

Διπλωματική Εργασία

του φοιτητή του Τμήματος Ηλεκτρολόγων Μηχανικών και
Τεχνολογίας Υπολογιστών της Πολυτεχνικής Σχολής του
Πανεπιστημίου Πατρών

ΠΕΝΤΑΡΗΣ ΚΩΝΣΤΑΝΤΙΝΟΣ του ΓΕΩΡΓΙΟΥ

Αριθμός Μητρώου: 7110

Θέμα

Σύστημα ηλεκτρονικής ψηφοφορίας για φοιτητική συνέλευση:

Μελέτη περίπτωσης με βάση το Blockchain

Επιβλέπων

Κλεάνθης Θραμπουλίδης

Αριθμός Διπλωματικής Εργασίας:

Πάτρα, Οκτώβριος 2020

ΠΙΣΤΟΠΟΙΗΣΗ

Πιστοποιείται ότι η Διπλωματική Εργασία με θέμα

Σύστημα ηλεκτρονικής ψηφοφορίας για φοιτητική συνέλευση:

Μελέτη περίπτωσης με βάση το Blockchain

Του φοιτητή του Τμήματος Ηλεκτρολόγων Μηχανικών και
Τεχνολογίας Υπολογιστών

ΠΕΝΤΑΡΗ ΚΩΝΣΤΑΝΤΙΝΟΥ του ΓΕΩΡΓΙΟΥ

Αριθμός Μητρώου: 7110

Παρουσιάστηκε δημόσια και εξετάστηκε στο Τμήμα
Ηλεκτρολόγων Μηχανικών και Τεχνολογίας Υπολογιστών στις
...13.../...10.../...2020...

Ο Επιβλέπων

Ο Διευθυντής του Τομέα

Κλεάνθης Θραμπουλίδης,
Καθηγητής

Βασίλειος Παλιουράς,
Καθηγητής

Αριθμός Διπλωματικής Εργασίας:

Θέμα:

Σύστημα ηλεκτρονικής ψηφοφορίας για φοιτητική συνέλευση:

Μελέτη περίπτωσης με βάση το Blockchain

Φοιτητής:

Κωνσταντίνος Πένταρης
του Γεωργίου

Επιβλέπων:

Κλεάνθης Θραμπουλίδης

Περίληψη

Η εργασία αυτή έχει ως αντικείμενο τη μελέτη απομακρυσμένων ηλεκτρονικών συστημάτων ψηφοφορίας σε συνδυασμό με τεχνολογίες blockchain. Επιλέγεται ως case study το σύστημα ψηφοφορίας που εφαρμόζεται κατά τη φοιτητική συνέλευση και προτείνεται ένα blockchain πρωτόκολλο το οποίο καλύπτει τις ανάγκες αυτού ενώ επιπλέον βελτιώνει και κάποιες ελλείψεις του.

Στόχος ήταν η δημιουργία ενός πλήρως αποκεντροποιημένου συστήματος ψηφοφορίας το οποίο να μπορεί να λειτουργήσει απλώς με ένα δίκτυο blockchain κόμβων, χωρίς τρίτα, κεντρικά ελεγχόμενα συστήματα. Για τη δημιουργία του πρωτοκόλλου χρησιμοποιούνται κρυπτογραφικά εργαλεία όπως ψηφιακές υπογραφές για την ταυτοποίηση των ψηφοφόρων, ομομορφική κρυπτογραφία για την επίτευξη μυστικής ψήφου με δυνατότητα καταμέτρησης, ασφαλείς υπολογισμοί πολλαπλών μερών για την παραγωγή κατανεμημένων κλειδιών αποκρυπτογράφησης καθώς και μη διαδραστικές αποδείξεις μηδενικής γνώσης.

Επιπλέον, στα πλαίσια της εργασίας δημιουργήθηκε ένα proof of concept σύστημα το οποίο υλοποιεί το σχεδιασμένο κρυπτο-πρωτόκολλο ενώ βασίζεται στην τεχνολογία έξυπνων συμβολαίων του Ethereum blockchain για την υλοποίηση της υποδομής ενός αποκεντροποιημένου συστήματος ψηφοφορίας.

Abstract

The object of this study is the research of online electronic voting systems in combination with blockchain technology. The student assembly voting system is selected as a case study and a blockchain protocol is suggested that aims to not only fulfill the system requirements but improve upon them, covering some of its shortcomings.

The goal was the creation of a fully decentralized voting system able to operate using only the network of blockchain nodes, without third party, centrally controlled, oracle systems. For the creation of the protocol multiple cryptographic primitives are used such as digital signatures for voter authentication, homomorphic encryption for achieving ballot secrecy combined with the ability to tally them, secure multiparty computation for the generation of distributed decryption keys and non-interactive proofs of knowledge.

Additionally, within the scope of this work, a proof of concept system was created which implements the designed crypto-protocol whilst leveraging smart contract technology provided by the Ethereum blockchain for the voting system infrastructure of a decentralized voting system.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον καθηγητή και επιβλέποντα κ. Κλεάνθη Θραμπουλίδη για τη συμβολή του στην εκπόνηση της εργασίας αυτής και για την καθοδήγησή του καθ' όλη τη διάρκεια της έρευνας που έγινε.

Ευχαριστώ τη φίλη μου Γεωργία Φίλιου για τις συζητήσεις που κάναμε οι οποίες με βοήθησαν να βρω λύσεις σε διάφορα θέματα στο στάδιο του σχεδιασμού.

Ευχαριστώ το φίλο Παναγιώτη Κανέλλο για την επιμέλεια του κειμένου.

Τέλος θα ήθελα να ευχαριστήσω τους γονείς μου για τη συνεχή υποστήριξή τους κατά τη διάρκεια της ακαδημαϊκής και επαγγελματικής μου πορείας.

Ο συγγραφέας βεβαιώνει ότι δεν έχουν χρησιμοποιηθεί κείμενα, εικόνες και άλλο υλικό από κείμενα τρίτων χωρίς την παραπομπή στο αντίστοιχο πρωτότυπο κείμενο.

Περιεχόμενα

1. Εισαγωγή	1
1.1. Εισαγωγικό σημείωμα	1
1.2. Στόχος της εργασίας.....	1
1.3. Διάρθρωση εργασίας	3
2. Απομακρυσμένη ηλεκτρονική ψηφοφορία	4
2.1. Φοιτητική συνέλευση	4
2.2. Σύστημα ψηφοφορίας	4
2.2.1. Πλεονεκτήματα συστήματος	5
2.2.2. Αδυναμίες συστήματος	5
2.3. Αντίστοιχα συστήματα ψηφοφορίας.....	6
2.3.1. Φοιτητικές και άλλες εκλογές	6
2.3.2. Αδυναμίες συστημάτων εκλογών.....	7
2.4. Η παρέμβασή μας στο σύστημα ψηφοφορίας.....	8
2.4.1. Use cases συστήματος.....	8
2.4.2. User stories συστήματος	8
2.4.3. Περιγραφή αλλαγών στο υπάρχον σύστημα	9
2.4.4. Περιγραφή νέου συστήματος.....	10
2.4.5. Πλεονεκτήματα της νέας προσέγγισης	12
2.4.6. Τεχνικά χαρακτηριστικά νέου συστήματος.....	13
3. Σχετική εργασία.....	15
3.1. Κρατικά συστήματα internet voting	15
3.1.1. I-Voting System Εσθονίας	15
3.1.2. Νορβηγικό e-Voting System.	16
3.2. Ιδιωτικά συστήματα internet voting.....	16
3.2.1. Helios.....	16
3.2.2. Prêt à Voter	16
3.2.3. Voatz	16

3.2.4.	FollowMyVote	17
4.	Θεωρητικές έννοιες	18
4.1.	Τεχνολογία κατακευματισμένου καθολικού / Blockchain	18
4.1.1.	Τι είναι blockchain	18
4.1.2.	Στοιχεία ενός blockchain	19
4.1.3.	Λειτουργίες ενός blockchain.....	21
4.1.4.	Λογισμικό ενός Blockchain	26
4.2.	Μαθηματικό θεωρητικό υπόβαθρο κρυπτογραφίας.....	26
	Πρώτοι αριθμοί	27
	Πρώτοι προς αλλήλους	27
	Ασφαλείς πρώτοι αριθμοί.....	27
	Αριθμητική υπολοίπων (Modular arithmetic)	27
	Ισοδύναμοι modulo p αριθμοί (congruence).....	28
	Modular Πολλαπλασιαστικός αντίστροφος.....	28
	Modular διαίρεση.....	28
	Αφηρημένη άλγεβρα.....	29
	Ομάδες (Groups)	29
	Διακριτός λογάριθμος (Discrete Log / DL)	30
	Υπολογιστικό πρόβλημα Diffie-Hellman (CDH).....	30
	Πρόβλημα απόφασης Diffie-Hellman (DDH).....	30
	Πολυώνυμα Lagrange.....	31
4.3.	Κρυπτογραφία, κρυπτοσυστήματα και πρωτόκολλα	31
4.3.1.	Συστήματα κρυπτογράφησης.....	32
4.3.2.	Ομοιομορφική κρυπτογραφία.....	33
4.3.3.	Διαμοιρασμός μυστικών / Secret sharing	35
4.3.4.	Ασφαλής υπολογισμός πολλαπλών μερών (Secure multi-party computation).....	35
4.3.5.	Αποδείξεις Μηδενικής Γνώσης.....	37

4.3.6.	Συναρτήσεις κατακερματισμού (Hash function)	37
4.3.7.	Ψηφιακές υπογραφές.....	37
5.	Σχεδιασμός συστήματος ηλεκτρονικής ψηφοφορίας	39
5.1.	Πρωτόκολλο blockchain	39
5.2.	Τεχνική υλοποίηση	50
5.3.	Αριθμητικό παράδειγμα πρωτοκόλλου	62
6.	Case study - Σύστημα ηλεκτρονικής ψηφοφορίας για φοιτητική συνέλευση	67
6.1.	Γενικά	67
6.2.	Σκοπός συστήματος	67
6.3.	Παρουσίαση εφαρμογής	68
6.4.	Σενάριο χρήσης	78
6.5.	Τεχνολογίες που χρησιμοποιήθηκαν.....	79
6.5.1.	Ethereum blockchain και smart contract	80
6.5.2.	Χρήση βιβλιοθήκης UniCrypt.....	82
6.6.	Διαφορές με το σύστημα που παρουσιάστηκε στο 5ο κεφάλαιο	82
7.	Συμπεράσματα και περαιτέρω εργασία	84
7.1.	Γνώσεις που αποκτήθηκαν μέσω της εκπόνησης της εργασίας	84
7.2.	Τελικά συμπεράσματα	84
7.3.	Προτάσεις για περαιτέρω εργασία.....	86
8.	Βιβλιογραφία.....	88

1. Εισαγωγή

1.1. Εισαγωγικό σημείωμα

Τα συστήματα ψηφοφορίας ξεκινώντας από τη σύλληψή τους εδώ και χιλιάδες χρόνια, αποτελούν σήμερα ακρογωνιαίο λίθο της δημοκρατίας στις ανθρώπινες κοινωνίες ενώ θεωρούνται ο κατ' εξοχήν δίκαιος τρόπος λήψης αποφάσεων με τη συμμετοχή των ενδιαφερόμενων. Λόγω της παλαιότητάς τους και της εφαρμογής τους σε πολλές περιστάσεις, έχουν κατά καιρούς υλοποιηθεί με διάφορους τρόπους, ανάλογα πάντα με τις ανάγκες που έπρεπε να καλύψουν αλλά και τις δυνατότητες της εκάστοτε εποχής. Από τα συστήματα δημόσιας ψήφου με χειροτονία όπως της εκκλησίας του δήμου της αρχαίας Αθήνας, στα κρυφά συστήματα Αυστραλιανής ψηφοφορίας, έχουμε φτάσει στον 21ο αιώνα στα ψηφιακά συστήματα ψηφοφορίας με χρήση ηλεκτρονικών μηχανών ψήφου ενώ κινούμαστε προς την καθαρά ηλεκτρονική και κυρίως απομακρυσμένη ψηφοφορία μέσω Internet.

Η ηλεκτρονική και απομακρυσμένη ψηφοφορία είναι μια από τις πιο πολυσυζητημένες ιδέες της εποχής μας στον τομέα της τεχνολογίας πληροφορίας [1] και έχει διερευνηθεί διεξοδικά για πάνω από είκοσι χρόνια. Πολλά συστήματα έχουν προταθεί, προς το παρόν όμως κανένα δεν έχει γίνει αποδεκτό ως λύση του προβλήματος, κυρίως λόγω ανησυχιών όσον αφορά την ασφάλεια και τη διατήρηση της ακεραιότητας του συστήματος. Παρ' όλα αυτά οι προσπάθειες συνεχίζονται μέχρι και σήμερα, αξιοποιώντας συνεχώς τις εξελίξεις στον τομέα της κρυπτογραφίας και κατανεμημένων συστημάτων [2].

1.2. Στόχος της εργασίας

Στόχος της εργασίας είναι η μελέτη και εξοικείωση με τις τεχνολογίες και τεχνικές που χρησιμοποιούνται σε συστήματα απομακρυσμένης ηλεκτρονικής ψηφοφορίας καθώς και η μελέτη της τεχνολογίας blockchain και της αξιοποίησής της σε αυτά. Ταυτόχρονα, γίνεται και μία προσπάθεια σχεδιασμού και υλοποίησης ενός πρότυπου συστήματος το οποίο να μπορεί να χρησιμοποιηθεί στα πλαίσια μιας φοιτητικής συνέλευσης.

Βασικό κίνητρο της προσπάθειας αυτής αποτέλεσε η τρέχουσα διαδικασία ψηφοφορίας που εφαρμόζεται στις συνελεύσεις του φοιτητικού συλλόγου. Ως εσωτερικός αλλά και ως εξωτερικός παρατηρητής μπορεί κάποιος να εντοπίσει πολλά μειονεκτήματα και προβλήματα τα οποία όχι μόνο καθιστούν τη συμμετοχή των φοιτητών δυσκολότερη και κοπιαστική αλλά κάποιες φορές δρουν και ενάντια στον ίδιο το σκοπό της συνέλευσης υπονομεύοντας τον τρόπο λήψης αποφάσεων καθώς και την ακεραιότητα των αποτελεσμάτων.

Μελετώντας το πρόβλημα και πιθανούς τρόπους βελτιστοποίησης και αντιμετώπισης των μειονεκτημάτων της διαδικασίας ψηφοφορίας, έγινε σαφές πως πολλά από αυτά παρατηρούνται και στα υπόλοιπα συμβατικά συστήματα φυσικής ψηφοφορίας ενώ ανάλογα με

τη φύση αυτής εμφανίζονται και νέα προβλήματα που την καθιστούν άβολη, κοστοβόρα και χρονοβόρα. Λαμβάνοντας υπ' όψιν αυτή την πραγματικότητα, η μελέτη προσαρμόστηκε με στόχο τη διερεύνηση ενός εναλλακτικού συστήματος που θα μπορεί να καλύψει τις ανάγκες μιας οποιασδήποτε ψηφοφορίας με ίδια χαρακτηριστικά με αυτά των ψηφοφοριών φοιτητικών συνελεύσεων.

Τα βασικά κοινά προβλήματα των αντίστοιχων συστημάτων που εντοπίστηκαν είναι τα εξής:

- Είναι δύσχρηστα. Ο ψηφοφόρος πρέπει να παρευρεθεί σε κάποιο συγκεκριμένο χώρο πολλές φορές σε συγκεκριμένη στιγμή ώστε να υποβάλλει την ψήφο του.
- Είναι χρονοβόρα. Η όλη διαδικασία μαζί με τη μετακίνηση στο χώρο διεξαγωγής μπορεί να διαρκέσει μέχρι και ώρες ενώ σε περιπτώσεις όπως οι βουλευτικές εκλογές όπου είναι πιθανό τα εκλογικά δικαιώματα του ψηφοφόρου να είναι και σε άλλη πόλη απαιτείται ολόκληρο ταξίδι. Επιπλέον, χρονοβόρα είναι και η καταμέτρηση και η ανακοίνωση του αποτελέσματος η οποία μπορεί να διαρκέσει μέρες ανάλογα με το σκοπό που εξυπηρετεί η ψηφοφορία.
- Είναι κοστοβόρα. Εκτός από το πιθανό κόστος μετακίνησης για τους ψηφοφόρους, ψηφοφορίες εθνικών εκλογών χαρακτηρίζονται και από μεγάλο οργανωτικό κόστος το οποίο μεσοσταθμικά κυμαίνεται μεταξύ 1 έως και 3 \$ ανά ψηφοφόρο [3], χωρίς να υπολογίζεται το κόστος λόγω της διακοπής της παραγωγικότητας των εργαζομένων.
- Είναι ανασφαλή. Παρ' ότι έχουν παρθεί πολλά μέτρα για τη διασφάλιση της ακεραιότητας και της ορθότητας του αποτελέσματος, τα συστήματα αυτά συνεχίζουν να πάσχουν από προβλήματα ανθρώπινης φύσεως, είτε αυτά είναι λάθη είτε είναι εσκεμμένες πράξεις.

Εφαρμόζοντας ένα απομακρυσμένο, ηλεκτρονικό σύστημα ψηφοφορίας μπορούμε να μετριάσουμε, αν όχι να εξαλείψουμε, τα παραπάνω προβλήματα. Απαλλάσσεται ο ψηφοφόρος από την υποχρέωση να ψηφίσει σε συγκεκριμένο χώρο και χρόνο, η διοργάνωση της ψηφοφορίας απαιτεί ραγδαία λιγότερους πόρους ενώ διασφαλίζεται η σωστή διεξαγωγή της διαδικασίας και εφαρμογή των κανόνων χωρίς να μειώνεται η διαφάνεια του συστήματος. Μία τέτοια αλλαγή μπορεί ταυτόχρονα να βελτιώσει και τα υπόλοιπα μέρη της εκλογικής διαδικασίας μέρος της οποίας είναι η ψηφοφορία.

Το σύστημα βασίζεται στην καινοτόμα “τεχνολογία κατανεμημένου καθολικού” (distributed ledger technology - “DLT” ή γνωστό και ως Blockchain). Με αυτή ως πυρήνα δημιουργήθηκε ένα κρυπτο-πρωτόκολλο με χρήση αρχέγονων κρυπτογραφικών στοιχείων όπως *ομομορφική κρυπτογραφία*, *υπολογισμοί πολλαπλών μερών* και *αποδείξεις μηδενικής γνώσης*, ώστε να επιτευχθεί η δημιουργία ενός πλήρως αποκεντρωμένου και ασφαλούς συστήματος.

1.3. Διάρθρωση εργασίας

Κεφάλαιο 2: Απομακρυσμένη ηλεκτρονική ψηφοφορία

Γίνεται παρουσίαση του συστήματος φοιτητικών συνελεύσεων καθώς και του συστήματος φυσικής ψηφοφορίας που εφαρμόζεται σε αυτές. Επίσης παρουσιάζεται η παρέμβαση μας σε αυτό, τα χαρακτηριστικά της και η επίδρασή της στο υπάρχον σύστημα.

Κεφάλαιο 3: Σχετική εργασία

Μελετάται η σχετική εργασία που έχει γίνει πάνω σε εναλλακτικά συστήματα ψηφοφορίας καθώς και σε εφαρμογές αυτών και των αποτελεσμάτων που παρουσίασαν.

Κεφάλαιο 4: Θεωρητικό υπόβαθρο

Γίνεται αναδρομή θεωρητικών εννοιών που χρησιμοποιούνται για την κατασκευή του πρότυπου συστήματος ηλεκτρονικής ψηφοφορίας. Παρουσιάζεται η έννοια του Blockchain καθώς και διάφορων κρυπτογραφικών primitive αλλά και προχωρημένων τεχνικών και σχημάτων όπως multi-party computation και ομομορφικής κρυπτογραφίας.

Κεφάλαιο 5: Πρότυπο σύστημα ηλεκτρονικής ψηφοφορίας

Παρουσιάζεται ο σχεδιασμός αποκεντρωμένου ηλεκτρονικού συστήματος απομακρυσμένης ψηφοφορίας βασισμένο σε blockchain πρωτόκολλο το οποίο επιτρέπει τη μυστική αλλά και ταυτόχρονα ελέγξιμη ψηφοφορία.

Κεφάλαιο 6: Case study - Σύστημα ηλεκτρονικής ψηφοφορίας για φοιτητική συνέλευση

Παρουσιάζεται η πρότυπη υλοποίηση του προαναφερθέντος συστήματος, προσαρμοσμένο για μια εικονική ψηφοφορία στα πλαίσια φοιτητικής συνέλευσης.

Κεφάλαιο 7: Συμπεράσματα και περαιτέρω εργασία

Γίνεται ανάλυση των συμπερασμάτων που εξήχθησαν κατά την εκπόνηση της εργασίας αυτής καθώς και της μελλοντικής εργασίας που απαιτείται για την αντιμετώπιση αδυναμιών και ελλείψεων του προτεινόμενου συστήματος.

2. Απομακρυσμένη ηλεκτρονική ψηφοφορία

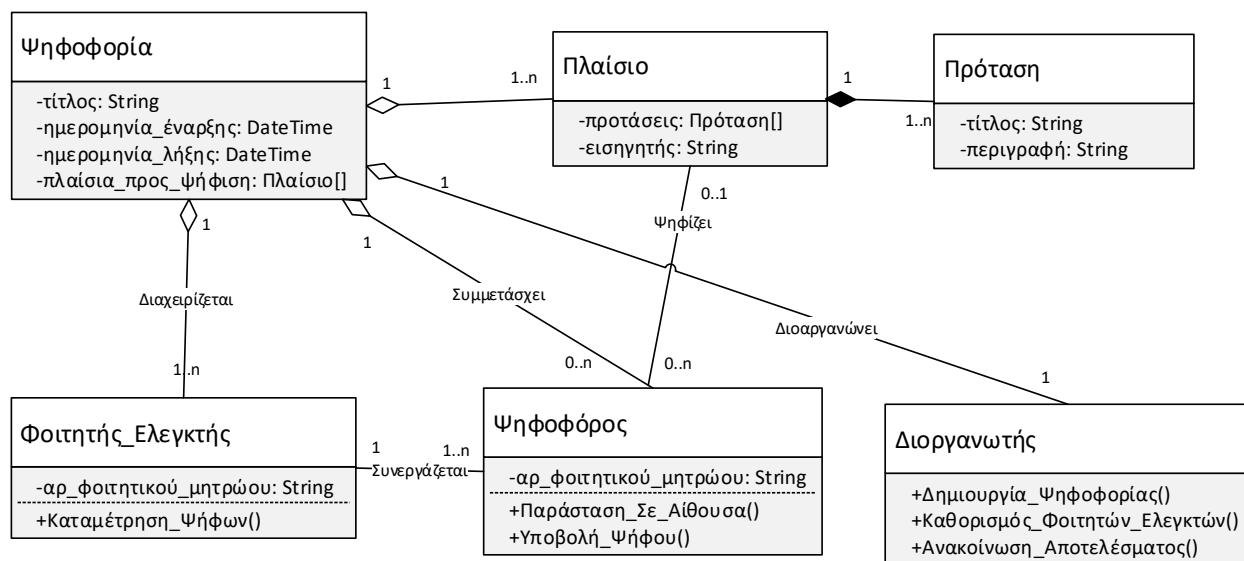
Όπως αναφέρθηκε και παραπάνω το σύστημα προς μελέτη είναι αυτό της ψηφοφορίας. Παρ' όλα αυτά κρίνεται σκόπιμο να γίνει μια εισαγωγή και στο ευρύτερο σύστημα στα πλαίσια του οποίου γίνεται ουσιαστικά χρήση ενός συστήματος ψηφοφορίας.

2.1. Φοιτητική συνέλευση

Στην παρούσα μορφή της, η φοιτητική συνέλευση επιτρέπει στους φοιτητές να αποφασίσουν από κοινού για την εκτέλεση ενός συνόλου δράσεων οι οποίες αφορούν θέματα που απασχολούν το σύλλογο. Όταν ληφθεί η απόφαση για τη διεξαγωγή συνέλευσης, ανακοινώνεται στους φοιτητές η ημερήσια διάταξη και η ημερομηνία και ώρα διεξαγωγής. Την ημέρα της συνέλευσης, συγκεντρώνονται τα μέλη του συλλόγου σε μια ελεύθερη αίθουσα του πανεπιστημίου και αν υπάρξει απαρτία, παρουσία πάνω από το 50% των φοιτητών του συλλόγου, η διαδικασία της συνέλευσης προχωράει. Γίνεται διαβούλευση πάνω στα ανακοινωθέντα θέματα ενώ εισηγητές παρουσιάζουν τις προτάσεις τους σχετικά με την αντιμετώπιση αυτών. Το σύνολο των προτάσεων κάθε εισηγητή ονομάζεται πλαίσιο και είναι αντικείμενο της ψηφοφορίας που ακολουθεί τη διαδικασία της διαβούλευσης. Το πλαίσιο που θα ψηφιστεί θεωρείται πως εκφράζει τη βούληση του συλλόγου και με την ανακοίνωσή του ξεκινούν οι διαδικασίες εφαρμογής των προτάσεων που περιέχει.

2.2. Σύστημα ψηφοφορίας

Με την ολοκλήρωση της συζήτησης και ανταλλαγής απόψεων, ο σύλλογος καλείται να επιλέξει ποιες προτάσεις θα ακολουθήσει. Η επιλογή γίνεται μέσω ανοιχτής ψηφοφορίας με χειροτονία και η καταμέτρηση γίνεται από συγκεκριμένους φοιτητές ελεγκτές, οι οποίοι συνήθως εκπροσωπούν τους εισηγητές προτάσεων. Στο σχήμα 1 φαίνεται το problem domain model της διαδικασίας. Συμμετοχή σε αυτήν έχουν μόνο οι φοιτητές που ανήκουν στο σύλλογο και είναι παρόντες στην αίθουσα κατά τη διεξαγωγή της. Κάθε φοιτητής έχει δικαίωμα να επιλέξει είτε ένα συγκεκριμένο πλαίσιο, είτε να ψηφίσει λευκό, είτε παρόν. Στην περίπτωση όπου το πρώτο σε ψήφους πλαίσιο δεν έχει μαζέψει αρκετές ψήφους ώστε να ξεπερνά το άθροισμα των ψήφων των υπόλοιπων πλαισίων συν του λευκού, τότε διεξάγεται δεύτερος γύρος ψηφοφορίας μεταξύ του πρώτου και του δεύτερου σε ψήφους πλαισίου. Οι διαθέσιμες επιλογές περιορίζονται είτε σε ένα από τα δύο πλαίσια είτε στο λευκό. Για να θεωρηθεί κάποιο πλαίσιο νικητήριο, θα πρέπει οι ψήφοι που έχει λάβει να ξεπερνούν το σύνολο των ψήφων που δόθηκαν στη δεύτερη επιλογή και στο λευκό. Στην περίπτωση που η προϋπόθεση αυτή δεν καλύπτεται, θεωρείται πως ο σύλλογος δεν έλαβε καμία απόφαση πάνω στα συζητηθέντα θέματα και καμία από τις προτεινόμενες δράσεις δεν προχωρά προς εκτέλεση.



Σχήμα 1: Problem domain model ψηφοφορίας φοιτητικής συνέλευσης

2.2.1. Πλεονεκτήματα συστήματος

- Ελέγχιμο αποτέλεσμα. Δηλώνοντας τις ψήφους σε φυσική μορφή και σε πραγματικό χρόνο μπροστά στο σύλλογο, μπορεί θεωρητικά ο οποιοσδήποτε να ελέγξει την εγκυρότητα της ψηφοφορίας. Σε περίπτωση διαμάχης για το αποτέλεσμα, μια απλή επανάληψη της καταμέτρησης από τους ίδιους ή και διαφορετικούς καταμετρητές λύνει το πρόβλημα σε ελάχιστο χρονικό διάστημα.
- Ευθύς τρόπος υποβολής ψήφου. Ο ψηφοφόρος δεν έχει παρά να σηκώσει το χέρι του τη στιγμή που καταμετρούνται οι ψήφοι για το πλαίσιο της αρεσκείας του.
- Διαδικασία ανεπηρέαστη από τρίτα συστήματα. Μηχανικές βλάβες συχνά λόγω αποτυχίας συστημάτων και συνεπώς μη περάτωσης της διαδικασίας που εξυπηρετούν. Η ψηφοφορία βασισμένη στη φυσική παρουσία έχει σχεδόν μηδενική εξάρτηση από τεχνολογίες, παρουσιάζοντας έτσι αντοχή στα προβλήματα που τις χαρακτηρίζουν.

2.2.2. Αδυναμίες συστήματος

Παρ' ότι η απαίτηση της φυσικής παρουσίας των φοιτητών προσφέρει διάφορα πλεονεκτήματα στο σύστημα της ψηφοφορίας συνέλευσης, το χαρακτηριστικό αυτό αποτελεί δυστυχώς και πηγή πολλών προβλημάτων λόγω της έλλειψης ελέγχου και της δυσκολίας διαχείρισης μεγάλων ομάδων σε ανοργάνωτο περιβάλλον, όπως αυτό της φοιτητικής συνέλευσης.

- Η διαδικασία της ψηφοφορίας είναι ανοιχτή με ανάταση χειρός και άμεση καταμέτρηση των ψήφων. Παρ' ότι η μέθοδος αυτή είναι βολική για την τωρινή μορφή της φοιτητικής συνέλευσης μιας και δεν απαιτεί έκδοση ψηφοδελτίων, κάλπες κλπ, έχει αποδειχθεί πως μπορεί να λειτουργήσει αντιδημοκρατικά. Σε πολλές περιπτώσεις κάποιος ψηφοφόρος έμμεσα αναγκάζεται να ψηφίσει κάποιο πλαίσιο με το οποίο δε συμφωνεί με σκοπό να

μην εκτεθεί σε φίλους, γνωστούς ή συναδέλφους με τους οποίους συνεργάζεται. Επιπλέον ο τρόπος με τον οποίο γίνεται η καταμέτρηση είναι επιρρεπής σε λάθη υπολογισμού για παράδειγμα είτε γιατί κάποιος ψηφοφόρος είναι εκτός του οπτικού πεδίου του καταμετρητή, είτε γιατί ψήφισε για περισσότερες από μια επιλογές και ο καταμετρητής δεν το έλαβε υπ' όψιν.

- Η φυσική παρουσία των φοιτητών είναι δύσκολα ελεγχόμενη. Κατά την ψηφοφορία δεν υπάρχει έλεγχος των ψηφοφόρων το οποίο επιτρέπει σε μη μέλη του συλλόγου να συμμετέχουν απλώς μπαίνοντας στην αίθουσα κατά τη συνέλευση. Επίσης υπάρχει η δυνατότητα αποκλεισμού φοιτητών από την ψηφοφορία για παράδειγμα κλειδώνοντας τις πόρτες πριν την έναρξη αυτής. Τέλος, είναι γνωστό πως λόγω των παραπάνω δυσκολιών, πολύ συχνά πραγματοποιούνται συνελεύσεις χωρίς να πληρούνται οι απαραίτητες συμμετοχές από τα μέλη του συλλόγου κάτι που καθιστά τα αποτελέσματα άκυρα, χωρίς όμως αυτό να τηρείται.
- Λόγω της απαίτησης φυσικής παρουσίας των φοιτητών, έχει επιλεχθεί οι συνελεύσεις να διεξάγονται σε χώρους του πανεπιστημίου τις καθημερινές και σε ώρες υπολογίζεται η προσέλευση να είναι εύκολη για την πλειονότητα του συλλόγου. Αυτό έχει ως αποτέλεσμα φοιτητές οι οποίοι αδυνατούν να παρευρεθούν στο πανεπιστήμιο την προκαθορισμένη χρονική περίοδο να χάνουν ουσιαστικά τη δυνατότητα ψήφου τους, κάτι το οποίο μπορεί να είναι και μόνιμο για φοιτητές οι οποίοι διαμένουν σε άλλες πόλεις. Επιπλέον ο χρόνος διεξαγωγής των συνελεύσεων επιλέγεται προς τη μέση της ημέρας το οποίο συχνά συνεπάγεται σε απώλεια μαθημάτων ή εργαστηρίων με αποτέλεσμα να διαταράσσεται το πρόγραμμα διδασκαλίας.
- Οι αίθουσες διεξαγωγής των συνελεύσεων πολλές φορές αδυνατούν να φιλοξενήσουν το σύνολο του συλλόγου, ειδικά σε τμήματα με μεγάλο αριθμό εισαχθέντων. Αυτό έχει ως αποτέλεσμα πολλοί φοιτητές να παραμένουν όρθιοι καθ' όλη τη διαδικασία της συνέλευσης η οποία μπορεί να διαρκέσει αρκετές ώρες. Αυτό, σε συνδυασμό με το κάπνισμα σε κλειστό χώρο, δημιουργούν δυσάρεστες συνθήκες σε βαθμό που πολλοί φοιτητές συνειδητά αποφασίζουν να τις αποφύγουν, θυσιάζοντας έτσι την ψήφο τους.

2.3. Αντίστοιχα συστήματα ψηφοφορίας

Παρόμοιο σύστημα ψηφοφορίας με το παραπάνω, συναντάμε και στην περίπτωση εκλογών όπως οι βουλευτικές, οι δημοτικές και πιο κοντά στη δική μας περίπτωση, οι φοιτητικές.

2.3.1. Φοιτητικές και άλλες εκλογές

Οι φοιτητικές εκλογές διεξάγονται μια φορά το χρόνο και έχουν ένα μοναδικό σκοπό, τον καθορισμό των μελών του διοικητικού συμβουλίου του φοιτητικού συλλόγου. Το ΔΣ όχι μόνο διοργανώνει τις φοιτητικές συνελεύσεις αλλά κυρίως εκπροσωπεί το σύλλογο στο διοικητικό σώμα της σχολής. Ο τρόπος εκλογής των μελών ΔΣ γίνεται μέσω αντίστοιχου συστήματος

ψηφοφορίας με αυτό που παρουσιάστηκε μερικές όμως κρίσιμες διαφορές. Η ψήφος είναι μυστική και κατατίθεται σε μορφή κλειστών ψηφοδελτίων σε κάλπη. Ο ψηφοφόρος έχει δικαίωμα να επιλέξει ένα από τα διαθέσιμα ψηφοδέλτια, αυτό της αντίστοιχης φοιτητικής ομάδας της αρεσκείας του ή λευκό. Η ψηφοφορία λαμβάνει μέρος όχι σε κάποιο χώρο του πανεπιστημίου αλλά σε κάποιο δημόσιο χώρο όπως κάποιο σχολικό κτήριο. Την οργάνωση και επίβλεψη της διαδικασίας αναλαμβάνουν φοιτητές εθελοντές οι οποίοι δρουν και ως εφορευτική επιτροπή. Τέλος, το αποτέλεσμα της ψηφοφορίας δεν είναι άμεσο, λόγω του ότι απαιτείται άνοιγμα και καταμέτρηση όλων των ψηφοδελτίων εντός της κάλπης, και συνήθως ανακοινώνεται την επόμενη ημέρα.

Σημειώνεται πως το σύστημα των φοιτητικών εκλογών αποτελεί μία μικρογραφία του συστήματος δημοτικών και βουλευτικών εκλογών που έχουμε στη χώρα μας. Στις βουλευτικές εκλογές για παράδειγμα, η διαδικασία είναι κατά μεγάλο βαθμό η ίδια σε μεγαλύτερη όμως κλίμακα. Δεσμεύονται δημόσιοι χώροι σε κάθε δήμο και μετατρέπονται σε προσωρινά εκλογικά κέντρα, καθήκοντα υποστήριξης και εφορευτικής επιτροπής αναλαμβάνουν πολίτες οι οποίοι επιλέγονται τυχαία, ενώ τα αποτελέσματα της καταμέτρησης ανακοινώνονται συνήθως μετά από 24 ώρες.

2.3.2. Αδυναμίες συστημάτων εκλογών

Όπως με το σύστημα ψηφοφορίας της φοιτητικής συνέλευσης, εντοπίζονται σημαντικές αδυναμίες και στα συστήματα ψηφοφορίας των εκλογών τα οποία είναι:

- Κοστοβόρα. Λόγω της φυσικής ψήφου, απαιτείται η διάθεση πολλών χώρων και σε πολλές περιοχές ώστε να υπάρχει βέλτιστη εξυπηρέτηση. Αυτό σημαίνει ότι θα πρέπει όλοι αυτοί οι χώροι να προετοιμαστούν κατάλληλα και να εφοδιαστούν με τον απαραίτητο εξοπλισμό (ψηφοδέλτια, κάλπες, γραφιστική ύλη). Χρειάζεται επίσης η επάνδρωσή τους με άτομα υπεύθυνα για τη σωστή διεξαγωγή της διαδικασίας, για τη διευκόλυνση και καθοδήγηση των ψηφοφόρων καθώς και για την καταμέτρηση των ψήφων στο κάθε εκλογικό κέντρο.
- Χρονικά και οικονομικά ασύμφορα. Με την έναρξη της περιόδου ψηφοφορίας, οι ψηφοφόροι αναγκάζονται να μετακινηθούν στους προκαθορισμένους χώρους με οποιοδήποτε μέσο τους είναι διαθέσιμο και να παραστούν αυτοπροσώπως σε συγκεκριμένο χρονικό διάστημα μέσα στη μέρα. Η διαδικασία της ψήφου αυτή καθαυτή διαρκεί 2 λεπτά όμως οι δευτερεύουσες διαδικασίες όπως η μετακίνηση στο χώρο και η αναμονή στην ουρά μπορεί να διαρκέσουν μέχρι και ώρες και να κοστίσουν αρκετά χρήματα ανάλογα με τη θέση του εκλογικού κέντρου στο οποίο δικαιούται να παραστεί ο κάθε ψηφοφόρος σε σχέση με τον τόπο κατοικίας του.
- Ανεσφαλή. Με τη λήξη της περιόδου ψηφοφορίας, αναλαμβάνουν την καταμέτρηση των ψήφων τα μέλη των εφορευτικών επιτροπών. Τα άτομα αυτά επιλέγονται τυχαία (ώστε το σύστημα να θεωρείται δίκαιο μιας και η συμμετοχή σε επιτροπή συνήθως

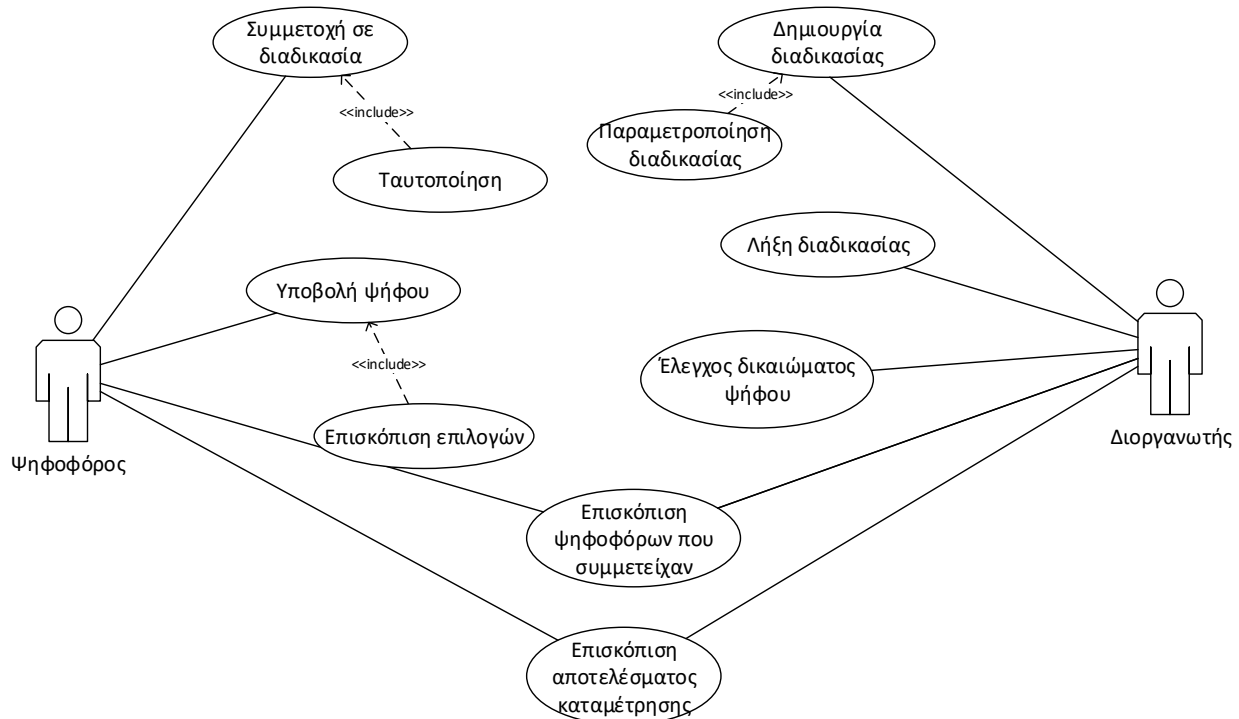
χαρακτηρίζεται ως αγγαρεία) χωρίς να έχουν ελεγχθεί από τη διοργανώτρια αρχή. Αυτό εισαγάγει στο σύστημα πιθανή ανασφάλεια που μπορεί να οδηγήσει σε αλλοίωση του αποτελέσματος μέσω παράνομης υποβολής ψήφων για ψηφοφόρους που δεν εμφανίστηκαν ή άλλου είδους επιρροή στην κάλπη [4].

2.4. Η παρέμβασή μας στο σύστημα ψηφοφορίας

Ο στόχος αυτής της εργασίας είναι η μελέτη, ο σχεδιασμός και η παρουσίαση μιας εναλλακτικής προσέγγισης που θα μπορούσε να αντιμετωπίσει τα προαναφερθέντα προβλήματα συστημάτων ψηφοφορίας αυτού του τύπου, διατηρώντας ταυτόχρονα τα πλεονεκτήματά τους.

2.4.1. Use cases συστήματος

Στη γενική του μορφή το σύστημα ψηφοφορίας έχει δύο τύπους χρηστών, το διοργανωτή και τον ψηφοφόρο με τα use cases που καταγράφονται στο σχήμα 2:



Σχήμα 2: Use case diagram συστήματος ψηφοφορίας

2.4.2. User stories συστήματος

Στο εναλλακτικό σύστημα ψηφοφορίας που προτείνεται, έχουμε εντοπίσει τα ακόλουθα user stories:

1. Ως ψηφοφόρος

- 1.1. Θέλω το σύστημα να είναι εύκολα και γρήγορα προσβάσιμο ανά πάσα στιγμή.
- 1.2. Θέλω να μπορώ να ταυτοποιήσω τον εαυτό μου με ασφάλεια.
- 1.3. Θέλω να μην μπορεί να με υποδυθεί ούτε να ψηφίσει κάποιος τρίτος εκ μέρους μου.
- 1.4. Θέλω να μπορώ να ψηφίζω όποτε το δικό μου πρόγραμμα το επιτρέπει.
- 1.5. Θέλω η ψήφος μου να είναι μυστική.
- 1.6. Θέλω να μπορώ να ελέγξω πως η ψήφος μου έχει υποβληθεί σωστά στο σύστημα.
- 1.7. Θέλω να μπορώ πιθανώς να αλλάξω την υποβεβλημένη ψήφο μου, εντός του χρονικού περιθωρίου της εκλογής.

2. Ως διοργανωτής

- 2.1. Θέλω να μπορώ να δημιουργώ ψηφοφορίες με παραμετροποιήσιμο όνομα, περίοδο, επιλογές και λίστα συμμετεχόντων.
- 2.2. Θέλω να μην επιτρέπεται η συμμετοχή σε χρήστες εκτός της προκαθορισμένης λίστας συμμετεχόντων.
- 2.3. Θέλω να μην επιτρέπεται η υποβολή ψήφου με επιλογή εκτός της προκαθορισμένης λίστας επιλογών.
- 2.4. Θέλω το μην επιτρέπεται η υποβολή ψήφου εκτός του προκαθορισμένου χρονικού διαστήματος.
- 2.5. Θέλω να επιτρέπεται μόνο μια ψήφος ανά ψηφοφόρο.

3. Ως χρήστης

- 3.1. Θέλω να μπορώ να ελέγξω πόσοι και ποιοι ψήφισαν.
- 3.2. Θέλω εγγύηση της επιβολής των κανόνων της ψηφοφορίας και αυτή να γίνεται χωρίς επίβλεψη.
- 3.3. Θέλω να μπορώ να έχω άμεση και γρήγορη επισκόπηση του αποτελέσματος των εκλογών χωρίς την πιθανότητα λάθους καταμέτρησης.

2.4.3. Περιγραφή αλλαγών στο υπάρχον σύστημα

Με την εφαρμογή της νέας πρότασης, το υπάρχον σύστημα αντικαθίσταται πλήρως. Επιγραμματικά οι αλλαγές είναι οι εξής:

- Δεν είναι απαραίτητη η φυσική παρουσία των ψηφοφόρων και η υποβολή ψήφου γίνεται ηλεκτρονικά μέσω κάποιας ψηφιακής εφαρμογής. Αυτό απευθείας σημαίνει πως δε χρειάζεται πια δέσμευση φυσικών χώρων και μετατροπή τους σε εκλογικά κέντρα.
- Αποφεύγεται η εκτύπωση ψηφοδελτίων εάν αυτή ήταν απαραίτητο. Οι υποψήφιος επιλογές αναγράφονται στην εφαρμογή ψηφοφορίας. Στην περίπτωση της ψηφοφορίας κατά τη φοιτητική συνέλευση γίνεται δυνατή η υποβολή κρυφής ψήφου σε πραγματικό χρόνο.
- Η ταυτοποίηση και ο έλεγχος του δικαιώματος ψήφου των ψηφοφόρων γίνεται ηλεκτρονικά, ενώ μπορεί να ελεγχθεί από όλους τους χρήστες του συστήματος, όχι μόνο από τους διαχειριστές.
- Ελεγκτικό προσωπικό δεν είναι πια απαραίτητο καθώς όλοι ψηφίζουν εξ αποστάσεως και η καταμέτρηση του αποτελέσματος γίνεται αυτόματα με ηλεκτρονικό τρόπο.
- Αλλάζει ο ρόλος της εφορευτικής επιτροπής η οποία δρα ως υπεύθυνη αρχή ψηφοφοριών ενώ καθήκον της είναι πια η διοργάνωση και παραμετροποίηση αυτών.

2.4.4. Περιγραφή νέου συστήματος

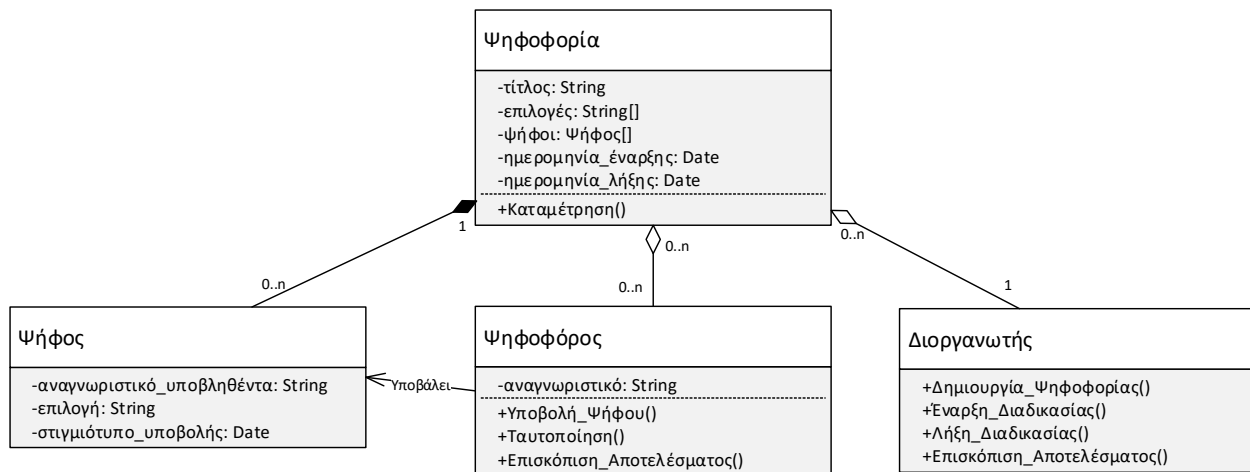
Η νέα υλοποίηση του συστήματος ψηφοφορίας βασίζεται σε μια ηλεκτρονική εφαρμογή η χρήση της οποίας απαιτεί απλώς μία οποιαδήποτε internet enabled συσκευή, όπως προσωπικό υπολογιστή, κινητό ή ακόμα και κάποιου είδους έξυπνο ρολόι. Η εφαρμογή είναι διαθέσιμη διαδικτυακά σε όλους τους ψηφοφόρους ενώ η υλοποίησή της είναι ανοιχτή (open source) και συνεπώς ελέγξιμη από οποιονδήποτε εξειδικευμένο χρήστη ή ερευνητή.

Οι χρήστες διοργανωτές έχουν τη δυνατότητα να δημιουργήσουν νέα ψηφίσματα παραμετροποιώντας τον τίτλο αυτών, τις διαθέσιμες επιλογές, τις ημερομηνίες έναρξης και λήξης καθώς και τους χρήστες με δυνατότητα συμμετοχής. Μπορούν να δημιουργηθούν πολλαπλά τέτοια ψηφίσματα ανά πάσα στιγμή, παραμένοντας πάντα πλήρως ανεξάρτητα μεταξύ τους.

Με τη δημιουργία του, ένα ψήφισμα επικοινωνείται στους χρήστες ψηφοφόρους οι οποίοι μπορούν ανά πάσα στιγμή, εντός πάντα των προκαθορισμένων περιόδων, να συμμετάσχουν υποβάλλοντας την ψήφο τους μέσω της ηλεκτρονικής εφαρμογής.

Με την περάτωση της ψηφοφορίας, ενεργοποιείται η αυτόματη καταμέτρηση των ψήφων δίνοντας έτσι τη δυνατότητα άμεσης επισκόπησης του αποτελέσματος σε όλους τους χρήστες.

Μετά το πέρας μιας ψηφοφορίας τα αποτελέσματα δεν χάνονται. Παραμένουν διαθέσιμα σε όλους τους χρήστες και διοργανωτές, δίνοντας έτσι τη δυνατότητα ελέγχου περασμένων ψηφοφοριών ακόμα και στο βαθύ μέλλον, χωρίς ιδιαίτερη κατανάλωση πόρων για τη συντήρηση των δεδομένων.



Σχήμα 3: E-Voting system problem domain model

Το νέο σύστημα έχει πιο απλοποιημένο μοντέλο που φαίνεται στο σχήμα 3 και διαθέτει τα εξής χαρακτηριστικά:

- Δυνατότητα προσαρμογής για αντίστοιχη εκλογική διαδικασία με την παραμετροποίηση επιλογών, καθορισμός χρονικής περιόδου, καθορισμός ψηφοφόρων (user story 2.1).
- Προσβασιμότητα, ανεξαρτήτως χώρου με μόνη προϋπόθεση την ύπαρξη διαδικτυακά συνδεδεμένης συσκευής (user story 1.1).
- Ασφαλή ταυτοποίηση χρήστη χωρίς την πιθανότητα να υποδυθεί το χρήστη κάποιος τρίτος (user stories 1.2, 1.3).
- Δυνατότητα υποβολής ψήφου ανεξαρτήτως χρονικής στιγμής, εντός πάντα της προκαθορισμένης χρονικής διάρκειας της ψηφοφορίας (user stories 1.4, 2.4).
- Απόκρυψη περιεχομένων ψήφου (user story 1.5).
- Δυνατότητα επισκόπησης περιεχομένων μόνο προσωπικής ψήφου (user story 1.6).
- Δυνατότητα υποβολής νέας ψήφου, εντός πάντα του χρονικού διαστήματος (user story 1.7).
- Δυνατότητα επισκόπησης ψηφοφόρων που συμμετείχαν στην ψηφοφορία (user story 3.1).
- Αυτόματη και σωστή επιβολή των κανόνων ψηφοφορίας (περιορισμός επιλογών και ψηφοφόρων, αριθμός ψήφων, υποβολή ψήφου εντός χρονικού περιθωρίου) (user stories 2.2, 2.3, 2.4, 2.5, 3.2).
- Άμεση και αυτόματη καταμέτρηση αποτελέσματος (user story 3.3).

Η διαδικασία έναρξης ψηφοφορίας, υποβολής ψήφου καθώς και καταμέτρησης του αποτελέσματος αποτελείται από τα εξής βήματα:

- Δημιουργία νέας ψηφοφορίας και απόδοση τίτλου αυτής.
- Καθορισμός λίστας διαθέσιμων επιλογών για το ψήφισμα.
- Καθορισμός ημερομηνίας ψηφίσματος.
- Δημοσίευση της νέας ψηφοφορίας και των παραμέτρων αυτής.
- Άνοιγμα εφαρμογής από τον ψηφοφόρο και προεπισκόπηση των διαθέσιμων επιλογών.
- Δημιουργία ψηφοδελτίου με βάση τις επιλογές του.
- Ταυτοποίηση ψηφοφόρου και υπογραφή ψηφοδελτίου.
- Δημοσίευση ψηφοδελτίου.
- Με το πέρας του χρονικού διαστήματος ψηφοφορίας, άθροισμα όλων των ψήφων και εξαγωγή του αποτελέσματος.

2.4.5. Πλεονεκτήματα της νέας προσέγγισης

Με τη νέα προσέγγιση ουσιαστικά αντιμετωπίζονται τα προβλήματα που έχουν προαναφερθεί στα υπάρχοντα συστήματα, βελτιώνοντάς τα και ταυτόχρονα επιτρέποντας τη χρήση τους σε μεγάλη κλίμακα.

- Όσον αφορά τα οικονομικά οφέλη, με το νέο απομακρυσμένο σύστημα μειώνεται δραματικά το κόστος οργάνωσης εκτέλεσης μιας διαδικασίας ψηφοφορίας. Δεν απαιτείται πια η δέσμευση και οργάνωση δημοσίων χώρων ούτε η παροχή εξοπλισμού (ψηφοδέλτια, γραφική ύλη, λίστες ψηφοφόρων κλπ). Οικονομικά οφέλη έχουν και οι ψηφοφόροι μιας και δεν απαιτείται πια να ταξιδέψουν και να παραστούν στο χώρο διεξαγωγής ο οποίος μπορεί να βρίσκεται μακριά από τον τόπο κατοικίας τους.
- Υπάρχουν επίσης χρονικά οφέλη. Οι ψηφοφόροι μπορούν να εκπληρώσουν τις εκλογικές τους υποχρεώσεις μέσα σε μερικά λεπτά. Επίσης, χωρίς την απαραίτητη φυσική παρουσία και ψήφο στις περιορισμένες κάλπες, αποφεύγεται το συγκεκριμένο bottleneck, παρέχοντας έτσι τη δυνατότητα σε ένα ιδανικό σενάριο να έχουμε εξαγωγή του αποτελέσματος μέσα σε μερικές ώρες αντί για μέρες. Χρονικά, ωφελείται επίσης και η διαδικασία οργάνωσης εκλογών μιας και αντί να απαιτείται η προετοιμασία και ο συγχρονισμός ολόκληρης της χώρας, χρειάζεται απλά ο συγχρονισμός της ηλεκτρονικής εφαρμογής με τις αντίστοιχες παραμέτρους ανάλογα το ψήφισμα.
- Η διαδικασία της ψήφου απλοποιείται και διευκολύνεται ραγδαία η εκτέλεσή της. Έχοντας απλά μία εφαρμογή η οποία μπορεί να χρησιμοποιηθεί από οποιαδήποτε από

τις βασικές ηλεκτρονικές συσκευές που είναι παρούσες σχεδόν σε όλα τα νοικοκυριά αυτή την εποχή, ο οποιοσδήποτε ψηφοφόρος μπορεί να συμμετάσχει με ευκολία και ελάχιστη ταλαιπωρία στις εκλογές, εκπληρώνοντας τις υποχρεώσεις του ανά πάσα στιγμή μέσα στη μέρα από την άνεση του σπιτιού του ή οποιουδήποτε χώρου τον εξυπηρετεί. Επίσης διευκολύνεται και το διαχειριστικό κομμάτι του εγχειρήματος. Ο κυβερνητικός μηχανισμός χρειάζεται απλά να ενημερώσει το πρωτόκολλο και τις παραμέτρους της εφαρμογής, κάτι το οποίο μπορεί να γίνει κεντρικά από μερικούς ανθρώπους και σε ελάχιστο χρόνο, σε αντίθεση με το τωρινό σύστημα το οποίο απαιτεί την αποστολή εκπροσώπων και εξοπλισμού καθώς και οργάνωση των χώρων και διαχείριση των εφόρων.

- Παρέχεται περισσότερη ασφάλεια με την αφαίρεση του ανθρώπινου παράγοντα και την αποκεντροποίηση της διαδικασίας, αυξάνοντας ακόμα περισσότερο την εμπιστοσύνη στο σύστημα. Βασίζοντας την απόκρυψη και καταμέτρηση της πληροφορίας σε μαθηματικούς αλγορίθμους και διαδικασίες αντί για φυσικά αντικείμενα και πρόσωπα, όπως οι κάλπες, οι φάκελοι και οι έφοροι, έχουμε εγγύηση για το αποτέλεσμα, εξαφανίζοντας την οποιαδήποτε αμφιβολία. Ταυτόχρονα, αποθηκεύοντας όλη την κρυπτογραφημένη πληροφορία σε ένα δημόσιο blockchain υπάρχει προστασία από αλλοίωση αυτής, είτε με τη μορφή άκυρων ψήφων είτε με την αφαίρεση έγκυρων.

2.4.6. Τεχνικά χαρακτηριστικά νέου συστήματος

Το νέο σύστημα εκμεταλλεύεται πλήρως τις ιδιότητες που προσφέρει μια blockchain υποδομή, οι οποία θα αναλυθεί στο κεφάλαιο 4.1. *Τεχνολογία κατανεμημένου καθολικού / Blockchain*. Η κατανεμημένη δομή των συστημάτων αυτών προσφέρει τεχνικά χαρακτηριστικά όπως:

- Αντοχή σε επιθέσεις καθώς και σε σενάρια καταστροφής (resilience).
- Αποκεντροποίηση και ανεξαρτητοποίηση από κεντρικούς παρόχους υπηρεσιών (decentralization).
- Διαθεσιμότητα χωρίς χωρικούς και χρονικούς περιορισμούς (availability).

Επιπλέον, η φύση του blockchain είναι τέτοια ώστε να παρέχει ανοσία σε αλλοίωση των δεδομένων (consistency). Τέλος, η ηλεκτρονική εφαρμογή ψηφοφορίας είναι απλοποιημένη σε μεγάλο βαθμό, απαιτώντας ελάχιστη συμμετοχή του χρήστη παρέχοντας έτσι ευκολία χρήσης (ease of use), ενώ εκμεταλλεύεται το blockchain χαρακτηριστικό της διαθεσιμότητας των δεδομένων για να πετύχει γρήγορη ανταπόκριση στην παραγωγή αποτελεσμάτων (responsiveness).

Όσον αφορά τη φοιτητική συνέλευση, η παρέμβαση ενός ηλεκτρονικού, απομακρυσμένου συστήματος ψηφοφορίας ανοίγει δρόμους για τη μοντερνοποίηση και κυρίως την εξυγίανση του υπάρχοντος συστήματος. Ταυτόχρονα η επιτυχής υιοθέτηση αυτού μπορεί να συνδυαστεί με τη δημιουργία μιας online πλατφόρμας η οποία θα φιλοξενήσει ολόκληρη τη διαδικασία της

φοιτητικής συνέλευσης. Παρουσίαση των πλαισίων θα γίνεται σε ηλεκτρονική μορφή και η διαβούλευση σε μορφή ερωτοαπαντήσεων σχετικά με τις προτάσεις των εισηγητών. Δίνεται έτσι η δυνατότητα να βελτιωθεί και η διαδικασία της συνέλευσης η οποία επίσης μαστίζεται από αντίστοιχα προβλήματα τα οποία πηγάζουν από τους περιορισμούς που θέτει ένα σύστημα βασισμένο σε φυσική παρουσία.

3. Σχετική εργασία

Με την έλευση του internet, ήταν φυσικό και επόμενο να γίνουν προσπάθειες εκμετάλλευσής του για τη διεξαγωγή καθαρά απομακρυσμένων ψηφοφοριών. Η δυνατότητα όχι της γρήγορης και ασφαλούς καταμέτρησης των ηλεκτρονικών ψήφων αλλά και το γεγονός ότι οι ψηφοφόροι δεν χρειάζεται να μετακινηθούν για να ψηφίσουν, κάνει τα online συστήματα ηλεκτρονικής ψηφοφορίας άκρως ελκυστικά.

Ένα από τα πρώτα συστήματα αμιγούς ηλεκτρονικής ψηφοφορίας προτάθηκε στις αρχές του 1980 από τον David Chaum [5], το οποίο βασιζόταν στην υποδομή Δημοσίου κλειδιού. Από τότε έχουν προταθεί, δημιουργηθεί και χρησιμοποιηθεί διάφορα συστήματα online ψηφοφορίας, μερικά από τα οποία θα παρουσιάσουμε παρακάτω.

3.1. Κρατικά συστήματα internet voting

Τα κρατικά συστήματα ψηφοφορίας που έχουν εφαρμοστεί κατά καιρούς έχουν δεχτεί πολλές κριτικές για την ασφάλεια που προσφέρουν σχετικά με τη μυστικότητα και την ακεραιότητα της ψήφου καθώς και με την αντοχή σε κυβερνοεπιθέσεις. Ένας σημαντικός παράγοντας για την κριτική αυτή είναι πως λόγω της υλοποίησης των συστημάτων από ιδιωτικές εταιρείες, ο πηγαίος κώδικας είναι συνήθως κρυφός και συνεπώς δεν μπορεί να ελεγχθεί από ειδήμονες του χώρου [6].

3.1.1. I-Voting System Εσθονίας

Η Εσθονία ήταν η πρώτη χώρα στην οποία οι πολίτες είχαν την δυνατότητα να ψηφίσουν ηλεκτρονικά με την χρήση του internet σε συνδυασμό με μια ηλεκτρονική κάρτα ταυτοποίησης (Identification Card - ID), που εκδόθηκε σε εθνικό εύρος από την κυβέρνηση. Η κάρτα έχει την δυνατότητα να δημιουργεί υπογραφές και χρησιμοποιείται πολύ εύκολα για αυθεντικοποίηση του χρήστη-ιδιοκτήτη, κρυπτογράφηση και ηλεκτρονική υπογραφή. Ο ψηφοφόρος πρέπει να κατεβάσει από την επιτροπή διενέργειας των εκλογών, σε ηλεκτρονική συσκευή την εφαρμογή ηλεκτρονικής ψηφοφορίας κάνοντας αυθεντικοποίηση με τη χρήση της ηλεκτρονικής του κάρτας. Εάν ο ψηφοφόρος έχει δικαίωμα ψήφου, εμφανίζεται μια λίστα με τις δυνατές επιλογές ψήφου. Η ψήφος κρυπτογραφείται με το Δημόσιο κλειδί της *εκλογικής επιτροπής* και υπογράφεται με το Ιδιωτικό κλειδί του ψηφοφόρου. Στη συνέχεια αποστέλλεται στο κεντρικό σύστημα συλλογής ψήφων που ελέγχεται από την εκλογική επιτροπή της κυβέρνησης. Εκεί ελέγχονται οι ψήφοι με το Δημόσιο κλειδί κάθε ψηφοφόρου και όλα τα αρχεία των ψήφων στη συνέχεια πηγαίνουν στο σύστημα ανοίγματος των “φακέλων ψηφοφορίας” που γίνεται η χρήση του Ιδιωτικού κλειδιού της επιτροπής. Αφού μαζευτούν όλες οι ψήφοι και αποκρυπτογραφηθούν, γίνεται η καταμέτρηση από το σύστημα και δημοσιοποιείται το αποτέλεσμα.

3.1.2. Νορβηγικό e-Voting System.

Εφαρμόστηκε για πρώτη φορά στις κοινοβουλευτικές εκλογές της 9^{ης} Σεπτεμβρίου του 2013. Το Project ξεκίνησε το 2008 και μια δοκιμή ευρείας κλίμακας έγινε στις τοπικές εκλογές του 2011. Το σύστημα αναπτύχθηκε από την εταιρεία ScytI Secure Electronic Voting SA. Το back-end του συστήματος είναι γραμμένο σε Java και ο «Voting client» τρέχει σε JavaScript σε browser του χρήστη-ψηφοφόρου. Μετά από έντονες κριτικές για την ασφάλεια του συστήματος από μια κυβερνοεπίθεση το σύστημα σταμάτησε να χρησιμοποιείται το 2014.

3.2. *Ιδιωτικά συστήματα internet voting*

3.2.1. Helios

Το Helios είναι ένα open source web based σύστημα ηλεκτρονικής ψηφοφορίας φτιαγμένο από τον Ben Adida. Η διαδικασία δημιουργίας ψήφων και καταμέτρησης αυτών είναι βασισμένη στο Simple Verifiable Voting Protocol του Benaloh [7] και χρησιμοποιεί ομομορφική κρυπτογραφία για τη διατήρηση της μυστικότητας της ψήφου. Μπορεί να χρησιμοποιηθεί από οποιονδήποτε αλλά απευθύνεται κυρίως σε χαμηλής σημασίας ψηφοφορίες με λίγους ψηφοφόρους, όπως φοιτητικές εκλογές. Υπάρχουν γνωστοί περιορισμοί σχετικά με την ασφάλεια και την ελεγχιμότητα του συστήματος ενώ έχουν κατά καιρούς βρεθεί και προβλήματα υλοποίησης τα οποία υπονομεύουν τη μυστικότητα της ψήφου.

3.2.2. Prêt à Voter

Το σύστημα Prêt à Voter, σχεδιάστηκε από τον Peter Ryan από το πανεπιστήμιο Λουξεμβούργου [8] και έχει εμπνευστεί από πρωτόκολλο του David Chaum. Είναι ένα πολύπλοκο σύστημα ψηφοφορίας το οποίο βασίζεται στη διαφάνεια όλων των διαδικασιών του για να εξασφαλίσει τη μυστικότητα της ψήφου, την εξαγορά ψήφου καθώς και την επιβεβαίωση καταμέτρησης της ψήφου στο τελικό αποτέλεσμα. Το σύστημα βασίζεται στη χρήση ενός Web Bulletin Board στο οποίο δημοσιοποιούνται όλα τα βήματα της διαδικασίας κάνοντάς τα έτσι ελέγξιμα από όλους τους συμμετέχοντες, ενώ η διαχείριση γίνεται από πολλά μέλη της εφορευτικής επιτροπής για να διασφαλιστεί η σωστή τήρηση των κανόνων. Παρ' ότι το σύστημα είχε αποδειχθεί ασφαλές και ανθεκτικό σε επιθέσεις, η ανάπτυξή του έχει σταματήσει από το 2014.

3.2.3. Voatz

Το Voatz είναι μια ιδιωτική πλατφόρμα για mobile voting φτιαγμένη από την εταιρεία Voatz, Inc. Βασίζεται σε τεχνολογία blockchain μέσω του Hyperledger για την αποθήκευση των ευαίσθητων πληροφοριών ταυτοποίησης των χρηστών. Η συντήρηση της αλυσίδας παρ' όλα αυτά δεν γίνεται από τους ίδιους τους χρήστες αλλά από 32 κατανεμημένα μηχανήματα που συντηρούν το καθένα το κοινό αντίγραφο της πληροφορίας, υπονομεύοντας έτσι σε μεγάλο βαθμό το δυνατότερο χαρακτηριστικό ενός blockchain. Η ταυτοποίηση του χρήστη γίνεται μέσω φωτογραφίας της ταυτότητας καθώς και μιας φωτογραφίας προσώπου η οποία συγκρίνεται

μέσω τεχνολογίας αναγνώρισης προσώπου με τη φωτογραφία που βρίσκεται στο blockchain. Ως ιδιωτική και κερδοσκοπική εφαρμογή, είναι κλειστού πηγαίου κώδικα το οποίο αποτελεί μεγάλο μέρος της κριτικής που έχει υποστεί κατά καιρούς μιας και δεν μπορεί να ελεγχθεί από ανεξάρτητους ειδήμονες του χώρου. Η εταιρεία Voatz υποστηρίζει πως η εφαρμογή της έχει περάσει από ελέγχους από πολλές ιδιωτικές εταιρείες αλλά δεν είναι ιδιαίτερα ανοιχτή με τα αποτελέσματα αυτών.

3.2.4. FollowMyVote

Το FollowMyVote είναι ένα open source project συντηρούμενο από μια ομάδα ανάπτυξης αλλά και από την ευρύτερη κοινότητα. Βασίζεται και αυτό σε blockchain υποδομή για την αποθήκευση των δεδομένων κάνοντάς το αρκετά ανθεκτικό σε επιθέσεις DDoS και γενικά σε επιθέσεις υποδομής σε αυτό το κομμάτι. Για την αυθεντικοποίηση και την μυστικότητα της ψήφου κάνει χρήση ενός πρωτοκόλλου βασισμένο σε κρυπτογραφία ελλειπτικών καμπυλών με τη χρήση δύο ξεχωριστών ζευγών Δημοσίου-Ιδιωτικού κλειδιού, ένα για την ταυτοποίηση του χρήστη και ένα για την κρυπτογράφηση της ψήφου του [9]. Το κυριότερο πρόβλημα που εντοπίζεται με τη συγκεκριμένη πλατφόρμα είναι πως για άλλη μια φορά γίνεται χρήση κεντρικών ελεγκτικών συστημάτων κατά τη διάρκεια της ψηφοφορίας (συγκεκριμένα ο ID Verifier και ο Registrar) τα οποία παρ' ότι δεν συντηρούν πληροφορία της ψηφοφορίας, είναι απαραίτητα για τη διεξαγωγή τους και βρίσκονται εκτός του blockchain συστήματος κάνοντάς τα στόχους επιθέσεων DoS.

4. Θεωρητικές έννοιες

4.1. Τεχνολογία κατανεμημένου καθολικού / Blockchain

4.1.1. Τι είναι blockchain

Στην πιο απλή του μορφή, ένα blockchain αποτελεί μια βάση δεδομένων. Η βασική λειτουργία του είναι η καταγραφή γεγονότων που ακολουθούν μια χρονική συνέχεια, ενώ η πληροφορία τους καθώς και η δομή αυτής υπάγονται σε κάποιους κανόνες, το λεγόμενο πρωτόκολλο. Η ειδοποιός διαφορά μεταξύ ενός blockchain και μίας κανονικής βάσης δεδομένων είναι πως στην περίπτωση του blockchain πρέπει να ακολουθούνται οι εξής κανόνες για την εισαγωγή δεδομένων [10] (Song, 2018):

- Δεν πρέπει να υπάρχει σύγκρουση με άλλα υπάρχοντα δεδομένα της βάσης (consistency).
- Δεδομένα μόνο προσαρτώνται, δεν αλλάζουν (immutability).
- Η κάθε καταχώρηση σχετίζεται και με ένα χρήστη (ownable).
- Όλοι οι χρήστες της βάσης συμφωνούν για την κατάσταση της βάσης χωρίς κεντρικούς φορείς/συστήματα (decentralized).

Με αυτό ως υπόβαθρο μπορούμε λοιπόν να χτίσουμε μια οποιαδήποτε εφαρμογή απαιτεί:

- Προστασία των δεδομένων από παράνομες τροποποιήσεις.
- Διαθεσιμότητα αυτών ανά πάσα στιγμή και από οποιοδήποτε σημείο.
- Διασφάλιση ότι τα καταγεγραμμένα γεγονότα δεν έχουν δημιουργηθεί τυχαία αλλά υπάγονται σε κάποιους προκαθορισμένους κανόνες.

Γενική περιγραφή λειτουργίας ενός blockchain

Η λειτουργία ενός συστήματος blockchain ακολουθεί τη λογική του ότι η γνώμη των πολλών αντικατοπτρίζει την πραγματικότητα. Για να το πετύχει αυτό βασίζεται σε μία αρχιτεκτονική όπου ο κάθε χρήστης/συμμετέχων στο σύστημα διατηρεί *τοπικά* μια προσωπική βάση δεδομένων στην οποία καταγράφει γεγονότα. Ένα γεγονός μπορεί να μοντελοποιεί οτιδήποτε, από μία συναλλαγή μεταξύ δύο χρηστών (αφαίρεση X μονάδων από το σύνολο χρήστη και πρόσθεση X μονάδων στο σύνολο του άλλου) έως τη θερμοκρασία τροφίμων εντός φορτηγού ψυγείου όπως καταγράφηκε σε ένα στιγμιότυπο από ένα IoT θερμόμετρο που βρίσκεται εντός του χώρου. Τα γεγονότα αυτά είτε έχουν δημιουργηθεί από τον ίδιο το χρήστη είτε έχει ενημερωθεί για τη δημιουργία τους από άλλους χρήστες.

Ο τύπος και η μορφή των γεγονότων που μπορούν να καταγραφούν δεν είναι αυθαίρετοι. Οι συμμετέχοντες έχουν αποδεχτεί ένα προαποφασισμένο σύνολο κανόνων που διέπουν το

σύστημα και κάθε γεγονός το οποίο είναι να καταγραφεί σε αυτό ως έγκυρο θα πρέπει να τους πληροί. Ο έλεγχος των κανόνων για κάθε γεγονός γίνεται τοπικά από κάθε χρήστη και ο ίδιος αποφασίζει αν αυτοί έχουν τηρηθεί και αν θα καταγράψει το γεγονός στην τοπική βάση δεδομένων του. Παρ' όλα αυτά, από τη στιγμή που όλοι οι χρήστες ακολουθούν τους ίδιους κανόνες και ενημερώνονται για όλα τα γεγονότα με τη σωστή χρονική σειρά εμφάνισής τους, τελικά θα καταλήξουν να έχουν την ίδια εικόνα γεγονότων στις τοπικές τους βάσεις. Συνεπώς, η εικόνα του συνόλου των γεγονότων που έχει ένας χρήστης τοπικά αντιστοιχεί και στην πραγματική εικόνα αυτών μιας και τη μοιράζονται όλοι οι χρήστες που συμμετέχουν στο σύστημα.

Η λειτουργία που παρουσιάστηκε, ταυτόχρονα αντιμετωπίζει και συμμετέχοντες οι οποίοι δεν ακολουθούν τους προαποφασισμένους κανόνες. Λόγω του ότι η βάση δεδομένων του κάθε χρήστη βρίσκεται τοπικά και ελέγχεται από μία εφαρμογή η οποία επίσης τρέχει τοπικά, δίνεται η δυνατότητα να εφαρμοστούν αυθαίρετες καταγραφές από ένα κακόβουλο χρήστη, ακυρώνοντας έτσι την αξιοπιστία των δεδομένων. Μεταδίδοντας ψευδή γεγονότα προς καταγραφή και στους υπόλοιπους χρήστες, κινδυνεύει να μολυνθεί το σύστημα από άκυρα γεγονότα. Το πρόβλημα αυτό αντιμετωπίζεται με τον ακόλουθο τρόπο. Οι ψευδείς πληροφορίες πιθανώς να αφομοιωθούν προσωρινά από έγκυρους χρήστες οι οποίοι θα αναπτύξουν μια ψευδή εικόνα της πραγματικότητας. Σε βάθος χρόνου όμως, αυτοί θα ενημερωθούν και από άλλους, πολύ περισσότερους από τους κακόβουλους χρήστες, για μία διαφορετική σειρά γεγονότων. Αυτομάτως θα αλλάξουν λοιπόν και τη δική τους οπτική, επιλέγοντας πάντα να ακολουθούν τη σειρά γεγονότων που ακολουθεί και η πλειοψηφία. Με αυτό τον τρόπο, οι αμφίβολοι συμμετέχοντες οι οποίοι προσπαθούν να ελέγξουν τα γεγονότα εξοστρακίζονται και ουσιαστικά αδυνατούν να συμμετέχουν στην των υπολοίπων παρά μόνο αν αποδεχτούν τη μορφή της βάσης που ακολουθούν αυτοί. Έχοντας ταυτόχρονα κίνητρο να συμμετέχουν στο σύστημα των πολλών, διακόπτουν τις προσπάθειες να ελέγξουν το σύστημα και συμμορφώνονται και αυτοί στους κανόνες του.

Βασιζόμενοι στην παραπάνω μέθοδο, καταλήγουμε λοιπόν σε μία βάση δεδομένων η οποία είναι αποκεντροποιημένη, δεν ανήκει σε κανέναν και ούτε μπορεί να επηρεαστεί από ένα υποσύνολο των χρηστών. Ταυτόχρονα λόγω της μορφής της, η οποία βασίζεται σε γεγονότα τα οποία παρουσιάζουν σταδιακές αλλαγές που έγιναν σε κάθε χρονικό στιγμιότυπο, παρέχει ολοκληρωμένο ιστορικό αυτών καθώς και δυνατότητες πλήρους ελέγχου (auditing).

4.1.2. Στοιχεία ενός blockchain

Γεγονός

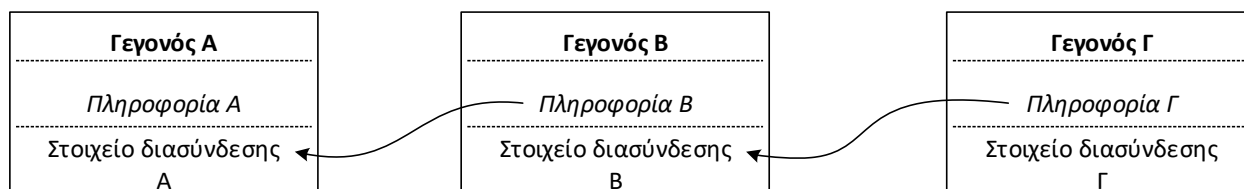
Το βασικό στοιχείο σε ένα blockchain είναι ένα γεγονός ή συμβάν. Το γεγονός μοντελοποιείται ως ένα πακέτο πληροφορίας το οποίο περιέχει στοιχεία όπως τον τύπο του συμβάντος, τα δεδομένα που χαρακτηρίζουν την αλλαγή που επιφέρει στο συνολικό σύστημα, το χρονικό στιγμιότυπο στο οποίο εκτελέστηκε, τους συμμετέχοντες σε αυτό καθώς και άλλες πληροφορίες

οι οποίες καθορίζονται από το πρωτόκολλο. Παίρνοντας ως παράδειγμα ένα blockchain στο οποίο καταγράφονται οικονομικές συναλλαγές, ένα γεγονός γεννιέται όταν “χρήματα” αλλάζουν χέρια. Συνεπώς, στο πακέτο πληροφορίας αυτού καταγράφεται το ποσό της συναλλαγής, ο χρήστης από τον οποίο αφαιρέθηκε αυτό, ο χρήστης στον οποίο προστέθηκε καθώς και το ακριβές χρονικό στιγμιότυπο της εκτέλεσης αυτού.

Αλυσίδα γεγονότων

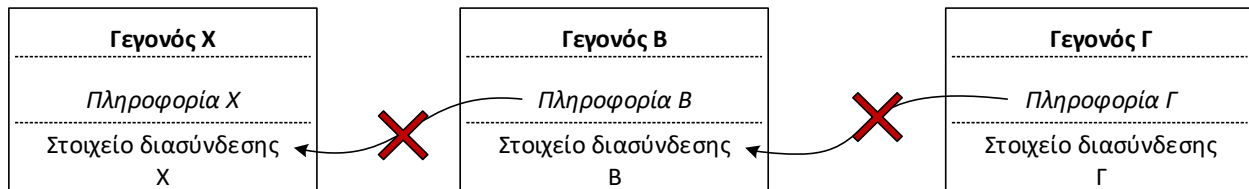
Ο πυρήνας ενός blockchain συστήματος είναι η αλυσίδα γεγονότων. Στην ουσία η αλυσίδα είναι η βάση δεδομένων του συστήματος. Περιέχει όλα τα γεγονότα που έχουν καταγραφεί από τη γέννηση του συστήματος. Κάθε καινούργιο γεγονός που εκτελείται, αφού διαδοθεί στους κόμβους που συμμετέχουν στο σύστημα, καταγράφεται από αυτούς και προστίθεται στην αλυσίδα τους σαν ο επόμενος «κρίκος» αυτής. Η αλυσιδωτή διασύνδεση των γεγονότων είναι το σημαντικότερο κομμάτι του συστήματος διότι είναι αυτή που προστατεύει ένα blockchain σύστημα από αλλοίωση της πληροφορίας του. Ο τρόπος με τον οποίο είναι συνδεδεμένοι οι κρίκοι αυτού είναι πάντα τέτοιος ώστε να καθιστά αδύνατη τη μετατροπή παρελθοντικών γεγονότων χωρίς να καταστραφούν όλα τα μετέπειτα γεγονότα. Με αυτό τον τρόπο, κάποιος “επιτιθέμενος” στο σύστημα δεν μπορεί να μεταδώσει ψευδή πληροφορία για κάποιο γεγονός που επιθυμεί να αλλοιώσει και από την άλλη δεν μπορεί να αλλοιώσει όλη την αλυσίδα γιατί, όπως εξηγήθηκε προηγουμένως, η πλειοψηφία θα τον απορρίψει.

Θεωρώντας την αλυσίδα του σχήματος 4, τρία διαδοχικά γεγονότα συνδέονται μεταξύ τους μέσω στοιχείων διασύνδεσης.



Σχήμα 4: Αλυσίδα γεγονότων

Κάθε στοιχείο διασύνδεσης είναι τέτοιο ώστε να εξαρτάται από την *πληροφορία* του γεγονότος. Συνεπώς μετατροπή αυτής συνεπάγεται και μετατροπή του στοιχείου διασύνδεσης. Επιπλέον, η πληροφορία κάθε γεγονότος περιέχει και το στοιχείο διασύνδεσης του προηγούμενου κρίκου της αλυσίδας όπως φαίνεται στο σχήμα. Στην περίπτωση προσπάθειας αλλοίωσης της αλυσίδας με στόχο την αλλαγή της πληροφορίας του γεγονότος Α, τότε απ’ ευθείας θα έχουμε και αλλαγή του στοιχείου διασύνδεσης Α. Αυτό θα έχει ως αποτέλεσμα η πληροφορία Β να αποσυνδεθεί από το προηγούμενο γεγονός, καθιστώντας άκυρο ολόκληρο το γεγονός Β. Αλυσιδωτά, καθίσταται άκυρο και το γεγονός Γ καθώς και όλα τα μετέπειτα γεγονότα.



Σχήμα 5: Αλλοιωμένη αλυσίδα γεγονότων

Κόμβοι συστήματος

Ως κόμβοι του συστήματος ορίζονται τα υπολογιστικά μηχανήματα που τρέχουν την εφαρμογή διαχείρισης και συμμετοχής στο blockchain και ταυτόχρονα συντηρούν και την αλυσίδα γεγονότων καταγράφοντάς την σε τοπικό αποθηκευτικό χώρο. Η διαδικασία συντήρησης της αλυσίδας περιλαμβάνει τον έλεγχο εγκυρότητας των καταγεγραμμένων γεγονότων και την επικύρωση νέων γεγονότων προς καταγραφή, έννοιες οι οποίες θα εξηγηθούν σε επόμενη ενότητα.

Η επικοινωνία μεταξύ των κόμβων βασίζεται στις υποδομές του σημερινού διαδικτύου (internet). Είναι σημαντικό χαρακτηριστικό, κυρίως διότι βασίζεται σε ανοιχτά πρωτόκολλα επικοινωνίας, δοκιμασμένα και υλοποιημένα από πολλούς παρόχους λογισμικού. Η επικοινωνία μπορεί να γίνει με ασφάλεια (από π.χ. man-in-the-middle attack) μέσω πρωτοκόλλων όπως το TLS και ανώνυμα μέσω δικτύου Tor.

4.1.3. Λειτουργίες ενός blockchain

Σύνδεση στο σύστημα

Όταν ένας νέος κόμβος συνδέεται για πρώτη φορά στο σύστημα δεν γνωρίζει τις διευθύνσεις άλλων συμμετεχόντων (peers). Σε αυτή την περίπτωση επικοινωνεί είτε με κάποιους γνωστούς και σταθερούς κόμβους η διεύθυνση των οποίων είναι στατικά εγγεγραμμένη στον κώδικα του συστήματος (hardcoded) είτε εκτελεί κάποιου είδους DNS ερώτημα το οποίο αντίστοιχα τον ενημερώνει για τις IP υπαρχόντων κόμβων.

Αφού ξεκινήσει την επικοινωνία έστω και με έναν από αυτούς, μπορεί να αρχίσει να ενημερώνεται από αυτόν για τις IP διευθύνσεις άλλων γνωστών του κόμβων. Όλες οι γνωστές διευθύνσεις με τις οποίες καταφέρνει να επικοινωνήσει καταγράφονται για περαιτέρω χρήση καθώς και για επόμενες επανασυνδέσεις.

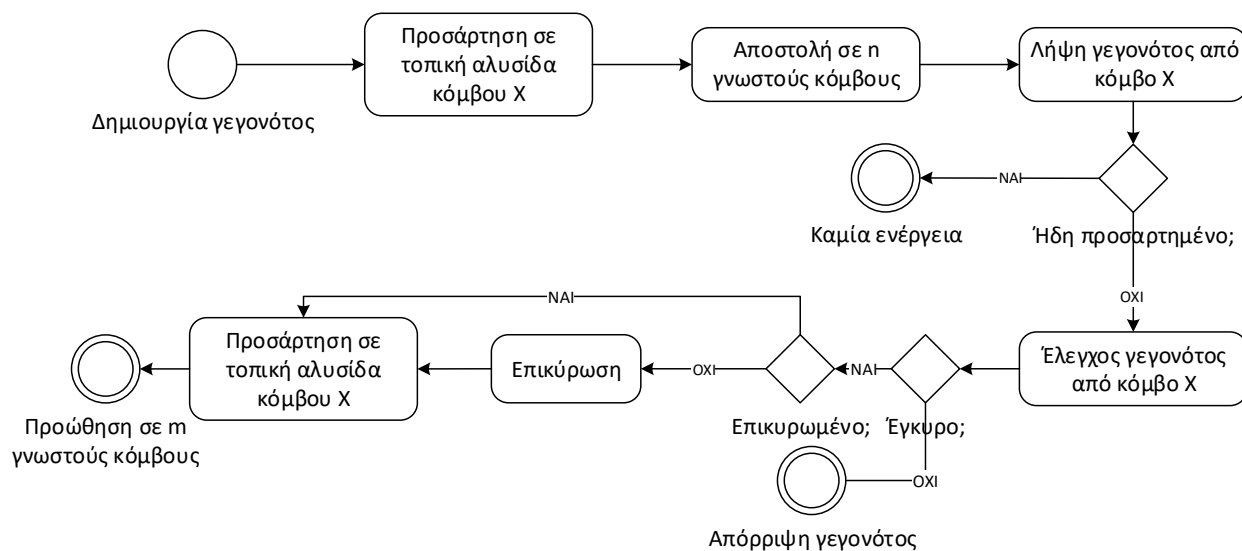
Λήψη δεδομένων αλυσίδας

Με την επιτυχή σύνδεση στο P2P δίκτυο, ξεκινάει η αρχικοποίηση του συστήματος και η λήψη των ήδη υπαρχόντων δεδομένων της αλυσίδας από τους υπόλοιπους κόμβους. Τα γεγονότα που καταφθάνουν, σώζονται τοπικά σε σκληρό δίσκο ή αντίστοιχο μόνιμο αποθηκευτικό χώρο. Με την ολοκλήρωση της λήψης της αλυσίδας ο νέος κόμβος εκτελεί μια διαδικασία ελέγχου των γεγονότων που έλαβε, ελέγχει ουσιαστικά αν πληρούνται οι κανόνες του πρωτοκόλλου του

[illegible]

Πηγή: https://en.bitcoin.it/wiki/Block_chain (CC By 3.0)

Η εκτέλεση κάποιας πράξης σε blockchain συστήματα ισοδυναμεί στην δημιουργία και προσάρτηση ενός γεγονότος στην αλυσίδα. Η δομή αυτού είναι προκαθορισμένη και βασίζεται στους κανόνες που περιγράφει το πρωτόκολλο του συστήματος. Για να θεωρηθεί πως ένα γεγονός έχει εισαχθεί πρέπει να ακολουθηθεί η διαδικασία του σχήματος 7. Δεν αρκεί να έχει προσαρτιστεί απλώς στην τοπική αλυσίδα του χρήστη δημιουργού αλλά πρέπει να διαδοθεί και στην πλειονότητα των κόμβων που συμμετέχουν στο σύστημα, να ελεγχθεί, πιθανώς να επικυρωθεί και να προστεθεί και στις δικές τους αλυσίδες. Η διάδοση αυτού γίνεται μέσω του δικτύου επικοινωνίας P2P μεταξύ κόμβων. Το μήνυμα δημιουργίας γεγονότος, μαζί με το πακέτο πληροφορίας που περιέχει τα στοιχεία του, επικοινωνείται από το δημιουργό σε όλους τους γνωστούς σε αυτόν συμμετέχοντες κόμβους οι οποίοι με τη σειρά τους το στέλνουν σε δικούς τους γνωστούς, διαδίδοντας έτσι το μήνυμα σε ολόκληρο το σύστημα.



22

Έλεγχος εγκυρότητας γεγονότος

Κάθε γεγονός το οποίο είναι να προστεθεί στην αλυσίδα, ελέγχεται ως προς την εγκυρότητά του με βάση τους κανόνες που διέπουν το blockchain σύστημα. Παίρνοντας πάλι το παράδειγμα της αλυσίδας χρηματικών συναλλαγών, όλοι οι συμμετέχοντες που ενημερώνονται για ένα γεγονός συναλλαγής, πριν το αποδεχτούν ως έγκυρο ελέγχουν τα εξής:

- Αν με βάση και όλα τα προηγούμενα γεγονότα, ο χρήστης από τον οποίο αφαιρέθηκε το ποσό, είχε ένα σύνολο χρημάτων ίσο ή μεγαλύτερο του αναγραφόμενου ποσού.
- Αν η συναλλαγή έχει όντως εκτελεστεί από το χρήστη ο οποίος δρα ως πληρωτής. Ο σκοπός είναι να αποφευχθούν κακόβουλες συναλλαγές οι οποίες δεν έχουν εκκινηθεί από χρήστες των οποίων ο λογαριασμός δρα ως η πηγή κατά την αποστολή.

Αν οποιοσδήποτε από τους παραπάνω ελέγχους αποτυγχάνει τότε η συναλλαγή είναι άκυρη διότι είτε εκτελέστηκε με μη υπάρχοντα χρήματα είτε δεν εκτελέστηκε από τον κάτοχο αυτών. Οι συμμετέχοντες την απορρίπτουν και δεν την καταγράφουν στις προσωπικές τους αλυσίδες καθιστώντας την εκτέλεσή της άκυρη, διασφαλίζοντας έτσι την αξιοπιστία του συστήματος.

Μηχανισμός ομοφωνίας (Consensus mechanism)

Κάθε γεγονός που είναι να εισαχθεί στην αλυσίδα πρέπει να περάσει από μία διαδικασία επικύρωσης, σκοπός της οποίας είναι ο νέος κρίκος να συνδεθεί με τέτοιο τρόπο ώστε να διατηρηθεί το χαρακτηριστικό αντοχής στην αλλοίωση πληροφορίας. Ως αλλοίωση της πληροφορίας ορίζεται η δημιουργία νέας διακλάδωσης της αλυσίδας, ξεκινώντας από κάποιο παλαιότερο γεγονός, με στόχο τη δημιουργία μιας νέας εικόνας της πραγματικότητας η οποία ευνοεί έναν κακόβουλο χρήστη. Παράδειγμα τέτοιας αλλοίωσης στην περίπτωση του blockchain συστήματος πληρωμών είναι η αποστολή χρημάτων και στη συνέχεια η διαγραφή της αποστολής αυτής, δημιουργώντας μια νέα διακλάδωση σε κάποιο σημείο πριν το γεγονός αποστολής.

Η διαδικασία επικύρωσης γεγονότος μπορεί και έχει υλοποιηθεί με διάφορους τρόπους οι οποίοι όμως εξυπηρετούν ένα συγκεκριμένο σκοπό. Την παραγωγή ενός στοιχείου το οποίο να συνδέει το τελευταίο γεγονός της αλυσίδας μαζί με το καινούριο. Ο τρόπος εύρεσης του στοιχείου αυτού πρέπει να πληροί τα εξής χαρακτηριστικά:

- Να δέχεται πολλαπλές εισόδους, ο συνδυασμός των οποίων να μεταφράζεται σε μια έξοδο. Αλλοίωση οποιασδήποτε εισόδου θα πρέπει να παράγει μια τελείως διαφορετική έξοδο.
- Να είναι δύσκολη ή χρονοβόρα για ένα χρήστη. Για τη σωστή λειτουργία του συστήματος, είναι απαραίτητο ο χρόνος που χρειάζεται κάποιος χρήστης μόνος του να δημιουργήσει το στοιχείο διασύνδεσης των γεγονότων να είναι πολλαπλάσιος του χρόνου προσάρτησης αυτών στην αλυσίδα.

- Να ολοκληρώνεται σε εύλογο χρονικό διάστημα (σχετικά πάντα με το εκάστοτε σύστημα) όταν συμμετέχουν πολλοί χρήστες ταυτόχρονα.
- Να είναι εύκολη και ταχύτατη (πολλές τάξεις μεγέθους από την εύρεση) η επιβεβαίωση της εγκυρότητας του στοιχείου εξόδου με βάση τις εισόδους από οποιονδήποτε χρήστη.

Τα παραπάνω χαρακτηριστικά εξυπηρετούν τους ακόλουθους σκοπούς:

- Δεχόμενοι πολλαπλές εισόδους οι οποίες δίνουν μοναδική έξοδο, μπορούμε να συνδέσουμε κάθε καινούργιο γεγονός της αλυσίδας με το αμέσως προηγούμενο, δίνοντας σαν εισόδους το πακέτο πληροφορίας του καινούριου γεγονότος και το στοιχείο εξόδου του προηγούμενου. Η ιδιότητα αυτή είναι και εκείνη που προστατεύει την αλυσίδα από την αλλοίωση του ιστορικού της. Για να προστεθεί ή να αλλαχθεί κάποιος ενδιάμεσος κρίκος αυτής, χρειάζεται να υπολογιστεί όχι μόνο το στοιχείο διασύνδεσης του νέου κρίκου αλλά και όλων των μετέπειτα κρίκων, αλλιώς η αλυσίδα ορίζεται μη έγκυρη.
- Καθώς η εύρεση του στοιχείου διασύνδεσης είναι χρονοβόρα, είναι αδύνατο για ένα κακόβουλο χρήστη να μπορέσει να υπολογίσει όλα τα στοιχεία από τον αλλοιωμένο κρίκο μέχρι και την κεφαλή της αλυσίδας. Ακόμα και αν τα καταφέρει, ο χρόνος που θα έχει αφιερώσει θα είναι τόσο μεγάλος που θα έχουν προστεθεί πολλαπλάσιοι καινούριοι κρίκοι, τόσοι ώστε ποτέ να μην μπορέσει να προλάβει την επέκταση αυτής καθιστώντας έτσι την προσπάθειά του αναποτελεσματική.
- Οποιοσδήποτε κόμβος μπορεί μόνος του και σε μικρό χρονικό διάστημα να ελέγξει την εγκυρότητα ολόκληρης ή μέρους της αλυσίδας. Η δυνατότητα αυτή είναι σημαντική διότι επιτρέπει τη γρήγορη αποδοχή (επικυρωμένων από τρίτους) γεγονότων ή την απόρριψή τους σε περίπτωση που έχουν διαδοθεί από κακόβουλο κόμβο.

Συντήρηση συστήματος

Παρ' ότι δεν αποτελεί μια λειτουργία από μόνη της, η συντήρηση του συστήματος είναι η σημαντικότερη διαδικασία στην οποία συμμετέχουν οι κόμβοι του συστήματος. Με βάση αυτά που παρουσιάστηκαν στην προηγούμενη παράγραφο διαπιστώνουμε πως η διαδικασία επικύρωσης είναι επίτηδες μια χρονοβόρα και κυρίως υπολογιστικά έντονη διαδικασία. Αυτό μεταφράζεται και σε αντίστοιχο ενεργειακό κόστος για τους κόμβους που πραγματοποιούν την εξαγωγή (το λεγόμενο *mining* [11]) του στοιχείου επικύρωσης. Δημιουργείται συνεπώς το ερώτημα του γιατί κάποιος να συμμετάσχει στη διαδικασία από τη στιγμή που θα υπάρξει προσωπικό κόστος (στη συγκεκριμένη περίπτωση αντικατοπτριζόμενο στο λογαριασμό ρεύματος).

Υπάρχοντα συστήματα βασισμένα σε blockchain υποδομή, με αντίστοιχες διαδικασίες επικύρωσης συναλλαγών, έχουν λύσει το πρόβλημα παρέχοντας κίνητρα στους συμμετέχοντες. Παίρνοντας το παράδειγμα του συστήματος οικονομικών συναλλαγών, δομείται το πρωτόκολλο

με τέτοιο τρόπο ώστε ο πρώτος κόμβος που επικυρώνει κάποια συναλλαγή επιβραβεύεται με ένα συγκεκριμένο χρηματικό ποσό το οποίο προστίθεται στο λογαριασμό του (έτσι λειτουργεί και η γέννηση νέων κρυπτονομισμάτων) ή και να χρεώσει το δημιουργό της συναλλαγής κάποιο ποσό για την επικύρωση αυτής.

Έχοντας τα σωστά κίνητρα είναι συμφέρον για τους συμμετέχοντες κόμβους να λαμβάνουν μέρος και να ανταγωνίζονται ο ένας τον άλλον για την επικύρωση συναλλαγών. Η συμπεριφορά αυτή είναι κρίσιμης σημασίας διότι εγγυάται της σωστής λειτουργίας ενός αποκεντροποιημένου συστήματος. Αν για παράδειγμα υπάρχει μόνο ένας χρήστης επικυρωτής, τότε έχει τον πλήρη έλεγχο όχι μόνο των συναλλαγών που επιτρέπει να κατοχυρωθούν αλλά έχει και τη δυνατότητα αλλοίωσης της αλυσίδας όπως αναφέρθηκε προηγουμένως [12].

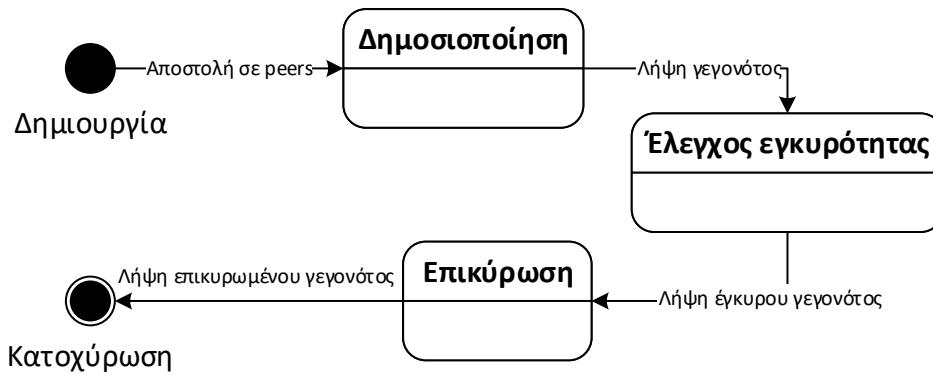
Κατοχύρωση γεγονότος

Η κατοχύρωση ενός γεγονότος και η προσάρτησή του στις προσωπικές αλυσίδες των κόμβων του συστήματος, είναι μια διαδικασία που εκκινείται με τη λήψη του επικυρωμένου γεγονότος από τον κόμβο που πρώτος βρήκε το σωστό στοιχείο επικύρωσης. Πριν την κατοχύρωση αυτού, γίνεται ένας τελικός έλεγχος επιβεβαίωσης ορθότητας ο οποίος περιέχει τα βήματα της λειτουργίας «Έλεγχος εγκυρότητας γεγονότος» σε συνδυασμό με τον έλεγχο του δημοσιοποιημένου στοιχείου επικύρωσης. Σε περίπτωση που καλύπτονται όλα τα προαπαιτούμενα, το γεγονός προστίθεται στις τοπικές αλυσίδες των κόμβων. Μια εγγραφή που βρίσκεται στην πλειονότητα των αλυσίδων μπορεί να θεωρηθεί ως κατοχυρωμένη και ότι αντιστοιχεί σε πραγματικό γεγονός.

Lifecycle γεγονότος

Με βάση τα παραπάνω, το lifecycle ενός γεγονότος έχει 5 καταστάσεις με σειρά όπως στο διάγραμμα καταστάσεων του σχήματος 8:

- Δημιουργία
- Δημοσιοποίηση
- Έλεγχος εγκυρότητας
- Επικύρωση
- Κατοχύρωση



Σχήμα 8: Lifecycle γεγονότος

Σημειώνεται πως ο μηχανισμός ομοφωνίας, η συντήρηση συστήματος και η κατοχύρωση γεγονότος ουσιαστικά συμβάλλουν στην πιθανοτική αντιμετώπιση του Byzantine Generals Problem. Ο συνδυασμός αυτός ονομάζεται proof-of-work και δημιουργήθηκε από τον Satoshi Nakamoto κατά τη διάρκεια της ανάπτυξης του Bitcoin blockchain [13].

4.1.4. Λογισμικό ενός Blockchain

Όλα τα στοιχεία και λειτουργίες που περιγράφονται στις προηγούμενες παραγράφους υλοποιούνται σε μια client τύπου εφαρμογή. Είναι σημαντικό να σημειωθεί ότι δεν υπάρχει καμία κεντρική εφαρμογή διαχείρισης, καμία κεντρική βάση δεδομένων και κανένα είδους λογισμικό στο οποίο έχουν πρόσβαση μόνο μερικοί χρήστες διαχειριστές, μιας και αυτό προσβάλλει τα χαρακτηριστικά της αποκέντρωσης, της ασφάλειας και της δικαιοσύνης που διέπουν τα συστήματα blockchain.

Ο πυρήνας της client εφαρμογής είναι η συντήρηση του blockchain τόσο σε τοπικό επίπεδο (διαχείριση των τοπικών αρχείων της αλυσίδας, επιβεβαίωση των block και γενικά εφαρμογή του πρωτοκόλλου) όσο και σε επίπεδο δικτύου μέσω της διάδοσης ή προώθησης μηνυμάτων καθώς και τη συμμετοχή στην επικύρωση block.

Ταυτόχρονα η εφαρμογή μπορεί να υποστηρίζει και της ανάγκες του χρήστη όπως η εκτέλεση μίας συναλλαγής (δημιουργία έγκυρου γεγονότος) και η επισκόπηση της παρούσας κατάστασης καθώς και του ιστορικού όλης της αλυσίδας (προσπέλαση των block αυτής). Η λειτουργικότητα αυτή καθίσταται σημαντική διότι επιτρέπει στο χρήστη να συμμετέχει στο δίκτυο χωρίς να χρειάζεται να γνωρίζει ακριβώς και να πρέπει να υλοποιεί σωστά όλες τις λεπτομέρειες του πρωτοκόλλου, κάτι πολύπλοκο και κυρίως επιρρεπές σε λάθη.

Κόμβος του συστήματος συνεπώς ορίζεται κάθε υπολογιστικό σύστημα το οποίο εκτελεί την εφαρμογή αυτή και ταυτόχρονα συνδέεται στο peer-to-peer δίκτυο.

4.2. Μαθηματικό θεωρητικό υπόβαθρο κρυπτογραφίας

Η αριθμητική υπολοίπων και οι πρώτοι αριθμοί είναι ιδιαίτερης σημασίας στην αφηρημένη άλγεβρα (θεωρία ομάδων, δακτυλίων και σωμάτων), η οποία με τη σειρά της παίζει θεμελιώδη

ρόλο στην σύγχρονη κρυπτογραφία. Στο υποκεφάλαιο αυτό, για λόγους κατανόησης των αλγορίθμων κρυπτογράφησης που θα περιγράψουμε στη συνέχεια, θα ασχοληθούμε με τους ορισμούς των παραπάνω εννοιών και με μερικά θεωρητικά αποτελέσματα που είναι συνέπεια των ορισμών που θα δούμε.

Πρώτοι αριθμοί

Πρώτοι αριθμοί ορίζονται ως οι φυσικοί αριθμοί μεγαλύτεροι του 1 οι οποίοι έχουν ως μοναδικούς διαιρέτες το 1 και τον εαυτό τους. Αριθμοί με επιπλέον διαιρέτες ονομάζονται σύνθετοι. Αυτές είναι οι δύο κατηγορίες των φυσικών αριθμών, ενώ το θεμελιώδες θεώρημα της αριθμητικής, αποδεδειγμένο από τον Ευκλείδη, ορίζει πως:

Θεώρημα 4.2.1

Κάθε φυσικός αριθμός μεγαλύτερος του 1 είναι είτε πρώτος είτε μπορεί να αναλυθεί σε γινόμενο πρώτων παραγόντων κατά ένα και μοναδικό τρόπο, αν δεν λάβουμε υπόψη μας την σειρά των παραγόντων στο γινόμενο.

Πρώτοι προς αλλήλους

Δύο ακέραιοι αριθμοί $x, y \in \mathbb{Z}$ ονομάζονται πρώτοι προς αλλήλους (ή σχετικά πρώτοι) αν ο $ΜΚΔ(x, y) = 1$. Εξ ορισμού, οι πρώτοι αριθμοί είναι και πρώτοι προς αλλήλους μεταξύ τους.

Ασφαλείς πρώτοι αριθμοί

Στη θεωρία αριθμών υπάρχει μια ειδική κατηγορία πρώτων αριθμών που ονομάζονται *ασφαλείς πρώτοι*. Οι ασφαλείς πρώτοι αποτελούν το ζεύγος ενός Sophie Germain πρώτου δηλαδή αν p είναι ένας Germain πρώτος τότε και ο αριθμός $2p + 1$ είναι πρώτος και μάλιστα ασφαλής πρώτος. Οι ασφαλείς πρώτοι παίζουν σημαντικό στην κρυπτογραφία λόγω της χρήσης τους σε κρυπτοσυστήματα βασισμένα σε προβλήματα διακριτών λογαρίθμων όπως η ανταλλαγή κλειδιών Diffie-Hellman καθώς και το Elgamal κρυπτοσύστημα.

Αριθμητική υπολοίπων (Modular arithmetic)

Από τους κανόνες της διαιρετότητας γνωρίζουμε ότι $\forall X, P \in \mathbb{Z}$ υπάρχουν ακέραιοι Y, K ώστε να ισχύει η σχέση

$$X = K * P + Y \quad (4.2.1)$$

Το Y το ονομάζουμε υπόλοιπο της διαίρεσης του X με το P . Με όρους αριθμητικής υπολοίπων παραπάνω σχέση (4.2.1) γράφεται

$$X \equiv Y \pmod{P} \quad (4.2.2)$$

Όταν ένας ακέραιος X διαιρείται με έναν ακέραιο P , τότε τα δυνατά υπόλοιπα της διαίρεσης είναι το σύνολο $\mathbb{Z}_p = \{0, 1, 2, 3, 4, \dots, p - 1\}$. Το σύνολο \mathbb{Z}_p ονομάζεται «σύνολο ακεραίων

modulo p ». Για παράδειγμα αν $p = 7$ το $\mathbb{Z}_p = \{0,1,2,3,4,5,6\}$. Αν θεωρήσουμε ότι το Y της εξίσωσης (4.2.1) ανήκει στο \mathbb{Z}_p και αν $Y = 4$, τότε η εξίσωση (4.2.1) γράφεται

$$X = K * 7 + 4 \quad (4.2.3)$$

όπου $K \in \mathbb{Z}$.

Ισοδύναμοι modulo p αριθμοί (congruence)

Ορισμός: Έστω ακέραιος $p > 1$ και ακέραιοι $a, b \in \mathbb{Z}$. Οι a και b λέγεται ότι είναι ισοδύναμοι $mod p$ εάν ο p είναι διαιρέτης της διαφοράς $a - b$

$$a - b = kn$$

Η ισοδυναμία $mod p$ γράφεται ως εξής

$$a \equiv b \pmod{p} \quad (4.2.4)$$

Πρακτικά αυτό σημαίνει ότι η διαίρεση του a με το n αφήνει το ίδιο υπόλοιπο με την διαίρεση του b με το n , δηλαδή a και b είναι ισοϋπόλοιποι.

Για ισοϋπόλοιπους αριθμούς $mod p$ ισχύουν οι εξής ιδιότητες:

1. Ανακλαστική:

$$a \equiv a \pmod{p} \quad (4.2.5)$$

2. Συμμετρική:

$$a \equiv b \pmod{p} \Leftrightarrow b \equiv a \pmod{p} \quad (4.2.6)$$

3. Μεταβατική:

$$a \equiv b \pmod{p} \text{ και } b \equiv c \pmod{p} \Rightarrow a \equiv c \pmod{p} \quad (4.2.7)$$

Επίσης αν $a \equiv b \pmod{p}$ και $c \equiv d \pmod{p}$ τότε:

$$a + c \equiv b + d \pmod{p} \quad (4.2.8)$$

$$ac \equiv bd \pmod{p} \quad (4.2.9)$$

Modular Πολλαπλασιαστικός αντίστροφος

Ο modular πολλαπλασιαστικός αντίστροφος ορίζεται ως ο ακέραιος x τέτοιος ώστε

$$a * x \equiv 1 \pmod{p} \quad (4.2.10)$$

Όπου φυσικά $x \in \{0,1,2, \dots, p-1\}$.

Ο πολλαπλασιαστικός αντίστροφος του $a \pmod{p}$ υπάρχει αν και μόνο αν οι a και p είναι σχετικά πρώτοι ($ΜΚΔ(a, p) = 1$).

Modular διαίρεση

Δοθέντων τριών φυσικών αριθμών a, b, p , ως modular διαίρεση ορίζεται η πράξη

$$c \equiv \frac{a}{b} \pmod{p} \quad (4.2.11)$$

Η modular διαίρεση ορίζεται εφόσον υπάρχει ο πολλαπλασιαστικός αντίστροφος $\text{mod } p$ του διαιρέτη. Έστω αντίστροφος b^{-1} , έχουμε

$$c \equiv a * b^{-1} \pmod{p} \quad (4.2.12)$$

Αφηρημένη άλγεβρα

Αφηρημένη άλγεβρα είναι ο κλάδος των μαθηματικών που μελετά αλγεβραϊκές δομές όπως ομάδες, δακτυλίους, πεδία, πλέγματα και άλλα. Πολλές από τις δομές αυτές έχουν μεγάλη σημασία για τις τεχνικές της μοντέρνας αλλά και της μελλοντικής κρυπτογραφίας.

Ομάδες (Groups)

Μια ομάδα είναι ένα διατεταγμένο σύνολο G εφοδιασμένο με μια πράξη $*$ και συμβολίζεται με $(G, *)$. Εάν η πράξη $*$ είναι η πρόσθεση ή ο πολλαπλασιασμός τότε η ομάδα αντίστοιχα ονομάζεται *αθροιστική* ή *πολλαπλασιαστική*. Για να ορίζει ένα διατεταγμένο σύνολο μια ομάδα πρέπει να ισχύουν οι παρακάτω τέσσερις ιδιότητες ονόματι *αξιώματα ομάδας*:

1. Να είναι κλειστή ως προς την πράξη $*$

$$\forall x, y \in G \text{ ισχύει } x * y \in G \quad (4.2.13)$$

2. Να ισχύει η προσεταιριστική ιδιότητα

$$\forall x, y, z \in G \text{ ισχύει } (x * y) * z = x * (y * z) \quad (4.2.14)$$

3. Να υπάρχει το ουδέτερο στοιχείο της πράξης

$$\forall x \in G \exists e \in G : x * e = e * x = x \quad (4.2.15)$$

4. Να υπάρχει το αντίστροφο στοιχείο της πράξης

$$\forall x \in G \exists y : x * y = y * x = e \quad (4.2.16)$$

Επιπλέον αν

$$\forall x, y \in G \text{ ισχύει } x * y = y * x \quad (4.2.17)$$

τότε η ομάδα λέγεται Αβελιανή (Abelian Group).

Ορισμοί

- Μια ομάδα G ονομάζεται πεπερασμένη ή άπειρη αν περιέχει πεπερασμένο ή άπειρο αριθμό στοιχείων αντίστοιχα. Το πλήθος των στοιχείων της G ονομάζεται τάξη (order) και συμβολίζεται ως $|G|$.
- Μια ομάδα G λέγεται κυκλική (cyclic group) αν υπάρχει στοιχείο $g \in G : \forall a \in G$ να υπάρχει $j \in \mathbb{Z}$ ώστε $a = g^j$. Το στοιχείο g ονομάζεται γεννήτορας (generator) της

κυκλικής ομάδας και γράφουμε $G = \langle g \rangle$. Να σημειωθεί ότι μπορεί να έχουμε περισσότερους του ενός γεννήτορες σε μια ομάδα.

Διακριτός λογάριθμος (Discrete Log / DL)

Υπενθυμίζουμε πως ο λογάριθμος $\log_b a$ ορίζει μία τιμή k όπου

$$k : b^k = a \quad (4.2.18)$$

Αναλογικά, διακριτός λογάριθμος ονομάζεται η τιμή αυτή k στην περίπτωση που δουλεύουμε εντός ομάδας G .

Ορισμός [14]

Για οποιοδήποτε στοιχείο b της ομάδας G και για οποιοδήποτε θετικό ακέραιο k εκφράζουμε ως b^k την k φορές επαναλαμβανόμενη εφαρμογή της πράξης $*$ της ομάδας στο στοιχείο b

$$b^k = \underbrace{b * b * b * b \dots b}_{k \text{ παράγωγες}} \quad (4.2.19)$$

Για στοιχείο $a \in G$, ο ακέραιος k που λύνει την εξίσωση (4.2.18) ονομάζεται διακριτός λογάριθμος του a με βάση b και γράφεται ως

$$k = \log_b a \quad (4.2.20)$$

Εκτός από κάποιες ειδικές περιπτώσεις, δεν υπάρχει αποτελεσματική μέθοδος για τον υπολογισμό διακριτού λογαρίθμου πέρα από την εξαντλητική αναζήτηση χρησιμοποιώντας συμβατικούς υπολογιστές, κάτι που κάνει σχεδόν αδύνατο τον υπολογισμό στην περίπτωση που έχουμε μεγάλες τιμές (εκατοντάδες bit). Σημειώνεται πως το ίδιο δεν ισχύει με εάν γίνει χρήση κβαντικού υπολογιστή μιας και ο αλγόριθμος του Shor μπορεί να δώσει αποτελέσματα σε πολύ μικρότερα χρονικά διαστήματα [15].

Υπολογιστικό πρόβλημα Diffie-Hellman (CDH)

Ορισμός [14]

Έστω κυκλική ομάδα $G = \langle g \rangle$ τάξης q και τιμές $a, b \in \{0, 1, 2 \dots q - 1\}$. Εάν έχουμε διαθέσιμες τις τιμές (g, g^a, g^b) τότε να υπολογιστεί η τιμή g^{ab} .

Αντίστοιχα με τον υπολογισμό διακριτού λογαρίθμου, το υπολογιστικό πρόβλημα Diffie-Hellman θεωρείται υπολογιστικά δύσκολο. Σημειώνεται πως δεν είναι δυσκολότερο από το πρόβλημα διακριτού λογαρίθμου: $CDH \leq DL$.

Πρόβλημα απόφασης Diffie-Hellman (DDH)

Ορισμός [14]

Έστω κυκλική ομάδα $G = \langle g \rangle$ τάξης q και τιμές $a, b, c \in \{0, 1, 2, \dots, q-1\}$. Έχοντας τις τιμές g^a, g^b, g^c να αποφασιστεί εάν $c = ab$.

Αντίστοιχα με το υπολογιστικό πρόβλημα Diffie-Hellman, το πρόβλημα απόφασης Diffie-Hellman θεωρείται υπολογιστικά δύσκολο. Σημειώνεται πως δεν είναι δυσκολότερο από το υπολογιστικό πρόβλημα Diffie-Hellman: $DDH \leq CDH$.

Στο πρόβλημα απόφασης Diffie-Hellman βασίζεται το κρυπτοσύστημα Elgamal [16] το οποίο ήταν έμπνευση για το ομομορφικό κρυπτοσύστημα που χρησιμοποιήθηκε στο πρωτόκολλο ψηφοφορίας το οποίο βασίζεται στο πρόβλημα εύρεσης διακριτού λογαρίθμου.

Πολυώνυμο Lagrange

Έστω σύνολο σημείων (x_j, y_j) , με x_j διαφορετικά μεταξύ τους, το $P(x)$ πολυώνυμο Lagrange είναι το πολυώνυμο ελάχιστου βαθμού όπου για κάθε τιμή x_j η τιμή του $P(x_j)$ ταυτίζεται με την τιμή y_j .

Πολυωνυμική παρεμβολή Lagrange

Έστω $n + 1$ σημεία $(x_0, y_0), \dots, (x_j, y_j), \dots, (x_n, y_n)$ όπου όλα τα x_j διαφορετικά μεταξύ τους. Το πολυώνυμο παρεμβολής Lagrange $P_n(x)$ βαθμού $\leq n$ δίνεται από τον τύπο:

$$P_{n(x)} = l_0(x)f(x_0) + l_1(x)f(x_1) + \dots + l_n(x)f(x_n) = \sum_{i=0}^n l_i(x)f(x_i) \quad (4.2.21)$$

με

$$l_i(x) = \prod_{0 \leq j \leq n, j \neq i} \frac{x - x_j}{x_i - x_j} \quad (4.2.22)$$

Η παρεμβολή Lagrange χρησιμοποιείται στη μέθοδο Shamir secret sharing την οποία θα αναλύσουμε παρακάτω.

4.3. Κρυπτογραφία, κρυπτοσυστήματα και πρωτόκολλα

Η κρυπτογραφία ξεκίνησε ως η μέθοδος μετατροπής ενός απλού κειμένου T (plain text) σε μη αναγνώσιμο κρυπτοκείμενο C (ciphertext). Παρ' ότι μη αναγνώσιμο στη γενική περίπτωση, εξουσιοδοτημένα άτομα που κατέχουν το κλειδί ή τη μέθοδο αποκρυπτογράφησης μπορούν εύκολα να επαναφέρουν το κρυπτοκείμενο C στην αρχική του μορφή T , κάνοντάς το αναγνώσιμο και πάλι.

Στη γενική της μορφή, σήμερα η κρυπτογραφία αναφέρεται στη δημιουργία και ανάλυση κρυπτοσυστημάτων ασφαλούς επικοινωνίας, στη διαχείριση απόρρητης πληροφορίας, στην ταυτοποίηση προσώπων και άλλα.

Τα πρωτόκολλα κρυπτογράφησης ισχυροποιήθηκαν κατά τη δεκαετία του 1970 επειδή εκμεταλλεύτηκαν τις ιδιότητες των ακέραιων αριθμών modulo n και προβλήματα της θεωρίας αριθμών για τα οποία μέχρι σήμερα δεν έχουν δοθεί θεωρητικές λύσεις. Τέτοια είναι η ανάλυση σε γινόμενο πρώτων παραγόντων, η εύρεση διακριτού λογαρίθμου και υπολογισμός πολλαπλασιαστέου γινομένου σημείου ελλειπτικής καμπύλης.

Στη συνέχεια του υποκεφαλαίου αυτού παρουσιάζονται κάποια αρχέγονα κρυπτογραφικά στοιχεία τα οποία χρησιμοποιούνται για τη δημιουργία κρυπτο-πρωτοκόλλων και πάνω στα οποία βασίζεται και το πρωτόκολλο ηλεκτρονικής ψηφοφορίας που παρουσιάζεται στο επόμενο κεφάλαιο.

4.3.1. Συστήματα κρυπτογράφησης

Υπάρχουν δύο τύποι συστημάτων κρυπτογράφησης πληροφορίας:

1. **Συστήματα συμμετρικής κρυπτογραφίας** στα οποία η κρυπτογράφηση και αποκρυπτογράφηση γίνονται με το ίδιο κλειδί. Τα πλεονεκτήματα των συστημάτων αυτών είναι πως είναι ασφαλή και γρήγορα, έχουν όμως το μεγάλο μειονέκτημα του ότι και οι δύο πλευρές πρέπει εξ αρχής να διαθέτουν το ίδιο κλειδί ως κοινό μυστικό για να αρχίσουν μια κρυπτογραφημένη επικοινωνία. Η κοινοποίηση του κλειδιού εξ αποστάσεως θεωρητικά μπορεί να γίνει μέσω ενός άλλου μυστικού κλειδιού το οποίο επίσης όμως πρέπει να είναι εξ αρχής γνωστό, προχωρώντας έτσι σε μια ατέρμονη παραγωγή εξαρτώμενων κλειδιών.

Ενδεικτικοί αλγόριθμοι συμμετρικής κρυπτογραφίας είναι οι DES, AES και ChaCha20.

2. **Συστήματα ασύμμετρης κρυπτογραφίας** στα οποία η κρυπτογράφηση και αποκρυπτογράφηση γίνονται με διαφορετικά κλειδιά. Το κλειδί κρυπτογράφησης είναι δημοσίως γνωστό και ονομάζεται Δημόσιο Κλειδί (Public Key) ενώ το κλειδί αποκρυπτογράφησης παραμένει αυστηρώς μυστικό και ονομάζεται Ιδιωτικό ή Κρυφό Κλειδί (Private Key).

Στα συστήματα αυτά ο αποστολέας μηνύματος το κρυπτογραφεί με το Public Key το παραλήπτη ο οποίος με τη σειρά του αποκρυπτογραφεί το μήνυμα χρησιμοποιώντας το αντίστοιχο Private Key που διαθέτει.

Παρ' ότι η Public key κρυπτογραφία είναι πιο χρονοβόρα, ειδικά για μεγάλα κείμενα, διαθέτει το μεγάλο πλεονέκτημα ότι λύνει το πρόβλημα της συμμετρικής κρυπτογραφίας μιας και επιτρέπει την ανταλλαγή πληροφορίας με ασφαλή τρόπο χωρίς να προϋπάρχει κοινή πληροφορία μεταξύ των δύο συμμετεχόντων. Μπορεί λοιπόν να χρησιμοποιηθεί όχι για επικοινωνία αλλά για την κοινοποίηση ενός κρυφού κλειδιού συμμετρικής κρυπτογραφίας μεταξύ δύο πλευρών.

Ενδεικτικά συστήματα ασύμμετρης κρυπτογραφίας είναι οι αλγόριθμοι RSA, Diffie-Hellman και Elgamal.

4.3.2. Ομομορφική κρυπτογραφία

Η ομομορφική κρυπτογραφία είναι μια μέθοδος κρυπτογράφησης η οποία επιτρέπει την εκτέλεση μαθηματικών πράξεων πάνω σε κρυπτογραφημένα δεδομένα, με τέτοιο τρόπο ώστε η αποκρυπτογράφηση του κρυπτο-αποτελέσματος να δίνει τιμή ίδια με αυτή που θα λαμβανόταν από την εκτέλεση των ίδιων πράξεων στα plain text δεδομένα.

Από μαθηματικής πλευράς, έστω μια συνάρτηση κρυπτογράφησης $E(x)$, ισχύει

$$E(x * y) = E(x) * E(y) \quad 4.2.23$$

Τα ομομορφικά κρυπτοσυστήματα προσφέρουν τη δυνατότητα εξαγωγής πορισμάτων από κρυπτογραφημένα δεδομένα, χωρίς ποτέ να χρειαστεί αυτά να αποκρυπτογραφηθούν, όπως για παράδειγμα την καταμέτρηση (πρόσθεση) μεμονωμένων ψήφων για εύρεση του νικητή, χωρίς όμως να χρειαστεί σε κανένα στάδιο να μαθευτούν οι επιμέρους επιλογές των ψηφοφόρων.

Ενδεικτικά κρυπτοσυστήματα με ομομορφικές ιδιότητες είναι το RSA, το Elgamal και το Paillier.

4.3.2.1. Αθροιστικό ομομορφικό κρυπτόςστημα διακριτού λογαρίθμου πολλαπλών μερών

Η χρήση ομομορφικών συστημάτων είναι πάγια στις περιπτώσεις σχεδιασμού συστημάτων ηλεκτρονικής ψηφοφορίας. Παρ' όλα αυτά, η κρυπτογράφηση σε αυτές τις περιπτώσεις γίνεται συνήθως, αν όχι πάντα, με τη χρήση ενός κοινού κλειδιού το οποίο γνωστοποιείται στους ψηφοφόρους και με βάση το οποίο κρυπτογραφούν τις επιλογές τους. Αυτό έχει ως αποτέλεσμα να υπάρχει ένα αντίστοιχο, κρυφό μεν, αλλά κοινό κλειδί αποκρυπτογράφησης για την αποκρυπτογράφηση του ομομορφικού αθροίσματος (ενδεικτικά [1], [17]). Το πρόβλημα με ένα κοινό κλειδί αποκρυπτογράφησης είναι πως εκτός από το ομομορφικό άθροισμα, μπορεί να χρησιμοποιηθεί και για την αποκρυπτογράφηση των επιμέρους όρων της πράξης, δηλαδή των μεμονωμένων ψήφων των ψηφοφόρων. Συνήθως λαμβάνονται μέτρα για την αντιμετώπιση του προβλήματος αυτού, όπως για παράδειγμα ο κατακερματισμός του κλειδιού μεταξύ n διαχειριστών της ψηφοφορίας με δυνατή την ανάκτηση του μόνο με την ταυτόχρονη παρουσία ενός ποσοστού αυτών (π.χ. πάνω από 50%). Για τη ρεαλιστική διαχείριση τέτοιων συστημάτων, ο αριθμός των διαχειριστών του κλειδιού δεν μπορεί να είναι πολύ μεγάλος (π.χ. 1000) με αποτέλεσμα να επιλέγονται σχετικά λίγοι, της τάξεως του 10. Όπως έχουμε δει και με τα blockchain συστήματα στο προηγούμενο υποκεφάλαιο, για μικρό αριθμό συμμετεχόντων οι πιθανότητες εξαναγκασμού ή διαφθοράς της ομάδας διαχείρισης αυξάνονται και φτάνουν τα ρεαλιστικά επίπεδα.

Θέλοντας λοιπόν να αποφευχθεί η οποιαδήποτε υπόνοια πιθανότητας εξαναγκασμού του συστήματος, ένα από τα προαπαιτούμενα κατά τη μελέτη που εκπονήθηκε για την εργασία αυτή ήταν το πρωτόκολλο να χαρακτηρίζεται από πλήρη αποκέντρωση, ξεκινώντας από τη διαδικασία υποβολής ψήφου έως και κατά την καταμέτρηση του αποτελέσματος. Για να επιτευχθεί αυτό

χρειαζόταν η εφαρμογή ενός αθροιστικά ομομορφικού κρυπτοσυστήματος το οποίο όμως να επιτρέπει κάθε όρος του αθροίσματος να έχει κρυπτογραφηθεί με διαφορετικό κλειδί.

Με έμπνευση το Elgamal [16] κρυπτοσύστημα και συγκεκριμένα την παραλλαγή αυτού που του προσδίδει αθροιστικές ομομορφικές ιδιότητες, εντοπίστηκε μπορεί να συνδυαστεί το πρώτο βήμα της παραγωγής δημοσίου κλειδιού g^S για την απευθείας κρυπτογράφηση του μηνύματος G^M . Στην περίπτωση αυτή, το νέο κρυπτοσύστημα βασίζεται στο πρόβλημα εύρεσης διακριτού λογαρίθμου και όχι στο πρόβλημα απόφασης Diffie-Hellman στο οποίο βασίζεται το Elgamal κρυπτοσύστημα. Παρακάτω ακολουθεί περιγραφή του κρυπτοσυστήματος.

Έστω n συμμετέχοντες στην ψηφοφορία. Κάθε ψηφοφόρος παράγει ένα κρυφό κλειδί s_i όπου $0 \leq i \leq n$. Έχοντας ορίσει μια κοινή κυκλική ομάδα με στοιχεία (g, G, p) όπου g και G γεννήτριες της ομάδας αυτής, ο κάθε ψηφοφόρος παράγει μια κρυπτογραφημένη μορφή του μηνυμάτος του (στην περίπτωση μας της ψήφου του) ως εξής:

$$v_i = g^{s_i} * G^{M_i} \bmod p \quad (4.2.24)$$

το οποίο δημοσιεύει στους υπολοίπους. Όταν δημοσιευτούν και οι n κρυπτογραφημένες ψήφοι, τότε αθροίζονται ομομορφικά, όπου στην περίπτωση μας εκμεταλλευόμαστε την ιδιότητα των δυνάμεων όπου το γινόμενο τους παράγει το άθροισμα των εκθετών ως εξής:

$$v_{all} \equiv v_0 * v_1 * \dots * v_n \equiv g^{s_0} G^{M_0} * \dots * g^{s_n} G^{M_n} \equiv g^{s_0 + \dots + s_n} * G^{M_0 + \dots + M_n} \bmod p \quad (4.2.25)$$

Έχοντας το αποτέλεσμα της σχέσης 4.2.25, το επόμενο βήμα είναι να διώξουμε τον όρο $g^{s_0 + \dots + s_n} = g^{key_{all}}$, το οποίο γίνεται μέσω *διαίρεσης υπολοίπου* του v_{all} με αυτόν.

$$\frac{v_{all}}{g^{key_{all}}} \equiv G^{(M_0 + \dots + M_n)} \bmod p \quad (4.2.26)$$

Ο εκθέτης key_{all} αποτελεί ουσιαστικά το οικουμενικό κλειδί όλων ψηφοφόρων που κρυπτογραφεί το άθροισμα των ψήφων τους. Διώχνοντας τον όρο $g^{key_{all}}$, το μόνο που μένει είναι να υπολογιστεί ο εκθέτης της τιμής 4.2.26 M_{all} , το οποίο ουσιαστικά αποτελεί πρόβλημα υπολογισμού διακριτού λογαρίθμου. Όπως και με το Elgamal κρυπτοσύστημα, ο υπολογισμός στην περίπτωση αυτή γίνεται με εξαντλητική μέθοδο, όπου δοκιμάζονται όλες οι τιμές του M_{all} με τη βάση G μέχρι να βρεθεί αυτή που ταιριάζει, η οποία είναι και η τιμή του αθροίσματος των ψήφων. Η εξαντλητική μέθοδος στην περίπτωση αυτή έχει πολυπλοκότητα $O(n)$ εκθετικών πράξεων, η οποία θεωρείται αποδεκτή για τον αναμενόμενο αριθμό ψηφοφόρων.

Είναι πολύ σημαντικό να σημειωθεί πως για την ανάκτησή του key_{all} εκτελείται μια αθροιστική πράξη πολλαπλών μερών (multi-party computation) χρησιμοποιώντας το σχήμα Shamir, όπως θα δείξουμε παρακάτω. Η μέθοδος αυτή ουσιαστικά επιτρέπει την παραγωγή ενός αθροίσματος n τιμών μεταξύ n συμμετεχόντων χωρίς να δημοσιευτούν οι επιμέρους τιμές αυτών.

4.3.3. Διαμοιρασμός μυστικών / Secret sharing

Ο διαμοιρασμός μυστικών αναφέρεται σε μεθόδους οι οποίες έχουν ως στόχο τη διάσπαση ενός μυστικού μεταξύ ενός αριθμού συμμετεχόντων. Κάθε ένας από αυτούς λαμβάνει μια τιμή άσχετη με το μυστικό, ονόματι *μερίδιο του μυστικού*, η οποία δεν έχει καμία χρησιμότητα από μόνη της. Το μυστικό μπορεί να αναδημιουργηθεί μόνο αν συνδυαστούν αρκετά μερίδια αυτού. Για ένα συνολικό αριθμό μεριδίων n ορίζεται εξ αρχής ο ελάχιστος αριθμός $t \leq n$, ονόματι *κατώφλι*, που απαιτείται για την ανάκτηση του μυστικού. Όπως είναι αναμενόμενο, η κοινοποίηση μεριδίων μεταξύ συμμετεχόντων υπονομεύει την ασφάλεια του συστήματος διότι ουσιαστικά μειώνει το κατώφλι για την ανάκτηση του μυστικού. Οι μέθοδοι αυτοί ονομάζονται και σχήματα κατωφλίου.

Οι μέθοδοι διαμοιρασμού μυστικών χρησιμοποιούνται συχνά σε σενάρια αποθήκευσης πληροφορίας η οποία πρέπει να παραμείνει μυστική αλλά και ταυτόχρονα να αντέχει στην απώλεια του αποθηκευτικού χώρου της. Κατακερματίζοντας για παράδειγμα ένα κλειδί χρηματοκιβωτίου σε πολλούς υπολογιστές μέσω μεθόδου διαμοιρασμού μυστικών, διατηρείται η μυστικότητά του ενώ ταυτόχρονα αντέχει και σε σενάρια απώλειας μίας ή περισσότερων μηχανών.

4.3.3.1. Shamir secret sharing

Ένας κλασικός αλγόριθμος διαμοιρασμού μυστικών είναι ο Shamir secret sharing ο οποίος επινοήθηκε από τον Adi Shamir [18]. Ακολουθεί βασική επεξήγηση.

Έστω χρήση σχήματος κατωφλίου (t, n) για διαμοιρασμό μυστικής τιμής S . Επιλέγονται $t - 1$ τυχαίοι ακέραιοι αριθμοί a_1, a_2, \dots, a_{t-1} ενώ $a_0 = S$. Με βάση αυτούς ως συντελεστές, χτίζεται το πολυώνυμο

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_{t-1}x^{t-1} \quad (4.2.27)$$

Με βάση αυτό, λαμβάνουμε n τυχαία σημεία $(i, f(i)) : i \neq 0$. Κάθε ένα σημείο κοινοποιείται σε έναν από τους n συμμετέχοντες. Για οποιοδήποτε υποσύνολο t σημείων, μπορεί να ανακατασκευαστεί το πολυώνυμο 4.2.27 χρησιμοποιώντας την παρεμβολή Lagrange. Έχοντας το πολυώνυμο $f(x)$, για την τιμή $x = 0$ λαμβάνουμε την τιμή $f(0) = a_0$ δηλαδή το μυστικό S .

Σημειώνεται πως για τη σωστή διατήρηση της μυστικότητας, όλες οι πράξεις γίνονται με στοιχεία ενός πεπερασμένου πεδίου F με μέγεθος P όπου P πρώτος αριθμός, μεγαλύτερος όλων των τιμών συντελεστών του πολυωνύμου καθώς και των τιμών t και n .

4.3.4. Ασφαλής υπολογισμός πολλαπλών μερών (Secure multi-party computation)

Ένας ασφαλής υπολογισμός πολλαπλών μερών είναι ένα πρωτόκολλο το οποίο επιτρέπει σε n συμμετέχοντες με n δεδομένα d_1, d_2, \dots, d_n να υπολογίσουν το αποτέλεσμα μίας συνάρτησης $F(d_1, d_2, \dots, d_n)$ χωρίς να αποκαλύψουν ο καθένας τους την τιμή του d .

Ένας τέτοιος υπολογισμός θα μπορούσε θεωρητικά να εκτελεστεί με την παρουσία ενός αδιάβλητου και έμπιστου διαιτητή εκτός των n συμμετεχόντων, στον οποίον ο κάθε ένας θα έδινε την τιμή του d_x και εκείνος θα υπολόγιζε σωστά την τιμή της F και θα ανακοίνωνε σε όλους μόνο το αποτέλεσμα. Ένα πρωτόκολλο ασφαλούς υπολογισμού προσφέρει στους συμμετέχοντες την ίδια δυνατότητα, στην περίπτωση που δεν μπορούν να εμπιστευτούν ή δεν υπάρχει ένας τέτοιος διαιτητής. Επιτρέπει τον υπολογισμό της τιμής της F μόνο μέσω ανταλλαγής μηνυμάτων μεταξύ των n συμμετεχόντων.

4.3.4.1. Shamir SMPC

Υπάρχουν διάφορα είδη SMPC πρωτοκόλλων. Στην δική μας περίπτωση ενδιαφερόμαστε και παρουσιάζουμε την υλοποίηση ενός αθροιστικού πρωτοκόλλου υπολογισμού της συνάρτησης $F(d_1, \dots, d_n) = d_1 + d_2 + \dots + d_n$ βασισμένο στη μέθοδο Shamir secret sharing που παρουσιάστηκε παραπάνω για n συμμετέχοντες με κατώφλι επίσης n .

Το πρωτόκολλο έχει τα εξής βήματα:

1. Κάθε συμμετέχοντας p με μια τιμή d δημιουργεί ένα τυχαίο πολυώνυμο n -οστού βαθμού με σταθερή τιμή την κρυφή του τιμή d_p .

$$f(x) = d_p + a_1x + a_2x^2 + \dots + a_nx^n$$
2. Υπολογίζει n τιμές του $f(x)$ για n διαφορετικές αλλά προκαθορισμένες τιμές x_p με $x_p \neq 0$, μια για κάθε συμμετέχοντα, συμπεριλαμβανομένου και του εαυτού του.
3. Στέλνει σε κάθε συμμετέχοντα p την αντίστοιχη τιμή $f(x_p)$.
4. Τα βήματα 1 έως 3 εκτελούνται από όλους τους συμμετέχοντες και ο καθένας στέλνει τις αντίστοιχες τιμές του τυχαίου πολυωνύμου $f(x)$. Ένα σημαντικό στοιχείο της διαδικασίας είναι πως οι τιμές f_p δεν αποστέλλονται τυχαία. Αν υποθέσουμε πως κάθε προκαθορισμένη τιμή x_p αντιστοιχίζεται σε ένα συγκεκριμένο συμμετέχοντα p , τότε πρέπει να του αποστέλλεται και η αντίστοιχη τιμή του $f(x_p)$ για το x που του αντιστοιχεί, από όλους τους συμμετέχοντες.
5. Έχοντας ο κάθε συμμετέχοντας p λάβει n τιμές $f_1(x_p), f_2(x_p), \dots, f_n(x_p)$ υπολογίζει το άθροισμά τους και το κοινοποιεί στους υπόλοιπους συμμετέχοντες.
6. Όταν κοινοποιηθούν όλα τα αθροίσματα, ο κάθε συμμετέχοντας τα χρησιμοποιεί για να εκτελέσει παρεμβολή Lagrange και να ανακατασκευάσει ένα νέο πολυώνυμο $f_{all}(x)$, ίσο με το άθροισμα των τυχαίων πολυωνύμων όλων των συμμετεχόντων.

$$f_{all}(x) = f_1(x) + f_2(x) + \dots + f_n(x)$$

Όντας το άθροισμα όλων των πολυωνύμων, είναι αναμενόμενο πως η σταθερά του $c_{all} = d_1 + d_2 + \dots + d_n$ και υπολογίζεται για $x = 0$, $f_{all}(0) = c_{all}$.

4.3.5. Αποδείξεις Μηδενικής Γνώσης

Αποδείξεις μηδενικής γνώσης είναι πρωτόκολλα τα οποία επιτρέπουν σε μια πλευρά, τον αποδεικνύοντα P , να αποδείξει τη γνώση μιας τιμής ή μιας πρότασης σε μια άλλη πλευρά, τον επαληθευτή V , χωρίς να αποκαλύψει την τιμή αυτή καθαυτή ούτε κάποια άλλη πληροφορία που οδηγεί σε αυτήν. Ένα απλό παράδειγμα χρήσης τέτοιων πρωτοκόλλων είναι κατά τη διαδικασία αυθεντικοποίησης όπου, σε αντίθεση με τις τωρινές μεθόδους, ένας χρήστης αποδεικνύει στον κεντρικό εξυπηρετητή γνώση του μυστικού κωδικού του χωρίς όμως να τον στείλει κατά την επικοινωνία τους. Αυτό προστατεύει το χρήστη από τρίτους που παρεμβαίνουν στη συνομιλία χρήστη – εξυπηρετητή (man in the middle attack) και θα μπορούσαν πιθανώς να υποκλέψουν τον κωδικό ταυτοποίησης.

4.3.5.1. Μη διαδραστική απόδειξη μηδενικής γνώσης

Στη βασική τους μορφή, τα πρωτόκολλα μηδενικής γνώσης απαιτούν την ταυτόχρονη συμμετοχή και του αποδεικνύοντα P και του επαληθευτή V . Υπάρχουν όμως και πρωτόκολλα μη διαδραστικής απόδειξης μηδενικής γνώσης τα οποία επιτρέπουν στον P να κοινοποιήσει τα στοιχεία της απόδειξης και στη συνέχεια οποιοσδήποτε V να μπορεί να εκτελέσει τη διαδικασία επαλήθευσης σε δικό του χρόνο.

Πρωτόκολλα απόδειξης μηδενικής γνώσης (διαδραστικά και μη) μπορούν να κατασκευαστούν για διάφορες τιμές ή και προτάσεις, όπως π.χ. “Το κρυπτοκείμενο C δημιουργήθηκε από μια από τις τιμές ενός συνόλου S ”. Πολλά πρωτόκολλα βασίζονται στο πρωτόκολλο απόδειξης γνώσης διακριτού λογαρίθμου Schnorr [19] ή σε αντίστοιχα πρωτόκολλα τριών κινήσεων ονόματι πρωτόκολλα Σίγμα.

4.3.6. Συναρτήσεις κατακερματισμού (Hash function)

Μια συνάρτηση κατακερματισμού αντιστοιχίζει ένα κείμενο αυθαίρετου μήκους σε μια τιμή σταθερού μήκους. Η συνάρτηση θα πρέπει να συμπεριφέρεται ως μονομορφισμός, δηλαδή δύο κείμενα με ελάχιστη διαφορά να παράγουν τελείως διαφορετικά αποτελέσματα. Τέτοιες συναρτήσεις χρησιμοποιούνται για διάφορους σκοπούς όπως την παραγωγή τυχαίων αριθμών, κρυπτογραφήματα, checksums και την παραγωγή αποτυπώματος ενός κειμένου. Γνωστές συναρτήσεις κατακερματισμού είναι οι MD5, RIPEMD και SHA.

4.3.7. Ψηφιακές υπογραφές

Οι ψηφιακές υπογραφές είναι βασικά κρυπτογραφικά εργαλεία τα οποία επιτρέπουν σε μια πλευρά να επιβεβαιώσει την προέλευση ενός μηνύματος καθώς και την μη-μετατροπή αυτού κατά τη μεταφορά του, διατηρώντας έτσι τα στοιχεία της ταυτοποίησης και της ακεραιότητας της επικοινωνίας. Τα στοιχεία αυτά είναι πολύ σημαντικά διότι προσφέρουν σιγουριά στην επικοινωνία μεταξύ δύο πλευρών και προστασία από επιθέσεις τύπου man in the middle ή προσπάθειες εξαπάτησης μέσω προσποίησης τρίτου προσώπου.

Οι ψηφιακές υπογραφές βασίζονται στην υποδομή της ασύμμετρης κρυπτογραφίας όπου η μια πλευρά παράγει ένα ζεύγος Δημοσίου-Κρυφού κλειδιού και γνωστοποιεί το Δημόσιο κλειδί. Όποτε θέλει να υπογράψει κάποιο μήνυμα, παράγει μια hash τιμή αυτού και στη συνέχεια παράγει μια τιμή ψηφιακής υπογραφής s του hash χρησιμοποιώντας το Κρυφό κλειδί. Η τιμή αυτή συνοδεύει το μήνυμα κατά τη μεταφορά του. Η πλευρά που θέλει να ταυτοποιήσει την προέλευση αλλά και την ακεραιότητα του μηνύματος, δεν έχει παρά να χρησιμοποιήσει το Δημόσιο κλειδί μαζί με την τιμή ψηφιακής υπογραφής s . Η τιμή που παράγεται θα πρέπει να είναι ίδια με την hash τιμή του μηνύματος που έχει λάβει.

Βασικό στοιχείο ενός σχήματος ψηφιακής υπογραφής είναι πως κάποιος που έχει διαθέσιμο μόνο το Δημόσιο κλειδί, δεν μπορεί ούτε να παράξει κάποια τιμή υπογραφής s η οποία να επιβεβαιώνεται με το ίδιο Δημόσιο κλειδί και ούτε μπορεί να ανακαλύψει το Κρυφό κλειδί βασιζόμενος στο Δημόσιο κλειδί.

Γνωστά σχήματα ψηφιακών υπογραφών είναι τα RSA, DSA και παραλλαγές αυτού.

5. Σχεδιασμός συστήματος ηλεκτρονικής ψηφοφορίας

Στο συγκεκριμένο κεφάλαιο αναλύεται η θεωρητική υλοποίηση του συστήματος ηλεκτρονικής ψηφοφορίας με χαρακτηριστικά που έχουν περιγράψει στο κεφάλαιο 2. Βασικός πυλώνας της προτεινόμενης online voting λύσης αποτελεί η τεχνολογία blockchain, ιδανική για χρήση σε τέτοια συστήματα μιας και οι λειτουργίες και ιδιαιτερότητες που περιγράφηκαν στο υποκεφάλαιο 4.1. *Blockchain* των θεωρητικών εννοιών πληρούν σε μεγάλο βαθμό τις λειτουργικές απαιτήσεις τους [20]. Βασική έμπνευση και πηγή πληροφοριών αποτελεί το Bitcoin blockchain [21], η τεχνολογία του οποίου είναι απλής μορφής και εξυπηρετεί συγκεκριμένο σκοπό (οικονομικές συναλλαγές) ο οποίος μπορεί να προσαρμοστεί και στη δική μας περίπτωση.

Στο υποκεφάλαιο 5.1. αναλύεται το blockchain πρωτόκολλο, δηλαδή οι κανόνες που διέπουν το σύστημα και την επικοινωνία των χρηστών. Κομμάτι των κανόνων αποτελούν οι διαθέσιμες ενέργειες, ο τρόπος εκτέλεσής τους καθώς και η μορφή των δεδομένων που ανταλλάσσονται και καταγράφονται στο blockchain.

Στο υποκεφάλαιο 5.2. παρουσιάζεται ο τρόπος με τον οποίο υλοποιείται το πρωτόκολλο, συγκεκριμένα περιγράφονται οι αλγόριθμοι και τα κρυπτοσυστήματα που χρησιμοποιούνται.

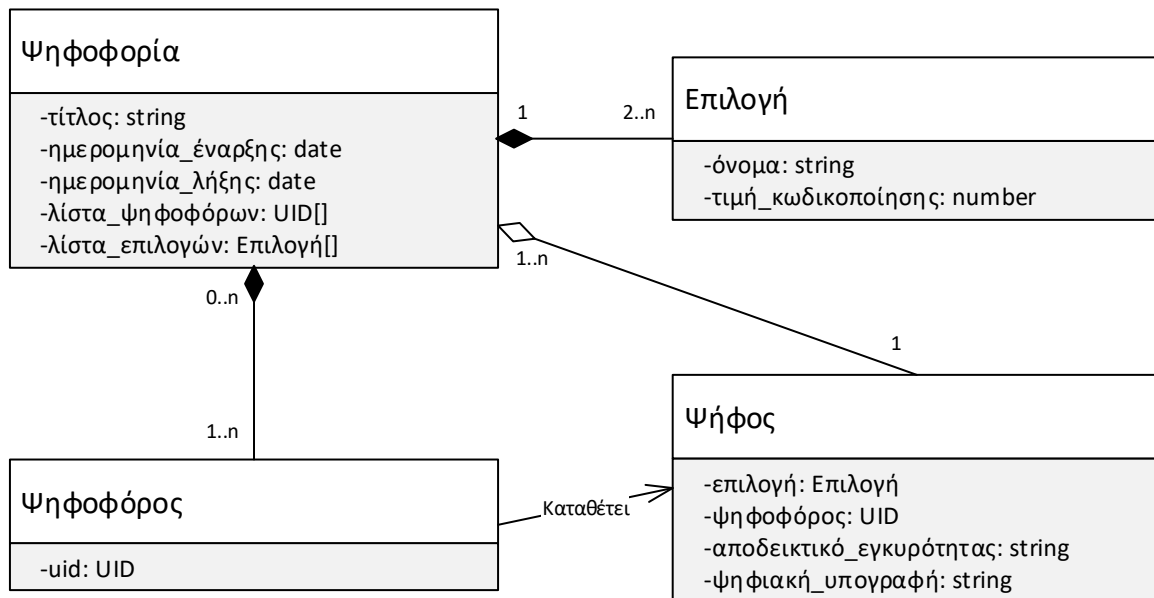
Στο υποκεφάλαιο 5.3. δίνεται ένα αναλυτικό αριθμητικό παράδειγμα, όπου παρουσιάζεται βήμα προς βήμα ένα σενάριο ψηφοφορίας με 5 ψηφοφόρους το οποίο έχει ως στόχο να διευκολύνει την κατανόηση του τρόπου εφαρμογής των κρυπτοσυστημάτων κυρίως από μαθηματικής άποψης.

Η υλοποίηση που παρουσιάζεται στο κεφάλαιο αυτό δεν σχετίζεται με κάποια συγκεκριμένη τεχνολογία, γλώσσα προγραμματισμού ή προϊόν. Ακολουθώντας τη λογική του blockchain, το σύστημα που σχεδιάστηκε αποτελείται μόνο από client εφαρμογές οι οποίες μπορούν να υλοποιηθούν από οποιονδήποτε με οποιαδήποτε τεχνολογία, με την προϋπόθεση ότι ακολουθούν πιστά το παρακάτω πρωτόκολλο και χρησιμοποιούν τους ίδιους αλγορίθμους και κρυπτοσυστήματα. Στο επόμενο κεφάλαιο, 6 *Case study - Σύστημα ηλεκτρονικής ψηφοφορίας για φοιτητική συνέλευση*, παρουσιάζεται μια δική μας υλοποίηση ως proof of concept (PoC) η οποία εκμεταλλεύεται κάποιες συγκεκριμένες τεχνολογίες ενώ χρησιμοποιεί και έτοιμη blockchain υποδομή πάνω στην οποία υλοποιείται το πρωτόκολλο ψηφοφορίας.

5.1. Πρωτόκολλο blockchain

Η δομή του πρωτοκόλλου του blockchain συστήματος πρέπει να είναι τέτοια ώστε η εξυπηρέτηση των αναγκών αυτού πρέπει να γίνονται με τον πιο λιτό και χαμηλής πολυπλοκότητας τρόπο. Αυτό βοηθά στην ελαχιστοποίηση των λαθών υλοποίησης και δυσκολεύει την νόμιμη αλλά κακόβουλη εκμετάλλευση των κανόνων.

5.1.1. Μοντέλο ψηφοφορίας



Σχήμα 9: Μοντέλο ψηφοφορίας συστήματος

Ψηφοφόρος/χρήστης

Ο ψηφοφόρος/χρήστης του συστήματος αποτελεί έναν κόμβο του blockchain δικτύου και συνδέεται σε αυτό μέσω οποιασδήποτε internet enabled συσκευής επικοινωνώντας P2P με τους υπόλοιπους ψηφοφόρους – χρήστες. Για να συμμετάσχει στο σύστημα πρέπει να παρέχει ένα μοναδικό στοιχείο ταυτοποίησης, το οποίο είναι ταυτισμένο με την προσωπικότητά του ως ψηφοφόρος, και γνωστοποιείται σε όλους τους υπόλοιπους χρήστες. Το στοιχείο αυτό είναι ένα μοναδικό αλφαριθμητικό ονόματι Unique ID (UID) το οποίο παράγει ο ίδιος ο χρήστης. Η γνωστοποίησή του γίνεται αυτοπροσώπως στην υπεύθυνη αρχή ψηφοφοριών (π.χ. στο ΔΣ φοιτητών) ή με κάποια άλλη μέθοδο επιβεβαίωσης της ταυτότητας του δηλώνοντα. Το αναγνωριστικό αυτό συνοδεύει την καταχώρηση ψηφοδελτίου του χρήστη ενώ ταυτόχρονα επιτρέπει και την επιβεβαίωση της εγκυρότητας της προέλευσης αυτού.

Ψηφοφορία

Η ψηφοφορία και τα στοιχεία της καθορίζονται από την εφορευτική επιτροπή και ορίζονται απ' ευθείας στο πρωτόκολλο του blockchain συστήματος ως στατικές τιμές. Στοιχεία ψηφοφορίας είναι τα εξής:

- Τίτλος. Αλφαριθμητική τιμή με στόχο την εύκολη ταυτοποίηση της ψηφοφορίας, π.χ. “Συνέλευση εξεταστική εαρινού 2020”.
- Περίοδος διάρκειας. Το χρονικό διάστημα μέσα στο οποίο επιτρέπεται να υποβληθούν ψήφοι, δηλαδή να εισαχθούν γεγονότα στην αλυσίδα. Προσπάθεια υποβολής ψήφων εκτός του διαστήματος δεν γίνεται δεκτή από τους συμμετέχοντες.

- Λίστα ψηφοφόρων. Αποτελείται από τα UUIDs των ψηφοφόρων, επιτρέποντας έτσι τον έλεγχο των καταχωρημένων ψήφων και την πιθανή ακύρωση ψήφων από μη εγκεκριμένους ψηφοφόρους.
- Λίστα διαθέσιμων επιλογών. Κάθε πιθανή επιλογή είναι μοναδική και προκαθορισμένη. Η καταχώρηση της επιλογής ως ψήφο είναι η μόνη ενέργεια που είναι διαθέσιμη στο χρήστη ενώ η δημιουργία του ψηφοδέλτιου και η δημοσιοποίησή του είναι αυτοματοποιημένες διαδικασίες.

Επιλογή

Κάθε επιλογή χαρακτηρίζεται από ένα όνομα ή περιγραφή και κωδικοποιείται με ένα συγκεκριμένο μοναδικό αριθμό, όσον αφορά την αναπαράστασή της στο blockchain. Η κωδικοποίηση είναι απαραίτητη για τον αυτόματο υπολογισμό του τελικού αποτελέσματος της ψηφοφορίας. Παίρνοντας ως παράδειγμα ένα δυαδικό σύστημα επιλογών ΝΑΙ – ΟΧΙ, μπορούμε να κωδικοποιήσουμε το ΝΑΙ με τον αριθμό 1 και το ΟΧΙ με τον αριθμό -1. Σε αυτή την περίπτωση, χωρίς παραβίαση της γενικότητας, αν έχουμε 10 ($V=10$) ψηφοφόρους και οι 6 ψηφίσουν ΝΑΙ ενώ οι υπόλοιποι 4 ΟΧΙ, αθροίζοντας τις επιλογές όλων θα πάρουμε ως αποτέλεσμα τον αριθμό 2 ($RESULT = 6-4 = 2$) το οποίο ταυτίζεται με τη διαφορά των ψήφων ΝΑΙ από των ψήφων ΟΧΙ. Στη γενική περίπτωση:

- $RESULT > 0 \rightarrow \text{ΝΑΙ}$
- $RESULT = 0 \rightarrow \text{Ισοβαθμία}$
- $RESULT < 0 \rightarrow \text{ΟΧΙ}$

Για περισσότερες από 2 επιλογές μπορούν να χρησιμοποιηθούν τιμές, το άθροισμα των οποίων να πολυπλέκει το διακριτό άθροισμα κάθε επιλογής. Παίρνοντας ως παράδειγμα ένα σενάριο με 100 ψηφοφόρους και 3 επιλογές [A,B,C], κωδικοποιούμε ως εξής:

- $A = 1$
- $B = 1000$
- $C = 1,000,000$

Οποιοσδήποτε συνδυασμός επιλογών θα παράξει άθροισμά τέτοιο ώστε να είναι ξεκάθαρο το διακριτό άθροισμα για κάθε μια επιλογή. Για παράδειγμα, αν οι ψήφοι κατανεμηθούν ως $A = 40, B = 50, C = 10$, το άθροισμα θα είναι:

$$40 \times 1 + 50 \times 1000 + 10 \times 1.000.000 = 10,050,040$$

Κάθε τάξη μεγέθους πολλαπλάσια του 10^3 περιέχει και τον αντίστοιχο αριθμό ψήφων που έχουν καταχωρηθεί σε κάθε μια από τις επιλογές.

Είναι σημαντικό να σημειωθεί πως για τεχνικούς λόγους, οι οποίοι εξηγούνται σε επόμενο υποκεφάλαιο, 5.2.10. *Περιορισμός επιλογών*, στη συγκεκριμένη ανάλυση και υλοποίηση επιλέγεται το σύστημα δυαδικής επιλογής ΝΑΙ – ΟΧΙ στο σύστημα κωδικοποίησης που περιγράφεται παραπάνω.

Ψήφος

Η ψήφος που κατοχυρώνει ένας ψηφοφόρος συνδυάζει τις ακόλουθες πληροφορίες:

- **Επιλογή**

Η διαλεγμένη από τις διαθέσιμες επιλογή, κρυπτογραφημένη πάντα με κλειδί το οποίο μπορεί να παράξει μόνο ο ίδιος ο ψηφοφόρος. Ο αλγόριθμος κρυπτογράφησης που χρησιμοποιείται είναι προκαθορισμένος και τέτοιος ώστε να έχει αθροιστικές ομομορφικές ιδιότητες.

- **Αποδεικτικό εγκυρότητας επιλογής**

Μαζί με την κρυπτογραφημένη επιλογή χρειάζεται να δοθεί και ένα αποδεικτικό στοιχείο για την πραγματική τιμή (plaintext value) που περιέχει το κρυπτοκείμενο. Ο στόχος εδώ είναι ο ψηφοφόρος να μπορεί να αποδείξει πως η ψήφος που έχει καταθέσει είναι έγκυρη και μια από τις διαθέσιμες τιμές, χωρίς όμως να αποκαλύψει ακριβώς την επιλεγμένη τιμή. Η απόδειξη επιτυγχάνεται με ένα non-interactive proof of value το οποίο δίνει τη δυνατότητα στους υπόλοιπους χρήστες, χωρίς να έρθουν σε επαφή με τον ψηφοφόρο, να σιγουρευτούν για την εγκυρότητα της επιλογής που περιέχεται στο κρυπτοκείμενο [22].

- **Αναγνωριστικό ψηφοφόρου**

Το αναγνωριστικό του ψηφοφόρου που περιγράφεται και παραπάνω. Ταυτοποιεί την ψήφο και δίνει τη δυνατότητα επιβεβαίωσης στοιχείων όπως το ότι ο ψηφοφόρος συμμετείχε στην ψηφοφορία, ότι δεν υπέβαλε περισσότερες ψήφους από τις επιτρεπτές καθώς και ότι ανήκει στη λίστα με αυτούς που τους επιτρέπεται να συμμετάσχουν.

- **Ψηφιακή υπογραφή ψήφου**

Ένα αλφαριθμητικό το οποίο παράγεται από τα στοιχεία της ψήφου σε συνδυασμό με το κρυφό κλειδί που συνοδεύει το δημόσιο αναγνωριστικό ψηφοφόρου. Η ψηφιακή υπογραφή, όταν περάσει από επιβεβαίωση με το δημόσιο κλειδί ψηφοφόρου, επιτρέπει την επιβεβαίωση πως τα περιεχόμενα της ψήφου έχουν δημιουργηθεί και σφραγιστεί από τον ίδιο τον ψηφοφόρο.

5.1.2. Είσοδος στο σύστημα

Το πρώτο πράγμα που χρειάζεται ένας νέος κόμβος με το που συνδεθεί επιτυχώς στο σύστημα είναι να συγχρονίσει την τοπική του αλυσίδα με εκείνη του P2P δικτύου. Το βήμα αυτό είναι

απαραίτητο για να μπορέσει να συμμετάσχει στη διαδικασία επιβεβαίωσης ορθότητας των προσαρτημένων ομάδων. Συγχρονισμός της αλυσίδας είναι ουσιαστικά η επαναδημιουργία, τοπικά, όλων των ομάδων που έχουν δημοσιευτεί στο δίκτυο. Αυτό επιτυγχάνεται με την υποβολή αιτημάτων σε 3^{ους} χρήστες του δικτύου με στόχο την ανακάλυψη αγνοούμενων ομάδων. Σημειώνεται πως η διαδικασία συγχρονισμού δεν είναι μόνο για πρωτοσυνδεόμενους χρήστες αλλά και για χρήστες οι οποίοι επανασυνδέονται μετά από μεγάλο χρονικό διάστημα.

Ο κόμβος που συγχρονίζεται, εκκινεί τη διαδικασία στέλνοντας ένα μήνυμα συγχρονισμού το οποίο περιέχει την ομάδα κεφαλής που γνωρίζει (δηλαδή την τελευταία ομάδα της καλύτερης τοπικής αλυσίδας του). Στην περίπτωση νέου κόμβου η μοναδική γνωστή του ομάδα είναι η ομάδα γένεσις. Οι 3^{οι} κόμβοι που δέχονται τα αιτήματα, απαντούν με λίστες ομάδων της δικής τους αλυσίδας μέχρι και την δική τους ομάδα κεφαλής η οποία, εάν οι κόμβοι είναι συγχρονισμένοι με την τελευταία μορφή της αλυσίδας, θα είναι και η τελευταία ομάδα που θα χρειαστεί. Από το σημείο αυτό και μετά ο (νέος) κόμβος είναι έτοιμος να δεχτεί νέες ομάδες προς επιβεβαίωση και προσάρτηση.

Η διαδικασία συγχρονισμού εκκινείται αυτόματα με το άνοιγμα της εφαρμογής, χωρίς την ανάγκη παρεμβολής του χρήστη.

5.1.3. Δημιουργία ψηφοφορίας

Η διαδικασία δημιουργίας ψηφοφορίας εκφράζεται μέσα από την παραμετροποίηση των βασικών παραμέτρων του μοντέλου του συστήματος, συγκεκριμένα της λίστας ψηφοφόρων, των διαθέσιμων επιλογών για τη συγκεκριμένη ψηφοφορία, του τίτλου και της περιόδου διάρκειας αυτής. Κάθε φορά που μια νέα ψηφοφορία πρέπει να λάβει μέρος, ανακοινώνεται η μορφή του πρωτοκόλλου blockchain που θα ακολουθηθεί από τους συμμετέχοντες και προαιρετικά εκκινείται και μια νέα αλυσίδα. Στην περίπτωση του συστήματος ψηφοφορίας για φοιτητική συνέλευση, η παραμετροποίηση του πρωτοκόλλου γίνεται από την εφορευτική επιτροπή περί φοιτητικών συνελεύσεων, ενώ ανακοινώνεται σε κάποιο online ιστότοπο μέσω του οποίου μπορούν οι ψηφοφόροι – φοιτητές να συγχρονίσουν τις τοπικές εφαρμογές τους ώστε να λάβουν μέρος στην εκάστοτε ψηφοφορία.

5.1.4. Διαδικασία υποβολής ψήφου

Δημιουργία ψηφοδελτίου

Αφού ο ψηφοφόρος ορίσει την επιλογή του, την κρυπτογραφεί ομομορφικά παράγοντας το αντίστοιχο ciphertext και μαζί με το αποδεικτικό εγκυρότητας τιμής, τα υπογράφει με την προσωπική του ψηφιακή υπογραφή. Αυτή η τριπλέτα πληροφοριών μαζί με το δημόσιο αναγνωριστικό ψηφοφόρου, ομαδοποιείται σε ένα μήνυμα το οποίο αποτελεί το ψηφιακό του ψηφοδέλτιο.

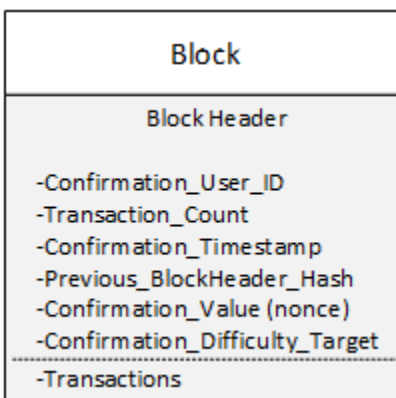
Δημοσιοποίηση ψηφοδελτίου

Η δημοσιοποίηση της ψήφου στους υπόλοιπους χρήστες γίνεται μέσω του peer-to-peer δικτύου πάνω στο οποίο λειτουργεί το σύστημα. Ο ψηφοφόρος ενημερώνει τους γνωστούς του κόμβους στέλνοντας ένα μήνυμα *συναλλαγής blockchain*, η οποία περιέχει και ψηφοδέλτιο. Αυτοί με τη σειρά τους ενημερώνουν τους δικούς τους γνωστούς, διαδίδοντας έτσι το μήνυμα ταχύτατα σε όλους τους συμμετέχοντες.

Δημιουργία ομάδας συναλλαγών ψηφοδελτίων (transaction block)

Η κάθε συναλλαγή που λαμβάνεται από χρήστες του συστήματος, πριν προστεθεί στην αλυσίδα πρέπει να επικυρωθεί με βάση τη διαδικασία που περιγράφεται στην παράγραφο *Μηχανισμός ομοφωνίας* του υποκεφαλαίου 4.1.3. Η επικύρωσή αυτή δεν γίνεται σε μεμονωμένες συναλλαγές άλλες σε μια ομάδα (block) αυτών. Η επικυρωμένη ομάδα αυτή αποτελεί και το νέο κρίκο που θα προσαρτηθεί στην αλυσίδα του blockchain. Η διαδικασία ομαδοποίησης αποτελεί μηχανισμό βελτιστοποίησης του συστήματος και του ρυθμού συναλλαγών που μπορεί να διαχειριστεί. Λόγω της χρονοβόρας διαδικασίας επικύρωσης που περιγράφηκε παραπάνω, η επεξεργασία μεμονωμένων συναλλαγών κρίνεται σπάταλη από πλευράς πόρων και προτιμάται η επεξεργασία μιας μεγάλης ομάδας αυτών.

Εκτός από τις συναλλαγές, μια ομάδα περιέχει και πολλές άλλες πληροφορίες που βοηθούν στη διαχείρισή της. Τα δύο βασικά χαρακτηριστικά όπως φαίνονται στο μοντέλο του σχήματος 10 είναι η κεφαλή (block header) και το σώμα.



Σχήμα 10: Μοντέλο ομάδας συναλλαγών

Το σώμα ουσιαστικά αποτελείται από τη λίστα των συναλλαγών ενώ η κεφαλή διαθέτει όλη τη μεταπληροφορία της ομάδας, συγκεκριμένα:

- **Μοναδικό αναγνωριστικό χρήστη επικύρωσης**

Οι ομάδες συναλλαγών δημιουργούνται και επικυρώνονται από οποιονδήποτε χρήστη του συστήματος. Ο χρήστης είναι υποχρεωμένος να προσθέσει ως στοιχείο αυτής το

μοναδικό αναγνωριστικό του για να μπορεί να αναγνωριστεί σε ποιον αποδίδεται η δημιουργία και επικύρωση της ομάδας.

- **Αριθμός συναλλαγών**

Κάθε block περιέχει πολλαπλές συναλλαγές. Ο αριθμός αυτών δεν είναι προκαθορισμένος αλλά πρέπει πάντα το συνολικό μέγεθος της πληροφορίας του block να πλησιάζει και να είναι μικρότερο από ένα προκαθορισμένο αριθμό byte. Η τιμή επιλέγεται κατά περίπτωση και συνήθως εξαρτάται από το μέσο δικτυακό bandwidth των αναμενόμενων χρηστών του συστήματος, πληρώντας πάντα τον ακόλουθο στόχο:

Το μέγεθος πληροφορίας της ομάδας συναλλαγών θα πρέπει να είναι τέτοιο ώστε ο πιο αργός χρήστης του συστήματος να προλαβαίνει να λάβει ολόκληρη την πληροφορία μιας καινούργιας ομάδας, σε χρόνο μικρότερο από το χρόνο δημιουργίας, επικύρωσης και προσάρτησής της στην αλυσίδα.

Εάν για παράδειγμα ο ρυθμός προσάρτησης ομάδας είναι κάθε 10 λεπτά και το μέγεθος είναι 1 gigabyte, ένας χρήστης ο οποίος στο P2P δίκτυο επικοινωνεί με ταχύτητα 1Mbps, δεν θα έχει προλάβει να λάβει όλη την πληροφορία στο χρονικό αυτό διάστημα. Όσο λοιπόν επεξεργάζεται την πληροφορία της πρώτης ομάδας, θα έχει ήδη δημοσιευτεί η επόμενη η οποία θα χρειαστεί αντίστοιχο χρόνο λήψης. Αυτό έχει ως αποτέλεσμα να μην μπορέσει ποτέ να συγχρονιστεί με την κεφαλή της αλυσίδας, αδυνατώντας έτσι να συμμετάσχει στο σύστημα.

Τυπικοί αριθμοί μεγέθους (block size) είναι 1MB (Bitcoin), 8MB (Bitcoin Cash), 2MB (ZCash). Υπάρχουν πολλά επιχειρήματα υπέρ και κατά μεγάλων ή μικρών μεγεθών ομάδας καθώς επιλέγοντας το μέγιστο δυνατό block size δεν δίνει πάντα βέλτιστο αποτέλεσμα. Αυτό εξαρτάται από πολλούς παράγοντες, όπως τις υπολογιστικές δυνατότητες των χρηστών του δικτύου, τη μέση ταχύτητα αυτού, τους στόχους των συναλλαγών ανά δευτερόλεπτο που πρέπει να επιτυγχάνονται και άλλα.

- **Χρονικό στιγμιότυπο δημιουργίας**

Κάθε ομάδα περιέχει και ένα χρονικό στιγμιότυπο δημιουργίας της. Στη δική μας περίπτωση πρόκειται για ένα UNIX στιγμιότυπο και ορίζεται από το δημιουργό και επικυρωτή της ομάδας συναλλαγών.

- **Στοιχείο επικύρωσης**

Κάθε ομάδα συναλλαγών περιέχει και το στοιχείο επικύρωσής της. Πρόκειται για έναν αριθμό ο οποίος παράγεται από το συνδυασμό των στοιχείων που χαρακτηρίζουν την ομάδα συναλλαγών, μαζί με ένα χαρακτηριστικό της προηγούμενης ομάδας της αλυσίδας, δένοντας έτσι τους κρίκους μεταξύ τους. Το δέσιμο αυτό είναι ένα πολύ σημαντικό χαρακτηριστικό διότι προστατεύει από την αλλοίωση παλαιότερων ομάδων

της αλυσίδας. Η προστασία προέρχεται από το γεγονός ότι για να προστεθεί, κακόβουλα, μια μη υπάρχουσα ομάδα συναλλαγών σε «παρελθοντική θέση» στην αλυσίδα, θα χρειαστεί να επανυπολογιστούν μαζί με το στοιχείο επικύρωσης της ομάδας και όλα τα στοιχεία επικύρωσης όλων των ομάδων μετά από αυτή. Χρονικά, αυτό το εγχείρημα είναι αδύνατο να επιτευχθεί από έναν ή μια μικρή ομάδα χρηστών, ενώ στατιστικά αρκεί το 51% να είναι έντιμοι χρήστες για να διασφαλιστεί η αξιοπιστία του συστήματος.

- **Χαρακτηριστικό προηγούμενης ομάδας**

Όπως αναφέρθηκε, προσθέτουμε και το χαρακτηριστικό της προηγούμενης ομάδας. Το χαρακτηριστικό στην περίπτωση μας είναι ένα αποτέλεσμα hash αλγορίθμου (SHA256) με εισόδους όλα τα στοιχεία της προηγούμενης ομάδας. Με αυτό τον τρόπο, δημιουργούμε ένα μοναδικό αλφαριθμητικό το οποίο εμπεριέχει κωδικοποιημένες τις συναλλαγές της προηγούμενης ομάδας, το στοιχείο επικύρωσής της καθώς και το χαρακτηριστικό της ακόμα προηγούμενης ομάδας, δένοντάς τες έτσι μέχρι και την πρώτη ομάδα στην αλυσίδα.

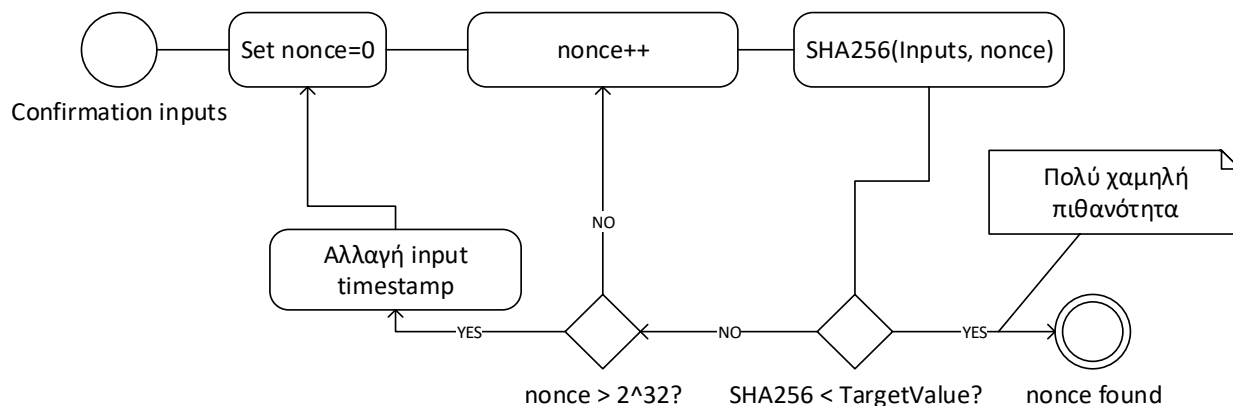
- **Δυσκολία – Στόχος επικύρωσης**

Ο ρυθμός επεξεργασίας και προσθήκης συναλλαγών στην αλυσίδα εξαρτάται κυρίως από το χρόνο επικύρωσης ομάδων συναλλαγών. Λόγω της φύσης της διαδικασίας επικύρωσης, είναι ευάλωτη σε αύξηση υπολογιστικής ισχύος του επικυρωτή. Για την αντιμετώπιση της αδυναμίας αυτής, η δυσκολία επικύρωσης είναι μεταβλητή. Όσο η ταχύτητα αυξάνεται τόσο αυξάνεται και η δυσκολία και αντίστροφα. Στην περίπτωση μας η δυσκολία αντιστοιχίζεται σε έναν αριθμό λεγόμενο στόχο και προστίθεται στην ομάδα συναλλαγών έτσι ώστε να μπορεί να επιβεβαιωθεί ότι το υπολογισμένο στοιχείο επικύρωσης πληροί τον αντίστοιχο στόχο που έχει τεθεί.

Επικύρωση ομάδας συναλλαγών

Η επικύρωση μιας ομάδας συναλλαγών μπορεί να γίνει από οποιονδήποτε χρήστη που λειτουργεί ως επικυρωτής. Όλες οι συναλλαγές που δημοσιοποιούνται και φτάνουν σε αυτόν ομαδοποιούνται με δική του ευχέρεια. Όταν μια ομάδα γεμίσει ξεκινάει η διαδικασία επικύρωσής της. Στην περίπτωση μας χρησιμοποιείται ένας αλγόριθμος τύπου proof of work (PoW) [23] βασισμένος στη μέθοδο Hashcash [24] όπως φαίνεται στο σχήμα 11. Ως εισοδοί δίνονται το μοναδικό αναγνωριστικό του χρήστη που εκτελεί την επικύρωση, οι συναλλαγές, το χρονικό στιγμιότυπο δημιουργίας της ομάδας, το χαρακτηριστικό της προηγούμενης ομάδας καθώς και η τιμή του στόχου δυσκολίας. Το στοιχείο επικύρωσης είναι η τελευταία είσοδος που δίνεται και είναι ένας αριθμός ο οποίος επιλέγεται από το χρήστη – επικυρωτή. Από όλα αυτά τα στοιχεία εισόδου παράγεται μια τιμή hash μέσω του αλγορίθμου SHA256. Ο σκοπός είναι η τιμή να είναι μικρότερη από την τιμή του στόχου δυσκολίας που έχει τεθεί. Με κάθε αποτυχία επιλέγεται μια άλλη τιμή μέχρι κάποια να καλύπτει την προϋπόθεση. Ένας απλός τρόπος παραγωγής στοιχείων επικύρωσης είναι η χρήση ενός αριθμού τύπου nonce ο οποίος αυξάνεται

με κάθε αποτυχία. Αν όλες οι πιθανές τιμές εξαντληθούν (έστω τιμή 32-bit), τότε ο επικυρωτής μπορεί να αλλάξει το χρονικό στιγμιότυπο που αναγράφεται στην ομάδα συναλλαγών και να ξαναπροσπαθήσει ξεκινώντας το στοιχείο επικύρωσης από το μηδέν.



Σχήμα 11: Διαδικασία επικύρωσης

Δημοσιοποίηση ομάδας συναλλαγών

Εφόσον η ομάδα έχει ολοκληρωθεί και περιέχει όλα τα στοιχεία που την καθιστούν έγκυρη, δημοσιοποιείται στο δίκτυο με τον ίδιο τρόπο που περιγράφηκε και για τις συναλλαγές. Είναι πιθανό να δημοσιοποιηθούν πολλές ομάδες συναλλαγών σε κοντινά χρονικά διαστήματα και λόγω του τρόπου με τον οποίο διαδίδονται είναι πολύ πιθανό διάφοροι χρήστες να λάβουν διαφορετικές επικυρωμένες ομάδες οι οποίες θα λάβουν την ίδια θέση στις αντίστοιχες αλυσίδες τους. Αυτό χαρακτηρίζεται ως διακλάδωση της αλυσίδας. Σε αυτή την περίπτωση, ο κάθε χρήστης συνεχίζει να προσαρτά επόμενες ομάδες στη δική του διακλάδωση ενώ ταυτόχρονα ενημερώνεται και για τις άλλες διακλαδώσεις. Με την πάροδο του χρόνου καταλήγει να έχει εικόνα για όλες τις διακλαδώσεις που έχουν δημιουργηθεί και σε αυτή την περίπτωση επιλέγει να συνεχίσει στη διακλάδωση που έχει τη μεγαλύτερη συσσωρευμένη δυσκολία επικύρωσης η οποία συνήθως ταυτίζεται με τη μακρύτερη διακλάδωση και είναι αυτή που έχει ακολουθήσει η πλειονότητα των χρηστών του συστήματος. Έτσι, παρ' ότι για κάποιο χρονικό διάστημα υπάρχει λανθασμένη αντίληψη των δεδομένων, το σύστημα αναπροσαρμόζεται και αυτοδιορθώνεται. Αυτό σημαίνει πως για να θεωρηθεί μια συναλλαγή ότι έχει όντως καταχωρηθεί, θα πρέπει η αλυσίδα να έχει προχωρήσει και να έχουν προσαρτιστεί επόμενες ομάδες έτσι ώστε να σιγουρευτούμε ότι η ομάδα της ανήκει στη μακρύτερη διακλάδωση.

Είναι σημαντικό να σημειωθεί ότι οι συναλλαγές που ανήκαν στην ομάδα η οποία προσαρτίστηκε σε διακλάδωση που δεν επιλέχθηκε δεν χάνονται. Κάθε συναλλαγή που έχει δημοσιοποιηθεί σημειώνεται από τους χρήστες επικυρωτές ώστε να μπει σε επόμενη ομάδα επικύρωσης. Συναλλαγές οι οποίες αναμένουν επικύρωση από ένα χρήστη επικυρωτή, αφαιρούνται μόνο αν κάποιος άλλος δημοσιεύσει επικυρωμένη ομάδα που τις περιέχει.

Σχετικά με την ασφάλεια του συστήματος από επιθέσεις άρνησης υπηρεσίας (DoS) με πλημμύρισμα με ψεύτικες συναλλαγές, κατά τη σύνθεση μιας ομάδας δίνεται προτεραιότητα σε συναλλαγές των οποίων τα μοναδικά αναγνωριστικά ψηφοφόρου δεν έχουν εκτελέσει προηγούμενες συναλλαγές και ουσιαστικά είναι η πρώτη τους ψήφος και όχι κάποια προσπάθεια αλλαγής της επιλογής τους.

Επιβεβαίωση και προσάρτηση ομάδας συναλλαγών

Κάθε επικυρωμένη ομάδα συναλλαγών που δημοσιοποιείται λαμβάνεται από τους υπόλοιπους χρήστες του συστήματος με σκοπό την προσάρτησή της στις τοπικές αλυσίδες τους. Για να γίνει όμως αυτό χρειάζεται πρώτα η ομάδα να περάσει από τη διαδικασία επιβεβαίωσης της ορθότητάς της με βάση τους κανόνες του πρωτοκόλλου. Εκτός από το βασικό έλεγχο πληρότητας των απαραίτητων στοιχείων της ομάδας, ακολουθούν οι έλεγχοι εγκυρότητας του στοιχείου επικύρωσης καθώς και της κάθε συναλλαγής που περιέχει.

Όσον αφορά το στοιχείο επικύρωσης, ο έλεγχος είναι πολύ απλός και ταχύτατος διότι ουσιαστικά εκτελείται ξανά ο αλγόριθμος SHA256 μόνο που σε αυτή την περίπτωση είναι γνωστές όλες οι είσοδοι και απλώς ελέγχεται αν το αποτέλεσμα είναι όντως μικρότερο από το στόχο δυσκολίας που έχει οριστεί από το σύστημα και αναφέρεται στην ομάδα.

Σχετικά με τις συναλλαγές, κάθε μια από αυτές αναλύεται και ελέγχεται αν ο ψηφοφόρος που την εκτέλεσε έχει δικαίωμα ψήφου καθώς και αν η υπογραφή που συνοδεύει τη συναλλαγή επιβεβαιώνεται με το μοναδικό αναγνωριστικό – δημόσιο κλειδί αυτού. Επίσης ελέγχεται η εγκυρότητα της κρυπτογραφημένης τιμής της ψήφου χρησιμοποιώντας το non-interactive proof of value που συνοδεύει την ψήφο.

Τέλος ελέγχεται αν η ομάδα συναλλαγών έχει δηλωθεί για προσάρτηση εντός του χρονικού περιθωρίου που έχει οριστεί για την ψηφοφορία, λαμβάνοντας πάντα υπόψη ασυγχρονισμούς συστημάτων καθώς και καθυστερήσεις μετάδοσης και διάδοσης των μηνυμάτων.

Εάν οποιοσδήποτε από τους ελέγχους βρεθεί άκυρος τότε η ομάδα συναλλαγών δεν προστίθεται στην αλυσίδα του χρήστη και απορρίπτεται. Αυτό αντικατοπτρίζεται από όλους τους χρήστες του συστήματος και συνεπώς παραμένουν συγχρονισμένες οι αλυσίδες τους.

Πρωταρχική ομάδα συναλλαγών – ομάδα γένεσις

Όπως εξηγήθηκε και στις προηγούμενες παραγράφους, κάθε ομάδα που είναι να προσαρτηθεί στην αλυσίδα είναι απαραίτητο να δεθεί με την προηγούμενή της προσθέτοντας το χαρακτηριστικό της κεφαλής της ως μεταπληροφορία της δικής της κεφαλής. Δημιουργείται συνεπώς το ερώτημα του πώς δημιουργείται η πρώτη ομάδα του συστήματος, μιας και δεν έχει κάποιο πρόγονο με τον οποίο μπορεί να δεθεί. Για να λυθεί το πρόβλημα χρησιμοποιείται μια ειδική ομάδα ονόματι ομάδα γένεσις (genesis block) η οποία είναι στατικά καταγεγραμμένη στον κώδικα της εφαρμογής, καθιστώντας την γνωστή σε όλους τους χρήστες. Η αλυσίδα

χτίζεται πάνω της ενώ ταυτόχρονα αποτελεί κοινό σημείο αναφοράς για όλους τους κόμβους όταν χρειάζεται να συγχρονίσουν τις αλυσίδες τους για πρώτη φορά με το υπόλοιπο δίκτυο.

5.1.5. Καταμέτρηση ψήφων

Με το πέρας της χρονικής διάρκειας ψηφοφορίας, παύει η δυνατότητα υποβολής ψήφου και το σύστημα περνάει στη φάση εξαγωγής του αποτελέσματος. Το αποτέλεσμα προκύπτει από το άθροισμα των τιμών κωδικοποίησης των υποβληθέντων ψήφων. Λόγω της κρυπτογραφημένης μορφής των επιλογών στα ψηφοδέλτια, χρειάζονται τα εξής βήματα για να λάβουμε το τελικό αποτέλεσμα:

1. Παραγωγή κρυπτογραφημένου αθροίσματος ψήφων

Έχοντας ο κάθε χρήστης διαθέσιμη την ολοκληρωμένη εικόνα της αλυσίδας, μπορεί να εκτελέσει τη διαδικασία της καταμέτρησης των ψήφων τοπικά. Αφού προσπελάσει την κάθε συναλλαγή και συγκεντρώσει τις έγκυρες ψήφους, εξάγει τις κρυπτογραφημένες επιλογές. Με αυτές, εκτελεί μια αθροιστική πράξη έτσι ώστε να παράξει ένα νέο κρυπτοκείμενο το οποίο αντιστοιχεί στο άθροισμα των τιμών κωδικοποίησης των ψήφων. Παρ' ότι σε αυτή τη φάση έχουμε διαθέσιμο το άθροισμα των ψήφων, παραμένει σε μορφή κρυπτοκειμένου. Για να αποκρυπτογραφηθεί η τελική τιμή απαιτείται ένα οικουμενικό κλειδί αποκρυπτογράφησης το οποίο θα προέρχεται από όλα τα επιμέρους κλειδιά που χρησιμοποιήθηκαν για την κρυπτογράφηση της εκάστοτε επιλογής που έχει συμπεριληφθεί στο αθροιστικό κρυπτοκείμενο.

Παράδειγμα:

Key	Plaintext	Ciphertext	
A	1	5	
B	-1	8	
C	-1	2	
D	-1	3	
ABCD	-2	18	SUM

2. Δημιουργία οικουμενικού κλειδιού αποκρυπτογράφησης

Η δημιουργία του οικουμενικού κλειδιού αποκρυπτογράφησης γίνεται με την εκτέλεση ενός αθροίσματος πολλαπλών μερών (multi-party computation - MPC). Όροι του αθροίσματος είναι τα επιμέρους κλειδιά του κάθε ψηφοφόρου τα οποία συνδυάζονται

χωρίς όμως να αποκαλυφθούν πλήρως στους υπόλοιπους συμμετέχοντες του υπολογισμού. Όπως έχει εξηγηθεί στην παράγραφο 4.3.4. *Ασφαλής υπολογισμός πολλαπλών μερών*, ο κάθε ψηφοφόρος θα πρέπει να στείλει μια τιμή σε κάθε συμμετέχοντα στον υπολογισμό. Οι τιμές αυτές πρέπει να αποσταλούν με τρόπο που μόνο ο προοριζόμενος παραλήπτης τους να μπορεί να τις διαβάσει. Η διαδικασία του υπολογισμού πολλαπλών μερών μπορεί να εκκινηθεί μετά τη λήξη της υποβολής ψήφων, ή μπορούν οι τιμές του κάθε ψηφοφόρου να δημοσιεύονται μαζί με την ψήφο ως κομμάτι της blockchain συναλλαγής.

3. Αποκρυπτογράφηση κρυπτοκειμένου αθροίσματος ψήφων

Έχοντας το τελικό κλειδί, ο κάθε χρήστης εκτελεί την αποκρυπτογράφηση στο κρυπτοκείμενο που παρήγαγε στο πρώτο βήμα και λαμβάνει το αποτέλεσμα της ψηφοφορίας.

Η διαδικασία καταμέτρησης εκκινείται αυτόματα με τη λήξη της ψηφοφορίας. Το άθροισμα των τιμών των ψήφων παράγεται υπολογιστικά, μέσω προσπέλασης των υποβληθέντων ψηφοδελτίων στις συναλλαγές του blockchain και προβάλλεται στο χρήστη μόλις γίνει διαθέσιμο.

5.1.6. Συντήρηση συστήματος

Όπως αναφέρθηκε στο προηγούμενο κεφάλαιο, τα blockchain συστήματα απαιτούν τη συμμετοχή των κόμβων για τη συντήρησή τους, μέσω της επικύρωσης των ομάδων συναλλαγών. Η διαδικασία επικύρωσης, εκτός από χρονοβόρα είναι και κοστοβόρα όσον αφορά την κατανάλωση υπολογιστικής ισχύος, κάτι που μεταφράζεται σε ενεργειακό κόστος σε μορφή ρεύματος. Για να συμμετέχουν συνεπώς οι χρήστες στη διαδικασία συντήρησης συνήθως δίνονται κάποια κίνητρα. Ανάλογα με το use case για το οποίο χρησιμοποιείται το σύστημα, η υπεύθυνη αρχή μπορεί να δημιουργήσει αντίστοιχα κίνητρα για τους χρήστες της. Για παράδειγμα στην περίπτωση της χρήσης του σε κρατικές ή δημοτικές εκλογές, θα μπορούσε το κίνητρο να έχει κάποια μορφή φοροαπαλλαγής η οποία θα βασιζόταν στον αριθμό επικυρωμένων block του κάθε κόμβου.

5.2. Τεχνική υλοποίηση

Με βάση το παραπάνω πρωτόκολλο, μπορούμε να περάσουμε σε μια περιγραφή των τεχνικών χαρακτηριστικών της υλοποίησης ενός τέτοιου συστήματος. Οι επιλεγμένοι αλγόριθμοι, κρυπτοσυστήματα και τεχνικές, έχουν παρουσιαστεί στο κεφάλαιο των θεωρητικών εννοιών ενώ σε αυτή την ενότητα αναλύουμε τους τρόπους εκμετάλλευσής τους για την εξυπηρέτηση των αναγκών του συστήματος. Παρ' ότι ένα μεγάλο κομμάτι αυτού αποτελεί το blockchain πρωτόκολλο, κάποιες από τις δραστηριότητες και διαδικασίες που παρουσιάστηκαν παραπάνω χρήζουν τεχνικής ανάλυσης όσον αφορά τον τρόπο υλοποίησής τους και σε αυτές θα επικεντρωθούμε στο υποκεφάλαιο αυτό.

5.2.1. Εισαγωγή κόμβου στο σύστημα

Όταν ένας ολοκαίνουριος χρήστης επιθυμεί να συνδεθεί στο δίκτυο για πρώτη φορά, εκτελούνται οι ακόλουθες ενέργειες:

1) Λήψη και εγκατάσταση client εφαρμογής

Το πρωτόκολλο δεν απαιτεί τη χρήση συγκεκριμένου ή εγκεκριμένου λογισμικού, συνίσταται παρ' όλα αυτά η χρήση της επίσημης και ανοιχτού κώδικα υλοποίησης αναφοράς. Αυτό έχει δύο σκοπούς:

- a) Το σύστημα να είναι ανεξάρτητο του λογισμικού κάτι το οποίο επιτρέπει δυνητικά στον οποιονδήποτε να δημιουργήσει μια δική του εφαρμογή σε περίπτωση που κρίνει ότι η υπάρχουσα λύση δεν τον καλύπτει. Επίσης, σε περίπτωση που η υπάρχουσα λύση αποσυρθεί, παρ' ότι θα χρειαστεί να επενδυθεί χρόνος για τη δημιουργία μιας καινούριας, το σύστημα δεν θα κλειδωθεί ανεπανόρθωτα.
- b) Η βασική υλοποίηση αναφοράς είναι ανοιχτή και ο πηγαίος κώδικας διαθέσιμος σε όλους έτσι ώστε να επιτρέπεται και να ενθαρρύνεται ο εξονυχιστικός έλεγχος, η κρίση των σχεδιαστικών επιλογών και η διόρθωση προβλημάτων και ελλείψεων, όχι μόνο από τους αρχικούς δημιουργούς του συστήματος αλλά και από την υπόλοιπη εξειδικευμένη κοινότητα. Επικεντρώνοντας πόρους σε συγκεκριμένο λογισμικό, επιτυγχάνεται ο έλεγχος αυτού με γρήγορους ρυθμούς και δημιουργείται ένα θωρακισμένο σύστημα, εγκεκριμένο όχι μόνο από κάποια οργάνωση (δημόσια ή ιδιωτική) αλλά και από την ευρύτερη κοινότητα ειδικών, αφαιρώντας έτσι ένα πιθανό single point of failure.

2) Σύνδεση με κόμβους είτε μέσω IP είτε μέσω DNS query

Θυμίζουμε ότι το δίκτυο, λόγω της peer to peer φύσης του, δεν έχει συγκεκριμένη δομή ούτε υπάρχει κάποιος σταθερός εξυπηρετητής που θα μπορεί να εισαγάγει ένα νέο κόμβο στο σύστημα. Όπως περιγράψαμε λοιπόν και στο κεφάλαιο *Λειτουργίες ενός Blockchain – Σύνδεση στο σύστημα* η λύση που έχει δοθεί για την αρχική επικοινωνία του χρήστη με άλλους συμμετέχοντες είναι είτε να υπάρχουν κάποιοι σταθεροί (γνωστοί προ της σύνδεσης) κόμβοι είτε να δημιουργηθούν κάποιοι σταθεροί DNS κόμβοι οι οποίοι απαντούν σε ερωτήματα με τις IP διευθύνσεις εγγεγραμμένων κόμβων.

3) Αποστολή μηνύματος δήλωσης συμμετοχής και αίτημα για γνωστοποίηση διευθύνσεων υπολοίπων κόμβων

Όταν βρεθεί κάποιος κόμβος (peer) που συμμετέχει στο σύστημα, στην πρώτη επικοινωνία αποστέλλεται ένα μήνυμα που δηλώνει την εμφάνιση του καινούριου κόμβου. Ο παραλήπτης αμέσως ενημερώνει τους υπόλοιπους γνωστούς του κόμβους για την ύπαρξη του αποστολέα ενώ ταυτόχρονα απαντά σε αυτόν με μια λίστα διευθύνσεων των συμμετεχόντων για τους οποίους έχει επίγνωση. Με αυτόν τον τρόπο επιτυγχάνεται ταχύτατη εισαγωγή νέου κόμβου στο σύστημα και χωρίς να χρειαστεί κάποια παραμετροποίηση ή άλλη ενέργεια από αυτόν.

4) Επικοινωνία με peers για τη λήψη των ομάδων που αποτελούν την αλυσίδα του συστήματος

Μετά την επιτυχημένη εισαγωγή ενός νέου κόμβου στο σύστημα το πρώτο πράγμα που χρειάζεται για να ξεκινήσει να συμμετέχει κανονικά είναι η λήψη και αποθήκευση ολόκληρης της μορφής της αλυσίδας, έτσι ώστε να μπορεί να δημιουργεί ή να λαμβάνει νέες προσαρτώμενες ομάδες, να τις ελέγχει και να τις προωθεί και στους υπόλοιπους αιτούντες. Για να επιτευχθεί αυτό, αποστέλλονται στους υπόλοιπους peers μηνύματα αίτησης για τη λήψη υπαρχόντων ομάδων.

5.2.2. Συμμετοχή σε νέα ψηφοφορία και λήψη στοιχείων αυτής

Κάθε νέα ψηφοφορία εκφράζεται ως αλλαγή του πρωτοκόλλου του συστήματος blockchain. Τα βασικά στοιχεία που αλλάζουν είναι ο τίτλος, το διάστημα διεξαγωγής αυτής και πιθανώς η λίστα ψηφοφόρων. Επιπλέον, παρ' ότι στην παρούσα υλοποίηση οι διαθέσιμες επιλογές παραμένουν σταθερές (ΝΑΙ – ΟΧΙ), ανάλογα με τον τύπο του συστήματος μπορεί να υποστηρίζονται και αλλαγές και στη λίστα των διαθέσιμων επιλογών όπως π.χ. ονόματα υποψηφίων.

Το πρωτόκολλο, όντας στατικό και εφαρμόσιμο απευθείας μέσω του κώδικα της εφαρμογής ψηφοφορίας, όταν χρειάζεται να ανανεωθεί ουσιαστικά επανυλοποιείται ο κώδικας και οι χρήστες λαμβάνουν την ενημερωμένη έκδοση που περιέχει τις αλλαγές. Για την απλοποίηση της διαδικασίας η διάθεση της ανανέωσης πρέπει να γίνεται μέσω κάποιας μορφής αυτοματοποιημένης αναβάθμισης όπως για παράδειγμα ένα “over the air” (OTA) update στην εκάστοτε συσκευή που χρησιμοποιείται.

5.2.3. Μοναδικό αναγνωριστικό ψηφοφόρου

Όπως έχει αναφερθεί παραπάνω, κάθε ψηφοφόρος ταυτοποιείται στο σύστημα μέσω ενός μοναδικού αναγνωριστικού. Η τιμή αυτού παράγεται από τον ίδιο τον ψηφοφόρο με συγκεκριμένο τρόπο και δηλώνεται στην υπεύθυνη αρχή διαχείρισης του συστήματος ψηφοφορίας. Υπενθυμίζεται πως το δημόσιο αναγνωριστικό αποτελεί ταυτόχρονα και το δημόσιο κλειδί ενός ζεύγους Δημοσίου-Κρυφού κλειδιού (με το κρυφό κλειδί να παραμένει γνωστό μόνο στον ίδιο τον ψηφοφόρο).

Η δυνατότητα ταυτοποίησης των ψηφοφόρων με τον παραπάνω τρόπο προσφέρει τα εξής πλεονεκτήματα:

- Επιτρέπει τον έλεγχο της προέλευσης των ψηφοφόρων. Προσθέτοντας στο πρωτόκολλο του blockchain τη λίστα με τα αναγνωριστικά μπορούμε να περιορίσουμε τις έγκυρες συναλλαγές μόνο στους χρήστες οι οποίοι είναι δηλωμένοι και εγκεκριμένοι. Επιπλέον μπορούμε να αναγνωρίσουμε κακόβουλες ψήφους από κόμβους προσπαθούν να υποδυθούν τρίτους ψηφοφόρους.
- Επιτρέπει ελέγχους στις ψήφους. Συνοδεύοντας την κάθε ψήφο με το αναγνωριστικό του ψηφοφόρου που τη δημιούργησε μπορούμε να ελέγξουμε:

1. Εάν ο χρήστης υπέβαλλε ή όχι ψήφο.
2. Ότι ο χρήστης δεν έχει υποβάλει πάνω από μια ψήφο ή εάν έχει μπορούμε να τις διακρίνουμε και να επιλέξουμε μια από αυτές, ανάλογα με το τι ορίζει το πρωτόκολλο.

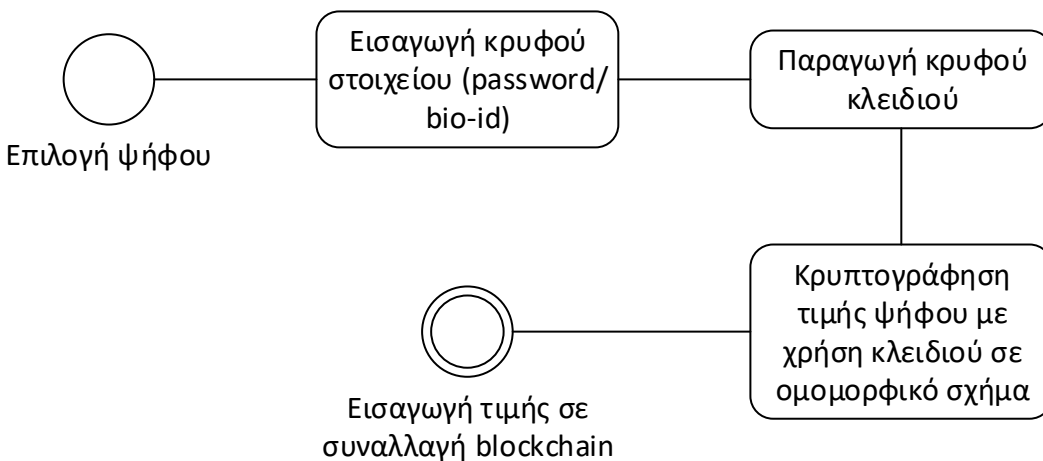
Για την παραγωγή του μοναδικού αναγνωριστικού, χρησιμοποιείται ένας αλγόριθμος παραγωγής Δημοσίου-Κρυφού κλειδιού στον οποίο δίνεται ως είσοδος (seed) μια τιμή, η αναπαραγωγή της οποίας θα πρέπει να είναι εύκολη για τον ψηφοφόρο αλλά αδύνατη για οποιονδήποτε άλλο. Πιθανές τέτοιες τιμές είναι οι εξής:

- Αλφαριθμητικό σε μορφή κωδικού πρόσβασης ή φράσης πρόσβασης. Αυτή είναι η απλούστερη μορφή εισόδου και έχει αποδειχθεί πως αν είναι αρκετά πολύπλοκη (π.χ. > 100 bit) είναι ουσιαστικά αδύνατη η ανάκτησή της με μεθόδους brute force. Το μειονέκτημα αυτής της προσέγγισης είναι πως η δυνατότητα ψήφου μπορεί να μεταφερθεί σε τρίτο χρήστη (κάποιες φορές και χωρίς τη βούληση του ιδιοκτήτη του κωδικού πρόσβασης), δίνοντάς του έτσι τη δυνατότητα να υποδυθεί τον ψηφοφόρο, ακυρώνοντας έτσι την ακεραιότητα του συστήματος.
- Τιμή παραγόμενη από βιομετρικές εισόδους όπως δακτυλικό αποτύπωμα, αμφιβληστροειδική σάρωση ή σάρωση προσώπου. Το πλεονέκτημα αυτής της προσέγγισης είναι πως δεν μπορεί εύκολα να μεταφερθεί σε κάποιον άλλο χρήστη και χρειάζεται την ενεργή παρουσία του ιδιοκτήτη κατά τη διάρκεια της υποβολής ψήφου, κάτι που αρμόζει στις προδιαγραφές των τωρινών συστημάτων. Μειονεκτήματα είναι η ανάγκη χρήσης εξειδικευμένου εξοπλισμού για την αναγνώριση βιομετρικών χαρακτηριστικών (όπως π.χ. smartphone που υποστηρίζει αντίστοιχες λειτουργίες), η αδυναμία αλλαγής της βιομετρικής τιμής καθώς και η πιθανότητα να εκβιαστεί η χρήση της από τρίτους ακόμα και χωρίς τη βούληση του χρήστη. Το κυριότερο όμως μειονέκτημα είναι πως αυτή τη στιγμή δεν έχει ακόμα δημιουργηθεί μια μέθοδος βιοαναγνώρισης που να μην είναι πιθανοτική. Αυτό έχει ως αποτέλεσμα να είναι αδύνατο για ένα βιομετρικό σύστημα να παράξει ντετερμινιστικές τιμές εξόδου, καθιστώντας τα μη εκμεταλλεύσιμα για το συγκεκριμένο σκοπό. Παρ' όλα αυτά εξετάζουμε τη χρησιμότητά της για την περίπτωση που μελλοντικά λυθεί το παραπάνω πρόβλημα.
- Ανακλητά βιομετρικά. Αποτελούν νέο τομέα έρευνας και ενώ λειτουργούν όπως περιγράφηκαν στην προηγούμενη παράγραφο, επιτρέπουν ανάκληση της τιμής τους. Αυτό δίνει τη δυνατότητα στο χρήστη να αναλάβει την κυριότητα της ψήφου του ανά πάσα στιγμή, ακόμα και αν η βιομετρική τιμή έχει παραβιαστεί από τρίτους.

5.2.4. Υποβολή ψήφου

Όταν ο χρήστης είναι έτοιμος να υποβάλει την ψήφο του στο σύστημα, ακολουθείται η διαδικασία του διαγράμματος του σχήματος 12 με τα εξής βήματα:

- Ο χρήστης διαλέγει από τις διαθέσιμες επιλογές.
- Εισάγει το κρυφό του στοιχείο.
- Με βάση το κρυφό στοιχείο παράγεται ένα κρυφό κλειδί καθαρά για την κρυπτογράφηση της ψήφου.
- Με το κλειδί αυτό γίνεται η κρυπτογράφηση της επιλογής.
- Η κρυπτογραφημένη επιλογή πακετάρεται μαζί με άλλα μεταδεδομένα σε μια συναλλαγή και δημοσιοποιείται στο δίκτυο.



Σχήμα 12: Activity diagram υποβολής ψήφου

5.2.5. Αλγόριθμος κρυπτογράφησης ψήφου

Όπως έχει αναφερθεί, η επιλογή/ψήφος του κάθε ψηφοφόρου δημοσιοποιείται σε μια blockchain συναλλαγή σε κρυπτογραφημένη μορφή. Το κρυπτοσύστημα το οποίο θα χρησιμοποιηθεί στην υλοποίηση που περιγράφεται είναι απαραίτητο να έχει αθροιστική ομομορφική ιδιότητα, δηλαδή να μπορεί να εφαρμοστεί μία πράξη πάνω σε κρυπτοκείμενα και το αποτέλεσμα αυτής, όταν αποκρυπτογραφηθεί, να αντιστοιχίζεται στο άθροισμα των επιμέρους αριθμητικών αναπαραστάσεων αυτών. Για παράδειγμα, έχοντας δύο πιθανές επιλογές:

- NAI = 1
- ΟΧΙ = -1

και έχοντας 3 χρήστες, ο καθένας με το δικό του κρυφό κλειδί, θα πρέπει να παράξουν όλοι μεταξύ τους ξεχωριστά κρυπτοκείμενα (σε δεκαεξαδική μορφή), έστω

1. NAI (1) → 0xb6cacb96ac9accd
2. NAI (1) → 0xa3cb45a7da458ca

3. OXI (-1) → 0xbc0d65bd3a4dc8

Το άθροισμα των κρυπτοκειμένων μας δίνει την τιμή

$$0xb6cacb96ac9accd + 0xa3cb45a7da458ca + 0xbc0d65bd3a4dc8 \\ = 0x16656e79a5a8535f$$

Αποκρυπτογραφώντας το άθροισμα θα πρέπει να αντιστοιχίζεται στην τιμή 1, το άθροισμα δηλαδή των plaintext τιμών

$$1 + 1 - 1 = 1$$

Εκμεταλλευόμενοι μία τέτοια ιδιότητα έχουμε τη δυνατότητα να παράξουμε ένα συνολικό αποτέλεσμα ψηφοφορίας από όλες τις ψήφους, χωρίς να χρειαστεί σε κανένα στιγμιότυπο της διαδικασίας να αποκρυπτογραφηθεί η οποιαδήποτε επιμέρους ψήφος, κάτι το οποίο θα έβαζε κίνδυνο τη μυστικότητα αυτής, ένα από τα βασικά στοιχεία που πρέπει να πληροί το σύστημα.

Το κρυπτόςστημα που χρησιμοποιούμε βασίζεται στο πρόβλημα δυσκολίας εύρεσης διακριτού λογαρίθμου και διαθέτει αθροιστικές ομομορφικές ιδιότητες. Οι τιμές αρχικοποίησης του συστήματος υπολογίζονται και ανακοινώνονται από την εφορευτική επιτροπή, διοργανωτή της διαδικασίας ψηφοφορίας και είναι κομμάτι του πρωτοκόλλου αυτού. Για τη συγκεκριμένη μέθοδο κρυπτογράφησης ορίζονται οι εξής τιμές αρχικοποίησης:

1. Κυκλική ομάδα O ($mod p$)
2. Ο ασφαλής πρώτος αριθμός p
3. Γεννήτρια g της ομάδας O
4. Δεύτερη γεννήτρια G της ομάδας O

Γνωρίζοντας λοιπόν τα παραπάνω, η διαδικασία κρυπτογράφησης της ψήφου ξεκινάει με την παραγωγή ενός κρυφού κλειδιού S . Με αυτό, ο ψηφοφόρος υπολογίζει την τιμή g^S . Επίσης υπολογίζει την τιμή G^M όπου M η κωδικοποιημένη τιμή της επιλογής του (π.χ. ΝΑΙ = 1). Τέλος υπολογίζεται το γινόμενο

$$g^S * G^M (mod p)$$

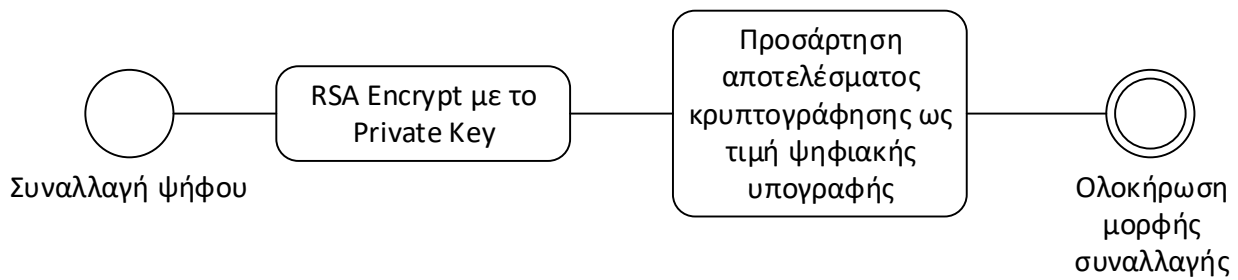
το οποίο αποτελεί το κρυπτοκείμενο που συμπεριλαμβάνεται στη blockchain συναλλαγή που διαδίδεται στο δίκτυο.

5.2.6. Ψηφιακή υπογραφή ψήφου

Όπως αναφέρθηκε παραπάνω, η συναλλαγή/ψήφος που κατατίθεται στο blockchain σύστημα περιέχει ως μεταπληροφορία και μια ψηφιακή υπογραφή όλου του μηνύματος, η οποία λειτουργεί ως εγγύηση για τον δημιουργό αυτού. Για τη δημιουργία και επιβεβαίωση ψηφιακών

υπογραφών χρησιμοποιείται ένα κρυπτοσύστημα ασύμμετρης κρυπτογραφίας όπως το RSA, το δημόσιο κλειδί του οποίου είναι ταυτόχρονα και το μοναδικό αναγνωριστικό ψηφοφόρου. Έχοντας αυτό στη διάθεσή του, όταν κληθεί από το σύστημα να υπογράψει τη συναλλαγή που περιέχει την ψήφο του, χρησιμοποιεί το κρυφό κλειδί και υπογράφει τα δεδομένα της blockchain συναλλαγής, προσθέτοντας σε αυτή και την τιμή της ψηφιακής υπογραφής όπως φαίνεται στο σχήμα 13. Εάν η υπογραφή που συνοδεύει το μήνυμα επιβεβαιώνεται με το δημόσιο κλειδί – αναγνωριστικό ψηφοφόρου τότε έχουμε εγγύηση ότι το μήνυμα δημιουργήθηκε και υπογράφηκε από αυτόν.

Η χρήση ψηφιακής υπογραφής για την επιβεβαίωση της προέλευσης των ψήφων είναι σημαντική διότι στο συγκεκριμένο σύστημα οποιοσδήποτε κόμβος μπορεί να δηλώσει μια συναλλαγή στο blockchain. Συνεπώς εάν δεν υπήρχε έλεγχος προέλευσης, οποιοσδήποτε χρήστης θα μπορούσε να δηλώσει ψευδείς συναλλαγές εκ μέρους άλλων ψηφοφόρων χωρίς καν να έχει λάβει το δικαίωμα αυτό.



Σχήμα 13: Ψηφιακή υπογραφή ψήφου

5.2.7. Παραγωγή κρυπτογραφημένου αποτελέσματος και τελικού συνόλου

Με τη λήξη της ψηφοφορίας, το σύστημα περνά στην επόμενη φάση για του τελικού αποτελέσματος. Για να γίνει αυτό χρειάζεται να υπολογιστεί το άθροισμα όλων των καταγεγραμμένων έγκυρων ψήφων. Ξεκινάμε με την ολική προσπέλαση της αλυσίδας όπου έχουν καταγραφεί όλες οι ψήφοι, διαβάζοντας μια μια τις ομάδες συναλλαγών. Από κάθε συναλλαγή, αφού ελεγχθεί και κριθεί έγκυρη, εξάγεται η κρυπτογραφημένη τιμή της καταχωρημένης ψήφου. Σε περίπτωση που βρεθούν παραπάνω συναλλαγές από τον ίδιο ψηφοφόρο, δηλαδή με το ίδιο μοναδικό αναγνωριστικό, απορρίπτονται. Κάθε εξαγόμενη τιμή συνδυάζεται με όλες τις προηγούμενες με τρόπο που θα μας επιτρέψει να λάβουμε το ομομορφικό άθροισμα αυτών. Με το πέρας της προσπέλασης της αλυσίδας ολοκληρώνεται η διαδικασία και έχουμε διαθέσιμο το, κρυπτογραφημένο μεν, σύνολο των ψήφων.

Παίρνοντας πάλι το παράδειγμα που δόθηκε στην προηγούμενη παράγραφο με τους 3 χρήστες, θα έχουμε τα εξής κρυπτοκείμενα:

1. $g^{s_1} * G^{M_1} \bmod p$
2. $g^{s_2} * G^{M_2} \bmod p$

3. $g^{s_3} * G^{M_3} \bmod p$

Για να παραχθεί το ομομορφικό τους άθροισμα ουσιαστικά χρειάζεται να πάρουμε το γινόμενο των κρυπτοκειμένων $\bmod p$

$$g^{x_1+x_2+x_3} * G^{M_1+M_2+M_3} \bmod p = C_{total}$$

Για να αποκρυπτογραφηθεί το C_{total} και να πάρουμε το πραγματικό τελικό αποτέλεσμα χρειάζεται να υπολογιστεί ένα συνολικό υπερκλειδί αποκρυπτογράφησης το οποίο θα προέρχεται από όλα τα κρυφά κλειδιά που έχουν χρησιμοποιηθεί για την παραγωγή των κρυπτοκειμένων των αντίστοιχων ψήφων. Στην περίπτωση αυτή το κλειδί θα πρέπει να είναι η τιμή

$$s_{all} = s_1 + s_2 + s_3$$

η οποία όταν οριστεί ως modular αρνητικός εκθέτης της τιμής C_{total} μας δίνει την τιμή

$$C_{total}^{-s_{all}} \bmod p = G^{M_1+M_2+M_3} \bmod p = G^{M_{all}} \bmod p$$

όπου M_{all} είναι το τελικό άθροισμα των ψήφων. Ο υπολογισμός το εκθέτη M_{all} γίνεται μέσω της πράξης λογαρίθμου $\log_G M_{all}$. Δυστυχώς όμως λόγω της υπόθεσης Diffie-Hellman δεν υπάρχει εύκολος τρόπος υπολογισμού διακριτού λογαρίθμου και για το λόγο αυτό, γνωρίζοντας ότι ο εκθέτης θα είναι σχετικά μικρός ($|M_{all}| \leq VotersCount$), ο υπολογισμός γίνεται με επαναλαμβανόμενες προσπάθειες υπολογισμού του g^i όπου

$$i \in [-VotersCount, VotersCount]$$

Αυτό επιτρέπει να ανακαλύψουμε την τιμή του M_{all} σχετικά γρήγορα, σε $O(n)$ πολυπλοκότητα.

Μία τεχνική επιτάχυνσης αυτής της διαδικασίας είναι ο προϋπολογισμός όλων των πιθανών τιμών G^i πριν την έναρξη της καταμέτρησης, μιας και η τιμή G είναι γνωστή εξ αρχής. Κάθε τιμή G^i που υπολογίζεται μπαίνει σε ένα look-up table μαζί με την τιμή i που της αντιστοιχεί. Ο πίνακας αυτός δημοσιοποιείται και έτσι ο κάθε χρήστης που υπολογίζει το τελικό αποτέλεσμα μπορεί άμεσα να βρει και την τιμή M_{all} που αντιστοιχεί.

5.2.8. Δημιουργία υπερκλειδιού αποκρυπτογράφησης αποτελέσματος

Για τη σωστή αποκρυπτογράφηση του τελικού αποτελέσματος απαιτείται η δημιουργία ενός υπερκλειδιού αποκρυπτογράφησης το οποίο αποτελείται από όλα τα κρυφά κλειδιά που έχουν χρησιμοποιηθεί στις κρυπτογραφημένες ψήφους οι οποίες ήταν κομμάτι του τελικού αθροίσματος. Λόγω της ανάγκης μυστικότητας της ψήφου, καθώς και της δημόσιας φύσης του ψηφοδέλτιου το οποίο καταγράφεται στην blockchain αλυσίδα, είναι απαραίτητο τα επιμέρους κομμάτια του υπερκλειδιού αποκρυπτογράφησης να παραμείνουν κρυφά από τρίτους. Καλούμαστε λοιπόν να δημιουργήσουμε ένα άθροισμα χωρίς τη γνωστοποίηση των επιμέρους τιμών αυτού.

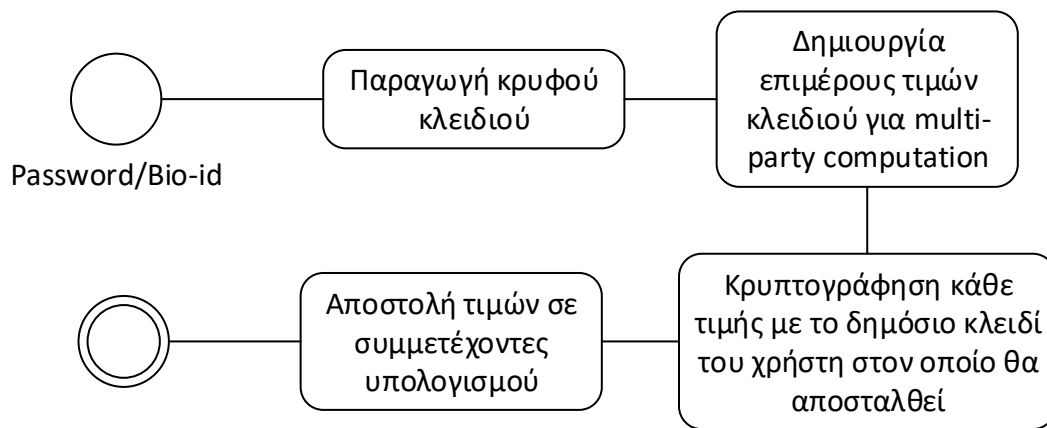
Τέτοια προβλήματα λύνονται μέσω secure multi-party computation (MPC). Για το σύστημα ψηφοφορίας χρησιμοποιούμε ένα σχήμα το οποίο βασίζεται σε μέθοδο secret sharing και συγκεκριμένα αυτή του Shamir (Shamir Secret Sharing). Όπως έχει εξηγηθεί σε προηγούμενο κεφάλαιο ο αλγόριθμος secret sharing μας επιτρέπει να διασπάσουμε μια μυστική τιμή σε επιμέρους τμήματα τα οποία μοιράζονται σε τρίτους χρήστες. Η δομή των τιμών αυτών είναι τέτοια ώστε να είναι αδύνατη η επαναδημιουργία της αρχικής κρυφής τιμής παρά μόνο αν συγκεντρωθούν από κάποιον όλα τα επιμέρους τμήματα. Επιπλέον, εκτός από το διαμοιρασμό και την επαναδημιουργία ενός μυστικού, ο αλγόριθμος του Shamir επιτρέπει και το διαμοιρασμό τμημάτων πολλών μυστικών καθώς και την επαναδημιουργία όχι ενός μυστικού αλλά ενός αποτελέσματος το οποίο προέρχεται από την εφαρμογή μιας αριθμητικής πράξης στις επιμέρους μυστικές τιμές. Μπορούμε συνεπώς να εκμεταλλευτούμε τον αλγόριθμο ως αθροιστικό multi-party computation σχήμα για την παραγωγή του υπερκλειδιού αποκρυπτογράφησης.

Σημειώνεται πως τα τμήματα στα οποία χωρίζεται κάθε μυστική τιμή είναι πολλά (π.χ. 200). Σκοπός αυτού είναι να εκμηδενίσει την πιθανότητα συνεργασίας χρηστών με σκοπό την ανάκτηση επιμέρους τιμών της MPC διαδικασίας. Η λογική αυτή είναι παρόμοια με εκείνη του blockchain συστήματος, βασισμένη στο γεγονός ότι σε ένα αρκετά μεγάλο αριθμό συμμετεχόντων οι κακοήθεις χρήστες θα είναι αισθητά λιγότεροι από τους καλοπροαίρετους. Εκμεταλλευόμενοι συνεπώς αλγορίθμους οι οποίοι απαιτούν τη συνεργασία πολλών αν όχι όλων των χρηστών μπορούμε ουσιαστικά να διασφαλίσουμε το σύστημα από τους λίγους αλλά υπαρκτούς επιτιθέμενους.

Το πρωτόκολλο ανάκτησης υπερκλειδιού αποτελείται από διάφορα στάδια τα οποία εκτελεί ο κάθε χρήστης σε συνεργασία με τους υπόλοιπους.

1. Παραγωγή και αποστολή επιμέρους τιμών MPC (Σχήμα 14)

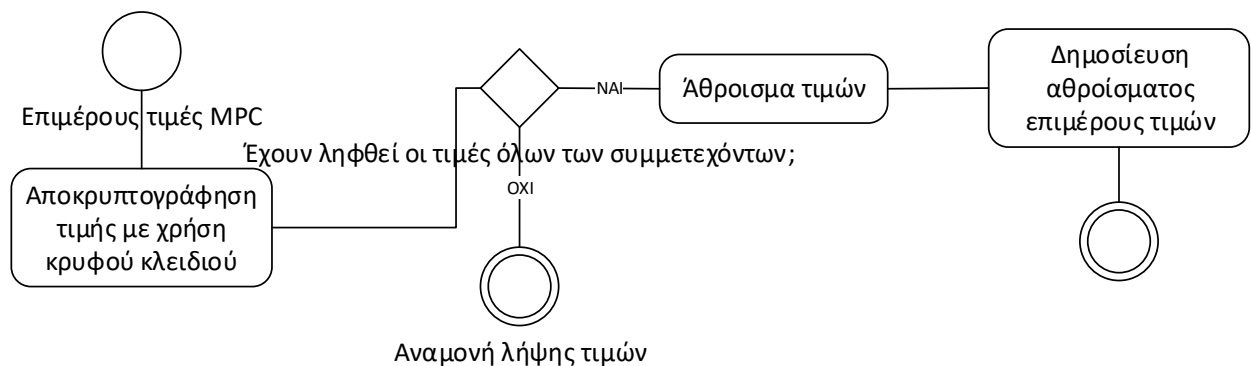
Το κρυφό κλειδί του χρήστη δίνεται σαν είσοδος στον αλγόριθμο Shamir από τον οποίο παράγονται οι επιμέρους τιμές που θα διαμοιραστούν στα μέλη της MPC διαδικασίας. Κάθε κομμάτι, πριν αποσταλεί, κρυπτογραφείται με το δημόσιο κλειδί του μέλους που θα το παραλάβει. Έτσι παραμένει κρυφό από οποιονδήποτε μπορεί να παρακολουθεί την επικοινωνία και επίσης μπορεί να αποκρυπτογραφηθεί μόνο από τον τελικό αποδέκτη.



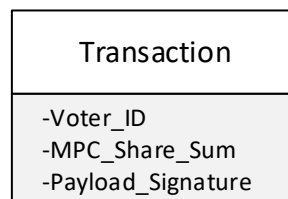
Σχήμα 14: Παραγωγή και αποστολή επιμέρους τιμών MPC

2. Συλλογή επιμέρους τιμών MPC (Σχήμα 15)

Ταυτόχρονα με την αποστολή των προσωπικών του τιμών για τον υπολογισμό υπερκλειδιού, ο χρήστης είναι υπεύθυνος να συλλέξει και τις αντίστοιχες τιμές που του αποστέλλουν οι υπόλοιποι συμμετέχοντες στη διαδικασία MPC. Όταν λάβει όλες τις επιμέρους τιμές από τους υπόλοιπους συμμετέχοντες τότε τις αθροίζει και το αποτέλεσμα το δημοσιεύει ως blockchain συναλλαγή με περιεχόμενο το μοντέλο του σχήματος 16



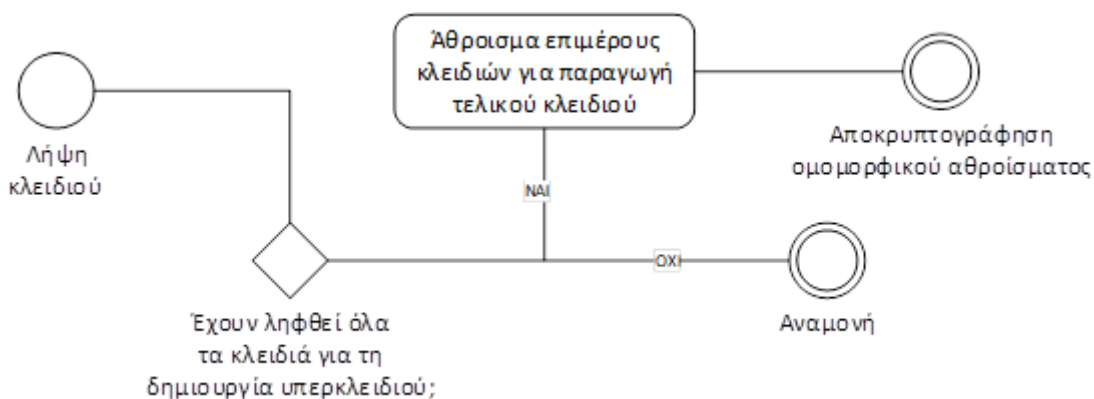
Σχήμα 15: Συλλογή επιμέρους τιμών MPC



Σχήμα 16: Μοντέλο συναλλαγής blockchain για το σύνολο των τιμών MPC

3. Υπολογισμός τελικού υπερκλειδίου (Σχήμα 17)

Τελευταίο βήμα είναι ουσιαστικά ο υπολογισμός του τελικού κλειδίου για την αποκρυπτογράφηση του ομομορφικού αθροίσματος. Όταν υπολογιστούν και δημοσιευθούν όλα τα αθροίσματα από τους MPC συμμετέχοντες, κάθε χρήστης πια έχει τη δυνατότητα να υπολογίσει το τελικό κλειδί και με αυτό να αποκρυπτογραφήσει το κρυπτοκείμενο που αντιστοιχεί στο άθροισμα των ψήφων. Είναι σημαντικό να σημειωθεί ότι το παραγόμενο υπερκλειδί είναι απαραίτητο να περιέχει όλα τα κλειδιά των χρηστών των οποίων οι ψήφοι έχουν συνυπολογιστεί στο τελικό αποτέλεσμα αλλιώς η αποκρυπτογράφηση αυτού καθίσταται αδύνατη. Παρ' όλα αυτά, αν κάποιος χρήστης αποφασίσει να μη συμμορφωθεί στο πρωτόκολλο παραγωγής υπερκλειδίου, το μόνο που χρειάζεται να γίνει είναι η ψήφος του να αφαιρεθεί από το ομομορφικό άθροισμα και ταυτόχρονα το κλειδί του δεν είναι πια απαραίτητο για την αποκρυπτογράφηση των ψήφων. Βλέπουμε συνεπώς ότι το σύστημα είναι ενισχυμένο ενάντια σε επιθέσεις μεμονωμένων χρηστών.



Σχήμα 17: Υπολογισμός τελικού υπερκλειδίου

5.2.9. Non-interactive proof ορθότητας ψήφου

Όπως έχει αναφερθεί παραπάνω, μαζί με την κρυπτογραφημένη ψήφο του ο χρήστης είναι υποχρεωμένος να παραθέσει και ένα αποδεικτικό στοιχείο της εγκυρότητας της τιμής που εμπεριέχεται στο κρυπτοκείμενο, στην περίπτωσή μας -1 ή 1. Το στοιχείο αυτό είναι απαραίτητο γιατί άκυρες τιμές μπορούν να υπονομεύσουν το αποτέλεσμα της ψηφοφορίας. Για παράδειγμα αν κάποιος κρυπτογραφούσε και έστειλε την τιμή 100 αντί για 1, λόγω της αθροιστικής διαδικασίας των ψηφοδελτίων αυτό ουσιαστικά αντιστοιχεί σε 100 ψήφους υπερ της τιμής 1, παραβιάζοντας έτσι τον κανόνα της μίας ψήφου ανά ψηφοφόρο.

Για να προσφερθεί αυτή η δυνατότητα ελέγχου, χρησιμοποιείται ένα είδος non-interactive zero-knowledge απόδειξης [22] και συγκεκριμένα μία *παραλλαγή* εμπνευσμένη από το σύστημα των Cramer *et al.* [17:8].

Παίρνοντας την περίπτωση που ο ψηφοφόρος επέλεγε να ψηφίσει ΝΑΙ με κωδικοποίηση την τιμή $v = 1$. Η ψήφος του κρυπτογραφείται χρησιμοποιώντας τις δημόσιες τιμές g και G που έχουν επιλεγεί για τη συγκεκριμένη ψηφοφορία καθώς και το μυστικό του κλειδί s . Για τη δημιουργία της μη διαδραστικής απόδειξης προ-επιλέγονται επιπλέον οι εξής τιμές:

- w
- r_1
- d_1

Με βάση τα παραπάνω υπολογίζονται οι επιπλέον τιμές:

- $h = g^s$
- $y = h * G^v$
- $b_1 = h^{r_1} * (y * G)^{d_1}$
- $b_2 = h^w$
- $c = \text{SHA256}(\text{User_PubKey}, y, b_1, b_2)$
- $d_2 = c - d_1$
- $r_2 = w - s * d_2$

Όλες οι τιμές δημοσιεύονται και αποτελούν τη μη διαδραστική απόδειξη. Για να επιβεβαιώσει ο οποιοσδήποτε χρήστης ότι η ψήφος περιέχει είτε την τιμή 1 είτε την τιμή -1 αρκεί να εκτελέσει τους εξής ελέγχους:

- $c = d_1 + d_2$
- $b_1 = h^{r_1} * (y * G)^{d_1}$
- $b_2 = h^{r_2} * \left(\frac{y}{G}\right)^{d_2}$

Αν οι έλεγχοι επιβεβαιώνονται τότε είμαστε σίγουροι πως το κρυπτοκείμενο περιέχει έγκυρες τιμές. Σε αντίθετη περίπτωση η ψήφος θεωρείται άκυρη και η blockchain συναλλαγή απορρίπτεται.

Σημειώνεται πως ο παραπάνω αλγόριθμος δημιουργίας της απόδειξης εξυπηρετεί την περίπτωση που η επιλογή του ψηφοφόρου έχει ως κωδικοποίηση την τιμή 1. Στην περίπτωση που η επιλογή κωδικοποιείται ως -1 τότε ο αλγόριθμος έχει τις εξής αλλαγές:

Αντί για τις τιμές r_1 και d_1 προ-επιλέγονται οι τιμές r_2 και d_2 . Επιπλέον, οι εξής τιμές υπολογίζονται διαφορετικά:

- $b_1 = h^w$
- $b_2 = h^{r_2} * \left(\frac{y}{G}\right)^{d_2}$
- $d_1 = c - d_2$
- $r_1 = w - s * d_1$

Παρ' ότι ο αλγόριθμος παραγωγής της απόδειξης αλλάζει, είναι σημαντικό το ότι ο αλγόριθμος επιβεβαίωσης δεν αλλάζει. Διατηρώντας τον ίδιο αλγόριθμο επιβεβαίωσης είναι αδύνατος να

διακριθεί ποιος αλγόριθμος δημιουργίας της απόδειξης δημιουργήθηκε, διασφαλίζοντας έτσι την ψήφο του ψηφοφόρου.

5.2.10. Περιορισμός επιλογών σε ΝΑΙ – ΟΧΙ

Όπως έχει αναφερθεί και στο υποκεφάλαιο 5.1.1. *Μοντέλο δεδομένων πρωτοκόλλου*, οι διαθέσιμες επιλογές του συστήματος περιορίζονται στις δύο, συνήθως *ΝΑΙ* και *ΟΧΙ*. Παρ' ότι όπως δείξαμε υπάρχει τρόπος κωδικοποίησης περισσότερων επιλογών, σε αυτές τις περιπτώσεις η τιμή του κωδικοποιημένου αθροίσματος των ψήφων αυξάνεται σε πολύ μεγάλους αριθμούς, συναρτήσει του αριθμού επιλογών και του αριθμού των ψήφων. Λόγω της ανάγκης εκτέλεσης εξαντλητικής μεθόδου για την εύρεση της τιμής διακριτού λογαρίθμου, όπως εξηγείται στο υποκεφάλαιο 5.2.7. *Παραγωγή κρυπτογραφημένου αποτελέσματος και τελικού συνόλου*, ο χρόνος εκτέλεσης πιθανώς να υπερβαίνει τα όρια που ορίζουν οι ανάγκες του συστήματος. Για το λόγο αυτό η παρούσα υλοποίηση περιορίζεται σε δύο μόνο επιλογές.

5.3. Αριθμητικό παράδειγμα πρωτοκόλλου

Παρακάτω παρουσιάζεται ένα υποθετικό σενάριο ψηφοφορίας και πώς αυτό αναπαρίσταται με βάση το πρωτόκολλο που αναλύθηκε με στόχος να διευκολυνθεί η κατανόηση του τρόπου χρήσης των εννοιών που παρουσιάστηκαν.

Σενάριο

Η ψηφοφορία είναι τύπου δημοψηφίσματος με επιλογές [ΝΑΙ, ΟΧΙ] οι οποίες κωδικοποιούνται ως εξής:

ΝΑΙ	1
ΟΧΙ	-1

Πίνακας 5.3.1: Κωδικοποίηση επιλογών ψηφοφορίας

Έχουμε 5 ψηφοφόρους. Ο καθένας έχει από ένα διακριτό δημόσιο μοναδικό αναγνωριστικό και αυτό έρχεται σε συνδυασμό με ένα κρυφό κλειδί.

Ψηφοφόρος	Αναγνωριστικό	Κρυφό κλειδί s
A	1	2
B	2	3
Γ	3	4
Δ	4	5
Ε	5	6

Πίνακας 5.3.2: Ζεύγη δημοσίων αναγνωριστικών ψηφοφόρων

Η εφορευτική επιτροπή της ψηφοφορίας έχει δημοσιεύσει τις εξής κρυπτογραφικές παραμέτρους:

<i>P</i>	19	Πρώτος αριθμός που χρησιμοποιείται ως modulo για το αριθμητικό <i>group</i> στο οποίο θα βασιστεί η κρυπτογραφία
<i>G</i>	2	<i>Group generator</i> κρυπτογράφησης
<i>G</i>	3	<i>Group generator</i> ψήφου

Πίνακας 5.3.3: Δημόσιες κρυπτογραφικές παράμετροι ψηφοφορίας

Ο πρώτος αριθμός p επιλέχθηκε έτσι ώστε να ισχύει η ανισότητα

$$\text{Αριθμός Ψηφοφόρων} \leq \lfloor p / 2 \rfloor$$

(στρογγυλοποίηση προς τα κάτω)

αλλά ταυτόχρονα και να δημιουργείται μία κυκλική ομάδα με τουλάχιστον 2 γεννήτριες (κάτι το οποίο δεν ισχύει για τις ομάδες $mod13$ και $mod17$).

Ψηφοφορία

Με βάση τα παραπάνω οι δημοσιευμένες τιμές των κρυπτογραφημένων ψήφων είναι οι εξής:

Ψηφοφόρος	Ψήφος v	Δημοσιευμένη τιμή $g^s * G^v \text{ mod } p$
A	OXI (-1)	14 ($2^2 * 3^{-1} \text{ mod } 19$)
B	OXI (-1)	9 ($2^3 * 3^{-1} \text{ mod } 19$)
Γ	OXI (-1)	18 ($2^4 * 3^{-1} \text{ mod } 19$)
Δ	NAI (1)	1 ($2^5 * 3^1 \text{ mod } 19$)
E	NAI (1)	2 ($2^6 * 3^1 \text{ mod } 19$)

Σημείωση: Στις περιπτώσεις όπου η ψήφος είναι OXI (-1) ουσιαστικά εκτελούμε πράξη *modular division*.

Πίνακας 5.3.4: Κρυπτογραφημένες τιμές των ψήφων

Με το πέρας της ψηφοφορίας πρέπει να εξαχθεί το τελικό αποτέλεσμα. Για να αθροιστούν οι ψήφοι ομομορφικά παίρνουμε το γινόμενο των δημοσιευμένων κρυπτοκειμένων.

$$Total = 14 * 9 * 18 * 1 * 2 \equiv 4536 \equiv \mathbf{14} \text{ mod } 19$$

Υπενθυμίζουμε ότι το γινόμενο που έχει παραχθεί αντιστοιχεί στην τιμή:

$$T = g^{2+3+4+5+6} * G^{(-1-1-1+1+1)} \text{ mod } 19$$

Υπερκλειδί αποκρυπτογράφησης

Για να εξάγουμε λοιπόν το άθροισμα των ψήφων πρέπει η τιμή T να διαιρεθεί με την τιμή g^{20} . Ο εκθέτης 20 όμως δεν είναι εξ αρχής γνωστός διότι προέρχεται από τα κρυφά κλειδιά των χρηστών, τα οποία παραμένουν *μυστικά* καθ' όλη τη διαδικασία. Για να παραχθεί το άθροισμα αυτών με ασφάλεια εκτελείται η MPC διαδικασία βασισμένη στην τεχνική *Shamir Secret Sharing* όπου ο κάθε χρήστης δηλώνει ως σταθερά πολυωνύμου Shamir το κρυφό του *κλειδί*:

Ψηφοφόρος	Πολυώνυμο $f(x)$
A	$2 + 7x + 2x^2 + 6x^3 + x^4$
B	$3 + 6x + 3x^2 + 5x^3 + 2x^4$
Γ	$4 + 5x + 4x^2 + 7x^3 + 3x^4$
Δ	$5 + 4x + 5x^2 + 8x^3 + 4x^4$
Ε	$6 + 3x + 6x^2 + 9x^3 + 5x^4$

Πίνακας 5.3.5: Πολυώνυμα Shamir για διαδικασία αθροιστικού MPC των κρυφών κλειδιών

Ο σκοπός μας είναι να παράξουμε το *αθροιστικό πολυώνυμο* των 5 ψηφοφόρων, η σταθερά του οποίου αντιστοιχεί στο άθροισμα των κρυφών κλειδιών:

$$f_{sum}(x) = 15x^4 + 35x^3 + 20x^2 + 25x + \mathbf{20}$$

όπου

$$S_A + S_B + S_\Gamma + S_\Delta + S_E = S_{A+B+\Gamma+\Delta+E} = 2 + 3 + 4 + 5 + 6 = \mathbf{20}$$

Για να το πετύχουμε αυτό χωρίς να γίνουν γνωστά τα επιμέρους πολυώνυμα εκμεταλλευόμαστε την αθροιστική ιδιότητα της παρεμβολής Lagrange ώστε να αναπαράξουμε το αθροιστικό πολυώνυμο δίνοντας ως σημεία το άθροισμα των σημείων των επιμέρους πολυωνύμων.

Κάθε ψηφοφόρος, αφού έχει παράξει το επιθυμητό πολυώνυμο, παράγει 5 τιμές δίνοντας 5 προκαθορισμένες τιμές εισόδου x οι οποίες αντιστοιχίζονται μια σε κάθε συμμετέχοντα. Ο λόγος είναι πως για να λειτουργήσει σωστά η διαδικασία πρέπει όλοι οι συμμετέχοντες να δώσουν τις ίδιες τιμές εισόδου στα πολυώνυμά τους και τα αποτελέσματα που θα πάρουν να διαμοιραστούν με βάση την τιμή εισόδου. Για παράδειγμα, ο ψηφοφόρος **A** θα πρέπει να δεχτεί από όλους, τιμές πολυωνύμων με είσοδο $x = 1$ ενώ ο **B** με $x = 2$.

Για τη διευκόλυνση της διαδικασίας προτείνεται το σύνολο των τιμών S να είναι είτε τα δημόσια κλειδιά των συμμετεχόντων είτε η ομάδα $\mathbb{Z}/\mathbb{Z}_{n+1}$ όπου n ο αριθμός των συμμετεχόντων. Στην

περίπτωσή μας, ανεξαρτήτως μεθόδου, το σύνολο είναι $S = [1,2,3,4,5]$ και κάθε τιμή ανήκει αντιστοίχα στους $[A, B, \Gamma, \Delta, E]$. Οι τιμές που διαμοιράζονται φαίνονται παρακάτω:

Δημιουργεί\Αποδέχεται	A	B	Γ	Δ	E
A	18	88	284	702	1462
B	19	99	345	907	1983
Γ	23	134	487	1304	2879
Δ	26	161	602	1637	3650
E	29	188	717	1970	4421

Πίνακας 5.3.6: Shamir shares για την εκτέλεση αθροιστικού MPC

Έχοντας όλες τις τιμές ο κάθε χρήστης τις προσθέτει και δημοσιοποιεί στους υπόλοιπους χρήστες το άθροισμα το οποίο αντιστοιχεί σε ένα από τα 5 σημεία που θα χρησιμοποιηθούν για την παρεμβολή Lagrange:

	A	B	Γ	Δ	E
SUM	115	670	2435	6520	14395

Πίνακας 5.3.7: Άθροισμα Shamir shares, τιμές παρεμβολής Lagrange για εξαγωγή αθροίσματος πολυωνύμων

Εκτελώντας παρεμβολή Lagrange για τα 5 σημεία:

$$(1, 115) (2, 670) (3, 2435) (4, 6520) (5, 14395)$$

λαμβάνουμε το αθροιστικό πολυώνυμο $f_{sum}(x)$ το οποίο όταν το υπολογίζουμε για $x = 0$ λαμβάνουμε την τιμή 20 η οποία αντιστοιχεί στο υπερκλειδί αποκρυπτογράφησης S_{all} .

Αποκρυπτογράφηση τελικού αποτελέσματος

Έχοντας την τιμή S_{all} υπολογίζουμε το $g^{S_{all}}$ και διαιρούμε (modular division) το κρυπτογραφημένο σύνολο ψήφων που υπολογίστηκε προηγουμένως:

$$\frac{T}{g^{S_{all}}} \equiv \frac{14}{4} \equiv 14 * 5 \equiv 13 \text{ mod } 19$$

Η τιμή αυτή αντιστοιχίζεται μοναδικά σε μία τιμή G^i όπου $-5 \leq i \leq 5$.

Για να βρούμε το i το οποίο ουσιαστικά θα μας δώσει το τελικό αποτέλεσμα υπολογίζουμε την τιμή

$$G^i \equiv 13 \text{ mod } 19$$

για κάθε i και μπορούμε εύκολα να δούμε ότι η σχέση αυτή ισχύει για την τιμή $i = -1$ το οποίο είναι και το άθροισμα των κωδικοποιημένων τιμών των ψήφων και μας δείχνει πως η διαφορά μεταξύ των ΝΑΙ (1) και ΟΧΙ (-1) είναι 1 ψήφος υπέρ του ΝΑΙ.

Non-interactive proof of validity

Όσον αφορά το αποδεικτικό εγκυρότητας ψήφου, έστω για τον χρήστη Δ , έχουμε διαλέξει τις εξής τιμές:

$$v = 1, g = 2, G = 3, w = 4, s = 5, r_1 = 6, d_1 = 7, h = g^s = 32$$

και υπολογίζουμε τις τιμές:

$$\begin{aligned} y &= h * G^v \equiv 96 \equiv 1 \text{ mod } 19 \\ b_1 &= g^{r_1} * (y * G)^{d_1} \equiv 14 \text{ mod } 19 \\ b_2 &= g^w \equiv 16 \text{ mod } 19 \\ c &= \text{SHA256}(V_{id}, y, b_1, b_2) \equiv 15 \text{ mod } 19 \\ d_2 &= c - d_1 = 8 \\ r_2 &= w - s * d_2 = -36 \end{aligned}$$

Όλες οι τιμές μαζί αποτελούν το αποδεικτικό στοιχείο εγκυρότητας. Για να την επιβεβαιώσει κάποιος άλλος χρήστης πρέπει να ισχύουν οι εξής ισότητες:

$$\begin{aligned} c &= \text{SHA256}(V_{id}, y, b_1, b_2) = d_1 + d_2 \\ b_1 &= g^{r_1} * (y * G)^{d_1} \\ b_2 &= 16 = g^{r_2} * \left(\frac{y}{G}\right)^{d_2} \equiv 4 * \left(\frac{1}{3}\right)^8 \equiv 2^{-36} * 13^8 \equiv 1 * 16 \text{ mod } 19 \end{aligned}$$

6. Case study- Σύστημα ηλεκτρονικής ψηφοφορίας για φοιτητική συνέλευση

6.1. Γενικά

Η υλοποίηση που έγινε στα πλαίσια της εργασίας αφορά το σενάριο ψηφοφορίας σε φοιτητική συνέλευση κατά τη διαβούλευση μιας συγκεκριμένης πρότασης ή ενός πλαισίου μόνο. Σε αυτές τις περιπτώσεις, οι διαθέσιμες επιλογές είναι μεταξύ του *ΝΑΙ* και *ΟΧΙ*. Η επιλογή του συγκεκριμένου σεναρίου έγινε για τεχνικούς λόγους οι οποίοι αναλύονται στο υποκεφάλαιο 5.2.10. *Περιορισμός επιλογών*.

Η υλοποίηση αποτελείται από μια desktop εφαρμογή η οποία επιτρέπει τη δημιουργία ενός ψηφίσματος από κάποιο χρήστη-διαχειριστή καθώς και την υποβολή ψήφου από εγκεκριμένους από το διαχειριστή χρήστες-φοιτητές. Χρησιμοποιεί μια έτοιμη τεχνολογία κατακευκμένου καθολικού, λεγόμενη Ethereum, ή οποία υλοποιεί όλο το προαπαιτούμενο υποσύστημα blockchain που αναλύεται στο πέμπτο κεφάλαιο. Τέλος, έχει υλοποιηθεί το κρυπτο-πρωτόκολλο που παρουσιάστηκε στο κεφάλαιο 5 για την υποβολή, επαλήθευση και καταμέτρηση των ψήφων.

6.2. Σκοπός συστήματος

Το proof of concept σύστημα ηλεκτρονικής ψηφοφορίας που δημιουργήθηκε εφαρμόζεται μόνο κατά τη στιγμή υποβολής ψήφου. Δεν επιδρά στη διαδικασία της φοιτητικής συνέλευσης και ανταλλαγής απόψεων. Έχει ως στόχο να δώσει στα μέλη του φοιτητικού συλλόγου τη δυνατότητα να καταθέσουν την ψήφο τους κρυφά και εκτός της αίθουσας διεξαγωγής της συνέλευσης. Ταυτόχρονα η απλή υλοποίηση αποσκοπεί στην προσιτότητα της εφαρμογής ενώ η χρήση κρυπτογραφίας και τεχνολογίας κατακευκμένου καθολικού διασφαλίζουν την ακεραιότητα του αποτελέσματος.

Με βάση τα παραπάνω επιλέξαμε το σύστημα να καλύπτει τα εξής use case:

1. Login στο σύστημα με βάση τα αναγνωριστικά ενός φοιτητή ή ενός διαχειριστή
2. Δημιουργία και παραμετροποίηση ψηφοφορίας από χρήστη διαχειριστή
3. Επισκόπηση ψηφοφορίας από χρήστη φοιτητή
4. Υποβολή ψήφου *ΝΑΙ* ή *ΟΧΙ* μόνο εντός του χρονικού περιθωρίου που έχει οριστεί για την ψηφοφορία
5. Αυτόματος υπολογισμός του αποτελέσματος με το πέρας του χρονικού περιθωρίου ψηφοφορίας

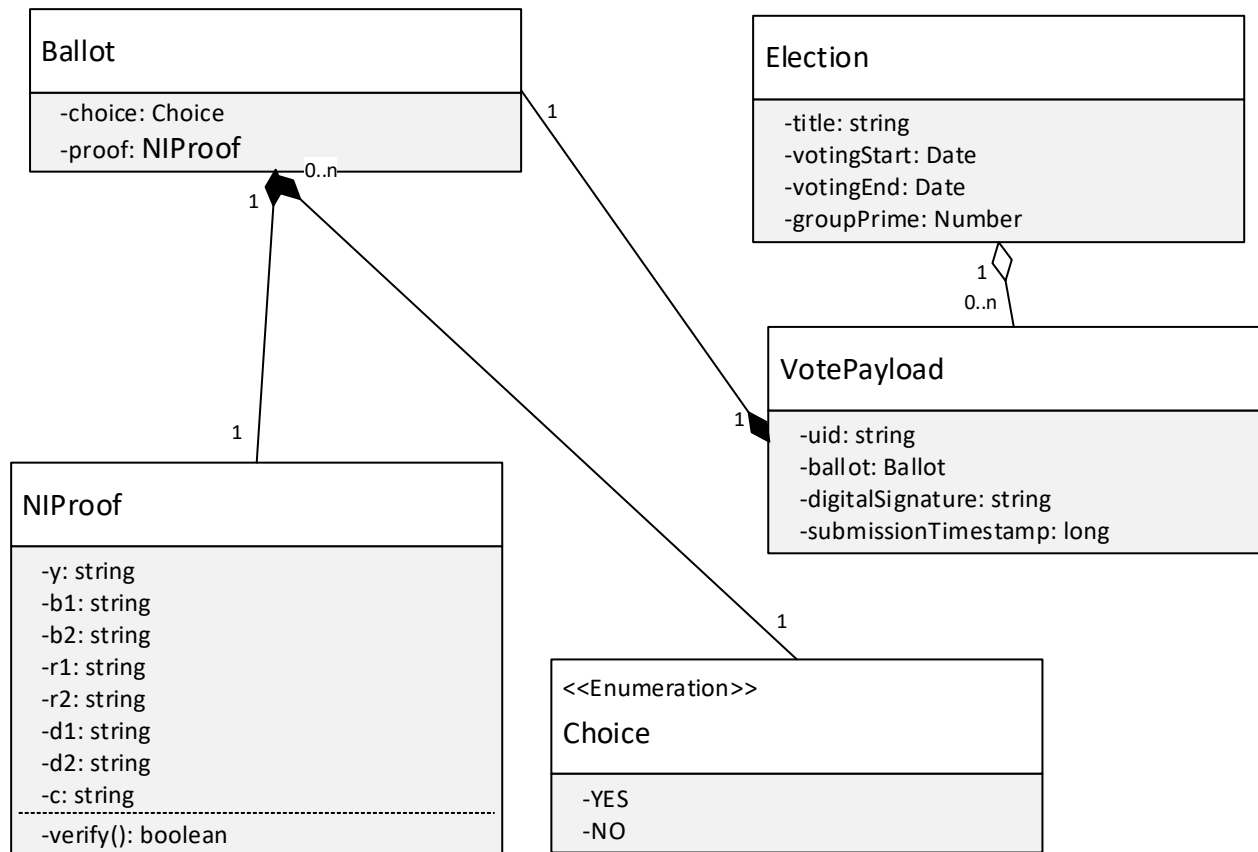
6.3. Παρουσίαση εφαρμογής

Η εφαρμογή ψηφοφορίας έχει τους εξής σκοπούς:

- Προσφέρει στο χρήστη μια διεπαφή ώστε να μπορεί να συμμετάσχει εύκολα στη διαδικασία της ψηφοφορίας, να δει και να διαχειριστεί τις παραμέτρους της ψηφοφορίας, να υποβάλει την ψήφο του και να δει το τελικό αποτέλεσμα.
- Αναλαμβάνει όλα τα σημεία του πρωτοκόλλου blockchain τα οποία πρέπει να εκτελεστούν τοπικά όπως η κρυπτογράφηση της ψήφου χρήστη, η ψηφιακή υπογραφή του μηνύματος καθώς και η παραγωγή του τελικού αποτελέσματος.
- Είναι υπεύθυνη για τη σωστή επικοινωνία με το Ethereum voting contract, αναλαμβάνοντας να καλεί τις σωστές συναρτήσεις για κάθε ενέργεια με τα σωστά ορίσματα.

Τα παραπάνω βασίζονται σε ένα μοντέλο δεδομένων για τη διαχείριση της ψηφοφορίας και των ψήφων όπου:

- Choice: ένα enumeration των διαθέσιμων επιλογών.
- NIPProof: η συλλογή των παραμέτρων απόδειξης μηδενικής γνώσης.
- Ballot: αντιπροσωπεύει μία ψήφο και περιέχει την κρυπτογραφημένη επιλογή καθώς και την απόδειξη μηδενικής γνώσης για την ορθότητα του κρυπτογραφήματος.
- VotePayload: η συνολική πληροφορία που αποθηκεύεται στο Ethereum blockchain κατά την υποβολή ψήφου του χρήστη. Μαζί με το Ballot περιέχει και το αναγνωριστικό χρήστη, την ψηφιακή υπογραφή της ψήφου του καθώς και το χρονικό στιγμιότυπο υποβολής.
- Election: η ψηφοφορία. Η παράμετρος groupPrime είναι ο πρώτος αριθμός p που θα χρησιμοποιηθεί από όλους τους ψηφοφόρους για τη δημιουργία της κρυπτογραφικής ομάδας κατά τη συγκεκριμένη ψηφοφορία.



Σχήμα 18: Μοντέλο δεδομένων εφαρμογής ψηφοφορίας

Η εφαρμογή αποτελείται από 3 οθόνες:

- Login
- Administration
- Voting

Οθόνη login

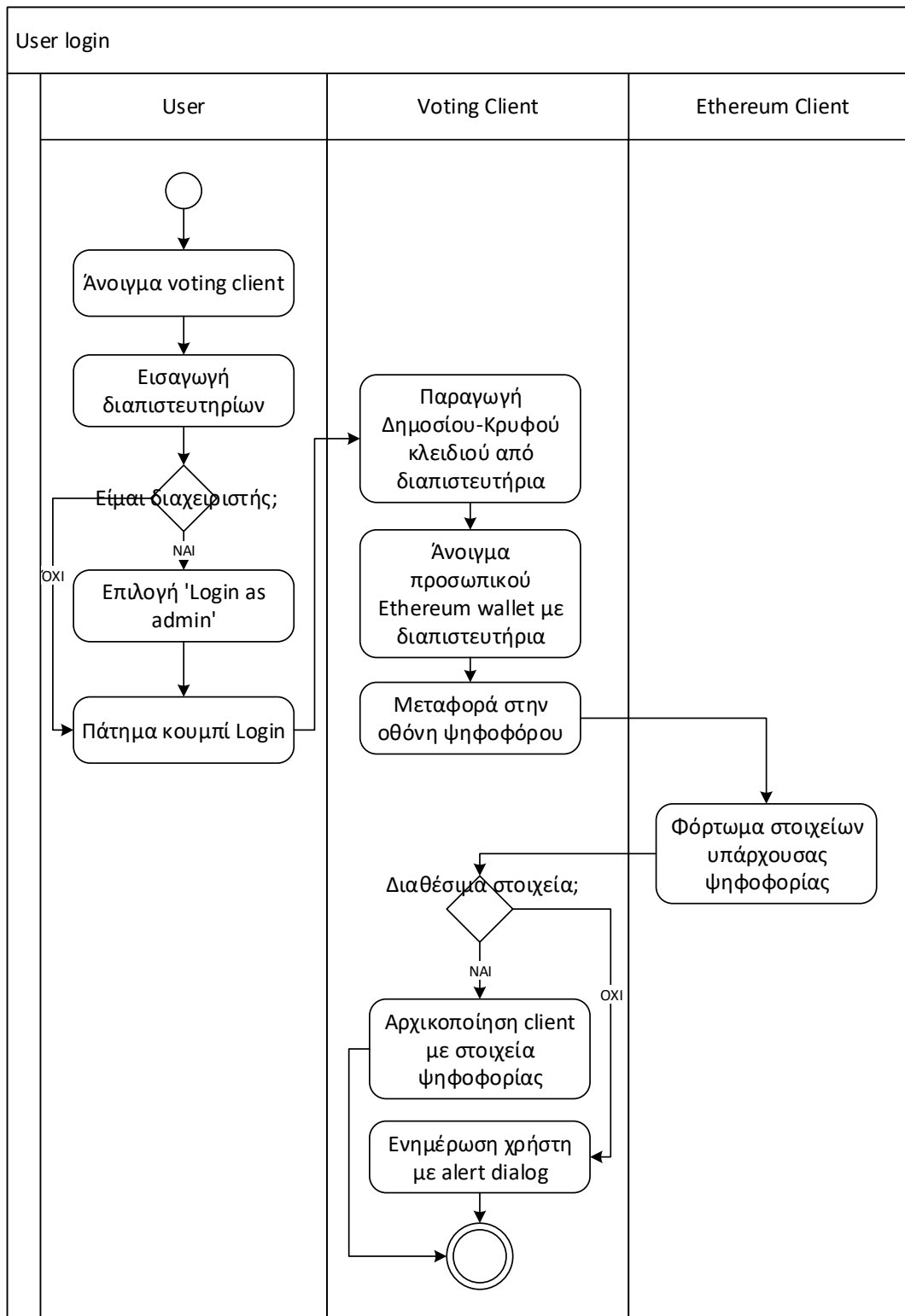
The screenshot shows a window titled "Voting Application" with a "Voting Application Login" form. The form includes:

- An "Email" field with the value `ece7110@upnet.gr`.
- A "Password" field with masked characters (dots).
- A checkbox labeled "Login as admin".
- A "Login" button.

Σχήμα 19: Οθόνη login

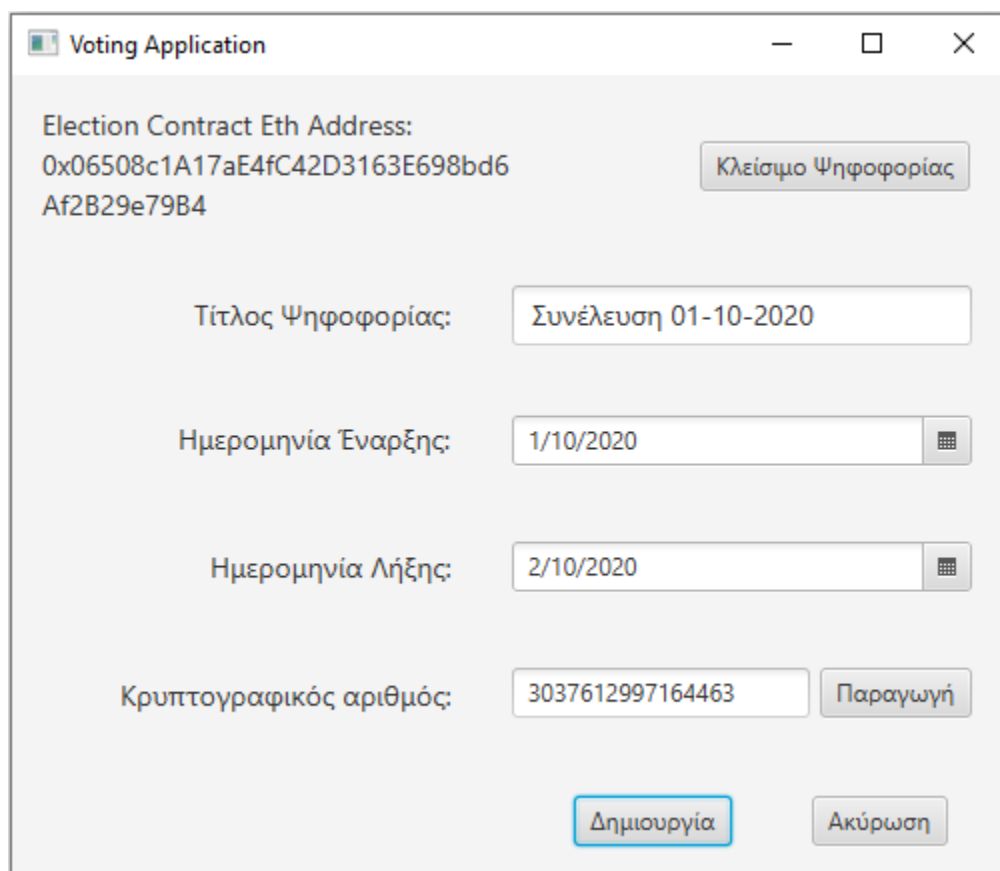
Η οθόνη login (Σχήμα. 19) είναι η αρχική οθόνη που παρουσιάζεται στο χρήστη. Απαιτεί την εισαγωγή των διαπιστευτηρίων αυτού και σκοπός της είναι, αρχικοποιώντας τα απαραίτητα κρυπτογραφικά κλειδιά, να τον εισάγει στο σύστημα με τρόπο που να μπορεί να συναλλαχθεί με το εν χρήση blockchain. Αυτά είναι η ψηφιακή υπογραφή του χρήστη καθώς και το κλειδί κρυπτογράφησης ψήφου, σε περίπτωση login ως ψηφοφόρος. Το checkbox επιτρέπει το login ως χρήστης διαχειριστής.

Για τη συναλλαγή του χρήστη με το Ethereum blockchain απαιτείται η χρήση ενός Ethereum wallet το οποίο αντιστοιχεί στο λογαριασμό του χρήστη. Το αρχείο wallet δημιουργείται από τον κάθε χρήστη μέσω μιας 'seed' τιμής και στην περίπτωση μας είναι τα διαπιστευτήρια αυτού. Κάθε αρχείο wallet περιέχει ένα δημόσιο κλειδί, η λεγόμενη δημόσια διεύθυνση αυτού, το οποίο χρησιμοποιείται για να ταυτοποιήσει το χρήστη κατά τη συναλλαγή του με το blockchain σύστημα. Για τη συναλλαγή του χρήστη ως διαχειριστής, θα πρέπει να έχει ταυτοποιηθεί με τα μοναδικά διαπιστευτήρια του διαχειριστή και να κάνει χρήση του wallet διαχειριστή. Οποιαδήποτε συναλλαγή απαιτεί δικαιώματα διαχειριστή συνεπώς είναι επιτρεπτή μόνο αν προέρχεται από τη, δημοσίως γνωστή, διεύθυνση διαχειριστή. Οποιοσδήποτε άλλος χρήστης μπορεί πάντα να προσπαθήσει να συναλλαχθεί ως διαχειριστής αλλά μη έχοντας πρόσβαση στο σωστό wallet η συναλλαγές του καθίστανται άκυρες.



Σχήμα 20: Login activity diagram

Οθόνη διαχείρισης



The screenshot shows a window titled "Voting Application" with standard Windows window controls (minimize, maximize, close). The interface is light gray and contains the following elements:

- Election Contract Eth Address:** A text label followed by the address `0x06508c1A17aE4fC42D3163E698bd6Af2B29e79B4` and a button labeled "Κλείσιμο Ψηφοφορίας".
- Τίτλος Ψηφοφορίας:** A text label followed by a text input field containing "Συνέλευση 01-10-2020".
- Ημερομηνία Έναρξης:** A text label followed by a date input field containing "1/10/2020" and a calendar icon.
- Ημερομηνία Λήξης:** A text label followed by a date input field containing "2/10/2020" and a calendar icon.
- Κρυπτογραφικός αριθμός:** A text label followed by a text input field containing "3037612997164463" and a button labeled "Παραγωγή".
- At the bottom, there are two buttons: "Δημιουργία" (highlighted with a blue border) and "Ακύρωση".

Σχήμα 21: Οθόνη διαχείρισης

Η οθόνη διαχείρισης (Σχήμα. 21) εμφανίζεται σε περίπτωση που κατά το login, το checkbox 'Login as admin' είναι ενεργοποιημένο. Από εδώ προσφέρεται η δυνατότητα δημιουργίας νέας ψηφοφορίας ή η παραμετροποίηση των στοιχείων υπάρχουσας ψηφοφορίας.

Μια ψηφοφορία αποτελείται από τα εξής στοιχεία:

1. Τίτλος Ψηφοφορίας:

Ένα οποιοδήποτε αλφαριθμητικό χαρακτηρίζει το ψήφισμα και βοηθάει τους ψηφοφόρους να γνωρίζουν για ποιο σκοπό ψηφίζουν.

2. Ημερομηνία Έναρξης:

Πριν από αυτή την ημερομηνία καμία ψήφος δεν γίνεται αποδεκτή.

3. Ημερομηνία Λήξης:

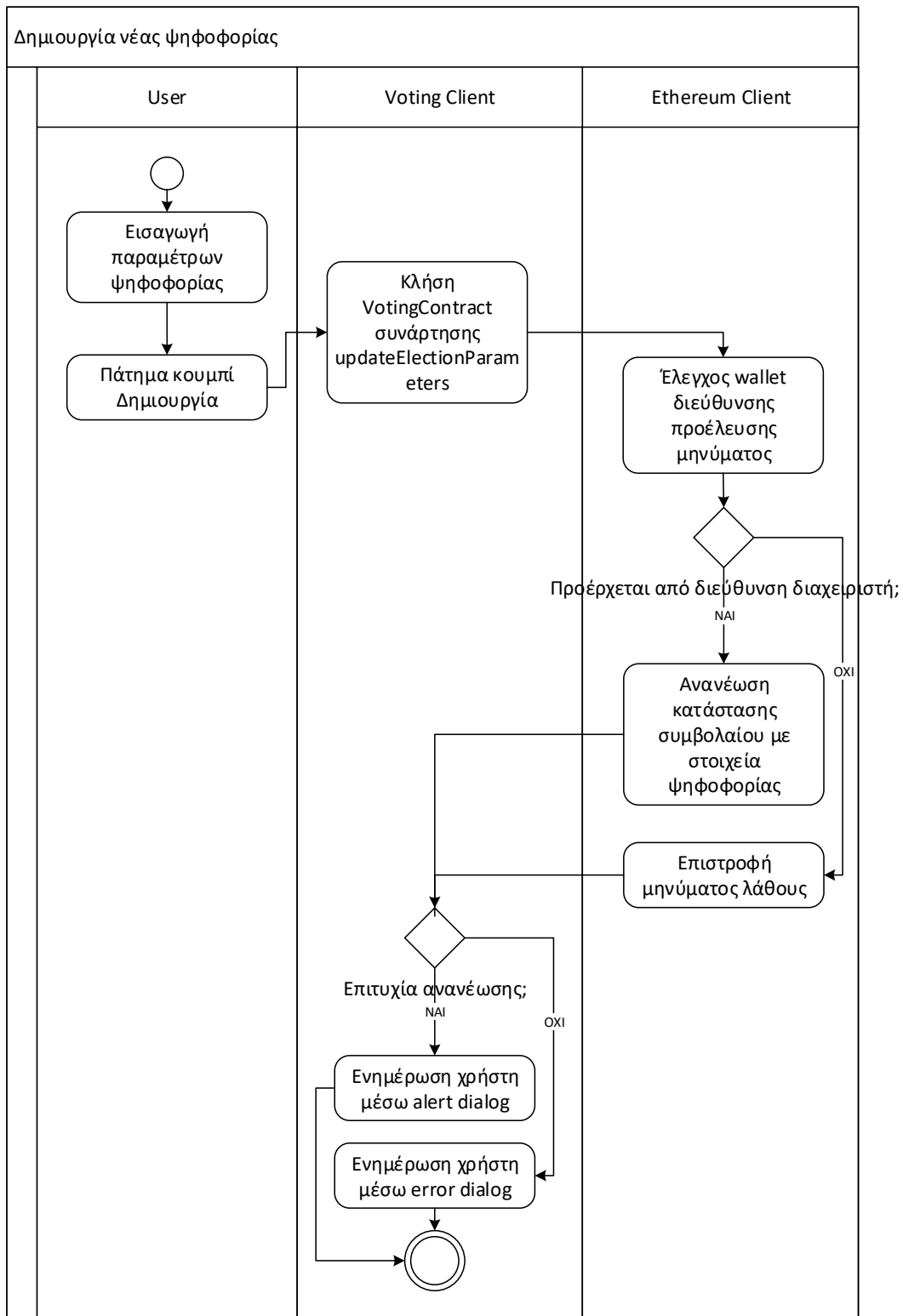
Μετά από αυτή την ημερομηνία καμία ψήφος δεν γίνεται αποδεκτή. Επίσης με τον ερχομό της ημερομηνίας λήξης ξεκινούν οι διαδικασίες εξαγωγής του τελικού αποτελέσματος.

4. Κρυπτογραφικός αριθμός:

Ένας ασφαλής πρώτος αριθμός με μέγεθος τουλάχιστον 48bit ο οποίος θα χρησιμοποιηθεί από όλους τους χρήστες κατά την κρυπτογράφηση των ψήφων τους. Ο αριθμός αυτός αντιστοιχίζεται στο modulo p από το οποίο εξάγεται η πεπερασμένη κυκλική ομάδα G η οποία θα χρησιμοποιηθεί για την κρυπτογράφηση. Προσφέρεται επίσης ένα κουμπί για την παραγωγή ενός τυχαίου τέτοιου πρώτου αριθμού για διευκόλυνση του χρήστη.

Εκτός από τα στοιχεία μίας ψηφοφορίας, η οθόνη διαχείρισης προσφέρει ακόμα δύο δυνατότητες στη συγκεκριμένη υλοποίηση. Πάνω αριστερά εμφανίζεται η διεύθυνση του Ethereum smart contract (το οποία θα αναλύσουμε σε επόμενο υποκεφάλαιο) που χρησιμοποιείται για τη συγκεκριμένη ψηφοφορία και επίσης δεξιά αυτού προσφέρεται ένα κουμπί το οποίο τερματίζει την ψηφοφορία πρόωρα. Η συγκεκριμένη δυνατότητα είναι χρήσιμη κατά την επίδειξη της εφαρμογής ώστε να αποφεύγεται η αναμονή μέχρι τη λήξη για την καταμέτρηση των ψήφων ενώ θα μπορούσε να φανεί χρήσιμη και σε πραγματική χρήση της εφαρμογής, σε περίπτωση που η ψηφοφορία γίνεται σε πραγματικό χρόνο και υπάρχει γνώση του αν έχουν καταθέσει όλοι οι ψηφοφόροι την ψήφο τους.

Είναι σημαντικό να σημειωθεί πως παρ' ότι οποιοσδήποτε χρήστης έχει δικαίωμα να επιλέξει το 'Login as admin', αυτό δεν σημαίνει πως θα έχει και τη δυνατότητα δημιουργίας ή παραμετροποίησης ψηφοφορίας. Το Ethereum blockchain που χρησιμοποιείται επιτρέπει τα συγκεκριμένα use case να εκτελούνται μόνο από ένα συγκεκριμένο χρήστη ο οποίος έχει δηλωθεί εξ αρχής κατά την αρχικοποίηση της blockchain υποδομής.



Σχήμα 22: Activity diagram παραμετροποίησης ψηφοφορίας

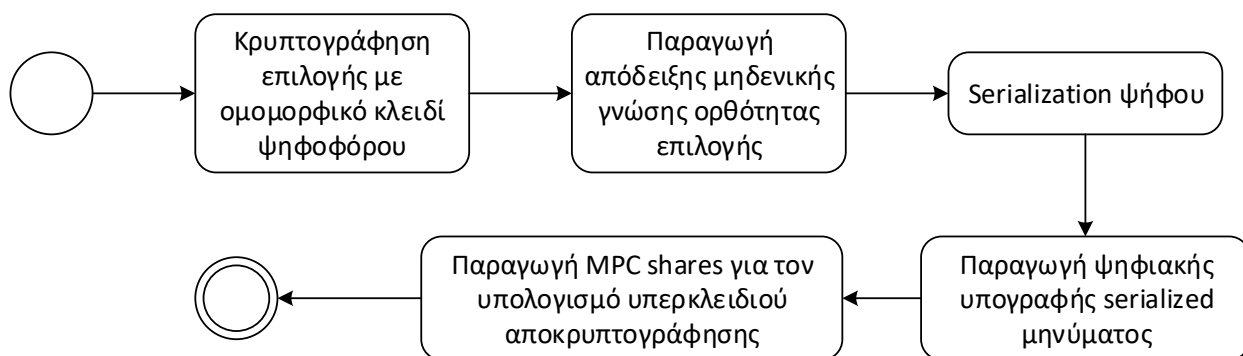
Οθόνη ψηφοφορίας

The screenshot shows a window titled "Voting Application". It contains the following elements:

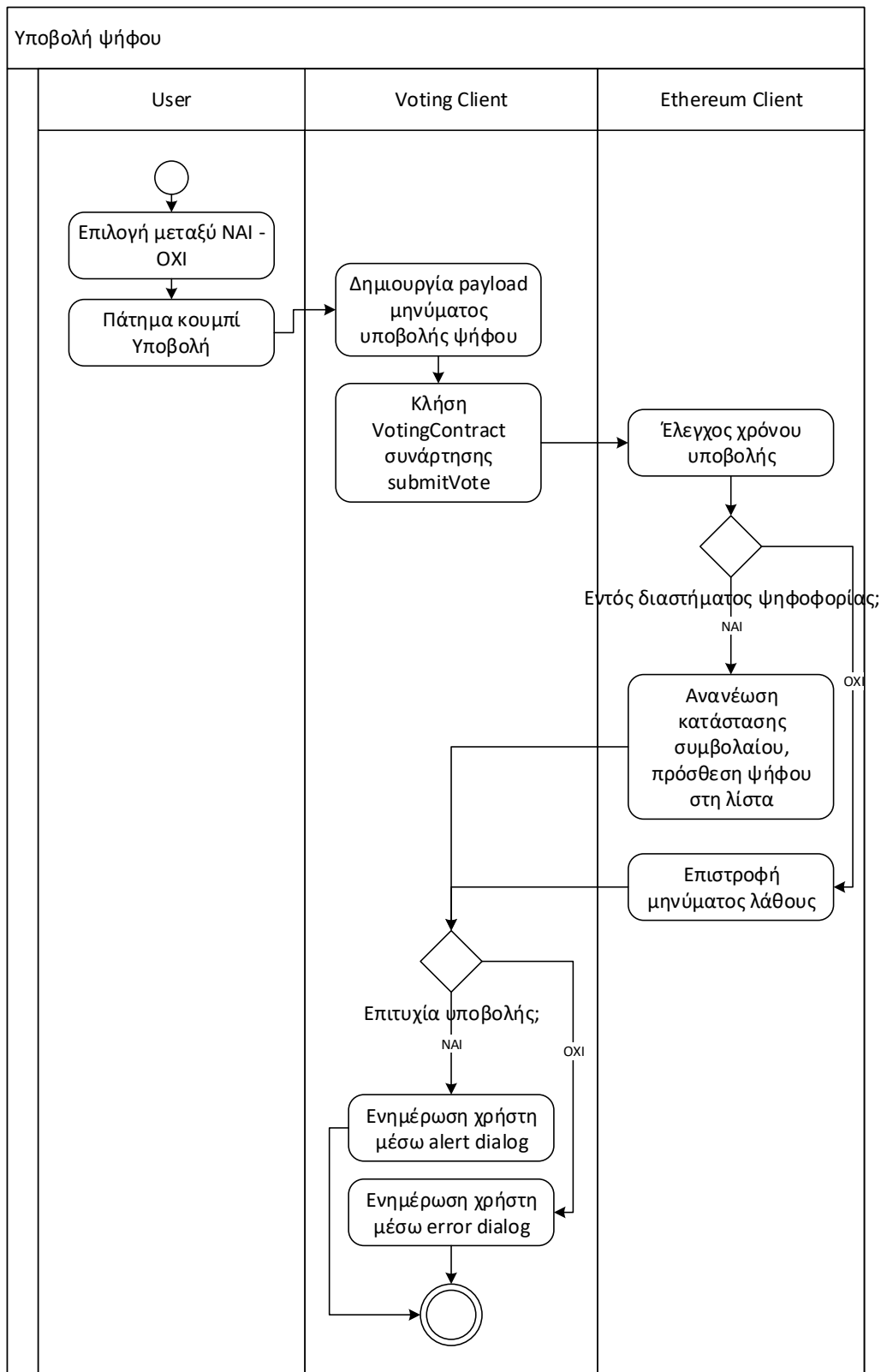
- A label "Αναγνωριστικό Ψηφοφόρου:" followed by the value "3791514487605918977..." and a "Copy" button.
- A label "Τίτλος Ψηφοφορίας:" followed by the value "Συνέλευση 01-10-2020".
- A label "Αποτέλεσμα Ψηφοφορίας:" followed by a dashed line "----".
- A label "Επιλογή:" followed by two radio buttons labeled "NAI" and "OXI".
- At the bottom, there are two buttons: "Υποβολή" (highlighted with a blue border) and "Ακύρωση".

Σχήμα 23: Οθόνη ψηφοφορίας

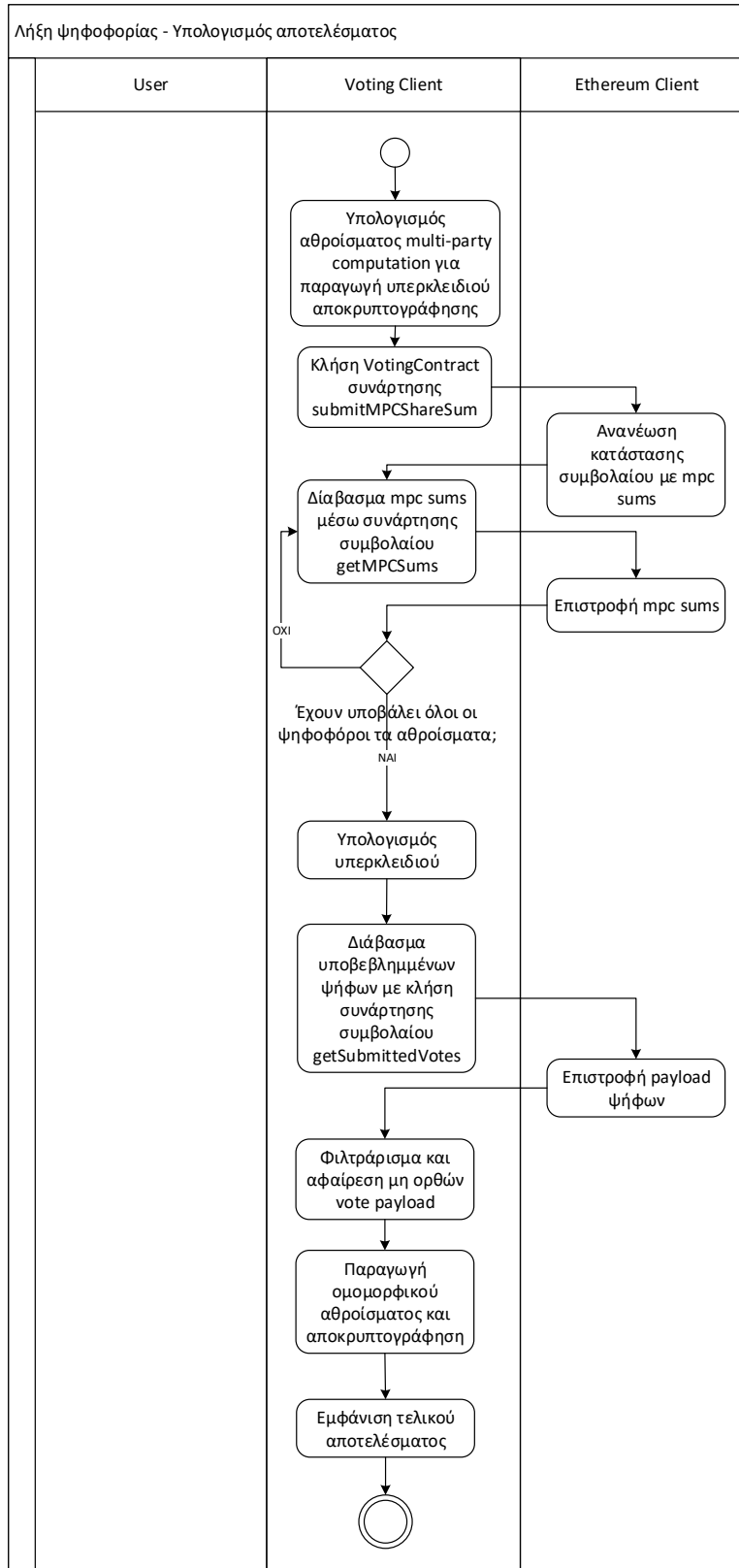
Η βασικότερη οθόνη που χρησιμοποιείται από όλους τους συμμετέχοντες είναι αυτή της ψηφοφορίας (Σχήμα. 23). Η μοναδικές ενέργειες που δίνονται στο χρήστη είναι αυτές της επιλογής και υποβολής της ψήφου. Στην οθόνη αυτή προσφέρεται ένα radio group με πιθανές επιλογές το *NAI* και το *OXI*. Με την υποβολή της ψήφου, αυτή κρυπτογραφείται και αποστέλλεται στο δίκτυο όπως φαίνεται στα activity diagram των σχημάτων 24, 25. Ο χρήστης έχει δικαίωμα να αλλάξει την ψήφο του όσο η ψηφοφορία δεν έχει ακόμα τερματιστεί. Με τον τερματισμό της ψηφοφορίας, καμία περαιτέρω υποβολή ψήφου δεν επιτρέπεται, ενώ η εφαρμογή ξεκινάει αυτόματα τις διαδικασίες για την καταμέτρηση των υποβεβλημένων ψήφων ακολουθώντας τα βήματα του activity diagram του σχήματος 26.



Σχήμα 24: Δημιουργία payload μηνύματος υποβολής ψήφου



Σχήμα 25: Activity diagram υποβολής ψήφου



Σχήμα 26: Activity diagram υπολογισμού τελικού αποτελέσματος

Αναγνωριστικό Ψηφοφόρου

Το αναγνωριστικό (UID) ενός ψηφοφόρου είναι ένας μοναδικός αριθμός με τον οποίο τον ταυτίζουν οι υπόλοιποι χρήστες του συστήματος. Η τιμή του δρα ως ψηφιακή υπογραφή και είναι ένα δημόσιο κλειδί τύπου RSA, κομμάτι ενός ζεύγους κλειδιών που παράγεται με το συνδυασμό email + password που δίνει ο χρήστης κατά το login. Με τον τρόπο αυτό δημιουργείται ένα ντετερμινιστικό κρυφό και δημόσιο κλειδί το οποίο έχει πολλαπλές χρήσεις:

- Αναγνώριση του χρήστη όσον αφορά την προέλευση ψήφου, το οποίο δίνει τη δυνατότητα επιβεβαίωσης ότι κάποιος έχει όντως ψηφίσει.
- Ασφαλή έλεγχο της προέλευσης μηνύματος το οποίο είναι υπογεγραμμένο από το χρήστη με το κρυφό κλειδί και επιβεβαιώνεται με το UID.
- Δημιουργία κρυφού μηνύματος προς το χρήστη και αποστολή αυτού μέσω ανασφαλούς P2P δικτύου, κρυπτογραφώντας το μήνυμα με το UID, το οποίο επιτρέπει την αποκρυπτογράφηση του μόνο με το αντίστοιχο κρυφό κλειδί.
- Έλεγχος του δικαιώματος ψήφου χρηστών, μέσω προκαθορισμένης από το διαχειριστή λίστας UID τιμών. Οποιοδήποτε μήνυμα-ψήφος αποσταλεί στο σύστημα υπογεγραμμένο από κάποιο UID που δεν ανήκει στις προκαθορισμένες τιμές δεν γίνεται αποδεκτό και δεν καταμετράται στο τελικό αποτέλεσμα.

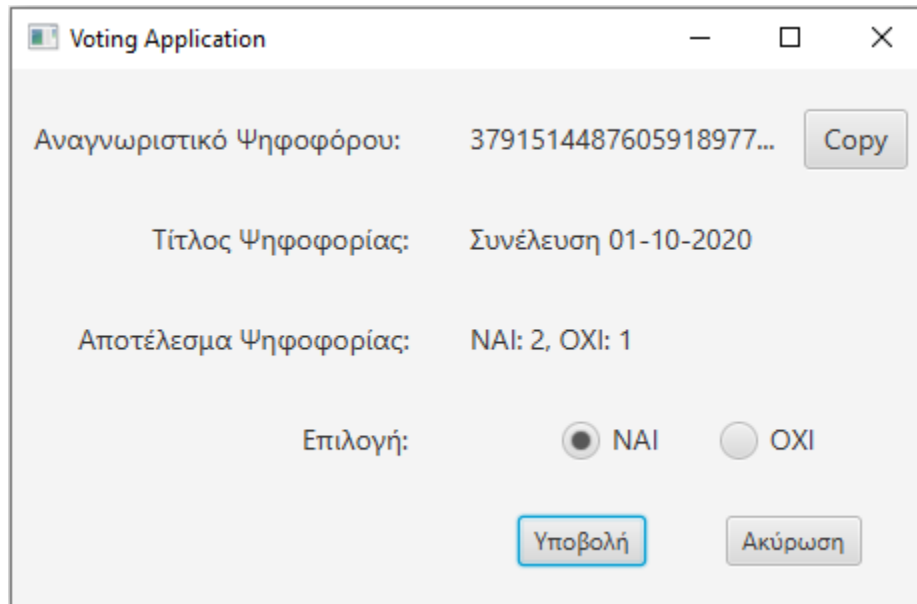
Με την παραγωγή της UID τιμής του, ο χρήστης πρέπει να τη δηλώσει στο διαχειριστή του συστήματος ο οποίος την καταγράφει και την προσθέτει στη λίστα με τις τιμές ψηφοφόρων. Η δήλωση είναι απαραίτητο να γίνεται με τρόπο που να επιτρέπει στο διαχειριστή να επιβεβαιώσει πως ο χρήστης που δηλώνει την UID τιμή είναι όντως αυτός που ισχυρίζεται. Πιθανοί τρόποι είναι είτε να γίνεται η δήλωση αυτοπροσώπως, είτε μέσω της φοιτητικής διεύθυνσης ηλεκτρονικού ταχυδρομείου με την υπόθεση πως δεν έχει κάποιος άλλος πρόσβαση σε αυτήν.

6.4. Σενάριο χρήσης

Ακολουθεί η παρουσίαση, βήμα προς βήμα, του σεναρίου χρήσης της εφαρμογής σε μια εικονική φοιτητική συνέλευση, θεωρώντας πως όλοι οι συμμετέχοντες έχουν δηλώσει τα δημόσια αναγνωριστικά τους στο διαχειριστή.

1. Με τη λήξη της διαβούλευσης, ο διαχειριστής ανοίγει την εφαρμογή, παραμετροποιεί την ψηφοφορία, δίνοντας τα απαραίτητα στοιχεία, και τη δημιουργεί.
2. Οι ψηφοφόροι με τη σειρά τους ανοίγουν την εφαρμογή, συνδέονται στο δίκτυο blockchain και λαμβάνουν τις πληροφορίες της ψηφοφορίας, επιβεβαιώνοντας πως ψηφίζουν σωστά.
3. Κάθε ψηφοφόρος κάνει την επιλογή του και υποβάλει την ψήφο του.

4. Στην περίπτωση που υποβληθούν οι ψήφοι όλων των ψηφοφόρων πριν τη λήξη της ψηφοφορίας, ο διαχειριστής μπορεί πρόωρα να την τερματίσει.
5. Με τον τερματισμό της διαδικασίας, οι ψηφοφόροι συνδέονται στις εφαρμογές τους οι οποίες εκκινούν την εκτέλεση του πρωτοκόλλου υπολογισμού αποτελέσματος.
6. Σε ελάχιστο χρόνο, το αποτέλεσμα εμφανίζεται στις οθόνες της εφαρμογής (Σχήμα 27).



The screenshot shows a window titled "Voting Application". It contains the following elements:

- A field for "Αναγνωριστικό Ψηφοφόρου:" (Voter ID) with the value "3791514487605918977..." and a "Copy" button.
- A field for "Τίτλος Ψηφοφορίας:" (Poll Title) with the value "Συνέλευση 01-10-2020".
- A field for "Αποτέλεσμα Ψηφοφορίας:" (Poll Result) with the value "ΝΑΙ: 2, ΟΧΙ: 1".
- A section for "Επιλογή:" (Selection) with two radio buttons: "ΝΑΙ" (selected) and "ΟΧΙ".
- Two buttons at the bottom: "Υποβολή" (Submit) and "Ακύρωση" (Cancel).

Σχήμα 27: Οθόνη ψηφοφορίας

6.5. Τεχνολογίες που χρησιμοποιήθηκαν

Επιγραμματικά, οι τεχνολογίες και βιβλιοθήκες που χρησιμοποιήθηκαν για την υλοποίηση της εφαρμογής είναι οι εξής:

1. Ethereum blockchain με smart contract γραμμένο στη γλώσσα Solidity για τη διαχείριση των δεδομένων της ψηφοφορίας.
2. RemixIDE (<https://remix.ethereum.org/>) για την υλοποίηση του κώδικα smart contract.
3. Geth Ethereum client, εφαρμογή για τη δημιουργία Ethereum node και για τη διαλειτουργικότητα με το blockchain.
4. JavaSE version 8 για την υλοποίηση της λογικής της εφαρμογής.
5. JavaFX για την υλοποίηση της γραφικής διεπαφής της εφαρμογής.
6. Web3J, open source Java βιβλιοθήκη για την επικοινωνία με τον Geth Ethereum client.

7. UniCrypt, open source Java βιβλιοθήκη μαθηματικών και κρυπτογραφίας για την υλοποίηση του κρυπτο-πρωτοκόλλου, διαθέσιμη μέσω του Bern University of Applied Sciences (BFH).

6.5.1. Ethereum blockchain και smart contract

Το Ethereum Blockchain είναι μια υπάρχουσα τεχνολογία κατακεντρωμένου καθολικού, όπως αυτή του Bitcoin. Σε αντίθεση με αυτό, ο στόχος του Ethereum δεν είναι η υλοποίηση ενός αποκεντρωποιημένου νομισματικού συστήματος αλλά η δημιουργία μιας αποκεντρωποιημένης πλατφόρμας για την εκτέλεση έξυπνων συμβολαίων (smart contract) και γενικά για την υποστήριξη αποκεντρωποιημένων εφαρμογών (Decentralized Applications – DApps).

Smart contracts

Με πολύ απλά λόγια, ένα smart contract, ή έξυπνο συμβόλαιο, είναι μια συμφωνία της οποίας η εκτέλεση είναι αυτοματοποιημένη. Μια πρωτόγονη μορφή μη ψηφιακών τέτοιων συμβολαίων μπορούν να θεωρηθούν οι μηχανές αυτόματης πώλησης (vending machines) ή τα ΑΤΜ. Έχοντας λάβει τις απαραίτητες εισόδους παραμετροποίησης, ένα vending machine, χωρίς επίβλεψη εκτελεί τις ενέργειες που χρειάζεται για να εκπληρώσει τους όρους που έχουν συμφωνηθεί, δηλαδή την παράδοση των αγαθών που επιλέχθηκαν ως αντάλλαγμα των χρημάτων που δόθηκαν.

Στη δική μας περίπτωση όπου ασχολούμαστε με ψηφιακά έξυπνα συμβόλαια, μπορούν να οριστούν ως ένα κομμάτι κώδικα λογισμικού, υλοποιημένο σε μια πλατφόρμα blockchain, το οποίο διαβεβαιώνει για την αυτόνομη και αυτο-επιβαλλόμενη φύση των όρων του, έναυσμα των οποίων είναι προκαθορισμένες συνθήκες κατάστασης του blockchain. Οι ιδιότητες ενός ψηφιακού έξυπνου συμβολαίου είναι [25]:

1. Ηλεκτρονική μορφή
2. Υλοποίηση σε μορφή λογισμικού
3. Εμπιστοσύνη
4. «Υπό όρους» φύση
5. Αυτό-επιβολή
6. Αυτάρκεια

Για την επίτευξη των παραπάνω χρειάζεται μια πλατφόρμα εκτέλεσης κώδικα η οποία να είναι αποκεντρωποιημένη και μη ελεγχόμενη από τρίτα συστήματα όπως το Ethereum Blockchain.

Ethereum Blockchain

Για την υποστήριξη έξυπνων συμβολαίων, το Ethereum Blockchain διαθέτει έναν διερμηνέα κώδικα λεγόμενο EVM (Ethereum Virtual Machine) ο οποίος επιτρέπει την εκτέλεση του συμβολαίου σε μορφή bytecode. Για τη δημιουργία συμβολαίου απαιτούνται τα εξής βήματα:

1. Συγγραφή του συμβολαίου σε μια συμβατή γλώσσα (π.χ. Solidity). Ο κώδικας του συμβολαίου προδιαγράφει τα δεδομένα του και τις μεθόδους που υποστηρίζει και μπορεί να αντιστοιχιστεί για παράδειγμα με το specification μιας κλάσης αντικειμενοστρεφούς προγραμματισμού.
2. Μεταγλώττιση του κώδικα συμβολαίου σε μορφή bytecode με χρήση κατάλληλου μεταγλωττιστή (π.χ. solc).
3. Δημοσίευση του συμβολαίου στο Ethereum blockchain. Κατά τη δημοσίευση ενός συμβολαίου δημιουργείται ένα στιγμιότυπο αυτού η κατάσταση του οποίου είναι αυτό που καταγράφεται ως δεδομένο της αλυσίδας. Η διαδικασία αυτή μπορεί να αντιστοιχιστεί με τη δημιουργία ενός instance μιας κλάσης αντικειμενοστρεφούς προγραμματισμού.

Με την επιτυχή δημοσίευση ενός συμβολαίου, το στιγμιότυπο που δημιουργήθηκε λαμβάνει μια διεύθυνση. Η ενέργεια δημοσίευσης μεταδίδεται σε όλους τους κόμβους του δικτύου ως συναλλαγή δημοσίευσης συμβολαίου, οι οποίοι καταλήγουν να διαθέτουν τον bytecode κώδικα προς εκτέλεση ενώ ταυτόχρονα δημιουργούν ο καθένας το δικό του στιγμιότυπο συμβολαίου. Όταν ένας χρήστης του συμβολαίου θέλει να εκτελέσει μια μέθοδο η οποία αλλάζει την κατάσταση αυτού, το μήνυμα που δημοσιεύεται στο blockchain είναι η μέθοδος που καλείται μαζί με το ορίσματα αυτής. Ο κάθε κόμβος που λαμβάνει το μήνυμα, εκτελεί τοπικά την κλήση χρησιμοποιώντας τον EVM και καταγράφει τη νέα κατάσταση του στιγμιότυπου στην τοπική αλυσίδα του. Αυτό έχει ουσιαστικά ως αποτέλεσμα να μπορούμε να συντηρήσουμε, με αποκεντρωποιημένο τρόπο, ένα πρόγραμμα ή μια εφαρμογή με ασφάλεια.

Voting smart contract

Για να αποφευχθεί η δημιουργία ενός προσαρμοσμένου για ηλεκτρονική ψηφοφορία blockchain, επιλέχθηκε να δημιουργηθεί η υποδομή αυτού σε μορφή Ethereum έξυπνου συμβολαίου. Με χρήση της γλώσσας Solidity, δημιουργήθηκε ένα συμβόλαιο το οποίο επιτρέπει:

1. Παραμετροποίηση της κατάστασης του συμβολαίου με τα στοιχεία της ψηφοφορίας όπως τίτλο, ημερομηνίες διεξαγωγής και λίστα ψηφοφόρων. Τα στοιχεία αυτά γίνονται διαθέσιμα στους ψηφοφόρους μέσω του συμβολαίου, επιτρέποντάς τους να κάνουν τους απαραίτητους ελέγχους για την διασφάλιση της ακεραιότητας της διαδικασίας όπως π.χ. έλεγχο δικαιώματος ψήφου.

2. Αποθήκευση και διάθεση κρυπτογραφημένων ψήφων. Εκτός από την ίδια την ψήφο, δημοσιεύονται και τα υπόλοιπα απαραίτητα στοιχεία όπως το non-interactive proof of validity και η ψηφιακή υπογραφή του ψηφοφόρου που διασφαλίζει την προέλευση της πληροφορίας.
3. Διαχείριση της κατάστασης της ψηφοφορίας. Ο διαχειριστής έχει τη δυνατότητα να την κλείσει πρόωρα αλλάζοντας την κατάσταση του συμβολαίου. Η αλλαγή αυτή γίνεται διαθέσιμη και στους χρήστες οι οποίοι μπορούν αυτόματα να ξεκινήσουν τις διαδικασίες εξαγωγής του αποτελέσματος.

Σημειώνεται πως το έξυπνο συμβόλαιο δεν αντικαθιστά το κρυπτο-πρωτόκολλο ψηφοφορίας που έχει οριστεί. Όπως και με τη χρήση ενός προσαρμοσμένου blockchain, το πρωτόκολλο είναι αυτό που καθορίζει τη μορφή των δεδομένων που καταγράφονται σε αυτό καθώς και τον τρόπο επικοινωνίας των χρηστών του συστήματος. Το έξυπνο συμβόλαιο απλώς μεταφέρει τη blockchain λειτουργικότητα στην υπάρχουσα λύση του Ethereum.

6.5.2. Χρήση βιβλιοθήκης UniCrypt

Η συγκεκριμένη βιβλιοθήκη επιλέχθηκε λόγω της ανάγκης χρήσης μαθηματικών primitive για την υλοποίηση του κρυπτο-πρωτοκόλλου. Το ομομορφικό κρυπτοσύστημα, το Shamir MPC αλλά και το non-interactive proof of validity, τα οποία έχουν προσαρμοστεί συγκεκριμένα για το σενάριο της αποκεντρωποιημένης ψηφοφορίας, δεν υπάρχουν αυτούσια στη μορφή που θέλουμε να τα χρησιμοποιήσουμε. Συνεπώς έγινε υλοποίηση αυτών, με αποτέλεσμα να χρειαστεί μια βιβλιοθήκη που δεν υλοποιεί μόνο κρυπτο-αλγορίθμους αλλά ταυτόχρονα δίνει πρόσβαση και στις μαθηματικές λειτουργίες που τους αποτελούν. Η βιβλιοθήκη UniCrypt καλύπτει τις παραπάνω απαιτήσεις, έχει καλή ταχύτητα εκτέλεσης και κυρίως είναι μια καθαρά Java υλοποίηση, το οποίο απλοποιεί πολύ την ένταξή της στο σύστημα.

6.6. Διαφορές με το σύστημα που παρουσιάστηκε στο 5ο κεφάλαιο

Σε σύγκριση με το σύστημα που παρουσιάστηκε στο 5^ο κεφάλαιο, η proof of concept υλοποίηση που έγινε έχει κάποιες βασικές διαφορές:

1. Η εφαρμογή δεν είναι διαθέσιμη σε οποιαδήποτε internet enabled συσκευή. Στα πλαίσια της εργασίας, κρίθηκε πως η πολυπλοκότητα και οι προκλήσεις της δημιουργίας μιας οικουμενικής εφαρμογής ήταν εκτός του σκοπού αυτής.
2. Δεν έχει υλοποιηθεί καμία λειτουργία τύπου επίβλεψης (auditing) όπως η επισκόπηση των υποβεβλημένων ψήφων. Οι λειτουργίες αυτού του τύπου δεν παρουσιάζουν κάποια τεχνική δυσκολία διότι η υλοποίησή τους απαιτεί ουσιαστικά μια διεπαφή προσπέλασης των δεδομένων του blockchain και στην περίπτωση του PoC του state του smart contract ψηφοφορίας.

3. Επίσης εκτός του σκοπού της εργασίας κρίθηκε και η υλοποίηση blockchain πρωτοκόλλου σε μορφή blockchain client. Επιλέχθηκε η υπάρχουσα λύση του Ethereum συστήματος το οποίο είναι αρκετά εξελιγμένο, ελεγμένο και εύκολα παραμετροποιήσιμο για τους στόχους μας μέσω της τεχνολογίας smart contract. Σημειώνεται παρ' όλα αυτά πως για λόγους ασφαλείας η τεχνολογία δεν συνίσταται για μια πραγματική υλοποίηση συστήματος ψηφοφορίας. Το Ethereum blockchain είναι γενικό και παρέχει πολλές λειτουργίες ώστε να μπορεί να υποστηρίξει κάθε είδους εφαρμογή που θέλει να βασιστεί σε τεχνολογία κατακευματισμένου καθολικού. Αυτό αυξάνει την πολυπλοκότητα της υλοποίησης και γίνεται πολύ πιθανή πηγή λαθών και μη αναμενόμενων συμπεριφορών, κάτι που δεν έχει θέση σε κρίσιμα συστήματα όπως αυτά της ψηφοφορίας. Επίσης η υποδομή των smart contract, παρ' ότι πολύ βολική και ευέλικτη, λόγω του ότι βασίζεται σε Turing complete γλώσσα για την εκτέλεση αυτών επίσης είναι πολύ πιθανή πηγή προβλημάτων. Σε αντίθεση για παράδειγμα, η αλυσίδα Bitcoin, παρ' ότι υποστηρίζει ενός είδους scripting για ενισχυμένες λειτουργίες έχει κάνει τη συνειδητή επιλογή να χρησιμοποιεί Turing complete γλώσσα, περιορίζοντας έτσι την πολυπλοκότητα και τις καταστάσεις στις οποίες μπορεί να βρεθεί το σύστημα.

7. Συμπεράσματα και περαιτέρω εργασία

7.1. Γνώσεις που αποκτήθηκαν μέσω της εκπόνησης της εργασίας

Με την εκπόνηση της εργασίας αυτής, αποκτήθηκαν γνώσεις στους ακόλουθους τομείς:

1. Μαθηματικά.

Ως προεργασία για την κατανόηση των κρυπτογραφικών σχημάτων και τεχνικών, διερευνήθηκε ο τομέας της αφηρημένης άλγεβρας, συγκεκριμένα η αριθμητική υπολοίπων, οι πρώτοι αριθμοί, διακριτοί λογάριθμοι και η θεωρία ομάδων, δακτυλίων και σωμάτων. Επίσης απαραίτητη ήταν και γνώση πάνω σε διάφορα ανοιχτά προβλήματα όπως το Diffie-Hellman problem (DHP) και Decisional Diffie-Hellman (DDH) assumption.

2. Κρυπτογραφία.

Όσον αφορά τις γνώσεις κρυπτογραφίας, καλύφθηκαν οι τομείς της συμμετρικής και ασύμμετρης κρυπτογραφίας, PKI (public key infrastructure), ομομορφικά κρυπτοσυστήματα, διαμοιρασμός μυστικών, υπολογισμός πολλαπλών μερών και αποδείξεις μηδενικής γνώσης.

3. Τεχνολογία κατανεμημένου καθολικού.

Στα πλαίσια της ανάγκης δημιουργίας ενός πλήρως αποκεντροποιημένου και μη ελέγξιμου συστήματος έγινε έρευνα πάνω σε τεχνολογίες κατανεμημένου καθολικού (DLT – blockchain) και κυρίως στις αλυσίδες Bitcoin και Ethereum. Η δεύτερη προσφέρθηκε και για διερεύνηση της τεχνολογίας των έξυπνων συμβολαίων, των πλεονεκτημάτων και των μειονεκτημάτων τους.

4. Υλοποίηση κρυπτοπρωτοκόλλων.

Τέλος, με την υλοποίηση του proof of concept συστήματος ψηφοφορίας φοιτητικής συνέλευσης αποκτήθηκε γνώση σχετικά με την υλοποίηση κρυπτοπρωτοκόλλων και με τη χρήση αντίστοιχων βιβλιοθηκών μαθηματικών και κρυπτογραφίας.

7.2. Τελικά συμπεράσματα

Ένα πλήρως αποκεντροποιημένο σύστημα ψηφοφορίας και γενικότερα μία αποκεντροποιημένη εφαρμογή παρουσιάζει διάφορες προκλήσεις υλοποίησης τόσο τεχνικές όσο και θεωρητικές. Όντας σύστημα κρίσιμης σημασίας όλα τα σενάρια πρέπει να είναι σωστά υλοποιημένα ενώ οι αποφάσεις σχεδίασης, οι επιλεγμένοι αλγόριθμοι και η αρχιτεκτονική πρέπει να έχουν λάβει υπ' όψιν τους όλες τις πιθανές μη αναμενόμενες καταστάσεις, επιθέσεις και ακραίες περιπτώσεις και να τις αντιμετωπίζουν κατάλληλα. Συγκεκριμένα για ένα σύστημα ηλεκτρονικής ψηφοφορίας:

1. Απαιτείται πολύ μεγάλη προσοχή στην επιλογή των κρυπτοσυστημάτων που θα χρησιμοποιηθούν. Ιδανικά πρέπει να εκμεταλλευόμαστε αλγορίθμους με αρκετά μεγάλο παρελθόν οι οποίοι βασίζονται σε ορθό μαθηματικό υπόβαθρο και γνωστά θεωρήματα. Επιπλέον έμφαση πρέπει να δοθεί και στην υλοποίηση του κρυπτοσυστήματος, κάτι που συχνά αποτελεί αδύνατο σημείο και επίκεντρο επιθέσεων από κακόβουλες πλευρές.
2. Απαιτείται επιπλέον πολύ μεγάλη προσοχή και στην επιλογή των εργαλείων, πρωτοκόλλων επικοινωνίας και γενικότερα των στοιχείων που αποτελούν την υποδομή της εφαρμογής. Για άλλη μια φορά, εργαλεία με αποδεδειγμένες ικανότητες και κυρίως σταθερή απόδοση χωρίς προβλήματα είναι προτιμότερα. Από τις υλοποιήσεις πρωτοκόλλων επικοινωνίας μέχρι τη γλώσσα προγραμματισμού, κάθε κομμάτι του συστήματος πρέπει να περάσει από εξονυχιστικό έλεγχο.
3. Ολόκληρος ο σχεδιασμός του συστήματος πρέπει να είναι όσο πιο λιτός γίνεται. Κάθε στοιχείο που συμμετέχει στην υλοποίηση προσθέτει μεγάλη πολυπλοκότητα και δυσκολεύει τόσο τον έλεγχο ορθότητας όσο και την επιδιόρθωση ή επέκτασή της.

Η δημιουργία ενός ορθού και εμπιστεύσιμου συστήματος ηλεκτρονικής ψηφοφορίας σίγουρα θα αποτελέσει τεχνολογικό επίτευγμα παρ' όλα αυτά δεν φαντάζει αδύνατο. Σε αυτό βοηθά και η έλευση της τεχνολογίας blockchain η οποία προσφέρει λύσεις σε διάφορα προβλήματα των πατροπαράδοτων συστημάτων.

1. Επιτρέπει τη λειτουργία ενός συστήματος χωρίς κεντρική διαχείριση και συνεπώς χωρίς κεντρικά σημεία προβλημάτων. Τόσο η έλλειψη εμπιστοσύνης στους διαχειριστές, όσο το γεγονός ότι τα συστήματα αυτά αποτελούν στόχο εξωτερικών επιθέσεων, ένα αποκεντροποιημένο σύστημα καθίσταται προτιμότερο για ηλεκτρονικές ψηφοφορίες.
2. Προτιμάται η χρήση blockchain συστήματος συγκεκριμένα υλοποιημένο για το σκοπό της ψηφοφορίας. Η χρήση τρίτων συστημάτων όπως π.χ. του Ethereum blockchain που έγινε στο case study προσθέτουν πολυπλοκότητα ενώ τα πιθανά προβλήματα που έχουν κληρονομούνται και στο σύστημα ψηφοφορίας.

Τα ομομορφικά κρυπτοσυστήματα και οι αποδείξεις μηδενικής γνώσης καθίστανται σχεδόν απαραίτητα σε ένα αποκεντροποιημένο σύστημα ψηφοφορίας. Χωρίς την ύπαρξη κεντρικής διαχείρισης με ταυτόχρονη απαίτηση τη μυστικότητα της ψήφου, η ομομορφική κρυπτογραφία φαίνεται να είναι η βέλτιστη επιλογή, σε συνδυασμό πάντα με κάποιο συμβατό σύστημα απόδειξης μηδενικής γνώσης ώστε να υπάρχει διασφάλιση της εγκυρότητας της ψήφου.

Τέλος, η δημιουργία ενός συστήματος ψηφοφορίας είναι ένα δύσκολο και απαιτητικό εγχείρημα το οποίο πρέπει να γίνει με τη συνεργασία πολλών ειδημόνων από διάφορους τομείς. Επιπλέον όλα τα στοιχεία που αποτελούν το σύστημα, από την υλοποίηση του blockchain πρωτοκόλλου μέχρι και το μεταγλωττιστή της επιλεγμένης γλώσσας προγραμματισμού πρέπει να είναι ανοιχτού κώδικα και διαθέσιμα για έλεγχο από όλους.

Proof of concept εφαρμογή

Η λύση που παρουσιάστηκε στη συγκεκριμένη εργασία καλύπτει κάποιες από τις παραπάνω προϋποθέσεις, σε καμία περίπτωση όμως δεν πλησιάζει το σημείο όπου θα μπορούσε να χρησιμοποιηθεί με ασφάλεια και σιγουριά. Ο στόχος της συγκεκριμένης υλοποίησης είναι να παρουσιάσει το πρωτόκολλο ψηφοφορίας που σχεδιάστηκε και αναλύθηκε στο 5^ο κεφάλαιο και να αποτελέσει μια βάση πάνω στην οποία μπορεί να μελετηθεί ένα πληρέστερο σύστημα.

7.3. Προτάσεις για περαιτέρω εργασία

Οι παρακάτω τομείς απαιτούν βελτίωση και περαιτέρω έρευνα:

1. Επίλυση των προβλημάτων ψηφοφορίας πολλαπλών επιλογών. Όπως ειπώθηκε και στα προηγούμενα κεφάλαια, κάθε διαθέσιμη επιλογή ψηφοφορίας πρέπει να κωδικοποιείται με μια αριθμητική τιμή, τέτοια ώστε το άθροισμα όλων των πιθανών συνδυασμών αυτών να παράγει πάντα ένα αποτέλεσμα από το οποίο να μπορεί να εξαχθεί ένα συμπέρασμα για τον αριθμό των ψήφων που έλαβε κάθε διαθέσιμη επιλογή. Παρ' ότι προτάθηκε μια λύση για το συγκεκριμένο πρόβλημα στο 5^ο κεφάλαιο, η συγκεκριμένη κωδικοποίηση σε συνδυασμό με το αθροιστικό ομομορφικό σχήμα διακριτού λογαρίθμου δεν μπορεί να εφαρμοστεί σε ρεαλιστικά σενάρια πολλών ψηφοφόρων σε ψηφοφορία πολλαπλών διαφορετικών επιλογών. Απαιτείται λοιπόν η διερεύνηση είτε ενός διαφορετικού συστήματος κωδικοποίησης είτε η χρήση ενός διαφορετικού αθροιστικού ομομορφικού σχήματος.
2. Βελτίωση παραγωγής μοναδικού αναγνωριστικού χρήστη (UID). Αυτή τη στιγμή, για λόγους ευκολίας, για την παραγωγή του UID χρησιμοποιείται ένας κωδικός πρόσβασης σε συνδυασμό με ένα μοναδικό χαρακτηριστικό όπως το φοιτητικό email ή το ΑΦΜ πολίτη. Παρ' όλα αυτά, κρίνεται σκόπιμη η αντικατάσταση ενός κωδικού πρόσβασης με κάτι πιο εύκολα διαχειρίσιμο, ειδικά για τη διευκόλυνση τεχνολογικά ακατάρτιστων ομάδων και ομάδων με δυσκολία συγκράτησης πληροφορίας. Η ασφάλεια ενός κωδικού πρόσβασης εξαρτάται από την πολυπλοκότητά του, είτε σε αριθμό είτε στο συνδυασμό μεγάλης γκάμας χαρακτήρων, κάτι το οποίο αυξάνει την πιθανότητα να ξεχαστεί. Αυτό έχει ως αποτέλεσμα σε πολλές περιπτώσεις οι χρήστες να καταγράφουν τον κωδικό σε φυσική μορφή το οποίο ουσιαστικά ρίχνει τη δυσκολία πρόσβασης από τρίτους στο να βρουν το σημείωμα και να αντιγράψουν τον κωδικό πρόσβασης. Για να αντιμετωπιστεί το παραπάνω πρόβλημα χρειάζεται κάποιου άλλου είδους μη αντιγράψιμο και εύκολα προσβάσιμο χαρακτηριστικό χρήστη, για παράδειγμα ένα είδος βιομετρικού αναγνωριστικού όπως το δακτυλικό αποτύπωμα, η αναγνώριση ίριδας ή προσώπου. Παρ' ότι τέτοιες μέθοδοι χρησιμοποιούνται είδη σε προϊόντα τεχνολογίας όπως για το ξεκλείδωμα smartphone, στη δική μας περίπτωση η ίδια μεθοδολογία δεν μπορεί να εφαρμοστεί. Ο λόγος είναι διότι το αποτέλεσμα βιο-αναγνώρισης είναι μη ντετερμινιστικό και βασίζεται σε πιθανοτικές μεθόδους, κάτι το οποίο είναι εμπόδιο όταν η τιμή αυτή πρέπει να χρησιμοποιηθεί ως seed για την παραγωγή μιας μοναδικής τιμής UID (η οποία στην περίπτωσή μας είναι το public key ενός ασύμμετρου ζεύγους). Απαιτείται λοιπόν περαιτέρω έρευνα στις μεθόδους βιομετρικής αναγνώρισης ή και στην χρήση των αποτελεσμάτων αυτής.

3. Διερεύνηση μεθόδων επιβεβαίωσης εγκυρότητας της εφαρμογής ψηφοφορίας αλλά και της συσκευής εκτέλεσης αυτής. Παρ' ότι η εφαρμογή είναι ανοιχτού κώδικα και η υλοποίηση μπορεί να ελεγχθεί από τον οποιονδήποτε, μεταξύ του κώδικα και της εφαρμογής η οποία τρέχει σε μια συσκευή υπάρχουν πολλά σημεία τα οποία μπορούν να εμφανίσουν θέματα ασφάλειας. Παραδείγματα είναι η διάθεση ενός πειραγμένου binary ή η παράνομη εγκατάσταση κακόβουλου λογισμικού στις συσκευές των χρηστών, το οποίο μπορεί είτε να υποκλέψει τα στοιχεία του χρήστη είτε να επηρεάσει τη λειτουργία της εφαρμογής ψηφοφορίας.
4. Υλοποίηση συστήματος ελέγχου της διαδικασίας και των αποτελεσμάτων αυτής. Παρ' ότι δεν υπάρχει ένας συγκεκριμένος κάτοχος του συστήματος και η πληροφορία είναι ελεύθερα διαθέσιμη σε όλους τους χρήστες, η μορφή αυτής δεν είναι εύκολα διαχειρίσιμη και προσπελάσιμη. Απαιτείται λοιπόν κάποιο σύστημα ελέγχου (auditing) ώστε να μπορεί να επιβεβαιωθεί από τους διαχειριστές μιας ψηφοφορίας ότι η διαδικασία εκτελέστηκε σωστά. Επιπλέον σε περιπτώσεις όπου εμφανίζονται προβλήματα είναι απαραίτητο να μπορεί να εντοπιστεί η πηγή αυτών, ειδικά στην περίπτωση όπου ευθύνεται κάποιος κακόβουλος χρήστης, ώστε να αντιμετωπιστούν κατάλληλα.
5. Έρευνα για την επίλυση προβλήματος ασφάλειας κατά το βήμα της παραγωγής υπερκλειδιού αποκρυπτογράφησης. Όπως παρουσιάστηκε και στο 5^ο κεφάλαιο, ένα από τα τελευταία στάδια της διαδικασίας είναι η παραγωγή του υπερκλειδιού αποκρυπτογράφησης του ομομορφικού αθροίσματος των ψήφων. Για να επιτευχθεί αυτό χρησιμοποιείται η τεχνική ασφαλούς υπολογισμού πολλαπλών μερών (secure multi-party computation) η οποία όμως αυτή τη στιγμή πάσχει από ένα βασικό πρόβλημα το οποίο μπορεί να εμποδίσει την ολοκλήρωση της ψηφοφορίας. Εάν κάποιος χρήστης, όταν κληθεί να μοιραστεί τα Shamir secret shares του κρυφού κλειδιού που χρησιμοποίησε για την κρυπτογράφηση της ψήφου του, επιλέξει να μοιραστεί τα shares μιας άλλης τιμής, τότε το παραγόμενο υπερκλειδί δεν θα μπορεί να αποκρυπτογραφήσει το ομομορφικό άθροισμα των ψήφων και επιπλέον θα είναι αδύνατον να εντοπιστεί ποιος από τους ψηφοφόρους έχει μολύνει τη διαδικασία. Ιδέες για την επίλυση του προβλήματος είναι η διερεύνηση ενός non-interactive proof of value για το πολυώνυμο που χρησιμοποιήθηκε για τα Shamir shares, είτε η ανάπτυξη κάποιας μεθόδου εντοπισμού κακόβουλων χρηστών που μολύνουν τη διαδικασία παραγωγής υπερκλειδιού.

8. Βιβλιογραφία

- [1] A. Kiayias, M. Korman and D. Walluck, "An Internet Voting System Supporting User Privacy," 2006 22nd Annual Computer Security Applications Conference (ACSAC'06), Miami Beach, FL, 2006, pp. 165-174, doi: 10.1109/ACSAC.2006.12.
- [2] Chaum, David. "Random-sample voting." White Paper (2016).
- [3] "How Much Do Elections Cost?" <http://aceproject.org/ace-en/focus/core/crb/crb03> [Jun. 11, 2020]
- [4] Patricia Mazzei, "Two women busted for election fraud in Miami-Dade in 2016", <https://www.miamiherald.com/news/politics-government/election/article111029767.html>, Nov. 14, 2018 [Jun. 11, 2020]
- [5] David L. Chaum. 1981. Untraceable electronic mail, return addresses, and digital pseudonyms. Commun. ACM 24, 2 (Feb. 1981), 84–90. DOI: 10.1145/358549.358563
- [6] "Release of E-Election Software Code 'Did Not Go Far Enough'" <https://news.err.ee/107807/release-of-e-election-software-code-did-not-go-far-enough>, Jul. 17, 2013 [Aug. 26, 2020]
- [7] Adida, Ben. "[Helios: Web-based Open-Audit Voting](#)" March. 15, 2018 [Aug. 27, 2020]
- [8] P. Y. A. Ryan, D. Bismark, J. Heather, S. Schneider and Z. Xia, "Prêt À Voter: a Voter-Verifiable Voting System," in IEEE Transactions on Information Forensics and Security, vol. 4, no. 4, pp. 662-673, Dec. 2009, doi: 10.1109/TIFS.2009.2033233
- [9] "Elliptic Curve Cryptography & Online Voting" <https://followmyvote.com/elliptic-curve-cryptography/> [Aug. 27, 2020]
- [10] Jimmy Song, "Why Blockchain is Hard", <https://medium.com/@jimmysong/why-blockchain-is-hard-60416ea4c5c>, May. 14, 2018 [Jun. 11, 2020]
- [11] "Mining", <https://en.bitcoin.it/wiki/Mining>, Jun. 2, 2020 [Jun. 11, 2020]
- [12] Pinzón, Carlos & Rocha, Camilo. (2016). Double-spend Attack Models with Time Advantage for Bitcoin. Electronic Notes in Theoretical Computer Science. 329. 79-103. 10.1016/j.entcs.2016.12.006.
- [13] Satoshi Nakamoto. Re: Bitcoin P2P e-cash paper. satoshi@vistomail.com (Nov. 13, 2008) <https://www.mail-archive.com/cryptography@metzdowd.com/msg09997.html>
- [14] Kiayias, A. (2005). CSE 364 Cryptography : Primitives and Protocols Lecture Notes.

- [15] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," Proceedings 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA, 1994, pp. 124-134, doi: 10.1109/SFCS.1994.365700.
- [16] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in IEEE Transactions on Information Theory, vol. 31, no. 4, pp. 469-472, July 1985, doi: 10.1109/TIT.1985.1057074.
- [17] Cramer R., Gennaro R., Schoenmakers B. (1997) A Secure and Optimally Efficient Multi-Authority Election Scheme. In: Fumy W. (eds) Advances in Cryptology — EUROCRYPT '97. EUROCRYPT 1997. Lecture Notes in Computer Science, vol 1233. Springer, Berlin, Heidelberg.
- [18] Adi Shamir. 1979. How to share a secret. Commun. ACM 22, 11 (Nov. 1979), 612–613. DOI: 10.1145/359168.359176
- [19] C. P. Schnorr. Efficient signature generation by smart cards. Journal of Cryptology, 4(3):161–174, 1991
- [20] FUNCTIONAL REQUIREMENTS FOR A SECURE ELECTRONIC VOTING SYSTEM https://link.springer.com/content/pdf/10.1007%2F978-0-387-35586-3_40.pdf
- [21] Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." White Paper, Nov. 11, 2008, <https://bitcoin.org/bitcoin.pdf>
- [22] M. Blum, P. Feldman, and S. Micali, "Non-interactive zero-knowledge and its applications," in Proceedings of the 20th Annual ACM symposium on Theory of computing (STOC '88), pp. 103–112, ACM, 1988.
- [23] Wikipedia, The Free Encyclopedia, s.v. "Proof of work" (accessed Feb. 10, 2020), https://en.wikipedia.org/wiki/Proof_of_work
- [24] Wikipedia, The Free Encyclopedia, s.v. "Hashcash" (accessed Feb. 22, 2020), <https://en.wikipedia.org/wiki/Hashcash>
- [25] Savelyev, Alexander, Contract Law 2.0: «Smart» Contracts As the Beginning of the End of Classic Contract Law (December 14, 2016). Higher School of Economics Research Paper No. WP BRP 71/LAW/2016.