2022-01

þÿ B l o c k c h a i n b a s e d e v o t i n g s y

þÿ µ ¼ À ¹ Ã Ä ¿ Ã Í ½ · º ± ¹ Ã Å ¼ ¼ µ Ä ¿ Ç ®

þÿ µ º » ¿ ³ - É ½ Ã Ä · ½ µ º » ¿ ³ ¹ º ® ´ ¹ ± ´ ¹

þÿ œ À ¿ » ¿ ² ¯ ½ · Â , “ µ Î Á ³ ¹ ¿ Â

þÿ œ µ Ä ± À Ä Å Ç ¹ ± º Ì Á Ì ³ Á ± ¼ ¼ ± Ã Ä ± » · Á ¿ Æ ¿ Á ¹ ± º ¬ £ Å Ã Ä ® ¼ ± Ä ± º ± ¹ Ä · ½ ¨ · Æ ¹ ± º
þÿ £ Ç ¿ » ® ” ¹ ¿ ¯ º · Ã · Â º ± ¹ • À ¹ Ã Ä ® ¼ · Â ¥ À ¿ » ¿ ³ ¹ Ã Ä Î ½ , ± ½ µ À ¹ Ã Ä ® ¼ ¹ ¿ • µ ¬ À ¿ » ¹ Â

ΙΑΝΟΥΑΡΙΟΣ 2022

ΣΧΟΛΗ

Οικονομικών, Διοίκησης και Πληροφορικής

ΤΙΤΛΟΣ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΔΙΑΤΡΙΒΗΣ:

Blockchain based e – voting systems: εμπιστοσύνη και συμμετοχή των εκλογέων στην εκλογική διαδικασία.

Γεώργιος Μπολοβίνης

Ιανουάριος, 2022

ΣΧΟΛΗ

Οικονομικών, Διοίκησης και Πληροφορικής

ΤΙΤΛΟΣ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΔΙΑΤΡΙΒΗΣ:

Blockchain based e – voting systems: εμπιστοσύνη και συμμετοχή των εκλογέων στην εκλογική διαδικασία.

Διατριβή η οποία υποβλήθηκε προς απόκτηση εξ αποστάσεως μεταπτυχιακού τίτλου σπουδών στα Πληροφοριακά Συστήματα και Ψηφιακή Καινοτομία στο Πανεπιστήμιο Νεάπολις

Γεώργιος Μπολοβίνης

Ιανουάριος, 2022

Πνευματικά δικαιώματα

ΠΕΡΙΕΧΟΜΕΝΑ

Κατάλογος εικόνων

Κατάλογος διαγραμμάτων

“ΣΕΛΙΔΑ ΕΓΚΥΡΟΤΗΤΑΣ” (“VALIDATION PAGE”)

Ονοματεπώνυμο Φοιτητή: Γεώργιος Μπολοβίνης

Τίτλος Μεταπτυχιακής Διατριβής: Blockchain based e – voting systems: εμπιστοσύνη και συμμετοχή των εκλογέων στην εκλογική διαδικασία.

Η παρούσα Μεταπτυχιακή Διατριβή εκπονήθηκε στο πλαίσιο των σπουδών για την απόκτηση εξ αποστάσεως μεταπτυχιακού τίτλου στο Πανεπιστήμιο Νεάπολις και εγκρίθηκε στις…….από τα μέλη της Εξεταστικής Επιτροπής.

Εξεταστική Επιτροπή:

Πρώτος επιβλέπων (Πανεπιστήμιο Νεάπολις Πάφος)……[ονοματεπώνυμο, βαθμίδα, υπογραφή]

Μέλος Εξεταστικής Επιτροπής: ……[ονοματεπώνυμο, βαθμίδα, υπογραφή]

Μέλος Εξεταστικής Επιτροπής: ……[ονοματεπώνυμο, βαθμίδα, υπογραφή

Ευχαριστίες

Ευχαριστώ θερμά το Δρ Χατζηχριστοφή Σάββα για την υποστήριξη του, καθ΄όλη την εκπόνηση της μεταπτυχιακής διατριβής.

Περίληψη

Η παρούσα μεταπτυχιακή διατριβή συνιστά βιβλιογραφική ανασκόπηση, με σκοπό τη μελέτη των ηλεκτρονικών συστημάτων ψηφοφορίας που βασίζονται στην τεχνολογία του Blockchain (Blockchain based e – voting systems) και συγχρόνως την εμπιστοσύνη που επιδεικνύουν οι εκλογείς σε αυτά κατά τη συμμετοχή τους στην εκλογική διαδικασία.

Προς τούτο, εξετάζονται βασικές παράμετροι ενός ηλεκτρονικού συστήματος ψηφοφορίας όπως η ασφάλεια της εκλογικής διαδικασίας, η ορθότητα της καταμέτρησης των ψήφων, η εγκυρότητα του εκλογικού αποτελέσματος, η διαφάνεια της διαδικασίας, ο ετεροκαθορισμός της πολιτικής βούλησης κατά την άσκηση του εκλογικού δικαιώματος και στο πώς οι παράμετροι αυτές επηρρεάζουν τη συμμετοχή των εκλογέων στην εκλογική διαδικασία.

Στο πλαίσιο της διατριβής επεξηγούνται θεμελιώδεις όροι, όπως τεχνολογία του Blockchain, διακρίσεις του Blockchain, εφαρμογές του Blockchain, πλεονεκτήματα και μειονεκτήματα αυτού καθώς και ζητήματα ασφάλειας που ενδεχομένως διαταράσσουν την εύρυθμη λειτουργία του.

Για την εκπόνηση της διατριβής αναζητήθηκαν ηλεκτρονικές πηγές πληροφόρησης στη βιβλιογραφική βάση Scopus (https://www.scopus.som), στο αντίστοιχο τμήμα του δεκαδικού συστήματος ταξινόμησης DEWEY, οι οποίες σχετίζονται με την τεχνολογία του Blockchain και τα εκλογικά συστήματα. Η αναζήτηση πραγματοποίηθηκε το Σεπτέμβριο του 2021 στην αγγλική γλώσσα. Κατόπιν ορισμού των κριτηρίων συμπερίληψης και αποκλεισμού, επελέγησαν και αναλύθηκαν συνολικά είκοσι (20) άρθρα. Τα αποτελέσματα της αναζήτησης κατέδειξαν την αυξανόμενη τάση του ερευνητικού ενδιαφέροντος σε αυτό το θεματικό πεδίο.

Εν συνεχεία, παρουσιάζονται τα ηλεκτρονικά συστήματα ψηφοφορίας και αναφέρονται η αρχιτεκτονική του συστήματος, οι οντότητες του συστήματος, η πειραματική εφαρμογή τους (σε όσα πραγματοποιήθηκε) και η εξαγωγή των συμπερασμάτων της πειραματικής διαδικασίας.

Εν τέλει, καταγράφονται συμπεράσματα σχετικά με τα βασικά ερωτήματα που θέτει η έρευνα. Στο πλαίσιο αυτό, αξιολογείται συγκεκριμένα το ηλεκτρονικό σύστημα της Εσθονίας και συνεκτιμώνται αποτελέσματα διαδικτυακής έρευνας που αφορούν στα εκλογικά συστήματα και την εκλογική συμπεριφορά.

Λέξεις κλειδιά: Blockchain, e – voting systems, e – democracy, εμπιστοσύνη εκλογέων, συμμετοχή εκλογέων.

Abstract

This master – thesis consists a literary review, focusing on Blockchain voting systems as well as on voters' confidence during the e – voting election process.

That for, basic parameters of an e – voting system such as procedure safety, autiding correctness, result integrity, procedure transaparency and coercion during voting, are examined. At the same time, is examined the impact of the foretold parameters on voters' election behavior.

Within this master – thesis, basic key concepts such as Blockchain, Blockchain types, Blockchain applications, Blockchain advantages and disadvantages as well as safety issues concerning Blockchain's technology are briefly examined.

During this master thesis, a search of electronic bibliographic sources was hold at Scopus sources (https://www.scopus.com), including the terms "Blockchain" and "voting systems". The search, was carried out in September 2021 in English. After having defined the inclusion and exclusion criteria, twenty academic articles were chosen and therefore analysed. The search results clearly showed the increasing researchers interest in that topic.

Afterwards, the e – voting systems are presented as well as the system architecture, entities, techniques, experimental implementation and empirical results are analysed.

Finally, results regarding the basic querries of this master thesis are recorded. Within that framework, the Estonian e – voting system is examined and the results of an internet scale research, regarding the election systems and voters behavior, are evaluated.

Keywords: Blockchain, e – voting systems, e – democracy, voters trust, voters participation.

Κεφάλαιο 1: Εισαγωγή

1.1 Η τεχνολογία του Blockchain

Η τεχνολογία του Blockchain αποτελεί τα τελευταία χρόνια μία ταχύτατα αναπτυσσόμενη προσέγγιση η οποία έχει βρει σημαντικές εφαρμογές κυρίως σε περιπτώσεις όπου η ασφάλεια, είναι βασική παράμετρος των απαιτήσεων. Η κύρια ιδέα πίσω από το blockchain, είναι να διανείμει την αρχή επικύρωσης των συναλλαγών σε μια κοινότητα κόμβων και να χρησιμοποιήσει κρυπτογραφικές τεχνικές για να εγγυηθεί το αμετάβλητο των συναλλαγών. Μία γενική περιγραφή του blockchain το προσδιορίζει ως μία ακολουθία (αλυσίδα – chain) από συγκροτήματα (blocks) οντοτήτων, η οποία σχηματίζει έναν κατάλογο καταγραφής (ledger) οντοτήτων. Η καταγραφή των οντοτήτων στα blocks και η τοποθέτηση των blocks στην αλυσίδα γίνεται με τρόπο τέτοιο, που η οποιαδήποτε μεταβολή σε ένα και μόνο χαρακτηριστικό από τις καταγεγραμμένες οντότητες είναι απολύτως ανιχνεύσιμη. Αυτό συμβαίνει, διότι κάθε Block συνδέεται κατά κάποιο μονοσήμαντο τρόπο τόσο με το προηγούμενο του όσο και με το επόμενο του, ώστε κάθε αλλαγή σε κάποιο από αυτά θα προκαλούσε ασυμβατότητες σε όλο το blockchain. Επιπλέον η δημιουργία του κάθε block γίνεται μέσα από πολύπλοκους αλγορίθμους που είναι δύσκολο να αναλυθούν. Το χαρακτηριστικό αυτό, είναι που καθιστά την προσέγγιση αυτή κατάλληλη οποτεδήποτε είναι ζωτικής σημασίας η αποτροπή παραχάραξης ή πλαστογράφησης μίας οντότητας. Επίσης το βασικό αυτό χαρακτηριστικό του blockchain, είναι ζητούμενο και σε περιπτώσεις όπου είναι απαιτητή ισχυρή κρυπτογράφηση. Η πολυπλοκότητα της κατασκευής του και η αντοχή της σε επίθεσης κρυπτανάλυσης, της δίνουν την δυνατότητα να λειτουργεί στο ανασφαλές περιβάλλον του διαδικτύου χωρίς να χρειάζεται να παρεμβάλλεται μία διαχειριστική έμπιστη αρχή(Choo, Ozcan, Dehhantanha & Parizi, 2020) (Monrat, Schelen, Anderson, 2020).

Το blockchain είναι ουσιαστικά ένα ψηφιακό μέσο καταγραφής δοσοληψιών που αντιγράφεται και διανέμεται σε ολόκληρο το δίκτυο υπολογιστών που συμμετέχουν στο σύστημα. Η πρόσβαση σε αυτό το μέσο ελέγχεται από άλλους συμμετέχοντες στο σύστημα. Κάθε μπλοκ στην αλυσίδα περιέχει έναν αριθμό συναλλαγών και κάθε φορά που πραγματοποιείται μια νέα συναλλαγή, μια αντίστοιχη εγγραφή αυτής της συναλλαγής προστίθεται σε ένα block το οποίο είναι ενεργό. Όταν το block αυτό συμπληρωθεί με έναν προκαθορισμένο αριθμό δοσοληψιών, τοποθετείται στην αλυσίδα αφού συνδεθεί με μοναδικό τρόπο με το προηγούμενο block. Οι δοσοληψίες καταγράφονται και διατηρούνται από όλους τους χρήστες με αμετάβλητο και επαληθεύσιμο τρόπο. Η αλυσίδα που δημιουργείται με τον τρόπο αυτό, συνιστά ένα είδος αποκεντρωμένης βάσης δεδομένων, της

οποίας η διαχείριση δεν είναι αρμοδιότητα μίας συγκεκριμένης οντότητας αλλά κατανέμεται σε όλους όσους συνεισφέρουν στην ανάπτυξη της. Η προσέγγιση αυτή για την αποθήκευση και διαχείριση δεδομένων ονομάζεται Distributed Ledger Technology (DLT). Τα χαρακτηριστικά των υλοποιήσεων που βασίζονται στην DLT είναι (Natarajan H., Krause, S, Gradstein, H., 2017):

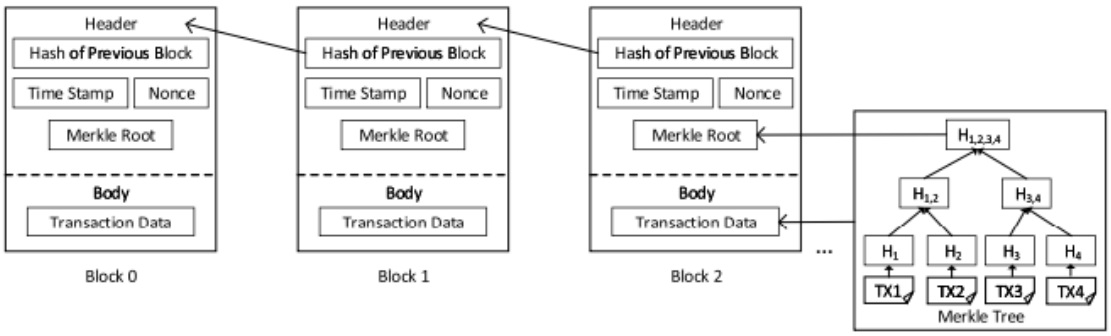
- Μπορούν να εκτελούν αυτοματοποιημένες, προγραμματίσιμες λειτουργίες.
- Εξασφαλίζονται από ισχυρές κρυπτογραφήσεις
- Είναι κατανεμημένες καθώς όλες οι οντότητες που συμμετέχουν κρατούν ένα αντίγραφο του καταγραφέα. Με αυτό τον τρόπο παράλληλα εξασφαλίζεται και η διαφάνεια των δοσοληψιών.
- Οι έγκυρες εγγραφές είναι προστατευμένες από τυχόν προσπάθειες αλλοίωσης ή παραχάραξης καθώς η μορφή με την οποία αποθηκεύονται εξαρτάται και είναι συνάρτηση του συνόλου της αλυσίδας του καταγραφέα.
- Παρέχουν υψηλό βαθμό ανωνυμίας στους συμμετέχοντες καθώς δεν είναι απαραίτητο οι οντότητες που τους αντιπροσωπεύουν στα συστήματα δοσοληψίων να περιλαμβάνουν την πραγματική τους ταυτότητα.
- Κάθε συναλλαγή προσδιορίζεται οπωσδήποτε και από τη στιγμή (ακριβής ημερομηνία – ώρα) που πραγματοποιήθηκε.
- Όλες οι συμμετέχουσες οντότητες συμφωνούν για την εγκυρότητα της κάθε εγγραφής στον καταγραφέα.

Το Blockchain είναι ουσιαστικά μια ανοιχτή κατανεμημένη βάση δεδομένων που διατηρείται από κόμβους σε δίκτυο ομότιμων κόμβων (Peer-to-Peer P2P). Όταν ένα blockchain χρησιμοποιείται για την καταγραφή δοσοληψιών μεταξύ κόμβων, μπορεί να θεωρηθεί ως κατανεμημένος κατάλογος. Μέσω κρυπτογραφικών τεχνικών, οι συναλλαγές που καταγράφονται σε ένα blockchain είναι ανθεκτικές στην παραποίηση. Με την διανομή αντιγράφων του καταλόγου σε όλους τους κόμβους του δικτύου, ένα blockchain μπορεί να ανταπεξέλθει εύκολα σε αστοχίες (σε σχέση με αντίστοιχα κεντρικοποιημένα συστήματα αποθήκευσης δεδομένων) (Rawat, Chaudhary, &Doku, 2020).

1.2 Δομή

Σε ένα δίκτυο που βασίζεται στην τεχνολογία blockchain, οι δοσοληψίες επικυρώνονται από μια κοινότητα κόμβων και στη συνέχεια καταγράφονται σε ένα μπλοκ. Κάθε μπλοκ αποτελείται από δύο βασικά τμήματα: μια κεφαλίδα και το τμήμα των δεδομένων των συναλλαγών. Η κεφαλίδα μπλοκ περιλαμβάνει την κατακερματισμένη σύνοψη του προηγούμενου μπλοκ, μια χρονοσφραγίδα (timestamp), το Nonce και τη ρίζα

Merkle. Η τιμή κατακερματισμού υπολογίζεται περνώντας την κεφαλίδα του προηγούμενου μπλοκ σε μια συνάρτηση κατακερματισμού. Με τον κατακερματισμό του προηγούμενου μπλοκ που είναι αποθηκευμένος στο τρέχον μπλοκ, το blockchain αυξάνεται με τα νέα μπλοκ που δημιουργούνται, να συνδέονται με αυτό. Επιπλέον, η μεθοδολογία αυτή της παραγωγής και ενσωμάτωσης της σύνοψης του προηγούμενου block στο τρέχον εγγυάται ότι η όποια παραποίηση σε κάποιο από τα block θα είναι εφικτό να εντοπιστεί. Η χρονική σήμανση αντιστοιχεί στην χρονική στιγμή που δημιουργείται το block. Το πεδίο Nonce χρησιμοποιείται στη δημιουργία και επαλήθευση ενός μπλοκ. Το δέντρο Merkle είναι ένα δυαδικό δέντρο στο οποίο κάθε κόμβος φύλλου επισημαίνεται με το hash μιας συναλλαγής, αποθηκευμένο στο σώμα του μπλοκ και τους εσωτερικούς κόμβους να επισημαίνονται με τη συνένωση του κατακερματισμού των θυγατρικών κόμβων τους. Η ρίζα Merkle, δηλαδή ο κατακερματισμός ρίζας ενός δέντρου Merkle, χρησιμοποιείται για τη μείωση των προσπαθειών επαλήθευσης των συναλλαγών σε ένα μπλοκ. Δεδομένου ότι μια μικρή αλλαγή σε μία συναλλαγή μπορεί να παράγει μια σημαντικά διαφορετική ρίζα Merkle, η επαλήθευση μπορεί να ολοκληρωθεί με απλή σύγκριση της ρίζας Merkle αντί για επαλήθευση όλων των συναλλαγών στο block (Hassan, Ali, Rahouti, Latif, &Kanhere, 2020). Στο παρακάτω σχήμα παρουσιάζεται η γενική μορφή μίας blockchain και των κόμβων της.



Εικόνα 1: Δομή block και blockchain

Συνοψίζοντας, τα δομικά στοιχεία και οι οντότητες που περιλαμβάνει η αρχιτεκτονική της τεχνολογίας του blockchain είναι:

- Κόμβος: Χρήστες ή υπολογιστές σε διάταξη blockchain (κάθε συσκευή έχει διαφορετικό αντίγραφο ενός πλήρους βιβλίου από το blockchain).
- Συναλλαγή: Είναι το μικρότερο δομικό στοιχείο του συστήματος blockchain (ταυτότητα και λεπτομέρειες περιγραφής), το οποίο χρησιμοποιεί το blockchain.

- Block: Ένα block είναι μια συλλογή δομών δεδομένων που χρησιμοποιούνται για την επεξεργασία συναλλαγών μέσω του δικτύου που διανέμονται σε όλους τους κόμβους.
- Αλυσίδα: Μια σειρά μπλοκ με μια συγκεκριμένη σειρά.
- Miners: Αντίστοιχοι κόμβοι για την επικύρωση της συναλλαγής και την προσθήκη αυτού του μπλοκ στο σύστημα blockchain.
- Συναίνεση: Μια συλλογή εντολών και λειτουργιών για την εκτέλεση διαδικασιών σχηματισμού του blockchain(Jafar, Juzaiddin, Aziz, & Shukur, 2021).

1.3 Κατηγορίες Blockchain

Βάσει του κανόνα για τη ρύθμιση των κόμβων στους οποίους μπορούν να έχουν πρόσβαση, την επαλήθευση και την επικύρωση των συναλλαγών που ξεκινούν από άλλους κόμβους, τα blockchains συνήθως χωρίζονται σε δημόσια blockchains, ιδιωτικά blockchains και κοινοπραξίες blockchains. Η χρήση κάθε κατηγορίας εξαρτάται από τις απαιτήσεις που καλείται να ικανοποιήσουν. (Wang, J., Wu, P., Wang, X., 2017)

- Δημόσια Blockchain: Τα δημόσια Blockchain σχεδιάζονται για να είναι προσβάσιμα και επαληθεύσιμα από όλους τους κόμβους στο δίκτυο. Συγκεκριμένα, όλοι οι κόμβοι σε ένα δημόσιο δίκτυο blockchain μπορούν να επαληθεύσουν συναλλαγές, να διατηρήσουν ένα τοπικό αντίγραφο του blockchain και να δημοσιεύσουν ένα νέο μπλοκ στο blockchain. Με την παροχή της εξουσιοδότησης διατήρησης ενός καθολικού αντιγράφου σε όλους τους κόμβους, τα δημόσια blockchains κατανέμονται πλήρως. Ένα τέτοιο blockchain χρησιμοποιείται ευρέως σε ανώνυμες συναλλαγές. Μειονέκτημα της προσέγγισης αυτής αποτελεί το γεγονός ότι οι συναλλαγές εκτελούνται σε χαμηλές ταχύτητες καθώς η επικύρωση των συναλλαγών περιλαμβάνει επεξεργασίες υψηλής πολυπλοκότητας για να διασφαλιστεί η εγκυρότητα του block που δημιουργείται και τοποθετείται στην blockchain. Παράδειγμα εφαρμογής δημοσίου blockchain είναι το σύστημα – δικτύου που υποστηρίζει το κρυπτονόμισμα Bitcoin.
- Ιδιωτικά blockchain: Συνήθως διατηρούνται από έναν μόνο οργανισμό. Τα δικαιώματα πρόσβασης στο blockchain και η επαλήθευση των συναλλαγών παραχωρούνται μέσω κεντρικού ελεγκτή στους κόμβους που είναι εξουσιοδοτημένοι να συμμετέχουν στο αντίστοιχο δίκτυο. Έτσι δημιουργείται ένα δίκτυο με αδειοδοτούμενους κόμβους, στο οποίο μόνο οι

εξουσιοδοτημένοι κόμβοι μπορούν να έχουν πρόσβαση σε ορισμένες συναλλαγές του blockchain ή/και να συμμετάσχουν στην εργασία για τη δημοσίευση νέων μπλοκ. Με αυτόν τον τρόπο, το απόρρητο των συναλλαγών βελτιώνεται σημαντικά και η αποκέντρωση της εξουσίας επικύρωσης συναλλαγών τελεί υπό τον έλεγχο του οργανισμού. Επιπλέον, με υψηλό επίπεδο εμπιστοσύνης μεταξύ των κόμβων στο δίκτυο, δεν απαιτείται αλγόριθμος επικύρωσης της ένταξης του μπλοκ στην αλυσίδα.

Blockchain κοινοπραξίας (Consortium Blockchain): Βασίζεται στην ίδια ιδέα που βασίζεται και το ιδιωτικό blockchain με την έννοια ότι και τα δύο υποστηρίζουν δίκτυα αδειοδοτημένων κόμβών. Η διαφορά είναι ότι στην κοινοπραξία blockchain, υπάρχουν πολλοί οργανισμοί που μοιράζονται το δικαίωμα πρόσβασης και επικύρωσης των συναλλαγών. Αν και αυτοί οι οργανισμοί μπορεί να μην εμπιστεύονται πλήρως ο ένας τον άλλον, μπορούν να συνεργαστούν αλλάζοντας τον αλγόριθμο συναίνεσης με βάση το επίπεδο εμπιστοσύνης μεταξύ τους (Choo, Ozcan, Dehghantanha, &Parizi, 2020)

Χαρακτηριστικά ασφαλείας των δημοσίων Blockchain

Τα χαρακτηριστικά ενός δημόσιου blockchain συνοψίζονται παρακάτω.

- Αποκέντρωση: Σε ένα δημόσιο δίκτυο blockchain, οι συναλλαγές καταγράφονται από όλους τους κόμβους του δικτύου και κάθε κόμβος έχει ένα τοπικό αντίγραφο του καθολικού καταλόγου στο οποίο καταγράφονται οι συναλλαγές. Με αυτόν τον τρόπο, το κατανεμημένο βιβλίο προστατεύεται από το μοναδικό σημείο αστοχίας.
- Μη εμπιστεύσιμο : Σε ένα δίκτυο blockchain, δεν απαιτείται η συμμετοχή μίας αξιόπιστης τρίτης οντότητας για την επικύρωση των συναλλαγών. Επιπλέον δεν χρειάζεται ο κάθε κόμβος να εμπιστεύεται άλλους για να μπορούν να πραγματοποιούν συναλλαγές. Ο αλγόριθμος συναίνεσης στο blockchain χρησιμοποιείται για την επικύρωση και καταγραφή των συναλλαγών με πιο δίκαιο - πλουραλιστικό τρόπο από την κεντρικοποιημένη προσέγγιση διαχείρισης των συναλλαγών.
- Αμετάβλητο: Χρησιμοποιώντας μια μονόδρομη κρυπτογραφική συνάρτηση κατακερματισμού, οποιαδήποτε τροποποίηση των προηγούμενων μπλοκ σε ένα blockchain ακυρώνει όλα τα συνακόλουθα δημιουργημένα μπλοκ. Έτσι, για να αλλοιώσει τις συναλλαγές που καταγράφηκαν σε προηγούμενο μπλοκ,

ο κακόβουλος κόμβος πρέπει να δημιουργήσει ένα νέο μπλοκ και να αναπαράγει όλα τα ακόλουθα μπλοκ. Καθώς άλλοι κόμβοι συνεχίζουν να δημιουργούν νέα μπλοκ, η κακόβουλη παρεμβολή είναι υπολογιστικά δύσκολο να επιτευχθεί χωρίς να γίνει αντιληπτή, γεγονός που καθιστά το blockchain ανθεκτικό σε επιθέσεις.

- Μη αποποίηση ευθύνης: Μια συναλλαγή υπογράφεται κρυπτογραφικά με ιδιωτικό κλειδί πριν μεταδοθεί σε άλλους. Η επαλήθευση ταυτότητας των συναλλαγών μπορεί να επαληθευτεί από άλλους μέσω του αντίστοιχου δημόσιου κλειδιού που είναι προσβάσιμο σε άλλους κόμβους. Δεδομένου ότι το ιδιωτικό κλειδί διατηρείται από τον κάτοχό του, αποκλείεται ένας κόμβος να μπορεί να μεταμφιεστεί σε άλλους για να ξεκινήσει συναλλαγές και μια επαληθευμένη συναλλαγή δεν μπορεί να αρνηθεί από τον συντάκτη της.
- Διαφάνεια: Σε ένα δημόσιο δίκτυο blockchain, κάθε κόμβος μπορεί να έχει πρόσβαση στις συναλλαγές που είναι αποθηκευμένες στο blockchain και να επαληθεύει τις συναλλαγές που έχουν καταχωρηθεί. Τα δεδομένα που αποθηκεύονται σε blockchain είναι επομένως διαφανή για όλους τους συμμετέχοντες, στο αντίστοιχο δίκτυο, κόμβους.
- Ιχνηλασιμότητα: Η κεφαλίδα μπλοκ προσαρτάται με μια χρονική σήμανση η οποία καταγράφει τον χρόνο δημιουργίας του μπλοκ. Οι κόμβοι μπορούν έτσι εύκολα να επαληθεύσουν και να εντοπίσουν την προέλευση των παρελθόντων μπλοκ(Liang, 2020).

1.4 Επιθέσεις

Αν και σχετικά ασφαλές, το blockchain εξακολουθεί να κινδυνεύει από πολλαπλά είδη επιθέσεων, όπως SelfishMining, MajorityAttack και επίθεση άρνησης υπηρεσίας (DenialOfService - DOS) (Al-Farsi, Rathore, &Bakiras, 2021) (Gomathi, Soni, Dhiman, &G, 2021).

1.4.1 Selfish Mining

Πρόκειται για μορφή επιθέσεων όπου εφαρμόζεται από τους κακόβουλους κόμβους για να παρακρατήσουν τα μπλοκ που έχουν εξορύξει με επιτυχία ή για να τα κρατήσουν και στη συνέχεια να απελευθερώσουν τα αντίστοιχα μπλοκ. Με αυτόν τον τρόπο, οι κόμβοι μπορούν να κάνουν άλλους miners να σπαταλήσουν τους υπολογιστικούς τους πόρους για να βρουν το Nonce που έχει βρεθεί ήδη από τους επιτιθέμενους. Από την άλλη πλευρά,

παρακρατώντας ένα mined block, ο επιτιθέμενος μπορεί να ξεκινήσει νωρίτερα από άλλους για να βρει το Nonce του επόμενου μπλοκ.

1.4.2 MajorityAttack

Αυτό το είδος επίθεσης συμβαίνει όταν ένας κόμβος ή ένας συνδυασμός κόμβων κατέχουν περισσότερο από το 50% των υπολογιστικών πόρων όλων των κόμβων στο δίκτυο. Με τον αλγόριθμο συναίνεσης PoW, τέτοιοι κόμβοι έχουν πιθανότητα μεγαλύτερη από 50% να επιτύχουν τη δημιουργία και τη δημοσίευση ενός νέου μπλοκ. Έτσι, μπορούν αυθαίρετα να αντιστρέψουν ή να σταματήσουν τις συναλλαγές δημοσιεύοντας νέα μπλοκ. Η επίθεση της πλειοψηφίας μπορεί επίσης να εκτελεστεί από έναν επιτιθέμενο χωρίς τόσο μεγάλο υπολογιστικό ποσοστό υπολογιστικών πόρων. Μπορούν να χρησιμοποιήσουν άλλους κόμβους για να το βοηθήσουν να επεκτείνει ιδιωτικά μια αλυσίδα με ένα μπλοκ που δημοσιεύεται από αυτούς. Μόλις η ιδιωτική αλυσίδα είναι μεγαλύτερη από την υπάρχουσα στο δίκτυο, ο επιτιθέμενος μπορεί να δημοσιοποιήσει τη νέα αλυσίδα. Με βάση τον κανόνα της μεγαλύτερης αλυσίδας, η νέα αλυσίδα θα γίνει αποδεκτή από άλλους κόμβους του δικτύου και οι συναλλαγές στο πρόσφατα αποδεκτό blockchain, οι οποίες ενδέχεται να ευνοήσουν τον επιτιθέμενο, θα γίνουν δεκτές.

1.4.3 Denial of Service

Αυτό το είδος επίθεσης συμβαίνει όταν κακόβουλοι κόμβοι καταλαμβάνουν πλήρως τους πόρους για την επαλήθευση ή τη μετάδοση των μπλοκ και των συναλλαγών. Συγκεκριμένα, οι κακόβουλοι κόμβοι μπορούν να ξεκινήσουν πολλές συναλλαγές σε άλλους κόμβους για να απενεργοποιήσουν τη μεταφορά και την επαλήθευση των συναλλαγών από άλλους κόμβους.

1.5 Πλεονεκτήματα του Blockchain

Σύμφωνα με την περιγραφή που προηγήθηκε, τα πλεονεκτήματα της τεχνολογίας του blockchain συνοπτικά περιλαμβάνουν τα αναφερόμενα στις επόμενες παραγράφους.

1.5.1 Ασφάλεια

Δημιουργώντας μια εγγραφή που δεν μπορεί να τροποποιηθεί και είναι κρυπτογραφημένη από άκρο σε άκρο, το blockchain βοηθά στην αποφυγή απάτης και μη εξουσιοδοτημένης δραστηριότητας. Τα ζητήματα απορρήτου μπορούν επίσης να αντιμετωπιστούν στο blockchain ανωνυμοποιώντας τα προσωπικά δεδομένα και

χρησιμοποιώντας δικαιώματα για να αποτραπεί η πρόσβαση. Οι πληροφορίες αποθηκεύονται σε ένα δίκτυο υπολογιστών και όχι σε έναν μόνο διακομιστή, καθιστώντας δύσκολο για τους κακόβουλους χρήστες του διαδικτύου να αποκτήσουν πρόσβαση στα δεδομένα.

1.5.2 Διαφάνεια

Με τον παραδοσιακό τρόπο αποθήκευσης των συναλλαγών, κάθε οργανισμός έπρεπε να διατηρεί ξεχωριστή βάση δεδομένων. Επειδή το blockchain χρησιμοποιεί ένα κατανεμημένο βιβλίο, οι συναλλαγές και τα δεδομένα καταγράφονται πανομοιότυπα σε όλους τους κόμβους του δικτύου. Όλες οι εξουσιοδοτημένες οντότητες, έχουν την δυνατότητα πρόσβασης στις ίδιες πληροφορίες ταυτόχρονα και με πλήρη διαφάνεια. Όλες οι συναλλαγές καταγράφονται αμετάβλητες και φέρουν σφραγίδα ώρας και ημερομηνίας. Αυτό επιτρέπει στις συμμετέχουσες να βλέπουν ολόκληρο το ιστορικό μιας συναλλαγής και ουσιαστικά εξαλείφει κάθε πιθανότητα για επιτυχημένη απάτη.

1.5.3 Άμεση ιχνηλασιμότητα

Το Blockchain δημιουργεί ένα μονοπάτι ελέγχου που τεκμηριώνει την προέλευση ενός περιουσιακού στοιχείου σε κάθε βήμα του κύκλου ζωής του. Το στοιχείο αυτό είναι κρίσιμο για περιπτώσεις όπου είναι σημαντική η εξασφάλιση των δεδομένων (οικονομικές συναλλαγές, προσωπικά δεδομένα κλπ).Καθώς το blockchain διατηρεί πλήρες ιστορικό των συναλλαγών, είναι εφικτό να ανακτάται, όποτε είναι απαιτητό, κάθε πληροφορία για την κάθε μία από αυτές. Η δυνατότητα αυτή διευκολύνει την διαχείριση των δεδομένων.

1.5.4 Απόδοση και ταχύτητα

Οι παραδοσιακές διαδικασίες που καλούνται να διαχειριστούν μεγάλο όγκο δεδομένων, είναι χρονοβόρες και πολλές φορές ευάλωτες στα σφάλματα του ανθρώπινου παράγοντα. Με τον εξορθολογισμό αυτών των διαδικασιών με blockchain, οι συναλλαγές μπορούν να ολοκληρωθούν γρηγορότερα και πιο αποτελεσματικά. Η τεκμηρίωση μπορεί να αποθηκευτεί στο blockchain μαζί με τα στοιχεία της συναλλαγής, εξαλείφοντας την ανάγκη ανταλλαγής δεδομένων. Δεν χρειάζεται να συμβιβαστούν πολλαπλά καθολικά, οπότε η εκκαθάριση και ο διακανονισμός μπορεί να είναι πολύ πιο γρήγορες.

1.5.6 Αυτοματοποίηση

Οι συναλλαγές μπορούν ακόμη και να αυτοματοποιηθούν με «έξυπνα συμβόλαια», τα οποία αυξάνουν την αποδοτικότητά των διεργασιών που βασίζονται σε αυτές και τις

επιταχύνουν ακόμη περισσότερο. Όταν πληρούνται οι προκαθορισμένες προϋποθέσεις, ενεργοποιείται αυτόματα το επόμενο βήμα στη συναλλαγή ή τη διαδικασία. Τα έξυπνα συμβόλαια μειώνουν την ανθρώπινη παρέμβαση καθώς και την εξάρτηση από τρίτα μέρη για να επαληθεύσουν ότι πληρούνται οι όροι μιας σύμβασης.

1.6 Εφαρμογές

1.6.1 Bitcoin

Η πιο γνωστή στο ευρύ κοινό εφαρμογή της τεχνολογίας blockchain είναι το κρυπτονόμισμα bitcoin. Η προσέγγιση του bitcoin είναι μία πρόταση για μία αγορά της οποίας οι συναλλαγές βασίζονται στην τεχνολογία των ηλεκτρονικών υπολογιστών και το διαδίκτυο. Φιλοδοξία των δημιουργών του είναι η μετάπτωση των συναλλαγών από την παραδοσιακή τους μορφή σε ένα αποκεντρωμένο μοντέλο διαχείρισης η οποία θα υλοποιείται απ΄ ευθείας από τους συμμετέχοντες στο δίκτυο τους. Το χρήμα σε αυτό το σύστημα δεν κυκλοφορεί σαν τραπεζογραμμάτιο ή νόμισμα αλλά ως σύνολο ψηφιακών δεδομένων μέσω του διαδικτύου. Επιπλέον ο έλεγχος δεν υφίσταται, κάποια κεντρική αρχή η οποία να εποπτεύει τη διαχείριση και τη διακίνηση του χρήματος.

Ένας ορισμός για το bitcoin αναφέρει ότι είναι ένα ολοκληρωμένο σύστημα ηλεκτρονικών συναλλαγών που δεν απαιτεί τη συμμετοχή μίας έμπιστης τρίτης οντότητας για τον έλεγχο και τη διαχείρισή τους. Αντ' αυτής, εφαρμόζονται ισχυροί κρυπτογραφικοί μηχανισμοί για την παραγωγή και διακίνηση των κρυπτονομισμάτων. Η λειτουργία του συστήματος στηρίζεται σε ένα δίκτυο ομότιμων κόμβων – συσκευών (με υπολογιστική ισχύ) συνδεδεμένων στο διαδίκτυο. Σε κάθε μία από τις συσκευές αυτές περιλαμβάνονται αρχεία με δομή που αντιστοιχεί σε πορτοφόλι (ηλεκτρονικό πορτοφόλι). Οι διαδικασίες δημιουργίας λογαριασμών και απόκτησης πορτοφολιού είναι πλέον σχετικά απλή για ανθρώπους με μέση εξοικείωση ως χρήστες διαδικτυακών εφαρμογών. Οι οικονομικές συναλλαγές με την χρήση bitcoins τίθενται υπό κανόνες που υλοποιούνται με ισχυρούς μηχανισμούς ασφαλείας. Οι μηχανισμοί αυτοί ακολουθούν το μοντέλο της υποδομής δημοσίου κλειδιού.

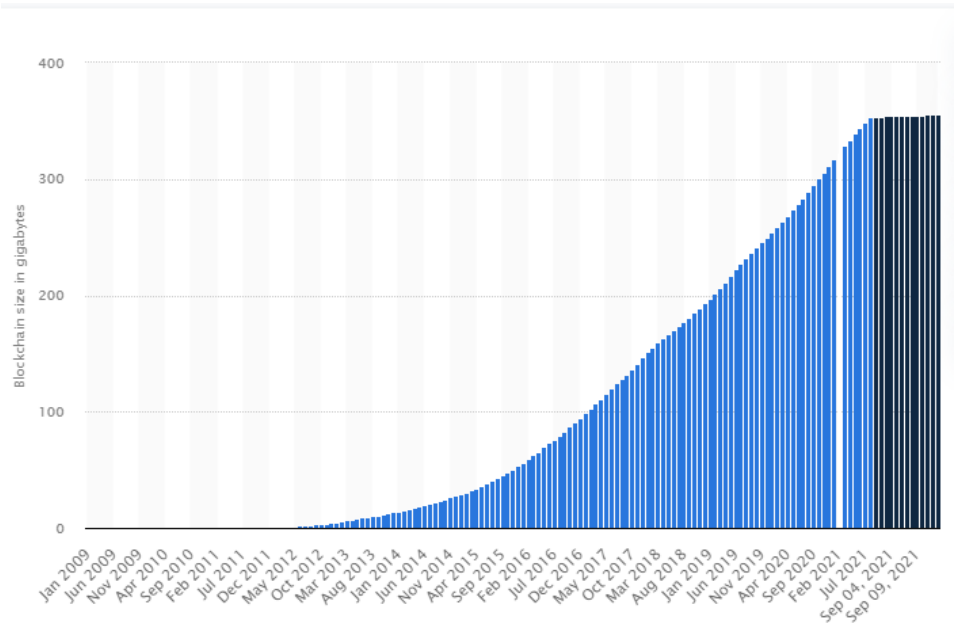
Σύμφωνα με την παραπάνω περιγραφή, το ψηφιακό νόμισμα Bitcoin είναι η βάση για ένα ψηφιακό χρηματικό σύστημα το οποίο δεν παρακολουθείται σε διαχειριστικό επίπεδο από κάποια θεσμική ή μη, αρχή. Η βάση αυτή χρησιμοποιείται για την αποθήκευση και την μετάδοση αξίας μεταξύ των συμμετεχόντων του δικτύου Bitcoin. Η έκδοση νέων Bitcoins πραγματοποιείται κατά την διαδικασία της πιστοποίησης συναλλαγών. Στις

διαδικασίες πιστοποίησης συναλλαγών συμμετέχουν δυνητικά όλα τα μέλη του δικτύου Bitcoin. Για την επιτυχή ολοκλήρωση των διαδικασιών αυτών ανταμείβονται με ένα ποσό νέων Bitcoins τα οποία πλέον του διατίθενται και είναι διαθέσιμα στην αγορά. Τα ποσά ανταμοιβής είναι προκαθορισμένα για συγκεκριμένες χρονικές περιόδους και υφίστανται μείωση με το πέρασμα του χρόνου. Αποτέλεσμα αυτού είναι να προβλέπεται ένα χρονικό πλαίσιο κορεσμού για την παραγωγή τους.

Ιστορική Αναδρομή

Η πρώτη αναφορά για το bitcoin καταγράφηκε το 2008 από Σατόσι Νακαμότο που πιστεύεται ότι είναι ένα ψευδώνυμο που χρησιμοποιήθηκε, του εμπνευστή του. Στην αναφορά αυτή χαρακτηρίστηκε ως μία αλληλουχία από ψηφιακές υπογραφές μέσω των οποίων η κάθε οντότητα μεταφέρει αξία στην άλλη. Αυτό γίνεται με την ψηφιακή υπογραφή της προηγούμενης συναλλαγής και το δημόσιο κλειδί του επόμενου ιδιοκτήτη. Τα δεδομένα αυτά προστίθενται στο τέλος του νομίσματος ώστε ο αποδέκτης της δοσοληψίας να έχει την δυνατότητα να επαληθεύσει τις υπογραφές, μέσα από την αλληλουχία της εναλλαγής της ιδιοκτησίας. (Mueller & Bergsträßer, 2018).

Ορόσημο στην ιστορία του bitcoin αποτέλεσε η ανάπτυξη της πρώτης τράπεζας Bitcoin από τη Circle. Η περίοδος από το 2015 μέχρι και τις αρχές του τρέχοντος έτους χαρακτηρίστηκε από συνεχή ανάπτυξη της blockchain του bitcoin. Το 2021 το μέγεθος της παρουσίασε μία σταθεροποίηση, όπως φαίνεται και στο παρακάτω σχήμα (Statista, 2021).



Εικόνα 2: Η εξέλιξη του μεγέθους του blockchain του bitcoin σε GB

1.6.2 Ακεραιότητα Δεδομένων στο Internet Of Things

Ο όρος Διαδίκτυο των πραγμάτων (InternetofThings) χρησιμοποιήθηκε για πρώτη φορά το 1999 για να περιγράψει τη διασύνδεση του δικτύου που υποστήριζε αυθεντικοποίηση μέσω RFID[1] με το Διαδίκτυο. Με την ανάπτυξη του διαδικτύου σε επίπεδο αριθμού διασυνδεδεμένων χρηστών και ποικιλίας εφαρμογών που υποστηρίζουν, σήμερα πλέον, ο όρος χρησιμοποιείται για να περιγράψει ένα δίκτυο συσκευών διαφορετικών σκοπιμοτήτων που συνδέονται στο διαδίκτυο. Οι συσκευές αυτές περιλαμβάνουν ενσωματωμένες δυνατότητες αναγνώρισης, ανίχνευσης και/ή ενεργοποίησης που τις καθιστά ικανές να χρησιμοποιούν και να εκμεταλλεύονται τις δυνατότητες του διαδικτύου παρέχοντας στους χρήστες τους υπηρεσίες προστιθεμένης αξίας. Η ανάπτυξη των τεχνολογιών του IoT τις τελευταίες δεκαετίες διεύρυνε τον προσανατολισμό των εφαρμογών του IoT. Οι εφαρμογές αυτές εκτείνονται σε ευρεία κλίμακα πολυπλοκότητας και σημαντικότητας για τις κάθε είδους δραστηριότητες και οι λειτουργίες τους περιλαμβάνουν διαχείριση συσκευών, ενεργοποίηση εφαρμογών, ανάλυση δεδομένων, αποθήκευση cloud, συνδεσιμότητα, κα. Μια από τις λειτουργίες που καλείται να φέρουν εις πέρας με επιτυχία οι συσκευές που συνδέονται στο IoT είναι η υποστήριξη σε μοντέλα

[1]Η συντομογραφία RFID προέρχεται από την αγγλική φράση Radio Frequency Identification. Πρόκειται για ηλεκτρονικά κυκλώματα τα οποία φέρουν ψηφιακή πληροφορία και χρησιμοποιούνται για την αναγνώριση των οντοτήτων με τις οποίες συσχετίζονται.

αδειοδότησης είτε αυτά έχουν ιδιοκτήτη είτε είναι ανοικτού κώδικα. Αυτή η κατάσταση δημιουργεί ένα κατακερματισμένο σύνολο από πλατφόρμες IoT οι οποίες δημιουργούν ένα σύνολο προκλήσεων που πρέπει να αντιμετωπιστούν για την αποδοτική λειτουργία των δικτύων. (Reyna, Martin, Chen, et al.) Οι κυριότερες εξ αυτών είναι:

- Κυβερνοασφάλεια
- Απόρρητο
- Μαζική διαχείριση δεδομένων
- Έλλειψη τυποποίησης και διαλειτουργικότητας

1.6.3 Mobile Edge Computing (MEC)

Το mobile edge computing (MEC) εκμεταλλεύεται τι σχετικά μεγάλες δυνατότητες που αποκτούν οι έξυπνες κινητές συσκευές, ειδικότερα όταν συνεργάζονται με διαδικτυακές εφαρμογές. Αν και στις μέρες μας η προσέγγιση αυτή έχει υιοθετηθεί σε πολλούς τομείς της ανθρώπινης δραστηριότητας, έχει εφαρμοστεί σχετικά σε μικρό βαθμό στο χώρο της υγείας. Οι πρόσφατες εξελίξεις στις συσκευές IoT έδωσαν τη δυνατότητα της μετάδοσης δεδομένων που σχετίζονται με την κατάσταση ασθενών μέσω του διαδικτύου. Έτσι η ιατρική απέκτησε ένα σημαντικό εργαλείο για την παρακολούθηση ασθενών και τη διάγνωση ασθενειών, χωρίς την ταυτόχρονη φυσική παρουσία ασθενούς και ιατρού στον ίδιο χώρο. Οι υπάρχουσες θεραπευτικές συσκευές χρησιμοποιούν το MEC ως ενδιάμεσο μεταξύ οντοτήτων που σχετίζονται με το φυσικό κόσμο, όπως τα θεραπευτικά αισθητήρια μέσα και οι κόμβοι IoT, και το υπολογιστικό νέφος. Με τη βοήθεια της αποκεντρωμένης αρχιτεκτονικής του Blockchain, το MEC μπορεί να παρέχει ανωνυμία, ιδιωτικότητα και μυστικότητα των θεραπευτικών δεδομένων, κάτι που είναι πολύ κρίσιμο για την λειτουργία των ιατρικού προσανατολισμού πληροφοριακών συστημάτων. Τα θεραπευτικά δεδομένα που παράγονται από τις συσκευές του IoT θα είναι ασφαλή και ανώνυμα, αν και το API υλικού IoT σχεδιάζεται και συντηρείται από οποιοδήποτε τρίτο μέρος μπορεί να υποστηρίξει τις ίδιες απαιτήσεις. Η ενσωμάτωση του blockchain εξασφαλίζει ακριβώς αυτά τα χαρακτηριστικά. Ένας ασθενής μπορεί να εκτελέσει οποιαδήποτε θεραπευτική δραστηριότητα ή μια συναλλαγή χωρίς την ανάγκη κεντρικού ή μεσάζοντα. Η αλυσίδα των μπλοκ θα περιέχει τα δεδομένα της ιατρικής δραστηριότητας και μία χρονοσφραγίδα.Τα δεδομένα υγείας μπορούν στη συνέχεια να διασφαλιστούν από κυβερνοεπιθέσεις ή μη εξουσιοδοτημένη πρόσβαση. Με τον τρόπο αυτό προστατεύονται οι ίδιοι οι ασθενείς από

την διαρροή των ιατρικών δεδομένων αλλά και τα ιδρύματα υγείας από νομικές κυρώσεις που επισύρουν οι προσβολές των διατάξεων ασφαλείας των βάσεων δεδομένων των πληροφοριακών τους συστημάτων. (Rahman, Hossaim, Hassanain & Alhamin, 2018)

Τα χαρακτηριστικά του blockchain που είναι χρήσιμα για τα συστήματα παρακολούθησης δεδομένων υγείας από συσκευές IoT είναι:

- Η διατήρηση πολλαπλών αντιγράφων των δεδομένων σε πολλούς κόμβους ώστε να μην υπάρχει ένα σημείο αστοχίας
- Η ισχυρή κρυπτογράφηση τους
- Η αδυναμία αλλοίωσης τους χωρίς αυτό να γίνει αντιληπτό
- Η δυνατότητα ασφαλούς αποθήκευσης των δεδομένων σε μία δομή που είναι δημόσια χωρίς να είναι απαραίτητο να εμπιστευθούν οι εμπλεκόμενοι κάποια τρίτη οντότητα.

1.6.4 Ηλεκτρονικές Ψηφοφορίες

Δεδομένου ότι σήμερα στα περισσότερα κράτη του πλανήτη, οι κυβερνήσεις προκύπτουν μέσα από εκλογικές διαδικασίες, η εκλογική ακεραιότητα αποκτά επιπρόσθετη σημασία για τη παγκόσμια ισορροπία. Υπό την έννοια αυτή, οι πολιτικές διαδικασίες ψηφοφορίας είναι καθοριστικές. Η βελτίωση και ο εκσυγχρονισμός των ηλεκτρονικών τεχνολογιών ψηφοφορίας έχουν την δυνατότητα να ενισχύσουν τη συμμετοχή και την εμπιστοσύνη των πολιτών στις διαδικασίες – που τα τελευταία χρόνια φθίνει. Ως αποτελεσματικό μέσο λήψης δημοκρατικών αποφάσεων, οι εκλογές αποτελούν από καιρό κοινωνικό μέλημα. Το σύστημα ψηφοφορίας είναι η μέθοδος μέσω της οποίας θα αποδωθεί η διακυβέρνηση ενός κράτους σε ανθρώπους που θα επιλέξουν οι εκλέκτορες. Η αποτελεσματικότητα μιας τέτοιας διαδικασίας καθορίζεται κυρίως από το επίπεδο πίστης που έχουν οι άνθρωποι στην εκλογική διαδικασία. Με την πάροδο των ετών, η ψηφοφορία έγινε ο πρωταρχικός πόρος για την έκφραση της βούλησης των πολιτών μέσα από τις επιλογές τους. Εκτός από το ανώτατο επίπεδο εφαρμογής των εκλογικών διαδικασιών που αφορά την κρατική διακυβέρνηση, οι εκλογές είναι το μέσο για την επιλογή επικεφαλής σε οργανισμούς διαφορετικών κλιμάκων και προσανατολισμών. Είναι επιπλέον το εργαλείο για την συλλογική αξιολόγηση εργασιών και επιδόσεων. (Shahzad, B., Crowcroft., J., 2020.)

Η διαδικτυακή ψηφοφορία είναι μια τάση που αποκτά δυναμική στην σύγχρονη εποχή που οι διαδικτυακές τεχνολογίες έχουν διεισδύσει σε πολλούς τομείς της δημόσιας διοίκησης. Η ενσωμάτωση των ψηφιακών τεχνολογίων στις εκλογικές διαδικασίες οδηγεί

στην μείωση του οργανωτικού κόστους και στην αύξηση της συμμετοχής των ψηφοφόρων. Το οφέλη αυτά προκύπτουν από μία σειρά αιτίες όπως η εξάλειψη της ανάγκης εκτύπωσης ψηφοδελτίων, την οργάνωση και λειτουργία εκλογικών κέντρων και την απασχόληση υποστηρικτικού προσωπικού. Ωστόσο οι υλοποιήσεις συστημάτων ηλεκτρονικών ψηφοφοριών δημιουργούν μία σειρά από προκλήσεις – οι περισσότερες εκ των οποίων αφορούν το αδιάβλητο τους – οι οποίες είναι απαραίτητο να αντιμετωπίζονται αποτελεσματικά. Οι προκλήσεις αυτές πηγάζουν από την φύση των ηλεκτρονικών εφαρμογών και πολύ περισσότερο από το ανασφαλές περιβάλλον του διαδικτύου.

Τα ηλεκτρονικά συστήματα ψηφοφορίας πρέπει να είναι νόμιμα, ακριβή, ασφαλή και αποδοτικά. Η ανάγκη αυτή γίνεται εντονότερη όσο αυξάνεται το διακύβευμα των εκλογών που υποστηρίζουν. Η τεχνολογία Blockchain είναι ικανή να αντιμετωπίσει με επιτυχία μεγάλο μέρος των προκλήσεων αυτών. Με την αποκεντρωμένη της δομή μπορεί να υποστηρίξει την κατανεμημένη πρόσβαση σε ένα πληροφοριακό σύστημα που υποστηρίζει εκλογικές διαδικασίες και να διαμορφώσει με ασφάλεια το περιεχόμενο μίας διαδικτυακής κάλπης. Οι μεθοδολογίες αυθεντικοποίησης και κρυπτογράφησης εξασφαλίζουν ισχυρή προστασία για το αποτέλεσμα των εκλογών. Τα συστήματα blockchain μπορούν να δώσουν πειστικές λύσεις σε προβλήματα που παρουσιάζουν τα τρέχοντα εκλογικά συστήματα – παραδοσιακά και ηλεκτρονικά.

Οι παραδοσιακές μορφές ψηφοφορίας παρέχουν ένα σχετικά υψηλό επίπεδο εξασφάλισης της ισότητας της συμμετοχής, του σεβασμού της ψήφου, της δικαιοσύνης του αποτελέσματος. Ωστόσο παρουσιάζουν σημαντικές αδυναμίες στο να τα εξασφαλίσουν όλα αυτά στο απόλυτο βαθμό. Οι δυνατότητες της τεχνολογίας, τις τελευταίες δύο δεκαετίες κυρίως, δημιούργησαν ευνοϊκές συνθήκες για την ενσωμάτωση ψηφιακών μεθοδολογιών που προσφέρουν αναβαθμισμένα επίπεδα προστασίας κατά της διαφθοράς, ενώ ταυτόχρονα διασφαλίζουν ότι η διαδικασία της ψηφοφορίας ακολουθεί τους νομικούς κανόνες που την διέπουν. Οι νέες τεχνικές και μέθοδοι ηλεκτρονικής ψηφοφορίας που εισήχθησαν αύξησαν την αξιοπιστία των εκλογών σε σύγκριση με τη μη αυτόματη ψηφοφορία, ενισχύσαν την αποτελεσματικότητα και την ακεραιότητα της διαδικασίας. Λόγω της ευελιξίας, της απλότητας χρήσης και του φθηνού κόστους σε σύγκριση με τις παραδοσιακές μορφές εκλογικών διαδικασιών, η ηλεκτρονική ψηφοφορία πλέον χρησιμοποιείται ευρέως σε διάφορες εφαρμογές, μεγάλης ή ήσσονος αξίας. Παρ 'όλα αυτά, οι υπάρχουσες ηλεκτρονικές μέθοδοι ψηφοφορίας διατρέχουν τον κίνδυνο υπερβολικής εξουσίας των διαχειριστών τους καθώς στην εξέλιξη τους υπεισέρχονται λεπτομέρειες εύκολα χειραγωγούμενες που επηρεάζουν τη θεμελιώδη δικαιοσύνη, την ιδιωτικότητα, το απόρρητο, την ανωνυμία και τη

διαφάνεια στη διαδικασία της ψηφοφορίας. Οι περισσότερες διαδικασίες είναι πλέον συγκεντρωτικές, αδειοδοτημένες από μία εξουσιοδότημένη ανώτερη αρχή, ελέγχονται, μετρούνται και παρακολουθούνται σε ένα σύστημα ηλεκτρονικής ψηφοφορίας, κάτι που μπορεί να αποτελεί πρόβλημα για την διαφάνεια της διαδικασίας. Τα ηλεκτρονικά πρωτόκολλα ψηφοφορίας διαθέτουν έναν μόνο ελεγκτή που επιβλέπει την διαδικασία ψηφοφορίας. Αυτή η τεχνική οδηγεί σε λανθασμένες επιλογές αν οι λειτουργοί της αρχής αυτής αποδειχθούν ανέντιμοι. Επιπλέον ένα τέτοιο σχήμα συστήματος ψηφοφορίας δεν περιλαμβάνει ικανοποιητικούς μηχανισμούς αποκάλυψης της διεφθαρμένης συμπεριφοράς των συμμετεχόντων στο υψηλό επίπεδο διαχείρισης.

Η λύση σε τέτοιες καταστάσεις θα ήταν η χρήση αποκεντρωμένων συστημάτων ηλεκτρονικών ψηφοφοριών. Ένα τέτοιο σχήμα διαμοιράζει την διαχείριση και τον έλεγχο της ορθής εξέλιξης των διαδικασιών σε πολλούς δρώντες, μειώνοντας τις πιθανότητες επιτυχούς εφαρμογής συμπεριφορών με χαρακτηριστικά διαφθοράς. Η τεχνολογία Blockchain είναι μία αποκεντρωμένη προσέγγιση για τις ηλεκτρονικές διαδικτυακές ψηφοφορίες που χρησιμοποιήθηκαν τα τελευταία χρόνια με επιτυχία, κυρίως λόγω των πλεονεκτημάτων επαλήθευσης από άκρο σε άκρο, που προσφέρουν. Το Blockchain είναι μια ελκυστική εναλλακτική λύση στα συμβατικά συστήματα ηλεκτρονικής ψηφοφορίας, καθώς στα χαρακτηριστικά της συγκαταλέγονται οι μη αποποίηση και προστασία ασφάλειας. Κάθε μπλοκ στην αλυσίδα περιέχει έναν κατακερματισμό, χρονική σήμανση και δεδομένα συναλλαγών από το προηγούμενο μπλοκ. Το blockchain δημιουργήθηκε για να είναι ανθεκτικό στις προσπάθειες αλλοίωσης των δεδομένων. Η κατάλληλη χρήση των χαρακτηριστικών του blockchain είναι ικανή να προσφέρει στις εκλογές διαφάνεια, απόρρητο και μη αποποίηση ενεργειών (Jafar, Juzaiddin, Aziz, &Shukur, 2021).

2. Μεθοδολογία

Στο κεφάλαιο αυτό, περιγράφεται η μεθοδολογία της βιβλιογραφικής ανασκόπησης η οποία πραγματοποιήθηκε για την παρούσα μεταπτυχιακή διατριβή. Όπως έχει προαναφερθεί στην εισαγωγή της διατριβής, στόχο αποτελεί ο εντοπισμός και η ανάλυση ηλεκτρονικών συστημάτων ψηφοφορίας που βασίζονται στην τεχνολογία του Blockchain. Προς τούτο, έλαβε χώρα συστηματική ανασκόπηση βιβλιογραφίας (systematic literature review) με τη χρήση της μεθοδολογίας PRISMA – ScR (Preferred Reporting Items of Systematic Reviews and Meta – Analysis). Με τη συγκεκριμένη μεθοδολογία:

1. Προσδιορίστηκαν τα ερευνητικά κριτήρια και οι στόχοι της βιβλιογραφικής ανασκόπησης
2. Αναζητήθηκε επιστημονική βιβλιογραφία στο Scopus (https://www.scopus.com).
3. Διαλέγησαν επιστημονικά άρθρα (η διαλογή πραγματοποιήθηκε εντός δύο φάσεων) έχοντας ορίσει διακριτά κριτήρια συμπερίληψης και αποκλεισμού.
4. Επιλέχθηκαν τα τελικά άρθρα με κριτήριο το πλήρες κείμενο.

2.1 Προσδιορισμός των ερευνητικών κριτηρίων

Τα κριτήρια που η βιβλιογραφική ανασκόπηση πληροί, συνίστανται στα εξής:

1. Έτος δημοσίευσης του άρθρου
2. Πρωτεύουσα συγγραφική υπευθυνότητα του άρθρου
3. Αριθμός αναφορών του άρθρου

2.2 Αναζήτηση επιστημονικής βιβλιογραφίας

Στο στάδιο αυτό, αναζητήθηκαν τα άρθρα τα οποία συμπεριλήφθηκαν στη βιβλιογραφική ανασκόπηση και τα οποία απαντούσαν στα ερευνητικά κριτήρια. Η αναζήτηση των άρθρων αυτών, πραγματοποιήθηκε στην αγγλική γλώσσα στη βιβλιογραφική βάση Scopus (https://www.scopus.com). Συγκεκριμένα, το ερώτημα αναζήτησης (search query) που πληρούσε τους προαναφερόμενους όρους, διαμορφώθηκε ως εξής: TITLE – ABS – KEY ((Όρος Α) AND (Όρος Β)). Πραγματοποιήθηκε σύνθετη αναζήτηση υπό τους όρους 1) “Blockchain” AND “e – voting”, 2) ”Blockchain” AND “electronic voting”, 3) “Blockchain” AND “voting systems”. Αναφέρεται ότι κριτήρια στα οποία επικεντρώνεται η αναζήτηση αποτελούν ο τίτλος, η περίληψη και οι λέξεις – κλειδιά στα οποία εστιάζει το επιστημονικό άρθρο.

2.3 Μέθοδος και κριτήρια διαλογής

Τα άρθρα ανακτήθηκαν από τη βιβλιογραφική βάση σε format CVS, και επεξεργάστηκαν σε ένα φύλλο εργασίας Excel, προκειμένου να αξιολογηθούν και να επιλεγούν εκείνα, τα οποία πληρούσαν τα ερευνητικά ερωτήματα.

Πριν τη μελέτη του πλήρους κειμένου του άρθρου, προηγήθηκε η εξέταση του τίτλου, της περίληψης καθώς και των λέξεων κλειδιών με τη χρήση κανόνων συμπερίληψης και αποκλεισμού. Η διαδικασία αυτή έλαβε χώρα εντός δύο φάσεων.

Κατά την πρώτη φάση, πραγματοποιήθηκε αποκλεισμός των άρθρων τα οποία δεν ενέπιπταν του θέματος της ανασκόπησης, με συγκεκριμένα κριτήρια συμπερίληψης και αποκλεισμού.

Κατά τη δεύτερη φάση, πραγματοποιήθηκε έλεγχος για το ποια από τα άρθρα συνιστούν surveys review papers και πραγματοποιήθηκε ο αποκλεισμός τους από την ανασκόπηση.

2.4 Επιλογή των άρθρων

Μετά το πέρας της δεύτερης φάσης, ελέγχθηκε το πλήθος των επιστημονικών άρθρων και εκτός της περίληψης, έγινε αξιοποίηση και του πλήρους κειμένου.

2.5 Προσδιορισμός των ερευνητικών ερωτημάτων

Η παρούσα μεταπτυχιακή διατριβή στοχεύει να απαντήσει στα εξής ερωτήματα: 1) Τα Blockchain based e – voting systems διασφαλίζουν την ασφάλεια της εκλογικής διαδικασίας; 2) εξασφαλίζουν την ιδιωτικότητα των εκλογέων; 3) εγγυώνται την ακεραιότητα των δεδομένων τους; 4) πληρούν τις παραμέτρους για την εγκυρότητα του εκλογικού αποτελέσματος; 5) αποτρέπουν τον ετεροκαθορισμό της πολιτικής βούλησης των εκλογέων; 6) μειώνουν το χρόνο της εκλογικής διαδικασίας; 7) μειώνουν τα λειτουργικά κόστη (χαρτί, μισθοδοσία); 8) αυξάνουν την εμπιστοσύνη των εκλογέων; 9) αυξάνουν τη συμμετοχή των εκλογέων στην εκλογική διαδικασία;

Κεφάλαιο 3: Ανάλυση αποτελεσμάτων

3.1 Αποτελέσματα αναζήτησης

Η βιβλιογραφική ανασκόπηση έλαβε χώρα στο Scopus (https://www.scopus.com) στις 23 Σεπτεμβρίου 2021. Ο συνολικός αριθμός των άρθρων ανήλθε στα 120. Από τα άρθρα αυτά αφαιρέθηκαν εκείνα τα οποία 1) δεν ήταν ακαδημαικά άρθρα, 2) η περίληψη τους δεν αφορούσε στο συγκεκριμένο θεματικό πεδίο, 3) η γλώσσα γραφής δεν ήταν η αγγλική, 4) ο αριθμός των αναφορών ήταν μικρός, 5) το έτος δημοσιεύσης ήταν μικρότερο του 2017.

3.2 Μελέτη και ανάλυση της βιβλιογραφίας

Τα είκοσι (20) άρθρα τα οποία επιλέγησαν, μελετήθηκαν αναλυτικά. Κατά τη μελέτη των επιστημονικών άρθρων κατεβλήθη η προσπάθεια να εντοπισθούν τα σημεία εκείνα τα οποία απαντούσαν στα ερωτήματα της έρευνας.

Κεφάλαιο 4: Αναλυτική παρουσίαση άρθρων

Στο κύριο μέρος, παρατίθενται συστήματα ηλεκτρονικής ψηφοφορίας τα οποία συνδυάζουν διάφορες τεχνολογίες, με κυριότερη την τεχνολογία του Blockchain, για τη δημιουργία πρωτοκόλλων που εγγυώνται βασικές παραμέτρους, όπως η ασφάλεια, η ιδιωτικότητα, η διαφάνεια, η εγκυρότητα της εκλογικής διαδικασίας καθώς και η αντιμετώπιση κακόβουλων επιθέσεων που διαβρώνουν την αυθεντικότητα του εκλογικού αποτελέσματος.

Η παρουσίαση των συστημάτων, συνίσταται στην περιγραφή της αρχιτεκτονικής του συστήματος, την καταγραφή των εμπλεκόμενων οντοτήτων, την επεξήγηση της εκλογικής διαδικασίας και την κατάδειξη αποτελεσμάτων της πειραματικής εφαρμογής του εκάστοτε συστήματος.

Στο άρθρο υπό τον τίτλο “E-voting with Blockchain: An E-voting Protocol with Decentralisation and Voter Privacy”, (Hardwick, Gioulis, Akram, Markantonakis, 2018) οι συγγραφείς αναφέρονται στη χρήση ενός συστήματος ηλεκτρονικής ψηφοφορίας, το οποίο βασίζεται στη χρήση της τεχνολογίας του Blockchain.

Σχετικά με τις οντότητες του συστήματος, αυτές αποτελούνται από τον εκλογέα (voter), κεντρική αρχή (central authority), ψήφο (vote), ψηφοφορία (ballot) και το εναλλακτικό ψηφοδέλτιο (alteration ballot).

Αναφορικά στην εκλογική διαδικασία, αυτή διακρίνεται σε τέσσερα στάδια. Το στάδιο εκκίνησης (initialization phase). Κατά το στάδιο εκκίνησης ορίζονται οι όροι της εκλογικής διαδικασίας και εκκινούν το Central Authority, το Blockchain και τα συστήματα του πρωτοκόλλου. Το στάδιο προετοιμασίας (preparation phase). Κατά το στάδιο προετοιμασίας, ο Voter εφαρμόζοντας την εφαρμογή χρήστη της e-voting πλατφόρμας, αυθεντικοποιεί την ταυτότητα του στο Central Authhority. Το στάδιο της ψηφοφορίας (voting phase). Κατά το στάδιο της ψηφοφορίας, ο εκλογέας δημιουργεί την ψήφο του και την αποστέλλει στο δίκτυο και το στάδιο καταμέτρησης (counting phase). Κατά το στάδιο αυτό οι εκλογείς αποκαλύπτουν το περιεχόμενο της ψήφου τους.

Κρίνεται σημαντικό, το σύστημα ηλεκτρονικής ψηφοφοφίας να διασφαλίζει παραμέτρους ασφαλείας. Το συγκεκριμένο υποστηρίζει τις κατωτέρω: αιρετότητα (eligibility), ιδιωτικότητα (privacy), αμεροληψία (fairness), ιδιωτική επαλήθευση/επιβεβαίωση (individual variability) και δημόσια επαλήθευση/επιβεβαίωση (universal verifiability).

Συμπερασματικά, το άρθρο προτείνει ένα σύστημα ηλεκτρονικής ψηφοφορίας, το οποίο βασίζεται στην τεχνολογία του Blockchain και το οποίο πληροί τις θεμελιώδεις εγγυήσεις του E-voting, όπως διαφάνεια , ανωνυμία, ασφάλεια και αξιοπιστία, ιδιαίτερα έναντι των " Denial of Service Attacks" καθώς και αμεταβλητότητα/σταθερότητα (δηλαδή, ακεραιότητα της εκλογικής διαδικασίας και τη ψήφου).

Οι εγγυήσεις αυτές, αποτελούν εναλλακτική λύση έναντι της αυξανόμενης πολιτικής απάθειας, ιδιαίτερα στους τεχνολογικά καταρτιζόμενους νέους.

Στο άρθρο υπό τον τίτλο " Platform-independent Secure Blockchain-Based Voting System", (Yu, B. et alt., 2018) οι συγγραφείς εστιάζουν στη χρήση ενός συστήματος ηλεκτρονικής ψηφοφορίας, το οποίο βασίζεται στις τεχνολογίες του Blockchain, του Linkable Ring Signatures, του συστήματος κρυπτογράφησης Paillier και των Smart Contracts.

Το σύστημα, θεμελιώνεται στις εξής λειτουργίες: Στην κωδικοποίηση και αποκωδικοποίηση του μηνύματος. Επεξηγηματικά, πριν την έναρξη της εκλογικής διαδικασίας, απαιτείται η κωδικοποίηση της ταυτότητας του εκλογέα, ώστε να είναι κατάλληλη για την καταγραφή των ψήφων. Στο σύστημα κρυπτογράφησης Pailler. Το σύστημα κρυπτογράφησης, εφαρμόζεται για την καταγραφή των κρυπτογραφημένων ψήφων. Συνεπικουρεί στις λειτουργίες "Key Generation", "Encryption", " Decryption", "Message Membership Proof of Knowledge" και " Decryption Correctness Proof of Knowledge". Στις Linkable Ring Signatures οι οποίες εφαρμόζονται για την προστασία της ιδιωτικότητας των ψηφοφόρων. Συνεπικουρεί στις λειτουργίες "Set up", "Key generation", "Signature", "Verification" και "Linkability". Στο Blockchain, το οποίο εφαρμόζεται με το πρωτόλλο "Practical BFT". Συγκρινόμενο με άλλα πρωτόκολλα, το PBFT, παρουσιάζει υφηλότερη απόδοση.

Σχετικά με τα smart contracts, ως περιβάλλον λειτουργίας τους, επιλέγεται το " Hyperledger Fabric". Το "Hyperledger Fabric", συνεπικουρεί στις λειτουργίες init(), η οποία εκκινεί τις παραμέτρους του smart contract, πριν ο χρήστης διαδράσει με αυτό, query(), η οποία διαχειρίζεται τα ερωτήματα των χρηστών και invoke(), η οποία καλείται όταν ο χρήστης επιθυμεί να καταχωρίσει τα δεδομένα στο Blockcchain.

Όσον αφορά τις οντότητες του συστήματος, αποτελούνται από τις "Smart Contract Administrator", "Voting Administrator" και " Smart Contract".

Η διαδικασία της ψηφοφορίας διακρίνεται στις λειτουργίες όπως, η αυτόματη εκκίνηση του smart contract, η ενεργοποίηση παραμέτρων, (όπως του δημόσιου κλειδιού, του συστήματος Pailler και του LRS), η εγγραφή των εκλογέων, η έναρξη της ψηφοφορίας, η αποστολή της ψήφου, η καταγραφή των ψήφων, η καταμέτρηση των ψήφων, η επαλήθευση της ψήφου από τον εκλογέα (προαιρετικά), η απόκτηση του εκλογικού αποτελέσματος από τον Administrator, η εμφάνιση του εκλογικού αποτελέσματος και επιβεβαίωση της ορθότητας αυτού και η αποδοχή και δημοσίευση του εκλογικού αποτελέσματος από τους εκλογείς.

Το σύστημα ηλεκτρονικής ψηφοφορίας διασφαλίζει τις παραμέτρους της ιδιωτικότητας, της ανωνυμίας, της αποφυγής διπλής ψήφου, της αδυναμίας πλαστογράφησης της ψήφου από τον αντίπαλο (“slanderability-avoided”), της αδυναμίας αποκάλυψης της ψήφου από τον αντίπαλο (“receipt-freeness”), της δημόσιας επαλήθευσης (“public verifiability”), της ορθότητας (“correctness”) και της καταχώρισης της ψήφου και αποχώρισης (“ vote-and-go”), δηλαδή δεν απαιτείται η αναμονή των εκλογέων έως το πέρας της εκλογικής διαδικασίας.

Σχετικά με την ανθεκτικότητα του συστήματος, αυτό είναι ανθεκτικό έναντι των “Man in the Middle Attacks” και “ Denial of Service (DoS) Attacks.

Σε σχέση με τον πειθαναγκασμό (“Coercion – Resistance Analysis”),το σύστημα δεν υποστηρίζει λειτουργία αποτροπής του ετεροκαθορισμού της βούλησης του εκλογέα.

Η πειραματική διαδικασία, εφαρμόσθηκε στην BFT πλατφόρμα Hyperledger Fabric.

Καταδείχθηκε ότι η αύξηση του χρόνου της διαδικασίας, συναρτάται του μεγέθους του block και του μήκους της αλυσίδας.

Καταληκτικά, το σύστημα ηλεκτρονικής ψηφοφορίας, διασφαλίζει τις παραμέτρους της ιδιωτικότητας του εκλογέα και της ορθότητας της εκλογικής διαδικασίας, μέσω της χρήσης της ομομορφικής κρυπτογράφησης, της linkable ring signature και του Blockchain.

Στο άρθρο υπό τον τίτλο “ Security e-voting based on blockchain in P2P network”, (Yi, H., 2019) ο συγγραφέας πραγματεύεται ένα σύστημα ηλεκτρονικής ψηφοφορίας, το οποίο βασίζεται σε τεχνικές που χρησιμοποιούνται για την επαύξηση της ασφάλειας της ηλεκτρονικής ψηφοφορίας, όπως DLT και ECC.

Αναλυτικότερα στην DLT, χρησιμοποιείται ένα συγχρονισμένο μοντέλο καταγραφής των ψήφων, το οποίο βασίζεται στην distributed ledger techonology,

προκειμένου να αποφευχθεί η πλαστογράφηση. Στην ECC, χρησιμοποιείται ένα μοντέλο καταγραφής των διαπιστευτηρίων του χρήστη, το οποίο βασίζεται στην elliptic curve cryptography (ECC), προκειμενου να εξασφαλισθεί η αυθεντικοποίηση (authentification) και η μη – αποκήρυξη της ψήφου (non repudiation).

Αναφορικά στον ορισμό του Block, αυτό αποτελείται από την ταυτότητα του εκλογέα ("voter's ID"), την ψήφο ("vote"), την υπογραφή του εκλογέα ("voter's signature"), τη σφραφίδα χρόνου ("timestamp"), προκειμένου να καταγράφεται ο χρόνος υποβολής της ψήφου και το hash του προηγούμενου block. Για τον υπολογισμό της αξίας του hash, χρησιμοποιείται ο αλγόριθμος SHA – 256.

Επίσης, χρησιμοποιείται ένα withdrawal model, ώστε ο εκλογέας να μπορεί να μεταβάλλει το περιεχόμενο της ψήφου του, πριν το πέρας της εκλογικής διαδικασίας.

Η εκλογική διαδικασία αποτελείται από το στάδιο εκκίνησης και το στάδιο ψηφοφορίας.

Τα διαπιστευτήρια των εκλογέων, βασίζονται στην EEC. Οι ψήφοι υπογράφονται από τους εκλογείς, ώστε ουδείς άλλος να γνωρίζει το περιεχομένο της ψήφου. Επίσης, οι εκλογείς χρησιμοποιούν το ιδιωτικό κλειδί τους, για να υπογράψουν το hash της ψήφου, με τη χρήση της ECDSA signature, ώστε να διαπιστώνεται η αυθεντικότητα της ψήφου.

Σχετικά με την εξόρυξη και δημιουργία blocks των ψήφων, όλες οι ψήφοι στο blockchain, συνδέονται μεταξύ τους κρυπτογραφημένες, από block σε block.

Η πειραματική διαδικασία του συστήματος, πραγματοποιήθηκε στην πλατφόρμα Linux, Vbuntu, με τη γλώσσα προγραμματισμού Python.

Συμπερασματικά, με τη χρήση των ανωτέρων τεχνικών, το σύστημα ηλεκτρονικής ψηφοφορίας διασφαλίζει την ανωνυμία του εκλογέα, την ασφάλεια της εκλογικής διαδικασίας, τη μη – αποκήρυξη ψήφου και τη δυνατότητα ανάκλησης της ψήφου.

Στο άρθρο υπό τον τίτλο " Verify - your - vote: A verifiable Blockchain – Based Online Voting Protocol", (Chaieb, Yousfi, Lafourcade, Robbana, 2018) οι συγγραφείς αναφέρονται σε ένα σύστημα ηλεκτρονικής ψηφοφορίας το οποίο θεμελιώνεται στις τεχνολογίες των Ethereum, Elliptic Curve Cryptography, Pairings και Identity – Based Encryption.

Οι οντότητες του συστήματος αποτελούνται από το Registration Server, ο οποίος εγγράφει τους δικαιούμενους εκλογείς και τους προμηθεύει με τις παραμέτρους

αυθεντικοποίησης. Τον Election Administrator, ο οποίος διαχειρίζεται την εκλογική διαδικασία, τους Eligible Voters, οι οποίοι έχουν τη δυνατότητα να ψηφίσουν κατ' επανάληψη και να διαφοροποιήσουν το περιεχόμενο της ψήφου τους. Μόνον η τελική τους ψήφος καταμετράται καθώς και τους Tallying Authorities οι οποίοι συμμετέχουν στην κατασκευή της κάλπης, την αποκρυπτογράφηση των ψήφων, τον υπολογισμό του τελικού αποτελέσματος και τη δημοσίευση τιμών που επιτρέπουν στους εκλογείς να ελέγξουν την ακρίβεια της καταμέτρησης.

Η διαδικασία ψηφοφορίας αποτελείται από τα στάδια του Setup, όπου ο election administrator δημιουργεί τις παραμέτρους και υπολογίζει τον αριθμό των δελτίων και το offset value και τα αποστέλλει στα Tallying Authorities, ώστε να ολοκληρωθεί η κατασκευή των δελτίων, του Registration phase, όπου ο δικαιούμενος εκλογέας εισάγει έναν κωδικό και ο registration server επιστρέφει στο δικαιούμενο εκλογέα τις παραμέτρους αυθεντικοποίησης, του Authentification phase, όπου ο εκλογέας κρυπτογραφεί τις παραμέτρους αυθεντικοποίησης με το δημόσιο κλειδί του administrator, τις υπογράφει με το μυστικό κλειδί υπογραφής και τις αποστέλλει στον Administrator. Ακολούθως, ο Administrator επαληθεύει την υπογραφή του εκλογέα και τις παραμέτρους αυθεντικοποίησης. Το στάδιο Voting, όπου τα tallying authorities, επιλέγουν ένα δελτίο για κάθε εκλογέα, το κρυπτογραφούν με το δημόσιο κλειδί του ψηφοφόρου και το αποστέλλουν στον ψηφοφόρο. Ο εκλογέας, επιλέγει τον υποψήφιο και κρυπτογραφεί την επιλογή του. Το στάδιο Tallying, όπου οι Tallying Authorities υπολογίζουν τον αριθμό των ψήφων μίας συγκεκριμένης pseudo ID και το στάδιο του Verification, το οποίο διακρίνεται σε δύο στάδια. Το πρώτο συνίσταται στην επανακατασκευή των counter values, που σχετίζονται με το δελτίο και το όνομα του υποψηφίου. Το δεύτερο συνίσταται στη χρήση του ομομορφισμού των pairings, για τον έλεγχο της ακρίβειας της καταμέτρησης.

Το δελτίο αποτελείται από τα μέρη του Ballot number, το οποίο είναι μοναδικό, από το όνομα υποψηφίου, το Pseudo ID υποψηφίου και το Counter value, το οποίο χρησιμοποιείται για την επαλήθευση/επιβεβαίωση.

Οι παράμετροι που διασφαλίζονται συνίστανται στις Eligibility, όπου κατά τη διαδικασία της εγγραφής, μόνο οι δικαιούμενοι εκλογείς προμηθεύονται τις παραμέτρους αυθεντικοποίησης. Fairness, όπου οι ψήφοι κρυπτογραφούνται πριν καταχωρισθούν. Integrity, κατά την οποία η καταχώριση και αποθήκευση των ψήφων προστατεύονται από τις ιδιότητες του Blockchain. Individual verifiability η οποία συνεπικουρείται από τη δομή του δελτίου, στο οποίο εμπεριέχονται counter values. Universal verifiability, στο οποίο οι tallying authorities, δημοσιεύουν τον αριθμό κάθε υποψηφίου και τα counter values. Receipt

– freeness, μέσω της οποίας δεν τεκμαίρεται η καταχώριση ψήφου, υπέρ συγκεκριμένου υποψηφίου. Εξ αντιδιαστολής, το συγκεκριμένο πρωτόκολλο, δε διαθέτει λειτουργίες κατά του πειθαναγκασμού/ετεροπροσδιορισμού της βούλησης του εκλογέα (coercion resistance).

Κατά την πειραματική διαδικασία χρησιμοποιήθηκε το verification tool "ProVerif", το οποίο αναλύει τη μυστικότητα, την ιδιωτικότητα και τις παραμέτρους αυθεντικοποίησης ενός πρωτοκόλλου.

Συμπερασματικά, οι παράμετροι ασφάλειας, διασφαλίζονται με τη χρήση των τεχνικών ECC, IBE και pairings.

Στο άρθρο υπό τον τίτλο " A smart contract for boardroom voting with maximum voter privacy", (McCorry, Shahandashti, Hao, 2017) οι συγγραφείς πραγματεύονται το σχεδιασμό ενός συστήματος ηλεκτρονικής ψηφοφορίας με στόχο την ύψιστη προστασία της ιδιωτικότητας του εκλογέα.

Σχετικά με την αρχιτεκτονική, το σύστημα ηλεκτρονικής ψηφοφορίας αποτελείται απο δύο smart contracts επεξεργασμένα στην Ethereum γλώσσα Solidity. Το πρώτο ονομάζεται "voting contract" και εφαρμόζει το πρωτόκολλο ψηφοφορίας, ελέγχει την εκλογική διαδικασία και επαληθεύει τους δύο τύπους zero knowledge proof. Το δεύτερο ονομάζεται cryptography contract και το οποίο, διανέμει τον κώδικα για τη δημιουργία των δύο τύπων zero knowledge proofs. Επίσης από τρεις HTML/Javascript σελίδες για τους χρήστες. Συγκεκριμένα, την "Election Administrator" (admin.html), η οποία διευθύνει την εκλογική διαδικασία, τη "Voter" (vote.html), στην οποία εγγράφεται ο εκλογέας για την εκλογική διαδικασία και την καταχώριση της ψήφου και την "Observer" (livefeed.html), η οποία παρακολουθεί τις λειτουργίες του Election Administrator και του Voter.

Η διαδικασία ψηφοφορίας αποτελείται από το στάδιο Setup, όπου ο Election Administrator επικαιροποιεί τη λίστα των δικαιούμενων εκλογέων, το Sign up, όπου οι εκλογείς εγγράφονται με τη χρήση του voting key, το commit (προαιρετικό), στο οποίο οι εκλογείς δημοσιεύουν ένα hash της ψήφου τους στο Blockchain του Ethereum, το Vote, κατά το οποίο οι εκλογείς δημοσιεύουν την κρυπτογραφημένη ψήφο και ένα από τα δύο zero knowledge proofs και το Tally, όπου ο Election Administrator ενημερώνει το Ethereum προκειμένου να υπολογιστούν οι εγγραφές.

Η ασφάλεια του συστήματος ηλεκτρονικής ψηφοφορίας, συνίσταται στις παραμέτρους του Individual, public verifiability, όπου ισχύει η υπόθεση ότι ο Η/Υ του εκλογέα είναι ασφαλής. Αυτό επιβεβαιώνεται με τον έλεγχο της εγγραφής της ψήφου στο

Blockchain και την αποκρυπτογράφηση της ψήφου με τη χρήση του κλειδιού x i. Στο Voter authentication, το οποίο επιτυγχάνεται μέσω της χρήσης δύο smart contracts, του tx.origin και του msg.sender. Στο Replay attacks defense, στο οποίο μέσω της χρήσης του smart contract, msg.gender αποφεύγεται η αντιγραφή των voting keys και των zero knowledge proofs, τα οποία έχουν αποσταλεί στο blockchain. Στην παράμετρο Timers όπου ο Election Administrator, καθορίζει μια λίστα χρονομετρητών προκειμένου να επιτραπεί η χρονική ομαλότητα της εκλογικής διαδικασίας. Στους Ethereum miners , οι οποίοι, ελέγχουν τη δομή των συναλλαγών σε ένα block, και την κανονικότητα της εκτέλεσης ενός contract. Στη δράση του Election administrator,: δεδομένου ότι τα contracts, δεν μπορούν να εκκινήσουν τη διαδικασία, ορίζεται εκ των προτέρων ένας administrator. Στην περίπτωση που περισσότεροι από ένας εκλογείς αποπειραθούν να εκκινήσουν τη διαδικασία, επιλέγεται μόνον ένας. Τελευταία παράμετρο αποτελεί το Light Ethereum Subprotocol. Το συγκεκριμένο πρωτόκολλο, είναι παρόμοιο με το απλοποιημένο πρωτόκολλο επιβεβαίωσης πληρωμής του Bitcoin, αντί του πλήρους Ethereum Blockchain. Μέσω της χρήσης του, ο χρήστης επιβεβαιώνει την ορθότητα του εκλογικού πρωτοκόλλου.

Κατόπιν πειραματικής εφαρμογής του Ethereum’s Test Network, καταδείχθηκε ότι το συνολικό κόστος, συμπεριλαμβανομένου του κόστους του administrator και του voter, ανέρχεται στα 0, 73$ και ότι ο χρόνος των επιμέρους διαδικασιών κυμαίνεται από 81 έως 573 milliseconds.

Οι τεχνικές δυσκολίες συνίστανται σε ζητήματα ελλιπούς κρυπτογράφησης, ζητήματα call stacks, στην έλλειψη debugging tools και τον περιορισμένο αριθμό χρηστών.

Εν κατακλείδι,το προτεινόμενο σύστημα ηλεκτρονικής ψηφοφορίας, εγγυάται σε μεγάλο βαθμό τις παραμέτρους ασφαλείας ενώ παρουσιάζει χαμηλό κόστος και υψηλές ταχύτητες κατά την εκλογική διαδικασία.

Στο άρθρο υπό τον τίτλο “ Bronco Vote: secure system using Ethereum’s blockchain”, (Dagher, Marella, Milojkovic, Mohler, 2018) οι συγγραφείς εστιάζουν στη χρήση ενός συστήματος το οποίο διαρθρώνεται ως κάτωθι.

Το σύστημα ηλεκτρονικής ψηφοφορίας χρησιμοποιεί τις τεχνικές Blockchain, Eth.calls, Paillier encryption και MetaMask.

Οι οντότητες του συστήματος συνίστανται στους Administrator, Voter, Creator, VoteUI. Html, Voting App.js και Crypto.js. Τα smarts contracts αποτελούνται από τα μέρη Registrar.sol, Creator.sol και Voting.sol.

Η διαδικασία ψηφοφορίας διακρίνεται στα επιμέρους στάδια. Στο Initial set up ο Administrator ενεργοποιεί τα Registrar και Creator contracts, για την εκκίνηση του συστήματος, την εγγραφή, την ψηφοφορία και τη δημιουργία νέων συμβολαίων. Στο Register voter, απαιτείται αριθμός ταυτότητας. Αφού συμπληρωθεί το πεδίο της ταυτότητας και του mail, στο VoteUI.html, τα δεδομένα αποστέλλονται στο Voting App.js. Κατόπιν, το eth.calls επιβεβαιώνει τα δεδομένα. Όταν ο έλεγχος επιβεβαιωθεί, το Voting App.js, αποστέλλει τη συναλλαγή στο Registrar Contract για την αποθήκευση των δεδομένων του εκλογέα. Ακολούθως, η διεύθυνση Ethereum συνδέεται με τη διεύθυνση mail, ώστε να αποφεύγονται οι διπλοεγγραφές. Στο Create ballot, κατά το οποίο δημιουργείται νέο συμβόλαιο, εισάγοντας την απαιτούμενη πληροφορία στο VoteUI.html. Για τη δημιουργία του ballot, απαιτείται η καταχώριση της διεύθυνσης e – mail του δημιουργού. Ακολούθως, ο creator επιλέγει αν θα δημιουργήσει ένα whitelisted ballot ή όχι. Έπειτα, το VotingApp.js, χρησιμοποιεί τρία eth calls. Τα δύο πρώτα αποστέλλονται στο Registrar Contract, για τον έλεγχο της διεύθυνσης του mail και του Ethereum. Το τρίτο αποστέλλεται για να επιβεβαιωθεί οτι ο creator έχει την απαιτούμενη άδεια. Μετά την επιβεβαίωση, το VotinAp.js, συλλέγει τα εισαχθέντα δεδομένα, δημιουργεί έναν αριθμό ID – ballot, και τα αποστέλλει στο Creator Contract για τη δημιουργία ενός νέου Voting Contract. Ακολούθως το Voting App.js, αποστέλλει ένα επιπλέον eth.call στο Creator Contract, για την ανάκτηση της νέας διεύθυνσης, του νέου Voting Contract. Εν τέλει, αποστέλλεται η ταυτότητα ballot και η διεύθυνση του συμβολαίου στο Registrar Contract, για τη δήλωση νέου ballot. Στο στάδιο, Load ballot, ο εκλογέας εισάγει την ταυτότητα του ballot στο VoteUI.html. Το VotingApp.js, αποστέλλει ένα eth.call, στο Registrar Contract, για την ανάκτηση της διεύθυνσης του Voting Contract η οποία σχετίζεται με την ταυτότητα του ballot. Ακολούθως το VotingApp.js, αποστέλλει ένα eth.call, στο Voting Contract και ανακτά τις κρυπτογραφημένες ψήφους. Στο στάδιο Vote, όπου ο εκλογέας εισάγει την επιλογή του και τη διεύθυνση mail στο VoteUI.html και η πληροφορία αυτή αποστέλλεται στο VotingApp.js. Κατόπιν το VotingApp.js, αποστέλλει eth.calls στο Registrar Contract, για την επαλήθευση του εκλογέα. Αν η επαλήθευση είναι επιτυχής, το VotingApp.js., αποστέλλει eth.calls στο Voting Contract, για τον έλεγχο του status του εκλογέα και το χρονικό περιορισμό της εκλογικής διαδικασίας. Αν ο έλεγχος του status είναι ορθός, η ψήφος του εκλογέα αποστέλλεται στο server για να κρυπτογραφηθεί. Έπειτα το VotingApp.js, αποστέλλει ένα eth.call στο Voting Contract για να ανακτηθεί ο αριθμός της κρυπτογραφημένης ψήφου. Κατόπιν, ο αριθμός της ψήφου και η ψήφος αποστέλλονται στο server για να καταχωρισθούν από κοινού. Εν τέλει, μέσω του VotinApp.js, η νέα ψήφος αποθηκεύεται στο Voting Contract.

Σχετικά με την πειραματική διαδικασία αυτή διεξήχθη σε διαφορετικά είδη εκλογών, στα οποία μετείχαν οι Administrator, Creator και οι Voters. Ακολούθησαν μετρήσεις για τον ορισμό του gas cost και του time cost.Τα κόστη διαφοροποιούνταν, ανάλογα με τον αριθμό των voting options. Συγκεκριμένα, έβαιναν αυξανόμενα με την αύξηση των voting options. Αναφορικά στο time cost, αυτό εξαρτάται από το hardware και συνεπαγωγικά από τη διαδικασία εξόρυξης.

Οι τεχνικές δυσκολίες συναρτώνται με τη γλώσσα προγραμματισμού συστήματος, Solidity. Επεξηγηματικά, με τη διαδικασία κρυπτογράφησης και τη λειτουργία των debugging tools.

Ανακεφαλαιωτικά, παρά τις τεχνικές δυσκολίες που ενδεχομένως το σύστημα ηλεκτρονικής ψηφοφορίας αντιμετωπίζει, οι τεχνικές που χρησιμοποιούνται με το Blockchain, τα eth.calls, την Paillier Encryption και το MetaMask, εγγυώνται τις παραμέτρους ασφαλείας.

Στο άρθρο υπό τον τίτλο " Decentralized e – voting systems based on the Blockchain technology", (Hsiao, Tso, Chen, Wu, 2018) οι συγγραφείς εστιάζουν σε ένα σύστημα ηλεκτρονικής ψηφοφορίας, με τα εξής χαρακτηριστικά.

Η αρχιτεκτονική του συστήματος, συγκεράζει τα χαρακτηριστικά της αποκεντρωμένης δομής της τεχνολογίας του Blockchain, και των smart contracts, προκειμένου να βελτιστοποιηθεί η επαλήθευση/επιβεβαίωση των δεδομένων, να μειωθεί το κόστος και να διατηρηθεί η διαφάνεια της εκλογικής διαδικασίας.

Παράλληλα, η ανωνυμία των εκλογέων και η ασφάλεια της διαδικασίας, διασφαλίζεται με τη χρήση του "secret sharing scheme" καθώς και του "Paillier's public key cryptosystem".

Η ιδέα του "secret sharing scheme", προτάθηκε από το Shamir, το 1979. Η χρήση του, έγκειται στην αποτελεσματική άμυνα έναντι των απειλών και των επιθέσεων.

Το σύστημα ηλεκτρονικής ψηφοφορίας αποτελείται από τα εξής επτά μέρη. Τους Voters, οι οποίοι είναι αρμόδιοι για την ψήφο, το Registration Server, ο οποίος επιβεβαιώνει την ταυτότητα του εκλογέα και παρέχει στους δικαιούμενους ψηφοφόρους το πιστοποιητικό της ψήφου, το Authentication server, ο οποίος επιβεβαιώνει τα πιστοποιητικά από το Registration Center, το Voting Website, το οποίο αποτελεί το διαδικτυακό τόπο της ψηφοφορίας του συστήματος και υπόκειται στον έλεγχο των εκλογικών αρχών, το Recording Center, οι λειτουργίες του οποίου συνίστανται στην αποθήκευση των

πιστοποιητικών των ψηφοφόρων και των υπογραφών για την ψηφοφορία, όταν οι εκλογείς ενασκούν το εκλογικό τους δικαίωμα, τους Distributed Data Servers, στόχο των οποίων αποτελεί η αποθήκευση των κρυπτογραφημένων συντεταγμένων σημείων του επιλεγμένου αριθμού όταν ο εκλογέας ψηφίζει, και το Smart Contract, το οποίο αντικαθιστά τη λειτουργικότητα του συμβατικού bulletin πίνακα. Έχει τη δυνατότητα να καταμετρά τις ψήφους, ώστε να επαυξάνεται η αξιοπιστία της εκλογικής διαδικασίας.

Η διαδικασία ψηφοφορίας αποτελείται από τα στάδια των Initial Phase, Registration Phase, Voting Phase και Billing phase.

Το προτεινόμενο σύστημα ηλεκτρονικής ψηφοφορίας, εγγυάται τις ακόλουθες παραμέτρους: Voter qualification, Voter anonymity, Ballot eligibility και Ballot verifiability.

Καταληκτικά, το συγκεκριμένο e – voting system, αξιοποιεί τη διαφάνεια των smart contracts, ώστε να καθίσταται δυνατός ο έλεγχος τόσο της καταγραφής όσο και της επαλήθευσης της ψηφοφορίας. Επαυξάνει την εμπιστοσύνη των εκλογέων και απομειώνει την αναποτελεσματική χρήση των εκλογικών πόρων.

Στο άρθρο υπό τον τίτλο " Blockchain – enabled E – voting", (Khestri, Voas, 2018) οι συγγραφείς προσεγγίζουν τη θεματική της ηλεκτρονικής ψηφοφορίας υπό την πρόσληψη του Blockchain.

Το άρθρο εστιάζει σε δύο βασικούς παράγοντες, που συνδιαμορφώνουν τη διαδικασία της ηλεκτρονικής ψηφοφορίας. Τη συμμετοχή και την εξαπάτηση των ψηφοφόρων κατά την εκλογική διαδικασία.

Εισαγωγικά, οι συγγραφείς ορίζουν τη χρήση της τεχνολογίας του Blockchain στις εκλογές, αντιπαραβάλλοντας την με εκείνη των οικονομικών συναλλαγών με ψηφιακά νομίσματα. Επεξηγηματικά, κάθε ψηφοφόρος διαθέτει ένα μοναδικό "πορτοφόλι", με μοναδικά διαπιστευτήρια χρήστη καθώς και ένα μοναδικό νόμισμα, το οποίο αντιπροσωπεύει μία ψήφο.

Ακολούθως, οι συγγραφείς παραθέτουν παραδείγματα χρήσης του Blockchain σε εκλογικές διαδικασίες. Συγκεκριμένα, αναφέρονται εκλογές στη Ρωσία, όπου με το πρόγραμμα "Moscow's Active Citizen Program", διοργανώνονται ετησίως 5.000 – 7.000 εκλογικές συναντήσεις. Χαρακτηριστικά, έως το Φεβρουάριο του 2018, 3.450 εκλογικές διαδικασίες είχαν διενεργηθεί, με αντικείμενο ψηφοφορίας θέματα τοπικού ενδιαφέροντος. Εκλογές στη Νότια Κορέα, στην επαρχία Gyenoggi – do's, όπου η κορεάτικη

χρηματιστηριακή start – up εταιρεία Block, χρησιμοποίησε την πλατφόρμα Blockchain, για τη διευθέτηση ζητημάτων της τοπικής κοινωνίας. Στην Εσθονία, στην ετήσια συνάντηση της εταιρείας LVH Group, οι μέτοχοι ψηφίζουν μέσω της πλατφόρμας Blockchain, που σχεδίασε ο όμιλος Nasdaq. Στη Σιέρα Λεόνε, η ελβετική start – up Agora, ανέλαβε τη διεξαγωγή των γενικών εκλογών κατά το έτος 2018.

Κατόπιν, επισημαίνονται τα πλεονεκτήματα της χρήσης του Blockchain, όπως η ακριβής, ασφαλής και διαφανής διαχείριση των εγγραφών, η μείωση του λειτουργικού κόστους της εκλογικής διαδικασίας (επί παραδείγματι, έξοδα μεταφορών). Η βελτιωμένη επαλήθευση της ταυτότητας του εκλογέα, μέσω της ηλεκτρονικής καταχώρισης των δελτίων ταυτότητας, διπλωμάτων οδήγησης και διαβατηρίων, ως διαπιστευτηρίων του χρήστη. Η αύξηση της ταχύτητας διενέργειας των εκλογών. Η μείωση της αμφίβολης καταμέτρησης των ψήφων, όπως αυτή πραγματοποιείται με τα συμβατικά συστήματα. Η βελτίωση της διαφάνειας των αποτελεσμάτων, καθώς αυτά γνωστοποιούνται σε όλους τους ψηφοφόρους. Η αποτελεσματική αντιμετώπιση κακόβουλων επιθέσεων, λόγω της αποκεντρωμένης δομής του Blockchain και η προστασία της ιδιωτικότητας των εκλογέων, η οποία επιτυγχάνεται με την κρυπτογράφηση των προσωπικών τους δεδομένων.

Εξ αντιδιαστολής, ακολούθως αναφέρονται μειονεκτήματα της τεχνολογίας όπως η έλλειψη εμπιστοσύνης των εκλογέων στην τεχνολογία του Blockchain, ο ηλεκτρονικός αναλφαβητισμός των εκλογέων, η ποιότητα του λογισμικού η οποία ενδέχεται να επηρρεάσει την ασφάλεια της διαδικασίας, η κρατικοκεντρική κουλτούρα των ψηφοφόρων η οποία αντιτίθεται στην αποκεντρωμένη δομή του Blockchain και το αυξημένο ενεργειακό κόστος και η επισφαλής αποδοχή του e – voting, από την καθεστηκυία εξουσία.

Συμπερασματικά, οι συγγραφείς επισημαίνουν ότι η τεχνολογία βρίσκεται σε πρώιμο στάδιο, ωστόσο είναι πιθανή η επέκταση της καθώς είναι πιθανή και η μετατροπή των συμβατικών συστημάτων σε ηλεκτρονικά.

Στο άρθρο υπό τον τίτλο “ Towards the intelligent agents for blockchain e – voting system”, (Pawlak, Poniszewska – Maranda, Kryvinska, 2018) οι συγγραφείς πραγματεύονται το σύστημα ηλεκτρονικής ψηφοφορίας “ Auditable Blockchain Voting System”, το οποίο αποτελεί ένα non – remote και supervised σύστημα, το οποίο χρησιμοποιεί μια σύνδεση Internet για τη μεταβίβαση ψήφων και την αποθήκευση τους στο Blockchain.

Το σύστημα αποτελείται από τα μέρη Super node, το οποίο συνιστά το ανώτερο node και το οποίο υπόκειται απευθείας στην Εθνική Επιτροπή Εκλογών. Τα Trusted nodes, τα οποία αποτελούν τα υπολειπόμενα nodes του blockchain και τα οποία έχουν εγκριθεί από την Εθνική Επιτροπή Εκλογών. Σκοπεύουν στη συλλογή των ψήφων και την καθιέρωση της ορθής αλυσίδας, χρησιμοποιώντας τον consensus algorithm. Επίσης, στοχεύουν στη δημιουργία μιας επιπλέον αλυσίδας, στην περίπτωση ζημίας ή απώλειας της κύριας αλυσίδας. Τέλος, τα Polling stations, τα οποία αποτελούν εφαρμογές που αντιπροσωπεύουν τις εκλογικές περιφέρειες.

Τα ως άνωθι μέρη του ABVS συστήματος, επικοινωνούν εντός ενός peer – to – peer network.

Η ψηφοφορία στο ABVS σύστημα διακρίνεται στις εξής φάσεις: στην εναρκτήρια φάση, στην οποία επιλέγονται τα ιδρύματα, τα οποία θα λειτουργήσουν ως nodes, στη φάση της ψηφοφορίας, στην οποία περιλαμβάνεται η εγκατάσταση του εξοπλισμού και του λογισμικού στις σχετικές εκλογικές περιφέρειες και στη φάση της καταμέτρησης και επιβεβαίωσης των ψήφων, κατά την οποία οι ψήφοι καταμετρώνται και επαληθεύονται από το super node chain και τα trusted nodes.

Το ABVS System, χρησιμοποιεί σύστημα πολλαπλών πρακτόρων.

Ένα σύστημα πολλαπλών πρακτόρων αποτελείται από ένα σύνολο πρακτόρων, οι οποίοι συνεργάζονται προκειμένου να επιτευχθούν κοινοί στόχοι, συνήθως σε καταστάσεις όπου απαιτείται η επίλυση σε επιμερισμένα ή περίπλοκης υπολογιστικής φύσης προβλήματα.

Η διάδραση μεταξύ των πρακτόρων λαμβάνει τις μορφές της συνεργασίας για την επίτευξη στόχου, του συντονισμού της αποτελεσματικής χρήσης των διαθέσιμων πόρων και της διαπραγμάτευσης, αν εγερθούν συγκρούσεις.

Το σύστημα ABVS, επιτρέπει τη χρήση έξυπνων πρακτόρων για την επαύξηση της ασφάλειας κατά την εκλογική διαδικασία.

Οι έξυπνοι πράκτορες, διακρίνονται σε: authorization – configuration agents, οι οποίοι ευθύνονται για την αυθεντικοποίηση της εφαρμογής στις εκλογικές περιφέρειες, καθώς και για τη συναλλαγή με ένα trusted node. Μέσω αυτών των συναλλαγών, οι εκλογείς λαμβάνουν μοναδικές ηλεκτρονικές κάρτες ψηφοφορίας, με τις οποίες ψηφίζουν.

Οι έξυπνοι πράκτορες, επιτελούν τις λειτουργίες τους σε τρεις φάσεις. Η πρώτη είναι η authorization phase, η οποία εκκινεί με την εγκατάσταση του λογισμικού στα polling stations. Η δεύτερη είναι η configuration phase και η τρίτη, η voting phase.

Οι έξυπνοι πράκτορες διακρίνονται επίσης στους voting agents, οι οποίοι προμηθεύουν τους εκλογείς με μία κάρτα ψηφοφορίας κι αποστέλλουν την ψήφο στα nodes, με όλα τα απαιτούμενα μεταδεδομένα.

Το κύριο πλεονέκτημα του agent – based συστήματος ηλεκτρονικής ψηφοφορίας, έγκειται στην επιβεβαίωση της ασφάλειας της εκλογικής διαδικασίας μέσω της διαμεσολάβησης πρακτόρων, οι οποίοι εκπληρώνουν τις λειτουργίες που σχετίζονται με την επεξεργασία και τη μεταβίβαση των ψήφων. Επιπλέον, οι πράκτορες επιμερίζονται από nodes, οπότε καθίσταται αδύνατη η τροποποίησή τους. Περαιτέρω, το σύστημα επιτρέπει τη χρήση των υπολογιστικών πόρων που ευρίσκονται στα polling stations, μειώνοντας έτσι το burden στα nodes.

Η ως άνωθι προτεινόμενη λύση, βελτιώνεται με τη χρήση smart contracts, τα οποία επιτρέπουν την αυτόματη εκτέλεση των συμβολαίων, χωρίς τη συμμετοχή τρίτων συμβαλλομένων. Συνεπώς, μπορούν να χρησιμοποιηθούν προκειμένου να αποστέλλουν τους έξυπνους πράκτορες μεταξύ των εκλογικών περιφερειών και των trusted nodes.

Στο άρθρο υπό τον τίτλο “ Trustworthy electroning voting using adjusted Blockchain technology”, (Shahzad, Crowcroft, 2019) οι συγγραφείς παρουσιάζουν το πλαίσιο εντός του οποίου η τεχνολογία του Blockchain, αντιμετωπίζει προβλήματα κατά την εκλογική διαδικασία, την επιλογή των κατάλληλων αλγορίθμων, την προσαρμογή του Blockchain, τη διαδικασία της διαχείρισης των εκλογικών δεδομένων καθώς την ασφάλεια και την αυθεντικότητα της εκλογικής διαδικασίας.

Στην εισαγωγή του άρθρου οι συγγραφείς επισημαίνουν τη σπουδαιότητα της εκλογικής διαδικασίας και της ενάσκησης του δικαιώματος του εκλέγειν, ως μέσο νομιμοποίησης της κυβερνητικής πολιτικής στις σύγχρονες δημοκρατίες. Παράλληλα, υπογραμμίζουν την καταγραφόμενη δυσπιστία των ψηφοφόρων έναντι της εκλογικής διαδικασίας. Η αυξανόμενη δυσπιστία, οφείλεται σε παράγοντες όπως η δυσλειτουργική οργάνωση των εκλογών, η παραβίαση των αρχών που διέπουν την ψηφοφορία, ο ετεροκαθορισμός των πολιτικών πεποιθήσεων των εκλογέων και η ανεπαρκής, μη εποπτευόμενη καταμέτρηση των ψήφων. Οι παράγοντες αυτοί, επαυξάνουν την απάθεια του εκλογικού σώματος ενώ κρίνουν απαραίτητη τη δημιουργία ενός συστήματος ηλεκτρονικής ψηφοφορίας.

Ακολούθως, οι συγγραφείς παραθέτουν ιστορικά παραδείγματα ηλεκτρονικής ψηφοφορίας που έλαβαν χώρα στην Ελβετία (2017), την Αυστρία (2009), την Ιρλανδία

(2002), τη Γερμανία και την Ολλανδία, καθώς και δυσλειτουργίες που ανέκυψαν, σχετιζόμενες με το hardware και το software καθώς και τους hash αλγορίθμους.

Όσον αφορά την εκλογική διαδικασία, οι συγγραφείς προτείνουν ένα πλαίσιο, το οποίο βασίζεται στις ηλεκτρονικές μηχανές ψηφοφορίας και τη βιομετρική ταυτοποίηση του εκλογέα. Η διαδικασία αποτελείται από τα στάδια της καταγραφής των εκλογέων στις εκλογικές λίστες και του ελέγχου των δεδομένων από βιομετρικό σύστημα. Την επιλογή, κατά βούληση, των υποψηφίων μέσω της ηλεκτρονικής οθόνης ψηφοφορίας. Την καταχώριση της ψήφου, σύμφωνα με την αρχή "one man – one vote". Την ολοκλήρωση της ψηφοφορίας καθώς και τη δημοσίευση των εκλογικών αποτελεσμάτων.

Όσον αφορά τον τύπο του Blockchain, δηλαδή public, private, consortium, οι συγγραφείς προτείνουν τη χρήση του consortium Blockchain, καθώς αυτό θα εποπτεύεται από μία εθνική αρχή.

Σχετικά με τους hashing αλγορίθμους, αναφέρονται οι Md2, Md3, Md4, Md5, οι RIPEMD – 128, RIPEMD – 160, RIPEMD – 256 και RIPEMD – 320, οι SHA 1, SHA 256 και SHA 512, καθώς και οι αλγόριθμοι της οικογένειας Keccak. Οι συγγραφείς κλίνουν προς τους αλγόριθμους SHA 256 και SHA 512, καθώς δεν παρουσιάζουν δυσλειτουργίες και είναι ιδιαίτερα ασφαλείς.

Όσον αφορά τη δημιουργία των blocks, αυτή έπεται της εξής διαδικασίας: 1) επιβεβαίωση του μοναδικού αριθμού ταυτότητας και της βιομετρικής ταυτοποίησης του president officer, 2) χορήγηση άδειας για τη δημιουργία block, 3) δημιουργία hash μέσω του αλγορίθμου SHA 256 και αποστολή του στο president officer και 4) δημιουργία block.

Η δημιουργία επιπλέον block, απαιτεί την προαναφερθείσα διαδικασία.

Όσον αφορά το σφράγισμα των blocks, απαιτείται είτε η ολοκλήρωση του εκλογικού χρόνου, είτε η περάτωση της ψηφοφορίας όλων των ψηφοφόρων. Επίσης, η επιβεβαίωση της διαδικασίας από τον President Officer καθώς και το hashing των δεδομένων με τη χρήση του αλγόριθμου SHA – 256.

Η διαδικασία επαναλαμβάνεται για τα επόμενα blocks.

Όσον αφορά τη συλλογή των εκλογικών αποτελεσμάτων, αυτή επιτυγχάνεται από τα αποθηκευμένα δεδομένα στα blocks, μέσω της ιδιαίτερης οργάνωσης των nodes στο Blockchain. Η διαδικασία αυτή, συνεπικουρείται από ένα Merkel Tree.

Συνοπτικά, οι συγγραφείς επισημαίνουν πως η έλλειψη εμπιστοσύνης αποτελεί σύνηθες φαινόμενο στις αναπτυσσόμενες χώρες, ωστόσο η ηλεκτρονική ψηφοφορία ως εναλλακτική μορφή εκλογικής διαδικασίας, είναι πολλά υποσχόμενη.

Στο άρθρο υπό τον τίτλο "Blockchain – based e – voting system", (Hjalmarsson, Hreibarsson, 2018) οι συγγραφείς προτείνουν ένα σύστημα ηλεκτρονικής ψηφοφορίας, βασιζόμενο σε ένα "permissioned blockchain", ώστε να επιτευχθεί η Ρευστή Δημοκρατία ("Liquid Democracy"). Το permissioned Blockchain, αποτελεί μία παραλλαγή του consortium blockchain το οποίο χρησιμοποιεί τον consensus algorithm, "Proof of Authority". Η Ρευστή Δημοκρατία, συναρθρώνεται από τις διαδικασίες τόσο της άμεσης όσο και της έμμεσης (αντιπροσωπευτικής δημοκρατίας).

Σύμφωνα με τους συγγραφείς, ένα σύστημα ηλεκτρονικής ψηφοφορίας για να εφαρμοσθεί επιτυχώς σε εκλογές εθνικού επιπέδου, πρέπει να αποτρέπει τον ετεροκαθορισμό της ψήφου, να αποτρέπει την ιχνηλάτηση της ψήφου του εκλογέα μέσω των αναγνωριστικών διαπιστευτηρίων του, να εγγυάται την ορθή καταμέτρηση της ψήφου, να αποτρέπει τη συμμετοχή τρίτου μέρους στην επισφράγιση του ψηφοδελτίου, να απαγορεύει τη νόθευση του εκλογικού αποτελέσματος και να ορίζει σαφώς τα προσόντα των δικαιούμενων εκλογέων.

Για το σχεδιασμό του προτεινόμενου συστήματος, προτείνονται οι τεχνικές του Blockchain και των smart contracts, ώστε να επιτευχθεί η ασφάλεια και η μείωση του λειτουργικού κόστους της εκλογικής διαδικασίας.

Οι οντότητες του συστήματος, αποτελούνται από τους election administrators, οι οποίοι διαχειρίζονται τον κύκλο ζωής της διαδικασίας και οι αρμοδιότητες των οποίων συνίστανται στη δημιουργία των εκλογών, την ενεργοποίηση των εκλογών, την παρακολούθηση των ψήφων, την περάτωση των εκλογών, την παρακολούθηση του αποτελέσματος και την κοινοποίηση του αποτελέσματος. Από τους voters, οι οποίοι είναι αρμόδιοι για την καταχώριση της ψήφου. Από τα district nodes, η κύρια λειτουργία των οποίων συνίσταται στην επαλήθευση των ψήφων και από τα bootnodes. Κάθε ίδρυμα με εξουσιοδοτημένη άδεια στο δίκτυο, διαθέτει ένα bootnode. Τα bootnodes, συνεπικουρούν στην επικοινωνία μεταξύ των district nodes.

Όσον αφορά στην εκλογική διαδικασία, αυτή αντιπροσωπεύεται από smart contracts, τα οποία δηλώνονται στο Blockchain από τον election administrator. Η εκλογική διαδικασία, διακρίνεται στα στάδια του election creation, στο οποίο ο election administrator,

δημιουργεί τα δελτία της ψηφοφορίας. Το στάδιο voter registration, κατά το οποίο δημιουργείται ένας κατάλογος με τους δικαιούμενους εκλογείς. Το vote transaction και τα tallying results, όπου καταμετρώνται τα αποτελέσματα της ψηφοφορίας και επαληθεύεται η ψήφος. Κάθε εκλογέας μέσω της ηλεκτρονικής του ταυτότητας, μπορεί να επαληθεύει των ψήφο στην αρμόδια εκλογική υπηρεσία.

Σχετικά με τη μέθοδο της ασφάλειας της αυθεντικοποίησης, το προτεινόμενο σύστημα έχει σχεδιαστεί ώστε να χρησιμοποιεί ηλεκτρονικές ταυτότητες αυθεντικοποίησης, μέσω του Auokenni, ο οποίος είναι ισλανδικός service provider, και χρησιμοποιείται για την επιβεβαίωση των ταυτοτήτων. Ο Auokenni, κάνει χρήση Nexus λογισμικού και RFID scanners. Αναλυτικότερα, όταν ο χρήστης εγγράφεται για την παροχή ηλεκτρονικής ταυτότητας, επιλέγει έναν αριθμό PIN, που αντιστοιχεί στην ηλεκτρονική του ταυτότητα και οποίος αποτελείται από έξι αριθμούς. Συνεπώς, ο χρήστης αυθεντικοποιεί τα στοιχεία του, σαρώνοντας την ταυτότητα του και επιδεικνύοντας τον αντίστοιχο κωδικό PIN.

Αναφορικά στην ασφάλεια του συστήματος, εγείρονται ζητήματα που σχετίζονται με τις επιθέσεις DDoS, την τρωτότητα της διαδικασίας αυθεντικοποίησης και τις επιθέσεις Sybil. Σχετικά με τις επιθέσεις DDoS, ο επιτιθέμενος πρέπει να επιτεθεί σε κάθε ένα bootnode του ιδιωτικού δικτύου ξεχωριστά. Σε μια τέτοια περίπτωση, ο ιδιώτης ή το ίδρυμα, θα εντοπιζόταν αμέσως καθώς κάθε node είναι εξοπλισμένο με ένα"Byzantine fault tolerance algorithm", ο οποίος εντοπίζει αυτές τις επιθέσεις.

Σχετικά με την τρωτότητα της αυθεντικοποίησης, κάθε χρήστης ταυτοποιείται και αυθεντικοποιείται από το σύστημα, επιδεικνύοντας την ηλεκτρονική ταυτότητα από τον provider Auokenni και τον αντίστοιχο εξαψήφιο κωδικό PIN. Δίχως επίβλεψη, ένας χρήστης θα μπορούσε να ψηφίσει για περισσότερους χρήστες, αν γνώριζε τον κωδικό τους. Για την αποφυγή αυτής της δυσλειτουργίας, θα μπορούσε να εισαχθεί μέθοδος ταυτοποίησης, μέσω βιομετρικών δεδομένων.

Όσον αφορά τις επιθέσεις Sybil, αυτές στοχεύουν σε συγκεντρωτικά συστήματα και κατά τις οποίες ο επιτιθέμενος, δημιουργεί μια πληθώρα nodes, προκειμένου να διαταράξει το δίκτυο. Καθώς το προτεινόμενο σύστημα, εφαρμόζεται σε ιδιωτικό δίκτυο, κανένας ιδιώτης δεν μπορεί να πραγματοποιήσει είσοδο, για να δημιουργήσει τέτοια nodes.

Συνεπώς, το προτεινόμενο σύστημα, μέσω των παραμέτρων ασφαλείας που εγγυάται, προσφέρει τη δυνατότητα στζι σύγχρονες δημοκρατίες να εξελίξουν τα εκλογικά τους συστήματα από συμβατικά("pen and paper"), σε ηλεκτρονικά, διασφαλίζοντας ταυτογχρόνως την ασφάλεια και τη διαφάνεια των εκλογών. Μέσω της χρήσης ενός ιδιωτικού blockchain, είναι δυνατό να πραγματοποιούνται εκατοντάδες συναλλαγές ανά

δευτερόλεπτο. Σε χώρες μεγάλου μεγέθους, απαιτούνται μέτρα για την αύξηση των συναλλαγών ανά δευτερόλεπτο, όπως για παράδειγμα η " parent and child architecture", η οποία μειώνει τον αριθμό των συναλλαγών που αποθηκεύονται στο blockchain κατά αναλογία 1:100, χωρίς να μειώνεται η ασφάλεια του δικτύου.

Στο άρθρο υπό τον τιτλο " Blockchain voting and its effects on election transparency cote voter confidence", (Moura, Gomes, 2017) οι συγγραφείς εστιάζουν στη χρήση της τεχνολογίας Blockchain κατά την εκλογική διαδικασία και στο πώς επηρρεάζει τη διαφάνεια των εκλογών και την εμπιστοσύνη του εκλογέα.

Εισαγωγικά, ως εμπιστοσύνη του εκλογέα(voter confidence), ορίζεται η εμπιστοσύνη του ψηφοφόρου, ότι η ψήφος του καταμετρήθηκε ορθά στις εκλογές. Σύμφωνα με την υπόθεση " Winner or Loser", οι εκλογείς που υπερψήφισαν το νικητή των εκλογών, τείνουν να εμπιστεύονται περισσότερο το εκλογικό αποτέλεσμα, σε αντίθεση με τους εκλογείς που τον καταψήφισαν. Συνεπώς, η εμπιστοσύνη των εκλογέων διαφέρει σημαντικά, υπονομεύοντας έτσι μία από τις θεμελιώδεις αρχές της αντιπροσωπευτικής δημοκρατίας, που είναι η δυνατότητα εκλογής μελών της κυβέρνησης.

Οι συγγραφείς θεωρούν ότι οι τρέχουσες μέθοδοι ψηφοφορίας, ηλεκτρονικές ή μη, παρουσιάζουν μειωμένα επίπεδα διαφάνειας. Χαρακτηριστικά, η ηλεκτρονική ψηφοφορία με " Direct Recording Electronic Systems", δε θεμελιώνει την ορθότητα του αποτελέσματος καθώς δεν εγγυάται την ανάμειξη τρίτων μερών στη καταμέτρηση των ψήφων. Επίσης, τα ηλεκτρονικά συστήματα είναι επιρρεπή στις κακόβουλες επιθέσεις, όπως αυτό του συστήματος WIN, της πολιτείας Virginia καθώς και του DRE συστήματος της Βραζιλίας, όπου ένας κακόβουλος χρήστης μπορεί να διασυνδέσει την ψήφο με τον ψηφοφόρο, καταστρατηγώντας έτσι τη θεμελιώδη αρχή της μυστικότητας της ψήφου.

Η χρήση της τεχνολογίας Blockchain στις εκλογές, κρίνεται αναγκαία λόγω των ιδιοτήτων της συγκεκριμένης τεχνολογίας, όπως η επιμερισμένη και αποκεντρωμένη δομή της, που συντελούν στην αύξηση της διαφάνειας της εκλογικής διαδικασίας και συνεπαγωγικά στην αύξηση της εμπιστοσύνης του πολίτη – εκλογέα.

Οι προτάσεις για την υιοθέτηση της τεχνολογίας Blockchain, αυξάνουν ιδιαίτερα μετά τις προεδρικές εκλογές στις Η.Π.Α., το 2016, οπότε διαδιδόταν ότι οι εκλογικές μηχανές είχαν στοχοποιηθεί από υπερπόντιους hackers, καθώς και στις εκλογές της Φλόριντα, το 2000, όπου είχε κριθεί απαραίτητη η επανακαταμέτρηση των ψηφοδελτίων μεταξύ του Ρεπουμπλικανού υποψηφίου George W. Bush και του Δημοκρατικού Al Gore.

Λόγω των προαναφερόμενων εκλογικών δυσλειτουργιών, έχουν εμφανιστεί projects, όπως τα “Follow my vote”, “Vote watcher”, “Australia’s postal service” και “Bit Congress”, τα οποία ενσωματώνουν την τεχνολογία Blockchain, προκειμένου να εξασφαλισθεί η διαφάνεια στην εκλογική διαδικασία.

Ωστόσο, το Blockchain, είναι δυνατό να εμφανισθεί ως διπρόσωπος Ιανός. Αφενός, η διαφάνεια, η προστασία της ιδιωτικότητας, η αξιοπιστία και η εμπιστοσύνη των ψηφοφόρων αποτελούν αναμφισβήτητα πλεονεκτήματα της συγκεκριμένης τεχνολογίας. Αφετέρου, για την επικοινωνία με άλλα nodes, σε ένα peer – to – peer network, τα συστήματα ψηφοφορίας, πρέπει να συνδεθούν σε αυτό το δίκτυο. Συνεπώς, τα nodes είναι επιρρεπή σε απειλές και ζητήματα cyber security.

Συμπερασματικά, η χρήση του Blockchain τείνει να αυξάνει καθώς επηρρεάζει προσδιοριστικούς παράγοντες της εκλογικής συμπεριφοράς, όπως η εμπιστοσύνη του πολίτη – εκλογέα. Στην περίοδο της ηλεκρονικής δημοκρατίας και της ψηφιακής διακυβέρνησης, η υιοθέτηση distributed ledger τεχνολογιών, ενδέχεται να βοηθήσει στη σύζευξη των σχέσεων πολίτη – πολιτείας.

Στο άρθρο υπό τον τίτλο “Towards secure e – voting using Ethereum Blockchain”, (Koc, Yavuz, Cabuk, Dalkilic, 2018) οι συγγραφείς αναφέρονται σε ένα σύστημα ηλεκτρονικής ψηφοφορίας που προορίζεται για τη διεξαγωγή εκλογών σε ένα πανεπιστήμιο όπως, εκλογή πρυτάνεως ή εκλογή φοιτητικών συμβουλίων.

Πρωταρχικό στόχο, αποτελεί ο έλεγχος της εκλογικής διαδικασίας και η διασφάλιση ότι οι εκλογές θα διεξάγονται online, προκειμένου όλοι να συμμετέχουν απρόσκοπτα στη διαδικασία. Για το λόγο αυτό στην εκλογική διαδικασία, ενσωματώνεται η Blockchain πλατφόρμα Ethereum. Γίνεται χρήση Ethereum smart contracts, τα οποία επιτρέπουν τον έλεγχο και την καταμέτρηση των ψήφων, όταν ο χρόνος των εκλογών περατωθεί. Τα συμβόλαια έχουν τη δυνατότητα, να ρυθμίσουν το χρόνο και τη διάρκεια της διαδικασίας, η οποία κυμαίνεται από τα 120 έως τα 3.000 λεπτά. Επίσης, κάθε Ethereum λογαριασμός μπορεί να συμπεριληφθεί στις εκλογές, χρησιμοποιώντας τις hash values κάθε λογαριασμού, χωρίς να αποκαλύπτεται η ταυτότητα των χρηστών.

Στο συγκεκριμένο project, το περιβάλλον Ethereum, επιλέγεται ως περιβάλλον ανάπτυξης της πλατφόρμας και ως δίκτυο Blockchain. Και αυτό γιατί, ενώ το Bitcoin προορίζεται για την έγκριση χρηματιστηριακών συναλλαγών, το δίκτυο Ethereum, προσφέρει ένα ευρύτερο φάσμα εφαρμογών, με τη χρήση των smart contracts. Πολλές

εφαρμογές που απαιτούν ένα web server για να εκτελεσθούν, με τη χρήση των smart contracts μπορούν να εκτελεστούν χωρίς server.

Στο δίκτυο Ethereum, οι λειτουργίες εκτελούνται σε πραγματικό χρόνο και όλα τα blocks, εγγράφονται στην τελική αλυσίδα. Τα smart contracts επεξεργάζονται στη γλώσσα προγραμματισμού Solidity και εκτελούνται από τους peers του δικτύου Ethereum, ανά 15 δευτερόλεπτα, ενώ πρέπει να εγκριθούν από άλλους δύο χρήστες για να ενεργοποιηθούν. Μετά από αυτό, οι λειτουργίες των contracts μπορούν να εκτελεσθούν, και τα συμβόλαια να διαμοιρασθούν με τους υπόλοιπους υποψηφίους.

Για την επιτυχή διεξαγωγή των online εκλογών, πρέπει να επιλυθούν τα ζητήματα της διαφάνειας, της αυθεντικοποίησης και της αποδειξιμότητας στην εκλογική πλατφόρμα. Πρέπει να επαληθεύεται ότι οι εκλογείς, χρησιμοποιούν έγκυρα διαπιστευτήρια τα οποία μπορούν να επαληθεύονται κάθε στιγμή και ότι η εκλογική διαδικασία είναι απολύτως διαφανής. Για το σκοπό αυτό, πρέπει να συλλέγονται και να αποθηκεύονται δεδομένα, καθώς κανείς δεν πρέπει να μεταβάλλει την ψήφο του, αφού την καταχωρίσει. Επίσης, απαιτείται ατομικότητα στην εκλογική διαδικασία, ώστε κανείς να μην ασκεί το εκλογικό του δικαίωμα, έναντι τρίτων.

Τα ζητήματα αυτά, επιλύονται με την “peer – to – peer technology”. Είναι δυνατόν, να οριστούν τα απαιτούμενα αυτο – εκτέλεσιμα smart contracts στο Blockchain. Αφού τα smart contracts έχουν ενεργοποιηθεί, δεν μπορούν να εξαχθούν από αυτό και οι χρήστες, μπορούν να διαπιστώνουν αν η εκτέλεση των smart contracts, είναι αληθής ή όχι. Στο δίκτυο Ethereum, δεν υφίσταται η ανάγκη μιας κεντρικής αρχής για την παροχή proof – of – work. Όλοι οι peers, μπορούν να υπολογίζουν τα αποτελέσματα των contracts, χωρίς καμμία παρέμβαση.

Ωστόσο, η χρήση του αυθεντικού δικτύου Ethereum, είναι κοστοβόρα και καταλαμβάνει μεγάλη μνήμη του συστήματος. Για τους λόγους αυτούς, δίνεται η δυνατότητα στους developers να δημιουργούν private Ethereum networks. Ένα από αυτά αποτελεί το “Rinkeby network”, το οποίο χρησιμοποιείται στο συγκεκριμένο project.

Στο άρθρο υπό τον τίτλο, “Decentralized voting platform based on Ethereum Blockchain”, (Khoury, Kfoury, Kassem, Harb, 2018) οι συγγραφείς εστιάζουν στη χρήση ενός αποκεντρωμένου συστήματος ηλεκτρονικής ψηφοφορίας, το οποίο βασίζεται στο Ethereum Blockchain. Η βασική συνεισφορά αυτού του συστήματος, έγκειται στον

περιορισμό των πολλαπλών ψήφων, ανά συσκευή κινητού τηλεφώνου (“Mobile Station International Subscriber Directory Number – MSISDN”).

Τα κύρια πλεονεκτήματα του συστήματος συνίστανται στην ενδυνάμωση της τρωτότητας και της εγκυρότητας των εκλογικών δεδομένων, τη διασφάλιση της αξιοπιστίας του εκλογικού συστήματος, την αποκέντρωση του μηχανισμού εγγραφής και επιβεβαίωσης των εκλογέων, τη διαφάνεια του εκλογικού συστήματος, τη δημοσιοποίηση των ψήφων, τον περιορισμό μιας ψήφου ανά αριθμό κινητού τηλεφώνου και την εμπιστευτικότητα των καταγεγραμμένων ψήφων.

Το σύστημα αποτελείται από τα μέρη Web Application, με το οποίο οι event admistrators δημιουργούν και διαχειρίζονται νέα εκλογικά γεγονότα. Κάθε εκλογικό γεγονός, αντιπροσωπεύεται από ένα συγκεκριμένο smart contract στο Blockchain. Από τους Event Management Servers, ο κύριος σκοπός των οποίων συνίσταται στην ανάπτυξη του smart contract στο δίκτυο, με τα δεδομένα που έχουν ληφθεί από το web application. Από smart contracts, τα οποία υποδιαιρούνται σε δύο κατηγορίες: τα Registration Contracts και τα Voting Contracts. Από μία SMS Gateway, η οποία διαθέτει εξέχουσα βαρύτητα καθώς αυθεντικοποιεί τους χρήστες μέσω της αποστολής SMS messages στην καθορισμένη MSISDN και μία Mobile application, η οποία χρησιμοποιείται από τους εκλογείς προκειμένου να εγγραφούν στο σύστημα και να ψηφίσουν.

Όσον αφορά τη διαδικασία της εγγραφής του εκλογεά, αυτή διενεργείται ως εξής: Η εφαρμογή, ανευρίσκει αυτόματα τον αριθμό τηλεφώνου του χρήστη (MSISDN), από την κάρτα SIM. Για το registration και το configuration του χρήστη, προαπαιτείται συγκεκριμένος αριθμός Ethers. Ακολούθως, η λειτουργία Register, καλείται με τη MSISDN του χρήστη. Κατόπιν, το smart contract εγκρίνει τη MSISDN και αποστέλλει ένα HTTP αίτημα, μέσω του Oraclize contract στο “True Random Number Generator, (TRNG)” server, ώστε να δημιουργήσει ένα τυχαίο κωδικό PIN. Επισημαίνεται ότι το Oralclize, είναι μια υπηρεσία η οποία παρέχει μία ασφαλή σύνδεση μεταξύ των smart contracts και των εξωτερικών web Api’s. Έπειτα, το smart contract, επικοινωνεί μέσω του Oraclize, με το “Short Message Service (SMS) Gateway”, η οποία αποστέλλει ένα SMS στο MSISDN, με τον κωδικό PIN. Ακολούθως ο χρήστης εισάγει τον κωδικό PIN στην εφαρμογή και το smart contract ελέγχει την ορθότητα του PIN.

Εκτός της διαδικασίας της εγγραφής του εκλογέα, υπάρχει και η λειτουργία της δημιουργίας ενός εκλογικού γεγονότος(“ Creating a voting event”). Για τη δημιουργία ενός γεγονότος, απαιτείται ο event organizer να εισάγει ερωτήσεις και να καταγράφει τις

απαντήσεις, μέσω του web. Σε τεχνικό επίπεδο, αυτό συνεπάγεται τη δημιουργία ενός voting contract στο Blockchain.

Σχετικά με τη διαδικασία της ψηφοφορίας, η εφαρμογή καλεί τη "Vote For(string option)" μέθοδο του smart contract που έχει αναπτυχθεί στο "Ethereum Virtual Machine". Ακολούθως το "voting contract", επικοινωνεί με το "registration contract", ώστε να ελέγξει αν ο χρήστης έχει ήδη εγγραφεί. Έπειτα, ελέγχει αν ο χρήστης έχει ήδη ψηφίσει ή το εκλογικό γεγονός έχει περατωθεί. Αν οι συνθήκες ικανοποιούνται, το smart contract, αυξάνει τον αριθμό καταχώρισης της ψήφου, βεβαιώνει ότι ο χρήστης έχει ψηφίσει και αποστέλλει ένα success message στην εφαρμογή.

Το smart contract, ακυρώνει αυτόματα, διπλές ψήφους, επιτρέποντας τον περιορισμό μιας ψήφου άνα MSIMDN. Η τελευταία λειτουργία συνιστά το κυριότερο πλεονέκτημα του προτεινόμενου συστήματος.

Κατά την πειραματική διαδικασία, καταδείχθηκε ότι η εγγραφή του χρήστη στο σύστημα, απαιτεί 2 – 4 λεπτά, ενώ η λειτουργία της ψηφοφορίας απαίτεί 40 δευτερόλεπτα έως 2 λεπτά.

Το συγκεκριμένο σύστημα, θα μπορούσε να αναπτυχθεί περαιτέρω ώστε να χρσιμοποιηθεί σε εθνικές γενικές εκλογές, να αντικαταστήσει τα συγκεντρωτικά συστήματα ψηφοφορίας και να βελτιώσει την εκλογική διαδικασία σε κυβερνήσεις, εκθέσεις και διαγωνισμούς.

Στο άρθρο υπό τον τίτλο "Investigating performance constraints for blockchain based secure – e voting system", (Khan, Arshad, Khan, 2020) οι συγγραφείς αναφέρονται στους περιορισμούς που επηρρεάζουν την απόδοση και scalability ενός συστήματος ηλεκτρονικής ψηφοφορίας.

Συγκεκριμένα, οι συγγραφείς εστιάζουν στην εντοπισμό και την ανάδειξη παραγόντων όπως το μέγεθος του block ("block size"), ο ρυθμός δημιουργίας block ("block generation rate") και η ταχύτητα επεξεργασίας των συναλλαγών ("transaction processing speed") προκειμένου να επιτευχθούν scalable λύσεις, μέσω της τεχνολογίας του Blockchain.

Η πειραματική διαδικασία, εφαρμόζεται τόσο σε permissioned όσο και σε permissionless blockchain συστήματα. Στο permissionless blockchain, προσομοιώνονται περιβάλλοντα με μικρότερο αριθμό χρηστών, υιοθετώντας ένα δημόσιο Blockchain. Η πειραματική διαδικασία ποικίλλει σχετικά με το επίπεδο δυσκολίας εξόρυξης νέου block, το μέγεθος του block και το μέσο χρόνο δημιουργίας ενός block. Τα πειράματα αυτά

αποκαλύπτουν σημαντικά trade – offs, μεταξύ του μεγέθους του block, το ρυθμό δημιουργίας block και την ταχύτητα επεξεργασίας της συναλλαγής.

Στο permissioned Blockchain, προσομειώνονται περιβάλλοντα ηλεκτρονικής ψηφοφορίας με μεγάλο αριθμό ψηφοφόρων, όπως στα δημόσια εκλογικά συστήματα. Η πειραματική διαδικασία συνίσταται στην αξιολόγηση του συστήματος, σχετικά με τον όγκο των συναλλαγών όσο και με τον αριθμό των κινητών μηχανών ψηφοφορίας που λειτουργούν από διαφορετικές τοποθεσίες του δικτύου, προκειμένουνα παρατηρηθεί η επίδραση αυτών των περιορισμών στη συνολική απόδοση του συστήματος.

Στο permissionless Blockchain, εφαρμόστηκαν δύο πειραματικές υποθέσεις, στις οποίες μετείχαν δέκα ψηφοφόροι και όλοι οι υποψήφιοι είχαν τον προνόμιο να εξορύξουν τις ψήφους στο Blockchain.

Στο permissioned Blockchain, μετείχαν καθορισμένα nodes ως miners και ως validators. Αυτό το μοντέλο, αντιπροσωπεύει μια δημόσια εκλογική διαδικασία, όπου τα καθορισμένα μέλη είναι υπεύθυνα για τη δίκαιη της εκλογικής διαδικασίας.

Η πειραματική διαδικασία κατέδειξε σημαντικές παρατηρήσεις σε σχέση με τη συνολική αποτελεσματικότητα και τη scalability του συστήματος, συμπεριλαμβανομένων trade - offs, μεταξύ διαφορετικών παραμέτρων όπως η ασφάλεια και η απόδοση του συστήματος.

Βασική συνεισφορά του άρθρου υπό τον τίτλο “Matrict: efficient, scalable and post – quantum Blockchain confidential transactions protocol”, (Esgin et alt., 2019) αποτελεί η εισαγωγή του Matrict, ενός αποτελεσματικού Ring CT πρωτοκόλλου, το οποίο εγγυάται την εμπιστευτικότητα των συναλλαγών στο Blockchain.

Η ασφάλεια του συγκεκριμένου πρωτοκόλλου, βασίζεται στις “post – quant lattice assumptions”. Το proof length του πρωτοκόλλου, υπολογίζεται σε δύο τάξεις μεγέθους μικρότερο από τις ήδη υπάρχουσες “post – quantum” προτάσεις και κλιμακώνεται αποτελεσματικά σε μεγάλα anonymity sets, σε αντίθεση με τις προυπάρχουσες προτάσεις.

Περαιτέρω, παρουσιάζεται η πρώτη εφαρμογή του πλήρους “post – quantum Ring CT”, αναδεικνύοντας την πρακτικότητα του πρωτοκόλλου.

Συγκεκριμένα, μία τυπική συναλλαγή μπορεί να δημιουργηθεί σε κλάσμα δευτερολέπτου και να επαληθευθεί σε 23 milliseconds, σε ένα standard H/Y. Επιπλέον, παρουσιάζεται το πώς το συγκεκριμένο σχήμα μπορεί να επεκταθεί, ώστε να επιτυγχάνεται

auditability, όπου ένας χρήστης έχει τη δυνατότητα να επιλέξει μια συγκεκριμένη αρχή (authority) από ένα κατάλογο αρχών, για να αποκαλύψει την ταυτότητα του. Ο χρήστης έχει επίσης τη δυνατότητα να επιλέξει "no - auditing". Όλες αυτές οι επιλογές auditing, μπορούν να συνυπάρξουν στο ίδιο περιβάλλον.

Τα βασικά μέρη του MatRiCT, τα οποία οποία προτείνονται στο συγκεκριμένο άρθρο αποτελούνται από 1) τη μικρότερη έως τώρα "scalable ring signature" μεταξύ των lattice assumptions, χωρίς να απαιτείται Γκαουσιανό sampling , 2) μία νέα zero – knowledge proof ισορροπία και 3) ένα αποσπώμενο "commitment scheme" από τα lattices.

Τα ανωτέρω χαρακτηριστικά είναι καίριας σημασίας για εφαρμογές που απαιτούν την εγγύηση της ιδιωτικότητας, όπως τα συστήματα ηλεκτρονικής ψηφοφορίας. Παρά την επιτρεπόμενη 64 – bit precision για τις συναλλαγές, το νέο balance proof και συνεπώς το πρωτόκολλο, δεν απαιτούν ένα εύρος proof σε ένα πλατύ εύρος (όπως 32 ή 63 bits εύρος), το οποίο αποτελούσε έως τώρα σημαντικό εμπόδιο έναντι της αποτελεσματικότητας των lattice – based λύσεων.

Επιπλέον, παρατίθενται νέοι ορισμοί για Ring CT πρωτόκολλα. Οι ορισμοί, είναι εφαρμόσιμοι σε γενικό πλαίσιο και ως εκ τούτου συνεισφέρουν στην ανάπτυξη μελλοντικών πρωτοκόλλων συναλλαγών, που απαιτούν εμπιστευτικότητα εν γένει (όχι μόνο στο lattice setting).

Στο άρθρο υπό τον τίτλο " Secure digital voting system based on blockchain technology", (Khan, Arshad, Khan, 2018) οι συγγραφείς εστιάζουν σε ένα σύστημα ηλεκτρονικής ψηφοφορίας, το Multichain, το οποίο πληροί τις παρακάτω προυποθέσεις : 1) Ιδιωτικότητα, το σύστημα κάνει χρήση των κρυποτογραφικών ιδιοτήτων του Blockchain για τη διασφάλιση της ιδιωτικότητας του εκλογέα. Με την εγγραφή του εκλογέα, δημιουργείται ένα hash του εκλογέα το οποίο αποτελεί το μοναδικό αναγνωριστικό του κάθε ψηφοφόρου. 2) Eligiblity, όλοι οι δικαιούμενοι χρήστες χρησιμοποιούν μοναδικά αναγνωριστικά, όπως κυβερνητικά έγγραφα, τεχνολογία δακτυλικού αποτυπώματος και βιομετρικά δεδομένα προκειμένου να αποφευχθεί η διπλή ψηφοφορία. 3) Ελευθερία ψήφου, το προτεινόμενο σύστημα δίνει τη δυνατότητα στον εκλογέα να ψηφίζει κατά βούληση, δημιουργώντας ένα κρυπτογραφικό hash για κάθε ψήφο. 4) Convinience, το σύστημα χρησιμοποιεί ένα φιλικό προς το χρήστη interface το οποίο απαιτεί την ελάχιστη εισαγωγή δεδομένων από τον εκλογέα, όπως δακτυλικό αποτύπωμα, αντί κωδικών και συνθηματικών. 5) Verifiability, μετά την καταχώριση της ψήφου, ο εκλογέας λαμβάνει μια μοναδική ταυτότητα συναλλαγής υπό τη μορφή ενός κρυπτογραφημένου hash.

Το σύστημα αποτελείται από τα επίπεδα “User interaction and fron – end security”, το οποίο χρησιμεύει στη διάδραση εκλογέα και administrator. Ενθυλακώνει δύο βασικές λειτουργίες, τον καθορισμό της αυθεντικότητας και τον καθορισμό της αρμοδιότητας του εκλογέα και του administrator. Από το “Access control management payer”, το οποίο δρα συνεπικουρικά στις λειτουργίες του επιπέδου 1 και 3, προκειμένου να επιτευχθούν οι λειτουργίες τους, όπως ο καθορισμός των ρόλων, οι πολιτικές ελέγχου εισόδου και ο ορισμός των εκλογικών συναλλαγών. Από το “E – voting transaction management layer”, το οποίο αποτελεί το κύριο επίπεδο της αρχιτεκτονικής του συστήματος, όπου η e – voting συναλλαγή η οποία έχει δημιουργηθεί στο επίπεδο “Role Management/Transactions”, χαράσσεται στο Blockchain προκειμένου να εξορυχθεί. Στο επίπεδο αυτό, εμπεριέχονται επίσης τα διαπιστευτήρια του χρήστη, του επιπέδου 1, όπως το δακτυλικό αποτύπωμα. Το επόμενο επίπεδο αποτελεί το “ Ledger Synchronisation layer”, που συγχρονίζει το Multichain ledger με την τοπική εφαρμογή βάσης δεδομένων. Οι ψήφοι καταγράφονται στον πίνακα δεδομένων της βάσης δεδομένων. Οι εκλογείς μπορούν να εντοπίσουν τις ψήφους τους, χρησιμοποιώντας την ταυτότητα που τους παρέχεται, μόλις η ψήφος τους έχει εξορυχθεί και προστεθεί στο blockchain ledger.

Η διαδικασία ψηφοφορίας, συναρθρώνεται ως εξής: Ο εκλογέας συνδέεται με το σύστημα μέσω του δακτυλικού αποτυπώματος του. Αν το αποτύπωμα αναγνωρισθεί επιτυχώς, εμφανίζεται η λίστα των υποψηφίων. Άλλως, περαιτέρω διαδικασίες απορρίπτονται. Μετά την ψηφοφορία, οι έγκυρες και επιβαιωμένες ψήφοι προστίθενται στο public ledger. Οι παράγοντες ασφαλείας της ψήφου, βασίζονται στην τεχνολογία blockchain με τη χρήση κρυπτογραφικών hashes, τα οποία διασφαλίζουν end – to – end επαλήθευση. Το σύστημα, διασφαλίζει την αρχή “one man – one vote”, με τη χρήση του μοναδικού δακτυλικού αποτυπώματος του εκλογέα, προκειμένου να αποφευχθεί η διπλή ψηφος. Ακολούθως της έγκρισης της ψήφου, ο εκλογέας ενημερώνεται μέσω μηνύματος ή mail, για την ταυτότητα της εκλογικής διαδικασίας με την οποία μπορεί να εντοπίσει την ψήφο του στο ledger.

Για την εφαρμογή του συστήματος, χρησιμοποιήθηκε Java EE, στην πλατφόρμα Nebeans και server Glassfish για τη φιλοξενία της εφαρμογής. Η εφαρμογή χρησιμοποιεί MySQL, ως backend database και περιέχει τα δεδομένα που εισήχθησαν από τον admin. Επίσης, η εφαρμογή υποστηρίζει την εισαγωγή δεδομένων με τη χρήση MS Excel spreadsheets.

Στο άρθρο υπό τον τίτλο, “ Distributed E – Voting and E – Bidding Systems based on Smart Contract”, (Tso, Liu, Hsiao, 2019) οι συγγραφείς εστιάζουν στη χρήση ενός συστήματος ηλεκτρονικής ψηφοφορίας, το οποίο αποτελείται απο τις τεχνολογίες Electronic bidding, Ethereum and smart contracts, Paillier cryptosystem, Additive Homomorphic Encryption, Shamir’s Secret Sharing Scheme και Oblivious transfer.

Επισημαίνεται ότι το Elctronic Bidding θεμελιώνεται στις διατάξεις των άρθρων του “Government Procurement Act”, αποτελείται δε, από τις φάσεις: Tender inviting phase, tender obtaining phase, tender submitting phase, tender opening phase, tender deciding phase και contract management phase.

Οι οντότητες του συστήματος διακρίνονται στους voter, registration server, authentication server, voting website, record center και smart contract.

Η εκλογική διαδικασία αποτελείται από τις φάσεις initial phase, registration phase, voting phase, opening phase και verification phase.

Όσον αφορά το E – bidding system, αυτό αποτελείται από τις οντότητες vendor, government certification administrator, financial authority, tender authority, tender website και smart contracts.

Σχετικά με τη διαδικασία E – bidding, αποτελείται από τις φάσεις initial phase, invitation phase, obtaining phase, bidding phase, opening phase, decision phase και contract management phase.

Κύριο στόχο του συγκεκριμένου πρωτοκόλλου, αποτελεί ο συνδυασμός ενός e – voting και e – bidding συστήματος το οποίο διαφοροποιείται από τα υπάρχοντα ηλεκτρονικά συστήματα και το οποίο αντικαθιστά τυχόν εμπλεκόμενα τρίτα μέρη, με ένα smart contract, το οποίο διαθέτει δημόσιες και διαφανείς λειτουργίες. Θεμελιώδη ιδέα, αποτελεί ο συνδυασμός της τεχνολογίας του Blockchain με την τεχνολογία της κρυπτογραφίας για την προστασία της ιδιωτικότητας, ώστε όλοι οι συμμετέχοντες να έχουν τη δυνατότητα να μετέχουν στην opening phase. Παράλληλα, στόχο αποτελεί η ανωνυμία των συμμετεχόντων, η ιδιωτικότητα των δεδομένων κατά τις συναλλαγές καθώς η εγκυρότητα και επαληθευσιμότητα των δεδομένων.

Ζητήματα που σχετίζονται με την ασφάλεια και την ιδιωτικότητα στο Blockchain, αναφέρονται στο άρθρο υπό τον τίτλο “ Bitcoin and Blockchain: Security and privacy”, (Zaghloul, Li, Mutka, Ren, 2020)

Οι συγγραφείς εστιάζουν στις κυριότερες προκλήσεις ασφάλειας και ιδιωτικότητας και πώς αυτές αντιμετωπίζονται μέσω της τεχνολογίας Blockchain. Επισημαίνονται οι σοβαρότερες απειλές ασφάλειας. Συγκεκριμένα, αναλύεται ο κίνδυνος των "double – spending attacks", η αξιολόγηση της πιθανότητας επιτυχίας των προαναφερόμενων επιθέσεων και η εξαγωγή συμπερασμάτων σχετικά με το κέρδος του επιτιθέμενου. Οι "double – spending attacks", διακρίνονται στις Race attacks, τις Finney attacks, τις Vector 76 attacks και τις 51% attacks. Επιπλέον παρατίθενται οι κίνδυνοι που σχετίζονται με το P2P Bitcoin network, όπως οι Denial Service Atttacks, Sybil Attacks, Eclipse Attacks και Routing Attacks.

Στο άρθρο υπό τον τίτλο "Blockchain Based E – Voting Recording System Desgin", (Hanifatunissa, Rahardjo. 2017), οι συγγραφείς αναφέρονται σε ένα ηλεκτρονικό σύστημα ψηφοφορίας του οποίου η συνεισφορά συνίσταται στην καταγραφή του εκλογικού αποτελέσματος με τη χρήση Blockchain αλγορίθμων. Σε αντίθεση με το Proof of Work του Bitcoin, οι συγγραφείς προτείνουν μια μέθοδο η οποία βασίζεται σε ένα προκαθορισμένο turn του συστήματος, για κάθε node, κατά τη δόμηση του Blockchain. Ο λόγος που συνέτεινε στο σχεδιασμό του συγκεκριμένου συστήματος, αποτελεί η παραποίηση των δεδομένων στις βάσεις δεδομένων. Οι συγγραφείς προτείνουν την τεχνολογία του Blockchain, προκειμένου να αντιμετωπιστεί η παραποίηση αυτή, χάριν της αποκεντρωμένης δομής του Blockchain. Συγκεκρίμενα, το εν λόγω σύστημα χρησιμοποιείται μετά το πέρας της εκλογικής διαδικασίας. Η χρήση hash values κατά την καταγραφή των εκλογικών αποτελεσμάτων σε κάθε εκλογικό τμήμα, συντείνει στην επαύξηση της ασφάλειας της καταγραφής των δεδομένων και η χρήση ψηφιακών υπογραφών, καθιστά το σύστημα περισσότερο αξιόπιστο.

Συνεπώς, το ανωτέρω Blockchain based e – voting system, επικεντρώνεται στη διασφάλιση της εγκυρότητας του εκλογικού αποτελέσματος.

Συμπερασματικά, ο σχεδιασμός και η χρήση ηλεκτρονικών συστημάτων με τη χρήση της τεχνολογίας του Blockchain, βαίνουν αυξανόμενοι. Οι δυσλειτουργίες που εμφανίζονταν τόσο στα συμβατικά συστήματα ψηφοφορίας όσο και σε κάποια από τα υπάρχοντα ηλεκτρονικά, οδήγησαν στην αύξηση της προσφοράς τέτοιων συστημάτων. Τα blockchain based e – voting systems, διασφαλίζουν βασικές παραμέτρους της εκλογικής διαδικασίας όπως ανωνυμία των χρηστών, ασφάλεια της εκλογικής διαδικασίας, ακεραιότητα των δεδομένων, αξιόπιστη καταμέτρηση ψήφων, διαφάνεια και εγκυρότητα του εκλογικού αποτελέσματος, μείωση του κόστους των εκλογών και μείωση του χρόνου διεξαγωγής της εκλογικής διαδικασίας.

Ως προς τις τεχνικές των συστημάτων, αυτές συνίστανται στη χρήση της αποκεντρωμένης τεχνολογίας του Blockchain, του consortium και private Blockchain της distributed ledger technology, του secret sharing scheme, του Pailler's public – cryptosystem, της elliptic curve cryptography, των post – quantum protocols, του permissionless Blockchain, του permissioned Blockchain, των Ethereum protocols και subprotocols, της additive homomorphic encryption, των SHA – 256 και SHA – 512 hashing algorithms καθώς και του multi – agent system.

Ως προς τις οντότητες των συστημάτων αυτές συνίστανται κυρίως στους election administrators, voters, registration servers, record centers, authentication servers, central authorities, voting administrators και tallying authorities.

Ως προς τις φάσεις της εκλογικής διαδικασίας, αυτές αποτελούνται κυρίως από το initial set – up, voter registration, registration phase, authetincation phase, ballot creation, ballot load, vote, voting, tallying και verification.

Η καταγραφή των ανωτέρω συστημάτων ηλεκτρονικής ψηφοφορίας, αναδεικνύει το ενδιαφέρον της επιστημονικής κοινότητας για τη διασφάλιση της εγκυρότητας της εκλογικής διαδικασίας, ως μέσου δημοκρατικής νομιμοποίησης της κυβερνητικής πολιτικής, με τη χρήση της τεχνολογίας του Blockchain.

Κεφάλαιο 5: Ερωτηματολόγιο

Για την παρούσα μεταπτυχιακή διατριβή κρίθηκε σκόπιμο να διενεργηθεί διαδικτυακή έρευνα, προκειμένου να προσδιορισθούν οι τάσεις των εκλογέων σχετικά με τις παραμέτρους που πληρούν τα Blockchain based e – voting systems και συνακόλουθα με την εμπιστοσύνη και τη συμμετοχή των εκλογέων στην εκλογική διαδικασία.

Τα ερωτήματα που υποβλήθηκαν, συνίστανται στα εξής:

1) Θεωρείτε ότι οι αρχές της άμεσης, μυστικής, καθολικής, ίσης, ταυτόγχρονης διεξαγωγής και αυτοπρόσωπης άσκησης της ψήφου, διασφαλίζονται πληρέστερα από το ισχύον συμβατικό εκλογικό σύστημα ή από ένα εναλλακτικό ηλεκτρονικό σύστημα ψηφοφορίας με τη χρήση της τεχνολογίας του Blockchain;
2) Θεωρείτε ότι η εγκυρότητα του εκλογικού αποτελέσματος και συνεπαγωγικά η νομιμοποίηση της Κυβέρνησης και η άσκηση της κυβερνητικής πολιτικής, διασφαλίζεται πληρέστερα από το ισχύον συμβατικό εκλογικό σύστημα ή από ένα εναλλακτικό ηλεκτρονικό σύστημα ψηφοφορίας με τη χρήση της τεχνολογίας του Blockchain;

3) Εμπιστεύεστε τους θεσμικούς πολιτειακούς λειτουργούς ή ένα ηλεκτρονικό σύστημα με τη χρήση της τεχνολογίας του Blockchain, για την ομαλή, αξιόπιστη και διαφανή τήρηση της εκλογικής διαδικασίας;
4) Θεωρείτε ότι το επίπεδο του ηλεκτρονικού αναλφαβητισμού συναρτάται με το ποσοστό συμμετοχής του εκλογικού σώματος στις εκλογικές διαδικασίες με ηλεκτρονικά συστήματα ψηφοφορίας;
5) Θεωρείτε ότι τα ηλεκτρονικά συστήματα με τη χρήση της τεχνολογίας του Blockchain, θα ενθάρρυναν ή θα αποθάρρυναν τη συμμετοχή του εκλογικού σώματος στην άμεση και απευθείας άσκηση της εξουσίας (άμεση δημοκρατία);
6) Θεωρείτε ότι η τρωτότητα του εκλογικού συστήματος είναι περισσότερο επισφαλής από παραβατική συμπεριφορά των θεσμικών πολιτειακών λειτουργών ή από κακόβουλες επιθέσεις στα ηλεκτρονικά συστήματα ψηφοφορίας (hacking);
7) Θεωρείτε ότι προσδιοριστικό παράγοντα της συμμετοχής του εκλογικού σώματος στην εκλογική διαδικασία, αποτελεί η πολιτική και πολιτειακή αγωγή του εκλογέα ή το εκλογικό σύστημα (συμβατικό/ηλεκτρονικό).

Κεφάλαιο 6: Συμπεράσματα

Τις τελευταίες δεκαετίες η ανάπτυξη της πληροφορικής και των τηλεπικοινωνιών, έχει επηρρεάσει ποικιλοτρόπως πολλές από τις πτυχές της ανθρώπινης δραστηριότητας. Στις περισσότερες περιπτώσεις συμβάλλουν στην ταχύτερη και ακριβέστερη ολοκλήρωση διαδικασιών που σχετίζονται με ποικίλες διαδικασίες. Οι διαδικασίες ψηφοφορίας στις περισσότερες περιοχές του πλανήτη είναι εκείνες που επηρρεάζουν τη σύνθεση των κυβερνήσεων. Αν και και η νομοθεσία κάθε χώρας μπορεί να καθορίζει τη ροή και τους κανόνες των διαδικασιών αυτών με διαφορετικό τρόπο, σε κάθε περίπτωση είναι εκείνες που καθορίζουν σε μεγάλο βαθμό τις τύχες των πολιτών. Οι διαδικασίες ψηφοφορίας χρησιμοποιούνται και σε άλλες περιπτώσεις, όπως σε έρευνες για τις τάσεις της κοινής γνώμης, σε διεργασίες καθορισμού νικητών σε διαγωνισμούς, σε προωθητικές ενέργειες και σε διαδικασίες λήψης αποφάσεων. Αντικειμενικός σκοπός των ψηφοφοριών είναι να καταδείξουν με δίκαιο τρόπο το νικητή, έναντι του ανταγωνισμού.

Η εμπλοκή της πληροφορικής στην υλοποίηση των διαδικασιών ψηφοφοριών, αποσκοπεί στην ταχύτερη επεξεργασία των ψήφων προς παραγωγή του αποτελέσματος με

τη βέλτιστη ακρίβεια. Η συνδρομή της πληροφορικής δύναται να διευκολύνει την προώθηση των ψήφων για την επεξεργασία τους αλλά και την άμεση μετάδοση του αποτελέσματος.

Από την ανωτέρω ανάλυση των είκοσι (20) άρθρων καταδείχθηκαν 1) οι ανάγκες που οδηγούν στη διεξαγωγή ψηφοφοριών, 2) στο κατά πόσο επηρρεάζουν διαχρονικά οι ψηφοφορίες τις ανθρώπινες κοινωνίες και τις πολιτικές εξελίξεις, εντοπίζοντας τη σπουδαιότητα της ποιότητας των ψηφοφοριών για τον άνθρωπο, 3) ποια είναι τα χαρακτηριστικά που πρέπει να πληρούν οι διαδικασίες ψηφοφορίας ούτως ώστε να προσδιορίζονται ως επιτυχημένες, 4) ποια είναι τα υπάρχοντα ή υπό σχεδίαση συστήματα ηλεκτρονικής ψηφοφορίας και με ποιον τρόπο αναδεικνύει το κάθε ένα απο αυτά το νικητή, 5) πώς διασφαλίζεται η εγκυρότητα του εκλογικού αποτελέσματος, η διαφάνεια της εκλογικής διαδικασίας, η προστασία της ανωνυμίας των εκλογέων, η ασφαλής διαχείριση των δεδομένων, η ορθή και αξιόπιστη καταμέτρηση των ψήφων, η προστασία της ακεραιότητας των δεδομένων και η ασφάλεια των ηλεκτρονικών συστημάτων ψηφοφορίας από κακόβουλες επιθέσεις (hacking), η μείωση του απαιτούμενου χρόνου διεξαγωγής των εκλογών καθώς και η μείωση του κόστους διεξαγωγής των εκλογών.

Τα ανωτέρω αποτελούν σημαντικούς προσδιοριστικούς παράγοντες συμμετοχής του εκλογικού σώματος στην εκλογική διαδικασία. Η συμμετοχή των εκλογέων καθίσταται κομβικής σημασίας καθώς η ενάσκηση του εκλογικού δικαιώματος, νομιμοποιεί την Κυβέρνηση και τη συνακόλουθη κυβερνητική πολιτική.

Ωστόσο, από την έρευνα δεν προκύπτει ότι η διεξαγωγή των εκλογών με ηλεκτρονικά συστήματα ψηφοφορίας, συνεπάγεται την αύξηση της εμπιστοσύνης και της συμμετοχής των εκλογέων στις εκλογικές διαδικασίες. Η μικρή συμμετοχή των ψηφοφόρων στις εκλογές, αποτελεί ένα γενικότερο παγκόσμιο φαινόμενο το οποίο είναι εξαιρετικά ανησυχητικό. Η συμμετοχή μικρού μέρους του εκλογικού σώματος στις ψηφοφορίες καθιστά επισφαλή τα εκλογικά αποτελέσματα και την αξιοπιστία της ανάδειξης των νικητών, καθώς η πιθανότητα αυτοί, να μην εκπροσωπούν την κυρίαρχη βούληση των πολιτών είναι αυξημένη. Μεγάλο μέρος των εκλογέων που απέχουν από τις εκλογικές διαδικασίες, ενεργούν έτσι λόγω της πολιτικής απάθειας. Υπάρχει επίσης ένα μεγάλο μέρος του πληθυσμού που για διαφορετικούς λόγους δε δύναται να ψηφίσει με φυσική παρουσία σε ένα συγκεκριμένο μέρος για μία δεδομένη χρονική περίοδο. Αν και οι περιορισμοί αυτοί, αίρονται ως ένα βαθμό με τη χρήση των ηλεκτρονικών συστημάτων ψηφοφορίας, τα οποία διασφαλίζουν βασικές αρχές της ψηφοφορίας, δεν τεκμαίρεται από τα δεδομένα της έρευνας ότι η εμπιστοσύνη των ψηφοφόρων και η συμμετοχή τους στις εκλογές βαίνει αυξανόμενη

με τη χρήση των e – voting blockchain systems. Η σύγχρονη βιβλιογραφία εστιάζει στη διεξοδική ανάλυση των τεχνικών χαρακτηριστικών του κάθε e – voting system project. Από τη μελέτη των άρθρων συνάγεται ότι τα Blockchain based e – voting systems, διασφαλίζουν την ασφάλεια της εκλογικής διαδικασίας, εξασφαλίζουν την ιδιωτικότητα των εκλογέων, εγγυώνται την ακεραιότητα των δεδομένων τους, πληρούν τις παραμέτρους για την εγκυρότητα του εκλογικού αποτελέσματος, μειώνουν το χρόνο της εκλογικής διαδικασίας, μειώνουν τα λειτουργικά κόστη (χαρτί, μισθοδοσία). Ωστόσο δεν εξάγονται συμπεράσματα που να επιβεβαιώνουν την αύξηση της εμπιστοσύνης και της συμμετοχής των εκλογέων στις εκλογές και τη συνεπαγόμενη νομιμοποίηση των δημόσιων πολιτικών, παρά τη χρήση ηλεκτρονικών συστημάτων ψηφοφορίας. Ενδεχομένως, η εκλογική συμπεριφορά καθορίζεται και από εξω – τεχνολογικούς παράγοντες. Χαρακτηριστικά αναφέρονται τα πρότυπα της εκλογικής συμπεριφοράς στις μνημειώδεις έρευνες "American Voter" (Campel et alt., 1960) και Political change in Britain (Butler, Stoke, 1969).

Η ιδέα της διεξαγωγής εκλογών με ηλεκτρονικά συστήματα ψηφοφορίας, απέκτησε ιδιαίτερη δημοφιλία στην Εσθονία το 2001. (European Commission, 2021). Η Εσθονία, αποτέλεσε το πρώτο κράτος το οποίο διοργάνωσε εκλογές με e – voting system, στις δημοτικές εκλογές το 2005. Επίσης, το 2007 η διεξαγωγή των βουλευτικών εκλογών με ηλεκτρονική ψηφοφορία, αποτέλεσε παγκόσμια πρωτοτυπία.

Η Εσθονία πληροί τις προυποθέσεις για τη διεξαγωγή εκλογών με ηλεκτρονικά συστήματα ψηφοφορίας. Οι πολίτες της Εσθονικής Δημοκρατίας, διακρίνονται για την υψηλή ηλεκτρονική ανάγνωση. Οι υποδομές της είναι σύγχρονες, με αποτελεσματικά κυβερνητικά IT programs ενώ παράλληλα η αγαστή συνεργασία μεταξύ ιδιωτικού και δημόσιου τομέα, επιτρέπει τη δημιουργία ηλεκτρονικών υπηρεσιών που προσανατολίζονται σε ένα κράτος με επίκεντρο τον πολίτη. Το 2002, το Εσθονικό Κοινοβούλιο, εισήγαγε τη νομοθετική βάση για τη διεξαγωγή ηλεκτρονικών ψηφοφοριών. Η ευρεία διάθεση εθνικών ID ταυτοτήτων υπήρξε ζωτικής σημασίας για την υιοθέτηση του ηλεκτρονικού συστήματος ψηφοφορίας. Η κάρτα ID, η οποία καθιερώθηκε από την Εσθονική Κυβέρνηση το 2002, αποτελεί το κύριο έγγραφο ταυτοποίησης με διττή λειτουργία: αφενός λειτουργεί ως φυσικό έγγραφο, αφετέρου ως ηλεκτρονική ταυτότητα.

Η υιοθέτηση e – voting system, παρέχει τη δυνατότητα στους εκλογείς, ιδιαιτέρως για αυτούς που βρίσκονται εκτός της εσθονικής επικράτειας ή σε μεγάλη απόσταση από τα τοπικά εκλογικά τμήματα, να ενασκούν τα εκλογικά τους δικαιώματα.

Επιπλέον είναι δυνατή η μείωση του κόστους όσον αφορά στην κατανάλωση χαρτιού που προορίζεται για τα ψηφοδέλτια και η μείωση του χρόνου της ψηφοφορίας.

Χαρακτηριστικά, κατά το έτος 2013, ο μέσος χρόνος ψηφοφορίας ανήλθε στο 1:29, το 2014 στο 1:21 και το 2015 στο 1:36 λεπτά. Σωρευτικά, η εξοικονόμηση χρόνου κατά τις βουλετικές εκλογές το 2011, ανήλθε στις 11.000 εργατοώρες οι οποίες αντιστοιχούν στην εξοικονόμηση 504.000 ευρώ.

Πάραυτα, η συμμετοχή των Εσθονών πολιτών στις Ευρωπαικές Εκλογές, παρουσιάζεται μειωμένη σε σχέση με τη συμμετοχή των πολιτών της Ελληνικής και της Κυπριακής Δημοκρατίας κατά τα έτη 2009, 2014 και 2019.

Συγκεκριμένα, σύμφωνα με τα δεδομένα του Ευρωπαικού Κοινοβουλίου για τη συμμετοχή των πολιτών ανά κράτος, στις εκλογές για την ανάδειξη των Ευρωβουλευτών, τα ποσοστά συμμετοχής ανά χώρα διαμορφώνονται ως εξής:

Χώρα	2009	2014	2019
Ελλάδα	52,54%	59,97%	58,69%
Εσθονία	43,90%	36,52%	37,60%
Κύπρος	59,40%	43,97%	44,99%

Συνεπώς, από τα στατιστικά δεδομένα προκύπτει ότι η συμμετοχή των εκλογέων της Ελληνικής και της Κυπριακής Δημοκρατίας που διατηρούν συμβατικά συστήματα ψηφοφορίας, υπερβαίνει της συμμετοχή των εκλογέων της Εσθονικής Δημοκρατίας η οποία έχει υιοθετήσει ηλεκτρονικό σύστημα ψηφοφορίας.

Ενδεχόμενα κωλύματα ως προς τη συμμετοχή των Εσθονών πολιτών στην εκλογική διαδικασία, προκύπτουν από την ελλιπή εμπιστοσύνη των εκλογέων στα e – voting systems, τον ηλεκτρονικό αναλφαβητισμό των ψηφοφόρων και τον απαιτούμενο τεχνολογικό εξοπλισμό για την προστασία της ιδιωτικότητας και της ακεραιότητας των δεδομένων. (European Parliament, 2021).

Στο πλαίσιο της παρούσας διατριβής, διενεργήθηκε διαδικτυακή έρευνα προκειμένου να διαπιστωθεί η εμπιστοσύνη των ψηφοφόρων στα εκλογικά συστήματα (συμβατικά και ηλεκτρονικά) και συνακόλουθα η συμμετοχή τους στις δημοκρατικές διαδικασίες παραγωγής της κρατικής βούλησης.

Επισημαίνεται ότι, λόγω του μικρού εύρους της διαδικτυακής έρευνας η στατιστική ανάλυση δεν έχει στατιστική βαρύτητα.

Αξίζει ωστόσο να σημειωθεί, εντός του εύρους αυτού, ότι ως προσδιοριστικός παράγοντας συμμετοχής στις εκλογικές διαδικασίες αξιολογείται η πολιτική αγωγή του πολίτη παρά το εκλογικό σύστημα.

Κατωτέρω, παρατίθεται η φόρμα του διαδικτυακού ερωτηματολογίου.

1.

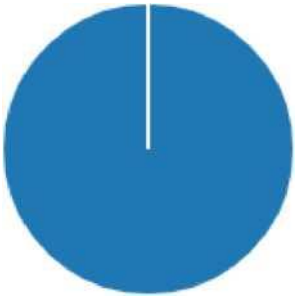
Το ερωτηματολόγιο δεν συλλέγει προσωπικά δεδομένα. Το ερωτηματολόγιο αποθηκεύει μόνο τις απαντήσεις και όχι πληροφορίες που αφορούν τους συμμετέχοντες.

Φύλο

Άντρας 11

Γυναίκα 7

Άλλο 0



3·

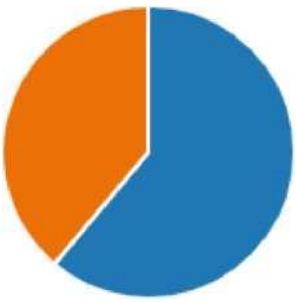
Ηλικία

<20 0

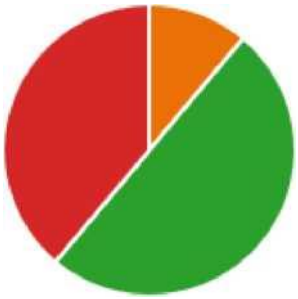
21-35 2

36-50 9

>50 7



4. Μορφωτικό επίπεδο

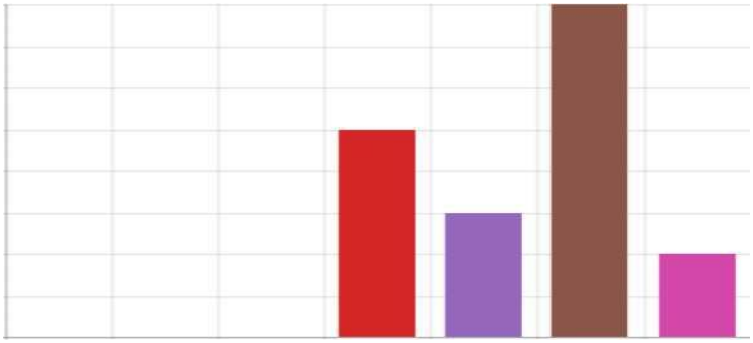


- ♦ Απόφοιτος Δημοτικού 0
- ♦ Απόφοιτος Γυμνασίου 0
- ♦ Απόφοιτος Λυκείου 0

♦ Ανώτερη μόρφωση (ΙΕΚ κ.λπ.) 5

- Ανώτατη μόρφωση (ΑΕΙ/ΤΕΙ) 3
- Μεταπτυχιακό 8

♦ Διδακτορικό 2



5·

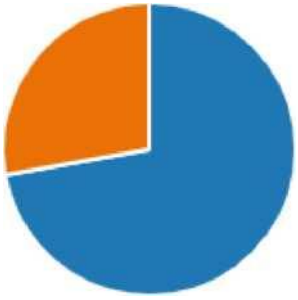
Θεωρείτε ότι οι αρχές της άμεσης, μυστικής, καθολικής, ίσης, ταυτόγχρονης διεξαγωγής και αυτοπρόσωπης άσκησης της ψήφου, διασφαλίζονται πληρέστερα

- Από το ισχύον συμβατικό εκλογικό σύστημα 13
- Από ένα εναλλακτικό ηλεκτρονικό σύστημα ψηφοφορίας με τη χρήση της τεχνολογίας του Blockchain 5

6.

Θεωρείτε ότι η εγκυρότητα του εκλογικού αποτελέσματος και συνεπαγωγικά η νομιμοποίηση της Κυβέρνησης και η άσκηση της κυβερνητικής πολιτικής, διασφαλίζεται πληρέστερα

Από το ισχύον συμβατικό εκλογικό σύστημα 11



Από ένα εναλλακτικό ηλεκτρονικό σύστημα ψηφοφορίας με τη χρήση της τεχνολογίας του Blockchain 7

7.

Εμπιστεύεστε

Τους θεσμικούς πολιτειακούς λειτουργούς 12

Ένα ηλεκτρονικό σύστημα ψηφοφορίας με τη χρήση της τεχνολογίας του Blockchain, για την ομαλή, αξιόπιστη και διαφανή τήρηση της εκλογικής διαδικασίας 6

8.

Θεωρείτε ότι το επίπεδο του ηλεκτρονικού αναλφαβητισμού συναρτάται με το ποσοστό συμμετοχής του εκλογικού σώματος στις εκλογικές διαδικασίες με ηλεκτρονικά συστήματα ψηφοφορίας;

Ναι 12

Όχι 6

9.

Θεωρείτε ότι τα ηλεκτρονικά συστήματα ψηφοφορίας με τη χρήση της τεχνολογίας του Blockchain

Θα ενθάρρυναν τη συμμετοχή του εκλογικού σώματος στην άμεση και απευθείας άσκηση της εξουσίας (άμεση δημοκρατία) 14

Θα αποθάρρυναν τη συμμετοχή του εκλογικού σώματος στην άμεση και απευθείας άσκηση της εξουσίας (άμεση δημοκρατία) 4

10.

Θεωρείτε ότι η τρωτότητα του εκλογικού συστήματος είναι περισσότερο επισφαλής

από παραβατική συμπεριφορά των θεσμικών πολιτειακών λειτουργών	7
από κακόβουλες επιθέσεις στα ηλεκτρονικά συστήματα ψηφοφορίας (hacking)	11

11.

Θεωρείτε ότι προσδιοριστικό παράγοντα της συμμετοχής του εκλογικού σώματος στην εκλογική διαδικασία, αποτελεί

η πολιτική και πολιτειακή αγωγή του εκλογέα	15
το εκλογικό σύστημα (συμβατικό/ηλεκτρονικό)	2

Εν κατακλείδι, από την έρευνα της βιβλιογραφίας προκύπτει ότι σχετικά με τα ερωτήματα, όπως αυτά τέθηκαν στο υποκεφάλαιο 2.5 (Προσδιορισμός των ερευνητικών ερωτημάτων), τα Blockchain based e – voting systems διασφαλίζουν την ασφάλεια της εκλογικής διαδικασίας, εξασφαλίζουν την ιδιωτικότητα των εκλογέων, εγγυώνται την ακεραιότητα των δεδομένων τους, πληρούν τις παραμέτρους για την εγκυρότητα του εκλογικού αποτελέσματος, δεν αποτρέπουν τον ετεροκαθορισμό της πολιτικής βούλησης των εκλογέων, μειώνουν το χρόνο της εκλογικής διαδικασίας και τα λειτουργικά κόστη. Πάραυτα, δε συνάγεται ότι τα Blockchain based e – voting systems αυξάνουν την εμπιστοσύνη των εκλογέων και τη συμμετοχή τους στην εκλογική διαδικασία.

Βιβλιογραφικές Αναφορές

Al – Farsi, S., Rathore, M. M., & Bakiras, S. (2021). *Applied science.* Ανάκτηση από:

Security of Blockchain-Based Supply Chain Management Systems: Challenges and Opportunities: https://arxiv.org/pdf/1904.00733

Choo, K. – K. R., Ozcan, S. Dehghantanha, A., & Parizi, R. M. (2020). Blockchain Ecosystem-Technological and Management Opportunities and Challenges. Ανάκτηση από:Researchgate:https://www.researchgate.net/publication/344810353_Blockchain_Ecosystem-Technological_and_Management_Opportunities_and_Challenges. Ανάκτηση από: https://ieeexplore.ieee.org/document/9226671.

Chaieb, M., Yousfi, S., Lafourcade, P., Robbana, R. (2018) *Verify – your – vote: A verifiable Blockchain – based Online Voting Protocol*. 15th European Mediterranean and Middle Eastern Conference on Information Systems. Ανάκτηση από: https://hal.archives-ouvertes.fr/hal-01874855.

Dagher, G. G., Marella, P. B., Milojkovic, M., Mohler, J. (2018). *Bronco Vote: Secure Voting System using Ethereum's Blockhain.* Proceedings of the 4th International Conference on Information Systems Security and Privacy CICISSP, (96 –107). Ανάκτηση από: https://www.researchgate.net/publication/322874160_BroncoVote_Secure_Voting_System_using_Ethereum's_Blockchain.

Esgin, M. F., et alt. (2019). *MatRiCT: Efficient, Scalable and Post – Quantum Blockchain Confidential Transactions Protocol*. 2019 ACM SIGSAC conference on Computer and Communication Security (CCS'19). Ανάκτηση από: https://research.monash.edu/en/publications/matrict-efficient-scalable-and-post-quantum-blockchain-confidenti.

Gomanthi, S., Soni, M,. Dhiman, G. & Ramya, G. (2021). A survey on applications and security issues of blockchain technology in business sectors. Ανάκτηση από: A survey on applications and security issues of blockchain technology in business sectors.

Estonian Internet Voting. Ανάκτηση από: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/2019/07/29/Estonian+Internet+voting.

European election results. Ανάκτηση από: https://www.europarl.europa.eu/about-parliament/en/in-the-past/previous-elections.

Hanifatunissa, R., Rahardjo, B. (2017). *Blockchain Based E – Voting Recording System Design.* 2017 11th International Conference on Telecommunications Systems Services and Applications. Ανάκτηση από: https://ieeexplore.ieee.org/document/8272896.

Hardwick, F. S., Gioulis, A., Akram, R. N., Markantonakis, K. (2018). *E – voting with Blockchain: An E – Voting Protocol with Decentralisation and Voter Privacy.* 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing) Ανάκτηση από: https://ieeexplore.ieee.org/abstract/document/8726645.

Hassan, F. u., Ali, A., Rahouti, M., Latif, S., & Kanhere, S. (2020*). Blockchain and the Future of the Internet: A Comprehensive Review.* Ανάκτηση από: https://arxiv.org/pdf/1904.00733.pdf.

Hjalamarsson, F. P., Hreibarsson, G., K. (2018). *Blockchain – Based E – Voting System.* 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), (983 – 986). Ανάκτηση από: file:///X:/Downloads/sensors-21-05874-v4%20(4).pdf.

Hsiao, J. H., Tso, R., Chen, C. M., Wu, M. E. (2018). Decentralized E – Voting Systems Based on the Blockchain Technology. *Advances in Computer Science and Ubquitous Computing, Lecture Notes in Electrical Engineering. 474.* Ανάκτηση από: https://www.researchgate.net/publication/321947971_Decentralized_E-Voting_Systems_Based_on_the_Blockchain_Technology.

Jafar, U., Juzaiddin, M., Aziz, A., & Shukur, Z. (2021). *). Blockchain for Electronic Voting System - Review and Open Research Challenges.* Ανάκτηση από: https://www.mdpi.com/1424-8220/21/17/5874/pdf.

Liang, Y.-C. (2020). *Blockchain for Dynamic Spectrum Management.* Ανάκτηση από: https://www.researchgate.net/publication/337306138_Blockchain_for_Dynamic_Spectrum_Management.

Khan, K. M., Arhsad, J. , Khan, M., M. (2020). Investigating performance constraints for Blockchain based secure e – voting system. *Future Generation Computer Systems, 105,* (13 – 26). Ανάκτηση από: https://www.sciencedirect.com/science/article/abs/pii/S0167739X19310805.

Khan, K. K., Arhsad, J., Khan, M., M. (2018). Secure Digital Voting System based on Blockchain Technology. *International Journal of Electronic Government Research*.

Khestri, N., Voas, J. (2018). Blockchain – Enabled E – voting. *IEEE Sofware, 35* (4), *(95 – 99).* Ανάκτηση από: https://www.igi-global.com/article/secure-digital-voting-system-based-on-blockchain-technology/206172.

Khoury, D., Kfoury, E. F., Kassem, A., Harb, H. (2018). *Decentralized Voting Platform Based on Ethereum Blockchain.* 2018 IEEE International Multidisciplinary Conference

on Engineering Technology (IMCET), (1 – 6). Ανάκτηση από: https://ieeexplore.ieee.org/document/8603050.

Koc, A. K., Yavuz, E., Cabuk, U. C., Dalkilic, G. (2018). *Towards Secure E – Voting Using Ethereum Blockchain.* 2018 6th International symposium on Digital Forensic and Security (ISDFS), (1 – 7). Ανάκτηση από: https://www.researchgate.net/publication/323318041_Towards_Secure_E-Voting_Using_Ethereum_Blockchain.

McCorry, P., Shahandashti, S. F., Hao, F. (2017). *A smart contract for Boardroom Voting with Maximum Voter Privacy*. International Conference on financial Cryptography and Data Security. Ανάκτηση από: https://www.researchgate.net/publication/322000346_A_Smart_Contract_for_Boardroom_Voting_with_Maximum_Voter_Privacy.

Monrat, A. A., Schelen, O., Anderson, K. (2020). *A Survey of Blockchain From the Prospectives of Applications, Challenges and Opporunities.* Ανάκτηση από IEEE: https://ieeexplore.ieee.org

Moura, T., Gomes, A. (2017). Blockchain Voting and its Effects on Election Transparency and Voter Confidence. *Proceedings of dg.o.* Ανάκτηση από: https://dl.acm.org/doi/10.1145/3085228.3085263.

Mueller, P., & Bergsträßer, S. (2018). *The Bitcoin Universe: An Architectural Overviewof the Bitcoin Blockchain.*Ανάκτηση από: https://dl.gi.de/bitstream/handle/20.500.12116/16570/DFN-Forum-Proceedings-001.pdf?sequence=1&isAllowed=y.

Natarajan, H., Krause, S., Gradstein, H. (2017). *Distrbuted Ledger Technology and Blockchain.* Fin Tech Note; No. 1. World Bank, Washington, DC. Ανάκτηση από OKR: https://openknowledge.worldbank.org.handle/10986/29053

Pawlak, M., Ponszewska – Maranda, A., Kryvinska, N. (2018). *Towards the intelligent agents for Blockchain e – voting system.* The 9th International Conference on Emerging Ubiquitious Systems and Pervasive Networks (EUSPN 2018), (239 – 246). Ανάκτηση από: https://www.sciencedirect.com/science/article/pii/S1877050918318271.

Rahman, A., Hossaim, S., Hassanain, E., & Alhamin, M. (2018*). Blockchain-Based Mobile Edge Computing Framework for Secure Therapy Applications.* Ανάκτηση από: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8534320.

Rawat, D. B., Chaudhary, V., & Doku, R. (2020*). Blockchain Technology: Emerging Applications and Use Cases for Secure and Trustworthy Smart Systems*. Ανάκτηση από: https://www.mdpi.com/2624-800X/1/1/2/pdf.

Reyna, A., Martin, C., Chen, J. Soler, E., Diaz, M. (2018). *On Blockchain and its integration with IoT. Challenges and Opprotunities.* Future Generation Computer Systems. Vol. 88, November 2018, pp. 173 – 190. Ανάκτηση από: Science Direct: https://sciencedirect.com/science/article/pii/50167739X1739205

Shahzad B., Crowcroft, J. (2019). *Trustworthy electronic voting using adjusted blockchain technology.* Ανάκτηση από: IEEE: https://ieeexplore.ieee.org/abstract/document/8651451

Statista. (2021). *Size of the Bitcoin blockchain from January 2009 to September 13, 2021*. Ανάκτηση από: https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/

Tso, R., Liu, Z.Y., Hsiao, J.H. (2019). Distributed E – Voting and E – Bidding Systems on Smart Contract. *Electronics 2019, 8.* Ανάκτηση από: https://www.researchgate.net/publication/332373069_Distributed_E-Voting_and_E-Bidding_Systems_Based_on_Smart_Contract.

Wang, J., Nu, P., Wang, X., Shou, W. (2017). *The outlook of blockchain technology for construction engineering management.* Frontiers. Eng. Manage. Vol. 4, no 1, pp. 67 – 75. Ανάκτηση από Western Sydney University: https://researchdirect.westernsydney.edu.au

Yi, H. (2019). Security e – voting based on blockchain in P2P network. *Yi EURASIP Journal on Wirelss Communications and Networking.* Ανάκτηση από: https://www.researchgate.net/publication/333439952_Securing_e-voting_based_on_blockchain_in_P2P_network.

Yu, B. et alt. (2018). *Platform – independent Secure Blockchain – Based Voting System.* International Conference on Information Security. (369 – 386). Ανάκτηση από:https://research.monash.edu/en/publications/platform-independent-secure-blockchain-based-voting-system.

Zaghloul, E,. Li, T., Mutka, M.W., Ren, J. (2020). Bitcoin and Blockchain Security and Privacy. *IEEE Internet of Things Journal.* Ανάκτηση από: https://ieeexplore.ieee.org/document/9122595.