακτηριστικά [COI]:

1. Πρέπει να έχει "ανοιχτό" κώδικα, και να λειτουργεί χωρίς την παρέμβαση τρίτων.
2. Όλες οι πληροφορίες πρέπει να φυλάσσονται σε ένα δημόσια προσβάσιμο δίκτυο blockchain. Λόγω της αποκέντρωσης, δεν μπορεί να υπάρχει κεντρικό σημείο επίθεσης.
3. Πρέπει να διαθέτουν κάποιου είδους κρυπτογραφικό token για πρόσβαση και πρέπει να ανταμείβουν τους συνεισφέροντες στο εν λόγω token, όπως εξορύκτες και stakers [Dim+22].

4. Πρέπει να έχει μια συναινετική μέθοδο που δημιουργεί tokens, όπως PoW ή PoS.

2.5 Blockchain τεχνολογίες στην καθημερινή ζωή

Η αποκέντρωση προσφέρει διάφορα πλεονεκτήματα σε σχέση με τις εφαρμογές που εκτελούνται σε ένα κεντρικό δίκτυο. Ταυτόχρονα, η αποστολή χρημάτων μέσω μιας αποκεντρωμένης εφαρμογής σημαίνει ότι υπάρχει πολύ μικρό κόστος. Αυτό εξοικονομεί χρήματα στους χρήστες και, δεδομένου ότι οι αποκεντρωμένες συναλλαγές είναι σχεδόν άμεσες, εξοικονομεί χρόνο.

Ο αποκεντρωμένος χαρακτήρας τους, τις καθιστά άτρωτες σε όλων των ειδών επιθέσεις. Αυτό εκτός από ασφαλή, τις καθιστά και προσβάσιμες ανά πάσα στιγμή, μιας και είναι αδύνατη η διακοπή λειτουργίας τους.

Θα μπορούσαν να εφαρμοστούν σε κάθε κλάδο, όπως ιατρική, διακυβέρνηση, αποθήκευση αρχείων κοκ. Η αποκεντρωμένη φύση των δεδομένων που προσφέρουν τέτοιες εφαρμογές θεωρείται Web3.0. [COI]

Μερικά παραδείγματα χρήσης dApps στην καθημερινότητα [Gry21] μπορεί να είναι:

- **Οικονομικές υπηρεσίες:** μπορούν να χρησιμοποιηθούν για τη διευκόλυνση οικονομικών συναλλαγών, ή και για τη διευκόλυνση της αγοράς και πώλησης ακινήτων απευθείας μεταξύ αγοραστή και πωλητή.

- **Διαχείριση εφοδίων:** μπορεί να χρησιμοποιηθεί για την παρακολούθηση της κυκλοφορίας αγαθών μέσω μιας αλυσίδας εφοδιασμού, διασφαλίζοντας τη διαφάνεια [Abd+21]. Η γνώση της κατάστασης και της προέλευσης κάθε προϊόντος σε μια αλυσίδα εφοδιασμού, είναι το κλειδί για επιχειρήσεις και καταναλωτές. Για παράδειγμα το Walmart χρησιμοποιεί το blockchain, για τη παρακολούθηση των αγροτικών προϊόντων.

- **Επαλήθευση ταυτότητας:** μπορεί να χρησιμοποιηθεί για την ασφαλή αποθήκευση και επαλήθευση στοιχείων ταυτότητας, όπως για συστήματα ψηφοφορίας ή εφαρμογές διαβατηρίων [Pap+23].

- **Υγειονομική περίθαλψη:** μπορούν να χρησιμοποιηθούν για την αποθήκευση και παρακολούθηση αρχείων υγειονομικής περίθαλψης, καθώς και για τη διευκόλυνση της επικοινωνίας και της συνεργασίας των επαγγελματιών υγείας.

- **Μέσα κοινωνικής δικτύωσης:** μπορούν να χρησιμοποιηθούν για τη δημιουργία αποκεντρωμένων πλατφορμών μέσων κοινωνικής δικτύωσης, επιτρέποντας στους χρήστες να αλληλεπιδρούν και να μοιράζονται περιεχόμενο χωρίς την ανάγκη μιας κεντρικής αρχής.

- **Πνευματική ιδιοκτησία:** μπορεί να χρησιμοποιούνται για να αποτρέψουν την κλοπή και την απάτη πνευματικών και δημιουργικών ιδιοκτησιών και να αποδείξουν την ιδιοκτησία. Οι περιπτώσεις χρήσης blockchain για IP μπορεί να περιλαμβάνουν πιστοποίηση προέλευσης, απόδειξη πρώτης χρήσης, διαχείριση ψηφιακών δικαιωμάτων κοκ.

- **Internet of Things:** Οι συσκευές IoT μπορούν να επωφεληθούν από τη χρήση των Blockchain για διαχείριση και έλεγχο των δεδομένων. Με τη χρήση των έξυπνων συμβολαίων, η εσωτερική επικοινωνία μεταξύ των μηχανών, θα μπορούσε να γίνει αυτοματοποιημένη. Μπορούν να γίνουν έλεγχοι στην πρόσβαση και στις άδειες των συσκευών και χρηστών [KK22]. Με αυτό το τρόπο βελτιώνεται η ασφάλεια και βελτιστοποιείται η διαφάνεια στον έλεγχο των δραστηριοτήτων κάθε συσκευής.

- **Ψηφοφορία και διακυβέρνηση:** Μια αποκεντρωμένη εφαρμογή ψηφοφορίας, η οποία θα εκμεταλλεύεται όλα τα οφέλη του Blockchain, θα μπορούσε να εγγυηθεί την ασφάλεια των

ψήφων, καθώς οι ανησυχίες για απάτες σχετικές με τα ψηφοδέλτια είναι μεγάλες. Ανεξάρτητες και ξένες οντότητες δε θα έχουν τον έλεγχο για τροποποίηση των ψήφων. Η αμετάβλητη βάση δεδομένων που μπορεί να διαθέτει μια αποκεντρωμένη εφαρμογή, διασφαλίζει εκτός από την ασφάλεια των ψήφων, την επαληθευσιμότητά τους, κάνοντας παράλληλα τη συνολική εκλογική διαδικασία πολύ πιο οικονομική.

Blockchain vs cloud

Το cloud computing, είναι βασισμένο σε δίκτυο για παροχή υπολογιστικών πόρων. Αντί να κατέχει κάποιος το υλικό του υπολογιστή τους, ή κέντρα δεδομένων, οι οργανισμοί ενδέχεται να νοικιάσουν πρόσβαση σε εφαρμογές και χώρο αποθήκευσης από έναν πάροχο cloud. Με απλά λόγια, το cloud computing είναι η παροχή υπολογιστικών υπηρεσιών — συμπεριλαμβανομένων διακομιστών, αποθήκευσης, βάσεων δεδομένων, δικτύωσης, λογισμικού, αναλυτικών στοιχείων και νοημοσύνης μέσω του Διαδικτύου (cloud).

Το Blockchain και το cloud computing είναι δύο από τις πιο αναγνωρίσιμες εξελίξεις. Και οι δύο παρέχουν σε εταιρείες υπηρεσίες που δεν ήταν διαθέσιμες στο παρελθόν. Το Blockchain έχει κερδίσει δημοτικότητα λόγω της καινοτόμου και πολλά υποσχόμενης τεχνολογίας του. Μειώνει τον κίνδυνο που σχετίζεται με κάθε συναλλαγή τεχνολογίας, αποφεύγει την απάτη και προσφέρει κλιμακούμενη διαφάνεια για διάφορους στόχους. Οι υπηρεσίες cloud computing παρέχουν προσαρμοστικότητα πόρων, ταχεία καινοτομία και επεκτασιμότητα. [muz22]

Κεφάλαιο 3

Ηλεκτρονική ψηφοφορία

3.1 Ανάγκη ηλεκτρονικής ψηφοφορίας

Η ψηφοφορία είναι ένα θεμελιώδες συστατικό μιας δημοκρατικής κοινωνίας. Τα δικαιώματα των πολιτών πρέπει να είναι εμπιστευτικά και να βασίζονται στην αρχή "Ένα άτομο, μία ψήφος". Η παραδοσιακή μέθοδος ψηφοφορίας, χαρακτηρίζεται από προβλήματα σε κάθε πτυχή της εκλογικής διαδικασίας, όπως συμπλήρωση ψηφοδελτίων, δωροδοκία, χειραγώγηση κατά τη ψηφοφορία, λάθη καταμέτρησης, υψηλό κόστος, ασαφή ψηφοδέλτια, χρονοβόρες διαδικασίες, ακόμη και σαμποτάζ στις κάλπες [Iwu18] - [OOW19].

Η εφαρμογή της ηλεκτρονικής ψηφοφορίας σε εθνικά εκλογικά συστήματα, εξετάζεται επί του παρόντος από πολλές χώρες. Μέσω της ηλεκτρονικής ψηφοφορίας, επιδιώκεται η βελτίωση διαφόρων πτυχών της εκλογικής διαδικασίας, που μπορεί να καθιστούν το παραδοσιακό τρόπο ψηφοφορίας δύσκολο. Μέσω της ηλεκτρονικής ψηφοφορίας, θα μπορούσαν να λυθούν τα προβλήματα πρόσβασης, που παρουσιάζονται στο παραδοσιακό τρόπο εκλογών, και καθιστούν δύσκολη ή και αδύνατη την ψηφοφορία μερικών πολιτών. Παράλληλα μπορεί να αναδειχθεί η δημοκρατία, και να οικοδομηθεί αξιοπιστία στα αποτελέσματα των εκλογών αυξάνοντας την αποτελεσματικότητα της εκλογικής διαδικασίας. Η δημιουργία μιας ασφαλούς πλατφόρμας ψηφοφορίας, που θα ικανοποιεί όλες τις αρχές ψηφοφορίας, ενώ παράλληλα υιοθετεί ένα αυστηρό σύστημα ταυτοποίησης πολιτών, θα μπορούσαν να εξαλειφθούν ορισμένα ζητήματα απάτης, επεξεργασίας αποτελεσμάτων, καθιστώντας την εκλογική διαδικασία πιο βολική και με μικρότερο κόστος.

Όμως σε συστήματα ηλεκτρονικής ψηφοφορίας παρουσιάζονται και διάφορες προκλήσεις στη κάλυψη των αναγκών μιας τέτοιας πολύπλοκης διαδικασίας. Πολλές προτάσεις για τέτοια συστήματα, στερούνται διαφάνειας είτε για τους ψηφοφόρους, είτε για τις εκλογικές αρχές, ενώ παράλληλα είναι δύσκολο να γίνουν πλήρως κατανοητές, μιας και απευθύνονται σε κάθε ηλικία και κοινωνική ομάδα. Επίσης, η διαχείριση του συστήματος από κεντρικές αρχές ή γενικότερα από μια ομάδα διαχειριστών, μειώνει τη διαφάνεια, και την αξιοπιστία που εκπέμπει αυτό το σύστημα στους πολίτες.

3.1.1 Αρχές ψηφοφορίας

Είτε μιλάμε για παραδοσιακή ψηφοφορία, είτε για ψηφοφορία μέσω ψηφιακών μηχανημάτων ψηφοφορίας ή διαδικτυακό σύστημα ψηφοφορίας, πρέπει να πληρούνται αρκετές αναγκαίες προϋποθέσεις / αρχές απαραίτητες για μια εκλογική διαδικασία. Στη συνέχεια θα δούμε τις αρχές, και το τρόπο με τον οποίο θα μπορούσαν να ικανοποιηθούν μέσω ενός ηλεκτρονικού συστήματος ψηφοφορίας.

Ταυτοποίηση

Μόνο οι νόμιμοι ψηφοφόροι θα πρέπει να μπορούν να λάβουν μέρος στην ψηφοφορία. Θα πρέπει να δημιουργηθεί μια λίστα με νόμιμους ψηφοφόρους, με τη χρήση ενός αξιόπιστου και ασφαλούς συστήματος αναγνώρισης, που θα απαγορεύει τη προσθήκη παράνομων ψηφοφόρων και θα καθιστά αδύνατη την κλοπή ενός λογαριασμού. Η επιλογή των πολιτών με δικαίωμα ψήφου και η ταυτοποίηση τους είναι από τα μείζων ζητήματα που χρήζουν επίλυσης όσον αφορά συστήματα ηλεκτρονικής ψηφοφορίας, και θα εστιάσουμε πολύ σε αυτό το τομέα στο σύστημα που προτείνεται από αυτή τη διπλωματική εργασία.

Μη επαναχρησιμοποίηση

Κάθε ψηφοφόρος μπορεί να ψηφίσει μόνο μία φορά. Εκ πρώτης όψεως, η εφαρμογή της μη επαναχρησιμοποίησης μπορεί να φαίνεται απλή, σημειώνοντας το στη λίστα συμμετοχής ώστε να μην του επιτραπεί η υποβολή επιπλέον ψήφων. Η δυσκολία της διαδικασίας αυτής υπόκειται στη παράλληλη διατήρηση της ανωνυμίας των ψήφων.

Απόρρητο

Κανείς δε θα πρέπει να γνωρίζει πληροφορίες για τους ψηφοφόρους των εκλογών. Το απόρρητο στη διαδικτυακή ψηφοφορία, ερμηνεύεται ότι μόνο ο ψηφοφόρος θα πρέπει να γνωρίζει τι ψήφισε στη ψηφοφορία. Η επίτευξη αυτής της ιδιότητας θα βασίζεται κυρίως σε μία μέθοδο κρυπτογράφησης που θα υιοθετεί το κάθε σύστημα.

Δικαιοσύνη

Κανείς δεν μπορεί να λάβει ενδιάμεσα αποτελέσματα ψηφοφορίας. Οι ψήφοι πριν αποθηκευτούν θα πρέπει να κρυπτογραφούνται ή ο αριθμός ψήφων για κάθε υποψήφιο να μπορεί να ανακτηθεί μόνο από τις αρχές με τη χρήση αξιόπιστων μεθόδων.

Επαληθευσιμότητα

Τα άκυρα ψηφοδέλτια θα πρέπει να εντοπίζονται και να μη λαμβάνονται υπόψη κατά την καταμέτρηση. Εκ πρώτης όψεως, φαίνεται σχετικά απλή λειτουργία, εάν οι ψήφοι αποκρυπτογραφηθούν ένας προς ένας. Ωστόσο, μια τέτοια διαδικασία ελέγχου έγκυρων ψηφοδελτίων είναι αρκετά περίπλοκη. Θα μπορούσε να αντιμετωπιστεί με τη δημιουργία ενός συστήματος, που θα αποτρέπει εξ αρχής την υποβολή άκυρων ψήφων.

Για την ορθή χρήση όλων των τεχνολογιών που αναφέρθηκαν, θα πρέπει να υπάρχει εμπιστοσύνη στο σύστημα. Ένα σύστημα ψηφοφορίας πρέπει να είναι πλήρως επαληθεύσιμο για να κερδίσει αυτήν την εμπιστοσύνη, δηλαδή, όλοι οι εμπλεκόμενοι μπορούν να διασφαλίσουν ότι το σύστημα συμμορφώνεται με τις αναφερόμενες ιδιότητες. Η διασφάλιση της επαληθευσιμότητας μπορεί να χωριστεί σε δύο κατηγορίες:

- **Προσωπική:** όταν ο ψηφοφόρος μπορεί να επαληθεύσει ότι το ψηφοδέλτιό του έχει καταγραφεί και καταμετρηθεί σωστά.

- **Καθολική:** όταν όλοι μπορούν να αποδείξουν ότι το σύστημα ως σύνολο λειτουργεί με ακρίβεια

Απαιτήσεις ασφαλείας

Παράλληλα με την τήρηση των παραπάνω αρχών, κάθε σύστημα ψηφοφορίας, θα πρέπει να συμβαδίζει με μερικές παραμέτρους ασφάλειας, και προστασίας των προσωπικών δεδομένων και δικαιωμάτων των πολιτών.

- **Ανωνυμία:** Κάθε ψήφος θα πρέπει να είναι ανώνυμη. Συνεπώς, οποιαδήποτε συσχέτιση μεταξύ των ψήφων και των προσωπικών δεδομένων των ψηφοφόρων θα πρέπει να αποφεύγεται.
- **Ακρίβεια:** Κανείς δεν μπορεί να τροποποιήσει ή να διαγράψει την ψήφο των άλλων πολιτών, είτε κατά τη διάρκεια της ψηφοφορίας, είτε κατά τη διάρκεια της τελικής καταμέτρησης.
- **Διαθεσιμότητα:** Τα συστήματα ψηφοφορίας θα πρέπει να είναι πάντα διαθέσιμα, την ημέρα που λαμβάνει χώρα η εκλογική διαδικασία.
- **Ανακτησιμότητα και Ταυτοποίηση:** Κάθε σύστημα ψηφοφορίας θα πρέπει να βρίσκεται σε θέση να ανακτήσει όλες τις πληροφορίες ψηφοφορίας και τις ψήφους σε περίπτωση επιθέσεων.

3.1.2 Οφέλη και αδυναμίες ηλεκτρονικής ψηφοφορίας

Στο βιβλίο [WNT11] παρουσιάζονται οφέλη και αδυναμίες που παρουσιάζονται σε συστήματα ηλεκτρονικής ψηφοφορίας.

Οφέλη

Τα πιο σημαντικά οφέλη που μπορεί να έχει η αντικατάσταση του παραδοσιακού τρόπου εκλογών, με ένα σύστημα ηλεκτρονικής ψηφοφορίας είναι:

- Γρηγορότερη καταμέτρηση των ψήφων.
- Λιγότερα σφάλματα στα αποτελέσματα.
- Αποτελεσματικός χειρισμός περίπλοκων τύπων εκλογικών συστημάτων, που απαιτούν επίπονες διαδικασίες καταμέτρησης.
- Βελτιωμένη παρουσίαση περίπλοκων ψηφοδελτίων.
- Αυξημένη ευκολία για τους ψηφοφόρους.
- Αυξημένη συμμετοχή. Επίλυση ζητημάτων προσβασιμότητας.
- Περισσότερο προσαρμοσμένο στις ανάγκες μιας ολοένα και πιο κινητικής κοινωνίας.
- Πρόληψη κάθε απάτης στα εκλογικά τμήματα.
- Μείωση των κατεστραμμένων ψηφοδελτίων, αλλά και ενημέρωση των πολιτών για τυχόν άκυρες ψήφους.
- Μειωμένο κόστος υλοποίησης των εκλογών.
- Εξοικονόμηση χρόνου.

Αδυναμίες

Παρά τα όσα οφέλη μπορεί να προσφέρει στη διαδικασία η ηλεκτρονική ψηφοφορία, υπάρχουν και πολλές αδυναμίες που χρήζουν αντιμετώπισης.

- Έλλειψη διαφάνειας.
- Δυσκολία κατανόησης και χρήσης της εφαρμογής από όλες τις κοινωνικές ομάδες.
- Δυσκολία ταυτοποίησης του ψηφοφόρου, και ταυτοποίησης της προέλευσης ψήφου.
- Πιθανή παραβίαση του απορρήτου της ψηφοφορίας.
- Δυσκολία επαληθευσιμότητας των ψήφων από τους ψηφοφόρους. Κίνδυνος για τροποποίηση η διαγραφή ψήφων από τις κεντρικές αρχές που ελέγχουν το σύστημα.
- Πιθανή έλλειψη εμπιστοσύνης του κοινού στις εκλογές που βασίζονται στην ηλεκτρονική ψηφοφορία ως αποτέλεσμα των παραπάνω αδυναμιών.
- Πιθανή ευπάθεια σε επιθέσεις από κακόβουλους χρήστες. Στην ερευνητική εργασία [AT13] αναφέρονται επιθέσεις που μπορούν να πραγματοποιηθούν σε μία εφαρμογή ψηφοφορίας:

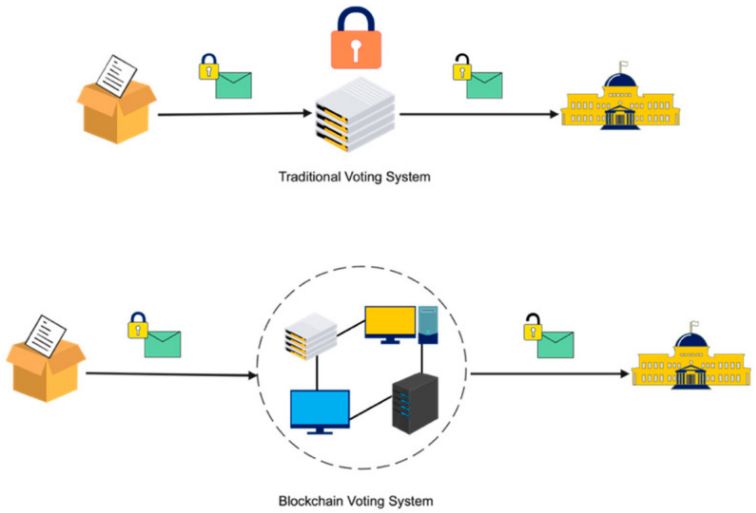
  1. Επίθεση κατανεμημένης άρνησης υπηρεσίας (**DDoS**). Μία τέτοια επίθεση θα μπορούσε να έχει καταστροφικές συνέπειες καθώς θα έθετε σε κίνδυνο τη διαθεσιμότητα ενός συστήματος ψηφοφορίας.
  2. **Ιοί**. Ένας ιός θα μπορούσε να προκαλέσει ανεπιθύμητες ενέργειες σε έναν ενεργό υπολογιστή. Υπάρχουν ιοί που θα μπορούσαν να καταστρέψουν συστήματα ηλεκτρονικής ψηφοφορίας. Αυτό θα μπορούσε να αλλοιώσει τη διαδικασία των εκλογών. Για παράδειγμα, θα μπορούσαν να προκληθούν αλλαγές στην ώρα των εκλογών, ή να δημιουργηθεί η ανάγκη για δεύτερες εκλογές.
  3. **Worms**: τύπος ιού που δε χρειάζεται η αλλοίωση ενός προγράμματος για την εξάπλωση του. Δημιουργεί αντίγραφα του εαυτού του σε έναν μολυσμένο υπολογιστή και εξαπλώνεται για να γίνει ενεργό σε άλλα συστήματα. Μπορούν να αντικαταστήσουν τμήματα αρχείων με τυχαία δεδομένα. Μια μόλυνση από worm, θα μπορούσε να οδηγήσει στην αντικατάσταση αρχείων και αλλοίωση των αποτελεσμάτων της ψηφοφορίας. ‘
  4. Δούρειοι Ίπποι (**Trojan Horses**). Είναι κομμάτια κώδικα που θα μπορούσαν να τροποποιήσουν ή να διαγράψουν ένα σημαντικό αρχείο από τον υπολογιστή, να δημιουργήσουν ιό, ή και να κλέψουν δεδομένα. Μόλις μπει σε έναν υπολογιστή, μπορεί να έχει πρόσβαση σε κωδικούς πρόσβασης και άλλες προσωπικές πληροφορίες. Αντιπροσωπεύει μια τεράστια απειλή για την ακεραιότητα των πληροφοριών των συστημάτων ηλεκτρονικής ψηφοφορίας.

- Κίνδυνος χειραγώγησης από άλλους πολίτες, ή από κάποιον επιτιθέμενο στο σύστημα.

3.2 Ηλεκτρονική ψηφοφορία μέσω Blockchain

Παρά το γεγονός ότι με τη χρήση ηλεκτρονικών συστημάτων ψηφοφορίας θα υπήρχε σαφής βελτίωση στην ασφάλεια και την αποτελεσματικότητα της ψηφοφορίας, δεν έχει ακόμη υιοθετηθεί σε εθνική κλίμακα, λαμβάνοντας υπόψη όλα τα πιθανά πλεονεκτήματά της. Αυτό οφείλεται κυρίως στις ανησυχίες σχετικά με την κεντρική αποθήκευση και διαχείριση των αρχείων και των αποτελεσμάτων. Ως εκ τούτου έχουν γίνει πολλές προσπάθειες και ερευνητικές μελέτες για τον σχεδιασμό αποκεντρωμένων ηλεκτρονικών συστημάτων ψηφοφορίας, που βασίζονται στο blockchain. Τα χαρακτηριστικά και οι τεχνολογίες που έχει το blockchain, καθιστώντας το ένα κρυπτογραφημένο διαφανές βιβλίο το καθιστούν ιδανικό για τον σχεδιασμό συστημάτων ηλεκτρονικής ψηφοφορίας αντέχοντας κάθε μορφής χειραγώγηση και απάτη [Hua+21].

Λόγω της κατανεμημένης του μορφής μειώνει κινδύνους που συνδέονται με την ηλεκτρονική ψηφοφορία και επιτρέπει την προστασία από παραβιάσεις για το σύστημα. Η ηλεκτρονική ψηφοφορία που βασίζεται σε blockchain βασίζεται στη μορφή του συστήματος να λειτουργεί μόνο του, χωρίς να ελέγχεται από κάποιο μεμονωμένο φορέα ή την κυβέρνηση. Μέσω της τεχνολογίας αυτής θα μπορούσαν να ξεπεραστούν όσοι κίνδυνοι υπάρχουν για την ηλεκτρονική ψηφοφορία [JAS21].



Σχήμα 11. Ψηφοφορία μέσω Blockchain

3.2.1 Λύσεις του Blockchain

Η τεχνολογία Blockchain αποτελείται από ένα ενιαίο αμοιβαία συμφωνημένο καθολικό συναλλαγών που μοιράζονται εκατομμύρια κόμβοι. Για να γίνει οποιαδήποτε αλλαγή στα υπάρχοντα δεδομένα στο δίκτυο, ο επιτιθέμενος θα πρέπει να έχει μια συναίνεση, η οποία συνεπάγεται «αναγκασμό» του 51% των συνολικών κόμβων σε προεπιλογή ταυτόχρονα. Θεωρώντας μια τέτοια επίθεση υπολογιστικά αδύνατη, δεν είναι δυνατή η αλλαγή μιας εγγραφής. Η κατανεμημένη φύση αυτής της τεχνολογίας, την καθιστά κατάλληλη για συστήματα ψηφοφορίας.

Αποκεντρωμένη βάση δεδομένων

Με την αποθήκευση των στοιχείων των πολιτών μέσω των οποίων θα γίνει η ταυτοποίηση τους, αλλά και των ψήφων σε μια κεντρική βάση δεδομένων, το σύστημα καθιστάτε επιρρεπές σε γεγονότα κυβερνοασφάλειας. Μια απλή επίθεση θα μπορούσε να οδηγήσει το σύστημα σε κατάρρευση προκαλώντας τη δυσαρέσκιά των πολιτών. Τα συστήματα όμως που βασίζονται σε

blockchain είναι αποκεντρωμένα. Ακόμα και αν ένας επιτιθέμενος παραβιάσει έναν κόμβο, θα πρέπει να κερδίσει την πλειοψηφία για να καταρρίψει το δίκτυο. Η ύπαρξη αυτής της αμετάβλητης βάσης, κερδίζει και την εμπιστοσύνη των ψηφοφόρων για την ακεραιότητα των ψήφων, καθώς γνωρίζουν ότι οι ψήφοι τους δεν μπορούν να τροποποιηθούν η να διαγραφτούν από το σύστημα.

Βιομετρική ταυτοποίηση χρηστών

Ένα από τα σοβαρότερα προβλήματα που αντιμετωπίζουν σχεδόν όλες οι κεντρικές αρχιτεκτονικές, ιδίως στην ψηφοφορία, είναι η κλοπή ταυτότητας. Οποιοσδήποτε θα μπορούσε να κλέψει την ταυτότητα κάποιου ψηφοφόρου και να ψηφίσει για λογαριασμό του. Η τεχνολογία Blockchain απαιτεί την επαλήθευση του αναγνωριστικού ενός χρήστη προτού μπορέσει να λάβει μέτρα στο σύστημα για να αποτρέψει την απώλεια μιας προσωπικής εγγραφής ταυτότητας. Για παράδειγμα, κάθε ψηφοφόρος για ένα εκλογικό σύστημα που υιοθετείτε στην Ελλάδα, θα πρέπει να εγγραφτεί στο blockchain, ώστε να του δοθεί η δυνατότητα να καταβάλει τη ψήφο του. Για αυτή την εγγραφή θα είναι απαραίτητη η επικύρωση και η ταυτοποίηση από κάποιο κεντρικό ελεγκτικό σύστημα. Επιπρόσθετα υπάρχουν και μέθοδοι, όπως κωδικοί πρόσβασης και OTP, που χρησιμοποιούν συχνά οι σύγχρονες εφαρμογές. Συστήματα που είναι χτισμένα και βασισμένα στο blockchain, απαιτούν την εγγραφή των χρηστών ώστε να μπορέσουν να αλληλεπιδράσουν με αυτό. Μια αντίστοιχη μέθοδος μπορεί να εφαρμοστεί και σε έναν ψηφοφόρο, αυξάνοντας έτσι τη συνολική ασφάλεια του συστήματος.

Ασφάλεια

Εκτός από τις κύριες πρακτικές ασφαλείας που ακολουθούνται από συστήματα ψηφοφορίας που βασίζονται σε blockchain, είναι απαραίτητο να συζητηθούν τα βασικά οφέλη της τεχνολογίας. Με τη χρήση του blockchain ως βάση δεδομένων, για την αποθήκευση των ψήφων και των στοιχείων λογαριασμών των χρηστών, η τροποποίηση ή διαγραφή των δεδομένων αυτών είναι αδύνατη, λόγω της κατανεμημένης φύσης του. Επομένως, κάθε μορφή επίθεσης που θα μπορούσε να συμβεί στη βάση δεδομένων ή που θα μπορούσε να θέσει την υπηρεσία εκτός λειτουργίας είναι αδύνατη.

Επιπρόσθετα η τεχνολογία αυτή διαθέτει μεθόδους κρυπτογράφησης. Για παράδειγμα το δίκτυο Bitcoin κάνει χρήση της κρυπτογραφίας Elliptic Curve. Κάθε ψηφοφόρος θα πρέπει να έχει δύο μοναδικά κλειδιά στο δίκτυο που δημιουργούνται μέσω μαθηματικών τύπων αμέσως μόλις δημιουργηθούν οι λογαριασμοί του. Το ένα κλειδί είναι δημόσιο (ταυτότητα του ψηφοφόρου), άρα και προσβάσιμο στο κοινό, το ιδιωτικό κλειδί παραμένει κρυφό από όλους και χρησιμοποιείται κυρίως από τον κάτοχο του λογαριασμού μόνο για τη διαδικασία της ταυτοποίησης.

Διαφάνεια

Η δωροδοκία ή παρακίνηση είναι ένα μείζων θέμα που αφορά συστήματα ψηφοφορίας. Αυτό το πιθανό ζήτημα καθιστά αμφίβολο κάθε σύστημα όταν συζητούνται οι πιο ευαίσθητες περιπτώσεις χρήσης, όπως η ψηφοφορία. Με τη βοήθεια του blockchain, μπορούμε πάντα να μετράμε τις ψήφους σε πραγματικό χρόνο, χωρίς να έχουμε καμία αμφιβολία για τη νομιμότητά του. Κάθε πολίτης θα πρέπει να έχει την πεποίθηση ότι η γνώμη του, που εκφράζεται μέσω ψηφοφορίας, θα γίνεται σεβαστή και θα πρέπει να είναι πάντα διαφανής, παρά το «επίπεδο» των εκλογών.

Θα πρέπει με τη χρήση όλων αυτών των τεχνολογιών ο ψηφοφόρος να έχει τη δυνατότητα να επαληθεύσει τα αποτελέσματα. Με τη βοήθεια της κρυπτογραφίας που προσφέρει το blockchain, διασφαλίζεται η διατήρηση του βέλτιστου επιπέδου διαφάνειας, με κάθε μέλος του δικτύου να απολαμβάνει ατομικό απόρρητο.

Γενική αρχιτεκτονική

Η ψηφοφορία, μπορεί να έχει διαφορετικές ανάγκες. Δεν αναφερόμαστε πάντα για την επιλογή ενός προέδρου σε εθνικό επίπεδο. Μπορεί να αφορά κάθε μορφή ψηφοφορίας, όπως πανεπιστημιακές εκλογές, δημοσκόπηση κοκ. Αφού κάθε μία από τις περιπτώσεις χρήσης έχει τις δικές της απαιτήσεις που θα μπορούσαν να διαφέρουν σε μεγάλο βαθμό, είναι σημαντικό να αντιμετωπίζονται δίκαια και ίσα σε επίπεδο κώδικα και αρχιτεκτονικής. Η τεχνολογία blockchain παρέχει την τέλεια σκοπιμότητα, και είναι εύκολα προσαρμόσιμη σε κάθε περίπτωση χρήσης εκλογών.

Φιλικό προς το περιβάλλον

Οι περισσότερες χώρες χρησιμοποιούν ακόμη την παραδοσιακή έντυπη μορφή ψηφοφορίας. Σύμφωνα με το [ori23] για τις εκλογές που διεξήχθησαν στις Ηνωμένες Πολιτείες το 2012, περίπου 126 εκατομμύρια ψηφοφόροι συνεισέφεραν στη «δημοκρατική διαδικασία», με τουλάχιστον ένα χαρτί χαμηλής ποιότητας ανά άτομο χρησιμοποιήθηκε για να ψηφίσει 1185 τόνοι ξύλο και περίπου 11 εκατομμύρια γαλόνια νερού χρησιμοποιήθηκαν για την κατασκευή του χαρτιού. Η σπατάλη στερεών υπολογίστηκε σε περίπου 981. 800 λίβρες. Ακόμη και αφού ληφθεί υπόψη ότι το 50% αυτών των ψηφοδελτίων ανακυκλώθηκαν, οι αριθμοί είναι τεράστιοι και καταστροφικοί για το περιβάλλον. Επομένως, η ανάγκη δημιουργίας και υιοθέτησης ηλεκτρονικών εκλογών είναι μεγάλες, καθώς θα βοηθούσαν δραματικά στην προστασία του περιβάλλοντος, αλλά θα καθιστούσαν και την εκλογική διαδικασία πολύ πιο οικονομική.

3.2.2 Σχετικά συστήματα

Πολλές προτάσεις και ερευνητικές εργασίες έχουν αναπτυχθεί για συστήματα ψηφοφορίας μέσω blockchain. Οι συγγραφείς του εγγράφου [Gar+19] έγραψαν μια εμπειρική ανασκόπηση των εφαρμογών ηλεκτρονικής ψηφοφορίας χρησιμοποιώντας τεχνολογία blockchain. Σε αυτή την εργασία παρουσιάζονται προκλήσεις που αντιμετωπίζουν οι εφαρμογές ηλεκτρονικής ψηφοφορίας σχετικά με το απόρρητο, έλλειψη αποδεικτικών στοιχείων, αντοχή στην απάτη, ευκολία χρήσης, επεκτασιμότητα, ταχύτητα και κόστος. Σύγκριναν 14 εφαρμογές σε 6 τομείς, υποδεικνύοντας σε έναν πίνακα εάν και πώς πληρούσε κάθε κριτήριο.

Οι συγγραφείς της εργασίας [Ben+22] έκαναν μια πιο πρόσφατη ανασκόπηση των εφαρμογών ηλεκτρονικής ψηφοφορίας που βασίζονται σε Blockchain. Ανέφεραν τις προκλήσεις που αντιμετωπίζουν οι εφαρμογές ηλεκτρονικής ψηφοφορίας όπως το απόρρητο, η έλλειψη αποδεικτικών στοιχείων, η αντίσταση στην απάτη, η ευκολία χρήση, επεκτασιμότητα, ταχύτητα και κόστος. Το σύστημα που θα προταθεί και θα υλοποιηθεί σε αυτή τη διπλωματική εργασία, θα βασίζεται στην ικανοποίηση αυτών των αναγκών, δίνοντας έμφαση στην ικανοποίηση της μεγαλύτερης δυσκολίας τέτοιων εφαρμογών που είναι η ταυτοποίηση των πολιτών.

Σε αυτό το κεφάλαιο θα βασιστούμε και θα ακολουθήσουμε παρόμοια στρατηγική με εκείνη των ερευνητών της εργασίας [Ben+22], μιας και αποτελεί μια πολύ πρόσφατη σύγκριση των μεθόδων που υιοθετούν εκλογικά συστήματα βασισμένα στο blockchain, παρέχοντας έτσι μια πληρέστερη σύγκριση. Θα σχολιαστούν και θα συγκριθούν εκλογικά συστήματα σύμφωνα με ένα συγκεκριμένο σύνολο κριτηρίων. Πιο συγκεκριμένα θα ακολουθήσει μια λεπτομερής σύγκριση εκλογικών συστημάτων σύμφωνα με: τις υλοποιήσεις που χρησιμοποιούνται, μέθοδοι ταυτοποίησης ψηφοφόρου, αλγόριθμοι κρυπτογράφησης/κατακερματισμού ψηφοφορίας, αντίσταση σε επιθέσεις και ιδιότητες ασφαλείας.

Υλοποιήσεις

Όλες οι υπάρχουσες εφαρμογές ηλεκτρονικής ψηφοφορίας, αλλά και προτάσεις ακολουθούν περίπου τον ίδιο τρόπο υλοποίησης.

1. Στο πρώτο στάδιο της υλοποίησης ενός εκλογικού συστήματος λαμβάνει χώρα η δημιουργία και αρχικοποίηση του έξυπνου συμβολαίου. Από το τρόπο με τον οποίο είναι γραμμένα το έξυπνο συμβόλαιο κρίνονται και τα επόμενα στάδια που αφορούν την ταυτοποίηση των πολιτών, αλλά και τη διαδικασία της ψηφοφορίας. Αυτό το στάδιο μπορεί να περιλαμβάνει και την εγγραφή των χρηστών ή τη δημιουργία λίστας με τους πολίτες ικανούς για ψηφοφορία.

2. Η δεύτερη φάση αφορά την ταυτοποίηση των ψηφοφόρων. Οι πολίτες ταυτοποιούνται σύμφωνα με την υλοποίηση του έξυπνου συμβολαίου. Υπάρχουν πολλοί τρόποι να επιτευχθεί αυτή η υλοποίηση, οι οποία θα αναφερθούν λεπτομερώς στη συνέχεια.

3. Η τρίτη φάση αφορά τη διαδικασία ψηφοφορίας. Με την επιτυχή ταυτοποίηση κάθε ψηφοφόρος καλείται να επιλέξει έναν ή περισσότερους υποψήφιους σύμφωνα με τους κανόνες ψηφοφορίας. Στη συνέχεια, η ψηφοφορία κρυπτογραφείται χρησιμοποιώντας έναν αλγόριθμο κρυπτογράφησης ή κατακερματίζεται χρησιμοποιώντας μια συνάρτηση κατακερματισμού, και προστίθεται στο blockchain. Αυτή η ψήφος είναι αόρατη και μη αναστρέψιμη ακολουθώντας τις αρχές της ψηφοφορίας. Υπάρχουν πολλές ερευνητικές εργασίες που προτείνουν λύσεις ώστε να δίνεται η δυνατότητα τροποποίησης ή αλλαγής ψήφου [SDS18], [Yi19].

4. Η τέταρτη φάση είναι η φάση της καταμέτρησης ψήφων. Με το πέρας των εκλογών, καθίσταται αδύνατη η αλλαγή ή η προσθήκη ψήφων. Εάν η διαδικασία μέτρησης πραγματοποιείται παράλληλα με τη ψηφοφορία, είναι σημαντικό να μην είναι ορατός ο τρέχων αριθμός ψήφων για κάθε υποψήφιο. Με αυτό το τρόπο μπορεί να αποφευχθεί η επιρροή σε ψηφοφόρους που δεν έχουν ψηφίσει ακόμη.

5. Η πέμπτη φάση αφορά την εξαγωγή και δημοσίευση αποτελεσμάτων. Μέσω ενός ασφαλούς λογαριασμού που συνήθως θα διοικείται από τις εκλογικές αρχές, θα ανακοινώνονται αναλυτικά τα αποτελέσματα και γίνονται προσβάσιμα σε όλους.

Τα περισσότερα συστήματα όπως και αυτό που θα υλοποιηθεί στη διπλωματική εργασία, χρησιμοποιούν το δίκτυο Ethereum, που υποστηρίζει έξυπνα συμβόλαια. Με τη χρήση των έξυπνων συμβολαίων θα εκτελείτε ο κώδικας που υπό άλλες συνθήκες θα έτρεχε στη server πλευρά της εφαρμογής, αλλά θα χρησιμοποιηθούν τόσο για τη καταγραφή όσο και για την καταμέτρηση των ψήφων. Εγγυούνται το απόρρητο και μπορούν να υποστηρίξουν προσαρμοσμένες μεθόδους κρυπτογράφησης. Παράλληλα υπάρχουν και πολλές ερευνητικές εργασίες όπως στη [BBJ18] που χρησιμοποιούν το δίκτυο Bitcoin για ηλεκτρονική ψηφοφορία. Η χρήση της τεχνολογίας blockchain δεν μπορεί να διαγράψει εντελώς την παρουσία κεντρικής αρχής που διενεργεί την ψηφοφορία, και η εφαρμογή της σε επίπεδο εθνικών εκλογών είναι δύσκολη, με πολλές ερευνητικές εργασίες να προσφέρουν ένα μερικώς αποκεντρωμένο blockchain.

Ταυτοποίηση πολιτών

Μια από τις παραμέτρους που καθιστούν δύσκολη μέχρι και σήμερα παρά τις πολλές προτάσεις που υπάρχουν, είναι η υλοποίηση ενός ασφαλούς αποκεντρωμένου συστήματος μέσω του οποίου θα πραγματοποιείται η εγγραφή και ταυτοποίηση των πολιτών με δικαίωμα ψήφου. Το ζήτημα της επαλήθευσης της ταυτότητας των ψηφοφόρων είναι θεμελιώδες για να διασφαλιστεί ότι οι ψήφοι δεν κλέβονται, πωλούνται ή εκβιάζονται. Έχουν προταθεί αρκετές μέθοδοι βασισμένες στο blockchain για τον ελέγχου ταυτότητας των ψηφοφόρων. Το μεγαλύτερο πρόβλημα που αντιμετωπίζουν σύγχρονα συστήματα και προτάσεις ηλεκτρονικής ψηφοφορίας, είναι η έλλειψη εγγύησης καλώς συνθηκών. Με την ύπαρξη ενός ασφαλούς και έμπιστου συστήματος ταυτοποίησης, παρέχεται εγγύηση στο απόρρητο της ψηφοφορίας.

Οι τεχνικές που υιοθετούνται για την ταυτοποίηση από συστήματα ηλεκτρονικής ψηφοφορίας είναι συγκεκριμένα.

- Ταυτοποίηση μέσω **τηλεφώνου**: Η μόνη ερευνητική εργασία στην οποία πραγματοποιείται η ταυτοποίηση με τη χρήση του αριθμού τηλεφώνου είναι εκείνη που παρουσιάζεται στο έγγραφο [Kho+18]. Στη μέθοδο που υλοποιείται σε αυτή την εργασία, κάθε ψηφοφόρος για να ψηφίσει θα πρέπει να έχει συνδρομή τηλεφώνου, σε κάποιο τηλεφωνικό πάροχο.

- Ταυτοποίηση με έλεγχο **ταυτότητας**: Σε αυτή τη μέθοδο αυθεντικοποίησης, το σύστημα θα πρέπει να επεξεργαστεί γρήγορα τα σαρωμένα αντίγραφα εκατομμυρίων χρηστών. Το κάθε σαρωμένο αντίγραφο θα πρέπει να ληφθεί αμέσως παρέχοντας βεβαίωση ότι δε πρόκειται για απάτη.

- Ταυτοποίηση με έλεγχο **ιδιωτικού / δημόσιου** κλειδιού: Αποτελεί τη πιο κοινή μέθοδο ελέγχου ταυτότητας σε εφαρμογές ηλεκτρονικής ψηφοφορίας μέσω blockchain. Κατά κύριο λόγο χρησιμοποιείται ο αλγόριθμος Elliptic curve, επειδή πληρεί πολλά κριτήρια ασφαλείας. Με τη χρήση αυτού του αλγορίθμού όμως, παραμονεύει ο κίνδυνος ένας ψηφοφόρος να πουλήσει το ιδιωτικό του κλειδί, ή να χάσει το κωδικό πρόσβασής του. Πιθανό να απαιτεί την αποθήκευση του από μια κεντρική αρχή, κάνοντας προβληματική τη διαφάνεια της ψηφοφορίας, και αφαιρώντας την αποκεντρικότητα στην οποία στοχεύει. Επομένως, ο έλεγχος ταυτότητας με δημόσιο/ιδιωτικό κλειδί δεν είναι τέλειος και φέρνει τη δυνατότητα μιας άλλης ισχυρότερης μεθόδου: του βιομετρικού ελέγχου ταυτότητας.

- **Βιομετρικός** έλεγχος ταυτότητας: Οι περισσότερες ερευνητικές εργασίες, όπως για παράδειγμα η [RS20], βασίζονται στη χρήση μεθόδου βιομετρικής επαλήθευσης ταυτότητας για το ψηφοφόρο κατά τη ψηφοφορία. Μέσω αυτής της μεθόδου αυθεντικοποίησης αντιμετωπίζεται το πρόβλημα ανταλλαγής κλειδιών που αναφέρθηκε παραπάνω. Προτείνεται η δημιουργία μιας τιμής κατακερματισμού που θα σχηματίζεται μέσω ενός δαχτυλικού αποτυπώματος ή φωτογραφίας του ματιού, καθιστώντας την ταυτοποίηση πιο ασφαλή από την αποστολή ενός κωδικού μέσω email. Με αυτό το τρόπο διασφαλίζεται ότι ο χρήστης που καταβάλει κάθε ψήφο, είναι αυτός που ισχυρίζεται ότι είναι. Για την υλοποίηση όμως μιας βιομετρικής μεθόδου ταυτοποίησης, απαιτεί κάθε ψηφοφόρος να έχει μια συσκευή που να επιτρέπει μετάδοση των βιομετρικών του δεδομένων. Λόγω του μεγάλου πλήθους κοινωνικών ομάδων η κατανόηση ή αγορά μιας τέτοιας τεχνολογίας είναι σχεδόν αδύνατη.

Αλγόριθμοι κρυπτογράφησης / κατακερματισμού ψηφοφορίας

Με την επιτυχία της ταυτοποίησης του χρήστη, πρέπει να ακολουθήσει η αποθήκευση της ψήφου στο blockchain, διατηρώντας παράλληλα την ανωνυμία που απαιτείται. Μέσω των αλγορίθμων κρυπτογράφησης / κατακερματισμού διασφαλίζεται η ασφάλεια και η ακεραιότητα των συναλλαγών κατά τη διάρκεια των εκλογών, συναλλαγές που μπορεί να αφορούν την αποθήκευση των ψήφων αλλά και άλλα δεδομένα απαραίτητα για την ταυτοποίηση των χρηστών. Υπάρχουν διάφοροι κρυπτογραφικοί αλγόριθμοι που χρησιμοποιούνται σε αντίστοιχα συστήματα ή προτάσεις συστημάτων ψηφοφορίας.

- Ένας από τους αλγορίθμους που χρησιμοποιείται περισσότερο σε αυτές τις περιπτώσεις είναι ο **SHA-256**, αλγόριθμος που εξηγήθηκε αναλυτικά στο κεφάλαιο 2. Είναι ένας από τους πλέον πιο αξιόπιστους αλγορίθμους.

- Η **ομομορφική** κρυπτογράφηση, επιτρέπει τη χρήση και λειτουργία κρυπτογραφημένων δεδομένων, χωρίς να απαιτείται η αποκρυπτογράφηση τους. Στην περίπτωση συστήματος ψηφοφορίας, αυτή η ιδιότητα επιτρέπει την καταμέτρηση κρυπτογραφημένων ψηφοδελτίων από τρίτο μέρος χωρίς να αποκαλύπτονται πληροφορίες που περιέχονται στο ψηφοδέλτιο.

- Η **Απόδειξη Μηδενικής Γνώσης** χρησιμοποιείται συχνά για την απόδειξη μιας κατάστασης, χωρίς να αποκαλύπτονται πρόσθετες πληροφορίες. Σε ένα εκλογικό σύστημα, μπορεί να χρησιμοποιηθεί έτσι ώστε ο ψηφοφόρος να αποδείξει την εγκυρότητα του ψηφοδελτίου του, χωρίς να αποκαλύψει τη ψήφο του.
- Η **τυφλή υπογραφή**, είναι πολύ χρήσιμη για την παροχή της ανωνυμίας του χρήστη. Τα συστήματα ψηφοφορίας χρησιμοποιούν τυφλή υπογραφή για να πείσουν το κέντρο μέτρησης ότι το ψηφοδέλτιο προέρχεται από έγκυρο ψηφοφόρο, χωρίς να αποκαλύπτεται ο ιδιοκτήτης του ψηφοδελτίου. Ταυτόχρονα, η αρχή που υπογράφει το ψηφοδέλτιο δε μαθαίνει τίποτα για τις επιλογές του ψηφοφόρου. Στην τυφλή υπογραφή, τόσο οι ψηφοφόροι όσο και το κέντρο καταμέτρησης πρέπει να εμπιστεύονται τον υπογράφοντα. Όταν ο ψηφοφόρος υπογράφει το ψηφοδέλτιο, πρέπει να περιλαμβάνει τα δημόσια κλειδιά άλλων ψηφοφόρων ώστε η υπογραφή του να μη διακρίνεται από εκείνες άλλων ψηφοφόρων. Συγκρίνοντας την ετικέτα δυνατότητας σύνδεσης, η αρχή μπορεί εύκολα να πει εάν αυτός ο ψηφοφόρος έχει ήδη ψηφίσει.

Αντίσταση σε επιθέσεις

Η αντίσταση των εκλογικών συστημάτων σε επιθέσεις είναι πολύ σημαντική. Ερευνητικές εργασίες που αναφέρθηκαν προηγουμένως αναφέρουν τη δυνατότητα αντίστασης σε ορισμένες επιθέσεις, καθώς είναι αδύνατο να ισχυριστεί κανείς ότι μια εφαρμογή είναι πλήρως ασφαλής έναντι όλων των κυβερνοεπιθέσεων, εάν δεν έχει δοκιμαστεί σε μεγάλη κλίμακα. Στην εργασία [Ben+22] γίνεται ένας λεπτομερής σχολιασμός ερευνητικών εργασιών για εκλογικά συστήματα μέσω blockchain και συγκεκριμένες επιθέσεις από τις οποίες προστατεύεται κάθε εφαρμογή. Πιο συγκεκριμένα αναφέρονται προτάσεις εκλογικών συστημάτων, που θα αντιμετώπιζαν επιτυχώς μερικές από τις παρακάτω 6 μορφές επιθέσεων.

1. **DDoS**: Η επίθεση κατανεμημένης άρνησης υπηρεσίας, όπως αναφέραμε και στο κεφάλαιο 3.1.2, αποτελούν μία από τις πιο κρίσιμες προκλήσεις που αντιμετωπίζουν σήμερα οι ειδικοί σε επιθέσεις στον κυβερνοχώρο. Η διανομή της υπηρεσίας σε διαφορετικούς κόμβους, η οποία είναι δυνατή με ένα blockchain, φαίνεται να είναι μια λύση στην επίθεση DDoS, επειδή είναι σχεδόν αδύνατο για τον αντίπαλο να παραβιάσει όλους τους διακομιστές. Εάν συμβεί μια επίθεση DDoS, το σύστημα θα συνεχίσει να λειτουργεί χωρίς καμία διακοπή λόγω της κατανεμημένης φύσης του.
2. **Sybil attack**: Μερικά συστήματα [Zha+18] - [Hjá+18] αναφέρουν την αντίσταση σε επίθεση Sybil. Σε μια τέτοια επίθεση, ο εισβολέας παρακάμπτει το σύστημα ενός κατανεμημένου peer-to-peer δικτύου δημιουργώντας μια μεγάλη ποσότητα ταυτοτήτων και χρησιμοποιώντας τες για να ασκήσει δυσανάλογη επιρροή, η οποία, στην περίπτωση της ψηφοφορίας, είναι δραματική. Μια τέτοια επίθεση θα μπορούσε να στρεβλώσει το αποτέλεσμα των εκλογών.
3. **MITM (Man-In-The-Middle)**: Μερικές ερευνητικές εργασίες όπως η [Lyu+19] αναφέρουν ότι είναι ανθεκτικά σε επιθέσεις MITM. Οι ιδιότητες του blockchain επιτρέπουν την αντίσταση σε αυτήν την επίθεση με αυτόματο τρόπο, καθώς κάθε συναλλαγή που υλοποιείται με το έξυπνο συμβόλαιο υπογράφεται από τους ψηφοφόρους. Αφού τα δεδομένα ψηφοφορίας είναι κρυπτογραφημένα, ένας επιτιθέμενος δεν μπορεί να πλαστογραφήσει την υπογραφή ή να αλλάξει τα δεδομένα που εμπλέκονται στις συναλλαγές.
4. **Βυζαντινό σφάλμα**: Αυτή η μορφή επίθεσης εμφανίζεται όταν κάποιοι από τους ψηφοφόρους δεν είναι αξιόπιστοι, και μπορούν να αλλάξουν τους κανόνες μιας ψηφοφορίας. Πολλές εργασίες είναι ανεκτικές σε βυζαντινά σφάλματα, πράγμα που σημαίνει ότι κανένας κόμβος στο δίκτυο δεν μπορεί να επηρεάσει άλλους κόμβους σχετικά με τη συναίνεση.

5. **Καταναγκασμός (Coercion-Resistance)**: Συμβαίνει όταν ένας ψηφοφόρος δεν μπορεί να αποδείξει ότι ψήφισε με συγκεκριμένο τρόπο. Οι περισσότερες εφαρμογές είναι επιρρεπείς σε αυτόν το τύπο επίθεσης, καθώς είναι αδύνατο να αποτραπεί ένας χρήστης από το να ψηφίσει μπροστά σε κάποιον άλλο ή να πουλήσει τη ψήφο του σε κάποιον οργανισμό.

6. **Brute-Force**:Μια επίθεση Brute-Force συνίσταται στην προσπάθεια εισαγωγής ενός μέγιστου κωδικού πρόσβασης στο σύστημα και κατά συνέπεια της ψηφοφορίας. Με την προσθήκη κλειδιών κατάλληλου μεγέθους ή με τη λήψη κατάλληλων μέτρων από το σύστημα είναι εύκολο να αποφευχθεί μια τέτοια μορφή επίθεσης.

Ιδιότητες ασφαλείας

Κάθε σύστημα ψηφοφορίας, είτε υλοποιείται με το παραδοσιακό τρόπο είτε είναι σε ηλεκτρονική μορφή θα πρέπει να είναι αξιόπιστο. Πάντα θα υπάρχουν κακόβουλοι που θα προσπαθούν να τροποποιήσουν ή να χειραγωγήσουν τις ψήφους και επομένως τα αποτελέσματα της ψηφοφορίας. Στο [Ben+22] ορίζονται μερικές ιδιότητες ελάχιστης ασφάλειας που θα πρέπει να έχει οποιοδήποτε εκλογικό σύστημα. Οι περισσότερες ερευνητικές εργασίες ελέγχουν μέσω audit εάν το σύστημα λειτουργεί σωστά σε όλα τα μέρη του.

Οι ιδιότητες ελάχιστης ασφάλειας που παρουσιάζονται είναι οι εξής:

- Η δυνατότητα **επαλήθευσης από τους ψηφοφόρους**: Κάθε χρήστης θα πρέπει να μπορεί να ελέγξει ότι η ψήφος του έχει προστεθεί και έχει καταμετρηθεί σωστά.

- Η **μεταβλητότητα των ψήφων**: ένας χρήστης θα μπορεί να έχει τη δυνατότητα να αλλάξει τη δική του ψήφο.

- Η **ακεραιότητα δεδομένων**: Η διαφάνεια και η ακεραιότητα των δεδομένων είναι βασικές ιδιότητες του blockchain. Εγγυάται ότι τα δεδομένα δεν πρέπει ποτέ να αλλοιωθούν κατά τη μετάδοση ή επεξεργασία τους.

- Η **ιδιωτικότητα**: είναι απαραίτητη για την προστασία των χρηστών από τη διαρροή των προσωπικών τους στοιχείων. Στα περισσότερα συστήματα, ένα ζεύγος στοιχείων σύνδεσης και κωδικών πρόσβασης παρέχονται από μια κεντρική αρχή.

- Η **εμπιστευτικότητα**: είναι μια από τις πιο σημαντικές ιδιότητες. Ένας ψηφοφόρος δεν πρέπει ποτέ να αναγνωρίζεται από την ψήφο του.

- Η **δικαιοσύνη**: κανείς δε θα πρέπει να γνωρίζει ποιος υποψήφιος προηγείται στις εκλογές και δεν θα επηρεαστούν άλλοι ψηφοφόροι.

- Η **επιλεξιμότητα**: μόνο οι δικαιούχοι μπορούν να ψηφίσουν. Αυτή η ιδιότητα δεν μπορεί να εκπληρωθεί αυστηρά σε μια απομακρυσμένη ηλεκτρονική ψηφοφορία επειδή απαιτεί σύνδεση στο Διαδίκτυο και υπολογιστή. Επίσης, η επέμβαση των εκλογικών αρχών για αυτό τον έλεγχο και τη λίστα ψηφοφόρων θα μπορούσε να θεωρηθεί αναγκαία.

- Η **διαφάνεια**: οποιαδήποτε μορφή ανοιχτού κώδικα είναι πάντα καλύτερη, ειδικά όταν προέρχεται από ένα έξυπνο συμβόλαιο λόγω των ιδιοτήτων διαφάνειας του.

- Η **απόδειξη ψήφου**: προορίζεται να αποτρέψει την αγορά ψήφων, καθώς ένας ψηφοφόρος δε θα μπορεί να αποδείξει την ψήφο του σε έναν τρίτο ή στις εκλογικές αρχές.

Πρόσθετες αναφορές

Υπάρχει μεγάλο πλήθος ερευνητικών εργασιών για τη δημιουργία ενός ασφαλούς εκλογικού συστήματος βασισμένο στο blockchain. Στο άρθρο [TT20] απαντιούνται 5 βασικές ερωτήσεις:

1. Ποια είναι τα τρέχοντα κενά σε συστήματα ηλεκτρονικής ψηφοφορίας;
2. Μπορεί η ιδέα του blockchain να βελτιώσει τα συστήματα ηλεκτρονικής ψηφοφορίας;
3. Ποια είναι τα ερευνητικά θέματα και οι προτεινόμενες λύσεις που έχουν δημοσιευθεί στην ηλεκτρονική ψηφοφορία βασισμένη στο blockchain;
4. Ποιες πλατφόρμες blockchain/μοντέλα συναίνεσης χρησιμοποιούνται;
5. Ποιες είναι οι μελλοντικές κατευθύνσεις έρευνας για το σύστημα ηλεκτρονικής ψηφοφορίας που βασίζεται σε blockchain;

Κεφάλαιο 4

Προτεινόμενο σύστημα

Έχοντας δει το τρόπο λειτουργίας των ήδη προτεινόμενων εκλογικών συστημάτων, και τις τεχνικές που εκείνα υιοθετούν, έχουμε τα δεδομένα που χρειαζόμαστε για τη δημιουργία ενός πιο ασφαλούς συστήματος εκλογών. Σκοπός του συστήματος θα είναι η πλήρης εκμετάλλευση των χαρακτηριστικών που προσφέρει το blockchain. Επομένως, το σύστημα θα είναι εντελώς αποκεντρωμένο ακόμη και στο τομέα της ταυτοποίησης όσο είναι δυνατό.

Σε αυτή την ενότητα, αρχικά θα κάνουμε μια πιο λεπτομερή μελέτη και αναφορά στα συστήματα / ερευνητικές εργασίες των οποίων τεχνικές θα υιοθετηθούν από το δικό μας προτεινόμενο σύστημα. Στη συνέχεια θα γίνει μια μελέτη στο τρόπο λειτουργίας του προτεινόμενου εκλογικού συστήματος και των φάσεων από τις οποίες θα αποτελείται.

4.1 Τεχνικές που υιοθετήθηκαν

Το Ethereum είναι η μεγαλύτερη ανοιχτή πλατφόρμα που εκτελείται στο blockchain [Shu+18], [Zha+19]. Το blockchain του Ethereum χρησιμοποιεί ένα δημόσιο κατανεμημένο δίκτυο. Κάθε συναλλαγή υπογράφεται κρυπτογραφικά και επικυρώνονται δημόσια, διασφαλίζοντας ότι τα κρυπτογραφημένα δεδομένα στο blockchain δεν μπορούν να τροποποιηθούν [Anw+22]. Έχοντας μελετήσει όλες τις τεχνικές που χρησιμοποιούν αντίστοιχα εκλογικά συστήματα και που έχουν αναλυθεί στην ερευνητική εργασία [Ben+22], σε αυτό το υπό κεφάλαιο θα κάνουμε μια πιο λεπτομερή μελέτη σε τεχνικές που υιοθετήθηκαν από συγκεκριμένες εργασίες και ήδη υπάρχοντα συστήματα. Θα αναφερθούμε κυρίως στο τομέα της ταυτοποίησης πολιτών, μιας και είναι ένα από τα πιο μείζων ζητήματα που χρήζουν επίλυσης. Οι υπόλοιπες λειτουργίες του εκλογικού συστήματος θα βασίζονται στην ταυτοποίηση. Σκοπός είναι η δημιουργία μιας πλήρης αποκεντρωμένης πλατφόρμας χωρίς την ύπαρξη κάποιας κεντρικής βάσης δεδομένων, η οποία θα καθιστά το σύστημα αναξιόπιστο στους ψηφοφόρους. Πιο συγκεκριμένα οι τεχνικές που υιοθετήθηκαν είναι οι εξής:

1. Σύμφωνα με το [Ben+22] η μόνη χρήση αριθμού τηλεφώνου για τον έλεγχο ταυτότητας ψηφοφόρου παρουσιάζεται στο έγγραφο [Kho+18]. Μόνο οι πολίτες που έχουν συνδρομή τηλεφώνου επιτρέπεται να έχουν πρόσβαση στην ψηφοφορία.

2. **i - voting**: Η Εσθονία είναι η πρώτη χώρα που εισήγαγε την ηλεκτρονική ψηφοφορία στις εθνικές εκλογές από το 2005 [Ehi+22], χρησιμοποιώντας ένα ηλεκτρονικό τσιπ ταυτότητας [Par20]. Αυτή η ταυτότητα δημιουργεί υπογραφές SHA1/SHA2 και χρησιμοποιήθηκε για την αναγνώριση πολιτών. Ο ψηφοφόρος θα έπρεπε να κατεβάσει την εφαρμογή, να ελέγξει την ταυτότητα και στη συνέχεια να ακολουθήσει η διαδικασία ψηφοφορίας. Η ψηφοφορία κρυπτογραφείται με το δημόσιο κλειδί των εκλογών και το ιδιωτικό κλειδί του χρήστη. Στη συνέχεια, η ψήφος αποθηκεύεται σε διακομιστή που ελέγχεται από την κυβέρνηση της Εσθονίας.

3. **Αριθμός Aadhaar**: Υπάρχουν πολλά μοντέλα ή προτάσεις που αναπτύσσονται για ινδικά εκλογικά συστήματα, χρησιμοποιώντας το UIDAI Aadhaar, το οποίο είναι ένα μοναδικό αναγνωριστικό που δημιουργήθηκε για κάθε εγγεγραμμένο χρήστη στην Ινδία. Αυτά τα συστήματα υιοθετούν το εσθονικό σύστημα και χρησιμοποιούν αυτό το αναγνωριστικό ως ιδιωτικό κλειδί, μαζί με το δημόσιο κλειδί των εκλογών, δημιουργόντας μια ψηφιακή υπογραφή για σκοπούς ψηφοφορίας [AS19]. Μια άλλη ερευνητική εργασία που δημοσιεύτηκε το 2020, προτείνει ένα σύστημα ψηφοφορίας που βασίζεται σε blockchain, το οποίο συνδυάζει τον αριθμό Aadhaar με τον βιομετρικό έλεγχο ταυτότητας. Ο ψηφοφόρος πρέπει να προεγγραφεί, χρησιμοποιώντας ένα εικονικό αναγνωριστικό που αποκτήθηκε από το UIDAI. Η ασύμμετρη κρυπτογράφηση χρησιμοποιείται για την επαλήθευση ψήφων. Το δακτυλικό αποτύπωμα των ψηφοφόρων μετατρέπεται σε ψηφιακή υπογραφή που μπορεί να χρησιμοποιηθεί για να διασφαλιστεί η ασφάλεια των ψήφων [RS20].

4. Ψηφοφορία με **έλεγχο ταυτότητας πολλαπλών παραγόντων**: Αυτό το μοντέλο χρησιμοποιεί μια βάση δεδομένων που περιέχει την ταυτότητα του ψηφοφόρου, μαζί με τον αριθμό τηλεφώνου και άλλες προσωπικές πληροφορίες. Κάθε ψηφοφόρος πρέπει να εγγραφεί και να δημιουργήσει το PIN του. Μετά την ταυτοποίηση κάθε δικαιούχου ψηφοφόρου με τον αριθμό ταυτότητας και το PIN του, λαμβάνει χώρα η διαδικασία ψηφοφορίας, εισάγοντας έναν κωδικό πρόσβασης μίας χρήσης (one time password) που έλαβε στη φάση ελέγχου ταυτότητας. Τέλος, η ψήφος αποθηκεύεται στο blockchain [AOB19].

5. Οι ερευνητές πρότειναν ένα εκλογικό σύστημα που λειτουργεί ως εξής. Κάθε ψηφοφόρος πρέπει να εγγραφεί, παρέχοντας τον αριθμό ταυτότητάς του και άλλα προσωπικά του δεδομένα, τα οποία αποθηκεύονται σε νέο μπλοκ. Το σύστημα προσθέτει ψηφοφόρους στη λίστα. Στη συνέχεια πραγματοποιείται η εκλογική διαδικασία, με το εκλογικό αποτέλεσμα να εμφανίζεται μόλις ολοκληρωθούν οι εκλογές [Anw+22].

6. Ερευνητές από την Ινδονησία πρότειναν ένα σύστημα ψηφοφορίας blockchain χρησιμοποιώντας το Metamask. Κάθε χρήστης με έγκυρη διεύθυνση πρέπει να είναι εγγεγραμμένος από τον διαχειριστή για να μπορεί να χρησιμοποιεί το δικαίωμα ψήφου. Έτσι, επισημαίνοντας τη διεύθυνση Metamask ως έγκυρη, δίνοντάς του τη δυνατότητα να ψηφίσει. Η καταμέτρηση των ψήφων εκτελείται αυτόματα από το έξυπνο συμβόλαιο [PA20]. Σε ερευνητική εργασία [VSB21] πρότεινε ένα σύστημα που χρησιμοποιεί επίσης το Metamask. Μέρες πριν από τις εκλογές, οι ψηφοφόροι λαμβάνουν μια δημόσια διεύθυνση, με αρκετή ποσότητα ethers, η οποία θα χρησιμοποιηθεί αργότερα για έλεγχο ταυτότητας.

7. Το σύστημα **Save**, είναι μια πρόταση ηλεκτρονικού συστήματος ψηφοφορίας για τις πανεπιστημιακές εκλογές. Σε αυτό το σύστημα, κάθε ψηφοφόρος προσδιορίζεται από τις εκλογικές αρχές. Κατά τη διάρκεια αυτής της διαδικασίας αναγνώρισης, κάθε ψηφοφόρος λαμβάνει μια τυχαία μαγνητική κάρτα, που περιέχει έναν 13ψήφιο αριθμό. Με τη χρήση αυτής της κάρτας, κάθε ψηφοφόρος αναγνωρίζεται ως έγκυρος ψηφοφόρος [OP17].

8. Οι ερευνητές πρότειναν ένα ηλεκτρονικό σύστημα ψηφοφορίας βασισμένο στο Ethereum, το οποίο χρησιμοποιεί μια μέθοδο αποθήκευσης Διαπλανητικού Συστήματος Αρχείων (**IPFS**) που βασίζεται σε blockchain. Προτείνει έναν νέο τρόπο διασφάλισης της εμπιστευτικότητας με βάση μια βάση δεδομένων. Κάθε ψηφοφόρος θα πρέπει να εγγραφεί δημιουργώντας ένα αναγνωριστικό μέλους και έναν κωδικό πρόσβασης, τα οποία αργότερα χρησιμοποιούνται για τη δημιουργία μιας νέας διεύθυνσης. Οι διευθύνσεις και οι τιμές αναγνωριστικού μέλους κρυπτογραφούνται με αλγόριθμο AES και αποθηκεύονται στη βάση δεδομένων. Οι ψήφοι αποθηκεύονται στο Ethereum blockchain, εκμεταλλευόμενοι το κατανεμημένο μορφή του [Ahn22].

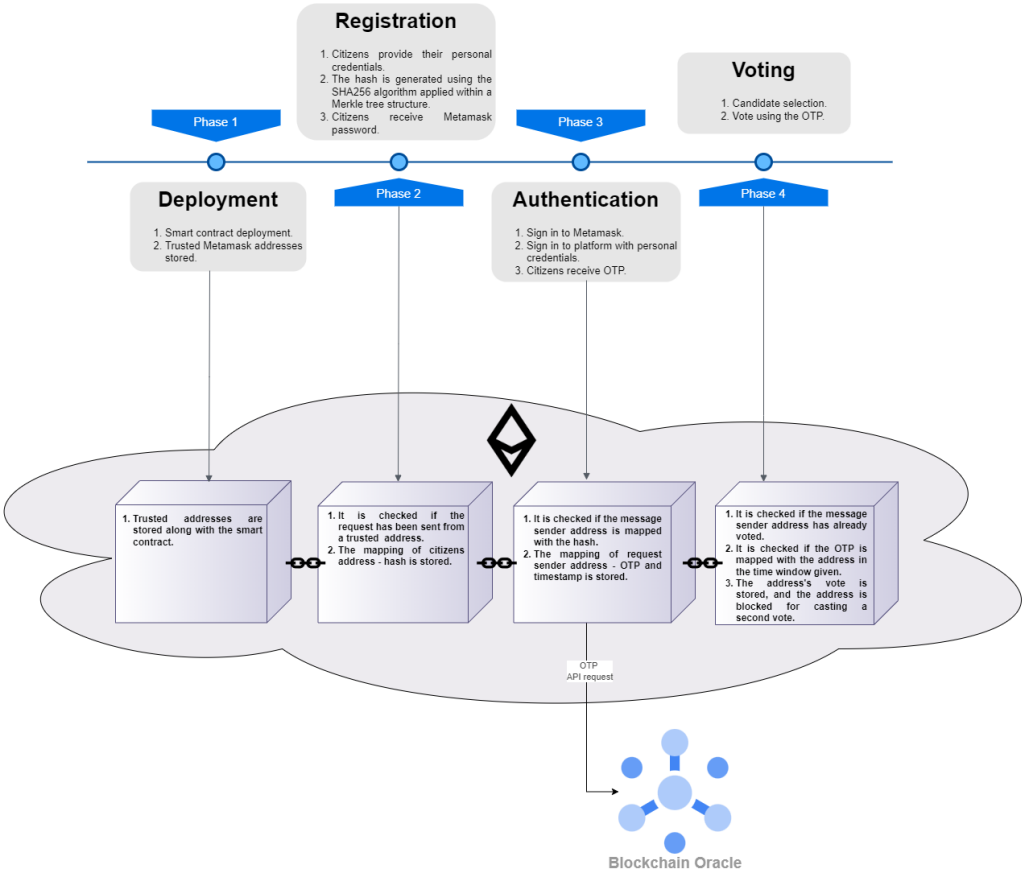
Παρά τον μεγάλο αριθμό ερευνητικών εργασιών, η ταυτοποίηση των πολιτών καθώς και το απόρρητο στην ψήφο εξακολουθεί να αποτελεί σημαντικό πρόβλημα για την ύπαρξη ενός ασφαλούς εκλογικού συστήματος, το οποίο θα μπορούσε να αλλάξει ριζικά τον τρόπο ψηφοφορίας σε όλο τον κόσμο. Σκοπός της παρούσας διπλωματικής εργασίας είναι η δημιουργία ενός εκλογικού συστήματος, με έμφαση στη γρήγορη, ασφαλή και χαμηλού κόστους αναγνώριση των πολιτών, που θα πραγματοποιηθεί με τη βοήθεια του Metamask και τη χρήση πολλαπλών παραγόντων ελέγχου ταυτότητας στο δημόσιο δίκτυο Ethereum. Η εργασία μας συνδυάζει τις μεθοδολογίες που προτείνονται στα παραπάνω συστήματα κυρίως στον τομέα της αναγνώρισης και ταυτοποίησης πολιτών. Με τον συνδυασμό και την τροποποίηση, όπου χρειάζεται, αυτών των μεθόδων ελέγχου ταυτότητας, και με την παράλληλη αντιστοίχιση των πολιτών με διευθύνσεις Metamask, θα μπορούσε να είναι ο ασφαλέστερος, ταχύτερος και πιο ολοκληρωμένος τρόπος για μια πλατφόρμα ψηφοφορίας χωρίς τη χρήση κεντρικής βάσης δεδομένων από τις αρχές. Στην εργασία μας θα σχολιάσουμε τους λόγους, για τους οποίους το σύστημά μας είναι μια βελτίωση των παραπάνω, σε οποιοδήποτε τομέα όπως η διαδικασία προ ψηφοφορίας, η ταυτοποίηση, η διαδικασία ψηφοφορίας, η ακεραιότητα των ψήφων, η προστασία των δικαιωμάτων των πολιτών και ο τρόπος με τον οποίο η ανάπτυξη τεχνολογιών blockchain και έξυπνων συμβολαίων μπορεί να επηρεάζουν παρόμοια συστήματα.

4.2 Λειτουργία συστήματος

Η ηλεκτρονική ψηφοφορία και οι παραδοσιακές μέθοδοι ψηφοφορίας σε χαρτί είναι τεχνικά αναξιόπιστες και δυσχεραίνουν την εξασφάλιση των αρχών των εκλογών. Το εκλογικό σύστημα που προτείνεται σε αυτή τη διπλωματική εργασία, βασίζεται σε blockchain, χωρίς τη χρήση οποιασδήποτε βάσης δεδομένων ή διακομιστή, επιτυγχάνοντας την πλήρη αποκεντροποίηση και διασφαλίζοντας το απορρήτου των εκλογών, και εστιάζει πλήρως στη **ταυτοποίηση** των ψηφοφόρων. Η διαδικασία ταυτοποίησης πολιτών με δικαίωμα ψήφου, η διαδικασία ψηφοφορίας και η αποθήκευση ψήφων θα βασίζεται αποκλειστικά στην αποθήκευση δεδομένων και στην κλήση λειτουργιών που θα υπάρχουν στο έξυπνο συμβόλαιο, το οποίο θα αποθηκευτεί στο δημόσιο blockchain του ethereum.

Η μόνη υπηρεσία που παρέχεται από τις αρχές είναι η καταγραφή της λίστας των πολιτών, με δικαίωμα ψήφου, στο blockchain. Επομένως, κάθε συναλλαγή είτε για αναγνώριση είτε για ψηφοφορία είναι δημόσια και μπορεί εύκολα να επαληθευτεί, αρκεί να διατηρηθούν παράλληλα όλα τα προσωπικά στοιχεία ασφαλή. Σε συστήματα που χρησιμοποιούν το blockchain ως βάση δεδομένων, και με τη χρήση των τεχνολογιών που προσφέρει, δεν είναι δυνατή η τροποποίηση ή η διαγραφή πληροφοριών. Σε κάθε ψηφοφόρο πολίτη θα εκχωρηθεί μια διεύθυνση Metamask - με τον **απαραίτητο αριθμό ethers**, για όλη την εκλογική διαδικασία.

Η εκλογική διαδικασία, και η διαδικασία που απαιτείται για τη ταυτοποίηση, ώστε να αποθηκευτεί μια ψήφος, χωρίζεται σε τέσσερις φάσεις. Οι πρώτες δύο από αυτές πραγματοποιούνται πριν από την ημέρα των εκλογών και είναι: Η ανάπτυξη της εφαρμογής και του έξυπνου συμβολαίου και η φάση εγγραφής. Οι άλλες δύο πραγματοποιούνται την ημέρα των εκλογών και περιλαμβάνουν την πιστοποίηση ταυτότητας των πολιτών και τη φάση της ψηφοφορίας.

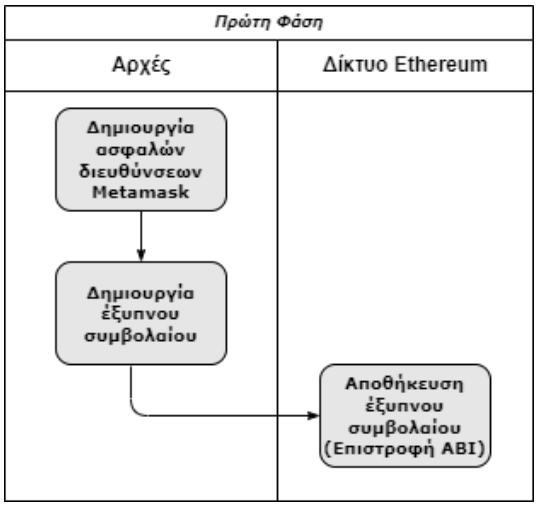


Σχήμα 12. Ψηφοφορια

Έχοντας δει τις τέσσερις φάσεις του συστήματός μου με ένα γενικό διάγραμμα, θα εξερευνήσουμε τις φάσεις αυτές με περισσότερη λεπτομέρεια και να εμβαθύνουμε ώστε να γίνουν κατανοητές οι λειτουργίες που πραγματοποιεί κάθε μία. Αυτό θα γίνει μέσω λεπτομερούς λεκτικής περιγραφής αλλά και ενός αναλυτικού διαγράμματος για κάθε φάση, το οποίο θα μας παρέχει βαθιά κατανόηση της λειτουργίας και των διαδικασιών που εμπλέκονται σε κάθε μία από αυτές τις φάσεις. Αυτή η λεπτομερής προσέγγιση θα μας επιτρέψει να ανακαλύψουμε τα πάντα για το πώς λειτουργεί το σύστημα, προσφέροντας μια εμπεριστατωμένη εικόνα του συνόλου των διαδικασιών που λαμβάνουν χώρα κατά τη διάρκεια της κάθε φάσης, και είναι απαραίτητη πριν προχωρήσουμε στην υλοποίηση.

4.2.1 Προεκλογικές φάσεις

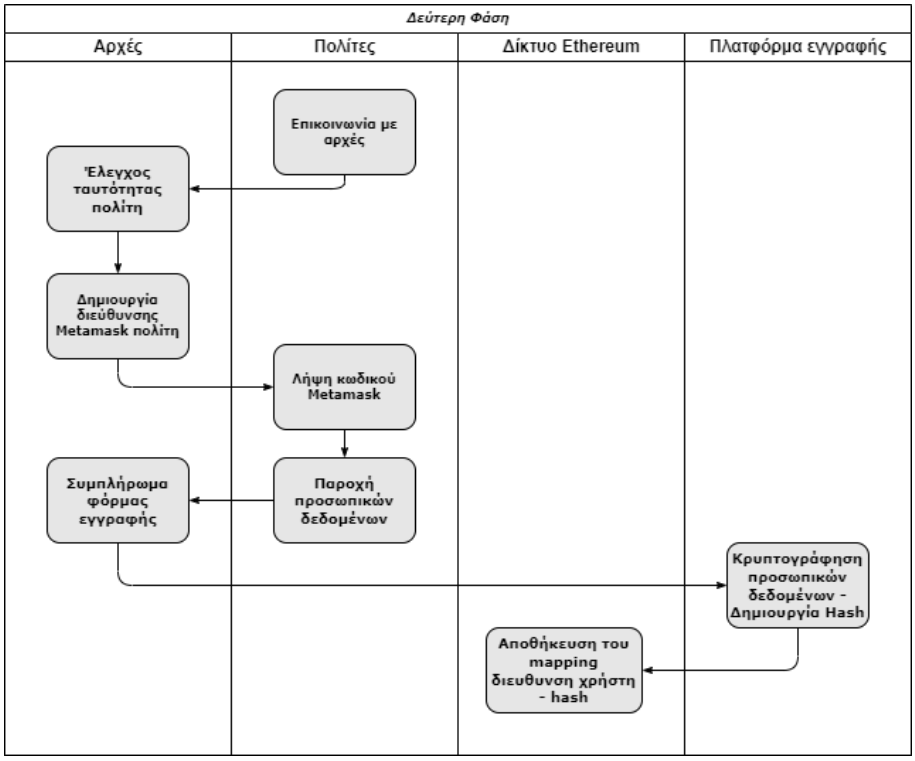
- Η πρώτη φάση αποτελείται από τη σύνταξη και την αποθήκευση του έξυπνου συμβολαίου στο blockchain Ethereum. Αρχικά δημιουργούνται διευθύνσεις Metamask, οι οποίες θα θεωρούνται 'έμπιστες' και θα ανήκουν στις εκλογικές αρχές. Μέσω αυτών των διευθύνσεων θα δημιουργηθεί το έξυπνο συμβόλαιο, καθώς επίσης μόνο αυτές οι έμπιστες διευθύνσεις θα έχουν δικαίωμα κλήσης συγκεκριμένων συναρτήσεων στο έξυπνο συμβόλαιο, δημιουργώντας περιορισμένη πρόσβαση, με σκοπό την αποφυγή από απάτες που θα μπορούσαν να διαστρεβλώσουν τα αποτελέσματα της ψηφοφορίας. Για παράδειγμα, μέσω μόνο έμπιστων διευθύνσεων θα αποθηκεύονται όλα τα ευαίσθητα προσωπικά δεδομένα των πολιτών με δικαίωμα ψήφου στο blockchain, όπως θα δούμε στη δεύτερη φάση, με στόχο τη χρήση αυτών των προσωπικών δεδομένων για έλεγχο ταυτότητας.



Σχήμα 13. Πρώτη φάση ψηφοφορίας

- Στη δεύτερη φάση, κάθε δικαιούχος πολίτης καλείται να εγγραφεί στην πλατφόρμα. Για να πραγματοποιηθεί η εγγραφή του, θα πρέπει είτε να παρευρεθεί είτε να επικοινωνήσει με τις αρχές. Οι αρχές πρέπει να συνδεθούν σε μία από τις «έμπιστες» διευθύνσεις (αναλύθηκαν στη **φάση 1**) και μετά τη δημιουργία ενός νέου λογαριασμού Metamask, με τον οποίο θα εκχωρηθεί ο πολίτης, θα εγγραφεί στην πλατφόρμα συνδέοντας τη διεύθυνση που δημιουργήθηκε πρόσφατα με προσωπικές πληροφορίες του πολίτη, όπως αριθμός ταυτότητας, όνομα, επώνυμο και αριθμός τηλεφώνου. Αν και οι μεταβλητές που θα αποθηκεύσουν τις πληροφορίες είναι ιδιωτικές, καθώς το δίκτυο Ethereum είναι δημόσιο, οποιοσδήποτε έχει αντίγραφο της αλυσίδας μπλοκ είναι σε θέση να ανακτήσει αυτές τις ιδιωτικές πληροφορίες. Για την αντιμετώπιση αυτού του κινδύνου, οι προσωπικές πληροφορίες κρυπτογραφούνται με τον κρυπτογραφικό αλγόριθμο SHA256, και με τη δομή ενός Merkle tree και αντιστοιχίζονται ως ζεύγος κλειδιού-τιμής με τη διεύθυνση που έχει εκχωρηθεί σε κάθε πολίτη. Αυτό σημαίνει ότι ο νέος λογαριασμός Metamask αποθηκεύτηκε στο blockchain, και έχει γίνει αντιστοίχιση με μια τιμή κατακερματισμού, της οποίας η αποκρυπτογράφηση είναι αδύνατη. Η επιλογή του κρυπτογραφικού αλγορίθμου SHA256, βασίζεται στην τεράστια δυσκολία αποκρυπτογράφησής του. Για μια διαδικασία όπως αυτή της ταυτοποίησης σε ένα εκλογικό σύστημα, δεν είναι επιθυμητή η αποκρυπτογράφηση ή τροποποίηση αυτών των προσωπικών δεδομένων, καθιστώντας το blockchain δίκτυο αλλά και το κρυπτογραφικό αλγόριθμο που επιλέχθηκε ιδανικά. Με την ολοκλήρωση της δεύτερης φάσης και αφού γίνει η αντιστοίχιση, κάθε πολίτης λαμβάνει τον κωδικό πρόσβασης για τον λογαριασμό Metamask με τον οποίο έχουν αντιστοιχιστεί. Η προσθήκη των δεδομένων στο Blockchain θα μπορούσε επί-

σης να γίνει σε ομάδες για μεγαλύτερη ευκολία. Τα επόμενα δύο στάδια πραγματοποιούνται την ημέρα των εκλογών.

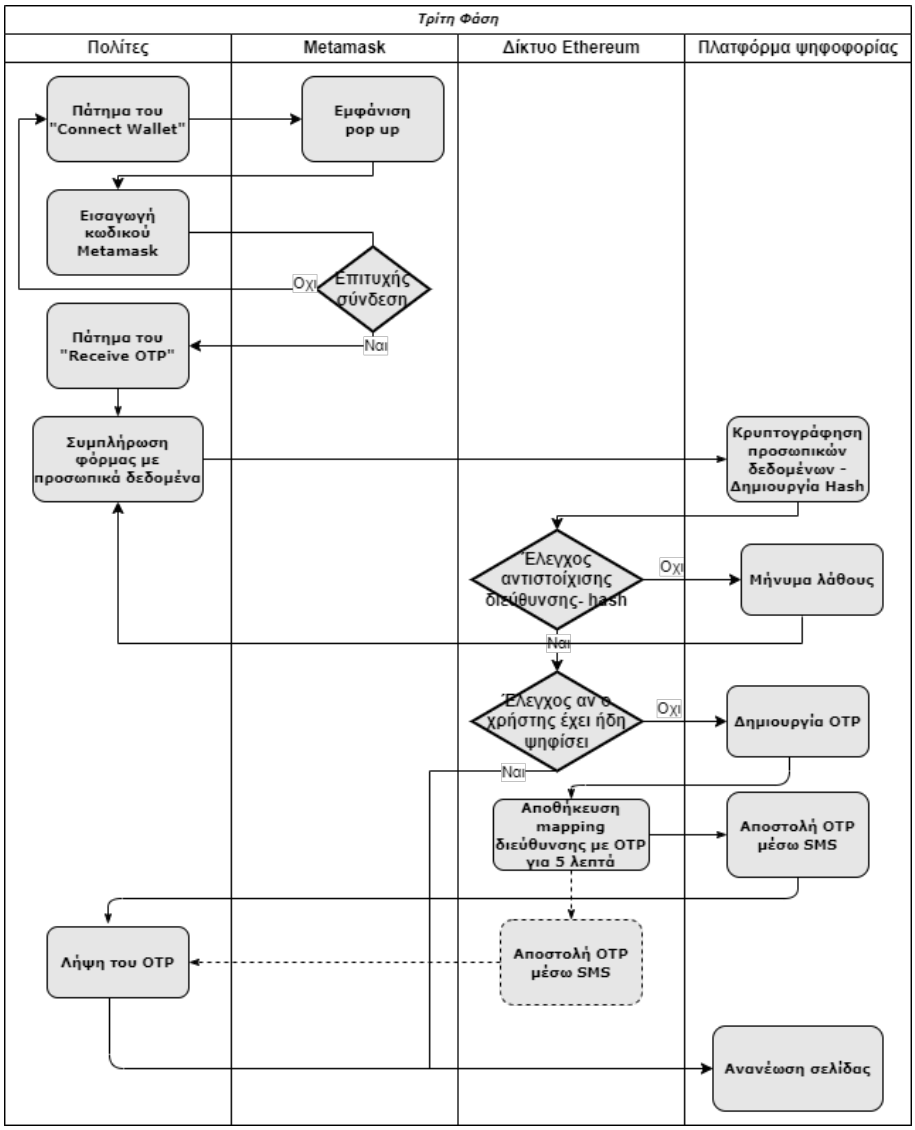


Σχήμα 14. Δεύτερη φάση ψηφοφορίας

4.2.2 Εκλογικές φάσεις

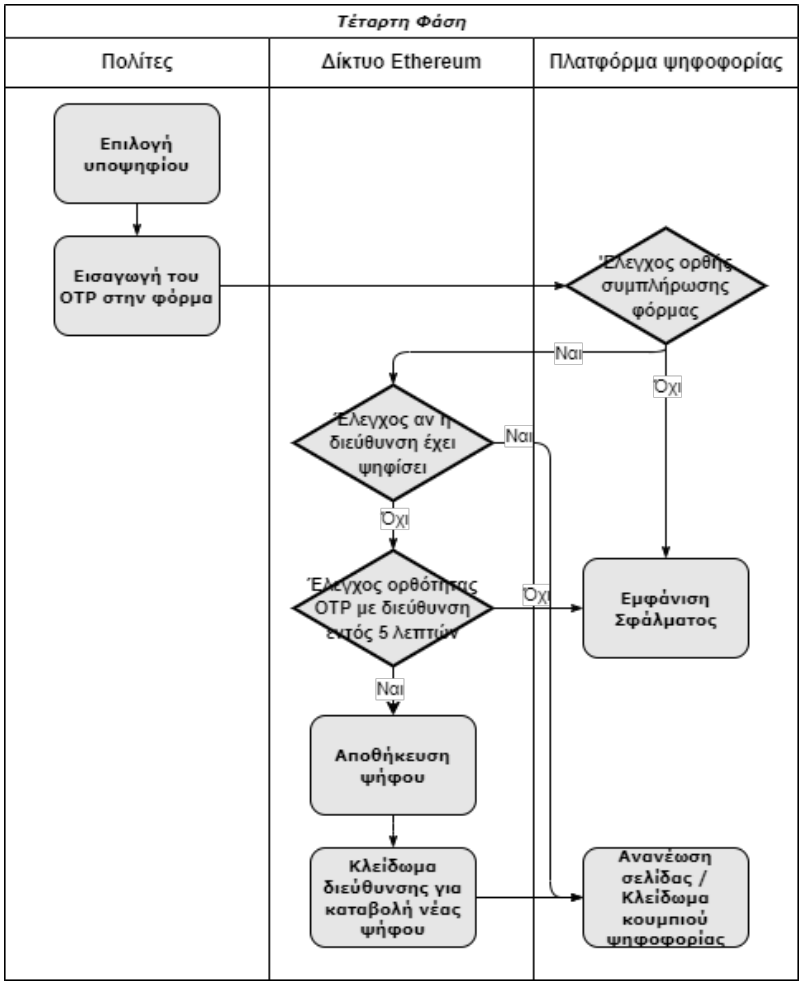
- Η τρίτη φάση είναι η διαδικασία ταυτοποίησης των ψηφοφόρων την ημέρα των εκλογών. Μόλις εισέλθουν στην πλατφόρμα ψηφοφορίας, θα πρέπει να συνδεθούν στον λογαριασμό τους στο Metamask εισάγοντας τον κωδικό πρόσβασης που έλαβαν την ημέρα της εγγραφής (**φάση 2**), δημιουργώντας έτσι την πρώτη παράμετρο αυθεντικοποίησης. Στη συνέχεια ως δεύτερη παράμετρος, θα πρέπει να συνδεθούν στην πλατφόρμα, εισάγοντας τα προσωπικά τους στοιχεία, με τα οποία έχει εκχωρηθεί η συγκεκριμένη διεύθυνση. Παρόμοια με το στάδιο 2, τα δεδομένα κρυπτογραφούνται με το SHA256. Έπειτα ακολουθεί ο έλεγχος αντιστοίχισης της διεύθυνσης αποστολής της συναλλαγής, με την τιμή κατακερματισμού που δημιουργήθηκε από την κρυπτογράφηση των προσωπικών δεδομένων. Η σύνδεση της πλατφόρμας με το Metamask, πριν ακολουθήσει η δεύτερη αυθεντικοποίηση είναι αναγκαία συνθήκη. Αν η αντιστοίχιση γίνει επιτυχώς, σημαίνει ότι το ζευγάρι " διεύθυνση - τιμή κατακερματισμού" υπάρχει στη λίστα ψηφοφόρων που δημιουργήθηκε στη δεύτερη φάση της εκλογικής διαδικασίας, και ότι η δεύτερη παράμετρος ταυτοποίησης ολοκληρώθηκε με επιτυχία. Σε αυτή την περίπτωση, θα δημιουργηθεί ένας μοναδικός κωδικός (OTP). Αυτός ο κωδικός αποθηκεύεται στο Blockchain, μαζί με την ώρα δημιουργίας του μπλοκ (**timestamp**), και αντιστοιχίζεται με τη διεύθυνση που αντιστοιχεί στον τρέχοντα ψηφοφόρο, ως ζεύγος κλειδιού - τιμής, όπως ακριβώς έγινε η αντιστοίχιση με τα προσωπικά στοιχεία, δημιουργώντας μια δεύτερη λίστα ψηφοφόρων, που λειτουργεί ως παράμετρος αυθεντικοποίησης για τη διαδικασία της ψηφοφορίας και όχι της ταυτοποίησης. Κάθε ψηφοφόρος λαμβάνει αυτόν τον μοναδικό κωδικό μέσω SMS στο τηλέφωνο που έχει δηλώσει. Ο αριθμός τηλεφώνου λαμβάνεται απευθείας από τη φόρμα, καθώς επιτυχής αντιστοίχιση της τιμής κατακερματι-

σμού, σημαίνει και σωστά προσωπικά δεδομένα. Η αποθήκευση της ώρας δημιουργίας του OTP, αποσκοπεί στη δημιουργία ενός παραθύρου χρόνου, για τη χρήση του. Με το πέρας αυτού του χρόνου, η ταυτοποίηση που παρουσιάστηκε σε αυτή τη φάση θα πρέπει να πραγματοποιηθεί ξανά. Ο αρχικός σχεδιασμός περιλαμβάνει την αποστολή του OTP, απευθείας από το έξυπνο συμβόλαιο μέσω ενός blockchain oracle (βλέπε διακεκομμένες σχήματος). Στην υλοποίηση ωστόσο, στάλθηκε από το κώδικα της διεπαφής, με την αποστολή μέσω ενός Oracle, να ορίζεται ως μελλοντική εργασία.



Σχήμα 15. Τρίτη φάση ψηφοφορίας

- Στη φάση 4, και στο τελευταίο στάδιο, αφορά τη διαδικασία της ψηφοφορίας. Κάθε ψηφοφόρος που έχει πραγματοποιήσει την ταυτοποίηση και έχει λάβει τον μοναδικό κωδικό στο κινητό, καλείται να ψηφίσει, επιλέγοντας από μια λίστα υποψηφίων, η οποία είναι επίσης αποθηκευμένη στο Blockchain. Μετά την επιλογή του υποψηφίου, ζητείται ο μοναδικός κωδικός που ελήφθη κατά την ταυτοποίηση προκειμένου να γίνει αποδεκτή η ψήφος. Σε περίπτωση που ο OTP είναι λανθασμένο ή έχει λήξει το χρονικό όριο, πρέπει να λάβει νέο OTP, εκτελώντας το δεύτερο στάδιο ταυτοποίησης που αναλύθηκε στη φάση 3. Σε αντίθετη περίπτωση, η συναλλαγή γίνεται με το blockchain, ο αριθμός των ψήφων του υποψηφίου που επιλέχθηκε από το ψηφοφόρο αυξάνεται κατά 1 και μετά την καταχώριση της ψήφου αλλάζει η κατάσταση της διεύθυνσης του ψηφοφόρου, ώστε να κλειδωθεί και να είναι δυνατό να προστεθούν περισσότερες από μία ψήφοι. Εάν η τρέχουσα διεύθυνση Metamask έχει καταχωρίσει την ψήφο του στο blockchain, σε αυτήν την περίπτωση, στο δεύτερο στάδιο αναγνώρισης δε θα δημιουργηθεί μοναδικός κωδικός και δεν υπάρχει δυνατότητα υποβολής δεύτερης ψήφου.



Σχήμα 16. Τέταρτη φάση ψηφοφορίας

Τέλος, οι αρχές, μέσω ασφαλών διευθύνσεων, λαμβάνουν τα αποτελέσματα των εκλογών, μόλις αυτές ολοκληρωθούν. Αυτή η διαδικασία δεν αφορά την ψηφοφορία ως προς την ταυτοποίηση, που εστιάζει η παρούσα διπλωματική εργασία, επομένως δε θεωρείτε ως ξεχωριστή φάση, και δε θα παρουσιαστεί αντίστοιχο διάγραμμα.

Κεφάλαιο 5

Υλοποίηση προτεινόμενου συστήματος

Γνωρίζοντας το τρόπο με τον οποίο θα λειτουργεί το εκλογικό σύστημα, θα παρουσιάσουμε την υλοποίηση. Θα ακολουθήσει μια μελέτη σχετικά με τα εργαλεία που είναι απαραίτητα για την υλοποίηση ενός αντίστοιχου συστήματος, συμπεριλαμβανομένων των γλωσσών προγραμματισμού που χρησιμοποιήθηκαν στην υλοποίηση αυτής της διπλωματικής εργασίας. Στη συνέχεια θα ακολουθήσει μια παρουσίαση της διεπαφής χρήστη, αλλά και μια προσομοίωση όλων των πιθανών ενεργειών που μπορεί να λάβουν μέρος στην πλατφόρμα συνοδευόμενες με τα κατάλληλα στιγμιότυπα οθόνης.

5.1 Εργαλεία

Για την υλοποίηση της πλατφόρμας ψηφοφορίας χρησιμοποιήθηκαν React Javascript για το περιβάλλον χρήστη και Solidity, για την δημιουργία του έξυπνου συμβολαίου.

5.1.1 React

Η React ή React Javascript, είναι βιβλιοθήκη JavaScript που αναπτύσσεται για την ανάπτυξη στοιχείων διεπαφής χρήστη (UI). Η React ουσιαστικά επιτρέπει την ανάπτυξη μεγάλων και πολύπλοκων εφαρμογών που βασίζονται στον ιστό που μπορούν να αλλάξουν τα δεδομένα του χωρίς επακόλουθες ανανεώσεις σελίδας. Χρησιμοποιείται ως προβολή στον ελεγκτή Model-View (MVC). Η React αφαιρεί το Document Object Model (DOM), προσφέροντας έτσι μια απλή, αποτελεσματική και ισχυρή εμπειρία ανάπτυξης εφαρμογών. Η React αποδίδει κυρίως στην πλευρά του διακομιστή χρησιμοποιώντας το NodeJS και η υποστήριξη για εγγενείς εφαρμογές για κινητά προσφέρεται χρησιμοποιώντας το React Native [Agg+18]. Η ReactJS παρουσιάζεται με μονόδρομη ροή δεδομένων μονής κατεύθυνσης μεταξύ των καταστάσεων και των επιπέδων σε μια εφαρμογή. Αυτό σημαίνει ότι τα δεδομένα μπορούν να ρέουν σε μία μόνο κατεύθυνση μεταξύ των καταστάσεων εφαρμογής και των επιπέδων. Με το περιορισμό πληροφοριών μίας κατεύθυνσης υπάρχει καλύτερος έλεγχος σε όλη την εφαρμογή.

JSX

Το JSX μπορεί καλύτερα να θεωρηθεί ως μια αυξημένη δομή γλώσσας που ακολουθεί την HTML [RM20]. Είναι ένας συνδυασμός της Javascript με την XML. Επιτρέπει το προσδιορισμό των στοιχείων DOM πριν από τα στοιχεία απευθείας στις εγγραφές JavaScript. [RM20]

DOM

Η React εισάγει την έννοια του εικονικού DOM (Document Object Model). Παρέχει δηλαδή μηχανισμό που επιτρέπει στη δομή (framework) να διατηρεί μια αναπαράσταση του όπως πρέπει να φαίνεται η διεπαφή χρήστη. Όταν αλλάξει η κατάσταση, το framework συγχρονίζει το εικονικό DOM με το «πραγματικό» DOM.

Npm

Το npm (Node Package Manager) [RM20] είναι ένας διαχειριστής πακέτων για τον κόμβο. Βοηθά στην εισαγωγή διαφορετικών πακέτων και στη διευθέτηση των διαφορετικών συνθηκών τους. Η χρήση πακέτων npm μπορεί να μειώσει το μέτρο του χρόνου που αναμένεται να ολοκληρωθεί η εκτέλεση.

5.1.2 Metamask

Το MetaMask είναι ένα πορτοφόλι κρυπτονομισμάτων που είναι διαθέσιμο ως επέκταση προγράμματος περιήγησης με σκοπό να βοηθήσει στην αλληλεπίδραση με αποκεντρωμένες εφαρμογές στο Ethereum. Συνδέοντας τους χρήστες με το MyEtherWallet, το MetaMask εξαλείφει την ανάγκη εισαγωγής ιδιωτικών κλειδιών κατά την εκτέλεση κάθε συναλλαγής κατά τη δημιουργία, αποθήκευση ή διαπραγμάτευση διακριτικών. Οι χρήστες μπορούν να αποθηκεύουν και να διαχειρίζονται τα Bitcoin, Ether και άλλα κρυπτονομίσματα χρησιμοποιώντας ένα πορτοφόλι blockchain, το οποίο είναι διαθέσιμο ως ψηφιακό ή διαδικτυακό πορτοφόλι. Μέσω του Metamask θα πραγματοποιούνται όλες οι επιθυμητές συναλλαγές με το Ethereum blockchain, που στη συγκεκριμένη εφαρμογή θα είναι ενέργειες όπως επαλήθευση στοιχείων, αποστολή ψήφου κοκ.

5.1.3 Solidity

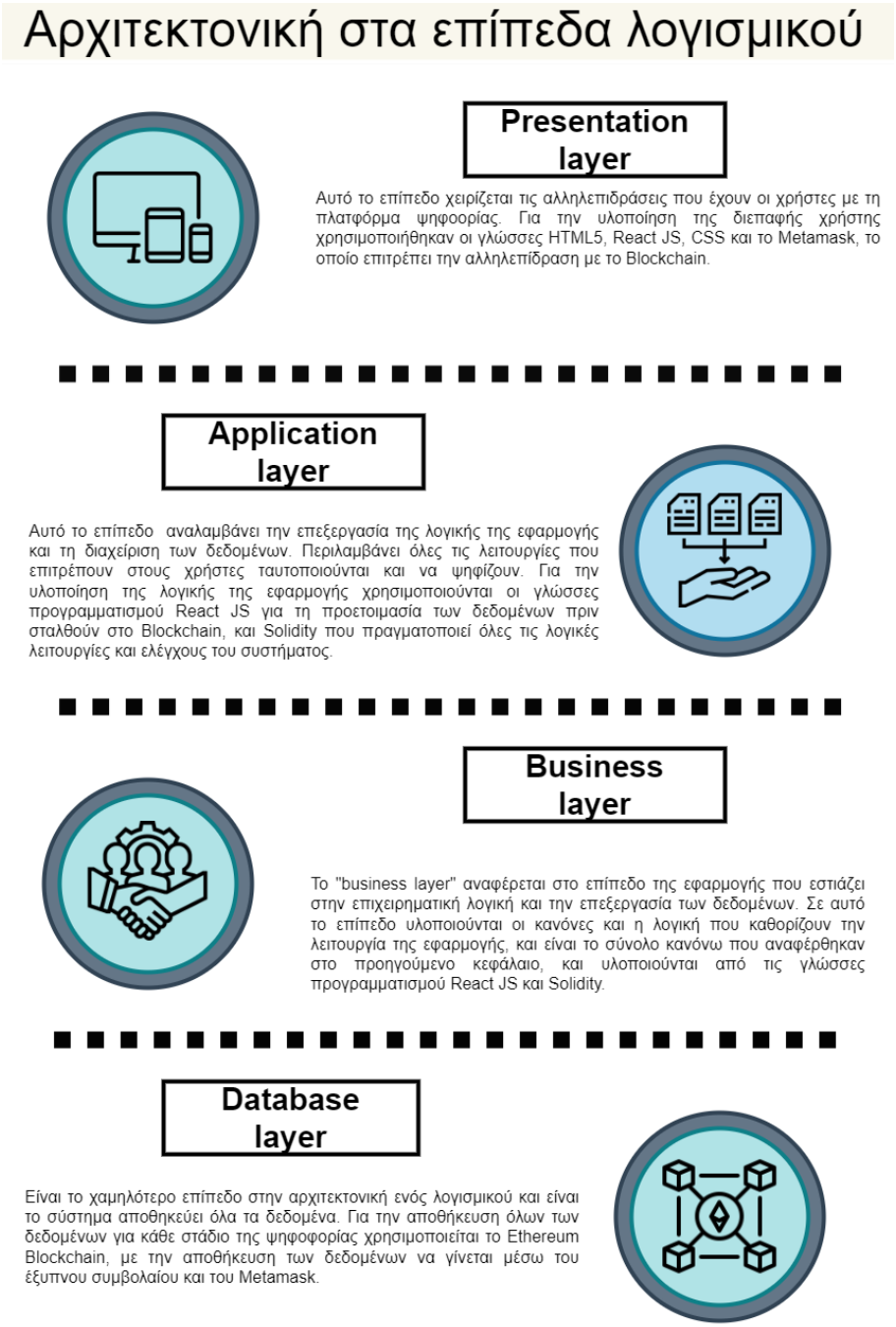
Σύμφωνα με το [WZ18] η Solidity είναι μια γλώσσα προγραμματισμού Turing υψηλού επιπέδου με παρόμοια σύνταξη JavaScript, που υποστηρίζει κληρονομικότητα και πολυμορφισμό, καθώς και βιβλιοθήκες και σύνθετους τύπους που ορίζονται από το χρήστη. Όταν χρησιμοποιείται το Solidity για την ανάπτυξη συμβολαίων, τα συμβόλαια είναι δομημένα παρόμοια με τις κλάσεις σε αντικειμενοστραφείς γλώσσες προγραμματισμού. Ο κώδικας του συμβολαίου αποτελείται από μεταβλητές και συναρτήσεις που τις διαβάζουν και τις τροποποιούν, όπως στον παραδοσιακό προγραμματισμό.

Η Solidity ορίζει ειδικές μεταβλητές (msg, block) που λειτουργούν ως δεσμευμένες λέξεις και περιέχουν ιδιότητες για πρόσβαση σε πληροφορίες σχετικά με μια συναλλαγή επίκλησης και την αλυσίδα μπλοκ, όπως η ανάκτηση της διεύθυνσης προέλευσης μιας συναλλαγής ή της ποσότητας του Ether των δεδομένων που αποστέλλονται.

Ένα άλλο ιδιαίτερο βολικό χαρακτηριστικό στη Solidity είναι οι modifiers. Είναι σε μορφή κλειστού κώδικα, και βοηθούν στη τροποποίηση της ροής εκτέλεσης κώδικα. Λόγω των modifiers, έχει τη μορφή προσανατολισμένου προγραμματισμού, με κύριο στόχο την αφαίρεση των “ υπό όρων“ μονοπατιών στις συναρτήσεις. Μπορούν να αλλάξουν εύκολα τη συμπεριφορά των συναρτήσεων. Μια τυπική περίπτωση χρήσης τους είναι ο έλεγχος ορισμένων συνθηκών πριν από την εκτέλεση της συνάρτησης, όπως στο σύστημά μας η αποστολή του αιτήματος από μια “ασφαλή διεύθυνση“.

Επίσης, άξιο αναφοράς, παρά το γεγονός ότι δε χρησιμοποιούνται στο σύστημά μας είναι τα **events**. Τα events δρουν ως σήματα που ενεργοποιήσουν τα έξυπνα συμβόλαια. Επιτρέπουν την “ακοή“ αυτών των events, από το επίπεδο της διεπαφής μιας εφαρμογής, ώστε να δράσει κατάλληλα.

Παρακάτω βλέπουμε μια εικόνα με τα επίπεδα που σχεδιάστηκαν με σκοπό να αντιπροσωπεύουν τη λειτουργία και τη δομή του λογισμικού μας. Έτσι μπορούμε να αντιληφθούμε καλύτερα το τρόπο υλοποίησης κάθε επιπέδου πριν ακολουθήσει η ανάλυση του έξυπνου συμβολαίου αλλά και της διεπαφής χρήστη.



Σχήμα 17. Επίπεδα αρχιτεκτονικής

/

5.2 Ανάλυση έξυπνου συμβολαίου

Αυτή η υπό ενότητα εξηγεί πως το προτεινόμενο σύστημα ψηφοφορίας, αναπτύσσεται και εκτελείται στο δίκτυο δοκιμής (test network) Sepolia του Ethereum. Οι λογαριασμοί Metamask χρησιμοποιούνται όχι μόνο για αλληλεπίδραση με το έξυπνο συμβόλαιο, αλλά και για έλεγχο ταυτότητας. Στην πρώτη φάση, αναπτύσσεται το έξυπνο συμβόλαιο. Οι διευθύνσεις Metamask των αρχών, που θεωρούνται ασφαλείς και αργότερα χρησιμοποιούνται για την εγγραφή του χρήστη, αποθηκεύονται στο έξυπνο συμβόλαιο μαζί με τους υποψηφίους. Οι υποψήφιοι αποθηκεύονται στο έξυπνο συμβόλαιο ως ιδιωτικές (**private**) τιμές uint256, οι οποίες αυξάνονται κάθε φορά που λαμβάνουν ψήφο. Αξίζει να επισημάνουμε ότι οι ονομασίες είναι ενδεικτικές καθώς το σύστημά μας εστιάζει κατά κύριο λόγο στο μεγαλύτερο πρόβλημα των συστημάτων ηλεκτρονικής ψηφοφορίας, που είναι η ταυτοποίηση ψηφοφόρων. Για μεγαλύτερη ασφάλεια, θα μπορούσαν να αποθηκευτούν τιμές κατακερματισμού ή γενικότερα κρυπτογραφημένες οι ονομασίες των υποψηφίων. Έτσι παρά το γεγονός ότι το blockchain είναι δημόσιο, δε θα γνωρίζει κανείς ποιος υποψήφιος έχει τις ψήφους που αναγράφονται.

```
uint256 private candidateA;
uint256 private candidateB;
uint256 private candidateC;
```

Σχήμα 18. Υποψήφιοι

Σε δεύτερη φάση, οι ψηφοφόροι επικοινωνούν με τις αρχές μέρες πριν τις εκλογές είτε τηλεφωνικά είτε αυτοπροσώπως, ώστε να εγγραφούν στο σύστημα. Οι αρχές δημιουργούν έναν λογαριασμό Metamask που θα συνδέεται με κάθε πολίτη, και θα τον αντιπροσωπεύει στην εκλογική διαδικασία. Μετά τη δημιουργία του πορτοφολιού, οι πολίτες παρέχουν στις αρχές, τα προσωπικά τους δεδομένα, όπως όνομα, επώνυμο,αριθμός ταυτότητας, τα οποία συνδυάζονται, κρυπτογραφούνται και αποθηκεύονται σε blockchain ως φράση κατακερματισμού ελέγχου ταυτότητας που συνδέεται με τη νέα διεύθυνση που δημιουργήθηκε.

Συνάρτηση “addUser“ που χρησιμοποιείται στην εγγραφή, μαζί με τις ιδιωτικές αντιστοιχίσεις που αποθηκεύονται οι φράσεις ελέγχου ταυτότητας. Η συνάρτηση για να εκτελεστεί απαιτεί να έχει σταλθεί το αίτημα από μια δεσμευμένη διεύθυνση, απαγορεύοντας τη χρήση από οποιοδήποτε πολίτη εκτός των αρχών (αυτό επιτυγχάνεται με την εντολή **require**).

```
address private owner =0x9CcD452bf6c33D1D7fe59cd8AA988e31Ad965Ca2;
mapping(address => string) private authentications;

function addUser(string memory authphrase, address _address) public{
  require(msg.sender == owner);
  userCount+= 1;
  authentications[_address]=authphrase;
}
```

Σχήμα 19. Συνάρτηση προσθήκης ψηφοφόρου

Την ημέρα των εκλογών, οι πολίτες θα πρέπει να μπουν στην πλατφόρμα ψηφοφορίας και να συνδέσουν το πορτοφόλι τους Metamask με την εφαρμογή. Για αυτή τη σύνδεση, ζητείται κωδικός πρόσβασης. Εκεί, θα πρέπει να εισάγουν τον κωδικό πρόσβασης που έλαβαν από τις αρχές στη φάση 2 και να συνδεθούν με τη διεύθυνση με την οποία έχουν χαρτογραφηθεί. Έπειτα, κάθε ψηφοφόρος θα πρέπει να λάβει έναν κωδικό πρόσβασης μίας χρήσης (OTP) για να ψηφίσει.

Για να λάβουν αυτό το κωδικό θα πρέπει να συνδεθούν χρησιμοποιώντας τα προσωπικά δεδομένα που υποβλήθηκαν κατά τη φάση 2, τα οποία συνδέονται με τη διεύθυνση που τους αναλογεί.

Συνάρτηση Solidity που ελέγχει εάν η αντιστοίχιση φράσης ελέγχου ταυτότητας και διεύθυνσης είναι σωστή.

```
function checkIfUserExists(string memory authphrase) public view returns(bool){

  if( keccak256(abi.encodePacked(authentications[msg.sender]))
  == keccak256(abi.encodePacked(authphrase)) )
    return true;
  else
    return false;
}
```

Σχήμα 20. Έλεγχος ταυτότητας ψηφοφόρου

Εάν η διεύθυνση που στέλνονται οι συναλλαγές συνδέεται με τη φράση ελέγχου ταυτότητας που έδωσε ο πολίτης κατά τη σύνδεση, δημιουργείται ένας κωδικός πρόσβασης μίας χρήσης (OTP), ο οποίος αντιστοιχίζεται με τη διεύθυνση αποστολέα και αποθηκεύεται στο blockchain, με τη μορφή μιας δομής που περιέχει λέξη-κλειδί μαζί με την ώρα που προστέθηκε αυτή η λέξη-κλειδί.

Δομή Solidity για την αποθήκευση των φράσεων / κλειδιών, μαζί με τις διευθύνσεις με τις οποίες αντιστοιχίζονται.

```
struct Keywrds{
  string key;
  uint256 keyTime;
}
mapping(address => Keywrds) private keyword;
```

Σχήμα 21. OTP διάρκειας 5 λεπτών αποθηκευμένα στο Blockchain

Αυτό το OTP δημιουργείται μόνο εάν αυτή η διεύθυνση δεν έχει υποβάλει ακόμη ψηφοφορία. Παρακάτω εικόνα μπορούμε να δούμε τις 2 συναρτήσεις που χρησιμοποιούνται για την είσοδο. Η "logUser", ελέγχει εάν η αντιστοίχιση φράσης / διεύθυνσης - ελέγχου ταυτότητας είναι σωστή.

```
function logUser(string memory authphrase, string memory keywrd) public returns(bool){
  require(! (voter[msg.sender].voted) );

  if( keccak256(abi.encodePacked(authentications[msg.sender]))
  == keccak256(abi.encodePacked(authphrase)) ){
      addKeyword(keywrd);
      return (true);
  }
  else
      return (false);
  }
```

Σχήμα 22. Έλεγχος ταυτοποίησης χρήστη

Εάν η αντιστοίχιση είναι επιτυχής, καλείται τη συνάρτηση “addKeyword“. Η συνάρτηση “add Keyword“, λαμβάνει τη λέξη-κλειδί και την αποθηκεύει μαζί με τη χρονική σήμανση του μπλοκ στο οποίο προστέθηκε.

```
function addKeyword(string memory keywrd) public {
  keyCount+=1;
  keyword[msg.sender] = Keywrds(keywrd, block.timestamp);
}
```

Σχήμα 23. Προσθήκη κωδικού

Μόλις προστεθεί ο κωδικός πρόσβασης στο blockchain, αποστέλλεται στον ψηφοφόρο. Αποστέλλεται μέσω SMS στο κινητό τηλέφωνο που συμπληρώνεται από τη φόρμα (με τον αριθμό τηλεφώνου να είναι σωστός, καθώς ο έλεγχος επαλήθευσης προσωπικών δεδομένων είναι επιτυχής).

Στο προτεινόμενο μοντέλο, ένα προσωπικό μήνυμα αποστέλλεται στο κινητό μέσω API, το οποίο λαμβάνεται από το front-end της εφαρμογής κάνοντας “fetch“ ένα ‘hhtp request“, με τα κλειδιά του API, να αποθηκεύονται ως “environment“ μεταβλητές. Σε αυτό το σημείο όπου ο ψηφοφόρος έχει ολοκληρώσει όλα τα στάδια ελέγχου ταυτότητας, πραγματοποιείται η διαδικασία της ψηφοφορίας. Έχοντας τον μοναδικό κωδικό που του επιτρέπει να ψηφίσει, κάθε ψηφοφόρος επιλέγει τον υποψήφιο που θέλει, συμπληρώνει τον κωδικό και πατά το κουμπί για να καταχωρήσει ψήφο.

Η συνάρτηση που ελέγχει εάν το OTP είναι έγκυρο, λειτουργεί ως εξής. Αρχικά γίνεται ένας έλεγχος αντιστοίχισης του κωδικού με τη διεύθυνση του αποστολέα. Στη συνέχεια, με την εντολή “block. timestamp“ λαμβάνουμε την τωρινή χρονοσφραγίδα στην οποία αφαιρούμε τη χρονοσφραγίδα προσθήκης του κωδικού. Έπειτα αν η αντιστοίχιση κωδικού-διεύθυνσης και ο έλεγχος χρόνου είναι επιτυχής επιστρέφει η τιμή “true“. Διαφορετικά επιστρέφεται “false“.

```
function checkIfKeywordIsCorrect(string memory keywrd) public view returns(bool){
  uint256 timeDiff = block.timestamp - keyword[msg.sender].keyTime;

  if ( keccak256(abi.encodePacked(keyword[msg.sender].key ))
  == keccak256(abi.encodePacked(keywrd)))
    if( timeDiff < 5 minutes )
      return true;
    else
      return false;
  else
    return false;
}
```

Σχήμα 24. Έλεγχος ορθού OTP

Εάν ο έλεγχος της παραπάνω συνάρτησης είναι επιτυχής, καλείται η συνάρτηση “Vote“. Κάθε διεύθυνση που ψηφίζει αποθηκεύεται σε μια δομή, η οποία περιέχει τη διεύθυνση, τη λέξη-κλειδί, την ακριβή ώρα που έγινε η ψηφοφορία και μια δυαδική μεταβλητή που δηλώνει εάν αυτή η διεύθυνση έχει ψηφίσει.

```
struct Voted{
    address sender;
    string key;
    uint256 timestamp;
    bool voted;
}
mapping(address => Voted) private voter;
```

Σχήμα 25. Δομή ψηφοφορίας

Η συνάρτηση "Vote" λειτουργεί ως εξής. Πριν την αποθήκευση ψήφου, γίνεται ακόμη ένας έλεγχος, αν η διεύθυνση αποστολής έχει καταθέσει ήδη ψήφο στο blockchain. Στη συνέχεια, αυξάνει τις ψήφους του υποψηφίου που επέλεξε ο ψηφοφόρος κατά 1 και η διεύθυνση σηματοδοτείται ότι έχει καταθέσει ψήφο, δηλαδή η τιμή της μεταβλητής "boolean" ορίζεται σε true. Με αυτόν τον τρόπο, κάθε ψηφοφόρος μπορεί να επαληθεύσει την ψήφο του με την απόδειξη συναλλαγής κατά τη ψηφοφορία, χωρίς όμως να γίνεται αναφορά στο περιεχόμενο της ψήφου.

```
function Vote (string memory keywrd, string memory candidate) public returns (bool){
    require(! (voter[msg.sender].voted) );
    votersCount+=1;
    if( keccak256(abi.encodePacked(candidate)) == keccak256(abi.encodePacked('candidateA'))){
        candidateA+=1;
        voter[msg.sender]=Voted(msg.sender,keywrd,block.timestamp,true);
        return true;
    }else if( keccak256(abi.encodePacked(candidate)) == keccak256(abi.encodePacked('candidateB'))){
        candidateB+=1;
        voter[msg.sender]=Voted(msg.sender,keywrd,block.timestamp,true);
        return true;
    }else if( keccak256(abi.encodePacked(candidate)) == keccak256(abi.encodePacked('candidateC'))){
        candidateC+=1;
        voter[msg.sender]=Voted(msg.sender,keywrd,block.timestamp,true);
        return true;
    }else
    return false;
}
```

Σχήμα 26. Συνάρτηση ψηφοφορίας

Μετά τις εκλογές, τα αποτελέσματα λαμβάνονται από τις αρχές. Στην παρακάτω εικόνα βλέπουμε τις 3 συναρτήσεις για τη λήψη των ψήφων που έλαβε ο κάθε υποψήφιος. Μόνο οι διευθύνσεις των αρχών έχουν το δικαίωμα να καλούν αυτές τις λειτουργίες, δηλαδή εκείνες που αρχικοποιηθήκαν ως ασφαλείς.

```
function getCandidateAVotes() public view returns (uint256){
  require(msg.sender == owner);
  return(candidateA);
}
  function getCandidateBVotes() public view returns (uint256){
  require(msg.sender == owner);
  return(candidateB);
}
  function getCandidateCVotes() public view returns (uint256){
  require(msg.sender == owner);
  return(candidateC);
}
```

Σχήμα 27. Λήψη αποτελεσμάτων από τις αρχές

Τέλος υπάρχει και μία ακόμη συνάρτηση η οποία πραγματοποιεί τον έλεγχο, εάν μια διεύθυνση έχει ήδη ψηφίσει. Αυτή η συνάρτηση ελέγχει τη τιμή boolean. Εάν είναι **true** επιστρέφει ότι η διεύθυνση έχει ήδη ψηφίσει διαφορετικά επιστρέφει το αντίθετο.

```
function checkIfVoted() public view returns(bool){

  if(voter[msg.sender].voted == true)
  return true;
  else
  return false;
}
```

Σχήμα 28. Έλεγχος αποφυγής διπλής ψηφοφορίας

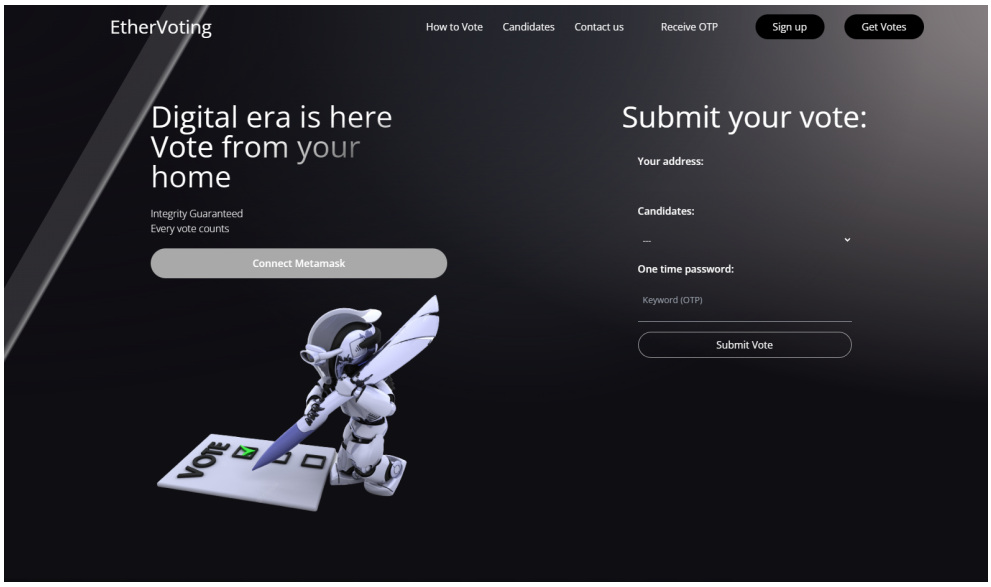
5.3 Διεπαφή χρήστη

Σε αυτό το υποκεφάλαιο θα γίνει μέσω στιγμιοτύπων οθόνης αναλυτική μελέτη στις ενέργειες που είναι απαραίτητες για όλη την εκλογική διαδικασία, στα τρία τελευταία στάδια της.

5.3.1 Αρχική οθόνη πλατφόρμας

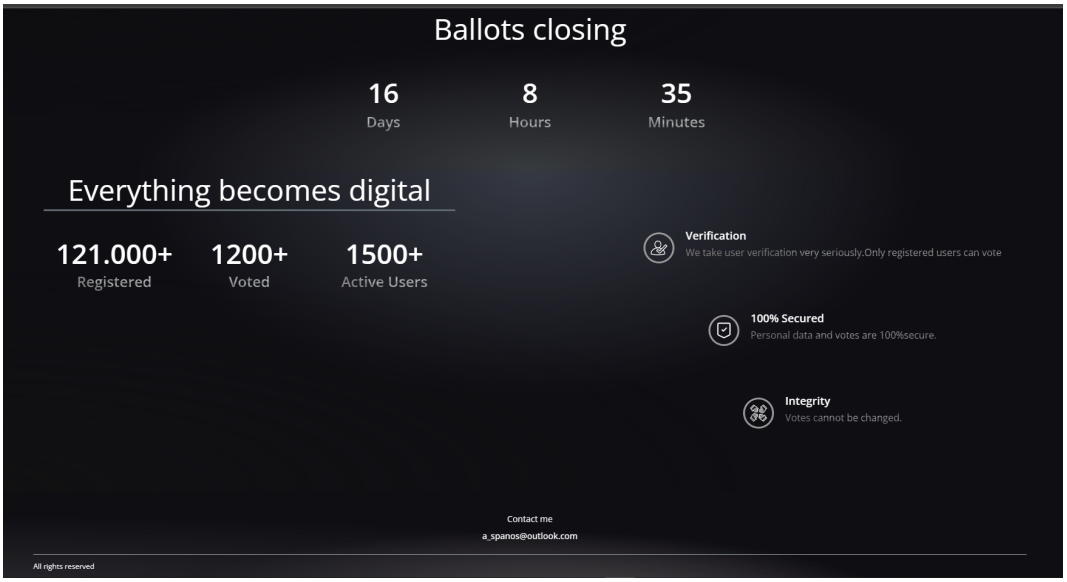
Η πλατφόρμα που υλοποιήθηκε ονομάζεται “Ether Voting“ και θα διαφέρει η έκδοση που θα λάβουν οι αρχές με εκείνη που θα κυκλοφορήσει για τους πολίτες.

Στην πρώτη εικόνα μπορούμε να δούμε αρχικά ένα μενού επιλογών, που εκτός από βασικές λειτουργίες όπως τρόπος ψηφοφορίας, στοιχεία υποψηφίων και στοιχεία εξυπηρέτησης πολιτών, παρέχει και τρία κουμπιά. Τα δύο είναι μόνο διαθέσιμα για την έκδοση της πλατφόρμας που θα λάβουν οι αρχές και αφορούν την εγγραφή των ψηφοφόρων και τη λήψη των τελικών αποτελεσμάτων. Το τρίτο κουμπί είναι ορατό και στους ψηφοφόρους και αφορά τη λήψη μοναδικού κωδικού. Στη συνέχεια μπορούμε να δούμε όλη τη διεπαφή η οποία αφορά την ψηφοφορία και θα αναλυθεί λεπτομερώς στη συνέχεια αυτού του κεφαλαίου.



Σχήμα 29. Αρχική οθόνη πλατφόρμας - Μέρος 1

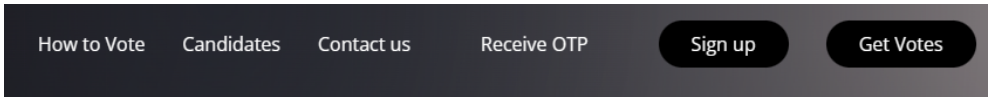
Το δεύτερο μέρος της πλατφόρμας που αφορά την εξυπηρέτηση πολιτών, και επιπλέον υπηρεσίες που παρέχονται, όπως η αντίστροφη μέτρηση μέχρι την έναρξη και λήξη των εκλογών, επικοινωνία, αλλά και υπηρεσίες που παρέχονται, όπως ασφάλεια και ακεραιότητα.



Σχήμα 30. Αρχική οθόνη πλατφόρμας - Μέρος 2

Μενού υπηρεσιών

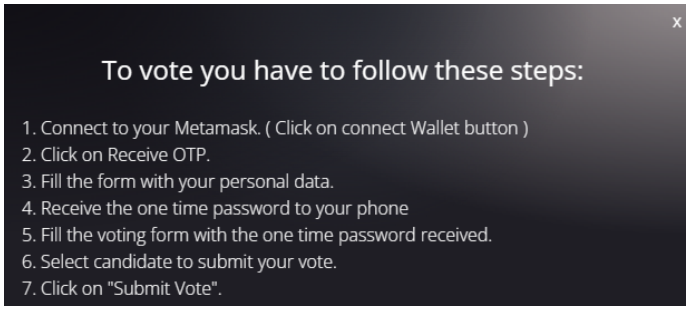
Η πλατφόρμα στο αρχικό μέρος της, περιέχει ένα μενού λειτουργιών, που προσφέρει μερικές δυνατότητες στους ψηφοφόρους.



Σχήμα 31. Μενού υπηρεσιών

Αυτό το μενού περιλαμβάνει 6 κουμπιά, εκ των οποίων μόνο τα 4 είναι ορατά στους πολίτες. Πιο συγκεκριμένα:

- **“How to Vote“** : εμφανίζει ένα παράθυρο με σαφείς οδηγίες για το σύνολο και τη σειρά ενεργειών που πρέπει να ακολουθήσει κάθε πολίτης για να καταβάλει επιτυχώς τη ψήφο του.

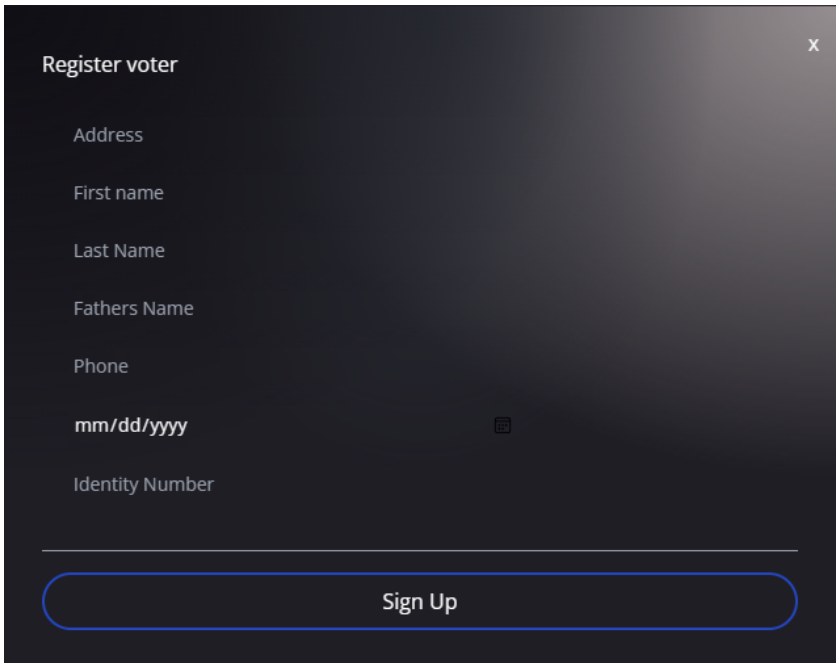


Σχήμα 32. Τρόπος ψηφοφορίας

- **“Candidates“** : εμφανίζεται η λίστα με τους υποψηφίους.
- **“Contact Us“** : εμφανίζεται ένα παράθυρο με τηλέφωνα των αρχών που θα παρέχουν πρώτου επιπέδου τεχνική υποστήριξη.
- **“Receive OTP“** : εμφανίζεται ένα παράθυρο, όπου κάθε ψηφοφόρος θα πρέπει να εισάγει όλα τα προσωπικά δεδομένα που έχουν συνδεθεί με τον λογαριασμό του στο Metamask. Μέσω αυτού του κουμπιού και αυτής της ταυτοποίησης θα μπορέσει να λάβει το μοναδικό κωδικό που θα του επιτρέψει να ψηφίσει.
- **“Sign up“** : εμφανίζεται μόνο στις αρχές. Εμφανίζεται ένα παράθυρο, το οποίο περιλαμβάνει μια φόρμα σύμφωνα με την οποία θα γίνεται η εγγραφή των ψηφοφόρων.
- **“Get Votes“** : εμφανίζεται μόνο στις αρχές. Εμφανίζεται ένα παράθυρο, το οποίο περιλαμβάνει μια φόρμα σύμφωνα με την οποία θα γίνεται η εγγραφή των ψηφοφόρων.

5.3.2 Εγγραφή ψηφοφόρων

Στο στάδιο προσθήκης των πολιτών στη λίστα με τους ψηφοφόρους θα πρέπει να παρευρεθούν στις αρχές. Οι αρχές αφού τους δημιουργήσουν ένα λογαριασμό Metamask, με τον κατάλληλο αριθμό Ethers που θα χρειαστούν για τη ψηφοφορία, δίνουν το κωδικό στον ψηφοφόρο, ώστε να μπορέσει να συνδεθεί με αυτό το λογαριασμό, με τον οποίο έχει πλέον αντιστοιχηθεί, την ημέρα των εκλογών. Στη συνέχεια, ακολουθεί η διαδικασία προσθήκης των προσωπικών δεδομένων, σε συνδυασμό με τη διεύθυνση που μόλις δημιουργήθηκε στο blockchain. Αυτή η λειτουργία γίνεται με τη χρήση του “Sign up“ που αναφέρθηκε προηγουμένως. Αξίζει να υπενθυμίσουμε πως αυτή η λειτουργία εμφανίζεται μόνο στις αρχές, και για να ολοκληρωθεί σωστά θα πρέπει να έχουν συνδεθεί με ένα λογαριασμό Metamask, ο οποίος θεωρείται αξιόπιστος, προκειμένου να ικανοποιηθεί η συνθήκη “**require(msg.sender == owner)**“, της συνάρτησης του έξυπνου συμβολαίου. Στην παρακάτω εικόνα βλέπουμε τη διεπαφή χρήστη για την εγγραφή.



Σχήμα 33. Εγγραφή ψηφοφόρων στην πλατφόρμα

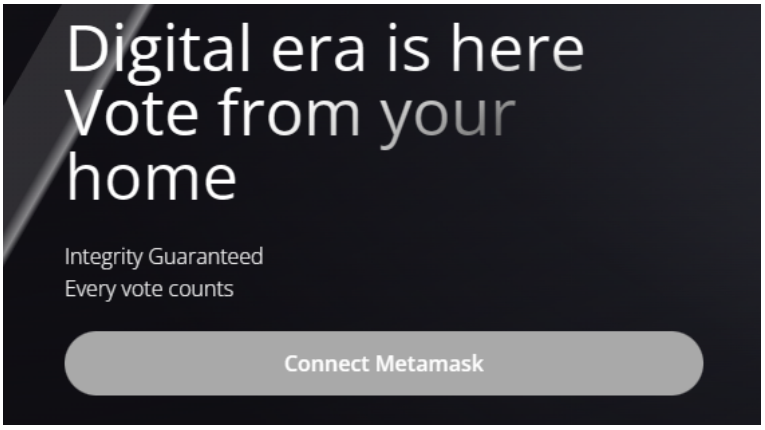
Σε αυτή τη φόρμα θα πρέπει να συμπληρωθούν τα παρακάτω πεδία:

- **Διεύθυνση**:η διεύθυνση Metamask του ψηφοφόρου που μόλις δημιουργήθηκε.
- **Όνομα**:Το όνομα του ψηφοφόρου.
- **Επώνυμο**: Το επώνυμο του ψηφοφόρου.
- **Όνομα πατρός**: Το όνομα πατρός του ψηφοφόρου.
- **Τηλέφωνο**: Το κινητό τηλέφωνο στο οποίο θα λάβουν και τον μοναδικό κωδικό (one time password) την ημέρα της ψηφοφορίας.
- **Ημερομηνία γέννησης**: Η ημερομηνία γέννησης του ψηφοφόρου.
- **Αριθμός ταυτότητας**: Ο αριθμός αστυνομικής ταυτότητας του ψηφοφόρου.

Αυτά τα δεδομένα κρυπτογραφούνται με τον κρυπτογραφικό αλγόριθμο SHA256, και χρησιμοποιώντας τη δομή ενός Merkle Tree (*Έγινε εξήγηση του Merkle tree στο κεφάλαιο 1*), δημιουργώντας ένα τελικό hash, με το οποίο θα αντιστοιχηθεί η διεύθυνση που συμπληρώθηκε, και θα αποθηκευτούν στο blockchain.

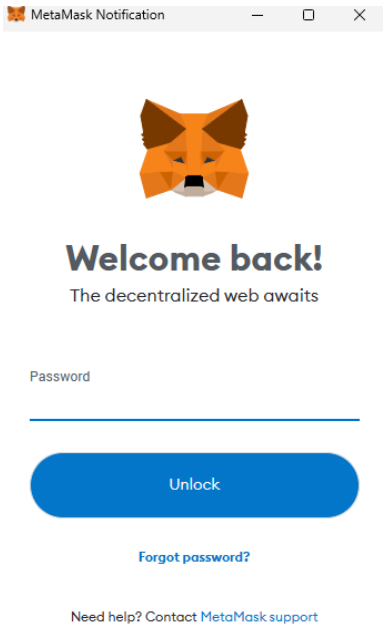
5.3.3 Ταυτοποίηση

Έχοντας ολοκληρωθεί το δεύτερο στάδιο, ακολουθεί το τρίτο στάδιο της ταυτοποίησης. Κάθε πολίτης θα πρέπει να συνδεθεί στο Metamask, πατώντας το κουμπί **“Connect Wallet“** που βλέπουμε παρακάτω.



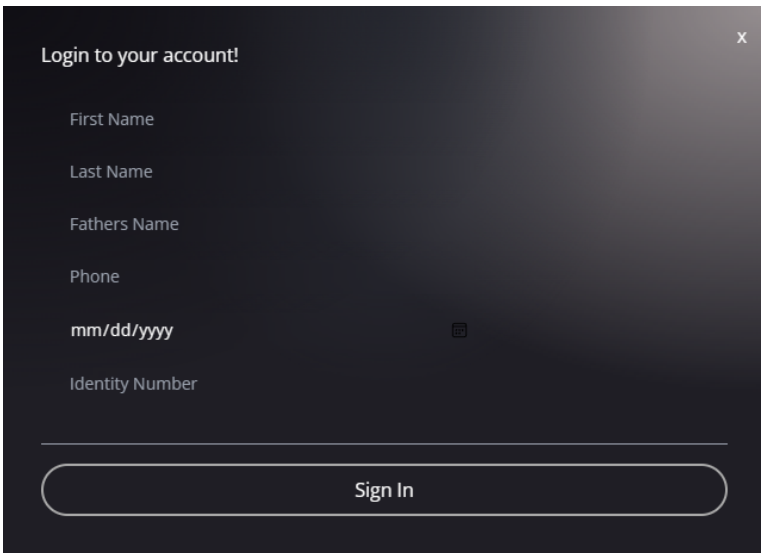
Σχήμα 34. Σύνδεση με το Metamask

Με το πάτημα του κουμπιού, γίνεται trigger και εμφανίζεται το pop up του Metamask, στο οποίο καλείται να συμπληρώσει το σωστό κωδικό για τον λογαριασμό που του αντιστοιχεί, δηλαδή εκείνον που έλαβε στο “ στάδιο 2“ από τις αρχές. Αν ο κωδικός είναι σωστός γίνεται επαναφόρτωση της σελίδας, με τη διεύθυνση να αναγράφεται στο πεδίο “**Your address:**“ στη φόρμα ψηφοφορίας, διαφορετικά εμφανίζεται το μήνυμα λάθους του Metamask.



Σχήμα 35. Metamask pop up

Στη συνέχεια θα πρέπει να πατήσει το κουμπί "**Get OTP**" για τη λήψη του μοναδικού κωδικού (one time password) που θα χρειαστεί για την αποθήκευση της ψήφου. Θα εμφανιστεί το pop up που βλέπουμε στην παρακάτω εικόνα.

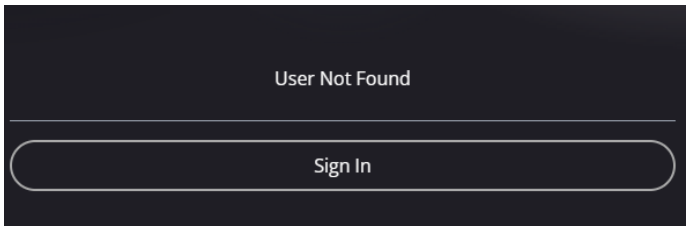


Σχήμα 36. Pop up λήψης μοναδικού κωδικού

Η φόρμα είναι αντίστοιχη με εκείνη της εγγραφής. Με αυτό το τρόπο ο κάθε πολίτης δε θα πρέπει να έχει πολλούς κωδικούς. Το μόνο που χρειάζεται είναι να τη συμπληρώσει με τα προσωπικά του δεδομένα. Τα δεδομένα αυτά κρυπτογραφούνται με παρόμοιο τρόπο όπως στην εγγραφή. Αν η φόρμα είναι συμπληρωμένη, και η τιμή κατακερματισμού που θα δημιουργηθεί αντιστοιχεί στη διεύθυνση Metamask με την οποία έχει συνδεθεί, η είσοδος του γίνεται επιτυχώς.

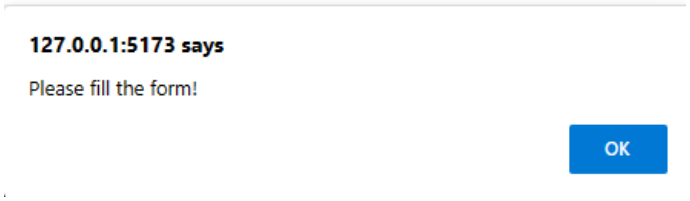
Παρακάτω βλέπουμε τα δύο μηνύματα λάθους:

1. Περίπτωση εσφαλμένων στοιχείων.



Σχήμα 37. Σφάλμα εσφαλμένων στοιχείων

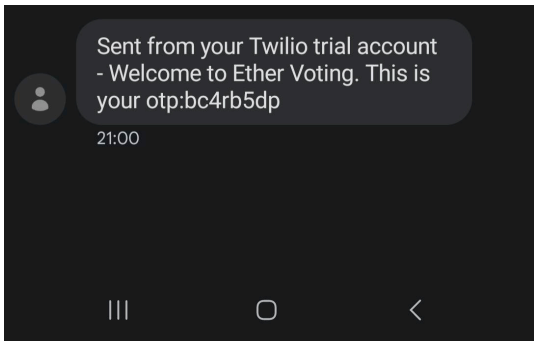
2. Ελλιπής συμπλήρωση της φόρμας.



Σχήμα 38. Σφάλμα συμπλήρωσης φόρμας

Στη συνέχεια ακολουθεί έλεγχος ψήφου αυτής της διεύθυνσης. Αν δεν έχει αποθηκευτεί ψήφος από εκείνη δημιουργείται ένας μοναδικός κωδικός ο οποίος στέλνεται μέσω SMS στο κινητό που έχει συμπληρωθεί στη φόρμα (δεδομένου ότι το hash είναι ίδιο, άρα και το κινητό τηλέφωνο θα είναι σωστό, οπότε δεν απαιτείται επιπλέον έλεγχος). Στην υλοποίηση μας, ο κωδικός στέλνεται κάνοντας “fetch“ ένα “post request“ με τη χρήση του **“Twilio API“**.

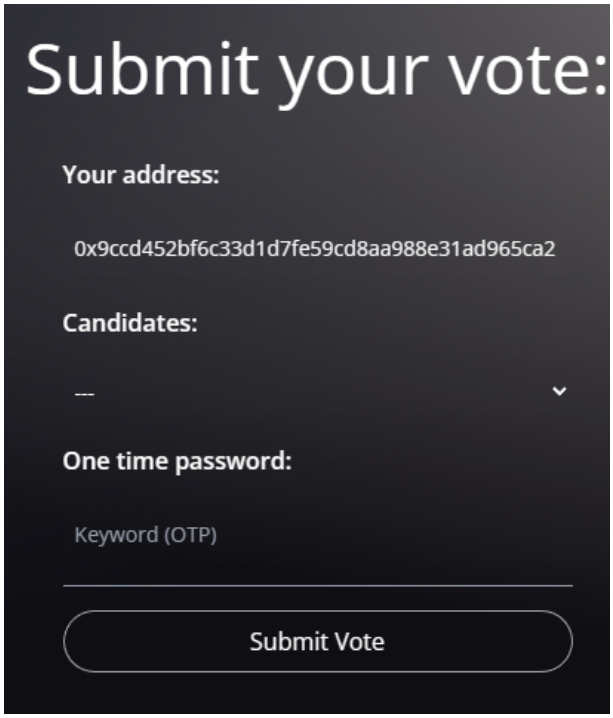
Στην παρακάτω εικόνα μπορούμε να δούμε έναν κωδικό που έχει σταλθεί στο κινητό για τη ψηφοφορία.



Σχήμα 39. Λήψη μοναδικού κωδικού μέσω SMS

5.3.4 Ψηφοφορία

Τέλος, ο κάθε ψηφοφόρος καλείται να ψηφίσει με αυτό το μοναδικό κωδικό εντός 5 λεπτών συμπληρώνοντας την παρακάτω φόρμα. Όπως θα δούμε αναγράφεται η διεύθυνση Metamask, με την οποία έχει γίνει σύνδεση, και υπάρχουν δύο πεδία, για τη συμπλήρωση του υποψηφίου και του κωδικού που θα επιτρέψει την ψηφοφορία.

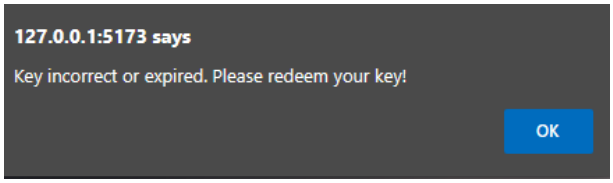


Σχήμα 40. Φόρμα ψηφοφορίας

Η επιλογή των υποψηφίων γίνεται μέσω ενός dropdown list.

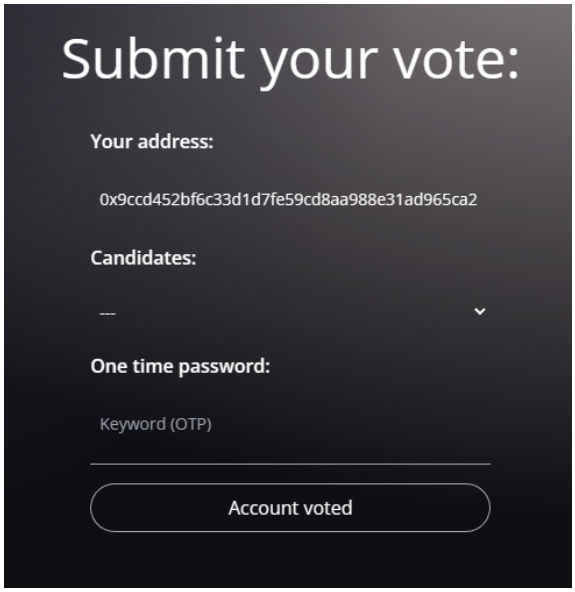
Σχήμα 41. Φόρμα ψηφοφορίας

Στην περίπτωση που εισάγει εσφαλμένο κωδικό ή το χρονικό περιθώριο έχει λήξει, εμφανίζεται αντίστοιχό μήνυμα λάθους.



Σχήμα 42. Σφάλμα κωδικού

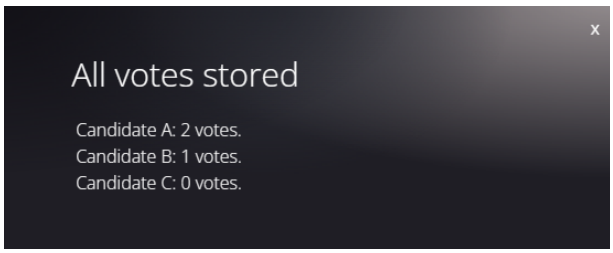
Όταν μια ψήφος αποθηκευτεί επιτυχώς, ο λογαριασμός κλειδώνεται, ώστε να μη παρέχεται η δυνατότητα εκ νέου ψηφοφορίας. Όπως θα δούμε στο παρακάτω στιγμιότυπο, απαγορεύεται η εκ νέου ψηφοφορία, και στο επίπεδο της διεπαφής, με το κουμπί "Submit Vote" να έχει τροποποιηθεί και κλειδωθεί.



Σχήμα 43. Κλειδωμένο κουμπί ψηφοφορίας

Στη περίπτωση που μια διεύθυνση, με την οποία συνδεθεί ο χρήστης, έχει ήδη ψηφίσει δε θα παραχθεί ο μοναδικός κωδικός και η επιλογή ψήφου θα είναι κλειδωμένη.

Τέλος, προκειμένου το σύστημα μας να είναι ολοκληρωμένο, δίνεται η δυνατότητα για τη λήψη αποτελεσμάτων, αρκεί οι αρχές να συνδεθούν με μια "ασφαλή" διεύθυνση Metamask, και να πατήσουν το κουμπί "**Get Votes**.



Σχήμα 44. Λήψη αποτελεσμάτων

Τον ολοκληρωμένο κώδικα, μπορείτε να τον βρείτε στο Github repo.

Κεφάλαιο 6

Αξιολόγηση προτεινόμενου συστήματος

Έχοντας πλέον υλοποιήσει το σύστημα μας, θα εξετάσουμε εξαντλητικές περιπτώσεις χρήσης για τις λειτουργίες του συστήματος ψηφοφορίας που αναπτύχθηκε με βάση την τεχνολογία blockchain. Θα εξετάσουμε τα προβλήματα που μπορεί να παρουσιαστούν, όσον αφορά τη τήρηση των αρχών για μια ψηφοφορία όπως η ακεραιότητα των ψηφοφοριών και της εγκυρότητας του αποτελέσματος. Θα αναλύσουμε επίσης τις δυνητικές αδυναμίες του συστήματος και θα προτείνουμε βελτιώσεις που μπορούν να γίνουν για την απόδοση και την ασφάλεια του συστήματος. Τέλος, θα εξετάσουμε εναλλακτικές μορφές ψηφοφορίας, στις οποίες θα μπορούσε ευκολότερα να υιοθετηθεί η τεχνολογία blockchain, αλλά και πιο συγκεκριμένα το σύστημα μας.

6.1 Περιπτώσεις ελέγχου

Δημιουργήθηκαν δοκιμαστικές περιπτώσεις ελέγχου για να εξασφαλιστεί η κατάλληλη λειτουργία του συστήματος ψηφοφορίας βασισμένου στο Ethereum Blockchain. Το πρώτο μέρος σχετίζεται αποκλειστικά με τις 2 φάσεις που λαμβάνουν χώρα πριν από την ημέρα των εκλογών και αφορούν τη δημιουργία του smart contract, τις διευθύνσεις Metamask των αρχών και τη διαδικασία εγγραφής κάθε ψηφοφόρου στην έγκυρη λίστα. Στον πίνακα Ι παρουσιάζεται μια λίστα με λειτουργικές δοκιμαστικές περιπτώσεις που σχετίζονται με αυτές τις 2 φάσεις και αφορούν κυρίως την εφαρμογή εγγραφής. Θεωρούμε ότι η ανάπτυξη του smart contract έγινε με τη βοήθεια του hardhat. Δεδομένου ότι η συμπλήρωση της φόρμας εγγραφής του ψηφοφόρου γίνεται από μέλη των αρχών, δεν υπήρξαν περιπτώσεις μη ολοκλήρωσης της φόρμας.

Δοκιμές ελέγχου προεκλογικών φάσεων			
ID	Περιγραφή δοκιμής ελέγχου	Επιθυμητό αποτέλεσμα	Αποτέλεσμα
1	Δημιουργία ασφαλούς / εξουσιοδοτημένου λογαριασμού Metamask	Δημιουργία και αποθήκευση εξουσιοδοτημένης διεύθυνσης	Επιτυχία
2	Ανάπτυξη έξυπνου συμβολαίου	Λήψη ABI του έξυπνου συμβολαίου	Επιτυχία
3	Σύνδεση της εξουσιοδοτημένης διεύθυνσης Metamask με την εφαρμογή	Σύνδεση λογαριασμού Metamask με το δίκτυο Ethereum	Επιτυχία
4	Δημιουργία διευθύνσεων Metamask ψηφοφόρων	Δημιουργία διεύθυνσης και λήψη κωδικού πρόσβασης	Επιτυχία

5	Κρυπτογράφηση προσωπικών δεδομένων ψηφοφόρων με τον αλγόριθμο SHA256 σε δομή Merkle tree	Δημιουργία κωδικού/τιμής κατακερματισμού προσωπικών δεδομένων	Επιτυχία
6	Καταχώρηση ψηφοφόρου χρησιμοποιώντας την εξουσιοδοτημένη διεύθυνση Metamask	Συσχέτιση τιμής κατακερματισμένου με τη διεύθυνση	Επιτυχία
7	Καταχώρηση ψηφοφόρου χρησιμοποιώντας μη εξουσιοδοτημένη διεύθυνση Metamask	Τα προσωπικά δεδομένα κρυπτογραφούνται αλλά δεν αποθηκεύονται / Σφάλμα	Επιτυχία

Πίνακας 3. Δοκιμές ελέγχου φάσεων 1-2

Στους παρακάτω πίνακες θα δούμε λίστες με λειτουργικές δοκιμές για τις επόμενες 2 φάσεις που λαμβάνουν χώρα την ημέρα των εκλογών. Στον ακόλουθο πίνακα θα δούμε τις λειτουργικές δοκιμές της τρίτης φάσης, που αφορούν την αυθεντικοποίηση των ψηφοφόρων.

Δοκιμές ελέγχου συναρτήσεων ταυτοποίησης			
ID	Περιγραφή δοκιμής ελέγχου	Επιθυμητό αποτέλεσμα	Αποτέλεσμα
1	”Connect Wallet” για τη σύνδεση στο Metamask	Εμφάνιση pop up του Metamask	Επιτυχία
2	Σύνδεση της πλατφόρμας με το Metamask. Συμπλήρωση ορθού κωδικού στο Metamask	Εμφάνιση διεύθυνσης στη φόρμα ψηφοφορίας	Επιτυχία
3	Σύνδεση της πλατφόρμας με το Metamask. Συμπλήρωση εσφαλμένου κωδικού στο Metamask	Εμφάνιση μηνύματος λάθους Metamask	Επιτυχία
4	”Receive OTP” με την πλατφόρμα συνδεδεμένη με το Metamask. Η φόρμα συμπληρώνεται με σωστά προσωπικά δεδομένα που αντιστοιχούν στη συνδεδεμένη διεύθυνση	Δημιουργία τιμής κατακερματισμού από την κρυπτογράφηση προσωπικών δεδομένων. Επιτυχής σύνδεση. Κλήση για δημιουργία και αποστολή OTP.	Επιτυχία
5	”Receive OTP” ενώ η πλατφόρμα είναι συνδεδεμένη με το Metamask. Η φόρμα συμπληρώνεται με **λανθασμένα** προσωπικά δεδομένα	Εμφάνιση μηνύματος λάθους: “User not found“	Επιτυχία
6	”Receive OTP” με σωστά προσωπικά δεδομένα, αλλά λανθασμένη διεύθυνση Metamask	Εμφάνιση μηνύματος λάθους: “User not found“	Επιτυχία
7	Πάτημα στο ”Receive OTP” ενώ η πλατφόρμα **δεν** είναι συνδεδεμένη με το Metamask	Error	Επιτυχία
8	Αποστολή και αποθήκευση κωδικού, έπειτα από επιτυχή ταυτοποίηση	Δημιουργία κωδικού, αποθήκευση του στο blockchain και αποστολή στο κινητό μέσω SMS	Επιτυχία

Πίνακας 4. Δοκιμές ελέγχου φάσης 3

Τέλος, στο παρακάτω πίνακα θα δούμε όλες τις λειτουργικές δοκιμές ελέγχου που αφορούν

τη διαδικασία της ψηφοφορίας. Αυτές οι περιπτώσεις δοκιμής περιλαμβάνουν κάθε πιθανή ενέργεια ψηφοφόρου. Επιπλέον, ο παρακάτω πίνακας περιλαμβάνει και δοκιμές ελέγχου που αφορούν τη λήψη των συνολικών αποτελεσμάτων, ενέργειες που θα γίνουν με το πέρας των εκλογών. Η ύπαρξη κατάλληλων λειτουργικών δοκιμών είναι απαραίτητη για τόσο σημαντικές εφαρμογές, καθώς βοηθούν στην αντίληψη του επιπέδου ασφάλειας και ιδιωτικότητας, αλλά και γενικότερα διατήρησης των αρχών των εκλογών.

Δοκιμές ελέγχου συναρτήσεων ταυτοποίησης			
ID	Περιγραφή δοκιμής ελέγχου	Επιθυμητό αποτέλεσμα	Αποτέλεσμα
1	Προσπάθεια ψήφου με διεύθυνση που δεν έχει ψηφίσει Συμπλήρωση της φόρμας με σωστό OTP, εντός 5 λεπτών	Η ψήφος αποθηκεύεται Αποκλεισμός διεύθυνσης για εκ νέου ψηφοφορία	Επιτυχία
2	Προσπάθεια ψήφου με διεύθυνση που δεν έχει ψηφίσει Συμπλήρωση της φόρμας με σωστό OTP, εντός 5 λεπτών, αλλά με **λανθασμένη** διεύθυνση	Σφάλμα ψηφοφορίας / κωδικού	Επιτυχία
3	Προσπάθεια ψήφου με διεύθυνση που δεν έχει ψηφίσει Συμπλήρωση της φόρμας με σωστό OTP, αλλά μετά το πέρας 5 λεπτών	Σφάλμα στο OTP	Επιτυχία
4	Προσπάθεια ψήφου με διεύθυνση που δεν έχει ψηφίσει Συμπλήρωση της φόρμας με λανθασμένο OTP	Σφάλμα στο OTP	Επιτυχία
5	Προσπάθεια ψήφου με διεύθυνση που έχει ψηφίσει ξανά	Απόρριψη ενέργειας από την πλατφόρμα	Επιτυχία
6	Προσπάθεια ψήφου ενώ η πλατφόρμα δεν έχει συνδεθεί με το Metamask	Σφάλμα ψηφοφορίας	Επιτυχία
7	Λήψη αποτελεσμάτων από διεύθυνση που έχει οριστεί ως ασφαλής	Λήψη συνολικών ψήφων κάθε ψηφοφόρου	Επιτυχία
8	Λήψη αποτελεσμάτων από μη εξουσιοδοτημένη διεύθυνση	Απόρριψη	Επιτυχία

Πίνακας 5. Δοκιμές ελέγχου φάσης 4

Έχοντας ελέγξει τη λειτουργικότητα των συναρτήσεων της πλατφόρμας, οφείλουμε να κάνουμε μια μελέτη, ώστε να απαντήσουμε σε μερικά ερωτήματα:

1. Ικανοποιεί το σύστημα όλες τις αρχές ψηφοφορίας;

2. Ποιες άλλες γενικές αδυναμίες παρουσιάζει το σύστημα;

3. Τι αλλαγές ή προσθήκες θα μπορούσαν να γίνουν ώστε να είναι ένα βήμα πιο κοντά σε μια ικανοποιητική πλατφόρμα, έτοιμη για χρήση;

4. Εκτός του επιπέδου εθνικών εκλογών, σε ποιες άλλες συνθήκες / μορφές εκλογών θα ήταν ιδανικότερο ένα τέτοιο σύστημα ψηφοφορίας;

6.2 Προβλήματα και λύσεις στις αρχές ψηφοφορίας

Η ψηφοφορία αποτελεί θεμελιώδη αρχή των δημοκρατικών κοινωνιών, καθώς παρέχει στους πολίτες τη δυνατότητα να εκφράσουν την πολιτική τους προτίμηση και να συμμετέχουν στη λήψη αποφάσεων. Ωστόσο, η αξιοπιστία του συστήματος ψηφοφορίας είναι απαραίτητη για τη διασφάλιση της δημοκρατικής διαδικασίας και της εμπιστοσύνης του κοινού στην πολιτική διακυβέρνηση. Σε αυτό το κεφάλαιο θα εξετάσουμε κατά πόσο μια εφαρμογή ψηφοφορίας μέσω blockchain πληροί τις αρχές της δημοκρατικής ψηφοφορίας, όπως η αναγνώριση της ανθρώπινης αξιοπρέπειας, η αρχή ”ένας άνθρωπος - μία ψήφος” και η διαφάνεια της διαδικασίας.

6.2.1 Αρχή “Ένας άνθρωπος - Μία ψήφος “

Η τήρηση της αρχής “Ένας άνθρωπος - Μία ψήφος“, μπορεί να ακούγεται φαινομενικά εύκολη, αλλά παρουσιάζει αρκετές δυσκολίες στην ηλεκτρονική ψηφοφορία. Αυτές οι δυσκολίες αφορούν το ζήτημα, ότι παρά τις μεθόδους αυθεντικοποίησης που παρέχονται από κάθε σύστημα, είναι αδύνατο να γνωρίζουμε αν κάποιος πολίτης ψήφισε ή χειραγώγησε κάποιον άλλον, ώστε να αλλάξει ή να αλλοιώσει τη ψήφο του.

Το σύστημα που υλοποιήθηκε σε αυτή τη διπλωματική, ανταποκρίνεται σε ικανοποιητικό βαθμό για την τήρηση αυτής της αρχής. Αντιστοιχίζοντας τους πολίτες με διευθύνσεις Metamask, καθώς και με το κλείδωμα αυτής της διεύθυνσης μόλις καταβληθεί ψήφος, αποφεύγεται η υποβολή δεύτερης ψήφου από κάθε πολίτη. Αυτή η αντιστοίχιση σε συνδυασμό με την ύπαρξη κωδικού μιας χρήσης, ο οποίος παράγεται με την εισαγωγή προσωπικών δεδομένων που μόνο ο κάθε πολίτης γνωρίζει, καθιστά αδύνατη τη “κλοπή“ μιας ψήφου. Επιπρόσθετα λόγω της αποστολής αυτού του κωδικού μέσω SMS, στο κινητό τηλέφωνο που έχει δηλωθεί την ημέρα της εγγραφής, απαιτεί τη φυσική παρουσία του πολίτη ή τη διαρκή επικοινωνία του, με εκείνον που τον χρηματοδότησε για την αγορά της ψήφου. Λόγω όλων αυτών των παραμέτρων ασφαλείας η αλλοίωση ή παρακίνηση μιας ψήφου μπορεί να γίνει μόνο με δύο τρόπους.

- Η πρώτη περίπτωση, μπορεί να λάβει χώρα μόνο εάν ένας πολίτης πουλήσει το κωδικό Metamask που έλαβε κατά την εγγραφή, σε συνδυασμό με όλα του τα προσωπικά δεδομένα (αριθμό ταυτότητας, κινητό κοκ.), ενέργεια η οποία θα μπορούσε πολύ δύσκολα να γίνει αποδεκτή από κάθε πολίτη. Επίσης, την ημέρα της ψηφοφορίας, ο πολίτης και ο “επιτιθέμενος“, θα πρέπει να βρίσκονται σε συνεχή επικοινωνία, για την έγκαιρη αποστολή του μοναδικού κωδικού που θα επιτρέψει την ψήφο.

- Η δεύτερη περίπτωση, αφορά τη φυσική ύπαρξη ενός προσώπου δίπλα στον πολίτη που καλείται να ψηφίσει. Αυτό το φυσικό πρόσωπο μπορεί να χειραγωγήσει τον ψηφοφόρο, καθώς δεν παρέχεται η δυνατότητα παρακολούθησης του ψηφοφόρου, ώστε να είναι βέβαιο ότι είναι μόνος του κατά τη διάρκεια της ψηφοφορίας.

Με αυτές τις δύο περιπτώσεις να είναι οι μόνες πιθανές περιπτώσεις να καταθέσει κανείς δύο ψήφους, μιας και η δυνατότητα αποστολής παραπάνω από μια ψήφους από την ίδια διεύθυνση έχει αποκλειστεί από κάθε πτυχή του συστήματος (δηλαδή και από τη διεπαφή αλλά και από το έξυπνο συμβόλαιο), θα μπορούσαμε να πούμε με σιγουριά πως το σύστημα μας ικανοποιεί αυτή την αρχή σε βαθμό πολύ πιο ικανοποιητικό από ότι στο παραδοσιακό τρόπο εκλογών ή από ότι οποιαδήποτε άλλη εφαρμογή ηλεκτρονικής ψηφοφορίας.

6.2.2 Αρχή μυστικότητας

Η έννοια της αρχής της μυστικότητας της ψηφοφορίας αναφέρεται στο γεγονός ότι κάθε ψηφοφόρος έχει το δικαίωμα να ψηφίσει με ελευθερία και ανωνυμία και ότι η ψήφος του δεν πρέπει να αποκαλυφθεί σε κανέναν.

Αυτό σημαίνει ότι κανένας δεν μπορεί να μάθει ποιος ψήφισε ποιον ή ποια είναι η ψήφος κάποιου συγκεκριμένου ψηφοφόρου. Η αρχή αυτή είναι σημαντική για τη διασφάλιση της ελεύθερης και δίκαιης διεξαγωγής των εκλογών ή άλλων διαδικασιών ψηφοφορίας και για τη διατήρηση της εμπιστοσύνης του κοινού στο σύστημα ψηφοφορίας.

Για την επίτευξη της μυστικότητας της ψηφοφορίας, χρησιμοποιούνται διάφορα μέσα, όπως η ανωνυμία του ψηφοφόρου και η ασφαλής διαχείριση και αποθήκευση των ψηφοδελτίων.

Το σύστημα μας, ικανοποιεί αυτή την αρχή των εκλογών, με την αντιστοίχιση των πολιτών με διευθύνσεις Metamask, και τον έλεγχο μέσω κρυπτογράφησης των προσωπικών δεδομένων. Η χρήση του κρυπτογραφικού αλγόριθμου SHA256, είναι ιδανική για τη περίπτωσή μας, λόγω του γεγονότος ότι είναι αδύνατη η αποκρυπτογράφιση αυτής της τιμής κατακερματισμού. Επομένως, όλα τα προσωπικά δεδομένα παραμένουν ασφαλή, επιτρέποντας παράλληλα να γίνεται η ταυτοποίηση όπως έχει οριστεί στο σύστημα, δηλαδή με έλεγχο ταιριάσματος των hashes που δημιουργούνται. Παράλληλα το σύστημα υιοθετεί μια ιδιαίτερη λειτουργία στην αποθήκευση ψήφων, αυξάνοντας τις ψήφους κάθε υποψήφιου, μόλις λάβει μια νέα ψήφο, χωρίς όμως να αποθηκεύεται η προέλευση αυτής της ψήφου. Επομένως, η εύρεση προέλευσης κάθε ψήφου, και σε συνδυασμό με την αποκρυπτογράφηση των hashes (εύρεση προσωπικών στοιχείων κάθε ψηφοφόρου), είναι αδύνατη, ικανοποιώντας την αρχή της μυστικότητας των εκλογών.

Παρά το γεγονός ότι δεν αποθηκεύεται η προέλευση κάθε ψήφου, με τους ελέγχους που γίνονται στο έξυπνο συμβόλαιο, για το εάν μια διεύθυνση έχει ψηφίσει, και σε συνδυασμό με τον μοναδικό κωδικό (OTP) που απαιτείται για τη ψηφοφορία, καθιστώντας αναγκαίο το στάδιο ταυτοποίησης, ικανοποιείται η αρχή της μυστικότητας σε συνδυασμό με την αρχή " Ένας άνθρωπος - Μία ψήφος". Η boolean τιμή που καθορίζει αν μια διεύθυνση έχει ψηφίσει, είναι ιδιωτική, επομένως μπορεί να τροποποιηθεί μόνο εντός του έξυπνου συμβολαίου, συνεπώς μόνο με την ικανοποίηση όλων των ελέγχων που απαιτούνται για την ψηφοφορία. Τέλος, ο κάθε ψηφοφόρος μπορεί να λάβει την απόδειξη συναλλαγής με το blockchain, ώστε παρά την ανωνυμία, να μπορεί να ελέγξει την ορθή αποθήκευση της ψήφου.

6.2.3 Αρχή εγκυρότητας

Η αρχή της εγκυρότητας στην ψηφοφορία αναφέρεται στο γεγονός ότι για μια ψήφο να θεωρείται έγκυρη, πρέπει να συμμορφώνεται με συγκεκριμένους κανόνες και προδιαγραφές που έχουν καθοριστεί για τη συγκεκριμένη ψηφοφορία. Αυτοί οι κανόνες μπορούν να περιλαμβάνουν διάφορα στοιχεία, όπως η απαίτηση για ταυτοποίηση του ψηφοφόρου, η ύπαρξη συγκεκριμένου επιτρεπόμενου τύπου ψηφοδελτίου ή η απαίτηση για σωστό συμπλήρωμα του ψηφοδελτίου.

Η αρχή της εγκυρότητας είναι σημαντική για να διασφαλίζεται ότι η ψηφοφορία διεξάγεται με διαφάνεια και ακρίβεια και ότι οι ψήφοι που μετρώνται αντιπροσωπεύουν πραγματικά την πρόθεση των ψηφοφόρων.

Αυτή η αρχή ικανοποιείται από το σύστημα που υλοποιήθηκε. Μέσω των πολλαπλών ελέγχων που γίνονται και στο τμήμα διεπαφής χρήστη αλλά και στο έξυπνο συμβόλαιο μας, δεν είναι δυνατή η καταβολή άκυρης ψήφου. Για να αποθηκευτεί μια ψήφος θα πρέπει να έχει γίνει αντιστοίχιση μοναδικού κωδικού με τη διεύθυνση Metamask, συνεπώς να έχει ολοκληρωθεί επιτυχώς το στάδιο της ταυτοποίησης. Σε διαφορετική περίπτωση όπως είδαμε και στο κεφάλαιο που έλαβαν χώρα οι " Περιπτώσεις ελέγχου", η αποθήκευση ψήφου δεν είναι δυνατή. Επιπρόσθετα λόγω της ηλεκτρονικής φύσης του συστήματος ψηφοφορίας, και του γεγονότος ότι για να σταλεί μια ψήφος, θα πρέπει να έχει επιλεχθεί υποψήφιος από μια λίστα υποψηφίων, η αποθήκευση "άκυρης" ψήφου είναι αδύνατη.

Τέλος, με την ύπαρξη λίστας έγκυρων ψηφοφόρων, γίνεται η αποφυγή πολλών λαθών που θα μπορούσαν να γίνουν κατά τη διάρκεια της ψηφοφορίας, ή της καταμέτρησης των ψήφων. Συνδυάζοντας όλες αυτές τις μεθόδους που χρησιμοποιήθηκαν από το σύστημα που υλοποιήθηκε, η αποθήκευση άκυρης ψήφου (ψήφος που δε θα έπρεπε να προσμετρηθεί), είναι αδύνατη.

Μέσω της ηλεκτρονικής ψηφοφορίας, μπορεί να τηρηθεί αυτή η αρχή, η οποία δημιουργεί πολλά προβλήματα στο παραδοσιακό τρόπο ψηφοφορίας. Οι έλεγχοι που γίνονται για την αποθήκευση μιας ψήφου μπορούν να τροποποιηθούν εύκολα από κάθε σύστημα ώστε να συμμορφώνονται στις ανάγκες αυτού.

6.3 Ανάλυση απειλών - Αντίσταση σε επιθέσεις

Το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) ορίζει την ανάλυση απειλών ως «τη διαδικασία επίσημης αξιολόγησης του διατάγματος απειλής για ένα πληροφοριακό σύστημα και την περιγραφή της φύσης της απειλής». Η ανάλυση απειλών, που ονομάζεται επίσης αξιολόγηση απειλών, είναι το ολοκληρωμένο σύνολο διαδικασιών και τεχνικών που εφαρμόζει ένας οργανισμός για να οικοδομήσει μια αποτελεσματική στρατηγική κυβερνοασφάλειας.

Υπάρχουν τρία είδη απειλών που πρέπει να αναλυθούν:

- **Τυχαίες απειλές**: Τις περισσότερες φορές, οι απειλές προέρχονται από ανθρώπινο λάθος. Σε περιβάλλοντα που βασίζονται σε κώδικα, τα λάθη μπορούν να δημιουργήσουν απειλές.
- **Εξωτερικές απειλές**: Οι φορείς απειλών συχνά στοχεύουν συγκεκριμένες εταιρείες ή βιομηχανίες για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε συστήματα, δίκτυα και συσκευές, ώστε να μπορούν να κλέψουν ευαίσθητες πληροφορίες.
- **Σκόπιμες απειλές**: Οι σκόπιμες απειλές είναι όταν οι εσωτερικοί χρήστες έχουν κακόβουλη πρόσβαση σε ευαίσθητα δεδομένα για δικό τους όφελος και για να βλάψουν τον οργανισμό.

Η τεχνολογία του blockchain έχει επαναστατήσει τον τρόπο με τον οποίο διεξάγονται οι ψηφοφορίες, επιτρέποντας μια αποκεντρωμένη, ασφαλή και διαφανή διαδικασία ψηφοφορίας. Σε αυτό το κεφάλαιο θα εξετάσουμε διάφορες απειλές που μπορούν να επηρεάσουν το σύστημα που υλοποιήθηκε και θα παρουσιάσουμε μεθόδους για την αντιμετώπιση τους.

6.3.1 Επιθέσεις στο δίκτυο του blockchain

Τα δίκτυα blockchain λειτουργούν με βάση τη βασική αρχή της αποκέντρωσης, της ανωνυμίας και της κρυπτογραφίας. Ουσιαστικά αυτό σημαίνει ότι δεν υπάρχει μια ενιαία οντότητα ελέγχου που διαχειρίζεται τη βάση δεδομένων, αλλά μάλλον διαφορετικοί κόμβοι στο δίκτυο που χρησιμοποιούν πρωτόκολλα συναίνεσης για την ασφαλή εκτέλεση συναλλαγών στο δίκτυο.

Όπως κάθε άλλη τεχνολογία, το Blockchain έχει τα μειονεκτήματά του παρά το γεγονός ότι διαθέτει ένα διαφανές και αμετάβλητο ψηφιακό καθολικό. Υπάρχουν διάφοροι διαφορετικοί τύποι απειλών ασφαλείας στους οποίους είναι ευάλωτα τα δίκτυα Blockchain [Cla+21].

Επίθεση 51%

Η επίθεση 51% είναι μια επίθεση στο blockchain, όπου μια ομάδα ελέγχει περισσότερο από το 50% της ισχύος κατακερματισμού του δικτύου. Αυτό τους δίνει τη δυνατότητα να εισάγουν ένα τροποποιημένο blockchain στο δίκτυο, να μπλοκάρουν συναλλαγές άλλων χρηστών, να αποκλείσουν άλλους miners, και γενικότερα να τροποποίησουν το blockchain όπως εκείνοι θέλουν, ενέργειες που γίνονται αποδεκτές μιας και οι επιτιθέμενοι κατέχουν το μεγαλύτερο ποσοστό του δικτύου, το οποίο γίνεται αποδεκτό μιας και οι επιτιθέμενοι θα καθορίζουν τα περιεχόμενα του. Μια επιτυχής επίθεση 51% θα ήταν καταστροφική για το σύστημα μας, καθώς θα μπορούσε να αλλοιώσει τα αποτελέσματα των εκλογών, ή να σταθεί εμπόδιο σε ολόκληρη την εκλογική διαδικασία. Ωστόσο, μια τέτοια επίθεση είναι πολύ δύσκολη και προκλητική εργασία σε κάποιο δίκτυο με μεγάλο ποσοστό συμμετοχής, με τεράστιο κόστος.

Εκτός από το κόστος, μια ομάδα που θέλει να επιτεθεί στο δίκτυο, με αυτή την επίθεση πρέπει όχι μόνο να ελέγχει το 51% των κόμβων του δικτύου, αλλά πρέπει επίσης να εισάγει το τροποποιημένο/α block στο blockchain σε πολύ ακριβή χρόνο. Ακόμα κι αν κατέχουν το 51% του ποσοστού κατακερματισμού δικτύου, ενδέχεται να μην είναι σε θέση να συμβαδίσουν με το ποσοστό δημιουργίας μπλοκ ή να εισαγάγουν την αλυσίδα τους πριν δημιουργηθούν έγκυρα νέα μπλοκ από το πραγματικό δίκτυο blockchain.

Μετά τη μετάβαση του Ethereum στο proof-of-stake, μια επίθεση 51% στο blockchain Ethereum έγινε ακόμη πιο ακριβή. Για να πραγματοποιηθεί αυτή η επίθεση, ένας χρήστης ή ομάδα θα πρέπει να κατέχει το 51% του στοιχηματισμένου ETH στο δίκτυο.

Η προστασία από αυτού του είδους επίθεσης είναι ένας από τους κύριους λόγους επιλογής του δικτύου του Ethereum για την υλοποίηση του συστήματος ψηφοφορίας, καθώς τα μεγάλα κρυπτονομίσματα είναι απίθανο να υποφέρουν από επιθέσεις 51% λόγω του απαγορευτικού κόστους απόκτησης τόσο μεγάλης ισχύος κατακερματισμού, αλλά και από το γεγονός ότι καθιστούν αδύνατη την εισαγωγή τροποποιημένου blockchain. Για το λόγο αυτό, η 51% επίθεση αποτελεί απειλή κυρίως σε κρυπτονομίσματα με λιγότερη συμμετοχή και ισχύ κατακερματισμού.

Επίθεση DOS

Μια επίθεση Distributed Denial-of-Service (DDOS) στους υπολογιστές είναι μια επίθεση, όπου ένας δράστης επιδιώκει να καταστήσει έναν πόρο δικτύου μη διαθέσιμο στους χρήστες του, πλημμυρίζοντας το δίκτυο με μεγάλο αριθμό αιτημάτων σε μια προσπάθεια να υπερφορτώσει το σύστημα. Είναι μια επίθεση από την οποία μπορεί να υποστούν όχι μόνο τα blockchain αλλά και οποιαδήποτε διαδικτυακή υπηρεσία.

Σε μια απλή μορφή, την επίθεση DOS (Denial-of-Service), όλα αυτά τα αιτήματα προέρχονται από την ίδια πηγή. Αυτό καθιστά κάπως εύκολη την πρόληψη. Εάν μια μεμονωμένη διεύθυνση IP αποστέλλει τεράστιο αριθμό αιτημάτων που δεν μπορούν να δικαιολογηθούν από νόμιμους λόγους, μπορεί να εφαρμοστεί ένα μέτρο που αποκλείει αυτόματα αυτήν τη διεύθυνση IP. Στην περίπτωση επίθεσης DDOS, το κατανεμημένο τμήμα αναφέρεται σε μεγάλο αριθμό διαφορετικών πηγών από τις οποίες προέρχονται τα κακόβουλα αιτήματα.

Λόγω της ψηφιακής του φύσης, το blockchain είναι επιρρεπές σε επίθεση και εκμετάλλευση. Οι επιθέσεις DDoS σε ένα blockchain επικεντρώνονται στο επίπεδο πρωτοκόλλου, με τη μεγαλύτερη απειλή για τα blockchain να είναι η πλημμύρα συναλλαγών. Οι παραδοσιακές επιθέσεις DDoS μπορούν να εκτελεστούν ενάντια σε μια αλυσίδα μπλοκ για να επιβραδύνουν τις λειτουργίες της.

Σε περίπτωση επίθεσης DDoS κάποιοι κόμβοι θα μπορούσαν να τεθούν εκτός λειτουργίας για ένα μικρό χρονικό διάστημα. Το δίκτυο blockchain λόγω της κατανεμημένης φύσης του, διασφαλίζει ότι οι συναλλαγές μπορούν να συνεχιστούν ακόμα και αφού ορισμένοι κόμβοι τεθούν εκτός σύνδεσης. Αυτό δεν υποδηλώνει όμως, ότι τα δίκτυα blockchain είναι πλήρως ανθεκτικά στις επιθέσεις DDoS.

Οι επιθέσεις DDoS θεωρούνται «όπλο μαζικής καταστροφής» στο Διαδίκτυο. Είναι πιο δύσκολο να αμυνθούν έναντι των επιθέσεων, και επί του παρόντος, δεν υπάρχουν προφυλάξεις που μπορεί να εφαρμόσει οποιοσδήποτε οργανισμός για να είναι ασφαλής 100%. Όσο μεγαλύτερη είναι η υπολογιστική ισχύς, τόσο μεγαλύτερες είναι οι πιθανότητες αντιμετώπισης μιας επίθεσης blockchain DDoS. Αυτός είναι ένας ακόμη λόγος επιλογής του δικτύου Ethereum, για την υλοποίηση του συστήματος ψηφοφορίας, καθώς προσφέρει ένα πολύ μεγάλο εύρος ασφάλειας σε τέτοιου είδους μαζικές επιθέσεις.

Επίθεση Sybil

Η επίθεση Sybil είναι μια προσπάθεια χειραγώγησης ενός κατανεμημένου δικτύου, όπου μια οντότητα έχει πολλές ψευδείς ταυτότητες. Για τον παρατηρητή, αυτές οι διαφορετικές ταυτότητες

μοιάζουν με κανονικούς χρήστες, αλλά πίσω από τα παρασκήνια, μια ενιαία οντότητα ελέγχει όλες αυτές τις ψεύτικες οντότητες ταυτόχρονα.

Σε ένα σύστημα ψηφοφορίας, μια Sybil επίθεση μπορεί να χρησιμοποιηθεί για να επηρεάσει το αποτέλεσμα της ψηφοφορίας. Ο επιτιθέμενος μπορεί να χρησιμοποιήσει τις πολλές ταυτότητες για να ψηφίσει πολλές φορές, επηρεάζοντας έτσι το αποτέλεσμα της ψηφοφορίας. Επίσης, ο επιτιθέμενος μπορεί να διασπείρει ψευδείς ψήφους στο σύστημα, προκαλώντας σύγχυση και αβεβαιότητα στους αληθινούς ψηφοφόρους.

Το σύστημα που δημιουργήσαμε είναι απόλυτα ανθεκτικό σε κάθε μορφή επίθεσης Sybil. Αυτό είναι δυνατόν χάρη στη μεθοδολογία αυθεντικοποίησης πολλών παραγόντων που απαιτείται για την εκλογική διαδικασία. Λόγω της ύπαρξης λίστας έγκυρων λογαριασμών - ψηφοφόρων, αλλά και των απαιτούμενων βημάτων αυθεντικοποίησης για την αποθήκευση μιας ψήφου, δεν είναι εφικτή η προσπάθεια καταβολής πολλών ψήφων από έναν λογαριασμό. Επιπλέον, η χρήση του δικτύου Ethereum αποτρέπει την εμφάνιση σημαντικής αύξησης στην κίνηση του blockchain, κάτι που αποτρέπει τις επιθέσεις Sybil από έναν κόμβο.

Με τη λήψη των κατάλληλων μέτρων για τη δημιουργία της λίστας έγκυρων ψηφοφόρων και τη συνεχή παρακολούθηση από το έξυπνο συμβόλαιο κάθε φορά που κάποιος αλληλεπιδρά με αυτό, σε συνδυασμό με τη χρήση του Ethereum και των αντίστοιχων πρωτοκόλλων, το σύστημα που υλοποιήσαμε σε αυτήν τη διπλωματική εργασία θεωρείται απόλυτα ασφαλές από επιθέσεις Sybil, καθώς δεν επιτρέπεται σε μη αυθεντικοποιημένους χρήστες να αλληλεπιδράσουν με το έξυπνο συμβόλαιο.

6.3.2 Λειτουργικές επιθέσεις στη διαδικασία ψηφοφορίας

Σε αυτή την υποενότητα, θα αναλύσουμε την ασφάλεια του συστήματος σε επιθέσεις που θα μπορούσαν να βλάψουν τις λειτουργικές διαδικασίες του συστήματος.

Man in The Middle

Η επίθεση “Man in the Middle “ είναι η επίθεση στην οποία ένας επιτιθέμενος τοποθετείται σε μια συνομιλία μεταξύ ενός χρήστη και μιας εφαρμογής. Ο επιτιθέμενος μέσω αυτής της επίθεσης θα βρίσκεται σε θέση να κλέψει προσωπικές πληροφορίες που ανταλλάσσονται μεταξύ του χρήστη και της εφαρμογής. Οι πληροφορίες που λαμβάνονται κατά τη διάρκεια μιας επίθεσης θα μπορούσαν να χρησιμοποιηθούν για πολλούς σκοπούς, συμπεριλαμβανομένης της κλοπής ταυτότητας, ή της ψήφου.

Υπάρχουν τρεις τρόποι επίθεσης:

1. **IP spoofing**: ένας εισβολέας μεταμφιέζεται σε εφαρμογή αλλάζοντας τις κεφαλίδες των πακέτων σε μια διεύθυνση IP. Έτσι, οι χρήστες που προσπαθούν να αποκτήσουν πρόσβαση σε ένα URL, αποστέλλονται στον ιστότοπο του εισβολέα.

2. **ARP spoofing**: η MAC διεύθυνση ενός εισβολέα συνδέεται με τη διεύθυνση IP ενός χρήστη σε ένα τοπικό δίκτυο. Έτσι όλα τα μηνύματα μεταδίδονται στον εισβολέα.

3. **DNS spoofing**: επίθεση σε έναν διακομιστή DNS με σκοπό την αλλαγή διευθύνσεων ενός ιστότοπου. Έτσι, οι χρήστες που προσπαθούν να εισέλθουν σε έναν ιστότοπο αποστέλλονται στον ιστότοπο του εισβολέα.

Στη συνέχεια για να γίνει μια MITM επίθεση επιτυχώς θα πρέπει ο επιτιθέμενος να αποκρυπτογραφήσει τα δεδομένα που λαμβάνει. Αυτή η αποκρυπτογράφηση, θα μπορούσε να περιλαμβάνει διάφορες τεχνικές όπως το SSL stripping, δηλαδή την υποβάθμιση μιας HTTPS σύνδεσης σε HTTP παρεμποδίζοντας τον έλεγχο ταυτότητας TLS που αποστέλλεται από την εφαρμογή στον χρήστη.

Για να παρεμποδιστεί αυτή η επίθεση από το σύστημα μας θα πρέπει να ληφθούν μερικά μέτρα. Το πιο σημαντικό είναι η αποκατάσταση ασφαλούς σύνδεσης. Εκτός από την end-to-end κρυπτογράφηση που παρέχεται, θα μπορούσαν να διαμορφωθούν πολιτικές HTTP Strict Transport Security (HSTS) για να επιβάλει τη χρήση της ασφάλειας SSL/TLS σε πολλούς υποτομείς. Αυτό βοηθά στην περαιτέρω ασφάλεια του ιστότοπου και της εφαρμογής Ιστού από επιθέσεις υποβάθμισης πρωτοκόλλου και απόπειρες παραβίασης cookie. Λόγω χρήσης του Metamask, και των μεθόδων ασφαλείας που παρέχει, ακόμα και στην περίπτωση που ένας επιτιθέμενος έκανε ARP spoofing και υποβάθμιση σε HTTP, ο διακομιστής δε θα μπορούσε να λειτουργήσει από τη μεριά του χρήστη, καθώς απαιτείται SSL κρυπτογράφηση για την ορθή λειτουργία του Metamask.

Επιπλέον, οι πολίτες θα πρέπει να ενημερωθούν από τις αρχές κατά την εγγραφή τους στο σύστημα, ώστε να προστατευτούν από phising email, που θα μπορούσαν να τους οδηγήσουν σε λανθασμένες ιστοσελίδες, ή να κατεβάσουν κακόβουλο κώδικα στη συσκευή τους.

Εκμετάλλευση έξυπνου συμβολαίου

Στις επιθέσεις εκμετάλλευσης έξυπνων συμβολαίων περιλαμβάνονται επιθέσεις όπου ο επιτιθέμενος εκμεταλλεύεται κάποια αδυναμία ή ευπάθεια στον κώδικα του συμβολαίου. Θα δούμε στη συνέχεια ορισμένες από τις συνηθέστερες επιθέσεις εκμετάλλευσης έξυπνου συμβολαίου, καθώς και τον τρόπο που αντιμετωπίζονται από το σύστημα μας

- **Reentrancy attacks** (επιθέσεις επανεισδοχής): Αυτή η επίθεση συμβαίνει όταν ένα έξυπνο συμβόλαιο καλείται επαναλαμβανόμενα από άλλο συμβόλαιο κατά τη διάρκεια μιας συναλλαγής, με στόχο να αποσπαστούν πόροι από το πρώτο συμβόλαιο πριν ολοκληρωθεί η συναλλαγή. Στο σύστημα που υλοποιήθηκε, έχουμε ορίσει τις μεταβλητές και τις συναρτήσεις που αφορούν ευαίσθητα προσωπικά δεδομένα ως **private**. Συνεπώς, δεν είναι δυνατή η κλήση τους από άλλα έξυπνα συμβόλαια. Παράλληλα οι δημόσιες συναρτήσεις περιλαμβάνουν πολλούς ελέγχους ταυτότητας, αποκλείοντας με αυτό το τρόπο ανεπιθύμητες διευθύνσεις.

- Επιθέσεις **front-running**: Αυτές οι επιθέσεις συμβαίνουν όταν κάποιος αναμένει την απόδοση κάποιου έξυπνου συμβολαίου και την εκτελεί πρώτος, πριν η αρχική συναλλαγή ολοκληρωθεί. Αυτό μπορεί να οδηγήσει σε απώλεια κεφαλαίου ή δυσλειτουργία του συμβολαίου. Μια front-running επίθεση στο σύστημα ψηφοφορίας, θα μπορούσε να πραγματοποιηθεί ως εξής: όταν κάποιος επιτιθέμενος εντοπίσει τις συναλλαγές ψηφοφορίας που πρόκειται να εκτελεστούν στο Ethereum, προσθέσει μια δική του συναλλαγή με μεγαλύτερη προμήθεια (gas fee) για να εκτελεστεί πρώτη. Αυτός ο επιτιθέμενος μπορεί να αλλάξει την ψήφο του χρήστη και να προσθέσει τη δική του ψήφο στο σύστημα ψηφοφορίας. Αυτή η μορφή επίθεσης δεν είναι εφικτή στο σύστημα μας, λόγω των μέτρων ταυτοποίησης που έχουν ληφθεί και απαιτούν τη σύνδεση της διεύθυνσης με έναν OTP μετά την ταυτοποίηση. Έτσι, αν κάποιος προσπαθήσει να ψηφίσει πριν από την αρχική ψηφοφορία, η ψήφος του δε θα επιβεβαιωθεί, διότι δε θα έχει προηγηθεί επαλήθευση ταυτότητας και ορισμός OTP.

- Επιθέσεις **timestamp**: Αυτές οι επιθέσεις συμβαίνουν όταν ένας επιτιθέμενος δημιουργεί μια συναλλαγή και αλλάζει το timestamp της, ώστε να επιτευχθεί μια επιθυμητή κατάσταση στο συμβόλαιο που επηρεάζει τη συναλλαγή. Αν ο επιτιθέμενος καταφέρει να αλλοιώσει την ώρα στην οποία υποβλήθηκαν οι ψήφοι στο σύστημα ψηφοφορίας, τότε μπορεί να υποβάλει μια ψήφο που θα μετρηθεί ως νόμιμη παρόλο που υποβλήθηκε μετά την καθορισμένη προθεσμία ψηφοφορίας. Αυτό μπορεί να οδηγήσει στην αλλοίωση των αποτελεσμάτων της ψηφοφορίας και σε αποτυχία του συστήματος ψηφοφορίας να λειτουργήσει σωστά. Ωστόσο, αυτή η μορφή επίθεσης είναι ακίνδυνη για το σύστημα μας, λόγω των ελέγχων timestamp που γίνονται από το έξυπνο συμβόλαιο, αλλά και των ενεργειών που λαμβάνουν οι αρχές, δηλαδή τη λήψη των ψήφων για κάθε υποψήφιο ακριβώς τη χρονική στιγμή λήξης των εκλογών.

- Επιθέσεις μεταβλητής **overflow/underflow**: Αυτές οι επιθέσεις συμβαίνουν όταν οι τιμές μιας μεταβλητής σε ένα εξυπνό συμβόλαιο ξεπερνούν τα όρια του εύρους τους, προκαλώντας απρόβλεπτη συμπεριφορά του συμβολαίου και πιθανώς απώλεια κεφαλαίου. Για αυτό το λόγο έχουν χρησιμοποιηθεί mappings και όχι πίνακες στο έξυπνο συμβόλαιο καθώς θα μπορούσαν να ξεπεράσουν τα όρια εύρους, καθώς μιλάμε για εκατομμύρια πολίτες και ψήφους.

6.3.3 Συνολική αξιολόγηση ασφάλειας

Παρότι κανένα σύστημα δεν είναι απόλυτα ασφαλές, η υλοποίησή προσφέρει ένα υψηλό βαθμό ασφάλειας και προστασίας από πολλές από τις κοινές και σοβαρές επιθέσεις που μπορούν να επηρεάσουν ένα σύστημα ψηφοφορίας μέσω blockchain. Το πλήθος τεχνικών και μηχανισμών ασφαλείας αποτελεί μια ισχυρή προστασία κατά των πιο διαδεδομένων απειλών.

Σχήμα 45. Παράμετροι ασφαλείας

Πάντα υπάρχει ένας βαθμός κινδύνου, όμως με τη χρήση της αρχιτεκτονικής του Ethereum blockchain, ενισχύεται σημαντικά η ασφάλεια του συστήματος. Επιπλέον, η χρήση end-to-end κρυπτογράφησης και του Metamask προστατεύει από κάθε πιθανό κίνδυνο κλοπής ή τροποποίησης δεδομένων, διασφαλίζοντας ότι οι επικοινωνίες μεταξύ των χρηστών και της πλατφόρμας παραμένουν ασφαλείς και αποτρέποντας την παραβίαση ή την παραποίηση των δεδομένων. Γενικά, το σύστημα που υλοποιήθηκε αντιμετωπίζει με επιτυχία τις περισσότερες και πιο δημοφιλείς επιθέσεις, προσφέροντας έναν υψηλό βαθμό ασφάλειας για τις διαδικασίες ψηφοφορίας. Ωστόσο, είναι σημαντικό να διατηρηθεί η πλατφόρμα ενημερωμένη και να λαμβάνετε υπόψη τις τελευταίες εξελίξεις στον τομέα της ασφάλειας, προκειμένου να προστατεύεστε από νέες απειλές και ευπάθειες που μπορεί να εμφανιστούν.

6.4 Προτάσεις για περαιτέρω μελέτη

Το σύστημα ψηφοφορίας που υλοποιήθηκε, είναι μια αξιοσημείωτη προσπάθεια για πιο δίκαιες και διαφανείς εκλογές, καθώς προσφέρει λύσεις σε προβλήματα που ταλαιπωρούν τις αρχές,

του ψηφοφόρους ή τις αρχές ψηφοφορίας στις παραδοσιακές εκλογές. Ωστόσο, κανένα σύστημα δεν είναι απόλυτα τέλειο και έχει πάντα αδυναμίες. Σε αυτό το κεφάλαιο θα εξετάσουμε προσεκτικά τις αδυναμίες του συστήματος, και θα παρουσιάσουμε πιθανές λύσεις για να βελτιωθεί η ασφάλεια και η αξιοπιστία του. Αυτό θα εξασφαλίσει ότι η εφαρμογή θα παραμείνει αξιόπιστη και έτοιμη για χρήση από το ευρύ κοινό.

6.4.1 Αδυναμίες συστήματος

Αποστολή SMS

Το σύστημα που υλοποιήθηκε παρουσιάζει μερικές αδυναμίες, η επίλυση των οποίων θα μπορούσε να το θέσει ιδανικό και έτοιμο για χρήση ακόμη και στο επίπεδο των εθνικών εκλογών.

Η πρώτη αδυναμία που χρήζει επίλυσης αφορά την αποστολή του κωδικού μιας χρήσης μέσω SMS. Όπως αναφέραμε η αποστολή γίνεται από τη πλευρά της διεπαφής χρήστη αποθηκεύοντας τα κλειδιά και τα αναγνωριστικά του API ως environment μεταβλητές. Η αποθήκευση ευαίσθητων δεδομένων στη διεπαφή χρήστη ως env μεταβλητές, ενδέχεται να εκθέσει τα API κλειδιά σε πιθανές απειλές ασφάλειας. Αυτό συμβαίνει επειδή ο κώδικας Javascript σε μια React. js εφαρμογή, εκτελείτε στην πλευρά του χρήστη, πράγμα που σημαίνει ότι οποιοσδήποτε έχει πρόσβαση στο πηγαίο κώδικα της εφαρμογής μπορεί ενδεχομένως να δει τα κλειδιά. Επιπλέον, η αποθήκευση των κλειδιών API ως μεταβλητές περιβάλλοντος σε μια εφαρμογή React.js, σημαίνει ότι θα είναι ορατά στην κονσόλα προγραμματιστή του προγράμματος περιήγησης, στην οποία μπορεί να έχει πρόσβαση οποιοσδήποτε χρησιμοποιεί την εφαρμογή. Αυτό μπορεί να θέσει τα κλειδιά σε κίνδυνο κλοπής ή κακής χρήσης.

Οι εφαρμογές που χρησιμοποιούν μεθόδους αποστολής μηνυμάτων, αποθηκεύουν τα κλειδιά API στην πλευρά του διακομιστή της εφαρμογής, ώστε να μην είναι ορατά στο κώδικα Javascript στη διεπαφή χρήστη. Αυτή η μέθοδος όμως δεν είναι επιθυμητή καθώς η ύπαρξη πλευράς διακομιστή, θα μπορούσα να αλλοιώσει την εμπιστευτικότητα της αποκεντρωμένης εφαρμογής μας.

Αποθήκευση ψήφων

Στην υλοποίηση της εφαρμογής μας δεν ασχοληθήκαμε ιδιαίτερα με την αποθήκευση ψήφων, καθώς οι ονομασίες και το πλήθος των υποψηφίων μπορεί να διαφέρει αναλόγως τις ανάγκες της κάθε ψηφοφορίας. Επομένως, για κάθε περίπτωση ψηφοφορίας, θα μπορούσαν να χρησιμοποιηθούν κατάλληλες μέθοδοι για την ασφαλή αποθήκευση ψήφων, που θα καθιστούσαν την αποθήκευση των ψήφων ασφαλή και μην προσβάσιμη.

Ωστόσο, οφείλουμε να αναφέρουμε πως η μέθοδος που χρησιμοποιήθηκε για την αποθήκευση των ψήφων παρουσιάζει αδυναμία, που έρχεται σε αντιπαράθεση με τις αρχές των εκλογών. Η χρήση ενός δημόσιου blockchain, όπως αυτό του Ethereum, σημαίνει ότι όλες οι μεταβλητές που αποθηκεύονται στο έξυπνο συμβόλαιο, είναι δημόσιες. Επομένως, είναι προσβάσιμες από κάθε έναν που θα μπορούσε να τρέχει στον υπολογιστή του κάποιο αντίγραφο αυτού του blockchain. Η έννοια της λέξης "**private**" που χρησιμοποιήθηκε μπροστά από πολλές μεταβλητές στο έξυπνο συμβόλαιο σημαίνει ότι αυτές οι μεταβλητές δε μπορούν να τροποποιηθούν, από μεθόδους που δεν ανήκουν σε αυτό το έξυπνο συμβόλαιο, χωρίς να εγγυάται ότι δε μπορούν να διαβαστούν από τους χρήστες με αντίγραφο του Ethereum, καθώς θα αλλοιωνόταν όλη η αποκεντρωμένη φύση του blockchain. Επομένως, μέσω της υλοποίησης μας θα μπορούσαν επιτιθέμενοι να διαρρεύσουν στοιχεία που θα αλλοίωναν τη διαδικασία της ψηφοφορίας, όπως πόσες ψήφους έχει ο κάθε υποψήφιος.

Να σημειωθεί ότι λόγω της κρυπτογράφησης, της αντικατάστασης με διευθύνσεις Metamask, αλλά και τη μη αποθήκευση του υποψηφίου που ψήφισε κάθε ψηφοφόρος, δεν αντιμετωπίζουμε το ίδιο πρόβλημα στο τομέα της μυστικότητας, καθώς είναι αδύνατο να βρει κανείς ποιος ψήφισε ποιον.

Δυσκολία χρήσης

Η ψηφοφορία μέσω blockchain έχει το δυναμικό να προσφέρει αξιόπιστη, διαφανή και ασφαλή μορφή ψηφοφορίας. Ωστόσο, η εφαρμογή της σε κοινωνικές ομάδες με διαφορετικά επίπεδα τεχνολογικής κατανόησης και πρόσβασης στην τεχνολογία μπορεί να αποτελέσει μια πρόκληση.

Η πρώτη δυσκολία αφορά την ανισότητα στην πρόσβαση στην τεχνολογία, καθώς πολλοί μπορεί να μη διαθέτουν κινητά τηλέφωνα, να μη γνωρίζουν που να τοποθετήσουν το Metamask, η γενικότερα να δυσκολευτούν στη διαδικασία ταυτοποίησης και ψηφοφορίας, καθώς δεν είναι εξοικειωμένοι με τη χρήση της τεχνολογίας.

Δεύτερον, η αστάθεια των συστημάτων ψηφοφορίας μέσω blockchain μπορεί να αποτρέψει τη συμμετοχή ανθρώπων με χαμηλή εμπιστοσύνη στην τεχνολογία. Αν το σύστημα δε λειτουργήσει σωστά ή δεν είναι ασφαλές, οι χρήστες μπορεί να απογοητευτούν και να μη θέλουν να χρησιμοποιήσουν το σύστημα ξανά στο μέλλον.

6.4.2 Προτάσεις βελτίωσης απόδοσης συστήματος

Παρά τα προβλήματα που αναφέρθηκαν, μπορούν να γίνουν τροποποιήσεις στο σύστημα, που θα μπορούσαν να προσφέρουν λύσεις, καθιστώντας το σύστημα πιο αξιόπιστο, ασφαλές και έτοιμο για χρήση.

Oracles

Η υποβολή αιτημάτων HTTP, μέσω ενός έξυπνου συμβολαίου είναι αδύνατη, καθώς αλλοιώνει την αποκεντρωμένη φύση του. Υπάρχουν πολλοί περιορισμοί στην αλληλεπίδραση των έξυπνων συμβολαίων με εξωτερικά συστήματα, κάτι που αποτελεί σημαντικό περιορισμό κατά την κατασκευή αποκεντρωμένων εφαρμογών. Λόγω αυτού, υπάρχει περιορισμένη ικανότητά για πρόσβαση σε εξωτερικά δεδομένα και υπηρεσίες που είναι απαραίτητες για τη δημιουργία πιο προηγμένων και πολύπλοκων αποκεντρωμένων εφαρμογών.

Για να μπορεί κανείς να κάνει ένα αίτημα HTTP χρησιμοποιώντας το έξυπνο συμβόλαιο με Solidity, πρέπει να αλληλεπιδράσει με εξωτερικά API και να ανακτήσει δεδομένα από υπηρεσίες web.

Τα Oracles είναι υπηρεσίες τρίτων (third - party) που λειτουργούν ως μεσάζοντες μεταξύ έξυπνων συμβολαίων και εξωτερικών συστημάτων. Μπορούν να παρέχουν έξυπνα συμβόλαια με πρόσβαση σε εξωτερικά δεδομένα και υπηρεσίες, συμπεριλαμβανομένης της δυνατότητας υποβολής αιτημάτων HTTP. Επιπλέον, η χρήση oracles μπορεί να αυξήσει την ασφάλεια των έξυπνων συμβολαίων, καθώς λειτουργούν ως ενδιάμεσος χώρος μεταξύ του έξυπνου συμβολαίου και των εξωτερικών συστημάτων, μειώνοντας τον κίνδυνο τρωτών σημείων ασφαλείας.

Υπάρχουν πολλές υπηρεσίες oracle που επιτρέπουν σε ένα έξυπνο συμβόλαιο να μοιάζει σαν να πραγματοποιεί κλήση API, ωστόσο το oracle πραγματοποιεί πραγματικά τις κλήσεις API εκτός αλυσίδας και δημοσιεύει το αποτέλεσμα στην αλυσίδα για χρήση έξυπνων συμβολαίων. Μερικά από αυτά περιλαμβάνουν το Chainlink, το Provable, το BandChain και το Tellor.

Μια πιθανή λύση είναι η χρήση του Chainlink για πάροχο Oracle. Το Chainlink είναι ένα αποκεντρωμένο δίκτυο oracle που συνδέει έξυπνα συμβόλαια με πηγές δεδομένων εκτός αλυσίδας, API και συστήματα πληρωμών. Οι κόμβοι Chainlink θα λειτουργούν ως oracles, παρέχοντας έξυπνα συμβόλαια με πρόσβαση σε εξωτερικά API και πηγές δεδομένων. Θα πρέπει να τροποποιήσουμε το έξυπνο συμβόλαια κατάλληλα ώστε να αλληλεπιδρά με το δίκτυο oracle του Chainlink, για την υποβολή ενός HTTP request, και πιο συγκεκριμένα ενός POST request, στο twilio, η το API που θα χρησιμοποιηθεί για την αποστολή των μηνυμάτων. Το συμβόλαιο θα ορίσει μια συνάρτηση που λαμβάνει μια διεύθυνση URL και μια συμβολοσειρά query ως παραμέτρους εισόδου και επιστρέφει το αποτέλεσμα του αιτήματος HTTP ως συμβολοσειρά. Η συνάρτηση θα χρησιμοποιήσει το Chainlink oracle για να κάνει το αίτημα HTTP και να ανακτήσει τα δεδομένα απόκρισης.

Πιο συγκεκριμένα το έξυπνο συμβόλαιο θα πρέπει να λειτουργεί ως εξής:

- Στέλνει ένα αίτημα στο Chainlink oracle, συμπεριλαμβανομένου του URL και της συμβολοσειράς του query.
- Το Chainlink oracle ανακτά τα δεδομένα απόκρισης από το εξωτερικό API ή την πηγή δεδομένων.
- Το Chainlink oracle στέλνει τα δεδομένα απόκρισης πίσω στο έξυπνο συμβόλαιο.
- Το έξυπνο συμβόλαιο επιστρέφει τα δεδομένα απόκρισης στην εφαρμογή κλήσης.

Πιο συγκεκριμένα θα πρέπει να υλοποιηθούν τα παρακάτω βήματα:

1. Δημιουργούμε ένα έξυπνο συμβόλαιο, που να κληρονομεί το έξυπνο συμβόλαιο Chainlink Client,με σκοπό την αλληλεπίδραση με το chainlink blockchain oracle.
2. Δημιουργούμε τη συνάρτηση που θα κάνει HTTP request. Για να υλοποιηθεί αυτό, αυτή η συνάρτηση θα πρέπει να καλεί την συνάρτηση requestOracleData() από το συμβόλαιο ChainlinkClient. Η συνάρτηση requestOracleData() λαμβάνει πολλές παραμέτρους, συμπεριλαμβανομένης της διεύθυνσης URL του API που θα καλέσουμε, της μεθόδου HTTP που θα χρησιμοποιήσουμε και της αναμενόμενης μορφής δεδομένων.
3. Πριν καλέσουμε τη συνάρτηση requestOracleData(), θα χρειαστεί να καθορίσουμε το συμβόλαιο orracle Chainlink που θα χειριστεί το αίτημα. Αυτό μπορεί να γίνει καλώντας τη συνάρτηση setChainlinkOracle() και περνώντας τη διεύθυνση του συμβολαίου oracle.
4. Συμπληρώνουμε το job ID του API που θέλουμε να καλέσουμε.
5. Αφού καθορίσουμε το συμβόλαιο Oracle και το αναγνωριστικό εργασίας, καλούμε τη συνάρτηση requestOracleData() για να υποβάλουμε το αίτημα HTTP. Αυτή η λειτουργία θα επιστρέψει ένα αναγνωριστικό αιτήματος για τη παρακολούθηση κατάστασης του αιτήματος.
6. Μόλις ολοκληρωθεί το αίτημα, το oracle θα καλέσει μια συνάρτηση επανάκλησης στο έξυπνο συμβόλαιό, με τα δεδομένα απόκρισης.

Για περισσότερες λεπτομέρειες σχετικά με την υιοθέτηση του Chainlink oracle, αλλά και όλων των προαπαιτούμενων για την υλοποίηση θα μπορούσε κανείς να διαβάσει την τεκμηρίωση του Chainlink (Chainlink documentation). Επίσης, όπως αναφέρθηκε προηγουμένως θα μπορούσαν να χρησιμοποιηθούν και άλλες υπηρεσίες όπως το Provable, που παρέχουν υπηρεσίες διαμεσολαβητή ενός έξυπνου συμβολαίου με υπηρεσίες εκτός του blockchain.

Ασφαλής αποθήκευση ψήφων

Παρά το γεγονός ότι σε αυτή τη διπλωματική δεν εμβαθύναμε στην ασφάλεια και απόκρυψη των ψήφων, κατά την αποθήκευσή τους, οφείλουμε να αναφέρουμε ότι είναι ένα μείζων ζήτημα που χρήζει επίλυσης. Παρότι η αποθήκευση των ψήφων σε ένα blockchain, είναι μια καλή ιδέα, καθώς το blockchain παρέχει μια ασφαλή και αξιόπιστη μέθοδο για την αποθήκευση και τη μεταφορά δεδομένων, για να διασφαλίσουμε την ασφάλεια των ψήφων στο blockchain του Ethereum, θα πρέπει να χρησιμοποιηθούν διάφορες κρυπτογραφικές μέθοδοι, επιλογή των οποίων θα γίνει βάσει των αναγκών των εκλογών.

Μια από τις κρυπτογραφικές μεθόδους που μπορούν να χρησιμοποιηθούν είναι η δημιουργία ενός κλειδιού κρυπτογράφησης για κάθε ψήφο. Το κλειδί αυτό θα πρέπει να είναι μοναδικό για κάθε ψήφο και να αποθηκεύεται στο blockchain. Στη συνέχεια, το κλειδί αυτό θα χρησιμοποιηθεί

για την αποκρυπτογράφηση της ψήφου μόνο από τον κάτοχο του κλειδιού. Αυτό εξασφαλίζει την ασφάλεια των ψήφων, καθώς μόνο ο κάτοχος του κλειδιού μπορεί να αποκρυπτογραφήσει την ψήφο του και να την καταμετρήσει.

Μια άλλη κρυπτογραφική μέθοδος που μπορεί να χρησιμοποιηθεί είναι η χρήση κρυπτογραφίας δημόσιου και ιδιωτικού κλειδιού. Κάθε ψηφοφόρος θα δημιουργεί ένα ζεύγος κλειδιών κρυπτογραφίας δημόσιου και ιδιωτικού κλειδιού. Η ψήφος του θα κρυπτογραφείται με το δημόσιο κλειδί του, ενώ η αποκρυπτογράφηση θα γίνεται μόνο με το ιδιωτικό κλειδί του. Τα κλειδιά θα αποθηκεύονται στο blockchain και θα είναι διαθέσιμα μόνο στον κάτοχο τους.

Επιπλέον, θα μπορούσαν να κρυπτογραφηθούν και οι υποψήφιοι μέσω ενός δημοσίου - ιδιωτικού κλειδιού, έτσι ώστε να μη γνωρίζει κανείς πόσες ψήφους έχει κάθε ψηφοφόρος. Με το πέρας των εκλογών οι ψήφοι κάθε ψηφοφόρου θα αποκρυπτογραφούνται και θα βγαίνουν τα αποτελέσματα των εκλογών.

Εκτός των παραπάνω μεθόδων κρυπτογράφησης, μπορεί να χρησιμοποιηθεί και η off-chain τεχνολογία για να διασφαλιστεί η ασφάλεια των ψήφων. Με τη χρήση της off-chain τεχνολογίας, οι ψήφοι δεν αποθηκεύονται απευθείας στο blockchain, αλλά σε ένα ασφαλές off-chain αποθηκευτικό μέσο. Η επιβεβαίωση της ψήφου γίνεται στη συνέχεια στο blockchain με τη χρήση επισφαλών αλλά γρήγορων μηχανισμών συναίνεσης που επιτρέπουν στους κόμβους του blockchain να επιβεβαιώσουν την ακρίβεια των ψήφων χωρίς να χρειάζεται να αποκαλύψουν την ταυτότητα του ψηφοφόρου ή το περιεχόμενο της ψήφου. Με αυτόν τον τρόπο, διατηρείται η ιδιωτικότητα του ψηφοφόρου ενώ εξακολουθεί να διασφαλίζεται η ακρίβεια της ψηφοφορίας. Για τη δημιουργία ενός έξυπνου συμβολαίου που θα συνδυάζει υποδομή εντός αλυσίδας (on-chain) με δεδομένα εκτός αλυσίδας (off-chain), θα πρέπει να δημιουργηθεί ένα υβριδικό έξυπνο συμβόλαιο. Ένα υβριδικό έξυπνο συμβόλαιο είναι μια εφαρμογή που αποτελείται από δύο μέρη:

1. έξυπνο συμβόλαιο—κώδικας που εκτελείται αποκλειστικά στο blockchain

2. αποκεντρωμένα δίκτυα Oracle—ασφαλείς υπηρεσίες εκτός αλυσίδας που υποστηρίζουν το έξυπνο συμβόλαιο

Τα δύο εξαρτήματα αλληλεπιδρούν μεταξύ τους με ασφάλεια για να σχηματίσουν μια ενιαία εφαρμογή. Το αποτέλεσμα είναι ο on-chain κώδικας που επαυξάνεται με διάφορους μοναδικούς και σημαντικούς τρόπους, ανοίγοντας πολλές νέες περιπτώσεις χρήσης που δεν θα ήταν δυνατές μόνο μέσω του on-chain κώδικα λόγω τεχνικών, νομικών ή οικονομικών περιορισμών.

Συμπερασματικά, τα Oracles που είδαμε προηγουμένως αποτελούν μια ιδανική λύση, και για το πρόβλημα κλήσης εξωτερικών APIs, που θα έδιναν στο σύστημα μας ένα παραπάνω στρώμα ασφαλείας, αλλά και για την αποθήκευση των ψήφων με ασφαλή τρόπο, χωρίς να χάνονται όλα τα προτερήματα που προσφέρει η τεχνολογία blockchain.

Τέλος, η πιο εύκολη μέθοδος απόκρυψης των ψήφων είναι η μέθοδος ανωνυμοποίησης στα έξυπνα συμβόλαια. Θα μπορούσε να χρησιμοποιηθεί η συνάρτηση κρυπτογράφησης των έξυπνων συμβολαίων **keccak256** για την ασφαλή κρυπτογράφηση των ψήφων.

Πιο συγκεκριμένα, η ψήφος του χρήστη θα καταγράφεται ως ένα bytes32 hashedVote. Η ψήφος αυτή ανωνυμοποιείται με την χρήση κρυπτογραφικών συναρτήσεων, όπως η keccak256. Η συνάρτηση vote ελέγχει εάν ο χρήστης έχει ήδη ψηφίσει και, αν όχι, καταγράφει την ψήφο του. Η συνάρτηση checkIfVoted επιστρέφει αν ο χρήστης έχει ήδη ψηφίσει και η συνάρτηση getVoteCount επιστρέφει τον αριθμό των ψήφων που επιλέχθηκαν για κάθε υποψήφιο. Επομένως, ο κώδικας του έξυπνου συμβολαίου για τη διαδικασία της ψηφοφορίας, θα μπορούσε να γίνει:

Κάθε ψήφος αποθηκεύεται στο mapping “voters“ με ένα hashed value, και όχι με το αρχικό. Το hashed value δημιουργείται από μια εξωτερική συνάρτηση της εφαρμογής και όχι εντός του συμβολαίου. Κατά την καταμέτρηση ψήφων γίνεται ένας έλεγχος αντιστοίχισης του hashed value του χρήστη με το ζητούμενο hashed value. Αυτός ο κώδικας μας δίνει μια γενική εικόνα για το τρόπο με τον οποίο θα μπορούσε να υλοποιηθεί. Ωστόσο μπορεί να υπάρξει πρόβλημα κατά τη

```
uint256 private candidateA;
uint256 private candidateB;
uint256 private candidateC;

struct Vote {
    bytes32 hashedVote;
    uint256 timestamp;
}

mapping(address => Vote) private voters;

function vote(bytes32 _hashedVote) public returns (bool) {
    require(voters[msg.sender].timestamp == 0);

    voters[msg.sender].hashedVote = _hashedVote;
    voters[msg.sender].timestamp = block.timestamp;

    return true;
}

function checkIfVoted() public view returns(bool) {
    return voters[msg.sender].timestamp != 0;
}

function getVoteCount(bytes32 _hashedVote) public view returns (uint256) {
    uint256 count = 0;
    for (uint256 i = 0; i < voters.length; i++) {
        if (voters[i].hashedVote == _hashedVote) {
            count++;
        }
    }
    return count;
}
```

Σχήμα 46. Ανώνυμη ψήφος

λήψη του πλήθους των εγγραφών από ένα mapping. Η χρήση πινάκων όμως, δεν είναι επιθυμητή καθώς θα μπορούσε να προκαλέσει overflow attacks.

Δυσκολία χρήσης

Η χρήση του Ethereum blockchain και του Metamask στην ψηφοφορία μπορεί να αποτελέσει την καλύτερη δυνατή λύση, καθώς προσφέρει μια δημόσια πλατφόρμα που είναι πιο εύκολη στη χρήση από οποιαδήποτε άλλη ηλεκτρονική ψηφοφορία.

Ένα από τα κύρια πλεονεκτήματα του Ethereum blockchain είναι η δημοσιότητα του. Αυτό σημαίνει ότι οποιοσδήποτε μπορεί να δει τις συναλλαγές που γίνονται στο δίκτυο, χωρίς να χρειάζεται να έχει πρόσβαση σε ειδικές άδειες ή συμβόλαια. Αυτό δίνει στους χρήστες την αίσθηση ότι η ψηφοφορία είναι διαφανής και δίκαιη.

Το Metamask είναι μια επέκταση του προγράμματος περιήγησης του διαδικτύου, που επιτρέπει στους χρήστες να συνδέονται με το δίκτυο του Ethereum blockchain. Είναι πολύ εύκολο στη χρήση και προσφέρει μια φιλική προς τον χρήστη διεπαφή που διευκολύνει τους χρήστες στη σύνδεσή τους με το δίκτυο του Ethereum blockchain και στην πραγματοποίηση ψηφοφορίας. Αυτό σε συνδυασμό με το ότι το Ethereum blockchain είναι ένα δημόσιο δίκτυο, που σημαίνει ότι οι χρήστες μπορούν να συνδεθούν και να χρησιμοποιήσουν το δίκτυο χωρίς να χρειάζεται να ζητήσουν άδεια ή να εγκριθούν από κάποιον διαχειριστή, καθιστά τη χρήση του Ethereum blockchain και του Metamask πολύ προσιτή και εύκολη για τους χρήστες, επιτρέποντάς τους να ψηφίζουν με άνεση και ασφάλεια από οποιαδήποτε συσκευή έχουν στη διάθεσή τους. Αυτό οφείλεται στο γεγονός, ότι το Ethereum είναι δημόσιο. Στην περίπτωση που γινόταν χρήση ενός ιδιωτικού blockchain, θα έπρεπε να πραγματοποιηθούν πολλές περισσότερες ενέργειες από τους πολίτες που θα ήταν προαπαιτούμενες για να τους επιτρέψουν τη ψηφοφορία.

Τέλος, επειδή το σύστημα αφορά εθνικές εκλογές, θα υπάρχει και αντίστοιχη βοήθεια, καθοδήγηση και τεχνική υποστήριξη από τις αρχές, προκειμένου να γίνει η διαδικασία της ψηφοφορίας εύκολη για όλους τους πολίτες ανεξαρτήτως του επιπέδου τεχνολογικής κατανόησης.

6.5 Εναλλακτικές μορφές ψηφοφορίας

Το υλοποιημένο σύστημα, ιδίως με τη χρήση των Oracles, θα μπορούσε να θεωρηθεί ιδανικό για εθνικές εκλογές. Ωστόσο, οι δυσκολίες και οι απαιτήσεις ενός τέτοιου συστήματος είναι υψηλές, καθώς αφορά πολύ μεγάλο εύρος κοινού. Η ευρύτερη εφαρμογή του συστήματός μας σε μικρού εύρους εκλογές, όπου συμμετέχει ένα μικρότερο κοινό, ανοίγει τον δρόμο για μια ευκολότερη υλοποίηση και ενσωμάτωση.

Μερικές μορφές ψηφοφορίας που θα μπορούσαν να επωφεληθούν από το σύστημα μας είναι:

- Ακαδημαϊκές ψηφοφορίες: Πανεπιστήμια θα μπορούσαν να χρησιμοποιήσουν το σύστημα μας, με σκοπό να πραγματοποιήσουν ότι είδους ακαδημαϊκών εκλογών απαιτηθεί. Παράλληλα η διαδικασία ταυτοποίησης θα γινόταν ευκολότερη, χωρίς να χρειαστεί να παρευρεθούν σε κάποια αρχή. Αντ'αυτού η εγγραφή στη λίστα, και η είσοδος τους στη πλατφόρμα θα μπορούσε να πραγματοποιηθεί με την είσοδο των ακαδημαϊκών τους στοιχείων. Η μόνη προεργασία που θα χρειαζόταν θα ήταν η δημιουργία λογαριασμού Metamask, για κάθε ψηφοφόρο.

- Εταιρικές ψηφοφορίες: Όμοια με τις ακαδημαϊκές, η υλοποίηση του συστήματος μας θα ήταν ευκολότερη, και πολύ πιο ασφαλής πραγματοποιώντας είσοδο με χρήση εταιρικών στοιχείων.

- Ψηφοφορία οργανώσεων / συλλόγων / κοινοτήτων: Η εφαρμογή του συστήματος για ένα μικρότερο κοινό γίνεται αυτομάτως πιο εύκολη και απλή σε σχέση με εκλογές μεγάλης κλίμακας, καθώς θα υπάρχει μεγαλύτερη ευκολία και ελαστικότητα στη διαχείριση, και λιγότερη σπατάλη πόρων που θα μπορούσαν να προκαλέσουν καθυστερήσεις στο Ethereum (μικρότερης σημασίας, καθώς χρησιμοποιείται καθημερινά από εκατομμύρια χρήστες).

Συνολικά, η εφαρμογή σε μικρότερα κοινά μπορεί να βελτιώσει την εμπειρία των ψηφοφόρων, να διευκολύνει τη διαδικασία ψηφοφορίας και να μειώσει τις πολυπλοκότητες που συνήθως σχετίζονται με εθνικές εκλογές, όπως η κρυπτογράφηση και αποθήκευση των ψήφων.

Βιβλιογραφικές Αναφορές

[Abd+21] Taha Abdelgalil, Vasileios Manolas, Leandros Maglaras, Ioanna Kantzavelou, and Mohamed Amine Ferrag. «Blockchain Technology: A Case Study in Supply Chain Management». In: *2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*. 2021, pp. 331–339. DOI: 10.1109/TPSISA52974.2021.00036.

[Agg+18] Sanchit Aggarwal et al. «Modern web-development using reactjs». In: *International Journal of Recent Research Aspects* 5.1 (2018), pp. 133–137.

[Ahn22] Byeongtae Ahn. «Implementation and Early Adoption of an Ethereum-Based Electronic Voting System for the Prevention of Fraudulent Voting». In: *Sustainability* 14.5 (2022), p. 2917.

[Ang+18] Stefano De Angelis, Leonardo Aniello, Roberto Baldoni, Federico Lombardi, Andrea Margheri, and Vladimiro Sassone. «PBFT vs proof-of-authority: applying the CAP theorem to permissioned blockchain». In: *Italian Conference on Cyber Security (06/02/18)*. Jan. 2018. URL: https://eprints.soton.ac.uk/415083/.

[Anw+22] Ch Anwar ul Hassan, Muhammad Hammad, Jawaid Iqbal, Saddam Hussain, Syed Sajid Ullah, Hussain AlSalman, Mogeeb AA Mosleh, and Muhammad Arif. «A Liquid Democracy Enabled Blockchain-Based Electronic Voting System». In: *Scientific Programming* 2022 (2022), pp. 1–10.

[AOB19] TP Abayomi-Zannu, IA Odun-Ayo, and TF Barka. «A proposed mobile voting framework utilizing blockchain technology and multi-factor authentication». In: *Journal of Physics: Conference Series*. Vol. 1378. 3. IOP Publishing. 2019, p. 032104.

[AS19] Spurthi Anjan and Johnson P Sequeira. «Blockchain based E-voting system for India using UIDAI's Aadhaar». In: *Journal of Computer Science Engineering and Software Testing* 5.3 (2019), pp. 26–32.

[AT13] Abdalla Al-Ameen and Samani A Talab. «The technical feasibility and security of e-voting.» In: *Int. Arab J. Inf. Technol.* 10.4 (2013), pp. 397–404.

[AWS-a] AWS. *Blockchain Technology*. Last accessed 6 January 2023. -. URL: https://aws.amazon.com/what-is/blockchain/.

[AWS-b] AWS. *What is Ethereum?* Last accessed 10 January 2023. -. URL: https://aws.amazon.com/blockchain/what-is-ethereum/.

[BA17] Baliga and Arati. «Understanding blockchain consensus models.» In: *Persistent* 4.1.1 (2017), pp. 4–7.

[BBJ18] Silvia Bartolucci, Pauline Bernat, and Daniel Joseph. «SHARVOT: secret SHARe-based VOTing on the blockchain». In: *Proceedings of the 1st international workshop on emerging trends in software engineering for blockchain*. 2018, pp. 30–34.

[Ben+14] Iddo Bentov, Charles Lee, Alex Mizrahi, and Meni Rosenfeld. «Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake [Extended Abstract]y». In: *SIGMETRICS Perform. Eval. Rev.* 42.3 (Dec. 2014), pp. 34–37. ISSN: 0163-5999. DOI: 10.1145/2695533.2695545. URL: https://doi.org/10.1145/2695533.2695545.

[Ben+22] Ali Benabdallah, Antoine Audras, Louis Coudert, Nour El Madhoun, and Mohamad Badra. «Analysis of blockchain solutions for e-voting: A systematic literature review». In: *IEEE Access* (2022).

[BG17] Vitalik Buterin and Virgil Griffith. «Casper the friendly finality gadget». In: *arXiv preprint arXiv:1710.09437* (2017).

[But+14] Vitalik Buterin et al. «A next-generation smart contract and decentralized application platform». In: *white paper* 3.37 (2014), pp. 2–1.

[Cha23] Vishal Chauhan. *What is Immutable Ledger in Blockchain and Its Benefits*. Last accessed 6 January 2023. 2023. URL: https://www.solulab.com/what-is-immutable-ledger-in-blockchain-and-its-benefits/.

[Cla+21] Nathan Clark, Leandros Maglaras, Ioanna Kantzavelou, Nestoras Chouliaras, and Mohamed Amine Ferrag. «Blockchain Technology: Security and Privacy Issues». In: *Blockchain Technology and Innovations in Business Processes*. Ed. by Srikanta Patnaik, Tao-Sheng Wang, Tao Shen, and Sushanta Kumar Panigrahi. Singapore: Springer Singapore, 2021, pp. 95–107. ISBN: 978-981-33-6470-7. DOI: 10.1007/978-981-33-6470-7_6. URL: https://doi.org/10.1007/978-981-33-6470-7_6.

[COI] COINTELEGRAPH. *What are DApps? Everything there is to know about decentralized applications*. Last accessed 11 January 2023. URL: https://cointelegraph.com/defi-101/what-are-dapps-everything-there-is-to-know-about-decentralized-applications.

[Coi] Cointelegraph. *A beginner's guide to the different types of blockchain networks*. Last accessed 7 January 2023. URL: https://cointelegraph.com/blockchain-for-beginners/a-beginners-guide-to-the-different-types-of-blockchain-networks.

[Dal21] Lyle Daly. «What Is Byzantine Fault Tolerance?» In: *The Motley Fool, November* 10 (2021).

[Dim+22] Vasileios Dimitriadis, Leandros Maglaras, Nineta Polemi, Ioanna Kantzavelou, and Nick Ayres. «Uncuffed: A Blockchain-Based Secure Messaging System». In: *Proceedings of the 25th Pan-Hellenic Conference on Informatics*. PCI '21. Volos, Greece: Association for Computing Machinery, 2022, pp. 340–345. ISBN: 9781450395557. DOI: 10.1145/3503823.3503886. URL: https://doi.org/10.1145/3503823.3503886.

[DW13] Christian Decker and Roger Wattenhofer. «Information propagation in the bitcoin network». In: *IEEE P2P 2013 Proceedings*. IEEE. 2013, pp. 1–10.

[DWB22] Sam Daley, Brennan Whitfield, and Omar Bheda. *Blocks in Blockchain Technology*. Aug. 31, 2022. URL: https://builtin.com/blockchain.

[Ehi+22] Piret Ehin, Mihkel Solvak, Jan Willemson, and Priit Vinkel. «Internet voting in Estonia 2005–2019: Evidence from eleven elections». In: *Government Information Quarterly* 39.4 (2022), p. 101718.

[Fra22a] Jake Frankenfield. «51% Attack: Definition, Who Is At Risk, Example, and Cost». In: *URL: https://www. investopedia. com/terms/1/51-attack. asp* (2022).

[Fra22b] Jake Frankenfield. *Decentralized Applications (dApps): Definition, Uses, Pros & Cons*. 2022.

[Ga16] Gervais and Arthur et al. «On the security and performance of proof of work blockchains.» In: *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security* (2016), pp. 3–10.

[Gar+19] Kanika Garg, Pavi Saraswat, Sachin Bisht, Sahil Kr Aggarwal, Sai Krishna Kothuri, and Sahil Gupta. «A comparitive analysis on e-voting system using blockchain». In: *2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*. IEEE. 2019, pp. 1–4.

[Gry21] Sergey Grybniak. *7 Ways Blockchain Will Impact Everyday Life in the Coming Decade*. Last accessed 11 January 2023. 2021. URL: https://blogs.sap.com/2021/03/23/7-ways-blockchain-will-impact-everyday-life-in-the-coming-decade/.

[Him22] Himanshi. *Byzantine Fault Tolerance (BFT) in Blockchain*. Last accessed 6 January 2023. 2022. URL: https://www.naukri.com/learning/articles/byzantine-fault-tolerance-in-blockchain/.

[Hjá+18] Friðrik Þ Hjálmarsson, Gunnlaugur K Hreiðarsson, Mohammad Hamdaqa, and Gísli Hjálmtỳsson. «Blockchain-based e-voting system». In: *2018 IEEE 11th international conference on cloud computing (CLOUD)*. IEEE. 2018, pp. 983–986.

[Hoo22] Parikshit Hooda. *practical Byzantine Fault Tolerance(pBFT)*. Last accessed 6 January 2023. 3Jul, 2022. URL: https://www.geeksforgeeks.org/practical-byzantine-fault-tolerancepbft/.

[Hua+21] Jun Huang, Debiao He, Mohammad S. Obaidat, Pandi Vijayakumar, Min Luo, and Kim-Kwang Raymond Choo. «The Application of the Blockchain Technology in Voting Systems: A Review». In: *ACM Comput. Surv.* 54.3 (Apr. 2021). ISSN: 0360-0300. DOI: 10.1145/3439725. URL: https://doi.org/10.1145/3439725.

[Iwu18] Victor Chidubem Iwuoha. «ICT and Elections in Nigeria: Rural Dynamics of Biometric Voting Technology Adoption». In: *Africa Spectrum* 53.3 (2018), pp. 89–113. DOI: 10.1177/000203971805300304. eprint: https://doi.org/10.1177/000203971805300304. URL: https://doi.org/10.1177/000203971805300304.

[JAS21] Uzma Jafar, Mohd Juzaiddin Ab Aziz, and Zarina Shukur. «Blockchain for electronic voting system—review and open research challenges». In: *Sensors* 21.17 (2021), p. 5874.

[Kho+18] David Khoury, Elie F Kfoury, Ali Kassem, and Hamza Harb. «Decentralized voting platform based on ethereum blockchain». In: *2018 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET)*. IEEE. 2018, pp. 1–6.

[KK22] Athanasios Kalogiratos and Ioanna Kantzavelou. *Blockchain Technology to Secure Bluetooth*. 2022. arXiv: 2211.06451 [cs.CR].

[Lep+20] Cristian Lepore, Michela Ceria, Andrea Visconti, Udai Pratap Rao, Kaushal Arvindbhai Shah, and Luca Zanolini. «A Survey on Blockchain Consensus with a Performance Comparison of PoW, PoS and Pure PoS». In: *Mathematics* 8.10 (2020). ISSN: 2227-7390. DOI: 10.3390/math8101782. URL: https://www.mdpi.com/2227-7390/8/10/1782.

[LSP19] Leslie Lamport, Robert Shostak, and Marshall Pease. «The Byzantine generals problem». In: *Concurrency: the works of leslie lamport*. 2019, pp. 203–226.

[Lyu+19] Jiazhuo Lyu, Zoe L Jiang, Xuan Wang, Zhenhao Nong, Man Ho Au, and Junbin Fang. «A secure decentralized trustless E-voting system based on smart contract». In: *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. IEEE. 2019, pp. 570–577.

[Mac21] Wahome Macharia. «Cryptographic Hash Functions». In: *mai. de* (2021).

[MSA19] Ahmed Afif Monrat, Olov Schelén, and Karl Andersson. «A survey of blockchain from the perspectives of applications, challenges, and opportunities». In: *IEEE Access* 7 (2019), pp. 117134–117151.

[muz22] muzammil. *Blockchain vs Cloud Computing Difference*. Last accessed 11 January 2023. 2022. URL: https://www.aalpha.net/articles/blockchain-vs-cloud-computing-difference/.

[Nak08] Satoshi Nakamoto. «Bitcoin: A peer-to-peer electronic cash system». In: *Decentralized business review* (2008).

[ngr22] ritesh nehru, rashi garg, and rinkiraghu2301. *Blockchain Hash Function*. Last accessed 6 January 2023. 13 Oct, 2022. URL: https://www.geeksforgeeks.org/blockchain-hash-function/.

[OOW19] O. Okediran, A. Sijuade A. O., and B. Wahab W. «Secure Electronic Voting Using a Hybrid Cryptosystem and Steganography». In: *Journal of Advances in Mathematics and Computer Science,* 34 (2019), pp. 1–26. URL: https://doi.org/10.9734/jamcs/2019/v34i1-230201.

[OP17] Xavier Ochoa and Enrique Peláez. «Affordable and secure electronic voting for university elections: the SAVE case study». In: *2017 Fourth International Conference on eDemocracy & eGovernment (ICEDEG)*. IEEE. 2017, pp. 110–117.

[ori23] originstamp. «How Blockchain Voting Systems Transform the Way We Vote». In: (2023).

[PA20] Deni Pramulia and Bayu Anggorojati. «Implementation and evaluation of blockchain based e-voting system with Ethereum and Metamask». In: *2020 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS)*. IEEE. 2020, pp. 18–23.

[Pap+18] Giuseppe Pappalardo, Tiziana Di Matteo, Guido Caldarelli, and Tomaso Aste. «Blockchain inefficiency in the bitcoin peers network». In: *EPJ Data Science* 7.1 (2018), pp. 1–13.

[Pap+23] Vasilis Papaspirou, Leandros Maglaras, Ioanna Kantzavelou, Naghmeh Moradpoor, and Sokratis Katsikas. *A Blockchain-based two Factor Honeytoken Authentication System*. 2023. arXiv: 2307.05047 [cs.CR].

[Par20] Arnis Parsovs. «Estonian electronic identity card: security flaws in key management». In: *Proceedings of the 29th USENIX Conference on Security Symposium*. 2020, pp. 1785–1802.

[RM20] Prateek Rawat and Archana N Mahajan. «ReactJS: A modern web development framework». In: *International Journal of Innovative Science and Research Technology* 5.11 (2020), pp. 698–702.

[RS20] TM Roopak and R Sumathi. «Electronic voting based on virtual id of aadhar using blockchain technology». In: *2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*. IEEE. 2020, pp. 71–75.

[S22] Ravikiran A S. *Merkle Tree in Blockchain: What is it, How does it work and Benefits*. Last accessed 15 January 2023. 2022. URL: https://www.simplilearn.com/tutorials/blockchain-tutorial/merkle-tree-in-blockchain.

[SDS18] Gautam Srivastava, Ashutosh Dhar Dwivedi, and Rajani Singh. «Crypto-democracy: A Decentralized Voting Scheme using Blockchain Technology.» In: *ICETE (2)*. 2018, pp. 674–679.

[Sha22] Toshendra Kumar Sharma. *Blockchain & Role Of P2P Network*. Last accessed 6 January 2023. September 1, 2022. URL: https://www.blockchain-council.org/blockchain/blockchain-role-of-p2p-network/.

[Shu+18] Shalini Shukla, AN Thasmiya, DO Shashank, and HR Mamatha. «Online voting application using ethereum blockchain». In: *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*. IEEE. 2018, pp. 873–880.

[SK23a] Achilleas Spanos and Ioanna Kantzavelou. *A Blockchain-based Electronic Voting System: EtherVote*. 2023. arXiv: 2307.10726 [cs.CR].

[SK23b] Achilleas Spanos and Ioanna Kantzavelou. «Poster: A Blockchain-based Electronic Voting System: EtherVote». In: *5th Summit on Gender Equality in Computing (GEC), Greek ACM-W Chapter Event*. GEC '23. Athens, Greece, June 2023.

[SY19] Mahendra Kumar Shrivas and Thomas Yeboah. «The disruptive blockchain: types, platforms and applications». In: *Texila International Journal of Academic Research* 2019 (2019), pp. 17–39.

[TT20] Ruhi Taş and Ömer Özgür Tanrıöver. «A systematic review of challenges and opportunities of blockchain for E-voting». In: *Symmetry* 12.8 (2020), p. 1328.

[VJR18] Dejan Vujičić, Dijana Jagodić, and Siniša Ranđić. «Blockchain technology, bitcoin, and Ethereum: A brief overview». In: *2018 17th international symposium infoteh-jahorina (infoteh)*. IEEE. 2018, pp. 1–6.

[VSB21] T Vairam, S Sarathambekai, and R Balaji. «Blockchain based voting system in local network». In: *2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS)*. Vol. 1. IEEE. 2021, pp. 363–366.

[WNT11] Peter Wolf, Rushdi Nackerdien, and Domenico Tuccinardi. *Introducing electronic voting: essential considerations*. International Institute for Democracy and Electoral Assistance …, 2011.

[WZ18] Maximilian Wohrer and Uwe Zdun. «Smart contracts: security patterns in the ethereum ecosystem and solidity». In: *2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*. IEEE. 2018, pp. 2–8.

[Yi19] Haibo Yi. «Securing e-voting based on blockchain in P2P network». In: *EURASIP Journal on Wireless Communications and Networking* 2019.1 (2019), pp. 1–9.

[Zha+18] Wenbin Zhang, Yuan Yuan, Yanyan Hu, Shaohua Huang, Shengjiao Cao, Anuj Chopra, and Sheng Huang. «A privacy-preserving voting protocol on blockchain». In: *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*. IEEE. 2018, pp. 401–408.

[Zha+19] Qixuan Zhang, Bowen Xu, Haotian Jing, and Zeyu Zheng. «Ques-chain: an ethereum based e-voting system». In: *arXiv preprint arXiv:1905.05041* (2019).

[Zhe+17] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang. «An overview of blockchain technology: Architecture, consensus, and future trends». In: *2017 IEEE international congress on big data (BigData congress)*. Ieee. 2017, pp. 557–564.