Προστασία της Ιδιωτικότητας σε περιβάλλον Αλυσίδας μπλοκ (Privacy on Blockchain)

Μια συγκριτική ανάλυση διαφορετικών προσεγγίσεων και τεχνικών.

Κωνσταντόπουλος Βάιος - baioskonst@gmail.com
Ε20081

Βαρελάς Απόστολος-Φοίβος - aposvarelas@gmail.com
Ε20014

Τμήμα Ψηφιακών Συστημάτων

Μάθημα: «Τεχνολογίες Διασφάλισης Ιδιωτικότητας»

Καθηγητής: Κ. Λαμπρινουδάκης

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
UNIVERSITY OF PIRAEUS

Duckster Team

Περίληψη

Η εργασία είναι μια εις βάθος εξερεύνηση της τομής μεταξύ της τεχνολογίας blockchain και της προστασίας της ιδιωτικής ζωής. Ξεκινά με μια επισκόπηση της τεχνολογίας blockchain, δίνοντας έμφαση στην εξάρτησή της από τα δίκτυα Τεχνολογίας Κατανεμημένης Λογιστικής (DLT) και Peer-to-Peer (P2P). Αυτά τα θεμελιώδη στοιχεία παρέχουν τη διαφάνεια και την ασφάλεια που κάνουν το blockchain ένα επαναστατικό εργαλείο σε διάφορους τομείς. Ωστόσο, εγείρουν επίσης σημαντικές ανησυχίες για την ιδιωτικότητα, τις οποίες η εργασία εξετάζει λεπτομερώς.

Η εργασία διερευνά τη χρήση ιδιωτικών και δημόσιων κλειδιών στο blockchain, μια κρίσιμη πτυχή της ταυτότητας του χρήστη και της ασφάλειας των συναλλαγών. Στη συνέχεια, εμβαθύνει σε κρυπτογραφικές μεθόδους που χρησιμοποιούνται για τη βελτίωση της ιδιωτικότητας σε συστήματα blockchain, συμπεριλαμβανομένης της χρήσης αποδείξεων μηδενικής γνώσης, υπογραφών δακτυλίου και διευθύνσεων Stealth. Αυτές οι τεχνικές παρέχουν τρόπους επαλήθευσης συναλλαγών και προστασίας των ταυτοτήτων των χρηστών χωρίς να αποκαλύπτονται περιττές πληροφορίες, ενισχύοντας έτσι την ιδιωτικότητα.

Συζητείται επίσης η έννοια της ανάμειξης, μια μέθοδος που χρησιμοποιείται για να αποκρύψει την ιχνηλασιμότητα των συναλλαγών. Στη συνέχεια, η εργασία παρέχει μια ολοκληρωμένη σύγκριση διαφορετικών συστημάτων απορρήτου blockchain, επισημαίνοντας τα μοναδικά χαρακτηριστικά, τα δυνατά και τα αδύνατα σημεία τους.

Κατηγοριοποιεί περαιτέρω τα συστήματα blockchain σε Δημόσια, Ιδιωτικά, Υβριδικά και Συστήματα Blockchain Consortium. Καθένα από αυτά τα συστήματα

προσφέρει διαφορετικά επίπεδα απορρήτου, διαφάνειας και ελέγχου, καθιστώντας τα κατάλληλα για διαφορετικές εφαρμογές και βιομηχανίες.

Η ενότητα "Ανάλυση-Σύνθεση" της εργασίας παρέχει μια ανάλυση των προβλημάτων που περιβάλουν το blockchain, καθώς και λύσεις αυτών των προβλημάτων, μέσω των τεχνικών και προσεγγίσεων που παρουσιάστικαν ήδη μέχρι αυτό το σημείο.

Τέλος, η εργασία ολοκληρώνεται με τα «Συμπεράσματα», συνοψίζοντας τα βασικά ευρήματα και τις επιπτώσεις της έρευνας. Υπογραμμίζει τη σημασία της ιδιωτικότητας στο blockchain και την ανάγκη για συνεχή έρευνα και ανάπτυξη για την αντιμετώπιση των ανησυχιών, καθώς η τεχνολογία blockchain συνεχίζει να εξελίσσεται και να αποκτά ευρεία υιοθέτηση.

Ουσιαστικά, η εργασία παρέχει μια ολοκληρωμένη εξερεύνηση της ιδιωτικότητας στο blockchain, παρουσιάζοντας μια ισορροπημένη άποψη των ευκαιριών και των προκλήσεων που παρουσιάζει αυτή η καινοτόμος τεχνολογία.

Περιεχόμενα

Εισαγωγή

Η έλευση της τεχνολογίας blockchain έχει φέρει αλλαγές σε διάφορους τομείς αφού παρέχει μια αποκεντρωμένη, διαφανή και ασφαλή πλατφόρμα για τη διεξαγωγή συναλλαγών και την αποθήκευση δεδομένων. Ένα από τα πιο σημαντικά χαρακτηριστικά του blockchain είναι η ικανότητά του να διατηρεί ένα διαφανές και αμετάβλητο αρχείο συναλλαγών που πραγματοποιούνται εντός του δικτύου. Ενώ το χαρακτηριστικό αυτό έχει επαινεθεί από πολλούς ως μια καινοτόμος ανακάλυψη, οι επιπτώσεις μιας τέτοιας δυνατότητας στον κλάδο της ιδιωτικότητας έχουν πυροδοτήσει συζητήσεις μεταξύ των ειδικών, των «παικτών» του κλάδου και των τελικών χρηστών.

Η βασική ιδέα του blockchain βασίζεται σε τεχνολογία «Distributed ledger (DLT)», όπου τα δεδομένα μοιράζονται και αναπαράγονται σε πολλούς κόμβους μέσα σε ένα δίκτυο. Αυτό διασφαλίζει την ακεραιότητα και την ανθεκτικότητα των αποθηκευμένων δεδομένων, καθιστώντας πρακτικά αδύνατο να παραβιαστούν. Ωστόσο, ένας απαραίτητος συμβιβασμός είναι ότι οποιοσδήποτε μπορεί να έχει πρόσβαση σε αυτά τα διαφανή αρχεία, εκθέτοντας ευαίσθητες πληροφορίες και διακυβεύοντας το απόρρητο των χρηστών. Αυτό το θέμα έχει προσελκύσει ευρεία προσοχή, ιδιαίτερα τα τελευταία χρόνια καθώς η τεχνολογία blockchain συνεχίζει να χρησιμοποιήται σε όλο και περισσότερες βιομηχανίες και εφαρμογές, που κυμαίνονται από τη χρηματοδότηση και τη διαχείριση της εφοδιαστικής αλυσίδας έως την υγειονομική περίθαλψη και τα συστήματα ψηφοφορίας.

Για να αντιμετωπιστούν οι ανησυχίες σχετικά με το απόρρητο στο blockchain, έχουν προταθεί και εφαρμοστεί διάφορες προσεγγίσεις και τεχνικές, καθεμία με το δικό της σύνολο πλεονεκτημάτων και περιορισμών. Η παρούσα εργασία έχει ως στόχο την παροχή μιας ολοκληρωμένης συγκριτικής ανάλυσης αυτών των διαφορετικών μεθοδολογιών, εστιάζοντας στην ικανότητά τους να επιτύχουν μια

ισορροπία μεταξύ της ανάγκης για διαφάνεια και της διατήρησης της ιδιωτικής ζωής.

Η σημασία της αντιμετώπισης των ζητημάτων ιδιωτικότητας στην τεχνολογία blockchain είναι κρίσιμη, καθώς διαδραματίζει θεμελιώδη ρόλο στην ευρεία υιοθέτηση και τη μακροπρόθεσμη επιτυχία αυτής της καινοτόμου τεχνολογίας. Καθώς το blockchain συνεχίζει να αποκτά έδαφος σε διάφορους τομείς, η ικανότητά του να διατηρεί μια λεπτή ισορροπία μεταξύ διαφάνειας και ιδιωτικότητας θα είναι καθοριστική στη δημιουργία εμπιστοσύνης μεταξύ των χρηστών και την εξασφάλιση της συμμόρφωσης ως προς τους κανονισμούς ιδιωτικότητας. Αυτό είναι ιδιαίτερα σημαντικό σε βιομηχανίες όπου ευαίσθητες πληροφορίες ανταλλάσσονται τακτικά, όπως οικονομικές υπηρεσίες, υγεία και κρατικές υπηρεσίες. Η μη αντιμετώπιση των ζητημάτων ιδιωτικότητας μπορεί να υπονομεύσει όχι μόνο τα πιθανά οφέλη της τεχνολογίας, αλλά και να εκθέσει τους χρήστες σε κινδύνους, όπως κλοπή ταυτότητας, απάτη και παραβίαση δεδομένων, που θα μπορούσε να εμποδίσει την ανάπτυξη και την ευρεία υιοθέτηση των λύσεων βασισμένων σε blockchain.

Τελικά, στόχος αυτής της εργασίας είναι να ρίξει φως στην περίπλοκη δυναμική του απορρήτου στα δίκτυα blockchain και να συμβάλει στη συνεχή συζήτηση γύρω από την ανάπτυξη ισχυρών, ασφαλών συστημάτων που βασίζονται σε blockchain που διατηρούν την ιδιωτικότητα. Παρουσιάζοντας μια διεξοδική συγκριτική ανάλυση, επιδιώκει την παροχή πολύτιμων γνώσεων για επαγγελματίες, ερευνητές και υπεύθυνους χάραξης πολιτικών, καθώς περιηγούνται στο ταχέως εξελισσόμενο περιβάλλον της τεχνολογίας blockchain και καθώς προσπαθούν να επιτύχουν τη λεπτή ισορροπία μεταξύ διαφάνειας, ασφάλειας και ιδιωτικότητας.

Blockchain and privacy protection

(Αλυσίδες μπλοκ και προστασία της ιδιωτικής ζωης)

Private and Public keys

Η χρήση ιδιωτικών και δημόσιων κλειδιών αποτελεί κρίσιμο στοιχείο της ιδιωτικότητας στα blockchain . Η ασύμμετρη κρυπτογραφία χρησιμοποιείται από τα συστήματα blockchain για τη διασφάλιση των συναλλαγών μεταξύ χρηστών. Κάθε χρήστης σε αυτά τα συστήματα διαθέτει ένα δημόσιο κλειδί και ένα ιδιωτικό κλειδί, τα οποία κλειδιά είναι τυχαίες σειρές αριθμών και συνδέονται κτυπτογραφικά. Τα κλειδιά αυτά συνδέονται κρυπτογραφικά και αποτελούνται από τυχαίους αριθμούς. (Contributors, 2023)

Δεδομένου ότι τα δημόσια κλειδιά δεν αποκαλύπτουν προσωπικές πληροφορίες, μπορούν να μοιραστούν με άλλους χρήστες του δικτύου. Χρησιμοποιώντας μια συνάρτηση κατακερματισμού, η διεύθυνση κάθε χρήστη δημιουργείται από το δημόσιο κλειδί. Αυτές οι διευθύνσεις χρησιμοποιούνται για τη μεταφορά και τη λήψη κρυπτονομισμάτων και άλλων περιουσιακών στοιχείων που βασίζονται στην αλυσίδα μπλοκ. Οι χρήστες μπορούν να εξετάσουν προηγούμενες συναλλαγές και δραστηριότητες που έχουν λάβει χώρα στο blockchain, δεδομένου ότι τα δίκτυα blockchain είναι κοινά για όλα τα μέλη. (Contributors, 2023)

Το ιδιωτικό κλειδί είναι αυτό που παρέχει σε έναν χρήστη κρυπτονομισμάτων την κυριότητα των κεφαλαίων σε μια συγκεκριμένη διεύθυνση. Το πορτοφόλι δημιουργεί και αποθηκεύει αυτόματα ιδιωτικά κλειδιά για τους χρήστης. Όταν στέλνει από ένα πορτοφόλι Blockchain, το λογισμικό υπογράφει τη συναλλαγή με το ιδιωτικό του κλειδί (χωρίς στην πραγματικότητα να το αποκαλύπτει), το οποίο υποδεικνύει σε ολόκληρο το δίκτυο ότι έχετε την εξουσία να μεταφέρετε τα κεφάλαια στη διεύθυνση από την οποία στέλνετε. (Blockchain.com, 2023)

Η ασφάλεια και η εγκυρότητα των συναλλαγών διασφαλίζονται με τη χρήση κρυπτογραφικών τεχνικών σε συνδυασμό με αυτά τα δημόσια και ιδιωτικά κλειδιά. Αυτό γίνεται έτσι ώστε, ακόμη και όταν μια συναλλαγή καταγράφεται στην αλυσίδα μπλοκ, να μην μπορεί να αλλάξει ή να παρέμβει χωρίς το αντίστοιχο ιδιωτικό κλειδί. Επιπλέον, με την ενεργοποίηση των ψηφιακών υπογραφών στις συναλλαγές blockchain ενισχύεται περαιτέρω την ασφάλεια και η ακεραιότητα των blockchain, αφού εγγυάται ότι μόνο εξουσιοδοτημένα μέρη μπορούν να πραγματοποιήσουν συναλλαγές. (Contributors, 2023)

Peer to peer

Μία από τις θεμελιώδεις πτυχές της τεχνολογίας blockchain είναι το δίκτυο Peer-to-Peer (P2P). Τα δίκτυα P2P αποτελούν αναπόσπαστο κομμάτι της λειτουργίας της τεχνολογίας blockchain, παρέχοντας την υποδομή που επιτρέπει την απευθείας κοινή χρήση δεδομένων μεταξύ συστημάτων χωρίς την ανάγκη κεντρικού διακομιστή. Αυτή η ενότητα θα εμβαθύνει στις περιπλοκές των δικτύων P2P, στον ρόλο τους στην τεχνολογία blockchain και στις επιπτώσεις που έχουν στην ιδιωτικότητα. (Finstocklearn.) (Council.)

Τα δίκτυα P2P είναι αποκεντρωμένα δίκτυα όπου κάθε κόμβος, ή «Peer», ενεργεί και ως πελάτης και ως διακομιστής, μοιράζοντας πόρους απευθείας με άλλους Peers χωρίς την ανάγκη κεντρικού διακομιστή ή αρχής. Αυτό έρχεται σε αντίθεση με τα παραδοσιακά μοντέλα πελάτη-διακομιστή όπου ένας κεντρικός διακομιστής παρέχει πόρους σε συνδεδεμένους πελάτες. Σε ένα δίκτυο P2P, κάθε κόμβος (peer) είναι ίσος και όλοι οι κόμβοι συνεισφέρουν στο δίκτυο μοιράζοντας τους πόρους τους, όπως το εύρος ζώνης, τον αποθηκευτικό χώρο και την υπολογιστική ισχύ. (Finstocklearn.)

Στο πλαίσιο της τεχνολογίας blockchain, τα δίκτυα P2P αποτελούν τη ραχοκοκαλιά του συστήματος. Κάθε κόμβος στο δίκτυο διατηρεί ένα αντίγραφο ολόκληρου του blockchain, διασφαλίζοντας ότι τα δεδομένα είναι πάντα διαθέσιμα και ανθεκτικά στη λογοκρισία. Όταν πραγματοποιείται μια συναλλαγή, μεταδίδεται σε ολόκληρο το δίκτυο και κάθε κόμβος επαληθεύει ανεξάρτητα τη συναλλαγή. Μόλις επαληθευτεί, η συναλλαγή προστίθεται στο blockchain και το ενημερωμένο blockchain μοιράζεται με όλους τους άλλους κόμβους. Αυτή η διαδικασία διασφαλίζει την ακεραιότητα και τη διαφάνεια του συστήματος, καθώς όλες οι συναλλαγές είναι δημόσια επαληθεύσιμες και δεν μπορούν να τροποποιηθούν μόλις προστεθούν στο blockchain.
(Finstocklearn.) (Council.)

Η αποκεντρωμένη φύση των δικτύων P2P φέρνει αρκετά πλεονεκτήματα στην τεχνολογία blockchain. Πρώτον, ενισχύει την ασφάλεια. Σε ένα κεντρικό σύστημα, ένα μόνο σημείο αστοχίας μπορεί να οδηγήσει σε κατάρρευση ολόκληρου του συστήματος. Ωστόσο, σε ένα δίκτυο P2P, τα δεδομένα κατανέμονται σε πολλούς κόμβους, καθιστώντας το ανθεκτικό σε μεμονωμένα σημεία αστοχίας. Ακόμα κι αν ένας κόμβος παραβιαστεί, το δίκτυο συνεχίζει να λειτουργεί, διασφαλίζοντας την ακεραιότητα και τη διαθεσιμότητα των δεδομένων. (Finstocklearn.)

Δεύτερον, τα δίκτυα P2P προάγουν τη διαφάνεια και την εμπιστοσύνη. Σε ένα δίκτυο P2P που βασίζεται σε blockchain, όλες οι συναλλαγές είναι ορατές σε όλους τους συμμετέχοντες στο δίκτυο, διασφαλίζοντας τη διαφάνεια. Αυτή η διαφάνεια δημιουργεί εμπιστοσύνη μεταξύ των συμμετεχόντων στο δίκτυο, καθώς όλες οι συναλλαγές είναι ανοιχτές για επαλήθευση από οποιονδήποτε συμμετέχοντα. (Council.)

Τρίτον, τα δίκτυα P2P στην τεχνολογία blockchain επιτρέπουν την άμεση αλληλεπίδραση μεταξύ των συμμετεχόντων, εξαλείφοντας την ανάγκη για μεσάζοντες. Αυτή η άμεση αλληλεπίδραση μπορεί να οδηγήσει σε ταχύτερες συναλλαγές και χαμηλότερο κόστος, ιδιαίτερα σε τομείς όπως ο χρηματοοικονομικός τομέας όπου οι μεσάζοντες συχνά επιβραδύνουν τις συναλλαγές και αυξάνουν το κόστος. (Finstocklearn.)

Παρά αυτά τα πλεονεκτήματα, τα δίκτυα P2P στην τεχνολογία blockchain αντιμετωπίζουν επίσης προκλήσεις. Μία από τις κύριες προκλήσεις είναι η διατήρηση της ιδιωτικότητας. Ενώ η διαφάνεια είναι ένα βασικό χαρακτηριστικό της τεχνολογίας blockchain, μπορεί επίσης να οδηγήσει σε ανησυχίες σχετικά με την ιδιωτικότητα, καθώς ευαίσθητες πληροφορίες μπορούν να εκτεθούν σε όλους τους συμμετέχοντες στο δίκτυο (Council.).

Διάφορες προσεγγίσεις και τεχνικές έχουν προταθεί για την αντιμετώπιση αυτού του ζητήματος, όπως Zero knowledge Proofs και Ring Signatures, οι οποίες στοχεύουν στη διατήρηση της ιδιωτικής ζωής διασφαλίζοντας παράλληλα τη διαφάνεια. (Cointelegraph.)

Μια άλλη πρόκληση είναι η επεκτασιμότητα. Καθώς αυξάνεται ο αριθμός των συμμετεχόντων σε ένα δίκτυο P2P, αυξάνεται και ο όγκος των δεδομένων που πρέπει να επεξεργαστεί και να αποθηκευτεί από κάθε κόμβο. Αυτό μπορεί να οδηγήσει σε ζητήματα απόδοσης, όπως πιο αργούς χρόνους συναλλαγών και αυξημένες απαιτήσεις αποθήκευσης. (Finstocklearn.)

Παρά αυτές τις εξελίξεις, η ιδιωτικότητα στα δίκτυα P2P παραμένει ένα περίπλοκο και προκλητικό ζήτημα. Καθώς η τεχνολογία blockchain συνεχίζει να εξελίσσεται και να βρίσκει νέες εφαρμογές, η ανάγκη για ισχυρές, ασφαλείς λύσεις και λύσεις που διατηρούν το απόρρητο θα γίνει πιο κρίσιμη. Είναι σημαντικό για τους ερευνητές, τους επαγγελματίες και τους υπεύθυνους χάραξης πολιτικής να συνεχίσουν να εξερευνούν και να αναπτύσσουν νέες μεθοδολογίες για την αντιμετώπιση αυτών των προκλήσεων.

Cryptographic methods for Privacy using Blockchains

(Κρυπτογραφικές μέθοδοι για την ιδιωτικότητα με χρήση Αλυσίδων Μπλοκ)

Zero-Knowledge Proofs in block chain privacy

1. **Πως οι Zero-Knowledge proofs ενισχύουν την ιδιωτικότητα σε ένα blockchain;**

Μέσω της χρήσης μιας κρυπτογραφικής τεχνικής που ονομάζεται απόδειξη μηδενικής γνώσης (ZKP), ένα μέρος - ο ελεγκτής - μπορεί να πείσει ένα άλλο μέρος - τον επαληθευτή - ότι μια δεδομένη δήλωση είναι αληθής χωρίς να αποκαλύπτει οποιαδήποτε πληροφορία σχετικά με τη δήλωση εκτός από την αλήθεια της. Η τεχνολογία blockchain μπορεί να χρησιμοποιήσει ZKPs για να βελτιώσει την ιδιωτικότητα και να επιτύχει μια σειρά από πλεονεκτήματα, συμπεριλαμβανομένων των ιδιωτικών συναλλαγών και της ασφαλούς πιστοποίησης ταυτότητας.

Μερικοί από τους τρόπους με τους οποίους το επιτυγχάνει είναι οι εξής:

i. Ασφαλής έλεγχος ταυτότητας: Πιθανές παραβιάσεις της ασφάλειας μπορούν να αποφευχθούν με τη χρήση ZKPs με την αυθεντικοποίηση χρηστών χωρίς να αποκαλύπτονται τα διαπιστευτήριά τους ή τα ιδιωτικά κλειδιά τους. Οι χρήστες μπορούν να αποδείξουν ότι διαθέτουν τα απαραίτητα διαπιστευτήρια χρησιμοποιώντας ZKPs χωρίς να τα αποκαλύπτουν, μειώνοντας τον κίνδυνο επιθέσεων που στοχεύουν σε πληροφορίες ή πρόσβαση χρηστών.

ii. Layer 2 Scaling: Οι ZKP μπορούν επίσης να εφαρμοστούν σε δίκτυα blockchain για να αυξήσουν την επεκτασιμότητα. Οι αποδείξεις μηδενικής γνώσης χρησιμοποιούνται από λύσεις Layer 2 Scaling, όπως οι ZK-Rollups, για να συνδυάσουν διάφορες συναλλαγές σε μια ενιαία απόδειξη που μπορεί να επικυρωθεί στην κύρια αλυσίδα. Αυτό διατηρεί το απόρρητο των συναλλαγών ενώ ελαφρύνει την πίεση στην κύρια αλυσίδα.

iii. Privacy-preserving Smart Contracts: Οι ZKPs μπορούν να χρησιμοποιηθούν για τη δημιουργία έξυπνων συμβολαίων που διατηρούν την ιδιωτικότητα στο πλαίσιο του Ethereum και άλλων πλατφορμών για έξυπνα συμβόλαια. Ενώ εξακολουθούν να

επιτρέπουν την επικύρωση της εκτέλεσης του συμβολαίου, τα ZKPs επιτρέπουν την εμπιστευτικότητα της εκτέλεσης και της κατάστασης ενός έξυπνου συμβολαίου. Στις αποκεντρωμένες εφαρμογές που βασίζονται σε πλατφόρμες blockchain, αυτό βελτιώνει την ιδιωτικότητα, επειδή οι ευαίσθητες πληροφορίες μπορούν να υποβάλλονται σε ασφαλή επεξεργασία χωρίς να αποκαλύπτονται. (Ethereum, 2023)

2. Τρόποι αποτροπής πιθανών επιθέσεων με την χρήση Zero-Knowledge Proofs

' Η χρήση Zero-Knowledge Proofs (ZKPs) μπορεί να βελτιώσει αρκετά την ιδιωτικότητα μέσα σε ένα blockchain με άφθονους τρόπους. Ένα από αυτούς είναι το λεγόμενο Anonymous payments το οποίο λειτουργεί ως εξής.

Ο σκοπός των κρυπτονομισμάτων ήταν να δώσουν στους καταναλωτές έναν τρόπο να πραγματοποιούν ανώνυμες, ομότιμες συναλλαγές. Ωστόσο, η πλειονότητα των συναλλαγών κρυπτονομισμάτων είναι εύκολα προσβάσιμες σε ανοικτές αλυσίδες μπλοκ. Οι ταυτότητες των χρηστών είναι συχνά ψευδώνυμες και μπορούν να συνδεθούν με τις ταυτότητες του πραγματικού κόσμου μέσω απλής ανάλυσης δεδομένων εντός και εκτός αλυσίδας, ή μπορούν να συνδεθούν σκόπιμα με αυτές (για παράδειγμα, τοποθετώντας διευθύνσεις ETH στα προφίλ του Twitter ή του GitHub).

Τα δίκτυα blockchain που εστιάζουν στην ιδιωτικότητα επιτρέπουν στους κόμβους να επικυρώνουν τις συναλλαγές χωρίς να απαιτείται πρόσβαση στα δεδομένα των συναλλαγών, ενσωματώνοντας τεχνολογίες μηδενικής γνώσης στο πρωτόκολλο.Οι συναλλαγές σε ανοικτές αλυσίδες μπλοκ γίνονται επίσης ανώνυμες μέσω αποδείξεων μηδενικής γνώσης. Ως παράδειγμα χρησιμεύει το Tornado Cash, ένα αποκεντρωμένο, μη εμπιστευτικό εργαλείο που επιτρέπει στους χρήστες να πραγματοποιούν ιδιωτικές συναλλαγές στο Ethereum. Για να διασφαλίσει το οικονομικό απόρρητο και να αποκρύψει τις λεπτομέρειες των συναλλαγών, το Tornado Cash χρησιμοποιεί αποδείξεις μηδενικής γνώσης. Δυστυχώς, επειδή αυτά τα εργαλεία ιδιωτικότητας απαιτούν χρήση "opt-in", συνδέονται με παράνομες δραστηριότητες. Για να παρακαμφθεί αυτό, η ιδιωτικότητα πρέπει τελικά να αποκτήσει προτεραιότητα στις ανοικτές αλυσίδες μπλοκ.

Ένας ακόμη τρόπος είναι μέσω του Identity protection, το οποίο δίνει την δυνατότητα διαχείρισης της πρόσβασης στα προσωπικά αναγνωριστικά (Identifications). Η απόδειξη της ιθαγένειάς σας χωρίς να αποκαλύπτετε τα στοιχεία του φορολογικού σας

μητρώου ή του διαβατηρίου σας είναι ένα καλό παράδειγμα για το πώς η τεχνολογία μηδενικής γνώσης επιτρέπει την αποκεντρωμένη ταυτότητα (Ethereum, 2023)

3. Παραδείγματα blockchain που χρησιμοποιούν Zero-Knowledge Proofs

Οι αποδείξεις μηδενικής γνώσης (ZKP) έχουν αναπτυχθεί σε διάφορες πλατφόρμες blockchain για τη βελτίωση της ιδιωτικότητας, της ασφάλειας και της επεκτασιμότητας. Μερικά παραδείγματα είναι τα εξής:

i. Zcash (ZEC):

Το Zcash είναι ένα κρυπτονόμισμα με σχεδιασμό που εστιάζει στην προστασία της ιδιωτικής ζωής και χρησιμοποιεί zk-SNARKs (zero-knowledge succinct non-interactive argument of knowledge), ένα συγκεκριμένο είδος ZKP, για την επίτευξη μυστικών συναλλαγών. Οι διαφανείς συναλλαγές στο Zcash είναι συγκρίσιμες με εκείνες του Bitcoin, αλλά οι θωρακισμένες συναλλαγές χρησιμοποιούν τα zk-SNARKs για να αποκρύψουν τις πληροφορίες της συναλλαγής, συμπεριλαμβανομένων του αποστολέα, του παραλήπτη και του ποσού, διατηρώντας παράλληλα την επικύρωση της συναλλαγής.

ii. Ethereum (ETH):

Οι ZKPs ερευνώνται και υλοποιούνται ενεργά από το Ethereum, μια πλατφόρμα blockchain γενικής χρήσης, για μια ποικιλία εφαρμογών, συμπεριλαμβανομένων των έξυπνων συμβολαίων που διατηρούν την ιδιωτικότητα και των λύσεων κλιμάκωσης επιπέδου 2, όπως οι ZK-Rollups. Παρόλο που τα ZKPs δεν έχουν ακόμη ενσωματωθεί στο βασικό στρώμα του Ethereum, οι προγραμματιστές μπορούν να χρησιμοποιήσουν τα ZKPs για να δημιουργήσουν αποκεντρωμένες εφαρμογές που εστιάζουν στην κλιμάκωση και την προστασία της ιδιωτικής ζωής πάνω στο Ethereum. (Ethereum, 2023)

Ring Signatures

Οι υπογραφές δακτυλίου είναι ένα ισχυρό κρυπτογραφικό εργαλείο που παρέχει μια μέθοδο για την επαλήθευση της αυθεντικότητας ενός ψηφιακού μηνύματος ή εγγράφου με τρόπο υπολογιστικά και λογικά ασφαλή. Είναι ένας τύπος ψηφιακής υπογραφής που μπορεί να εκτελεστεί από οποιοδήποτε μέλος μιας ομάδας χρηστών που ο καθένας έχει κλειδιά. Ένα μήνυμα

υπογεγραμμένο με υπογραφή δακτυλίου υποστηρίζεται από κάποιον σε μια συγκεκριμένη ομάδα ανθρώπων, αλλά δεν αποκαλύπτει ποιος ήταν ο πραγματικός υπογράφων. (Rivest, 2001) (Monero)

Η έννοια των ring signatures εισήχθη για πρώτη φορά από τους Rivest, Shamir και Tauman το 2001, παρέχοντας έναν νέο τύπο ψηφιακής υπογραφής που όχι μόνο δεν είναι πλαστός αλλά προσφέρει επίσης μια ισχυρή μορφή ανωνυμίας (Rivest, 2001) (Anderson, 2018). Το όνομα "ring signature" προέρχεται από τη δακτυλιοειδή δομή του αλγορίθμου υπογραφής, όπου οι πιθανοί υπογράφοντες μετατίθενται κυκλικά και κάθε υπογράφον εκτελεί μια λειτουργία που εξαρτάται από το αποτέλεσμα του προηγούμενου υπογράφοντος. Αυτή η δομή διασφαλίζει ότι κανείς δεν μπορεί να καθορίσει ποιος από τους πιθανούς υπογράφοντες στο δακτυλίδι παρήγαγε την υπογραφή. (Anderson, 2018)

Οι υπογραφές δακτυλίου έχουν βρει πολλές εφαρμογές σε διάφορους τομείς, ιδιαίτερα σε σενάρια όπου η ανωνυμία είναι υψίστης σημασίας. Για παράδειγμα, χρησιμοποιούνται στην καταγγελία, όπου ένας υπάλληλος σε έναν μεγάλο οργανισμό χρειάζεται να διαρρεύσει ορισμένες μυστικές πληροφορίες χωρίς να αποκαλύψει την ταυτότητά του. Ο πληροφοριοδότης μπορεί να χρησιμοποιήσει μια υπογραφή δακτυλιδιού για να υπογράψει το έγγραφο, συμπεριλαμβανομένων των δημόσιων κλειδιών άλλων υπαλλήλων στο δακτυλίδι. Με αυτόν τον τρόπο, οποιοσδήποτε μπορεί να επαληθεύσει ότι το έγγραφο υπογράφηκε από κάποιον από τους αποστολείς, αλλά δεν μπορεί να αποδείξει ποιος. (Monero) (Anderson, 2018)

Μια άλλη εφαρμογή είναι στην ηλεκτρονική ψηφοφορία. Μια ψήφος μπορεί να είναι μια δακτυλική υπογραφή με το δακτυλίδι των δικαιούχων ψηφοφόρων, επιτρέποντας τη δημόσια καταμέτρηση των ψήφων χωρίς να αποκαλύπτονται μεμονωμένες επιλογές ψηφοφορίας. Για να αποφευχθεί η

διπλή ψηφοφορία, μια ιδιότητα συνδεσιμότητας μπορεί να προστεθεί στο βασικό σχήμα υπογραφής δακτυλίου. (Monero) (Anderson, 2018)

Το αρχικό σχήμα υπογραφής δακτυλίου χρησιμοποιούσε κρυπτογράφηση δημόσιου κλειδιού για να επιτύχει την ανωνυμία και την έλλειψη πλαστογραφίας. Αυτή η ευελιξία επεκτάθηκε σε μεταγενέστερες εργασίες, όπου αποδείχθηκε ότι τα σχήματα υπογραφής δακτυλίου θα μπορούσαν να βασίζονται σε δημόσια κλειδιά κρυπτογράφησης ακόμα κι αν τα κλειδιά δεν είναι όλα του ίδιου τύπου. Ωστόσο, αυτά τα σχήματα βασίστηκαν σε τυχαίους χρησμούς, μια θεωρητική κατασκευή που αντικαταστάθηκε από μια συνάρτηση κατακερματισμού στην πράξη. Αυτή η εξάρτηση θεωρήθηκε ως μειονέκτημα, καθώς αποδείχθηκε ότι το τυχαίο μοντέλο “oracle” δεν είναι ασφαλές. Αυτό οδήγησε στην ανάπτυξη σχημάτων δακτυλιδιών υπογραφών χωρίς τυχαίους χρησμούς (oracles). (Anderson, 2018) (Bender, 2006)

Εκτός από την ανάπτυξη ενός σχήματος υπογραφής δακτυλίου που δεν χρησιμοποιεί τυχαίους χρησμούς, προτάθηκαν οι ισχυρότερες απαιτήσεις ασφαλείας για ανωνυμία και έλλειψη πλαστογραφησιμότητας και αποδείχθηκε ότι το σχήμα τους πληροί αυτές τις απαιτήσεις. Οι δύο ισχυρότερες απαιτήσεις ανωνυμίας που προτείνονται είναι η ανωνυμία έναντι των επιθέσεων απόδοσης και η ανωνυμία έναντι της πλήρους έκθεσης κλειδιού. Η πρώτη από αυτές τις απαιτήσεις εγγυάται την ανωνυμία ακόμα κι αν δοθούν στον αντίπαλο τα μυστικά κλειδιά για όλους εκτός από έναν από τους πιθανούς υπογράφοντες στο ρινγκ. Η ανωνυμία έναντι της πλήρους έκθεσης του κλειδιού είναι η ισχυρότερη από τις δύο απαιτήσεις, που εγγυάται την ανωνυμία ακόμα κι αν ο αντίπαλος γνωρίζει τα μυστικά κλειδιά για όλα τα μέλη του δακτυλίου. (Anderson, 2018) (Fujisaki, 2007)

Ενώ το σχήμα που παρουσιάζεται πληροί την ασθενέστερη από αυτές τις δύο απαιτήσεις, προτάθηκε μια παραλλαγή του σχήματός τους που πληροί την ισχυρότερη απαίτηση. Αυτή η παραλλαγή περιλαμβάνει τη δημιουργία

κλειδιών κρυπτογράφησης από τους χρήστες για τα οποία οι ίδιοι δεν γνωρίζουν καν το μυστικό κλειδί. Ωστόσο, αυτή η παραλλαγή δεν συνάδει με την ad-hoc φύση των υπογραφών δακτυλίου, επειδή οι άλλοι χρήστες που περιλαμβάνονται στο δαχτυλίδι μπορεί να γνωρίζουν πραγματικά τα δικά τους μυστικά κλειδιά και επομένως ο πραγματικός υπογράφων μπορεί να διακριθεί από τα άλλα μέλη του δαχτυλιδιού με το να είναι ο μόνος μέλος που δεν μπορεί να παράγει το μυστικό κλειδί του. (Fujisaki, 2007) (Bender, 2006)

Προκειμένου οι υπογραφές του δαχτυλιδιού να είναι αρνητικές, όλα τα κλειδιά που χρησιμοποιούνται από τον υπογράφοντα πρέπει να μην διακρίνονται από τα κλειδιά των άλλων μελών του δαχτυλιδιού, ακόμη και στην περίπτωση που ο υπογράφων εξαναγκάζεται να αποκαλύψει το μυστικό του κλειδί. Αυτή είναι μια ισχυρή απαίτηση και δεν ικανοποιείται από πολλά υπάρχοντα σχήματα ring signature. Ωστόσο, είναι μια σημαντική ιδιότητα για ορισμένες εφαρμογές, όπως το whistleblowing, όπου ο υπογράφων μπορεί να εξαναγκαστεί να αποκαλύψει το μυστικό κλειδί του. (Fujisaki, 2007) (Bender, 2006)

Μία από τις πιο αξιοσημείωτες υλοποιήσεις ring signatures είναι στο κρυπτονόμισμα Monero. Το Monero χρησιμοποιεί υπογραφές δακτυλίου για να παρέχει το απόρρητο των συναλλαγών κρύβοντας την ταυτότητα του αποστολέα μεταξύ μιας ομάδας πιθανών αποστολέων. Σε μια συναλλαγή Monero, το δημόσιο κλειδί του πραγματικού αποστολέα αναμιγνύεται με δημόσια κλειδιά από προηγούμενες συναλλαγές στο blockchain. Αυτό δημιουργεί έναν δακτύλιο πιθανών αποστολέων, αποκρύπτοντας την πραγματική προέλευση της συναλλαγής. Η υπογραφή αποδεικνύει ότι ένα από τα δημόσια κλειδιά στο δαχτυλίδι είναι ο πραγματικός αποστολέας, αλλά δεν αποκαλύπτει ποιο. (Monero)

Η υλοποίηση υπογραφών δακτυλίου από το Monero περιλαμβάνει επίσης ένα χαρακτηριστικό που ονομάζεται RingCT (Ring εμπιστευτικών

συναλλαγών), το οποίο κρύβει το ποσό της συναλλαγής εκτός από την ταυτότητα του αποστολέα. Αυτό ενισχύει περαιτέρω το απόρρητο καθιστώντας δύσκολη την ανίχνευση συναλλαγών ή την ανάλυση του γραφήματος συναλλαγών. (Monero)

Ωστόσο, ενώ οι υπογραφές δακτυλίου παρέχουν ισχυρές εγγυήσεις απορρήτου, συνοδεύονται επίσης από ορισμένους συμβιβασμούς. Ένα από τα κύρια μειονεκτήματα είναι το μέγεθος των υπογραφών. Καθώς το μέγεθος του δακτυλιδιού (δηλαδή, ο αριθμός των πιθανών υπογράφων) αυξάνεται, το μέγεθος της υπογραφής αυξάνεται επίσης. Αυτό μπορεί να οδηγήσει σε προβλήματα επεκτασιμότητας, ειδικά σε συστήματα όπως τα blockchains όπου η αποθήκευση δεδομένων είναι κρίσιμος παράγοντας. Για παράδειγμα, στο Monero, οι υπογραφές δακτυλίου αποτελούν σημαντικό μέρος του μεγέθους της συναλλαγής, οδηγώντας σε μεγαλύτερο μέγεθος blockchain σε σύγκριση με άλλα κρυπτονομίσματα. (Monero)

Μια άλλη πρόκληση είναι το υπολογιστικό κόστος. Η δημιουργία και η επαλήθευση υπογραφών δακτυλίου απαιτούν περισσότερους υπολογιστικούς πόρους καθώς αυξάνεται το μέγεθος του δακτυλίου. Αυτό μπορεί να επιβραδύνει την επεξεργασία των συναλλαγών και να περιορίσει τη συνολική απόδοση του συστήματος. (Monero)

Παρά τις προκλήσεις αυτές, οι υπογραφές δακτυλίου παραμένουν ένα ισχυρό εργαλείο για τη διασφάλιση του απορρήτου στις ψηφιακές επικοινωνίες και συναλλαγές. Προσφέρουν ένα μοναδικό μείγμα ανωνυμίας και αυθεντικότητας, επιτρέποντας στους χρήστες να αποδείξουν την προέλευση ενός μηνύματος χωρίς να αποκαλύπτουν την ταυτότητά τους. Αυτό τα καθιστά ιδιαίτερα χρήσιμα σε σενάρια όπου το απόρρητο είναι πρωταρχικής σημασίας, όπως σε συστήματα εμπιστευτικής ψηφοφορίας, ανώνυμα κρυπτονομίσματα και ασφαλείς πλατφόρμες καταγγελίας. (Monero) (Anderson, 2018)

Συμπερασματικά, οι υπογραφές δακτυλίου αντιπροσωπεύουν μια σημαντική πρόοδο στον τομέα της κρυπτογραφίας, παρέχοντας έναν ισχυρό μηχανισμό για τη διασφάλιση της ιδιωτικότητας και της αυθεντικότητας στις ψηφιακές επικοινωνίες. Ενώ συνοδεύονται από ορισμένους συμβιβασμούς, όπως αυξημένες απαιτήσεις υπολογισμού και αποθήκευσης, τα οφέλη τους όσον αφορά την παροχή ισχυρών εγγυήσεων ανωνυμίας τα καθιστούν ένα ανεκτίμητο εργαλείο σε διάφορες εφαρμογές. Καθώς ο ψηφιακός κόσμος συνεχίζει να εξελίσσεται και το απόρρητο γίνεται όλο και πιο σημαντικό μέλημα, ο ρόλος των υπογραφών δακτυλίου και παρόμοιων κρυπτογραφικών τεχνικών είναι πιθανό να γίνει ακόμη πιο κρίσιμος. (Anderson, 2018) (Bender, 2006) (Fujisaki, 2007) (Monero) (Rivest, 2001)

Stealth address in block chain privacy

Ορισμένα συστήματα κρυπτονομισμάτων χρησιμοποιούν κρυφές διευθύνσεις, μια τεχνολογία που βελτιώνει την ιδιωτικότητα και συμβάλλει στην προστασία της ιδιωτικής ζωής των χρηστών, αποκρύπτοντας τη διεύθυνση του παραλήπτη. Χρησιμοποιούνται κυρίως σε κρυπτονομίσματα με έμφαση στην προστασία της ιδιωτικής ζωής, όπως το Monero (XMR), αλλά μπορούν επίσης να χρησιμοποιηθούν σε άλλα δίκτυα blockchain.

Ο αποστολέας δημιουργεί μια μοναδική δημόσια διεύθυνση που ονομάζεται " stealth address" για κάθε συναλλαγή, ώστε να κρατάει μυστική τη διεύθυνση του πραγματικού παραλήπτη. Αυτό ενισχύει την ανωνυμία του παραλήπτη καθιστώντας δύσκολο για τους εξωτερικούς παρατηρητές να συνδέσουν τις συναλλαγές με έναν μόνο παραλήπτη.

1. Πλεονεκτήματα των Stealth Address

Αν και δεν είναι η μόνη μέθοδος προστασίας της ιδιωτικής ζωής, η χρήση μιας μυστικής διεύθυνσης είναι ανώτερη από άλλες. Το Coinjoin, το οποίο ομαδοποιεί τις συναλλαγές με άλλους χρήστες, είναι ένα λανθασμένο παράδειγμα. Η εύρεση ενός άλλου κατόχου Bitcoin για μια κοινή συναλλαγή είναι απαραίτητη για αυτή την προσέγγιση, η οποία περιορίζεται στο Bitcoin.

Οι μυστικές διευθύνσεις θα μπορούσαν να επιτρέψουν την προστασία της ιδιωτικής ζωής σε διάφορες περιπτώσεις χρήσης, όπως οι συναλλαγές με NFTs, POAPs (ψηφιακά

συλλεκτικά αντικείμενα που κατασκευάζονται μέσω του πρωτοκόλλου name-brand) και ENS domains. Ο Vitalik Buterin εξηγεί: "Για παράδειγμα, αν ο Bob θέλει να λαμβάνει POAPs, τότε ο Bob θα μπορούσε να δώσει στο POAP πορτοφόλι του (ή ακόμα και σε ένα όχι πολύ ασφαλές web interface) το κλειδί προβολής του για να σαρώσει την αλυσίδα και να δει όλα τα POAPs του, χωρίς να δώσει σε αυτό το interface τη δυνατότητα να ξοδέψει αυτά τα POAPs". (CoinLoan, 2023)

2. Προβλήματα των Stealth Address

Οι μυστικές διευθύνσεις έχουν δεχθεί πυρά από τις φορολογικές και ρυθμιστικές αρχές, δεδομένου ότι παραβιάζουν τα κριτήρια εντοπισμού. Τέτοιες ιδιωτικές διευθύνσεις θα μπορούσαν θεωρητικά να χρησιμοποιηθούν για οποιαδήποτε παράνομη δραστηριότητα, συμπεριλαμβανομένης της εμπορίας ναρκωτικών, της χρηματοδότησης της τρομοκρατίας και του ξεπλύματος χρήματος.

Ένα άλλο ζήτημα είναι η φοροδιαφυγή. Οι κυβερνήσεις και οι ρυθμιστικές αρχές δημιουργούν προγράμματα όπως η επιχείρηση "Hidden Treasure" για την εύρεση παραβατών. Αυτό το πρόγραμμα της IRS, το οποίο εισήχθη το 2021, απευθύνεται σε φορολογούμενους που δεν καταγράφουν συναλλαγές που αφορούν κρυπτονομίσματα.

Οποιαδήποτε μέθοδος συσκότισης έχει δύο μειονεκτήματα. Ακόμη και αν αυξάνει την ανωνυμία σύμφωνα με την αρχική υπόσχεση του κρυπτονομίσματος, μπορεί να βοηθήσει ανέντιμα ή κακά μέρη. Ακόμα και αν ειπωθεί, οι περισσότεροι χρήστες είναι τίμιοι- σύμφωνα με τους υπολογισμούς της Chainanalysis, μόνο το 0,15% όλων των συναλλαγών το 2021 χρησιμοποιήθηκε για παράνομη δραστηριότητα. Την επόμενη χρονιά, παρά το γεγονός ότι οι κυρώσεις προκάλεσαν τον παράνομο όγκο συναλλαγών να φτάσει σε ιστορικό υψηλό, αυξήθηκε μόνο κατά 0,24% (CoinLoan, 2023)

3. Κβαντικά ανθεκτική ασφάλεια μέσω Stealth Address

Αν οι κβαντικοί υπολογιστές γίνουν πρόβλημα, θα πρέπει να στραφούμε σε αλγόριθμους ανθεκτικούς στους κβαντικούς υπολογιστές. Υπάρχουν δύο φυσικοί υποψήφιοι γι' αυτό: ισογονίες ελλειπτικών καμπυλών και πλέγματα.

Οι ισογονίες ελλειπτικών καμπυλών, μια εντελώς διαφορετική μαθηματική δομή που βασίζεται στις ελλειπτικές καμπύλες, αποφεύγουν τη δημιουργία κυκλικών ομάδων που μπορούν να υποστούν επιθέσεις διακριτού λογαρίθμου με κβαντικούς υπολογιστές, ενώ παράλληλα έχουν τις ιδιότητες γραμμικότητας που μας επιτρέπουν να εκτελούμε διάφορα κρυπτογραφικά κόλπα.

Το κύριο ελάττωμα της κρυπτογραφίας που βασίζεται στην ισογένεια είναι ο κίνδυνος πιθανών επιθέσεων που καλύπτονται από την πολυπλοκότητα των υποκείμενων μαθηματικών της. Παρόλο που ορισμένα πρωτόκολλα που βασίζονται στην ισογένεια παραβιάστηκαν πέρυσι, άλλα εξακολουθούν να είναι ασφαλή. Τα θεμελιώδη πλεονεκτήματα των ισογενειών είναι τα σχετικά μικρά μεγέθη κλειδιών τους και η άμεση φορητότητα πολλών διαφορετικών μεθόδων που βασίζονται σε ελλειπτικές καμπύλες.

Σε αντίθεση με τις ισογένειες ελλειπτικών καμπυλών, τα πλέγματα είναι ένας θεμελιωδώς διαφορετικός τύπος κρυπτογραφικής αρχιτεκτονικής που μπορεί να εκτελέσει ορισμένες πολύ ισχυρές λειτουργίες, όπως η πλήρως ομομορφική κρυπτογράφηση. Τα πλέγματα θα μπορούσαν να χρησιμοποιηθούν για την υποστήριξη συστημάτων κρυφών διευθύνσεων, ενώ ο ιδανικός σχεδιασμός είναι ακόμη υπό συζήτηση. Οι δομές που βασίζονται σε πλέγματα, ωστόσο, έχουν συνήθως σημαντικά μεγαλύτερα μεγέθη κλειδιών. (Buterin, 2023)

4. Παραδείγματα συστημάτων που χρησιμοποιούν Stealth Address

i. Monero (XMR):

Προκειμένου να παρέχει στους χρήστες υψηλό επίπεδο ιδιωτικότητας, το Monero, ένα δημοφιλές κρυπτονόμισμα με έμφαση στην προστασία της ιδιωτικότητας, χρησιμοποιεί κρυφές διευθύνσεις, υπογραφές δακτυλίου και RingCT (Ring Confidential Transactions). Στο Monero, οι μυστικές διευθύνσεις χρησιμοποιούνται για να αποκρύψουν την πραγματική διεύθυνση του παραλήπτη, καθιστώντας δύσκολη τη σύνδεση των συναλλαγών με συγκεκριμένους χρήστες.

ii. Particl (PART):

Μια αποκεντρωμένη πλατφόρμα που εστιάζει στην προστασία της ιδιωτικής ζωής και ονομάζεται Particl επιτρέπει αποκεντρωμένες εφαρμογές (dApps) και ένα εγγενές νόμισμα που ονομάζεται PART. Για να παρέχει στους χρήστες χαρακτηριστικά ιδιωτικότητας, το Particl κάνει χρήση των διευθύνσεων stealth, των εμπιστευτικών συναλλαγών (CT) και του RingCT.

iii. Bitcoin (BTC) and Litecoin (LTC):

Παρόλο που το Bitcoin και το Litecoin δεν περιλαμβάνουν εγγενή υποστήριξη για κρυφές διευθύνσεις έχουν προσθέσει αυτή τη δυνατότητα για να

αυξήσουν την ιδιωτικότητα των χρηστών. Η χρήση των stealth διευθύνσεων σε αυτά τα δίκτυα δεν προσφέρει το ίδιο επίπεδο μυστικότητας όπως στα δίκτυα που δέχονται εγγενώς stealth διευθύνσεις, όπως το Monero, είναι ζωτικής σημασίας να τονιστεί.

Mixing

Η τεχνολογία Blockchain, με την αποκεντρωμένη, διαφανή και ασφαλή πλατφόρμα της, έχει φέρει επανάσταση σε διάφορους τομείς. Ωστόσο, η διαφάνεια και η ακεραιότητα των συναλλαγών blockchain, αν και συμφέρουν για τη λογοδοσία και την ασφάλεια, μπορεί να θέσουν σε κίνδυνο την ιδιωτικότητα των χρηστών. Εδώ μπαίνει στο παιχνίδι η έννοια της μίξης. Η ανάμειξη (mixing) ή η ανατροπή (tubing) είναι μια στρατηγική που χρησιμοποιείται για τη βελτίωση της ιδιωτικότητας στις συναλλαγές blockchain, ιδιαίτερα σε κρυπτονομίσματα, αποκρύπτοντας την ιχνηλασιμότητα των συναλλαγών. (Cryptocurrency tumbler, x.x.)

Στην ουσία, η μίξη περιλαμβάνει τη χρήση μιας υπηρεσίας τρίτου μέρους για να σπάσει τη σύνδεση μεταξύ του αποστολέα και του παραλήπτη σε μια συναλλαγή κρυπτονομίσματος. Αυτό επιτυγχάνεται με τη συγκέντρωση πολλών συναλλαγών και στη συνέχεια την ανακατανομή τους έτσι ώστε η αρχική πηγή κεφαλαίων να είναι δύσκολο να εντοπιστεί (Cryptocurrency tumbler, x.x.). Ο πρωταρχικός στόχος της μίξης είναι να ενισχύσει το απόρρητο και την ανωνυμία των χρηστών καθιστώντας δύσκολη την παρακολούθηση της ροής των συναλλαγών στο blockchain.

Το Bitcoin, το πιο ευρέως χρησιμοποιούμενο κρυπτονόμισμα, λειτουργεί σε ένα δημόσιο blockchain όπου κάθε συναλλαγή καταγράφεται και μπορεί να εντοπιστεί. Αυτή η διαφάνεια επιτρέπει σε οποιονδήποτε να παρακολουθεί τη ροή των bitcoin από τη μια διεύθυνση στην άλλη, θέτοντας μια ανησυχία για την ιδιωτικότητα. Οι υπηρεσίες Mixing, γνωστές και ως tumblers,

αντιμετωπίζουν αυτό το ζήτημα απορρήτου κρύβοντας τα ίχνη των συναλλαγών, καθιστώντας δύσκολο για οποιονδήποτε να εντοπίσει την προέλευση των κεφαλαίων. (Cryptocurrency tumbler, x.x.)

Υπάρχουν διάφοροι τύποι υπηρεσιών ανάμειξης, ο καθένας με τα δικά του πλεονεκτήματα και περιορισμούς. Οι κεντρικοί μίκτες (Centralized mixers), για παράδειγμα, είναι εταιρείες που δέχονται το bitcoin σας, το αναμειγνύουν με άλλες συναλλαγές και στη συνέχεια στέλνουν πίσω διαφορετικά bitcoin έναντι αμοιβής (CoinDesk). Ωστόσο, αυτές οι υπηρεσίες εξακολουθούν να παρουσιάζουν μια πρόκληση απορρήτου, καθώς διατηρούν αρχείο συναλλαγών, αποκαλύπτοντας πιθανώς τη σύνδεση ενός χρήστη με τα νομίσματα στο μέλλον.

Από την άλλη πλευρά, οι αποκεντρωμένοι μίκτες (decentralized mixers) χρησιμοποιούν πρωτόκολλα όπως το CoinJoin για να αποκρύψουν πλήρως τις συναλλαγές μέσω μιας συντονισμένης ή peer-to-peer μεθόδου (CoinDesk). Αυτή η μέθοδος επιτρέπει σε μια μεγάλη ομάδα χρηστών να συγκεντρώσουν μια ποσότητα bitcoin και στη συνέχεια να την αναδιανείμουν έτσι ώστε όλοι να πάρουν πίσω το bitcoin τους, αλλά κανείς δεν μπορεί να πει ποιος πήρε τι ή από πού προήλθε. Αυτή η μέθοδος θεωρείται πιο ασφαλής καθώς δεν βασίζεται σε ένα μόνο σημείο αποτυχίας και δεν απαιτεί εμπιστοσύνη σε τρίτους.

Ωστόσο, τα μίξερ έχουν ελαττώματα. Για παράδειγμα, εάν μια υπηρεσία επιβολής του νόμου γνωρίζει τη διεύθυνση που χρησιμοποιεί ο πρώτος ύποπτος και εάν ο δεύτερος ύποπτος είναι ο μόνος που έχει λάβει λίγο λιγότερο από το συγκεκριμένο ποσό, δεν θα είναι πολύ δύσκολο να επανασυνδέσει τη ροή των χρημάτων (Times). Αυτό το πρόβλημα γίνεται πιο δύσκολο να λυθεί όσο περισσότεροι άνθρωποι χρησιμοποιούν τον μίξερ. Επιπλέον, ορισμένοι μίκτες ενδέχεται να διατηρούν αρχεία καταγραφής συναλλαγών, στα οποία θα μπορούσαν ενδεχομένως να έχουν πρόσβαση οι

χάκερ ή οι υπηρεσίες επιβολής του νόμου, θέτοντας έτσι σε κίνδυνο το απόρρητο που σκοπεύουν να παρέχουν. (Investopedia)

Ένα πραγματικό παράδειγμα μιας υπηρεσίας μίξης είναι η Bitcoin Fog, μια εταιρεία που ιδρύθηκε με στόχο την ενίσχυση της ιδιωτικότητας των συναλλαγών με bitcoin. Η προσέγγιση της εταιρείας περιλαμβάνει τον διαχωρισμό κάθε ανάληψης σε έναν τυχαίο αριθμό πληρωμών, την τυχαιοποίηση του σχετικού μεγέθους κάθε πληρωμής και την κατανομή του χρόνου αυτών των πληρωμών σε μια καθορισμένη χρονική περίοδο. Ωστόσο, τέτοιες υπηρεσίες έχουν υποβληθεί σε νομικό έλεγχο λόγω της δυνατότητάς τους να διευκολύνουν παράνομες δραστηριότητες.

Ένα χαρακτηριστικό παράδειγμα είναι η σύλληψη του Larry Harmon, του χειριστή μιας υπηρεσίας ξεπλύματος κρυπτονομισμάτων που βασίζεται στο Darknet που ονομάζεται Helix (Justice). Ο Harmon κατηγορήθηκε για ξέπλυμα εκατοντάδων εκατομμυρίων δολαρίων για χρήστες του Darknet σε όλο τον κόσμο, υπογραμμίζοντας την πιθανή κατάχρηση των υπηρεσιών ανάμειξης για παράνομες δραστηριότητες. Αυτή η υπόθεση χρησιμεύει ως έντονη υπενθύμιση των νομικών συνεπειών που συνδέονται με τη χρήση αναμικτηρίων.

Παρά την πιθανότητα κακής χρήσης, είναι σημαντικό να σημειωθεί ότι δεν εμπλέκονται όλοι οι χρήστες των υπηρεσιών μίξης σε παράνομες δραστηριότητες. Ορισμένοι χρήστες μπορεί απλώς να επιθυμούν να ασκήσουν το δικαίωμά τους στην ιδιωτικότητα. Για παράδειγμα, το Dash, ένα κρυπτονόμισμα που εστιάζει στην ιδιωτικότητα, προσφέρει μια δυνατότητα μίξης που ονομάζεται PrivateSend, η οποία λειτουργεί σε ένα αποκεντρωμένο δίκτυο και επιτρέπει στους χρήστες να συνδυάζουν τις συναλλαγές τους με άλλους, ενισχύοντας έτσι την ιδιωτικότητά τους.

Η χρήση υπηρεσιών μίξης στις συναλλαγές blockchain δεν περιορίζεται στα κρυπτονομίσματα. Μπορούν επίσης να χρησιμοποιηθούν σε άλλες εφαρμογές της τεχνολογίας blockchain όπου το απόρρητο αποτελεί ανησυχία. Για παράδειγμα, στη διαχείριση της εφοδιαστικής αλυσίδας, οι υπηρεσίες ανάμειξης μπορούν να χρησιμοποιηθούν για να κρύψουν τα ίχνη των συναλλαγών, προστατεύοντας έτσι ευαίσθητες πληροφορίες σχετικά με προμηθευτές και πελάτες.

Ωστόσο, η χρήση υπηρεσιών μίξης σε αυτές τις εφαρμογές εγείρει μια σειρά ηθικών και νομικών ζητημάτων. Για παράδειγμα, ενώ οι υπηρεσίες μίξης μπορούν να βελτιώσουν την ιδιωτικότητα, μπορούν να χρησιμοποιούνται επίσης για τη διευκόλυνση παράνομων δραστηριοτήτων όπως ξέπλυμα χρήματος και απάτη. Ως εκ τούτου, είναι ζωτικής σημασίας για τις ρυθμιστικές αρχές και τους φορείς χάραξης πολιτικής να επιτύχουν μια ισορροπία μεταξύ της προστασίας της ιδιωτικής ζωής και της πρόληψης παράνομων δραστηριοτήτων.

Οι υπηρεσίες ανάμειξης διαδραματίζουν κρίσιμο ρόλο στην ενίσχυση του απορρήτου στις συναλλαγές blockchain. Ωστόσο, η χρήση τους εγείρει μια σειρά από ηθικά, νομικά και τεχνικά ζητήματα που πρέπει να εξεταστούν προσεκτικά. Καθώς η τεχνολογία blockchain συνεχίζει να εξελίσσεται, είναι ζωτικής σημασίας για τους ερευνητές, τους επαγγελματίες και τους υπεύθυνους χάραξης πολιτικής να συνεχίσουν να εξερευνούν αυτά τα ζητήματα και να αναπτύσσουν λύσεις που εξισορροπούν την ανάγκη για ιδιωτικότητα με την ανάγκη για διαφάνεια και υπευθυνότητα.

Comparison of blockchain privacy systems

(Σύγκριση συστημάτων ιδιωτικότητας Αλυσίδων μπλοκ)

Public Blockchain Systems

Οι δημόσιες αλυσίδες μπλοκ δεν έχουν άδειες και είναι πλήρως αποκεντρωμένες. Επιτρέπουν σε οποιονδήποτε να ενταχθεί και να συμμετάσχει στο δίκτυο blockchain. Όλοι οι κόμβοι σε ένα δημόσιο blockchain έχουν ίσα δικαιώματα πρόσβασης, δημιουργία νέων μπλοκ δεδομένων και επικύρωση μπλοκ δεδομένων. Αυτός ο τύπος blockchain είναι διαφανής και όλες οι συναλλαγές είναι διαθέσιμες για όλους, προωθώντας τη διαφάνεια και την εμπιστοσύνη. Το Bitcoin, το Ethereum και το Litecoin είναι παραδείγματα δημόσιων blockchain. Ωστόσο, οι δημόσιες αλυσίδες μπλοκ τείνουν να έχουν μεγαλύτερους χρόνους επικύρωσης για νέα δεδομένα λόγω του μεγάλου αριθμού κόμβων και του μεγέθους των συναλλαγών. (Blockchains) (Medium) (TechTarget)

Private Blockchain Systems

Οι ιδιωτικές αλυσίδες μπλοκ, γνωστές και ως διαχειριζόμενες αλυσίδες μπλοκ, είναι επιτρεπόμενες αλυσίδες μπλοκ που ελέγχονται από έναν μόνο οργανισμό. Σε ένα ιδιωτικό blockchain, η κεντρική αρχή καθορίζει ποιος μπορεί να είναι κόμβος και δεν εκχωρεί απαραίτητα σε κάθε κόμβο ίσα δικαιώματα για την εκτέλεση λειτουργιών. Οι ιδιωτικές αλυσίδες μπλοκ είναι αποκεντρωμένες μόνο εν μέρει, επειδή η δημόσια πρόσβαση σε αυτές τις αλυσίδες μπλοκ είναι περιορισμένη. Η κεντρική αρχή μπορεί να ελέγχει την πρόσβαση για τους χρήστες της και μπορεί επίσης να ελέγχει άλλες πτυχές του blockchain, όπως ο περιορισμός των συναλλαγών με βάση την ταχύτητα ή την πρόθεση. Το Ripple και το Hyperledger είναι παραδείγματα ιδιωτικών blockchain. Οι ιδιωτικές αλυσίδες μπλοκ τείνουν να είναι πιο αποτελεσματικές

και ασφαλείς, αλλά είναι πιο επιρρεπείς σε παραδοσιακές ευπάθειες hacking λόγω της κεντρικής φύσης τους. (Blockchains) (Medium) (TechTarget)

Hybrid Blockchain Systems

Οι υβριδικές αλυσίδες μπλοκ στοχεύουν να συνδυάσουν τις καλύτερες πτυχές τόσο του δημόσιου όσο και του ιδιωτικού blockchain. Ελέγχονται από έναν μόνο οργανισμό, αλλά με ένα επίπεδο εποπτείας που εκτελείται από το δημόσιο blockchain, το οποίο απαιτείται για την εκτέλεση ορισμένων επικυρώσεων συναλλαγών. Οι υβριδικές αλυσίδες μπλοκ επιτρέπουν στους διαχειριστές να είναι επιλεκτικοί με το ποιος έχει πρόσβαση, ενώ εξακολουθούν να έχουν χαρακτηριστικά όπως η διαφάνεια και η ασφάλεια. Ένα παράδειγμα υβριδικής αλυσίδας μπλοκ είναι το IBM Food Trust, το οποίο αναπτύχθηκε για να βελτιώσει την αποτελεσματικότητα σε ολόκληρη την αλυσίδα εφοδιασμού τροφίμων.

Consortium Blockchain Systems

Οι μπλοκ αλυσίδες κοινοπραξίας είναι επιτρεπόμενες αλυσίδες μπλοκ που διέπονται από μια ομάδα οργανισμών και όχι από μια οντότητα. Τα blockchains κοινοπραξίας απολαμβάνουν μεγαλύτερη αποκέντρωση από τα ιδιωτικά blockchain, με αποτέλεσμα υψηλότερα επίπεδα ασφάλειας. Ωστόσο, η σύσταση κοινοπραξιών μπορεί να είναι μια δύσκολη διαδικασία, καθώς απαιτεί συνεργασία μεταξύ ορισμένων οργανισμών. Το Global Shipping Business Network Consortium είναι ένα παράδειγμα blockchain κοινοπραξίας. (LLP)

Συμπερασματικά, η επιλογή του τύπου blockchain εξαρτάται από τις συγκεκριμένες ανάγκες και απαιτήσεις των χρηστών. Τα δημόσια blockchain είναι ιδανικά για εφαρμογές που απαιτούν διαφάνεια και αποκέντρωση, ενώ τα ιδιωτικά blockchain είναι κατάλληλα για οργανισμούς που χρειάζονται έλεγχο στο δίκτυο blockchain τους. Οι υβριδικές αλυσίδες μπλοκ προσφέρουν μια ισορροπία μεταξύ των δύο, παρέχοντας διαφάνεια και έλεγχο. Τα blockchain κοινοπραξιών, από την άλλη πλευρά, προσφέρουν μια συλλογική προσέγγιση

στη διακυβέρνηση του blockchain. Καθώς η τεχνολογία blockchain συνεχίζει να εξελίσσεται, αναμένεται ότι θα εμφανιστούν περισσότεροι τύποι συστημάτων blockchain, καθένας με τα μοναδικά χαρακτηριστικά και τις εφαρμογές του.

Ανάλυση-Σύνθεση

Ένα από τα πιο κρίσιμα προβλήματα που συναντάμε κατά την ιδιωτικότητα στα blockchain είναι η ασφάλεια των δεδομένων που είναι αποθηκευμένη μέσα σε μία αλυσίδα. Η διαφάνεια είναι ένα βασικό στοιχείο της τεχνολογίας blockchain που εγγυάται την ακεραιότητα των συναλλαγών και μειώνει την απάτη. Αυτό το χαρακτηριστικό, ωστόσο, συνεπάγεται επίσης ότι όλες οι πληροφορίες που είναι αποθηκευμένες στην αλυσίδα μπλοκ είναι προσβάσιμες σε όλους τους χρήστες, θέτοντας ενδεχομένως σε κίνδυνο ευαίσθητα δεδομένα.

Το αμετάβλητο των δεδομένων που αποθηκεύονται στην αλυσίδα μπλοκ είναι ένα άλλο πρόβλημα. Όταν μια συναλλαγή προστίθεται στην αλυσίδα μπλοκ, δεν μπορεί να αλλάξει ή να αφαιρεθεί, γεγονός που καθιστά δύσκολη την τήρηση του δικαιώματος λήθης του GDPR και άλλων κανονισμών προστασίας της ιδιωτικής ζωής των δεδομένων. Μια παραβίαση δεδομένων ή άλλη κακόβουλη δραστηριότητα μπορεί να γίνει πιο πιθανή ως αποτέλεσμα της συσσώρευσης μη αναγκαίων δεδομένων που επιφέρει η αδυναμία αφαίρεσης δεδομένων που είναι αποθηκευμένα στην αλυσίδα μπλοκ.

Μερικές λύσεις για την ενίσχυση του απορρήτου των δεδομένων στην τεχνολογία blockchain είναι οι εξής:

a) Εφαρμογή τεχνολογιών βελτίωσης της ιδιωτικότητας: Στις συναλλαγές blockchain, τα προσωπικά δεδομένα μπορούν να διασφαλιστούν με τη χρήση τεχνολογίας που ενισχύει την ιδιωτικότητα, όπως η ομομορφική κρυπτογράφηση, οι υπογραφές δακτυλίου και οι αποδείξεις μηδενικής γνώσης. Αυτές οι τεχνολογίες μπορούν να παρέχουν ιδιωτική μεταφορά δεδομένων διατηρώντας παράλληλα την ασφάλεια.
b) Ψευδωνυμοποίηση και επαλήθευση ταυτότητας: Στο δίκτυο blockchain, οι ταυτότητες των χρηστών μπορούν να προστατεύονται με τη χρήση ψευδωνύμων. Για να σταματήσει η κατάχρηση των ψευδωνύμων, είναι απαραίτητοι οι μηχανισμοί επαλήθευσης και πιστοποίησης ταυτότητας. Αυτές οι προφυλάξεις μπορεί να περιλαμβάνουν πρωτόκολλα για τη γνώση του πελάτη σας (γνωστό και ως "KYC")

και την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες (γνωστό και ως "AML"). ((Intern), 2023)

Μία ακόμα απειλή των blockchain είναι οι επιθέσεις routing. Η μεταφορά τεράστιων ποσοτήτων δεδομένων σε πραγματικό χρόνο είναι απαραίτητη για ένα δίκτυο blockchain και τις εφαρμογές του. Η ανωνυμία ενός λογαριασμού μπορεί να χρησιμοποιηθεί από χάκερ για να υποκλέψουν τα δεδομένα που αποστέλλονται στους παρόχους υπηρεσιών διαδικτύου.

Επειδή η μεταφορά δεδομένων και οι λειτουργίες συνεχίζονται κανονικά εν όψει μιας επίθεσης routing, οι συμμετέχοντες στην αλυσίδα μπλοκ συνήθως αγνοούν τον κίνδυνο. Ο κίνδυνος είναι ότι αυτές οι επιθέσεις θα μπορούσαν τακτικά να αποκαλύπτουν ιδιωτικές πληροφορίες ή να κλέβουν χρήματα εν αγνοία του χρήστη.

Για την αποφυγή μία τέτοιας επίθεσης θα πρέπει να χρησιμοποιηθεί μια πληθώρα από τεχνικές. Μια από αυτές είναι η εφαρμογή ασφαλών πρωτοκόλλων δρομολόγησης. Μερικές ακόμα τεχνικές είναι η κρυπτογράφηση των δεδομένων που βρίσκονται σε μία αλυσίδα μπλοκ, η τακτική αλλαγή κωδικών των χρηστών της αλυσίδας, όπως και η επιμόρφωση των χρηστών για κινδύνους όπως το phishing. (Shah, 2022)

Ένα ακόμα σοβαρό πρόβλημα των blockchain είναι η συνδεσιμότητα (Linkability). Αυτό το πρόβλημα αναφέρεται στις διευθύνσεις που χρησιμοποιούν οι χρήστες. Παρόλο που χρησιμοποιούνται ψευδώνυμες διευθύνσεις, στην περίπτωση που μια διεύθυνση μπορεί να οδηγήσει στην πραγματική διεύθυνση του χρήστη, τότε όλες οι συναλλαγές θα μπορούσαν τελικά να οδηγήσουν στον τελικό χρήστη, κάνοντας τον στόχο.

Μια λύση αυτού του προβλήματος είναι η σωστή κρυπτογράφηση των δεδομένων αυτών ή ακόμα και η αποθήκευση τους εκτός της αλυσίδας. Έτσι, όλα τα κρυπτογραφημένα δεδομένα δεν θα μπορούσαν να γίνουν εύκολα αναγνώσιμα χωρίς τον κατάλληλο τρόπο αποκρυπτογράφησης και το κατάλληλο κλειδί. **Invalid source specified.**

Τέλος, η λεγόμενη 51% Attack είναι ένας ακόμα κίνδυνος των blockchain. Ένα άτομο ή μια ομάδα (κακοί χάκερ) μπορεί να καταλάβει περισσότερο από το μισό του ρυθμού κατακερματισμού και να καταλάβει ολόκληρο το σύστημα σε μια επίθεση 51%, η οποία μπορεί να αποβεί μοιραία. Οι συναλλαγές μπορούν να αλλοιωθούν και μπορούν επίσης να σταματήσουν την επιβεβαίωσή τους, από τους χάκερς. Επίσης, είναι σε θέση ακόμη και να αναιρέσουν ήδη ολοκληρωμένες συναλλαγές, γεγονός που οδηγεί σε διπλές δαπάνες.

Υπάρχουν διάφοροι τρόποι να αποφευχθεί μία επίθεση 51%. Ένας από αυτούς τους τρόπους είναι η εφαρμογή ισχυρών μηχανισμών συναίνεσης και η διατήρηση ενός αποκεντρωμένου δικτύου. Επίσης μερικοί ακόμα τρόποι είναι η βεβαίωση ότι ο ρυθμός κατακερματισμού είναι υψηλός και να μην χρησιμοποιούνται τεχνικές συναίνεσης proof-of-work(PoW) (Shah, 2022)

Υπάρχουν ακόμα πολλές απειλές για την ιδιωτικότητα σε μια αλυσίδα μπλοκ, όμως λόγω του περιορισμένου χώρου που έχουμε για την έκταση αυτή της εργασία αποφασίσαμε να αναπτύξουμε μερικές από αυτές.

Συμπεράσματα

Η εξερεύνηση της ιδιωτικότητας στην τεχνολογία blockchain σε αυτήν την εργασία έχει αποκαλύψει μια σειρά από κρίσιμες ιδέες και πιθανές κατευθύνσεις για μελλοντική έρευνα και ανάπτυξη. Η εγγενής ένταση μεταξύ της διαφάνειας του blockchain και της ανάγκης για ιδιωτικότητα δεν είναι απλώς μια τεχνική πρόκληση, αλλά και μια φιλοσοφική πρόκληση. Μας αναγκάζει να επανεξετάσουμε την κατανόησή μας για την ιδιωτικότητα στην ψηφιακή εποχή και πώς μπορούμε να την συμβιβάσουμε με το αίτημα για διαφάνεια και ασφάλεια στις διαδικτυακές συναλλαγές.

Οι διάφορες κρυπτογραφικές τεχνικές και τα συστήματα που συζητήθηκαν στην εργασία, όπως αποδείξεις μηδενικής γνώσης, υπογραφές δακτυλίου, μυστικές διευθύνσεις και μίξη, αντιπροσωπεύουν πολλά υποσχόμενες λύσεις για τη βελτίωση της ιδιωτικότητας στο blockchain. Ωστόσο, υπογραμμίζουν επίσης την πολυπλοκότητα της επίτευξης αληθινής ιδιωτικότητας σε ένα σύστημα σχεδιασμένο για διαφάνεια. Κάθε λύση έρχεται με το δικό της σύνολο αντισταθμίσεων και δεν υπάρχει μια προσέγγιση που ταιριάζει σε όλους.

Η κατηγοριοποίηση των συστημάτων blockchain σε Δημόσια, Ιδιωτικά, Υβριδικά και Συστήματα Blockchain Κοινοπραξίας απεικονίζει περαιτέρω τις ποικίλες εφαρμογές της τεχνολογίας blockchain. Υποδηλώνει ότι το μέλλον του blockchain μπορεί να μην βρίσκεται σε ένα ενιαίο, καθολικό μοντέλο, αλλά σε μια ποικιλία εξειδικευμένων συστημάτων προσαρμοσμένων σε συγκεκριμένες ανάγκες και κλάδους.

Η ανάθεση υπογραμμίζει επίσης τη σημασία των ρυθμιστικών παραμέτρων για την ανάπτυξη και την υιοθέτηση της τεχνολογίας blockchain. Καθώς το blockchain συνεχίζει να διεισδύει σε διάφορους τομείς, η ανάγκη για ένα σαφές, ολοκληρωμένο ρυθμιστικό πλαίσιο που προστατεύει την ιδιωτικότητα των χρηστών ενώ παράλληλα επιτρέπει την καινοτομία γίνεται ολοένα και πιο σημαντική.

Συμπερασματικά, αυτή η εργασία όχι μόνο παρείχε μια ολοκληρωμένη επισκόπηση της ιδιωτικότητας στο blockchain, αλλά έθεσε επίσης σημαντικά ερωτήματα για μελλοντική εξερεύνηση. Υπογράμμισε την ανάγκη για συνεχή έρευνα, καινοτομία και διάλογο για την επιδίωξη ενός συστήματος blockchain που εξισορροπεί τη διαφάνεια, την ασφάλεια και το απόρρητο. Καθώς προχωράμε προς τα εμπρός, οι πληροφορίες που προκύπτουν από αυτήν την εργασία θα χρησιμεύσουν ως πολύτιμος οδηγός για την πλοήγηση στο περίπλοκο περιβάλλον της τεχνολογίας blockchain και της ιδιωτικής ζωής.

Βιβλιογραφία

(Intern), T. A. (2023, April 19). *Data Privacy Issues in Blockchain*. Ανάκτηση από AMLEGALS: https://amlegals.com/data-privacy-issues-in-blockchain/

Anderson, B. (2018, October 21). Ring Signatures and Anonymisation. Ανάκτηση από https://medium.com/asecuritysite-when-bob-met-alice/ring-signatures-and-anonymisation-c9640f08a193

Bender, A. K. (2006). Ring signatures: Stronger definitions, and constructions without random oracles. *Journal of Cryptology*, 114-138. Ανάκτηση από https://eprint.iacr.org/2005/304.pdf

Blockchain.com. (2023, January 15). *What are public and private keys and how do they work?* . Ανάκτηση από Blockchain.com: https://support.blockchain.com/hc/en-us/articles/4417082520724-What-are-public-and-private-keys-and-how-do-they-work-

Blockchains, 1. (χ.χ.). Hybrid Blockchain: The Best of Both Public and Private. Ανάκτηση από https://101blockchains.com/hybrid-blockchain/

Buterin, V. (2023, January 20). *Stealth Addresses and Confidential Transactions*. Ανάκτηση από Vitalik Buterin's website: https://vitalik.ca/general/2023/01/20/stealth.html

CoinDesk. (χ.χ.). Bitcoin Mixers: How Do They Work and Why Are They Used? Ανάκτηση από https://www.coindesk.com/learn/bitcoin-mixers-how-do-they-work-and-why-are-they-used/

CoinLoan. (2023, March 24). *Stealth address guide: Keeping crypto transactions private*. Ανάκτηση από CoinLoan: https://coinloan.io/blog/stealth-address-guide-keeping-crypto-transactions-private/

Cointelegraph. (χ.χ.). What are Peer-to-Peer (P2P) Blockchain Networks and How Do They Work. Ανάκτηση από https://cointelegraph.com/learn/what-are-peer-to-peer-p2p-blockchain-networks-and-how-do-they-work

Contributors, W. (2023, March 7). *Privacy and blockchain*. Ανάκτηση από Wikipedia: https://en.wikipedia.org/wiki/Privacy_and_blockchain

Council., B. (χ.χ.). Peer-to-Peer Network. Ανάκτηση από https://www.blockchain-council.org/blockchain/peer-to-peer-network

Cryptocurrency tumbler. (χ.χ.). Ανάκτηση από Wikipedia : https://en.wikipedia.org/wiki/Cryptocurrency_tumbler

Ethereum. (2023, May 19). *Zero knowledge proofs.* Ανάκτηση από Ethereum: https://ethereum.org/en/zero-knowledge-proofs/#further-reading

Finstocklearn. (χ.χ.). Understanding Peer-to-Peer Networks in Blockchain. Ανάκτηση από https://finstocklearn.com//understanding-peer-to-peer-networks-in-blockchain

Fujisaki, E. &. (2007). Traceable ring signature. Ανάκτηση από https://eprint.iacr.org/2006/389.pdf

Investopedia. (χ.χ.). Bitcoin Mixer (Tumbler) Explained. Ανάκτηση από https://www.investopedia.com/terms/b/bitcoin-mixer.asp

Justice, D. o. (χ.χ.). Ohio Resident Charged with Operating Darknet-Based Bitcoin “Mixer,” which Laundered Over $300 Million. Ανάκτηση από https://www.justice.gov/opa/pr/ohio-resident-charged-operating-darknet-based-bitcoin-mixer-which-laundered-over-300-million

LLP, F. &. (χ.χ.). Types of Blockchain: Public, Private, or Something in Between. Ανάκτηση από https://www.foley.com/en/insights/publications/2021/08/types-of-blockch

Medium. (χ.χ.). What are Public, Private and Hybrid Blockchains? Ανάκτηση από https://medium.com/@blockchain101/what-are-public-private-and-hybrid-blockchains-e01d6e21eb41.

Monero. (χ.χ.). Ring Signatures. Ανάκτηση από https://www.getmonero.org/resources/moneropedia/ringsignatures.html

Rivest, R. S. (2001). How to leak a secret. Στο *Advances in Cryptology — ASIACRYPT 2001* (σσ. 552-565). Springer Berlin Heidelberg.

Shah, M. (2022, February 02). *Fast Company*. Ανάκτηση από Blockchain security issues and how to prevent them: https://www.fastcompany.com/90722111/5-blockchain-security-issues-and-how-to-prevent-them

TechTarget. (χ.χ.). What are the 4 different types of blockchain technology? Ανάκτηση από https://www.techtarget.com/searchcio/feature/What-are-the-4-different-types-of-blockchain-technology.

Times, I. B. (χ.χ.). Bitcoin tumbler: The business of covering tracks in the world of cryptocurrency laundering. Ανάκτηση από https://www.ibtimes.co.uk/bitcoin-tumbler-business-covering-tracks-world-cryptocurrency-laundering-1487480