Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών
και Μηχανικών Υπολογιστών
Τομέας Επικοινωνιών, Ηλεκτρονικής και
Συστημάτων Πληροφορικής

Ανάλυση της ιδιωτικότητας στις συναλλαγές Bitcoin: Αξιολόγηση του CoinJoin στην πράξη

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΓΙΑΝΝΟΥΛΗΣ ΑΛΕΞΑΝΔΡΟΣ

Επιβλέπων : Μιλτιάδης Αναγνώστου
Καθηγητής Ε.Μ.Π.

Αθήνα, Μάρτιος 2023

Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών
και Μηχανικών Υπολογιστών
Τομέας Επικοινωνιών, Ηλεκτρονικής και
Συστημάτων Πληροφορικής

Ανάλυση της ιδιωτικότητας στις συναλλαγές Bitcoin: Αξιολόγηση του CoinJoin στην πράξη

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΓΙΑΝΝΟΥΛΗΣ ΑΛΕΞΑΝΔΡΟΣ

Επιβλέπων : Μιλτιάδης Αναγνώστου
Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 6η Μαρτίου 2023.

.....	.....	.....
Ιωάννα Ρουσσάκη Αν. Καθηγήτρια Ε.Μ.Π.	Ευστάθιος Συκάς Καθηγητής Ε.Μ.Π.	Μιλτιάδης Αναγνώστου Καθηγητής Ε.Μ.Π.

Αθήνα, Μάρτιος 2023

.....

Γιαννούλης Αλέξανδρος

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

Copyright © Γιαννούλης Αλέξανδρος, 2023.
Με επιφύλαξη παντός δικαιώματος. All rights reserved.

Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας εργασίας, εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Ερωτήματα που αφορούν τη χρήση της εργασίας για κερδοσκοπικό σκοπό πρέπει να απευθύνονται προς τον συγγραφέα.

Οι απόψεις και τα συμπεράσματα που περιέχονται σε αυτό το έγγραφο εκφράζουν τον συγγραφέα και δεν πρέπει να ερμηνευθεί ότι αντιπροσωπεύουν τις επίσημες θέσεις του Εθνικού Μετσόβιου Πολυτεχνείου.

Περίληψη

Κατά τα πρώτα χρόνια διάδοσης του bitcoin, υπήρχε η ψευδαίσθηση πως η χρήση διευθύνσεων ως δημόσια αναγνωριστικά αντί προσωπικών στοιχείων παρέχει αποτελεσματική ιδιωτικότητα. Γρήγορα ωστόσο έγινε αντιληπτό πως αυτή η χρήση ψευδωνύμων δεν επαρκεί, αφού τα κρυπτονομίσματα μπορούν εύκολα να ιχνηλατηθούν μεταξύ συναλλαγών με την χρήση απλών ευριστικών μεθόδων. Η παρούσα εργασία στοχεύει στην συνολική μελέτη του ζητήματος της ιδωτικότητας στο bitcoin. Γίνεται περιγραφή του προβλήματος και των διάφορων κινδύνων απώλειας της ανωνυμίας. Αναλύονται οι χρησιμοποιούμενες τεχνικές ενίσχυσης της ιδιωτικότητας όπως και προτεινόμενες μέθοδοι που παρουσιάζουν προοπτικές. Δίνεται έμφαση στη μέθοδο CoinJoin μέσω της στατιστικής μελέτης στην δημοφιλή υλοποίηση του Wasabi Wallet. Αναδεικνύονται έτσι τα υψηλά ποσοστά αποτελεσματικότητας της, αλλά και οι παράγοντες που υποσκάπτουν την χρησιμότητα της. Εξερευνάται επίσης η εξέλιξη της μεθόδου στο πλαίσιο των πρόσφατων βελτιώσεων της υλοποίησης. Αυτή η έρευνα τέλος, ανοίγει τον δρόμο για περαιτέρω μελέτη και βελτίωση του CoinJoin και για την συνολική ενίσχυση της ιδιωτικότητας στο bitcoin.

Λέξεις κλειδιά

Κρυπτονομίσματα, Καθολικό κρυπτονομίσμάτων, Ιδιωτικότητα, Ανωνυμία, Ανάμιξη συναλλαγών, Πορτοφόλι κρυπτονομισμάτων, Ιχνηλάτηση κρυπτονομισμάτων

Abstract

During the early years of bitcoin's spread, there was an illusion that using addresses as public identifiers instead of personal information provided effective privacy. However, it was quickly realized that this use of pseudonyms is not enough, since coins can easily be traced between transactions using simple heuristics. This thesis aims to comprehensively study the issue of privacy in bitcoin. The problem and various risks of loss of promising anonymity are described. The techniques used to enhance privacy are analyzed as well as proposed methods. Emphasis is placed on the CoinJoin method through statistical study on the popular Wasabi Wallet implementation. Thus, its high efficiency rates are highlighted, but also the factors that undermine its usefulness. Finally, the evolution of the method in the context of improved implementations such as Wasabi version 2.0 (WabiSabi) is explored.

Key words

Cryptocurrencies, Bitcoin, Blockchain, Privacy, Anonymity, Coin Mixing, CoinJoin, Wasabi Wallet, Bitcoin Tracing

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή της διπλωματικής μου εργασίας κύριο Μιλτιάδη Αναγνώστου. Η καθοδήγηση και η τεχνογνωσία του ήταν πολύτιμα εφόδια για την τέλεση της εργασίας μου. Είμαι ευγνώμων για την υπομονή, την υποστήριξη και όλη τη βοήθεια του στη διάρκεια αυτής της πορείας. Θα ήθελα επίσης να εκφράσω τις ειλικρινείς μου ευχαριστίες στους φίλους και συμφοιτητές μου που συμπορευθήκαμε τα όμορφα αυτά χρόνια της σχολής. Τέλος, δεν θα μπορούσα να έχω ολοκληρώσει αυτόν τον αγώνα χωρίς την οικογένεια μου και την αμέριστη υποστήριξη και ενθάρρυνση τους σε αυτήν την διαδρομή. Ευχαριστώ απο καρδιάς τη σύζυγο μου, της οποίας η κατανόηση και η αγάπη αποτέλεσαν τα σημαντικότερα στηρίγματα που θα μπορούσα να χρειαστώ.

Γιαννούλης Αλέξανδρος,

Αθήνα, 6η Μαρτίου 2023

Περιεχόμενα

Περίληψη 5

Abstract 7

Ευχαριστίες 9

Περιεχόμενα 11

Κατάλογος σχημάτων 13

1. Εισαγωγή 15
- 1.1 Blockchain και κρυπτονομίσματα 15
- 1.2 Ιδιωτικότητα, ανωνυμία και κρυπτονομίσματα 15
- 1.3 Τεχνικές ενίσχυσης ιδιωτικότητας 16
- 1.4 Σκοπός της εργασίας 17
- 1.5 Δομή της εργασίας 17

2. Θεωρητική επισκόπηση και προσέγγιση των προβλημάτων ανωνυμίας του bitcoin 19
- 2.1 Σύντομή εισαγωγική επισκόπηση του bitcoin 19
- 2.2 Κίνδυνοι απώλεια ανωνυμίας στο bitcoin 21
  - 2.2.1 Εσφαλμένες υποθέσεις για την ανωνυμία του bitcoin και εξέλιξη των μεθόδων παραβίασης της. 21
  - 2.2.2 Μέθοδοι απώλειας ανωνυμίας με χρήση της αλυσίδας blockchain 23
  - 2.2.3 Εναλλακτικές μέθοδοι επίθεσης στην ανωνυμία του bitcoin 26

3. Μέθοδοι ενίσχυσής της ιδιωτικότητας στο bitcoin 29
- 3.1 Εφαρμογές προστασίας της ανωνυμίας κατά τον χειρισμό και την μετάδοση δεδομένων 29
  - 3.1.1 Αποστολή και χρήση κρυπτονομισμάτων 29
  - 3.1.2 Συγχρονισμός δεδομένων 30
  - 3.1.3 Προτεινόμενες μέθοδοι σε εξέλιξη 31
- 3.2 Αντιμετώπιση των ευριστικών μεθόδων επίθεσης στην ανωνυμία του bitcoin . . 32
  - 3.2.1 Επαναχρησιμοποίηση διευθύνσεων 32
  - 3.2.2 Μυστικές διευθύνσεις 33
  - 3.2.3 Υπογραφές δαχτυλιδιών 33
  - 3.2.4 Εμπιστευτικές συναλλαγές 34
  - 3.2.5 Zero-knowledge proofs και zk-SNARKs 34
  - 3.2.6 Βελτίωση των Scripts 35
  - 3.2.7 Off-chain transactions - Lightning Network 36
  - 3.2.8 Συγκεντρωτικές Υπηρεσίες Μίξης 36

4. Η εξέλιξη του CoinJoin και η ασφάλεια που παρέχει σε σύγχρονές υλοποιήσεις . . . 39
4.1 Ανασκόπηση στην εξέλιξη του Coinjoin . . . 39
4.1.1 Η μέθοδος Coinjoin . . . 39
4.1.2 Υλοποιήσεις CoinJoin . . . 40
4.2 Η περίπτωση του Wasabi Wallet . . . 41
4.2.1 Zerolink . . . 41
4.2.2 Chaumian CoinJoin . . . 42
4.3 Αξιολόγηση της αποτελεσματικότητας των CoinJoins . . . 45
4.3.1 Περιγραφή μεθόδου . . . 45
4.3.2 Αποτελέσματα . . . 47
4.4 Έξοδοι μεταβλητής ποσότητας και η νέα βελτίωση του WabiSabi . . . 49

5. Συμπεράσματα . . . 51

Αρκτικόλεξα - Ακρωνύμια . . . 55

Απόδοση ξενόγλωσσων όρων . . . 57

Βιβλιογραφία . . . 59

Κατάλογος σχημάτων

2.1 Παράδειγμα blockchain 20
2.2 Wikileaks για την ανωνυμία στο Bitcoin 22
2.3 New York Times για την ανωνυμία στο Bitcoin 22
2.4 Στατιστικά επαναχρησιμοποίησης διευθύνσεων 23
2.5 Παράδειγμα προβληματικής συναλλαγής 25
2.6 Bitcoin clustering 26
2.7 Παράδειγμα ανάλυσης αλυσίδας 26

3.1 Το δίκτυο λειτουργίας του TOR 31
3.2 Παράδειγμα υπηρεσίας μίξης 38

4.1 Ρυθμίσεις στρατηγικής μίξης στο Wasabi Wallet 43
4.2 Προηγμένες ρυθμίσεις στρατηγικής μίξης στο Wasabi Wallet 43
4.3 Χειροκίνητη επιλογή νομισμάτων στο Wasabi Wallet 44
4.4 Εφαρμογή στατιστικής ανάλυσης CoinJoins 46
4.5 Παράδειγμα συναλλαγής 48
4.6 Αποτελέσματα ανάλυσης CoinJoins του Wasabi Wallet 49

Κεφάλαιο 1

Εισαγωγή

1.1 Blockchain και κρυπτονομίσματα

Το 2009 δημοσιεύτηκε με το ψευδώνυμο Satoshi Nakamoto [1] το white paper με τίτλο « Bitcoin: A Peer-to-Peer Electronic Cash System». Το bitcoin, αποτελεί την πρώτη απο μια πληθώρα εφαρμογών, οι οποίες βασίζόνται σε μια δομή που ονομάζεται blockchain και επιτρέπει την αποκεντρωμένη αποθήκευση δεδομένων Η τεχνολογία blockchain έχει πολλά πλεονεκτήματα και η επέκταση τους στο σύγχρονο κόσμο των ψηφιακών συναλλαγών προκαλεί ενδιαφέρον. Πρόκειται για μια κατανεμημένη, αποκεντρωμένη (ανεξάρτητη δηλαδή απο οποιαδήποτε κεντρική αρχή) αποθήκευση ιστορικού, με τα δεδομένα να είναι διαθέσιμα σε κάθε ενδιαφερόμενο. Η διαφάνεια αυτή συντείνει στην εμπιστοσύνη μεταξύ των χρηστών, οι οποίοι μπορούν οποιαδήποτε στιγμή να επαληθεύσουν την εγκυρότητα των δεδομένων. Η διαγραφή δεδομένων θεωρείται αδύνατη, γεγονός που καθιστά την εισαγωγή σε αυτήν την «αλυσίδα» ως την μόνη πιθανή μέθοδο τροποποίησης της. Ως εκ τούτου, η δημιουργία αυτή ενέπνευσε την ανάπτυξη μεγάλου εύρους εφαρμογών βασισμένων στο blockchain. Μερικά τέτοια παραδείγματα αποτελούν η διαχείρίση της εφοδιαστικής αλυσίδας επιχειρήσεων, η ταυτοποίηση, τα συστήματα διεξαγωγής εκλογών [2], τα «έξυπνα συμβόλαια» (smart contracts) [3], τα λογιστικά κ.α. Η εφαρμογή που ξεχωρίζει ασφαλώς είναι αυτή των κρυπτονομισμάτων.

Πρέπει να γίνει ωστόσο αντιληπτό το ότι η τεχνολογία αυτή έιναι ακόμη αρκετά ευάλωτη απο πλευράς ασφάλειας, ιδιωτικότητας, επεκτασιμότητας, βιωσιμότητας κτλ. Σε αυτήν την εργασία επιλέξαμε να ερευνήσουμε την ιδιωτικότητα των κρυπτονομισμάτων, χρησιμοποιώντας ως βάση, το bitcoin, ως πρώτο και δημοφιλέστερο κρυπτονόμισμα, η τεχνολογία του οποίου χρησιμοποιείται σε παραλλαγές της απο την πλειοψηφία και των λοιπών κρυπτονομισμάτων. Η σκοπιά της μελέτης μας, όπως θα δούμε και αναλυτικότερα σε επόμενη ενότητα, αφορά την κατανόηση της ανάγκης χρησιμοποίησης συγκεκριμένων μεθόδων τήρησης της ανωνυμίας στις συναλλαγές του bitcoin και της παρουσίασης των τελευταίων τεχνολογικά εξελίξεων βελτίωσης των ανεπτυγμένων υλοποιήσεων πορτοφολιών.

1.2 Ιδιωτικότητα, ανωνυμία και κρυπτονομίσματα

Σύμφωνα με την βιβλιογραφία [4] η ιδιωτικότητα ορίζεται ως η αξίωση ατόμων, ομάδων ή ιδρυμάτων να προσδιορίσουν τα ίδια πότε, πώς και σε ποιο βαθμό οι πληροφορίες για αυτά κοινοποιούνται σε άλλους. Η προστασία της ψηφιακής ιδιωτικότητας είναι υψίστης σημασίας, αφού στην εποχή της δραματικής αύξησης του ρόλου της τεχνολογίας στην ζωή μας, καθορίζει την δυνατότητα επιλογών σχετικά με την αποκάλυψη ευαίσθητων πληροφοριών, όπως είναι οι συναλλαγές και κατ' επέκταση οι οικονομικές συνθήκες, το βιωτικό επίπεδο και πολλά ακόμη δεδομένα για την ζωή εκάστου ατόμου.

Στον κόσμο των υλοποιήσεων blockchain, βασικό ρόλο διαδραματίζει η δημόσια παροχή αναλυτικών ιστορικών δεδομένων. Στην περίπτωση των κρυπτονομισμάτων, τα δεδομένα αυτά αφορούν την αναλυτική παρουσίαση συναλλαγών. Η τεχνολογία αυτή βασίζεται στο ότι οι πληροφορίες αυτές διατίθενται με τρόπο ανώνυμο, χωρις δηλαδή να είναι δυνατή η αντιστοίχιση

δεδομένων με πραγματικές οντότητες. Η ανωνυμία ενός ατόμου ορίζεται [4] στο πλαίσιο ορισμένου συνόλου ατόμων με δυνητικά τα ίδια χαρακτηριστικά και σημαίνει ότι το υποκείμενο δεν είναι αναγνωρίσιμο μέσα στο συγκεκριμένο σύνολο το οποίο αποκαλείται και σύνολο ανωνυμίας.

Η αρχική θεώρηση πως το bitcoin προσφέρει πλήρη ανωνυμία στις συναλλαγές, γρήγορα αποδείχθηκε ψευδής. Μετά απο ποικίλες μελέτες [5, 6, 7, 8, 2] κ.α, είναι πλέον αποδεδειγμένο πως υπάρχουν πολλοί τρόποι απώλειας αυτής της ανωνυμίας και παραβίασης της ιδιωτικότητας των χρηστών στις συναλλαγές τους. Η δήλωση αυτή αντιβαίνει στην μέχρι τώρα θεώρηση του συγκεκριμένου θέματος απο μεγάλη μερίδα χρηστών καθώς και από διεθνείς οργανισμούς, ιστοσελίδες και εταιρίες. Στην πραγματικότητα, η υλοποίηση του bitcoin με την αντιστοίχηση οντοτήτων σε σύνολα απο ιδιωτικά παραγόμενες - αλλά δημόσια διαθέσιμες διευθύνσεις (μέσω επισκόπησης του ιστορικού των blockchains) προσφέρει μονάχα ψευδωνυμία και όχι ανωνυμία! Η ψευδωνυμία αυτή ειναι εύθραυστη και εύκολα παραβιάζεται.

Θεωρούμε σκόπιμο λοιπόν για την καλύτερη κατανόηση των κινδύνων και της ανάγκης εφαρμογής εξελιγμένων τεχνικών, να αφιερώσουμε ξεχωριστό κεφάλαιο στην περιγραφή και την ανάλυση των μεθόδων που χρησιμοποιούνται για την παραβίαση των ανωνυμίας και επιφέρουν την κατάργηση της ιδιωτικότητας στις συναλλαγές του bitcoin.

1.3 Τεχνικές ενίσχυσης ιδιωτικότητας

Η ερευνητική κοινότητα έχει δείξει μεγάλο ενδιαφέρον για την εύρεση μεθόδων ενίσχυσης και εξασφάλισης της ιδιωτικότητας στην χρήση κρυπτονομισμάτων. Ο βασικός διαχωρισμός τους αφορά το αν πρόκειται για μεθόδους που βασίζονται στην ενίσχυση υπαρχόντων κρυπτονομισμάτων ή αν πρόκειται για δημιουργία κρυπτονομισμάτων με εγγενείς ιδιότητες με στόχο την ανωνυμία.

Στην δεύτερη κατηγορία, ανήκουν τα λεγόμενα «privacy-coins» (κρυπτονομίσματα αυξημένης ιδιωτικότητας). Τέτοιες υλοποιήσεις είναι το Monero, το Zcash, Mina, Decred κ.α Τα πρωτόκολλα που χρησιμοποιούν αυτά τα κρυπτονομίσματα είναι πολύ ισχυρά, ωστόσο η εφαρμογή τους στο bitcoin και σε άλλα δημοφιλή υπάρχοντα κρυπτονομίσματα έχει μεγάλες πρακτικές δυσκολίες και δεν καθίσταται εφικτή. Αντίθετα, στην πρώτη κατηγορία συγκαταλέγονται οι μέθοδοι που είναι εφαρμόσιμες με το bitcoin.

Η πιό απλή και εύκολη μέθοδος ενίσχυσης της ιδιωτικότητας είναι η αποφυγή επαναχρησιμοποίησης της ίδιας διέυθυνσης σε παραπάνω απο μία συναλλαγή. Μια ακόμη ευρέως χρησιμοποιούμενη μέθοδος είναι η εναλλαγή μεταξύ διαφορετικών κρυπτονομισμάτων (atomic swaps), με σκοπό του «κοψίματος» κάθε σύνδεσης μεταξύ κρυπτονομισμάτων και οντοτήτων. Ένα τέτοιο παράδειγμα αποτελεί εναλλαγή του bitcoin με νομίσματα σε Monero (το πιο διαδεδομένο privacy-coin σήμερα).

Ίσως η σημαντικότερη τεχνική που χρησιμοποιείται σήμερα είναι η λεγόμενη «μίξη (mixing). Η λογική της μίξης είναι απλή και βασίζεται στήν εναλλαγή συναλλαγών με αντίστοιχα άλλων χρηστών με σκοπό την εξάλειψη της πιθανότητας να βρεθούν «χνάρια» σύνδεσης μεταξύ διευθύνσεων απο το ιστορικό του blockchain. Κάτι τέτοιο είναι δυνατόν με χρήση ενδιάμεσων υπηρεσίων. Η εμπιστοσύνη ωστόσο σε κεντροποιημένες online υπηρεσίες ενέχει σοβαρούς κινδύνους, τους οποίους θα μελετήσουμε σε επόμενη ενότητα. Οι δυνατότητες σε πλήρη ανωνυμία που προσφέρει η μίξη νομισμάτων είναι δύσκολο να αγνοηθούν. Κατά συνέπεια, έχει διεξαχθεί σημαντική έρευνα σχετικά με αποκεντρωμένες λύσεις. Σε αποκεντρωμένες υλοποιήσεις μίξης, τον ρόλο της υπηρεσίας αναλαμβάνει ένα «peer-to-peer» (δίκτυο ομότιμών κόμβων) πρωτόκολλο . Κατ' αυτόν τον τρόπο επιλύονται τα προβλήματα ασφάλειας και αποφεύγεται η όποια πιθανότητα κλοπής απο ενδίαμεσους. Τέτοια μέθοδος είναι το Coinjoin [9]. Το Coinjoin χρησιμοποιεί ώς βασική λειτουργικότητα το γεγονός πως σε μία συναλλαγή μπορούν να συνδυαστούν πολλές είσοδοι (απο διαφορετικές διευθύνσεις) και πολλές έξοδοι. Συνεπώς με την χρήση κατάλληλων πρωτοκόλλων, υπάρχει η δυνατότητα απόκρυψης των ζευγών εισόδου-εξόδου μεταξύ συναλλαγών, μέσα στο σύνολο ανωνυμίας που ορίζεται από το πλήθος των εισόδων και των εξόδων που συμμετέχουν

στην συναλλαγή. Οι πιο δημορφιλείς υλοποιήσεις Coinjoin είναι αυτές του Samourai wallet και του Wasabi wallet [10]. Και οι 2 κατευθύνσεις ξεκίνησαν με βάση την κοινή τους δημιουργία - το λεγόμενο ZeroLink framework. Στην συνέχεια ωστόσο διαφοροποιήθηκαν, με το Wasabi wallet να υιοθετεί το Chaumian CoinJoin και το δίκτυο Tor, ενώ το Samourai βασίστηκε στην υλοποίηση Whirlpool.

1.4 Σκοπός της εργασίας

Σκοπός αυτής της εργασίας είναι κατ'αρχάς η αναλυτική μελέτη και επισκόπηση της έρευνας γύρω απο κινδύνους στην ιδιωτικότητα των κρυπτονομισμάτων και συγκεκριμένα του bitcoin. Θέλουμε λοιπόν να ανατρέξουμε στις έρευνες που οδήγησαν σε διαφόρων ειδών παραβιάσεις της ιδιωτικότητας και να αναδείξουμε τις ελείψεις των πρωτοκόλλων που περιορίζουν την διάδοση μιας εκ των σημαντικότερων τεχνολογικών δημιουργιών αυτού του αιώνα.

Ύστερα, θα δώσουμε έμφαση στις υλοποιήσεις αποκεντρωμέμένου CoinJoin και θα αναλύσουμε τα πρωτόκολλα που χρησιμοποιούν τα πιο δημοφιλή πορτοφόλια του bitcoin, με σκοπό την επίτευξη της ιδιωτικότητας. Θα εμβαθύνουμε ιδαίτερα στην υλοποίηση του CoinJoin απο το Wasabi η οποία είναι η πιο διαδεδομένη. Θα αξιολογήσουμε σε πρακτικό επίπεδο τα αποτελέσματα που επιφέρει και μιλήσουμε για την επερχόμενη εξέλιξη του με την έκδοση Wasabi 2.0 (WabiSabi).

1.5 Δομή της εργασίας

Στο 2ο κεφάλαιο της εργασίας αρχικά θα κάνουμε μια σύντομη επισκόπηση του bitcoin και κάποιων σημαντικών εννοιών. Στις επόμενες υποενότητες θα δώσουμε έμφαση στην εξήγηση των κινδύνων απώλειας ανωνυμίας στα κρυπτονομίσματα, αναφέροντας τις διαδεδομένες μεθόδους κατάργησης της. Δίνεται έμφαση σε τεχνικές ανάλυσης γράφου, εφαρμογές δηλαδή που χρησιμοποιούν κατά κύριο λόγο το ιστορικό στο blockchain, δημιουργώντας συνδέσεις τόσο μεταξύ διευθύνσεων που χρησιμοποιήθηκαν σε κοινή συναλλαγή, όσο και απευθείας μεταξύ φυσικών προσώπων και διεθύνσεων.

Επειτα, στο 3ο κεφάλαιο παρουσιάζουμε σύντομα την βιβλιογραφία σε σχέση με την ενίσχυση της ιδιωτικότητας στα κρυπτονομίσματα, φτάνοντας μέχρι τις υλοποιήσεις CoinJoin, στις οποίες δίνεται περαιτέρω έμφαση στην εργασία μας.

Στο 4ο κεφάλαιο γίνεται αναλυτική μελέτη της μεθόδου CoinJoin. Ξεκινάμε με την περιγραφή του πρωτοκόλλου και την αναφορά υλοποιήσεων του που εμφανίζονται στην αγορά και καταλήγουμε στην περιγραφή της τεχνολογίας του Wasabi Wallet. Αναλύεται η μέθοδος αξιολόγησης που κατασκευάσαμε και παρουσιάζονται τα αντίστοιχα στατιστικά αποτελέσματα. Εξηγείται τέλος η μετάβαση στο WabiSabi μετά την εύρεση αδυναμίας στο υπάρχον πρωτόκολλο. Η εργασία μας συμπληρώνεται με την ανασκόπηση και την αναφορά των βασικών συμπερασμάτων, καθώς και την προεπισκόπηση των δυνατοτήτων νέων εξελισσόμενων τεχνολογιών, ικανών να βελτιώσουν την τήρηση της ανωνυμίας στο bitcoin.

Κεφάλαιο 2

Θεωρητική επισκόπηση και προσέγγιση των προβλημάτων ανωνυμίας του bitcoin

Σκοπός αυτού του κεφαλαίου είναι η κατανόηση των προβλημάτων ανωνυμίας του bitcoin. Προτού γίνει μελέτη αυτών θεωρούμε χρήσιμο να ξεκινήσουμε την ανάλυση μας αναφέροντας κάποια βασικά χαρακτηριστικά των οντοτήτων που συνθέτουν το θεωρητικό υπόβαθρο αυτού του κεφαλαίου.

2.1 Σύντομή εισαγωγική επισκόπηση του bitcoin

Η ιδέα του blockchain δημιουργήθηκε το 1991 όταν οι Stuare Haber et al. παρουσίασαν την ιδεά της ψηφιακής υπογραφής ηλεκτρονικών αρχείων ως μέσο προστασίας κατά της αλλοίωσης τους [11, 12]. Στην πραγματικότητα όμως, η τεχνολογία αυτή έγινε δημοφιλής, όταν ο/η Satoshi Nakamoto [1] χρησιμοποίησε την έννοια της αλυσίδας συνδεδεμένων blocks (με hash pointers) για την κατασκευή του bitcoin, μιας δημιουργίας που άλλαξε τον ορίζοντα της ασφαλούς ψηφιακής καταγραφής δεδομένων.

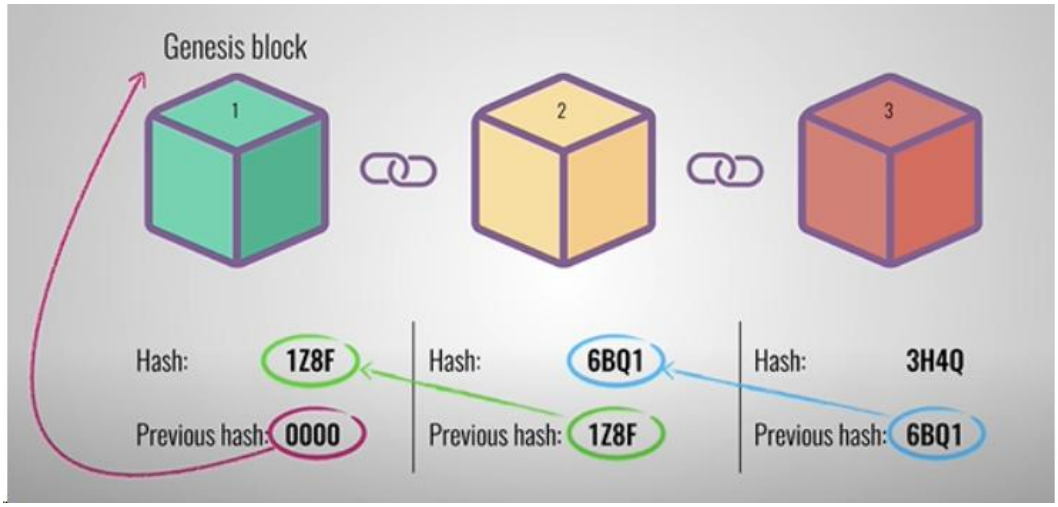
Το blockchain λοιπόν αποτελεί μια αλυσίδα ψηφιακών blocks, συνδεδεμένων μεταξύ τους με hash pointers, με τρόπο τέτοιο ώστε κάθε block να συσχετίζεται με το προηγούμενο. Κατά αυτόν τον τρόπου επιτυγχάνεται η δημιουργία ενός κατανεμημένου καθολικού, το οποίο αποκαλείται συνήθως και κατάστιχο (ledger). Τέτοια δίκτυα χρησιμοποιούνται σε δίκτυα ομότιμων κόμβων και είναι αποκεντρωμένα, αφού κάθε κόμβος δύναται να δημιουργείται σε ανεξάρτητη συσκευή απο τους υπόλοιπους, χωρίς να υπάρχει η ανάγκη ύπαρξης κεντρικού συστήματος ή αρχής.

Όπως σε μια παραδοσιακή βάση δεδομένων, έτσι και στο blockchain είναι δυνατή η αποθήκευση τεράστιων όγκων δεδομένων. Η διαφορά αυτών των κατασκευών έγκειται ωστόσο στην εντελώς διαφορετική δομή τους. Μια βάση δεδομένων τυπικά αποτελείται απο εγγραφές (records). Σε blockchains, τα δεδομένα αποθηκεύονται σε blocks, τα οποία αποθηκεύονται σε μια σειρά με τρόπο μη αναστρέψιμο, με σκοπό την διασφάλισή τους απο οποιαδήποτε απόπειρα αλλοίωσης. Τα δεδομένα αυτού του μέσου αποθήκευσης είναι κοινά, διαθέσιμα πρός επισκόπηση στην επιλεγμένη και προσωπική συσκευή κάθε ενδιαφερόμενου. Σημειώνεται πως το πρώτο block που δημιουργήθηκε στο Bitcoin αποκαλείται «Genesis Block» και δεν εμπεριέχει δείκτη σε κάποιο άλλο.

Στο bitcoin, τα δεδομένα που αποθηκεύονται στα blocks αφορούν τις αποστολές (συναλλαγές) ποσών της μονάδας satoshi. Αυτές εκτελούνται απο μία ή περισσότερες διευθύνσεις που αποκαλούνται και είσοδοι της συναλλαγής, σε μία ή περισσότερες διευθύνσεις, τις οποίες ονομάζουμε εξόδους. Τα δεδομένα ενός μεγάλου αριθμού συναλλαγών δημιουργούν ένα block και κάθε block προστίθεται στην αλυσίδα μέσω μιας ανταγωνιστικής διαδικασίας χρήσης υπολογιστικής ισχύος. Η διαδικασία αυτή ονομάζεται «εξόρυξη» (mining). Πρόκειται για την επίλυση ενός μαθηματικού puzzle μέσω της εξαντλητικής δοκιμής αστρονομικού συνόλου τιμών απο ισχυρές επεξεργαστικές μονάδες. Στην εργασία αυτή δεν θα γίνει μεγαλύτερη ανάλυση στον μηχανισμό αυτό. Αναφέρουμε μονάχα πως οι εξορύκτες έχουν καταλυτική συνεισφορά στην παραγωγή των blocks και την ορθή λειτουργία του πρωτοκόλου συναίνεσης του κρυπτονομίσματος.

Στον μηχανισμό αυτόν βασίζεται μεγάλο μέρος της επιτυχίας του bitcoin. Οι κόμβοι που

συμμετέχουν στην παραγωγή των blocks ελέγχουν παράλληλα την εγκυρότητα των συναλλαγών, μέσω της επαλήθευσης των υπολογισμών που προκύπτουν απο τις συναλλαγές και την σύγκριση τους με τα UTXOs (Unspent transaction outputs). Τα UTXOs με απλά λόγια, είναι οι έξοδοι απο προηγούμενες συναλλαγές που είναι διαθέσιμες για χρήση. Για παράδειγμα: Έστω πως ο Bob στέλνει 5 bitcoins σε μια διεύθυνση της Alice για την τέλεση πληρωμής 4ων bitcoins. Τότε 1 bitcoin θα επιστρέψει στην διεύθυνση επιλογής του Bob, ώς υπόλοιπο της συναλλαγής. Σε αυτή τη διαδικασία τα 5 bitcoins διαγράφονται ως UTXOs. Δημιουργούνται ταυτόχρονα 2 νέα UTXOs. Το πρώτο αντιστοιχεί στα 4 bitcoins και βρίσκεται στην κατοχή της Alice, ενώ το 2ό έχει αξία 1 bitcoin και πρόκειται για το ποσό που επέστρεψε στον Bob. Μπορούμε να αντιληφθούμε λοιπόν το κάθε UTXO ως σύνολο μιας ποσότητας κρυπτονομίσματος που δημιουργήθηκε σε κοινή συναλλαγή και μπορεί να χρησιμοποιηθεί μόνο ώς ενιαία ποσότητα.



Σχήμα 2.1: Στην παραπάνω εικόνα απεικονίζεται ένα απλό παράδειγμα blockchain

Οι διευθύνσεις στο bitcoin, αποτελούν μοναδικά αναγνωριστικά και φανερώνουν την ψηφιακή «τοποθεσία» μιας ποσότητας bitcoins. Αποτελούνται απο 26 μέχρι και 35 αλφαριθμητικούς χαρακτήρες. Μεγάλο ενδιαφέρον παρουσιάζει ο τρόπος δημιουργίας αυτών των διευθύνσεων και τα χαρακτηριστικά μέσω των οποίων στοχεύεται η ανωνυμία στην συναλλαγές.

Τα δημόσια και ιδιωτικά κλειδιά εμφανίστηκαν για πρώτη φορά το 1976 απο τους Whitfield Diffie και Martin Hellman [13, 14]. Η ιδέα τους αποτέλεσε την πρώτη υλοποίηση ασύμμετρης κρυπτογράφησης. Σε αυτήν την μέθοδο χρησιμοποιούνται 2 κλειδιά, ένα δημόσιο, οπου είναι γνωστό σε κάθε ενδιαφερόμενο και ένα ιδιωτικό, όπου μόνο ο ιδιοκτήτης που παρήγαγε το ζεύγος κλειδιών το γνωρίζει. Τα κλειδιά αυτά είναι ζεύγος, καθώς η δημιουργία τους είναι ενιαία. Υπάρχουν αρκετοί αλγόριθμοι για την παραγωγή αυτών των κλειδιών. Ο ευρύτερα χρησιμοποιούμενος αλγόριθμος γι αυτόν τον σκοπό είναι ο RSA [15, 16]. Το σύνολο των μεθόδων που χρησιμοποιούν αυτού του είδους την τεχνική ανήκουν στην κατηγορία της κρυπτογραφίας δημοσίου κλειδιού (Public key Cryptography). Στο πλαίσιο του bitcoin, το δημόσιο κλειδί χρησιμοποιείται ως ταυτότητα κάποιου χρήστη, ενώ το ιδωτικό κλειδί αποτελεί τον προσωπικό κωδικό που πιστοποιεί την ιδιοκτησία της διεύθυνσης που δημιουργείται μέσω αυτού, καθώς και ψηφιακών υπογραφών του κατά την τέλεση συναλλαγών.

Η παραγωγή ενός ζεύγους κλειδιών είναι απαραίτητη για τις ψηφιακές υπογραφές. Μέσω αυτών επιτρέπεται στους χρήστες να ταυτοποιούνται και να υπογράφουν τις συναλλαγές που εκτέλουν. Συγκεκριμένα, υπογράφεται ψηφιακά το δημόσιο κλειδί της διεύθυνσης εξόδου της συναλλαγής, σε συνδυασμό με τις εισόδους απο προηγούμενες συναλλαγές που χρησιμοποιούνται, αφού περάσουν πρώτα από συνάρτηση κατακερματιμού. Ο αλγόριθμος που χρησιμοποιείται στο Bitcoin για τις ψηφιακές υπογραφές ονομάζεται ECDSA (Eliptic Curve Digital Signature Algorithm) [17]. Δημιουργήθηκε το 1999 απο τους Don Johnson και Alfred Menezes. Πρόκειται

για μια παραλλαγή του αλγορίθμου DSA [18] χρησιμοποιώντας ελλειπτικές καμπύλες. Το ζεύγος δημόσιου-ιδιωτικού κλειδιού λοιπόν επιτελεί σημαντικό ρόλο στις ψηφιακές υπογραφές. Υπάρχει ωστόσο και δεύτερη εφαρμογή τους στο bitcoin. Πρόκειται για την παραγωγή των διευθύνσεων.

Αφού παραχθεί το ιδιωτικό κλειδί, υπολογίζεται το αντίστοιχο (δημόσιο) κλειδί και στην συνέχεια αυτό συμπιέζεται και κρυπτογραφείται με αποτέλεσμα την δημιουργία μιας διέυθυνσης bitcoin[19]. Μέσα απο αυτή τη συσχέτιση της διεύθυνσης με το δημόσιο κλειδί καταλαβαίνουμε πως το κλειδί αυτό διαδραματίζει το ρόλο δημόσιας ταυτότητας του ιδιοκτήτη του. Μονάχα ο κάτοχος του ιδιωτικού κλειδιού μπορεί να χρησιμοποιήσει την αντίστοιχη διεύθυνση. Παρατηρούμε επιπλέον πως η δημιουργία της εκάστοτε διέυθυνσης δεν απαιτεί επαλήθευση ταυτότητας ή και μοναδική διέυθυνση για κάθε χρήστη. Όλα γίνονται ανώνυμα, έτσι ώστε το κάθε άτομο μπορεί να έχει όσα ζεύγη κλειδιών επιθυμεί. [9]. Οι παραπάνω αρχές συνάδουν με την ιδέα της αποκεντρωμένης ψηφιακής ταυτότητας. Ο όρος αυτός αναφέρεται στην βιβλιογραφία ώς Self-Sovereign Identity (SSI) και δημιουργήθηκε απο τον Christopher Allen [20]. Σημειώνουμε πως κατά την παραγωγή των διευθύνσεων γίνεται χρησιμοποίηση ισχυρής γεννήτριας τυχαίων αριθμών, ώστε να υπάρχει εγγύηση πως είναι πρακτικά αδύνατον να βρεθούν 2 χρήστες με την ίδια διέυθυνση (αφού το κλειδί έχει μήκος 256 bits).

Οι συναλλαγές του bitcoin δημιουργούνται μέσω της γλώσσας «Script». Πρόκειται για μια απλή γλώσσα που δεν είναι Turing complete και χρησιμοποιείται απλώς για να ορίσει τον τρόπο που ξοδεύεται η ποσότητα bitcoins μια συναλλαγής. Ο πιο συνηθισμένος τύπος script είναι ο Pay-to-Public-Key-Hash (P2PKH) [21], δηλαδή μια απλή πληρωμή. Υπάρχουν πιο σύνθετοι τύποι scripts, μέσω των οποίων επιτρέπεται η αποστολή απο πλήθος διευθύνσεων εισόδων, με την χρήση αντίστοιχου πλήθους υπογραφών (multi-signatures).

Η διαχείριση των κρυπτονομισμάτων γίνεται ώς επι το πλείστον μέσω ψηφιακών πορτοφολιών. Πρόκειται για εφαρμογές μέσω των οποίων μπορούμε να στέλνουμε, να λαμβάνουμε και να διαχειριζόμαστε κρυπτονομίσματα. Η δυνατότητα αυτή επιτυγχάνεται μέσω της αποθήκευσης του ζεύγους κλειδιών που ταυτοποιούν την εκάστοτε διεύθυνση. Ο βασικός διαχωρισμός των ψηφιακών πορτοφολιών είναι ανάμεσα σε online υλοποιήσεις και σε εφαρμογές διαθέσιμες για λήψη και εγκατάσταση (τόσο σε φορητές όσο και σταθερές συσκευές). Σε κάθε περίπτωση τα πορτοφόλια πρέπει να προστατεύονται απο ισχυρούς κωδικούς και επαλήθευση 2 βημάτων. Πολλοί χρήστες επιλέγουν για διευκόλυνση τα online πορτοφόλια συναλλακτικών υπηρεσίων. Τα περισσότερα πορτοφόλια παρέχουν χρήσιμες λειτουργίες, όπως είναι η αποθήκευση διαχείριση μεγάλου πλήθους διευθύνσεων, η αυτόματη δημιουργία διευθύνσεων κ.α. Στο 3ο κεφάλαιο θα περιγραφούν επιπλέον λειτουργικότητες και οι υλοποιήσεις που τις παρέχουν με σκοπό την ενίσχυση της ανωνυμίας στις συναλλαγές.

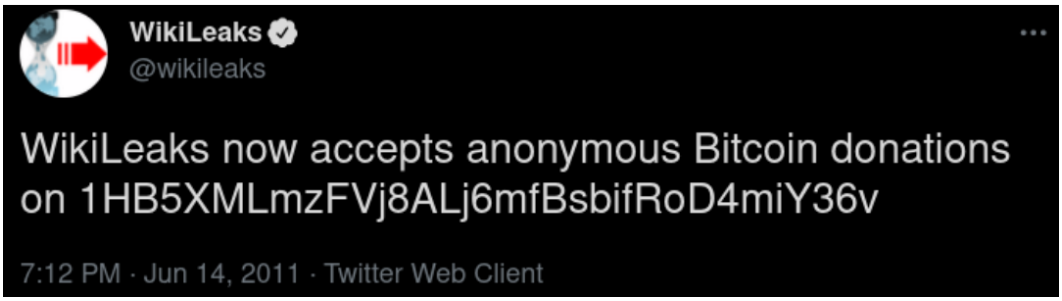
2.2 Κίνδυνοι απώλεια ανωνυμίας στο bitcoin

Σε αυτήν την ενότητα θα γίνει μια ανάλυση των κινδύνων απώλειας της ανωνυμίας στο bitcoin.

2.2.1 Εσφαλμένες υποθέσεις για την ανωνυμία του bitcoin και εξέλιξη των μεθόδων παραβίασης της.

Κατά τα πρώτα χρόνια διάδοσης του Bitcoin υπήρχε η εντύπωση πως η χρήση διευθύνσεων παραγόμενων με συναρτήσεις κατακερματισμού παρέχει ανωνυμία και καθιστά την ιχνηλάτηση των στοιχείων των χρηστών αδύνατη.

Υπάρχουν πολλοί τρόποι παραβίασης της ανωνυμίας των χρηστών και αυτοί εξαρτώνται κατά κύριο λόγο απο τις επιλογές του εκάστοτε χρήστη. Ωστόσο ακόμη και για αρκετά προσεκτικούς χρήστες η διατήρηση της ανωνυμίας δεν είναι καθόλου δεδομένη. Χαρακτηριστικό παράδειγμα αποτελεί η υπόθεση της εγκληματικής οργάνωση DarkSide [22], η οποία αποτελούνταν από hackers και κατάφερε να λάβει ώς λύτρα 75 bitcoins συνολικής αξίας άνω των 5 εκατομμυρίων.



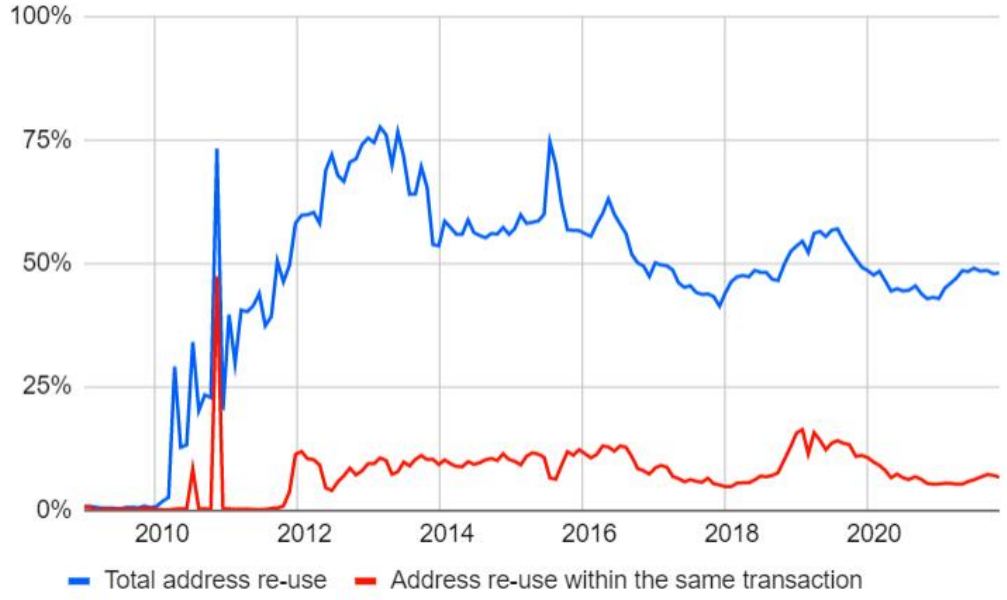
Σχήμα 2.2: Το 2011, η ιστοσελίδα Wikileaks υποστηρίζει πώς οι συναλλαγές στο Bitcoin γίνονται ανώνυμα.

Η οργάνωση αυτή προσπάθησε μέσω διαδοχικών συναλλαγών και διευθύνσεων να κρύψει τα κρυπτονομίσματα και να εξαφανίσει κάθε ίχνος. Οι αρχές ωστόσο κατάφεραν να ακολουθήσουν τα ίχνη τους στο blockchain, παρ'ότι τα «λάφυρα» αυτής τους της παράνομης πράξης είχαν μεταφερθεί μεταξύ τουλάχιστον εικοσιτριών διευθύνσεων.

Σχήμα 2.3: Το 2021, η ιστοσελίδα New York Times αναφέρεται στην ανωνυμία του Bitcoin.

Στην πραγματικότητα, η συμπεριφορά των περισσότερων χρηστών είναι πολύ περισσότερο απλοϊκή απο αυτήν της προαναφερθείσας εγκληματικής οργάνωσης. Σύμφωνα με μελέτη [23], αναδεικνύεται πώς μεγάλο μέρος των χρηστών δεν τηρεί ούτε την απλούστερη μέθοδο ενίσχυσης της ανωνυμίας, η οποία είναι η αποφυγή επαναχρησιμοποίησης διευθύνσεων. Η συγκεκριμένη οδηγία είναι γνωστή και προτεινόμενη ακόμα και στο white paper του bitcoin [1].

Είναι γεγονός πως πολλές επιχειρήσεις, όπως και κυβερνητικές υπηρεσίες, έχουν προχωρήσει στην δημιουργία εργαλείων ανάλυσης της αλυσίδας των κρυπτονομισμάτων. Αυτή είναι η κύρια απειλή στην διατήρηση της ανωνυμίας των κατόχων κρυπτονομισμάτων. Οι υπηρεσίες αυτές χρησιμοποιούν ευριστικούς αλγορίθμους σχετικά με συγκεκριμένα μοτίβα και συμπεράσματα που μπορούν να ληφθούν απο την αλυσίδα. Στην επόμενη υποενότητα θα δώσουμε έμφαση στην



Σχήμα 2.4: Στον πίνακα αναπαρίσταται το ποσοστό επαναχρησιμοποίησης διευθύνσεων τόσο στην ίδια συναλλαγή (στις εισόδους και στις εξόδους ταυτόχρονα), όσο και σε διαφορετικές συναλλαγές. [24]

κατανόηση του τρόπου υλοποίησης τέτοιων μηχανισμών.

2.2.2 Μέθοδοι απώλειας ανωνυμίας με χρήση της αλυσίδας blockchain

Σε μια απο τις πρώτες σημαντικές αναλύσεις στην βιβλιογραφία [5] παρουσιάστηκαν οι παρακάτω ευριστικές μέθοδοι στην βιβλιογραφία:

Ευριστική 1. *Το σύνολο των διευθύνσεων εισόδου μια συναλλαγής είναι πολύ πιθανόν να ανήκουν στην ίδια οντότητα.*

Σύμφωνα με αυτήν την ευριστική μέθοδο, όταν σε μια συναλλαγή εμφανίζονται πολλαπλές είσοδοι, το πιθανότερο ενδεχόμενο είναι πως αυτές οι διευθύνσεις ανήκουν στην ίδια οντότητα. Άλλωστε για κάθε είσοδο απαιτείται ψηφιακή υπογραφή, απο τον κάτοχο της διεύθυνσης, γεγονός που μειώνει την πιθανότητα συνεργασίας διαφορετικών χρηστών σε κοινή συναλλαγή. Χαρακτηριστικό τεκμήριο της εγκυρότητας αυτής της ευριστικής αποτελεί η έρευνα [25], σύμφωνα με την οποία περίπου το 69% των διευθύνσεων ενός κοινού πορτοφολιού μπορεί εύκολα να ομαδοποιηθεί. Όπως θα δούμε παρακάτω, το λεγόμενο CoinJoin δημιουργήθηκε με το σκοπό να μειώσει την αποτελεσματικότητα αυτής της μεθόδου.

Ευριστική 2. *Νέες διευθύνσεις που παράγονται και χρησιμοποιούνται ως έξοδοι για την λήψη του υπολοίπου σε μια συναλλαγή ενδέχεται να ανήκουν στην ίδια οντότητα με τον κάτοχο της διεύθυνσής εισόδου [26].*

Η συγκεκριμένη ευριστική μέθοδος που σχετίζεται με το υπόλοιπο μια συναλλαγής οδηγεί σε αρκετές διαφορετικές υποπεριπτώσεις που αναλύονται επίσης στην βιβλιογραφία [27]. Η πιο κοινή περίπτωση προκύπτει όταν μια συναλλαγή έχει δύο εξόδους και η μία έχει εμφανιστεί ξανά στην αλυσίδα. Τότε, είναι ασφαλές να υποθέσουμε πώς η νέα διεύθυνση παράχθηκε για τα «ρέστα» και ανήκει στον κάτοχο των διευθύνσεων εισόδου.

Επιγραμματικά, οι λοιπές ευριστικές που σχετίζονται με τον εντοπισμό της διεύθυνσης για το υπόλοιπο (το οποίο θα αποκαλούμε και επιστροφή) μια συναλλαγής, είναι:

- Αν όλες οι είσοδοι έχουν προκύψει απο τον ίδιο τύπο script, τότε θεωρείται πολύ πιθανόν πως και η διεύθυνση επιστροφής θα έχει τον ίδιο τύπο (π.χ Pay-to-PubkeyHash (P2PKH), Pay-to-Script-Hash(P2SH)).

- Οι διευθύνσεις εξόδου των οποίων οι ποσότητες που λαμβάνουν δεν είναι στρογγυλοί αριθμοί, είναι πιθανότερο να είναι διευθύνσεις επιστροφής (αφού συνήθως το ποσό πληρωμής σε συναλλαγές είναι στρογγυλός αριθμός).

- Όταν μια διεύθυνση εμφανίζεται τόσο στις εισόδους όσο και στις εξόδους της συναλλαγής, είναι εξαιρετικά πιθανόν να πρόκειται για διεύθυνση επιστροφής.

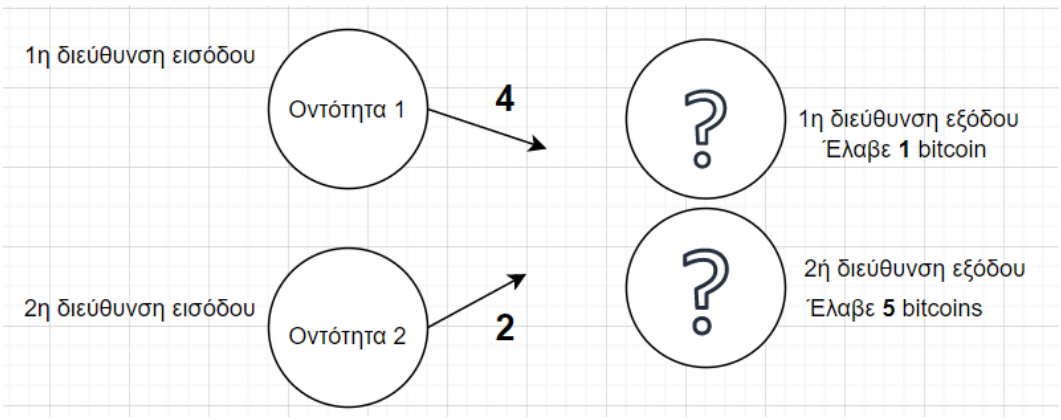
- Πολλές φορές, λεπτομέρειες κατά την υλοποίηση των συναλλαγών απο τα ηλεκτρονικά πορτοφόλια μπορούν να φανερώσουν σημαντικά στοιχεία τους («wallet fingerprinting»). Για παράδειγμα, απλοί χρήστες συνήθως χρησιμοποιούν 2 εξόδους στις συναλλαγές τους. Η μία έξοδος αφορά την διεύθυνση πληρωμής και η άλλη την παραγόμενη διεύθυνσης επιστροφής του υπολοίπου. Αντίθετα, εταιρίες όπως casino, στέλνουν τις συναλλαγές τους σε παρτίδες (batching), με πολλαπλές εισόδους και εξόδους -πολλές φορές- συγκεκριμένου μεγέθους. Μεταβλητός είναι επίσης ο τρόπος που γίνεται η επιλογή των UTXOs μεταξύ των διαθέσιμων για μια συναλλαγή. Κάποιοι εκ των χρησιμοποιηθέντων αλγορίθμων είναι ευδιάκριτοι και εύκολα προσδιορίσιμοι. Μια άκομη σημαντική παράμετρος είναι η χρήση (ή μη) της επιλογής nLockTime στις πληροφορίες της συναλλαγής. Μέσω αυτής της επιλογής προσδιορίζεται ένα ελάχιστο χρονικό διάστημα στο οποίο η συναλλαγή δεν μπορεί να εισαχθεί σε block. Η χρήση της ωστόσο, είναι προαιρετική.

- Η ευριστική που αφορά το λεγόμενο μοτίβο «peeling chain» κάνει λόγο για την περίπτωση που είναι μεγάλο ποσό πληρώνει σε μία σειρά συναλλαγών μικρά πόσα σε διάφορες διευθύνσεις, με το μεγαλύτερο μέρος του ποσού να περνάει κάθε φορά σε νέα διεύθυνση. Σε μια τέτοια περίπτωση φαίνεται εύκολα ο προορισμός του υπόλοιπου της εκάστοτε συναλλαγής.

- Μια ακόμη ευριστική υποθέτει πώς η έξοδος με το μικρότερο ποσό είναι πιθανόν να αποτελεί change address (διεύθυνση υπολοίπου).

- Τέλος, κλασσική περίπτωση θεωρείται όταν η πιθανότητα χρησιμοποίησης περιττών εισόδων φανερώνει το ποσό πληρωμής και το ποσό επιστροφής στον χρήστη. Έστω το παρακάτω εικονιζόμενο παράδειγμα: Σε αυτή τη περίπτωση έχουμε μια συναλλαγή που αποτελείται απο 2 εισόδους. Για την ιδιαίτερα απλή περίπτωση μας οι διευθύνσεις αυτές είναι λογικό και πιθανότερο να ανήκουν στην ίδια οντότητα, ωστόσο το ίδιο ισχύει και στην περίπτωση που έχουμε 2 διαφορετικές οντότητες, την 1 και την 2. Θεωρούμε πως η πρώτη στέλνει 4 bitcoins και η 2η στέλνει 2 bitcoins σε κοινή συναλλαγή. Έστω λοιπόν πως οι διευθύνσεις εξόδου λαμβάνουν 1 και 5 bitcoins αντίστοιχα. Αν θέλουμε να προσδιορίσουμε ποιά απο τις 2 εξόδους έγινε για πληρωμή, αρκεί να σκεφτούμε πώς σε περίπτωση που το ποσό πληρωμής ήταν 1 bitcoin, η χρησιμοποίηση 2 εισόδων μεγαλύτερων αυτής της ποσότητας είναι περιττή. Συνεπώς είναι σχεδόν βέβαιο πώς η διεύθυνση που έλαβε το 1 bitcoin ανήκει στην ίδια οντότητα, αυτήν δηλαδή που εκτέλεσε την συναλλαγή.

Συνεχίζοντας, ένα απο τα μεγαλύτερα λάθη που έχει παρατηρηθεί κατά την τέλεση συναλλαγών είναι η επαναχρησιμοποίηση διευθύνσεων για την έξοδο συναλλαγής. Αν υποθέσουμε πως μια διέυθυνση που εμφανίζεται σε μια συναλλαγή έχει χρησιμοποιηθεί στο παρελθόν, τότε είναι εύκολη η σύνδεση όλων των συναλλαγών που αφορούν την συγκεκριμένη διεύθυνση, γεγονός που μπορεί να οδηγήσει σε απώλεια ανωνυμίας. Επιπλέον, τα σύχρονα πορτοφόλια παράγουν αυτόματα νέα διέυθυνση για την αποθήκευση του υπολοίπου των συναλλαγών, συνεπώς είναι



Σχήμα 2.5: Στην εικόνα παρουσιάζουμε παράδειγμα συναλλαγής, όπου δεν δίνεται προσοχή στην διατήρηση της ανωνυμίας.

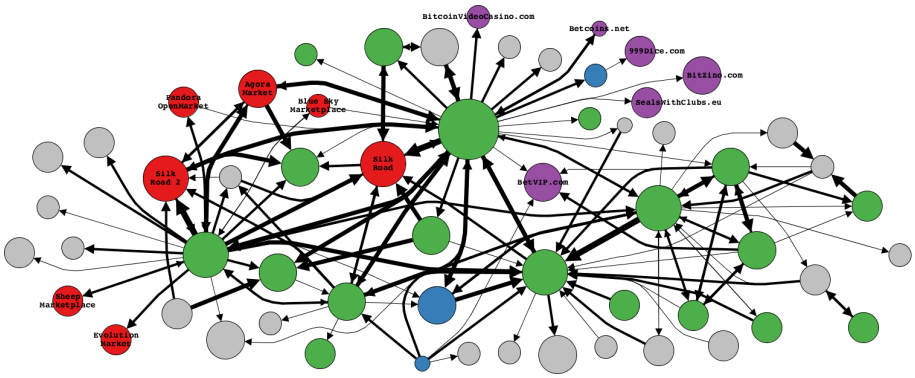
ευνόητο πώς σε μια συναλλαγή όπου εμφανίζεται μια νέα διεύθυνση καθώς και κάποια που επαναχρησιμοποιείται, η υπάρχουσα αφορά κάποια πληρωμή και η νέα χρησιμοποιείται για τα ρέστα. Ο εντοπισμός των διευθύνσεων που έχουν χρησιμοιηθεί είναι εντελώς διαδεδομένος. Υπάρχουν μάλιστα πολλές εφαρμογές, όπως είναι η ιστοσελίδα checkbitcoinaddress [28], όπου μπορεί να ελεγθεί αυτή η πληροφορία στιγμιαία για οποιαδήποτε διεύθυνση αναζητηθεί. Σημειώνεται πώς ακόμη και αν οι χρήστες δημιουργούν νέα διεύθυνση για κάθε συναλλαγή, ο κίνδυνος απώλειας της ανωνυμίας κάθε άλλο παρά εξαφανίζεται. Σε αυτό το συμπέρασμα κατέληξαν έρευνες, όπως αυτή των δημιουγών [5] των παραπάνω ευριστικών μέσα απο πείραμα σε πανεπιστήμιο, όπου το 40% των συναλλαγών εντοπίστηκε και ομαδοποιήθηκε με την χρήση απλών ευριστικών.

Οι παραπάνω μέθοδοι που περιγράψαμε ώς κυριότερες ευριστικές χρησιμοποιούνται σε συνδυασμό με την δομή του γράφου για να περιγράψουν τα συμπεράσματα που προκύπτουν και να φανερώσουν τις σχέσεις μεταξύ διευθύνσεων και συναλλαγών. Συγκεκριμένα, η ανάλυση της αλυσίδας του bitcoin σε γράφο υποθέτει πώς οι διευθύνσεις αποτελούν κόμβους και οι συναλλαγές είναι οι ακμές μεταξύ αυτών. Με την χρήση των ευριστικών οι διευθύνσεις ομαδοποιούνται (address clustering [29]) σε σύνολα που θεωρείται πως ανήκουν στην ίδια οντότητα. Η ψευδωνυμία, που όπως είπαμε παρέχει το bitcoin, εμποδίζει τον άμεσο συσχετισμό αυτών των οντοτήτων με άτομα ή σύνολα ατόμων. Ωστόσο, αν έστω και ένα μέρος του συνόλου των διευθύνσεων που έχουν ομαδοποιηθεί μπορεί να συσχετιστεί με πραγματικά άτομα, η ταυτοποίηση ολοένα και περισσότερων στοιχείων γίνεται δυνατή. Για το σκοπό αυτο αξιοποιούνται συμπληρωματικές μέθοδοι, όπως είναι δεδομένα στο επίπεδο δικτύου, πληροφορία απο τα μέσα κοινωνικής δικτύωσης, παράνομη ηλεκτρονική παρακολούθηση κτλ.

Έρευνες [30] αποδεικνύουν πώς απο τα πρώτα χρόνια μέχρι και σήμερα υπάρχουν εντοπισμένα clusters στα οποία ανήκουν χιλιάδες διευθύνσεις. Παράλληλα, η βιβλιογραφία [6, 7, 31] έχει καταδείξει τα βήματα ανάλυσης και εντοπισμού της ροής των κρυπτονομισμάτων μέσα απο ακολουθίες μεγάλου πλήθους συναλλαγών. Στην έρευνα τους χρησιμοποίησαν μεταξύ άλλων και γνωστά παραδείγματα, όπως αυτό των συναλλαγών που σχετίζονται με τις διευθύνσεις της παράνομης οργάνωσης Silk Road, της οποίας η εξάρθρωση οδήγησε σε κατάσχεση περισσότερων απο 50.000 bitcoins.

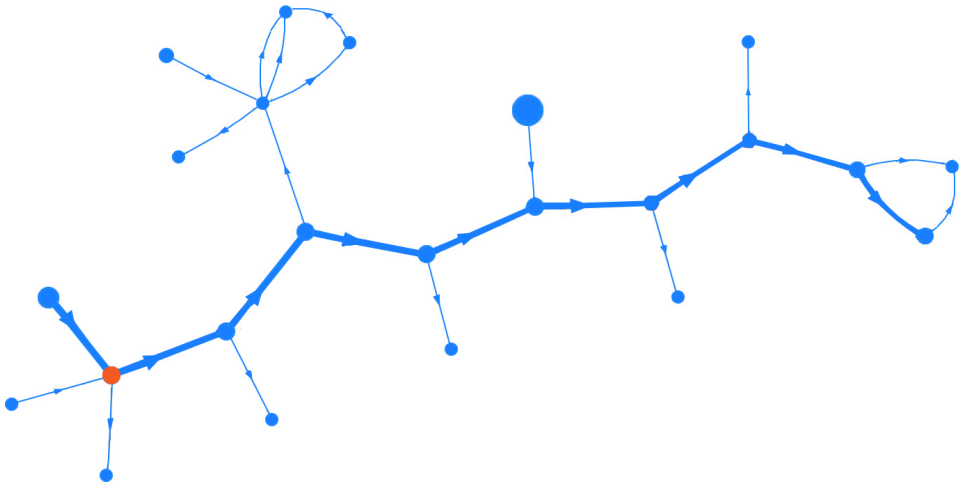
Υπάρχουν ποικίλες εφαρμογές ανάλυσης της αλυσίδας του bitcoin , όπως και παρόμοιων σε κατασκευή κρυπτονομισμάτων. Μερικές εξ αυτών, είναι το BitExtract [32], Blockchain Explorer [33], BitRef [34], Wallet explorer [35], chainanalysis [36] κ.α. Επιλέξαμε την εύχρηστη και δωρεάν διαθέσιμη εφαρμογή oxt.me [24] ώστε να παρατηρήσουμε την αποτελεσματικότητα των παραπάνω μεθόδων σε απλές περιπτώσεις. Με αυτόν τον τρόπο είδαμε σε πρακτικό επίπεδο, το πώς μπορεί να χρησιμοποιηθεί η δύναμη της πληροφορίας του bitcoin, όταν γίνει αναλυτική μελέτη και γίνουν οι όποιες πιθανές συνδέσεις μεταξύ των οντοτήτων.

Η δομή που χρησιμοποιεί η εφαρμοργή oxt.me, είναι αυτή του κατευθυνόμενου ακυκλικού



Σχήμα 2.6: Γραφική αναπαράσταση των σημαντικότερων clusters κατά τα 5 πρώτα χρόνια χρήσης του bitcoin [30]. Ενδεικτικά, οι κόκκινες διεθύνσεις ανήκουν στην αγορά του darknet, οι μόβ σε υπηρεσίες τζόγου, οι πράσινες σε exchanges και οι μπλέ σε «ομάδες εξόρυξης» (mining pools).

γράφου. Οι κόμβοι αναπαριστούν συναλλαγές και οι ακμές αποτελούν UTXOs. Το γραφικό περιβάλλον επιτρέπει την αναπαράσταση συναλλαγών και την παρατήρηση της χρήσης ευρυστικών και άλλων μεθόδων που απειλούν την ψευδωνυμία του bitcoin.



Σχήμα 2.7: Στην παραπάνω εικόνα φαίνεται ένα απλό παράδειγμα όπου ακολουθείται το peeling chain, την περίπτωση δηλαδή όπου ένα μεγάλο ποσό bitcoins, μειώνεται σταδιακά με συναλλαγές 2 εξόδων. Η μία έξοδος πρόκειται για πολύ μικρό ποσό, γεγονός που μας οδηγεί στο συμπέρασμα πώς πρόκειται για κάποια πληρωμή. Σε τέτοιες περιπτώσεις, ο προσδιορισμός των διευθύνσεων όπου επιστρέφουν τα ρέστα και η ομαδοποίηση τους ώς διευθύνσεις της ίδιας οντότητας, είναι προφανής.

Στην τελευταία υποενότητα θα συμπληρώσουμε το γνωστικό υπόβαθρο των σημαντικότερων κινδύνων ανωνυμίας, με εκείνους που εκμεταλλεύονται εξωτερικούς παράγοντες και μέσα πρός άντληση πληροφορίας.

2.2.3 Εναλλακτικές μέθοδοι επίθεσης στην ανωνυμία του bitcoin

- Μία μέθοδος συσχετισμού χρηστών με συναλλαγές είναι η παρατήρηση της χρονικής στιγμής επιβεβαίωσης μιας συναλλαγής απο το δίκτυο, σε σχέση με την αλληλεπίδραση τους

με συγκεκριμένες εφαρμογές και υπηρεσίες. Σε σχετική μελέτη [37] οι συγγραφείς χρησιμοποίησαν δεδομένα που αφορούν την υπηρεσία LocalBitcoins.com, οπού είναι δυνατή η αγοροπωλησία κρυπτονομισμάτων σε αντάλλαγμα με χρήματα και επιτρέπονται αντίστοιχες διαφημίσεις απο εγγεγραμμένους χρήστες. Μέσα απο συνδυασμο ευριστικών μεθόδων, ιδιαιτεροτήτων στις συναλλαγές και στις διευθύνσεις της υπηρεσίας LocalBitcoins.com καθώς και άντληση νόμιμων στοιχείων χρησιμοποιηθέντων διευθύνσεων απο forums και μέσα κοινωνικής δικτύωσης, δημιουργήθηκαν κατάλληλα datasets για εξαγωγή συμπερασμάτων. Κρίσιμο στοιχείο στην ερευνά τους ωστόσο ήταν η μελέτη των διαθέσιμων δεδομένων (απο το προσβάσιμο API της εφαρμογής) που αφορούν τις διαφημίσεις. Με βάση τον χρονικό προσδιορισμό δημοσίευσης και εκπλήρωσης προσφορών και των λοιπών πληροφοριών για τους χρήστες που αφορούν εξάχθηκαν επαρκή στοιχεία για να μειωθεί σημαντικά ο χώρος αναζήτησης ανταλλαγών της εφαρμογής, μέσα στο σύνολο των συναλλαγών της αλυσίδας του bitcoin.

- Ένας ακόμα τρόπος συσχετισμού διευθύνσεων και συναλλαγών με οντότητες είναι η χρησιμοποίηση της ποσότητας των συναλλαγών. Συγκεκριμένα, υπάρχουν υπηρεσίες, οι οποίες φανερώνουν σε ορισμένους χρήστες (ή διαχειριστές) πληροφορίες που αφορούν πληρωμές με χρήση χαρτονομισμάτων. Όταν αυτού του είδους οι πληρωμες οδηγούν σε συναλλαγές κρυπτονομισμάτων, bitcoins αντίστοιχης αξίας μεταφέρονται μεταξύ των διευθύνσεων και οι αντίστοιχες συναλλαγές αποθηκεύονται στο blockchain. Συνδυασμός αυτής της μεθόδου με άλλες ευριστικές (όπως αυτή του χρονικού συσχετισμού που είδαμε παραπάνω) ενδέχεται να οδηγήσει σε αρση ανωνυμίας. Η μέθοδος αυτή έχει αξιοποιηθεί επιτυχώς στην βιβλιογραφία [38], με σχετικό παράδειγμα την άντληση δεδομένων της πλατφόρμας ShapeShift [39]. Το API της εταιρίας αυτής παρέχει μεταξύ άλλων πληροφορίες για τις τελευταίες 50 συναλλαγές μεταξύ οποιονδήποτε χρηστών.

- Αξίζει να σημειώσουμε την ύπαρξη περισσότερων συμπεριφορών χρηστών, οι οποίες πολλές φορές αναπόφευκτα οδηγούν στην δυνατότητα εξαγωγής συμπερασμάτων για την ταυτότητα τους. Για παράδειγμα, απο τις εισόδους μια συναλλαγής, μπορεί να φανερωθεί το ελάχιστον πιθανό ποσό που έχει στην κατοχή του ο ιδιοκτήτης, όταν η διευθύνση επιστροφής είναι εύκολα προσδιορίσιμη. Επιπρόσθετα, συναλλαγές που ξεχωρίζουν για τις τιμές των παραμέτρων τους, είναι ευκολότερο να οδηγήσουν σε απώλεια ανωνυμίας. Τέτοια περίπτωση αποτελεί η χρήση ιδιαίτερου script. Ο πιο συνηθισμένος τύπος script είναι ο λεγόμενος «2-of-3 multi-sig». Ως multi-sig χαρακτηρίζονται τα scripts που απαιτούν υπογραφή απο τουλάχιστον 2 ιδιωτικά κλειδιά για την εκτέλεση μιας συναλλαγής. Επιπλέον, ο τύπος 2-of-3 υποδηλώνει πώς απαιτούνται μόνο 2 απο τις 3 υπογραφές.

- Στη συνέχεια είναι χρήσιμο να αναφέρουμε πώς η επιλογή του πορτοφολιού για τον εκάστοτε χρήστη είναι ιδιαίτερα σημαντική. Ασφαλώς, η ασφαλέστερη επιλογή είναι η χρησιμοποίηση συσκευών αποθήκευσης χωρίς σύνδεση στο διαδίκτυο. Τέτοια επιλογή γίνεται συνήθως απο επενδυτες που σκοπεύουν σε μακροπρόθεσμη διατήρηση των νομισμάτων τους. Σε τέτοιες περιπτώσεις, ο σημαντικότερος κίνδυνος είναι η απώλεια του μέσου αποθήκευσης. Τις περισσότερες φορές βέβαια η ταχύτητα και η διευκόλυνση που προσφέρουν τα online (ή αλλιώς «hot») πορτοφόλια αυξάνουν την χρήση τους, παρά το ρίσκο που τα συνοδεύει. Τα online πορτοφόλια [40], αποτελούν επιλογές όπου το βασικό χαρακτηριστικό είναι η έκθεση των κλειδιών του χρήστη στο διαδίκτυο. Το πιο συνηθισμένο παράδειγμα online πορτοφολιού είναι αυτό που παρέχουν συναλλακτικές υπηρεσίες, όπως είναι το Coinbase και το Crypto.com. Άλλη επιλογή αποτελεί το κατέβασμα εφαρμογής σε υπολογιστή ή και φορητή συσκευή. Η χρησιμοποίηση web πορτοφολιών είναι βέβαια αυτή με το μεγαλύτερο κίνδυνο. Επιπλέον, ένας βασικός διαχωρισμός των web πορτοφολιών είναι μεταξύ κηδεμονικά και μή. Τα κηδεμονικά πορτοφόλια ουσιαστικά απαλλάσσουν τον χρήστη απο την ανάγκη αποθήκευσης και ασφάλισης των κλειδιών του. Η εφαρμογή χειρίζεται την ασφάλεια τους, στην οποία δίνεται πλήρης έλεγχος. Σε τέτοιες περιπτώσεις

απαιτείται πλήρης εμπιστοσύνη στις προθέσεις της υπηρεσίας και των μεθόδων που χρησιμοποιεί. Γι αυτό και τέτοιες υλοποιήσεις θεωρείται πως έχουν την μικρότερη εν γένει ασφάλεια ως προς την ανωνυμία. Σε επόμενο κεφάλαιο θα δούμε πώς υλοποιήσεις πορτοφολιών ως λογισμικό προς κατέβασμα παρέχουν μεγαλύτερη ανωνυμία και τις τεχνικές που χρησιμοποιούν γι αυτόν τον σκοπό.

- Τέλος, σημαντικός είναι ο κίνδυνος που δημιουργείται απο πιθανές επιθέσεις ανωνυμίας, σε επίπεδο δικτύου. Η επικοινωνία μεταξύ των κόμβων του bitcoin γίνεται μέσω αποστολής πακέτων. Όπως υπέδειξε ο Dan Kaminsky το 2011 στο συνέδριο Black Hat, η γνώση των διευθύνσεων IP των κόμβων και της σειράς με την οποία λαμβάνονται πακέτα μπορούν να οδηγήσουν σε παραβίαση της ανωνυμίας. Συγκεκριμένα, ο πρώτος κόμβος που θα κοινοποιήσει μια συναλλαγή είναι σημαντικά πιθανότερο να την έχει δημιουργήσει [41]. Αν αυτή η πληροφορία ληφθεί απο πληθώρα συνεργαζόμενων κόμβων της επιτιθέμενης πλευράς, η άρση της ανωνυμίας καθίσταται εφικτή. Επίσης, η επιτυχής χρήση επιθέσων δικτύου και η παρακολούθηση της σύνδεσης χρηστών και των δεδομένων που ανταλλάσσουν με υπηρεσίες όπως web πορτοφόλια μειώνει την ασφάλεια δραματικά [42]. Ένα τέτοιο παράδειγμα αυξημένης επικινδυνότητας είναι η χρήση blockchain explorers (μηχανών αναζήτησης), για την εύρεση συναλλαγών η διευθύνσεων. Δημιουργείται συνεπώς η ανάγκη χρήσης εγγυημένα ανώνυμων συνδέσεων δικτύου, προς μεγαλύτερη ασφάλεια. Όπως θα δούμε στο επόμενο κεφάλαιο, μια απο τις επικρατέστερες λύσεις σε αυτό το πρόβλημα, είναι το Tor [43].

Κεφάλαιο 3

Μέθοδοι ενίσχυσής της ιδιωτικότητας στο bitcoin

Σε αυτό το κεφάλαιο θα παρουσιάσουμε τις μεθόδους ενίσχυσης της ιδιωτικότητας στην χρήση κρυπτονομισμάτων και ιδιαίτερα στο bitcoin. Θα επικεντρωθούμε στις τεχνικές που χρησιμοποιούνται για την αποφυγή των κινδύνων που παρουσιάστηκαν στο 2ο κεφάλαιο. Θα δώσουμε έμφαση στην καταπολέμηση των ευριστικών μεθόδων που βασίζονται στο blockchain του bitcoin και στον χειρισμό των διευθύνσεων με τον ασφαλέστερο δυνατό τρόπο. Θα παρουσιαστούν οι σημαντικότερες τεχνικές αποφυγής των κινδύνων που δημιουργούνται απο τον συσχετισμό μεταξύ συναλλαγών ή διευθύνσεων με οντότητες και πιθανούς κατόχους κρυπτονομισμάτων. Θα αναφερθούμε επίσης στα μέτρα προστασίας της ιδιωτικότητας εκτός του πλαισίου των συναλλαγών που αποθηκεύονται στην αλυσίδα. Σε αυτήν την κατηγορία ανήκουν οι τεχνικές που αφορούν στην απόκτηση και τον χειρισμό κρυπτονομισμάτων μέσω συναλλακτικών υπηρεσίων, την χρησιμοποίηση ασφαλούς και ανώνυμου δικτύου αλλά και επιπλέον μέτρα που αφορούν κυρίως εξορύκτες.

3.1 Εφαρμογές προστασίας της ανωνυμίας κατά τον χειρισμό και την μετάδοση δεδομένων

3.1.1 Αποστολή και χρήση κρυπτονομισμάτων

Ο βασικότερος τρόπος ενίσχυσης της ανωνυμίας στην χρήση κρυπτονομισμάτων είναι η αποφυγή υπηρεσιών που απαιτούν προσωπικές πληροφορές κατά την εγγραφή όπως είναι το όνομα, η ταυτότητα, το τηλέφωνο κ.α. Μέρος του ρόλου αυτών την υπηρεσιών θεωρείται η αποτροπή χρησιμοποίησης του bitcoin για εγκληματικούς σκοπούς αλλά και η διασφάλιση της τήρησης των σχετικών νόμων και κανονισμών. Η διαδικασία αυτή αναφέρεται ώς KYC (Know Your Customer) [44]. Η εφαρμογή της είναι διαδεδομένη στήν πλειονότητα των συναλλακτικών υπηρεσίων κατά την εγγραφή, στην δημιουργία χρεωστικών καρτών bitcoin όπως και στα bitcoin ATMs (μηχανές αντίστοιχες με τα ATMs των τραπεζών, όπου γίνονται αποκλειστικά μετατροπές μεταξύ κρυπτονομισμάτων και χρημάτων). Συνεπώς, για την διασφάλιση της ιδιωτικότητας προτείνεται η χρησιμοποίηση των πορτοφολιών που παρακάμπτουν τον έλεγχο προσωπικών δεδομένων.

Όσον αφορά την απόκτηση bitcoins μέσω αγοράς, υπάρχουν ορισμένοι απλοί τρόποι πληρωμής που επιτρέπουν την απόκρυψη πληροφοριών που θα μπορούσαν να φανερώσουν πληροφορίες για τον αποδέκτη των κρυπτονομισμάτων. Μια τέτοια μέθοδος είναι βέβαια η χρησιμοποίηση μετρητών αντί κάρτας. Μετρητά μπορούν ακόμη να χρησιμοποιηθούν σε κάποια bitcoin ATMs. Ομοίως, καλή επιλογή θεωρείται η απευθείας κατάθεση μετρητών στον λογαριασμό του πωλητή των κρυπτονομισμάτων (έναντι αμοιβής της εκάστοτε τράπεζας). Τέλος, κάποιοι χρήστες επιλέγουν ακόμα και την πληρωμή μέσω ταχυδρομείου. Για την εξυπηρέτηση της κοινότητας στην τέλεση αυτών των μεθόδων έχουν δημιουργηθεί υπηρεσίες όπως η Paxful [45] όπου δίνεται η δυνατότητα αγοραπωλησίας bitcoins με εκατοντάδες διαφορετικούς τρόπους. Ενδεικτικά, τέτοιοι τρόποι είναι: η κατάθεση μετρητών σε τράπεζα ή σε αντίστοιχη υπηρεσία (Amazon Cash, Western Union κ.α), η χρήση δωροκαρτών, ψηφιακών καρτών αλλά ακόμα και η αγοραπωλησία

με χρυσό.

Η απόκτηση κρυπτονομισμάτων μέσω εξόρυξης είναι επίσης θεωρητικά ασφαλής και παρέχει μερική ανωνυμία. Σημαντικοί ωστόσο παράγοντες που πρέπει να ληφθούν υπόψιν είναι η πιθανή παρατήρηση της ιδιαίτερα αυξημένης κατανάλωσης ενέργειας όπως και της αγοράς εξειδικευμένου εξοπλισμού. Παράλληλα ο μεγάλος ανταγωνισμός στην διαδικασία της εξόρυξης έχει οδηγήσει την πλειονότητα των χρηστών σε συμμετοχή ανά ομάδες, οι οποίες ονομάζονται «ομάδες εξόρυξης» (mining pools). Έτσι, η υπολογιστική ισχύς του κάθε χρήστη ενεργεί σε συνεργασία με τα υπόλοιπα μέλη της ομάδας και τα πιθανά κέρδη απο την επιτυχημένη εξόρυξη διαμοιράζονται ανάλογα με την υπολογιστική ισχύ που προσφέρει ο κάθε χρήστης. Η συμμετοχή σε ομάδες εξόρυξης πολλές φορές απαιτεί την αποκάλυψη προσωπικών στοιχείων. Το γεγονός αυτό σε συνδυασμο με την πολύ μικρή πιθανότητα επιτυχημένης εξόρυξης με ατομική συμμετοχή μειώνει σημαντικά την χρηστικότητα αυτής της μεθόδου ως προς την ανώνυμη απόκτηση κρυπτονομισμάτων.

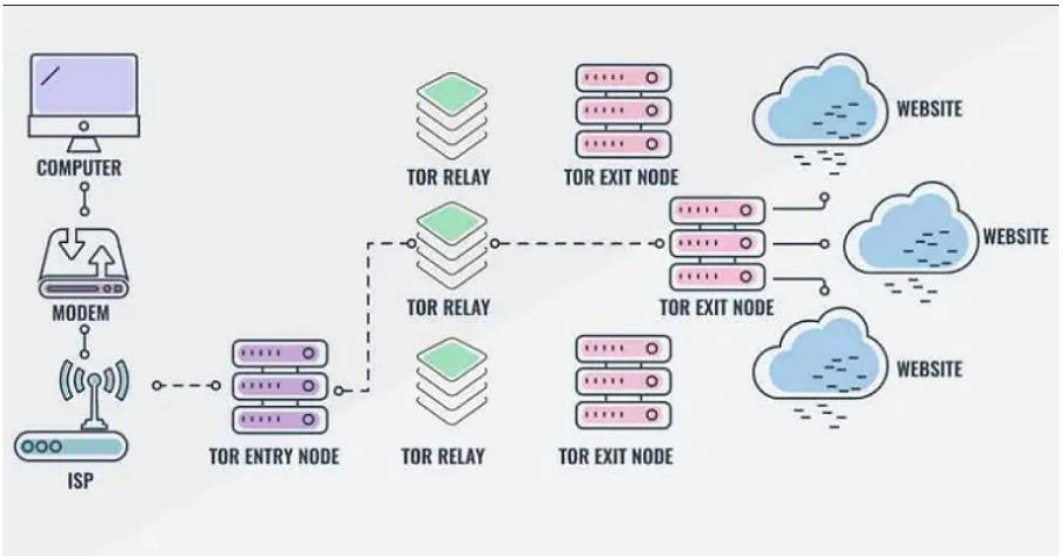
Όπως και κατά την αγορά κρυπτονομισμάτων, έτσι και στην αγορά αγαθών με χρήση bitcoins, ενδείκνυται η προσπάθεια απόκρυψης προσωπικών στοιχείων, όπως είναι η διεύθυνση και το email του εκάστοτε αγοραστή.

3.1.2 Συγχρονισμός δεδομένων

Συνεχίζωντας, ένα ζήτημα το οποίο είναι σημαντικό για την ιδιωτικότητα στο bitcoin αφορά τον τρόπο λήψης δεδομένων για τον συγχρονισμό του πορτοφολιού που χρησιμοποιεί ο εκάστοτε χρήστης. Για τον λόγο αυτό, περισσότερο ασφαλής επιλογή θεωρείται η χρησιμοποίηση «πλήρους» κόμβου [46]. Ως πλήρεις κόμβοι αναφέρονται οι εφαρμογές μέσω των οποίων πραγματοποιείται ενεργή συμμετοχή στην λειτουργία του bitcoin. Ρόλος τους είναι η συμμετοχή στην διάδοση των νέων συναλλαγών και blocks. Πρωτού προχωρήσουν στην αναμετάδοση τους κατεβάζουν και ανανεώνουν τακτικά ολόκληρο το ιστορικό της αλυσίδας και επαληθεύουν την εγκυρότητα των δεδομένων. Έτσι, καταργείται πλέον η ανάγκη χρησιμοποίησης εξωτερικών εφαρμογών για την επαλήθευση συναλλαγών και blocks. Ενισχύεται κατά αυτόν τον τρόπο η προστασία του χρήστη του πλήρους κόμβου απο επιθέσεις που αφορούν παρακολούθηση μέσω διεύθυνσης IP και κινήσεων που σχετίζονται με διαδικτυακή λήψη δεδομένων. Παρ'ολα αυτά, η συμμετοχή στην διάδοση της πληροφορίας και η λήψη των δεδομένων χρησιμοποιώντας διεύθυνση IP δεν εξαλείφουν πλήρως τον συγκεκριμένο κίνδυνο. Γι'αυτόν τον λόγο προτείνεται η εφαρμογή συμπληρωματικών μέτρων. Μια απο τις σχετικές διαδεδομένες μεθόδους αποτελούν τα VPNs (Virtual Private Networks). Το VPN [47] κρυπτογραφεί όλη την κίνηση και «κρύβει» τις διευθύνσεις IP. Παράλληλα προστατεύει το απόρρητο των δραστηριοτήτων και του ιστορικού περιήγησης. Έτσι μειώνεται σημαντικά το ενδεχόμενο παρακολούθησης τόσο απο hackers όσο ακόμα και απο υπηρεσίες παροχής διαδικτύου (ISPs). Λειτουργεί δρομολογώντας την εκάστοτε σύνδεση στο διαδίκτυο μέσω ενός απομακρυσμένου διακομιστή, ο οποίος ενδέχεται να βρίσκεται ακόμη και σε εντελώς διαφορετική περιοχή. Πρόκειται για τεχνολογία ευρέως χρησιμοποιούμενη και με χαμηλό κόστος.

Στο ίδιο πλαίσιο με την επιλογή του VPN και για ακόμα περισσότερη ασφάλεια, προτείνεται η χρήση του Tor (The Onion Router) [43]. Το Tor είναι μια τεχνολογία ενίσχυσης της ανωνυμίας που χρησιμοποιεί μια σειρά απο τυχαία επιλεγμένους servers για την δρομολόγηση συνδέσεων στο διαδίκτυο. Η διαχείριση του γίνεται απο εθελοντές και η αποτελεσματικότητα του στην απόκρυψη των διευθύνσεων IP είναι πολύ μεγάλη. Η ιδεά του Tor βασίζεται στην επιλογή ενός τυχαίου μονοπατιού πολλαπλών βημάτων για την σύνδεση με την διεύθυνση που επιθυμούμε. Μέσω αυτής της επιλογής παραβλέπεται η δυνατότητα απευθείας σύνδεσης με τον στόχο και προτιμάται η μείωση της πιθανότητας παρακολούθησης της κίνησης μας. Το όνομα «The Onion Router» προέρχεται απο την τεχνική Onion Routing. Πρόκειται για μια διαδικασία πολλαπλών επιπέδων (κρυπτογράφησης), στοιχείο που αποτέλεσε την αφορμή για τον ονομαστικό συσχετισμό με το κρεμμύδι. Σε κάθε επίπεδο της διαδικασίας, η πληροφορία (αίτημα σύνδεσης) μεταφέρεται απο έναν τυχαία επιλεγμένο κόμβο του δικτύου σε κάποιον επόμενο. Το συνολικό

μονοπάτι μέχρι τον προορισμό είναι άγνωστο στους ενδιάμεσους κόμβους, οι οποίοι λαμβάνουν μονάχα πληροφορία για τον προηγούμενο και τον επόμενο κόμβο στον οποίο καλούνται να περάσουν την «σκυτάλη». Σε κάθε βήμα χρησιμοποιείται ένα διαφορετικό σύνολο κλειδιών (με κρυπτογράφηση δημοσίου κλειδιού) δυσκολεύοντας σημαντικά οποιονδήποτε επιχειρήσει την ιχνηλάτηση αυτών των βημάτων. Το επίπεδο ασφάλειας που παρέχεται απο την χρήση του Tor θεωρείται υψηλότερο απο το VPN, ωστόσο έχει το μειονέκτημα της αργής σύνδεσης (λόγω των πολλών βημάτων λειτουργίας του). Για αυτό τον λόγο, όπως αναφέρεται στην βιβλιογραφία [48], κάποιες φορές γίνεται μερική χρήση του Tor, μονάχα δηλαδή για την διάδοση συναλλαγών και blocks και όχι για την λήψη του μεγάλου όγκου των δεδομένων που απαιτείται.



Σχήμα 3.1: Στην παραπάνω εικόνα φαίνεται ένα απλοποιημένο παράδειγμα του δικτύου δρομολόγησης συνδέσεων στο διαδίκτυο με χρήση του Tor. Ως κόμβος εισόδου (entry node) χαρακτηρίζεται ο κόμβος εκκίνησης της σύνδεσης με το Tor. Καθήκοντα του αποτελούν η αποκρυπτογράφηση του εξωτερικού επιπέδου κρυπτογράφησης που εφαρμόστηκε πρίν την εισαγωγή στο δίκτυο. Στην συνέχεια, η κίνηση μεταφέρεται μεταξύ ενός ή περισσότερων «middle nodes», όπου ακολουθείται η τεχνική του onion routing για την κρυπτογράφηση και την απαλλαγή απο ίχνη. Τέλος, ο κόμβος εξόδου (exit node) είναι υπέυθυνος για την αποκρυπτογράφηση και την σύνδεση με τον τελικο στόχο.

Ενδεικτικά, κάποια απο τα πορτοφόλια που κάνουν χρήση του Tor είναι το Bitcoin Core, το Wasabi Wallet, το Samourai Wallet κ.α. Όπως έχει αναφερθεί, τα 2 τελευταία εκ των παραπάνω πορτοφόλια δημιουργήθηκαν με κεντρικό σκοπό την επίτευξη ανωνυμίας στο bitcoin. Ως εκ τούτου, η χρήση του Tor είναι εγγενής. Όσον αφορά το Bitcoin Core, πρόκειται για την βασική υλοποίηση «πλήρους κόμβου» του bitcoin. Εκτός αυτού, εμπεριέχει ενσωματωμένό πορτοφόλι. Η βασική έκδοση του παρ'ολαυτά δεν χρησιμοποιεί κάποια ισχυρή τεχνική ενίσχυσης της ιδιωτικότητας. Για τον λόγο αυτό δημιουργήθηκε το Tor Bitcoin Core, όπου συνδυάζεται η βασική λειτουργία της εφαρμογής με την προστασία που παρέχει το Tor.

3.1.3 Προτεινόμενες μέθοδοι σε εξέλιξη

Υπάρχουν ποικίλες τεχνολογίες των οποίων η ενδεχόμενη εφαρμογή μπορεί να καταστεί καταλυτική για την ιδιωτικότητα κατά τη μεταφορά δεδομένων κίνησης του bitcoin. Μια τέτοια μέθοδος είναι το Private information retrieval (PIR) [49]. Το PIR αποτελεί πρωτόκολλο που επιτρέπει την λήψη δεδομένων απο κάποιον server χωρίς την φανέρωση οποιασδήποτε πληροφορίας. Η ενσωμάτωση του σε εφαρμογές όπως το bitcoin είναι ακόμα σε πειραματικό στάδιο, όπως

αναφέρεται στην βιβλιογραφία [50]. Τα τελευταία χρόνια έχει γίνει έρευνα σχετικά με τη μετάδοση δεδομένων του bitcoin απευθείας μέσω κεραίας. [51]. Υπάρχει μάλιστα σχετικά υλοποίηση στην αγορά [52] όπου ένα δίκτυο κεραιών αναμεταδίδει τα δεδομένα του bitcoin σε συμβατές κεραίες σε οποιοδήποτε μέρος του κόσμου. Πρόκειται για ιδιαίτερα υποσχόμενη τενχολογία της οποίας η διάδοση είναι ακόμη σε αρχικό στάδιο. Τέλος, η τεχνική Dandelion [53] είναι μια μέθοδος που επιδρά στον τρόπο διάδοσης των συναλλαγών μεταξύ των κόμβων του bitcoin. Στόχος αυτής της τεχνικής είναι η αντιμετώπιση μεθόδων παρακολούθησης της κίνησης και των συναλλαγών ενός κόμβου μέσω της διεύθυνσης IP. Λειτουργεί σε 2 βήματα τα οποία αποκαλούνται «stem phase» και «fluf phase». Στο πρώτο βήμα γίνεται «μερική» διάδοση των συναλλαγών σε τυχαία επιλεγμένα κόμβους και στο δεύτερο βήμα προχωρά στην διάδοση της συναλλαγής στο υπόλοιπο δίκτυο. Δυσχαιρένεται κατά αυτόν τον τρόπο η δυνατότητα παρακολούθησης του αποστολέα της κάθε συναλλαγής και παρέχεται ένα επιπλέον επίπεδο ασφάλειας στην ανωνυμία των χρηστών. Μέχρι τώρα το Bitcoin Core αποτελεί την κεντρική υλοποίηση που περιλαμβάνει αυτήν την τεχνική.

3.2 Αντιμετώπιση των ευριστικών μεθόδων επίθεσης στην ανωνυμία του bitcoin

Μέχρι τώρα περιγράψαμε διάφορες χρήσιμες μεθόδους ενίσχυσης της ανωνυμίας στο bitcoin. Επρόκειτο για περιπτώσεις που συνδέδονται με την μεταφορά και διάδοση δεδομένων απο το λογισμικό χρησιμοποίησης καθώς και την απόκρυψη προσωπικών δεδομένων. Για να επιτευχθεί ιδιωτικότητα ωστόσο στην χρήση του bitcoin απαιτείται η αντιμετώπιση των εγγενών προβλημάτων ανωνυμίας που δημιουργεί η διαθεσιμότητα συναλλαγών, διευθύνσεων και λοιπών δεδομένων μέσω του blockchain. Όπως είδαμε, η σύνθεση και ανάλυση τους αποτελεί αντικείμενο συστηματικής έρευνας. Έχουν δημιουργηθεί πολλά εξειδικευμένα εργαλεία ανάλυσης αλυσίδας που κάνουν χρήση ευριστικών μεθόδων και ιδιαιτεροτήτων της εκάστοτε υλοποίσης πορτοφολιού. Σε αυτήν την ενότητα λοιπόν θα μελετήσουμε τις σημαντικότερες και πιο σύγχρονες μεθόδους που χρησιμοποιούνται για την αντιμετώπιση αυτών των κινδύνων και συντείνουν στην διασφάλιση της ανωνυμίας. Θα αναφέρθουμε επίσης στις σημαντικότερες νέες μεθόδους για τις οποίες ερευνάται η δυνατότητα εφαρμογής στο bitcoin.

3.2.1 Επαναχρησιμοποίηση διευθύνσεων

Το πρόβλημα της επαναχρησιμοποίησης διευθύνσεων έχει τεθεί απο το ξεκίνημα του bitcoin. Ακόμη και στο white paper [1] του/της Nakamoto αναφέρεται πώς ένα νέο ζευγάρι κλειδιών θα πρέπει να δημιουργείται για κάθε συναλλαγή ώστε να μην γίνει σύνδεση αυτών με τον ίδιο ιδιοκτήτη. Έτσι, τα περισσότερα πορτοφόλια παρέχουν αυτόματες λειτουργίες δημιουργίας διεθύνσεων. Συγκεκριμένα, ο πιο συνηθισμένος τύπος πορτοφολιού αναφορικά με τρόπο δημιουργίας διευθύνσεων είναι ο ντετερμινιστικός. Πρώτη αναφορά στα ντετερμινιστικά πορτοφόλια έγινε απο τον Gregory Maxwell to 2011 [54]. Ο σχεδιασμός τους βασίζεται στην παραγωγή ενός αρχικού «σπόρου» κατά τη δημιουργία του πορτοφολιού μέσω του οποίου να μπορεί στην συνέχεια να δημιουργηθεί αυτόματα μεγάλος αριθμός διευθύνσεων. Ο σπόρος συνήθως είναι ένα σύνολο απο λέξεις (στις περισσότερες υλοποιήσεις αποτελείται απο 9 ή 12 τυχαίες λέξεις) που μπορούν επιπλέον να χρησιμοποιηθούν για την ανάκτηση του ιδιωτικού κλειδιού. Εξέλιξη των ντετερμινιστικών πορτοφολιών αποτελούν τα ιεραρχικά ντετερμινιστικά (hierarchical deterministic (HD) wallets) [55] των οποίων τα κλειδιά είναι οργανωμένα σε δομή δένδρου. Κάθε κόμβος του δένδρου αντιστοιχεί σε ένα ιδιωτικό κλειδί οπότε και μια διεύθυνση. Ο σπόρος των ντετερμινιστικών πορτοφολιών παράγεται κατά την πρώτη σύνδεση και δημιουργία ενός πορτοφολιού. Ο χρήστης καλείται συνήθως να επιλέξει έναν κωδικό και στην συνέχεια ενημερώνεται για το σύνολο των τυχαία παραγόμενων λέξεων που αντιστοιχούν στο νέο του πορτοφόλι. Η παραγωγή του σπόρου ακολουθεί συγκεκριμένα πρότυπα και γίνεται απο εξειδικευμένες συναρτήσεις, με την BIP32 [56]

να είναι περισσότερη διαδεδομένη. Αυτές οι συναρτήσεις δημιουργούν συνήθως ένα «master» ιδιωτικό κλειδί το οποίο αποτελεί ρίζα παραγωγής των υπολοίπων. Ο ακριβής τρόπος υλοποίησης τους ξεφευγεί απο τον σκοπό της εργασίας μας, αξίζει να αναφέρουμε ωστόσο πώς δεδομένου ενός master ιδιωτικού κλειδιού και λαμβάνοντας υπόψιν την ντετερμινιστική φύση αυτής της υλοποίησης, η ακολουθία κλειδιών που μπορεί να παραχθεί είναι μοναδική. Η απόκρυψη και αποθήκευση τόσο του κωδικού όσο και λέξεων του σπόρου έχει ασφαλώς μεγάλη σημασία για την ασφάλεια και την δυνατότητα χειρισμού ενός πορτοφολιού. Οι περισσότερες μοντέρνες υλοποιήσεις έχουν αυτόματα ενεργοποιημένη την επιλογή δημιουργίας νέας διεύθυνσης για τα ρέστα μια συναλλαγής. Παρέχουν επίσης την δυνατότητα άμεσης παραγωγής διευθύνσεων με τον τρόπο που περιγράψαμε και προτρέπουν τους χρήστες να δημιουργούν νέα διεύθυνση για κάθε τους κίνηση, χωρίς βέβαια να τους το επιβάλλουν.

Στα περισσότερα bitcoin πορτοφόλια η επιλογή των UTXOs που θα χρησιμοποιηθούν σε μια συναλλαγή γίνεται αυτόματα. Κατά αυτόν τον τρόπο οι συναλλαγές πραγματοποιούνται γρήγορα καθώς ελαχιστοποιούνται οι απαιτούμενες επιλογές απο τους χρήστες. Κάποια πορτοφόλια παρ'ολαυτα παρέχουν την δυνατότητα επιλογής των UTXOs που θα χρησιμοποιήσουν σε μια συναλλαγή. Έτσι, οι χρήστες με περισσότερη εμπειρία μπορούν να δίνουν μεγαλύτερη προσοχή στην τήρηση της ανωνυμίας τους. Η δυνατότητα αυτή ονομάζεται «έλεγχος νομισμάτων» («Coin Control») και παρέχεται σε πορτοφόλια με προσανατολισμό των ιδιωτικότητα όπως είναι το Wasabi αλλά και το Electrum.

3.2.2 Μυστικές διευθύνσεις

Με τον όρο «μυστικές διευθύνσεις» (stealth addresses [57]) αναφερόμαστε σε μια ακόμη μέθοδο που επικεντρώνεται στην ενίσχυση της ανωνυμίας των παραληπτών για τις συναλλαγές του bitcoin. Η δημιουργία αυτής της τεχνικής έγινε το 2013 στο πλαίσιο της υλοποίησης του «privacy coin» Monero. Απο τότε, κάποια πορτοφόλια όπως το Dark Wallet και το ShadowCash έχουν προχωρήσει σε ενσωμάτωση της. Η γενική ιδεά είναι πως χρησιμοποιείται ένα τυχαίο ιδιωτικό κλειδί το οποίο σε συνδυασμό με το υπάρχουν δημόσιο κλειδί μιας διεύθυνσης παράγει μια νέα δημόσια διεύθυνση μιάς χρήσης. Κατά την διάδοση της συναλλαγής και την εγγραφή της αλυσίδα το ιδιωτικό κλειδί μιας χρήσεως αποκρυπτογραφεί την πραγματική δημόσια διεύθυνση ώστε να γίνει σωστά η μεταφορά των νομισμάτων. Παρ'ολα αυτά, μόνο ο παραλήπτης της συναλλαγής γνωρίσει την πραγματική δημόσια διεύθυνση. Κατά αυτόν τον τρόπο ενισχύεται η ιδιωτικότητα του παραλήπτη, αφού δεν μπορούν να συσχετιστούν συναλλαγές στις οποίες είναι αποδέκτης. Η διάδοση αυτής της μεθόδου δεν είναι ιδιαίτερα μεγάλη. Πιθανά αίτια είναι η πολυπλοκότητα υλοποίησης της, η «μερική» ανωνυμία που προσφέρει (αφού δεν προστατεύει τους αποστολείς) αλλά και ο περιττός όγκος δεδομένων που προσθέτει στην αλυσίδα (με τις διευθύνσεις μιάς χρήσης) που μπορεί να επηρεάσει σε ταχύτητα και επεκτασιμότητα το συνολικό δίκτυο.

3.2.3 Υπογραφές δαχτυλιδιών

Οι «υπογραφές δαχτυλιδιών» (Ring Signatures) αναφέρθηκαν πρώτη φορά στην βιβλιογραφία απο τον Ronald Rivest [58] το 2001. Πρόκειται για μία μέθοδο υπογραφής που έχει στόχο της διατήρηση της ανωνυμίας του υπογράφοντος. Ταυτόχρονα, έχει αποκεντρωμένη φύση και δεν απαιτεί συντονισμό απο κάποια αρχή. Αφορά σε δομές που χρησιμοποιούν ζεύγη δημοσίου-ιδιωτικού κλειδιού όπως είναι και το bitcoin. Για την δημιουργία των κλειδιών, είναι δυνατή η χρήση τυπικά χρησιμοποιούμενων σχετικών αλγορίθων όπως έιναι ο RSA και ο ESDSA. Σύμφωνα με την βιβλιογραφία [59, 60], η γενική ιδεά είναι η χρησιμοποίηση ενός συνόλου δημοσίων κλειδιών ώστε να είναι δύσκολος ο ακριβής εντοπισμός του δημοσίου κλειδιού που ευθύνεται για την αποστολή ενός μηνύματος (ή την υπογραφή μια συναλλαγής στην περίπτωση του bitcoin). Τέτοιες υλοποιήσεις φροντίζουν ώστε η πληροφορία να υπογράφεται με χρήση του σωστού ιδιωτικού κλειδιού και να επαληθεύεται απο όποια συνάρτηση ελέγχου εφαρμόζεται κατά την διάδοση

της κίνησης. Η πιο διαδεδομένη χρήση των υπογραφών δαχτυλιδιών είναι απο το κρυπτονόμισμα Monero και το πρωτόκολλο RingCT. Όπως και στην περίπτωση των stealth addresses, παρ'ότι υπάρχουν αρκετές προτάσεις [59, 61] και πιθανά λειτουργικές υλοποιήσεις που συνδυάζουν την χρήση των υπογραφών δαχτυλιδιών με άλλα πρωτόκολλα ενίσχυσης της ανωνυμίας του bitcoin, η ενσωμάτωση τους δεν είναι διαδεδομένη. Το γεγονός αυτό πιθανόν να οφείλεται στον υπολογιστικά ακριβό αλγόριθμο τους και την σημαντική αύξηση του μεγέθους των δεδομένων που προκαλλούν.

3.2.4 Εμπιστευτικές συναλλαγές

Ο όρος «εμπιστευτική συναλλαγή» (confidential transaction) αναφέρεται σε πρωτόκολλα που παρέχουν τη δυνατότητα απόκρυψης ποσών κατά τη τέλεση συναλλαγών. [62]. Η ιδέα βασίζεται στην χρησιμοποίηση «ομομορφικής» κρυπτογράφησης (homomorphic encryption), κατά την οποία η κρυπτογράφηση των δεδομένων δεν εμποδίζει την επαλήθευση της εγκυρότητας και την τέλεση όποιων αναγκαίων ελέγχων απαιτούνται στο εκάστοτε πεδίο χρήσης τους. Για την περίπτωση λοιπόν των συναλλαγών, η ομομορφική κρυπτογράφηση επιτρέπει την πρόσθεση και επικύρωση των ποσών που μεταφέρονται, ενώ αυτά παραμένουν κρυπτογραφημένα. Ο Maxwell [63] εισήγαγε τις εμπιστευτικές συναλλαγές όπου οι ποσότητες εισόδου και εξόδου «κρύβονται» μέσα σε δεσμεύσεις Pedersen (Pedersen commitments) [64], μιά ειδική μέθοδο ομομορφικής κρυπτογράφησης. Σε αυτή τη μέθοδο γίνεται χρήση συνάρτησης κατακερματισμού με εισόδους το μήνυμα πρός κρυπτογράφηση και μια τυχαία τιμή, για την παραγωγή μιας δέσμευσης, μιας υπόσχεσης δηλαδή που είναι επαληθεύσιμη παρ'ότι δεν φανερώνει πληροφορίες για το αρχικό μήνυμα. Στο πλαίσιο των εμπιστευτικών συναλλαγών και του bitcoin, οι δεσμεύσεις Pedersen μπορούν να εφαρμοστούν στην απόκρυψη τόσο των ποσών στις εισόδους μια συναλλαγής όσο και στις εξόδους. Παρά τα προφανή πλεονεκτήματα στην διατήρηση της ανωνυμίας που παρέχουν οι εμπιστευτικές συναλλαγές, η εφαρμογή τους στο bitcoin απαιτεί «soft fork». Με τον όρο «soft fork» αναφέρεται οποιαδήποτε μεγάλη τροποποίηση του πρωτοκόλου του bitcoin. Για να εφαρμοστεί μια αλλαγή, απαιτείται η συλλογική αποδοχή και η ενημέρωση της έκδοσης του bitcoin που χρησιμοποιείται απο την πλειοψηφία κατοχής της συνολικής ισχύος εξόρυξης (mining power). Όταν μάλιστα η αλλαγή επιφέρει τόσο μεγάλα αποτελέσματα όσο η απόκρυψη των ποσών στις συναλλαγές, η κοινότητα συμπεριφέρεται με δυσπιστία. Οι εμπιστευτικές συναλλαγές εφαρμόζονται σε κρυπτονομίσματα με ιδιότητες αυξημένες ιδιωτικότητας όπως είναι το Monero. Όσον αφορά όμως το bitcoin, η μόνη σχετική υλοποίηση σε λειτουργία είναι αυτή του Liquid Network [65]. Το Liquid Network αποτελεί «παράπλευρη αλυσίδα» (sidechain) του bitcoin. Ως «παράπλευρες αλυσίδες» περιγράφονται υλοποιήσεις blockchain συνδεδεμένες με κάποια άλλη αλυσίδα, απο την οποία μπορεί να γίνει μεταφορά περουσιακών στοιχείων και να χρησιμοποιηθούν ανεξάρτητα. Βασικό πλεονέκτημα τέτοιων υλοποιήσεων είναι η δυνατότητα δοκιμής νέεων λειτουργιών και πρωτοκόλλων χωρίς να επηρεάζεται η κύρια αλυσίδα. Κατά αυτόν τον τρόπο και το Liquid Network επωφελείται απο την ασφάλεια και την αξιοπιστία του bitcoin. Εμφανίζει ωστόσο τα δικά του σοβαρά μειονεκτήματα αφού η χρήση του επιφέρει επιπλέον κόστος, ενώ δεν είναι αποκεντρωμένο, οπότε και παραβιάζεται τόσο η ασφάλεια όσο και η ιδιωτικότητα στην χρήση του. Τέλος, ανασταλτικός παράγοντας στην πιθανότητα αποδοχής των εμπιστευτικών συναλλαγών απο την κοινότητα του bitcoin αποτελεί η μεγάλη αύξηση (τριπλάσιες) του μεγέθους των συναλλαγών που επιφέρει.

3.2.5 Zero-knowledge proofs και zk-SNARKs

Με τον όρο «αποδείξεις μηδενικής γνώσης» (Zero-knowledge proofs ή ZKPs) αναφέρονται στη βιβλιογραφία ένα σύνολο μεθόδων ανωνυμοποίησης με προοπτική ενσωμάτωσης στη χρήση του bitcoin. Σύμφωνα με την βιβλιογραφία [66] υπάρχουν δύο συμμετέχοντες: Το άτομο που θέλει να αποδείξει την εγκυρότητα κάποια συνθήκης (αποδεικνύων) και το άτομο που αναλαμβάνει τον έλεγχο και την επικύρωση της. Στόχος είναι η ολοκλήρωση της διαδικασίας χωρίς

την φανέρωση οποιασδήποτε επιπλέον πληροφορίας για τον αποδεικνύοντα. Οι τεχνικές που χρησιμοποιούνται στις αποδείξεις μηδενικής γνώσης ποικίλλουν, αλλά συχνά περιλαμβάνουν έννοιες όπως κρυπτογραφία ελλειπτικής καμπύλης, συναρτήσεις κατακερματισμού και θεωρία αριθμών. Όπως και στις εμπιστευτικες συναλλαγές, το πεδίο πιθανής χρήσης του στο bitcoin αφορά την υπογραφή και τέλεση συναλλαγών με ανώνυμο τρόπο. Ως γνωστόν, για την τέλεση μιας συναλλαγής στο bitcoin φανερώνονται τόσο οι διευθύνσεις απο τις οποίες προέρχονται τα UTXOs εισόδου όσο και οι διευθύνσεις αποστολής αλλά και οι ποσότητες. Η διάθεση όλων αυτών των δεδομένων θα μπορούσε να αποφευχθεί με την χρήση των ZKPs. Η πρώτη υλοποίηση και ενσωμάτωση σε κρυπτονόμισμα έγινε με τη δημιουργία του κρυπτονομίσματος Zcash [67]. Η συγκεκριμένη μέθοδος ονομάστηκε zk-SNARK's. Στο Zcash εκτελείται η παραγωγή ενός αποδεικτικού κατά την τέλεση συναλλαγών. Η απόδειξη δημιουργείται χρησιμοποιώντας έναν συνδυασμό αλγορίθμων και μπορεί να επαληθευτεί αποτελεσματικά, διασφαλίζοντας ότι η συναλλαγή είναι έγκυρη χωρίς να εκτίθενται ευαίσθητες πληροφορίες για τον αποστολέα. Το αποδεικτικό παράγεται με χρήση του δημοσίου κλειδιού της εκάστοτε διεύθυνσης και κρυπτογραφείται με το ιδιωτικό. Το σημαντικότερο μειονέκτημα αυτής της μεθόδου είναι η μεγάλη χρήση υπολογιστικής ισχύος και κατά συνέπεια το κόστος που απαιτείται. Επιπρόσθετα, εχει αμφισβητηθεί η δυνατότητα ομαλής επέκτασης της στο δίκτυο του bitcoin. Πρόκειται για ένα πεδίο όπου εξελίσσεται διαρκής έρευνα στον τομέα της κρυπτογραφίας.

3.2.6 Βελτίωση των Scripts

Ένας ακόμη τρόπος ενίσχυσης της ιδιωτικότητας στο bitcoin είναι η βελτίωση των scripts ώστε να μην είναι δυνατή η συσχέτιση συναλλαγών λόγω τών χαρακτηριστικών τους. Γι'αυτόν τον σκοπό έχουν προταθεί ποικίλες μέθοδοι. Μια πρόσφατη προσθήκη είναι η συμπλήρωση του πρωτοκόλλου ECDSA με τις υπογραφές Schnorr. Πρόκειται για ένα σχήμα ψηφιακών υπογραφών που προσφέρει σημαντικά οφέλη. Μάλιστα, είναι μια μέθοδος που δημιουργήθηκε πρίν απο το ECDSA, ωστόσο τα δικαιώματα ευρεσιτεχνίας ήταν κατοχυρωμένα κατά τη περίοδο δημιουργίας του bitcoin και μέχρι πρότεινως δεν υπήρξε τυποποίηση της μεθόδου. Πρόκειται για ένα σύνθετο πρωτόκολλο που χρησιμεύει ιδιαίτερα στην περίπτωση πολλαπλών υπογράφών στην ίδια συναλλαγή. Το πλεονέκτημα εμφανίζεται τόσο στις υπογραφές διαφορετικών εισόδων UTXOs όσο και στην ίδια είσοδο, όταν απαιτείται παραπάνω απο μία υπογραφή για την τέλεση συναλλαγής. Με απλά λόγια, επιτυγχάνεται ή ενοποιήση όλων των υπογραφών, ώστε να φαίνονται σαν μια κοινή. Έτσι, μειώνεται σημαντικά το μέγεθος της συναλλαγής στην αλυσίδα ενώ ενισχύεται η ιδιωτικότητα των υπογραφόντων. Οι υπογραφές Schnorr προστέθηκαν στο bitcoin με το τελευταίο σημαντικό soft fork που ονομάστηκε Taproot [68].

Με το Taproot η κοινότητα του bitcoin εκμεταλεύεται την γραμμικότητα των υπογραφών Shnorr (που έχει ώς αποτέλεσμα τη δυνατότητα συγκέντρωσης πολλών υπογραφών διατηρώντας την εγκυρότητα τους) και χρησιμοποιεί σε συνδυασμό τα δέντρα Merkle για να γίνουν οι υπογραφές συναλλαγών πιο αποτελεσματικές. Τα Merkle trees (ή αλλιώς Binary hash trees) [69, 70] αποτελούν μια ιδιαίτερα αποδοτική και χρήσιμη δομή. Πρόκειται για εφεύρεση του Ralph Merkle η οποία αναπαρίσταται απο ένα δυαδικό δένδρο. Το δέντρο Merkle στην περίπτωση των υπογραφών χρησιμοποιείται για να αναπαραστήσει ένα σύνολο πιθανών συνθηκών, ενώ μια μεμονωμένη υπογραφή Schnorr χρησιμοποιείται για να αποδείξει τη γνώση ενός ιδιωτικού κλειδιού εκ των χρησιμοποιηθέντων στο σύνολο τών συνθηκών. Σημειώνουμε πώς τα Merkle trees χρησιμοποιούνται και σε άλλες περιοχές του bitcoin, με την πιο σημαντική να είναι στη δομή των συναλλαγών στο εκάστοτε block της αλυσίδας.

Οι υπογραφές Schnorr ανοίγουν τον δρόμο για την υλοποίηση επιπλέον μεθόδων απλοποίσης των scripts που χρησιμοποιούνται στο bitcoin. Μιά τέτοια μέθοδος είναι τα «Scriptless» scripts [71]. Στην παρουσίαση του ο Poelstra περιέγραψε την μεθοδολογία που ελαχιστοποιεί τα δεδομένα που γράφονται στα scripts του bitcoin, ώστε να εμφανίζονται στην αλυσίδα μονάχα τα δημόσια κλειδιά και οι υπογραφές. Μια αρχική και απλοποιημένη έκδοση των scriptless scripts (Pay-to-Taproot (P2TR)) περιλαμβάνεται στο Taproot update. Αν και δεν πρόκειται

για την υλοποίση επακριβώς του αλγορίθμου του Poelstra, είναι ένα σημαντικό βήμα προς την κατεύθυνση της ανωνυμοποίησης κατά τις υπογραφές συναλλαγών στο bitcoin.

3.2.7 Off-chain transactions - Lightning Network

Με τον όρο «off-chain» transactions για το bitcoin αναφερόμαστε στις συναλλαγές που λαμβάνουν χώρα εκτός αλυσίδας. Ο βασικός μηχανισμός προυποθέτει την δέσμευση ποσών bitcoins για το «άνοιγμα» καναλιών όπου μπορούν να εκτελούνται συναλλαγές εκτός αλυσίδας. Μία απο τις πιο δημοφιλείς υλοποιήσεις είναι αυτή του Lightning Network [72], όπου δίνει έμφαση στην πολύ γρήγορη εκτέλεση μικροπληρωμών κρατώντας τις περισσότερες εκ των συναλλαγών εκτός αλυσίδας [73]. Σε αυτές τις υλοποιήσεις, τα δεδομένα που τελικά γράφονται στην αλυσίδα με το κλείσιμο του καναλιού είναι ελάχιστα και καθορίζουν την τελική κατανομή των δεσμευμένων νομισμάτων ακολουθώντας τα πρωτόκολλα ελέγχουν των συναλλαγών του bitcoin. Αυτές οι λύσεις έχουν την προοπτική να παρέχουν ιδιαίτερα αυξημένη ιδιωτικότητα στους χρήστες οι οποίοι θα απαλλαγούν απο τους κινδύνους ιχνηλάτησης των κινήσεων τους με την χρήση ευριστικών. Πρέπει ωστόσο να έχουμε υπόψιν πως πρόκειται για νέα τεχνολογία η οποία δεν έχει ακόμη δοκιμαστεί επαρκώς. Ως εκ τούτου ενδέχεται να δημιουργέι διαφορετικούς κινδύνους στην παραβίαση της ανωνυμίας και της ασφάλειας ανάλογα με τον τρόπο διαχείρισης των καναλιών της εκάστοτε υλοποίησης.

3.2.8 Συγκεντρωτικές Υπηρεσίες Μίξης

Απο τα πρώτα χρόνια διάδοσης του bitcoin, ο πιο δημοφιλής τρόπος ενίσχυσης της ανωνυμίας στις συναλλαγές ήταν η χρησιμοποίηση των λεγόμενων «υπηρεσιών μίξης» [9]. Πρόκειται για online υπηρεσίες που συνήθως αποκαλούνται «tumblers» και προσφέρουν την δυνατότητα ανάμιξης νομισμάτων με άλλους χρήστες. Αυτό σημαίνει πρακτικά την αποστολή νομισμάτων στην υπηρεσία μίξης με την υπόσχεση πώς εκείνη θα στείλει πίσω τα νομίσματα, σε μια νέα διεύθυνση. Η υπηρεσία κάνει το ίδιο για πολλούς χρήστες και στην συνέχεια ανακατανέμει τα νομίσματα.

Σε αυτό το σημείο έχει σημασία να εξηγήσουμε κάποιες λεπτομέρειες σχετικά με την λειτουργία των υπηρεσιών μίξης. Οι υπηρεσίες μίξης κάνουν χρήση του ότι το bitcoin επιτρέπει συναλλαγές με πολλές εισόδους και πολλές εξόδους. Λειτουργούν σε γύρους και κάθε γύρος αντιστοιχεί σε μια συναλλαγή. Κάθε είσοδος της είναι ουσιαστικά ένα UTXO. Στην ίδια συναλλαγή ενδέχεται να συμμετέχουν UTXOs απο την ίδια οντότητα μέσω της ίδιας διεύθυνσης ή και διαφορετικών. Για την περιγραφή των υπηρεσιών μίξης θα κάνουμε την παραδοχή πώς οι συμμετέχουσες είσοδοι δεν συνδέονται άμεσα μεταξύ τους μέσω κάποιας προηγούμενης συναλλαγής και δεν προέρχονται απο την ίδια διεύθυνση. Στο επόμενη κεφάλαιο όμως θα δώσουμε έμφαση μεταξύ άλλων και στις συνέπειες που προκύπτουν όταν αυτή η παραδοχή δεν ισχύει. Σε κάθε γύρο μίξης λοιπόν συμμετέχουν πολλαπλές είσοδοι. Κάθε οντότητα που συμμετέχει (άτομο ή ομάδα ατόμων) λαμβάνει στην διεύθυνση εξόδου της επιλογής της τα «καθαρά» νομίσματα που έχουν αναμιχτεί. Σε όλες σχεδόν τις σύγχρονες υλοποιήσεις ο γύρος μίξης λαμβάνει χώρα σε μια μόνο συναλλαγή.

Τόσο οι είσοδοι όσο και οι έξοδοι της συναλλαγής εμφανίζονται στην αλυσίδα ενώ τα δεδομένα για τις διευθύνσεις και τα ποσά που μεταφέρθηκαν είναι επίσης διαθέσιμα. Είναι λοιπόν ευνόητο πως αν οι έξοδοι που παράγονται έχουν διακριτές τιμές μεταξύ τους, τότε πολύ εύκολα μπορεί να γίνει αντιστοίχιση τους σε εισόδους. Αν δηλαδή επιτρεπόταν η μίξη διαφορετικών τιμών στον ίδιο γύρο για την διευκόλυνση των χρηστών, τότε θα ήταν πολύ εύκολο να αντιστοιχιστεί μεγάλο μέρος των UTXOs εξόδου με τις διευθύνσεις απο τις οποίες προήλθαν τα νομίσματα και να ακυρωθεί η προσπάθεια διατήρησης της ιδιωτικότητας. Για να είναι αποτελεσματική λοιπόν αυτή η μέθοδος απαιτείται κάθε έξοδος της συναλλαγής απο αυτές που «καθαρίζουν» νομίσματα να είναι της ίδιας ποσότητας. Ασφαλώς, αυτό δημιουργεί την δυσκολία του να βρεθούν αντίστοιχες είσοδοι των οποίων το άθροισμα να ισοδυναμεί επακριβώς με το ποσό επιλογής της

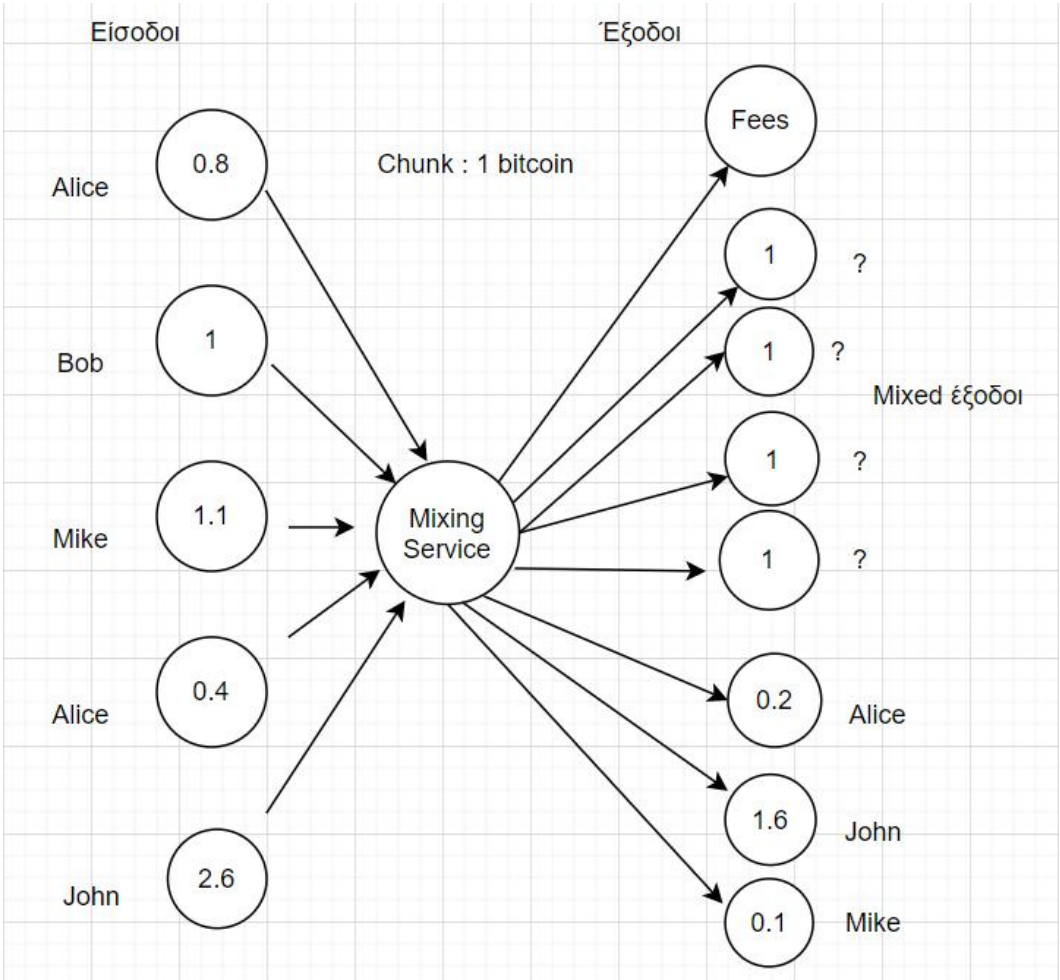
υπηρεσίας μίξης για τον κάθε πιθανό συμμετέχοντα. Οι περισσότερες υπηρεσίες λοιπόν έχουν υιοθετήσει την επιλογή μιας σειράς απο τυποποιημένα ποσά, «chunk sizes», τα οποία αποτελούν ποσότητες ικανές για την συμμετοχή σε κάποιον γύρο μίξης. Συνήθως τα chunk sizes κυμαίνονται σε υποδιαιρέσεις του bitcoin, με υποδιαιρέσεις της μονάδας όπως 0,01 και 0,001 να είναι ιδιαίτερα συνηθισμένες. Όταν λοιπόν όλες οι έξοδοι είναι της ίδιας ποσότητας λέμε πώς επιτυγχάνεται «anonymity set» (πλήθος ανωνυμίας) ίσο με το πλήθος αυτών των εξόδων. Αυτό σημαίνει για κάθε είσοδο της συναλλαγής πώς δεν μπορεί να αντιστοιχιστεί με κάποια συγκεκριμένη εκ των ίδιας αξίας UTXOs εξόδου. Μπορεί μονάχα να δοθεί πιθανότητα ίση με $\frac{1}{anonymitySet}$ αντιστοίχισης με οποιαδήποτε εξ αυτών. Στις περισσότερες περιπτώσεις οι είσοδοι που υποβάλλουν οι χρήστες είναι ποσοτικά μεγαλύτερες απο το προβλεπόμενο ποσό πρός μίξη. Επομένως, και σε περίπτωση δηλαδή που το σύνολο των εισόδων που συνεργάζονται για την παραγωγή μιας εξόδου καταθέτει UTXOs αθροιστικής αξίας μεγαλύτερης του chunk size, τότε δημιουργείται εποπλέον έξοδος ενός ποσού για τα ρέστα, σε διεύθυνση επιλογής του εκάστοτε αποστολέα. Είναι ασφαλώς σημαντικό η διεύθυνση αυτή να είναι επίσης νέα και αχρησιμοποίητη, ωστόσο σε κάθε περίπτωση το υπολοιπόμενο ποσό που στέλνεται εκεί δεν θεωρείται καθαρό, αφού εν γένει μπορεί εύκολα να αντιστοιχιστεί στην είσοδο απο την οποία προήλθε.

Στο παρακάτω σχήμα (3.3) παρουσιάζεται ένα απλοποιημένο παράδειγμα. Στον συγκεκριμένο γύρο υπάρχουν 4 συμμετέχοντες. Οι 3 εξ αυτών παρέχουν UTXO απο 1 διεύθυνση ώς είσοδο ενώ η Alice συνδυάζει 2 UTXOs αποθηκευμένα σε διαφορετικές διευθύνσεις. Για απλότητα θεωρούμε πώς τα fees είναι μηδενικά. Για την τέλεση της μίξης οι συμμετέχοντες εμπιστεύονται την υπηρεσία για την ανακατανομή των νομισμάτων τους και παρέχουν τις διευθύνσεις στις οποίες επιθυμούν την αποστολή τους. Ο Bob ήταν ο μόνος που συμμετείχε με είσοδο ίση με το chunk size (1 bitcoin). Οι υπόλοιποι χειάστηκε να παρέχουν διευθύνσεις για τα ρέστα τους, οι οποίες εύκολα αντιστοιχίζονται στους ιδιοκτήτες τους. Οι 4 ίσες έξοδοι αποτελούν τα καθαρά UTXOs τα οποία πλέον δεν μπορούν να αντιστοιχιστούν στους ιδιοκτήτες τους. Δεδομένου πώς οι έξοδοι αυτές είναι 4 (anonymity set size) η θεωρητική πιθανότητα αντιστοίχης της κάθε μίας σε κάποιον απο τους συμμετέχοντες είναι $\frac{1}{4} = 25\%$. Οι συμμετέχοντες συνήθως είναι πάνω απο 50 ενώ το fee υπολογίζεται απο το πλήθος τους, το οποίο ουσιαστικά καθορίζει το βαθμό ανωνυμίας που προσφέρει ο γύρος μίξης.

Η τεχνολογία της «ανάμιξης» των νομισμάτων που περιγράψαμε είναι απο τις πιο αποτελεσματικές μεθόδους ενίσχυσης της ιδιωτικότητας στο bitcoin. Παρουσιάζει ωστόσο σημαντικά προβλήματα. Οι συμμετέχοντες εμπιστεύονται τα νομίσματα τους σε μια υπηρεσία κεντροποιημένη και συγκεντρωτική. Το ρίσκο αυτό είναι τεράστιο και παραβιάζει τις βασικές αρχές της αποκεντρωμένης φύσης του bitcoin. Ο κίνδυνος προκύπτει τόσο απο τις πιθανές κακόβουλες προθέσεις της εκάστοτε εταιρίας [74] όσο και απο την ανεπαρκή διαχείριση στο τομέα της ασφάλειας που ενδέχεται να οδηγήσει σε παραβίαση και κλοπές [75]. Παράλληλα, η συμμετοχή σε υπηρεσία μίξης προϋποθέτει την ταυτοποίηση του χρήστη και την αποθήκευση προσωπικών δεδομένων του στο σύστημα της εταιρίας. Έτσι προκύπτει ανεπανόρθωτη ζημιά στην ιδιωτικότητα των χρηστών και χάνεται η ουσία της χρήσης τέτοιων υπηρεσιών. Σε κάποιες περιπτώσεις οι εταιρίες υπόσχονται την ορθή και τίμια διαχείριση των προσωπικών δεδομένων, γεγονός που αποτελεί ουσιαστικά «υπόσχεση» και όχι συνθήκη που μπορεί να θεωρηθεί δεδομένη. Σημειώνουμε πώς υπάρχουν κάποιες προτάσεις, όπως αυτή του BlindCoin [76], που μειώνουν σημαντικά το ρίσκο κλοπής, χωρίς ωστόσο να παρέχουν λύση στο εγγενές πρόβλημα της ανωνυμίας που συνοδεύει της συγκεντρωτικές υλοποιήσεις. Αξιοσημείωτη είναι επίσης η υλοποίηση του TumbleBit [77] η ποία παρέχει ισχυρές εγγύησεις ιδιωτικότητας αλλά όχι και ασφάλειας.

Συμπαιρένουμε επομένως πώς παρά τα πλεονεκτήματα αυτής της μεθόδου στην αύξηση της δυσκολίας ιχνηλάτησης της αλυσίδας, έχει μεγάλα μειονεκτήματα που καθιστούν την χρήση της ιδιαίτερα επικίνδυνη τόσο για την ανωνυμία όσο και για την ασφάλεια των περουσιακών στοιχείων την χρηστών της.

Κάπως έτσι δημιουργήθηκε η ανάγκη βελτίωσης αυτής της μεθόδου και εξάλειψης των παραγόντων που υποσκάπτουν την λειτουργία της. Η απάντηση δόθηκε με την τεχνική CoinJoin. Το



Σχήμα 3.2: Στην εικόνα παρουσιάζουμε ένα απλοποιημένο παράδειγμα μίξης μέσω υπηρεσίας.

CoinJoin αποτελεί υλοποίηση μίξης που αντικαθιστά την ύπαρξη κεντροποιημένες υπηρεσίας με ένα δίκτυο ομότιμων κόμβων. Εξαλείφεται έτσι η ανάγκη εμπιστοσύνης σε τρίτη υπηρεσία και οι συμμετέχοντες στο CoinJoin γύρο μίξης υπογράφουν την χρήση των νομισμάτων τους με πλήρη ασφάλεια και χωρίς καμία ανάγκη συλλογής προσωπικών δεδομένων. Θεωρούμε τη μέθοδο μια απο τις σημαντικότερες λύσεις που προσφέρεται για την ενίσχυση ανωνυμίας του bitcoin και ώς εκ τούτου στο 4ο κεφάλαιο θα περιγράψουμε αναλυτικά την λειτουργία και την χρήση της.

Κεφάλαιο 4

Η εξέλιξη του CoinJoin και η ασφάλεια που παρέχει σε σύγχρονές υλοποιήσεις

Σε αυτό το κεφάλαιο θα γίνει ανάλυση της μεθόδου CoinJoin ως πιο ολοκληρωμένης διαθέσιμης λύσης για την βελτίωση της ιδιωτικότητας στο bitcoin. Θα ξεκινήσουμε με την περιγραφή της λειτουργίας και των βασικών πλεονεκτημάτων αυτης της μεθόδου και στην συνέχεια θα ανατρέξουμε σε συγκεκριμένα παραδείγματα υλοποίησης της. Στην συνέχεια θα περιγράψουμε αναλυτικότερα το πρωτόκολλο που χρησιμοποιεί το Wasabi Wallet το οποίο αποτελεί την πιο διαδεδομένη χρήση αυτής της μεθόδου. Για τον σκοπό αυτό, θα παρουσιάσουμε μια εφαρμογή που δημιουργήσαμε για την παραγωγή στατιστικών ενδείξεων σχετικά με την αποτελεσματικότητα του CoinJoin. Η εφαρμογή μας χρησιμοποιεί γνωστές ευριστικές μεθόδους αναγνώρισης των συναλλαγών που εκτελούν CoinJoin και το δωρεάν API που παρέχει η εταιρία Blockchain.com [78]. Συλλέγει και αναλύει τις εισόδους και τις εξόδους για κάθε συναλλαγή και παρέχει μια σειρά δεικτών αξιολόγησης τους. Θα καταλήξουμε σε βασικά συμπεράσματα σχετικά με την ανωνυμία που προσφέρεται σε σχέση με την υποσχόμενη και σε ποιό βαθμό οι χρήστες αξιοποιούν αυτή τη μέθοδο ή μετριάζουν τα πλεονεκτήματα της με απρόσεκτη χρήση, διακυβεύοντας έτσι εν αγνοία τους την ιδιωτικότητα τους.

4.1 Ανασκόπηση στην εξέλιξη του Coinjoin

4.1.1 Η μέθοδος Coinjoin

Το CoinJoin αποτελεί την αποκεντρωμένη υλοποίηση ανάμιξης νομισμάτων στο bitcoin. Η πρώτη αναφορά και περιγραφή στο CoinJoin έγινε το 2013 απο τον Gregory Maxwell [79] σε ένα φόρουμ του bitcoin. Εκεί πρότεινε την ιδέα της ανάμιξης εισόδων στην ίδια συναλλαγή, με σκοπό την ενίσχυση της ιδιωτικότητας και την αντιμετώπιση των προβλημάτων αντίστοιχων κεντροποιημένων υλοποιήσεων. Η ιδέα του αντικαθιστούσε την ύπαρξη υπηρεσίας με εξουσία στην διαδικασία με τον μηχανισμό του «συντονιστή». Στην παραδοσιακή μίξη νομισμάτων που περιγράψαμε στο 3ό κεφάλαιο, οι χρήστες στέλνουν τα νομίσματα τους στην υπηρεσία, η οποία με την σειρά της αναλαμβάνει την επαναποστολή των καθαρών νομισμάτων στους κατόχους τους. Αντίθετα, στο CoinJoin ο συντονιστής έχει μονάχα την ευθύνη σύνταξης του script της συναλλαγής που θα επιτελέσει το CoinJoin. Ο τελευταίος λόγος ανήκει στους συμμετέχοντες, οι οποίοι υποχρεωούνται να ελέγξουν την ορθότητα της συνταχθείσας συναλλαγής προτού γίνει αποστολή της. Ο συντονιστής δεν έχει ούτε το δικαίωμα αλλά ούτε και την δυνατότητα εκτέλεσης διαφορετικών κινήσεων ενώ δεν γνωρίζει βέβαια και τα ιδιωτικά κλειδιά των εισόδων της συναλλαγής. Πρόκειται λοιπόν για μια υπηρεσία που έχει ουσιαστικά τον ρόλο της «διοργάνωσης» γύρων μίξης και της σύνταξης των αντίστοιχων scripts.

Οι υλοποιήσεις CoinJoin διακρίνονται σε εφαρμογές που απαιτούν λήψη και εγκατάσταση (σε σταθερό υπολογιστή ή και σε φορητές συσκευές) και σε online υπηρεσίες. Μεγαλύτερη ασφάλεια παρέχεται απο την πρώτη κατηγορία αφού αποτρέπεται η κοινοποίηση προσωπικών δεδομένων και δεδομένων ταυτοποιήσης με την υπηρεσία καθώς και η έκθεση τους στο διαδίκτυο. Σημαντική είναι γι αυτόν τον λόγο και η χρησιμοποίηση κατάλληλων πρωτοκόλλων για την

διάδοση της πληροφορίας και την ενημέρωση των δεδομένων των εφαρμογών, οπότε και εφαρμόζονται μέτρα προστασίας αυτής της κίνησης όπως είναι η χρήση του Tor. Οι διαδεδομένες υπηρεσίες CoinJoin εφαρμόζονται ταυτόχρονα σε υλοποιήσεις bitcoin πορτοφολιών. Συνεπώς συγκεντρώνεται η διαχείριση των νομισμάτων με το μέσο ανωνυμοποίησης τους και διευκολύνονται οι χρήστες. Παρέχεται συνήθως η δυνατότητα αυτόματης συμμετοχής σε γύρους μίξης ανα συγκεκριμένα χρονικά διαστήματα. Η συχνότητα τους καθορίζεται απο την αμοιβή του συστήματος που διατίθενται να πληρώσει ο κάθε χρήστης. Είναι αξιοσημείωτο πως η συμμετοχή σε διαδοχικούς γύρους μίξης παρέχει εκθετικά μεγαλύτερη ενίσχυση της ανωνυμίας όπως θα εξηγήσουμε και στο πρακτικό μέρος της εργασίας μας.

4.1.2 Υλοποιήσεις CoinJoin

Σε αυτήν την υποενότητα θα αναφέρουμε εν συντομία σε 2 αξιοσημείωτες αποκεντρωμένες υλοποίησεις του μηχανισμού CoinJoin πρωτού επιστήσουμε την προσοχή μας σε αυτή του Wasabi Wallet.

JoinMarket

Το JoinMarket [80] είναι μια απο τις πρώτες αποκεντρωμένες υλοποιήσεις πορτοφολιού με ενσωματωμένη τη δυνατότητα CoinJoin. Δημιουργήθηκε το 2015 ως ένα έργο ανοιχτού κώδικα. Η υλοποίηση του είναι ιδιαίτερη και περιλαμβάνει μοναδικά χαρακτηριστικά σε σχέση με κάθε άλλη στην αγορά. Συγκεκριμένα, το JoinMarket επιτρέπει ανά πάση στιγμή τη δήλωση συμμετοχής σε γύρο μίξης με οποιαδήποτε πιθανή ποσότητα. Για την εξυπηρέτηση αυτών των αιτημάτων το πορτοφόλι εισήγαγε την έννοια των «κατασκευαστών» οι οποίοι είναι χρήστες που διαθέτουν τα νομίσματα τους για την λειτουργία των γύρων μίξης με αντάλλαγμα ένα μικρό αντίτιμο. Ο μηχανισμός CoinJoin του JoinMarket παράγει ανομοιόμορφα ποσά, γεγονός που δημιουργεί ρίσκο σύνδεσης τους με τις εισόδους της συναλλαγής. Ως εκ τούτου το πορτοφόλι παρέχει τη δυνατότητα αυτόματης συμμετοχής σε γύρους μίξης ανά τακτά χρονικά διαστήματα. Η συμμετοχή σε διαδοχικούς γύρους μίξης ενισχύει σημαντικά την ιδιωτικότητα και μειώνει την πιθανότητα ιχνηλάτησης των νομισμάτων. Επιπλέον, για την αποτελεσματικότητα του πρωτοκόλλου είναι απαραίτητη η παραγωγή τουλάχιστον δύο εξόδων για κάθε είσοδο της συναλλαγής μίξης. Στα μειονεκτήματα του JoinMarket περιλαμβάνεται το υψηλό κόστος σε σχέση με τις υπόλοιπες υπηρεσίες μίξης. Κατά περιόδους επίσης υπάρχει μεγάλη έλλειψη ρευστότητας στην αγορά του η οποία δημιουργεί μεγάλες καθυστερήσεις στην ολοκλήρωση γύρων μίξης. Επιπλέον, για την χρήση αυτού του πορτοφολιού απαιτείται η γνώση χρήση του λειτουργικού συστήματος Linux και η εξοικείωση με εντολές στο τερματικό του. Η συντήρηση του γίνεται απο εθελοντές γεγονός που δικαιολογεί την έλλειψη χρηστικότητας. Πρόκειται παρ'όλα αυτά για μια υλοποίηση με σταθερή παρουσία στον χώρο των μηχανισμών μίξης και ένα απο τα πρότυπα εφαρμογών ενίσχυσης της ιδιωτικότητας του bitcoin.

Samourai Wallet

Το Samourai Wallet αποτελεί πορτοφόλι διαθέσιμο μόνο για φορητές συσκευές. Ξεκίνησε ώς λογισμικό κλειστού κώδικα και το 2019 έγινε διαθέσιμο για επισκόπηση και συνεισφορά. Βασίζεται στο λογισμικό Whirlpool [81] το οποίο αξιοποιεί το Chaumian CoinJoin. Το Chaumian CoinJoin αποτελεί πολύ ενδιαφέρον πρωτόκολλο για το οποίο θα αφιερώσουμε ξεχωριστή υποενότητα κατά την περιγραφή του Wasabi Wallet. Κάθε γύρος μίξης στο Whirlpool παράγει «καθαρές» εξόδους ίδιας ποσότητας και η ελάχιστη ποσότητα μίξης ειναι 0.01 BTC. Για την οργάνωση των διαδικασιών του CoinJoin το Samourai Wallet χρησιμοποιεί κεντροποιημένο συντονιστή. Ως εκ τούτου απαιτεί σε μεγάλο βαθμό εμπιστοσύνη στην εφαρμογή και περιορίζονται τα πλεονεκτήματα του. Αποτελεί παρ'όλα αυτά ένα από τα δημοφιλέστερα πορτοφόλια, μεταξύ εκείνων που δίνουν έμφαση στην ιδιωτικότητα.

4.2 Η περίπτωση του Wasabi Wallet

4.2.1 Zerolink

Το Wasabi Wallet ξεκίνησε την λειτουργία του το 2018 με στόχο την εδραίωση ως πορτοφόλι υψηλής ιδιωτικότητας. Πρόκειται για υλοποίηση «ανοιχτού κώδικα» που σημαίνει πως η εφαρμογή είναι δημόσια διαθέσιμη για επισκόπηση, συνεισφορά και παρέχει πλήρη διαφάνεια. Η λήψη και εγκατάσταση της είναι διαθέσιμη προς το παρόν μόνο για υπολογιστές και όχι φορητές συσκευές. Ο Adam Ficsor υπήρξε ο εμπνευστής και δημιουργός του λογισμικού που ονομάστηκε ZeroLink [82] και στο οποίο βασίστηκε το Wasabi Wallet. Το ZeroLink είναι ένα αποκεντρωμένο πρωτόκολλο που υλοποιεί το CoinJoin. Λειτουργεί με την χρήση δικτύου ομότιμων κόμβων για τη λήψη και τη διάδοση δεδομένων. Το ZeroLink λοιπόν παρέχει μια τεχνική μίξης νομισμάτων bitcoin ορίζοντας τις έννοιες: πορτοφόλι «προ-μίξης» (pre-mix wallet), πορτοφόλι «μετά-τη-μίξη» (post-mix wallet) και δένοντάς τες με κάποιον αλγόριθμο υλοποίησης CoinJoin. Οι όροι αυτοί αναφέρονται στην κατάσταση και τις συνθήκες ενός πορτοφολιού και των αντίστοιχων UTXOs που εμπεριέχει πρίν απο την συμμετοχή σε γύρους μίξης και μετά. Για τις δύο διακριτές καταστάσεις ενός πορτοφολιού θέτει διαφορετικά κριτήρια και μέτρα προστασίας της ιδιωτικότητας. Με άλλα λόγια το πρωτόκολλο αυτό έχει κατασκευαστεί με τρόπο ώστε να είναι δυνατή η εγκατάσταση του σε διαφορετικές υλοποιήσεις πορτοφολιών, αρκεί να ικανοποιούν συγκεκριμένες ιδιότητες.

Για την κατάσταση «πρό-μίξης» οι απαραίτητες συνθήκες που πρέπει να τηρούνται είναι ίδιες με τις απαιτούμενες για κάθε πορτοφόλι σχετικά με τον τρόπο λήψης και διάδοσης δεδομένων, όπως αναλύθηκαν στο 3ο κεφάλαιο. Γι'αυτόν τον λόγο και δεδομένης της ανάγκης τήρησης της ιδιωτικότητας καθ'όλη τη λειτουργία και χρήση του, το Wasabi Wallet ενεργεί αποκλειστικά στο δίκτυο Tor και επωφελείται απο την ασφάλεια που παρέχει. Επιπλέον, για τις υλοποιήσεις ιεραρχικά ντετερμινιστικών πορτοφολιών όπως είναι το Wasabi Wallet, είναι απαραίτητος ο προσεκτικός χειρισμός του σπόρου και του δένδρου των κλειδιών που παράγεται, δηλαδή με τρόπο που να διασφαλίζεται η προστασία αυτών των δεδομένων. Σε αντίθετη περίπτωση όλες οι διευθύνσεις του εκάστοτε πορτοφολιού συνδέδονται με τον ιδιοκτήτη τους.

Όσον αφορά στην κατάσταση «μετά-μίξης», τα μέτρα που πρέπει να λαμβάνονται για την διατήρηση της ανωνυμίας στα «καθαρά» νομίσματα είναι αυστηρότερα. Ο κυριότερος περιορισμός αφορά τον τρόπο χρήσης αυτών των νομισμάτων σε μετέπειτα συναλλαγές. Είναι σημαντική η αποφυγή χρησιμοποίησης εξόδου CoinJoin σε συνδυασμό με κάποια διεύθυνση η οποία δεν είναι ακόμη ανωνυμοποιημένη και μπορεί να δημιουργήσει σύνδεση με την ίδια οντότητα. Σε αυτή τη περίπτωση ακυρώνεται ουσιαστικά η επίδραση της μίξης για τα συγκεκριμένα νομίσματα. Οι συνέπειες ωστόσο δεν τελειώνουν εκεί. Έστω πως ένας γύρος μίξης A έχει σύνολο ανωνυμίας 55 ισόποσων εξόδων. Έστω επίσης πως 20 απο αυτές τις εξόδους συνδέονται μέσω επόμενων συναλλαγών με κάποιες εκ των εισόδων του γύρου μίξης A. Τότε το πραγματικό σύνολο ανωνυμίας των υπολοίπων συναλλαγών είναι στην καλύτερη περίπτωση 35. Συνεπώς παρατηρούμε πως η συμμετοχή σε γύρο μίξης δημιουργεί μια εξάρτηση μεταξύ των μελών του, καθώς ο τρόπος χειρισμού των καθαρών νομισμάτων έχει αρνητικό αντίκτυπο όχι μόνο για την ιδιωτικότητα του εκάστοτε άτομου, αλλά και των υπολοίπων μελών. Για την αντιμετώπιση του παραπάνω προβλήματος το ZeroLink προτείνει την απαγόρευση συνδυασμού «καθαρών» νομισμάτων και μη, ως εισόδους στην ίδια συναλλαγή. Είναι προφανές πως μια τέτοια ρύθμιση μειώνει την χρηστικότητα του εκάστοτε πορτοφολιού. Επιπλέον, η απογόρευση αυτή μπορεί εύκολα να παραβιαστεί με την αποστολή των καθαρών νομισμάτων σε διευθύνσεις εκτός διαχείρισης του εκάστοτε πορτοφολιού. Συμπεραίνουμε πως ακόμη και αν τα μέτρα που λαμβάνει ένα πορτοφόλι για την προστασία της ιδιωτικότητας μετά απο γύρους μίξης είναι τα μέγιστα δυνατά, η τήρηση της εναπόκειται στον σύνολο των μελών του κάθε γύρου.

Το Wasabi Wallet έχει επιλέξει την διαχείρηση αυτού του ζητήματος με μια «μέση λύση». Κάθε UTXO βαθμολογείται με «βαθμό ανωνυμίας» (anonymity score) ανάλογα με τον αριθμό των διαδοχικών γύρων μίξης στους οποίους έχει συμμετάσχει. Ο βαθμός ανωνυμίας ξεκινάει απο

το 1 για τα νέα UTXOs και λαμβάνεται υπόψιν στον αλγόριθμο επιλογής εισόδων του πορτοφολιού. Η διαδικασία που ακολουθείται είναι η εξής: Το πορτοφόλι ρυθμίζεται για την αυτόματη μίξη των νομισμάτων που εμπεριέχει ανά συγκεκριμένα χρονικά διαστήματα. Η επιλογή των παραμέτρων μίξης γίνεται μέσω συγκεκριμένων διαβαθμίσεων που παρέχει η εφαρμογή. Υπάρχουν 3 πλάνα στρατηγικής μίξης όπως φαίνεται στην οθόνη του σχήματος 4.1. Τα 3 πλάνα διαφέρουν ως πρός το βαθμό ανωνυμοποίησης που υπόσχονται, την ταχύτητα εκτέλεσης και ταξινομούνται με το κόστος συμμετοχής τους. Το 3ο εξ αυτών ονομάζεται «Maximize Privacy» (Μεγιστοποίηση Ιδιωτικότητας) και παρέχει τις αυστηρότερες ρυθμίσεις τήρησης της ιδιωτικότητας. Περιλαμβάνει ασφαλώς το μεγαλύτερο κόστος συμμετοχής. Κατά την επιλογή αυτού τού πλάνου αυτόματα ενεργοποιείται η ρύθμιση «Red Coin Isolation». Με την ρύθμιση αυτή απαγορεύεται ο συνδυασμός UTXOs στα οποία να περιλαμβάνεται περισσότερο απο ένα UTXO με βαθμό ανωνυμίας ίσο με 1. Απομονώνονται κατά αυτόν τον τρόπο αυτά τα νομίσματα μέχρις ότου να γίνει μίξη τους. Η εφαρμογή παρ'όλα αυτά επιτρέπει την προσαρμογή κάποιων εκ των παραμέτρων ιδιωτικότητας όπως φαίνεται στο σχήμα 4.2. Οι επιλογές αυτές περιλαμβάνουν την απενεργοποίηση του «Red Coin Isolation» και την ενεργοποίηση κάτω ορίου στο αποδεκτό σύνολο ανωνυμίας των γύρων μίξης. Σε κάθε περίπτωση, η επιλογή των UTXOs που θα χρησιμοποιηθούν ως είσοδοι στην εκάστοτε συναλλαγή μίξης γίνεται αυτόματα και με βάση τις παραπάνω επιλογές.

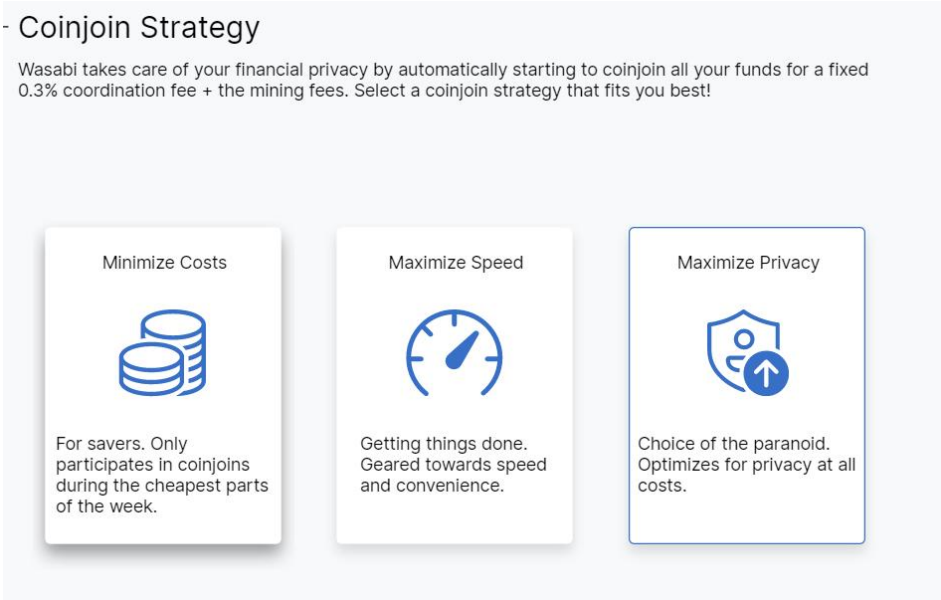
Τέλος, το Wasabi Wallet κατά τη τέλεση «κανονικών» συναλλαγών (και όχι γύρους μίξης) επιλέγει αυτόματα UTXOs. Ο βαθμός ανωνυμίας και το επιλεγμένο πλάνο CoinJoin δεν λαμβάνονται υπόψιν. Παρ'όλα αυτα το Wasabi Wallet επιτρέπει εναλλακτικά και την χειροκίνητη επιλογή των UTXOs. Εκεί εμφανίζεται ο βαθμός ανωνυμίας της κάθε εισόδου αλλά δεν επιφέρει περιορισμούς. Για την επαλήθευση του τρόπου λειτουργίας του δημιουργήσαμε πορτοφόλι στο *testnet*. Το *testnet* αποτελεί αλυσίδα όμοια με αυτή του bitcoin που ακολουθεί τους ίδιους κανόνες και τον ίδιο τρόπο χρήσης. Η διαφορά τους εγγύται στο οτι το *testnet* δεν έχει αξία και χρησιμοποιείται μόνο για δοκιμές και πειράματα στην ανάπτυξη λογισμικού. Τα περισσότερα πορτοφόλια (συμπεριλαμβανομένου του Wasabi Wallet) παρέχουν τη δυνατότητα χρήσης του *testnet* με τον ίδιο ακριβώς τρόπο όπως και το bitcoin. Στο σχήμα 4.3 παρουσιάζουμε την επιλογή χειροκίνητης συναλλαγης που εκτελέσαμε. Για να είναι αντιπροσωπευτικό το παράδειγμα μας, χρησιμοποιήσαμε ένα μέρος των UTXOs του πορτοφολιού σε γύρους CoinJoin. Έπειτα συνδυάσαμε επιτυχώς αυτά τα UTXOs με νομίσματα που έχουν βαθμό ανωνυμίας ίσο με το 1 για την δημιουργία συναλλαγής.

Συμπαιρένουμε πως το Wasabi Wallet αποθαρρύνει αλλά επιτρέπει τον συνδυασμό «καθαρών» εισόδων και μη, ώστε να διευκολύνει την τέλεση συναλλαγών και να μην περιορίσει την χρηστικότητα του πορτοφολιού. Περιλαμβάνει μονάχα κατ'επιλογήν περιορισμό των UTXOs χρησιμοποίησης σε γύρους μίξης με χρήση του «Red Coin Isolation». Είναι σημαντικό λοιπόν να αξιολογήσουμε τον βαθμό, στον οποίο επηρεάζεται η λειτουργία του πρωτοκόλλου απο αυτήν την ελευθερία. Για τον λόγο σε επόμενη υποενότητα θα εκτελέσουμε στατιστική ανάλυση σε συναλλαγές μίξης του Wasabi Wallet και θα επιχειρήσουμε την ποσοτικοποίηση αυτού του φαινομένου.

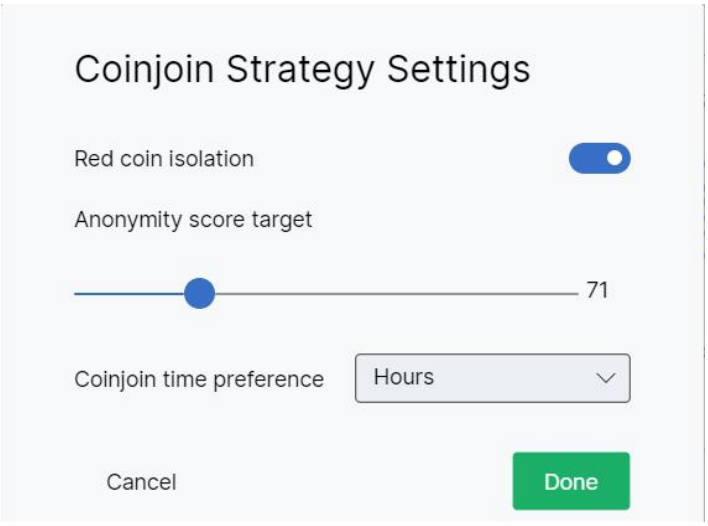
4.2.2 Chaumian CoinJoin

Σε αυτήν την εποενότητα θα περιγράψουμε το πρωτόκολλο Chaumian CoinJoin όπως χρησιμοποιείται στο Wasabi Wallet. Το Chaumian CoinJoin αποτελεί υλοποίηση του CoinJoin βασισμένη στις «τυφλές» υπογραφές του Chaum (Chaum «blind» signatures) [83]. Οι «τυφλές» υπογραφές Chaum αποτελούν ένα είδος πρωτοκόλλου ψηφιακής υπογραφής με σκοπό την επικύρωση και την υπογραφή κρυπτογραφημένων μηνυμάτων (χωρίς να χρειάζεται ανάγνωση τους). Η πρώτη αναφορά στον συσχετισμό της τεχνικής μίξης στο bitcoin με τις υπογραφές Chaum έγινε το 2013 [84] στο bitcointalk forum. Στο πλαίσιο του CoinJoin, το πρωτόκολλο αυτό χρησιμοποιείται απο την υλοποίηση του λογισμικού Zerolink και συνεισφέρει σημαντικά στην διατήρηση της ανωνυμίας.

Συγκεκριμένα, η διαδικασία που ακολουθείται στο Chaumian CoinJoin είναι η εξής [82]:

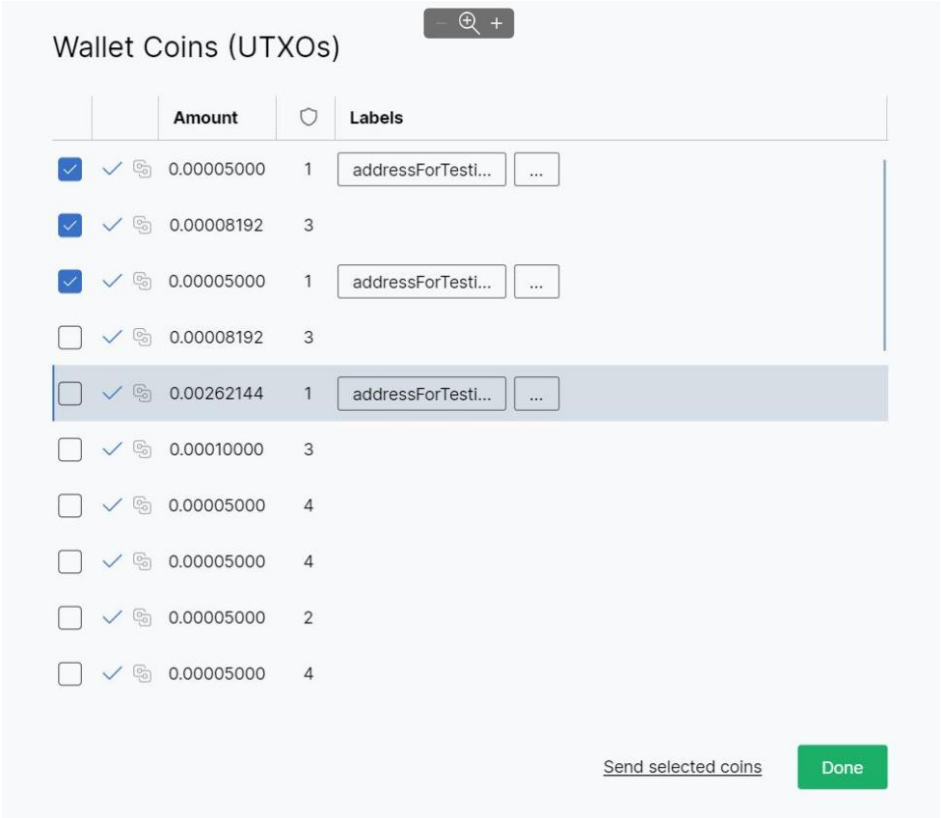


Σχήμα 4.1: Με την παραπάνω οθόνη το Wasabi Wallet δίνει την επιλογη εναλλακτικών πλάνων μίξης



Σχήμα 4.2: Προηγμένες ρυθμίσεις στρατηγικής μίξης στο Wasabi Wallet

- Κάθε χρήστης στέλνει στον server τα εξής δεδομένα:
  - UTXOs εισόδου
  - Αποδείξεις υπογραφής αυτών με τα ιδιωτικά τους κλειδιά
  - Διευθύνσεις για τα ρέστα αν χρειάζονται
  - Διευθύνσεις εξόδου των καθαρών νομισμάτων σε κρυπτογραφημένη μορφή
- Στη συνέχεια, ο συντονιστής ελέγχει και επικυρώνει την εγκυρότητα των εισόδων ως προς τις εξής συνθήκες:
  - Επάρκεια ποσότητας εισόδων
  - Έλεγχο για το αν οι είσοδοι είναι πράγματι διαθέσιμες (δηλαδή δεν έχουν ξοδευτεί) και επικυρωμένες



Σχήμα 4.3: Στην παραπάνω εικόνα φαίνεται η χειροκίνητη δυνατότητα επιλογής νομισμάτων εισόδου στο Wasabi Wallet. Κάθε γραμμή του πίνακα αντιστοιχεί σε ένα UTXO. Η στήλη με τις αριθμητικές τιμές φανερώνει τον βαθμό ανωνυμίας του κάθε UTXO. Ο συνδυασμός εισόδων δεν έχει περιορισμούς.

  - Επικύρωση για κάθε UTXO πως δεν χρησιμοποιείται παραπάνω απο μια φορά στην συναλλαγή
  - Έλεγχο εγκυρότητας των αποδείξεων

  Αυτή η διαδικασία γίνεται χωρίς να μπορεί να αποσπάσει πληροφορίες για αυτά τα δεδομένα. Έτσι υπογράφει την κάθε υποβληθείσα είσοδο και την στέλνει πίσω στον ιδιοκτήτη της.

- Εκείνοι με την σειρά τους αποκρυπτογραφούν τα δεδομένα εισόδου τους, τα υπογράφουν και τα υποβάλλουν εκ νέου, χρησιμοποιώντας διαφορετική σύνδεση απο πρίν.

- Στην συνέχεια ο συντονιστής δημιουργεί μια ενιαία συναλλαγή και αναμένει την τελική επαλήθευση όλων των συμμετεχόντων.

Η απλότητα του αυτού του πρωτοκόλλου το καθιστά ως μια απο τις πιο αποτελεσματικές διαθέσιμες υλοποιήσεις μίξης. Χρονικά, το πρώτο στάδιο εγγραφής εισόδων στην διαδικασία εκτελείται κατά μέσο όρο σε 3 λεπτά. Η υπόλοιπη διαδικασία χρειάζεται μονάχα μερικά δευτερόλεπτα, σε περίπτωση που οι συμμετέχοντες παραμείνουν ενεργοί. Σε αντίθετη περίπτωση και αν υπάρξουν αποσυνδέσεις και ιδιαίτερα αργή απόκριση απο τα μέλη της συναλλαγής, η καθυστέρηση ενδέχεται να διαρκέσει 2-3 ακόμη λεπτά. Είναι βέβαια λογική και και αποδεκτή η διαφορά στην εκτέλεση μιας τέτοιας συναλλαγής σε σχέση με τις απλές (που εκτελούνται μέσα σε δευτερόλεπτα), δεδομένης της ευκολίας ρύθμισης και αυτοματοποίησής της.

4.3 Αξιολόγηση της αποτελεσματικότητας των CoinJoins

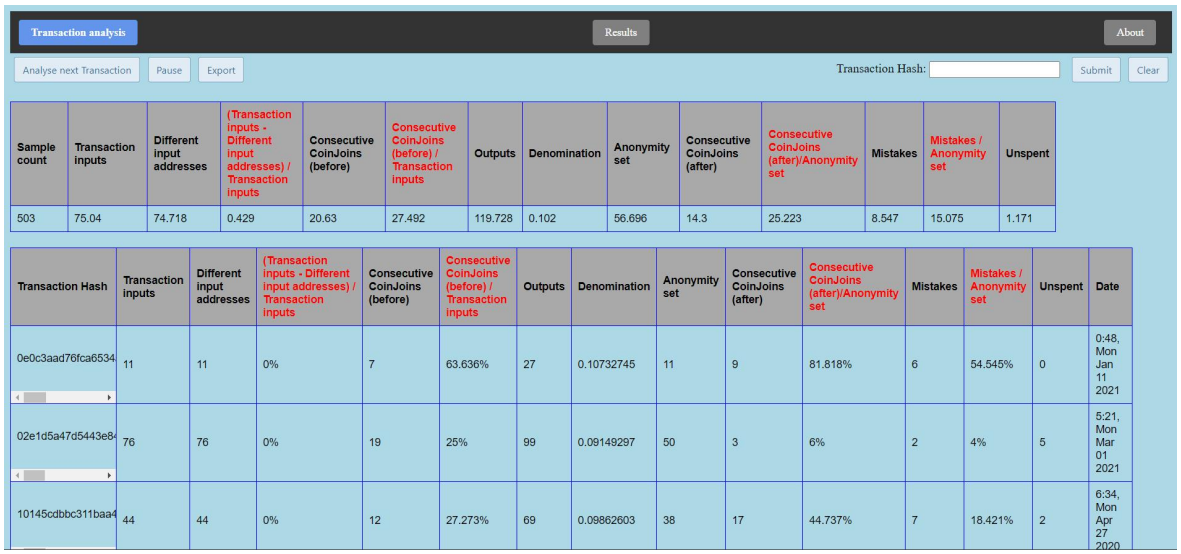
Σε αυτήν την ενότητα επιχειρούμε την αξιολόγηση της μεθόδου CoinJoin χρησιμοποιώντας ως παράδειγμα την υλοποίηση του Wasabi Wallet. Σύμφωνα με την έρευνα μας, η βιβλιογραφία σε σχέση με την πρακτική αξιολόγηση της αποτελεσματικότητας των CoinJoins ειναι ελλιπής. Ο Adam Ficsor ως δημιουργός του Wasabi Wallet ήταν ο πρώτος που ανέφερε την ύπαρξη ευριστικών ικανών να εντοπίσουν με αποτελεσματικότητα συναλλαγές CoinJoin [10]. Συγκεκριμένα, αναφέρει πως κάθε συναλλαγή με περισσότερες απο 10 εξόδους ακριβώς της ίδιας ποσότητας είναι με βεβαιότητα συναλλαγή του Wasabi Wallet. Χρησιμοποίησε αυτήν την ευριστική καθώς και παρόμοια μέθοδο για την ανταγωνίστρια εταιρία Samourai για την παραγωγή στατιστικών σύγκρισης της χρήσης των 2 πορτοφολιών [85] αλλά και αξιολόγησης του δικού του πρωτοκόλλου [86]. Στην συνέχεια, η βιβλιογραφία [87] περιλαμβάνει την προσπάθεια ανίχνευσης συναλλαγών CoinJoin μέσω της συνεχούς αποστολής ερωτημάτων (queries) για την νόμιμη παρακολούθηση των δεδομένων που διαδίδει το API του συντονιστή του Wasabi Wallet. Μια ακόμη ποσοτική έρευνα [88] σχετικά με τα CoinJoin ασχολήθηκε με τους τρόπους ανίχνευσης τέτοιων συναλλαγών. Συγκεκριμένα, στην έρευνα αυτή χρησιμοποιήθηκε τόσο η ευριστική μέθοδος του Fiscor όσο και ένα μοντέλο μηχανικής μάθησης που εκπαιδεύτηκε στην ανίχνευση τέτοιων συναλλαγών. Σε αυτή τη μέθοδο μάλιστα χρησιμοποιήθηκε ένα dataset παραγόμενο απευθείας απο τον συντονιστή του Wasabi Wallet. Κατέληξαν στο ό,τι η μέθοδος της μηχανικής μάθησης παρουσιάζει αρκετά μεγάλη ακρίβεια, ωστόσο η χρήση της ευριστικής έχει ακόμη μεγαλύτερη αποτελεσματικότητα. Στην συνέχεια χρησιμοποίησαν την πρώτη μέθοδο για την παραγωγή ενός dataset με παραπάνω απο 30.000 αναγνωριστικά (transaction IDs) συναλλαγών του Wasabi Wallet στο block range 530,500 μέχρι 725,348 και δηλαδή στο διάστημα (05-07-2018 με 28-02-2022). Η έρευνα τους ολοκληρώθηκε με την στατιστική ανάλυση αυτού του δείγματος ως προς δύο συνιστώσες. Μελέτησαν την οικονομική επίδραση του Wasabi Wallet στο δίκτυο του bitcoin ώς πρός τον όγκο των νομισμάτων που μεταφέρουν σε συναλλακτικές υπηρεσίες και αξιολόγησαν την ιδιωτικότητα σε αυτές τις συναλλαγές. Όσον αφορά το 2ο σκέλος που εμπίπτει βέβαια στον τομέα της δικής μας έρευνας, χρησιμοποίησαν την υπηρεσία Graphsense [89] η οποία δημιουργεί clusters απο οντότητες μέσω της ευριστικής για τις εισόδους κοινής συναλλαγής. Μελέτησαν κατά αυτόν τον τρόπο την επίδραση της ομαδοποίησης στις εισόδους αλλά και στις εξόδους των CoinJoins.

Σε αυτή την εργασία, στοχεύουμε να βασιστούμε στην υπάρχουσα βιβλιογραφία παρέχοντας μια πιο ολοκληρωμένη στατιστική ανάλυση των συναλλαγών CoinJoin χρησιμοποιώντας το ίδιο σύνολο δεδομένων με περισσότερες από 30.000 συναλλαγές Wasabi CoinJoin. Συγκεκριμένα, θα υπολογίσουμε το ποσοστό των εισόδων και των εξόδων σε κάθε συναλλαγή που έχουν «λάθη ανωνυμίας» και μειώνουν το πραγματικό σύνολο ανωνυμίας, παρέχοντας μια πιο λεπτομερή εικόνα για τους κινδύνους ιδιωτικότητας από τη χρήση συναλλαγών CoinJoin. Επιπλέον, θα διερευνήσουμε το ποσοστό των εισόδων και των εξόδων που συμμετείχαν σε CoinJoins πολλές φορές στη σειρά γεγονός που αποτελεί παράγοντα σημαντικής ενίσχυσης της ιδιωτικότητας. Το εργαλείο που δημιουργήσαμε παρέχει επιπλέον χρήσιμες χρήσιμες μετρήσεις και την δυνατότητα ανάλυσης οποιασδήποτε επιπλέον συναλλαγής δοθεί ώς είσοδος. Με αυτόν τον τρόπο, ελπίζουμε να συνεισφέρουμε στην κατανόηση της αποτελεσματικότητας των συναλλαγών CoinJoin και του βαθμού, στον οποίο μπορούν να προστατέψουν το δικαίωμα απορρήτου των χρηστών.

4.3.1 Περιγραφή μεθόδου

Για το πρακτικό μέρος της εργασίας μας δημιουργήσαμε μια εφαρμογή χρησιμοποιώντας την γλώσσα προγραμματισμού JavaScript. Φτιάξαμε έναν express server με την δυνατότητα διαχείρισης ερωτημάτων για συναλλαγές, διευθύνσεις και blocks του bitcoin. Ο server μας ρυθμίστηκε για την αποστολή ερωτημάτων στο API του blockchain.com [78] το οποίο παρακολουθεί την αλυσίδα του bitcoin και επιστρέφει δεδομένα σε μορφή JSON. Στην συνέχεια ο server μας διαχειρίζεται τα αποτελέσματα και τα μεταφέρει στο front-end της δημιουργίας μας, το οποίο

γράφτηκε επίσης σε «καθαρή» JavaScript με συνδυασμό HTML5 και CSS για την παραγωγή ενός φιλικού περιβάλλοντος διεπαφής. Στο front-end μας παρέχουμε τη δυνατότητα αναζήτησης οποιασδήποτε συναλλαγής στο bitcoin μέσω του αναγνωριστικού της ή την αυτόματη προσπέλαση αναγνωριστικών συναλλαγών απο αρχείο. Σε κάθε περίπτωση, η ανάλυση μιας συναλλαγής γίνεται με μιά σειρά απο scripts που δημιουργήσαμε με σκοπό την παραγωγή στατιστικών αποτελεσμάτων. Μετά το πέρας της εκάστοτε ανάλυσης, η συναλλαγή εμφανίζεται σε πίνακα στην αρχική σελίδα της εφαρμογής. Παρέχεται επίσης 2ος πίνακας στο πάνω μέρος της σελίδας, όπου ενημερώνονται αυτόματα οι συγκεντρωτικοί μέσοι όροι των δεικτών μας για όλες τις επεξεργασμένες συναλλαγές. Ο κώδικας της εργασίας μας είναι δημόσια διαθέσιμος σε αποθετήριο του Github.



Sample count	Transaction inputs	Different input addresses	(Transaction inputs - Different input addresses) / Transaction inputs	Consecutive CoinJoins (before)	Consecutive CoinJoins (before) / Transaction inputs	Outputs	Denomination	Anonymity set	Consecutive CoinJoins (after)	Consecutive CoinJoins (after)/Anonymity set	Mistakes	Mistakes / Anonymity set	Unspent
503	75.04	74.718	0.429	20.63	27.492	119.728	0.102	56.696	14.3	25.223	8.547	15.075	1.171

Transaction Hash	Transaction inputs	Different input addresses	(Transaction inputs - Different input addresses) / Transaction inputs	Consecutive CoinJoins (before)	Consecutive CoinJoins (before) / Transaction inputs	Outputs	Denomination	Anonymity set	Consecutive CoinJoins (after)	Consecutive CoinJoins (after)/Anonymity set	Mistakes	Mistakes / Anonymity set	Unspent	Date
0e0c3aad76fca6534	11	11	0%	7	63.636%	27	0.10732745	11	9	81.818%	6	54.545%	0	0:48, Mon Jan 11 2021
02e1d5a47d5443e8	76	76	0%	19	25%	99	0.09149297	50	3	6%	2	4%	5	5:21, Mon Mar 01 2021
10145cdbbc311baa4	44	44	0%	12	27.273%	69	0.09862603	38	17	44.737%	7	18.421%	2	6:34, Mon Apr 27 2020

Σχήμα 4.4: Στην εικόνα παρουσιάζουμε μια ενδεικτική απεικόνιση της εφαρμογής κατά την ανάλυσης μεγάλου πλήθους συναλλαγών.

Στην συνέχεια θα παρουσιάσουμε τους δείκτες αξιολόγησης που επιλέξαμε για την ανάλυση μας όπως απεικονίζονται στον πίνακα ανάλυσης συναλλαγών. Για κάθε συναλλαγή παράγουμε τα εξής αποτελέσματα:

- Η πρώτη στήλη (μετά την ένδειξη μέτρησης των συναλλαγών) αναφέρει των αριθμό εισόδων της συναλλαγής.

- Στην συνέχεια χρησιμοποιούμε 2 ακόμη στήλες που αφορούν την πιθανή επαναχρησιμοποίηση διεύθυνσης στο ίδιο CoinJoin. Το CoinJoin επιτρέπει την συμμετοχή κάθε χρήστη με διαφορετικά UTXOs τα οποία ενδέχεται να προέρχονται ακόμη και απο την ίδια διεύθυνση. Θεωρήσαμε λοιπόν χρήσιμο να μετρήσουμε κατά πόσο αυτό συνηθίζεται. Για τον λόγο αυτό μετράμε τις διακριτές διευθύνσεις εισόδου και στην συνέχεια το ποσοστό επαναχρησιμοποίησης διευθύνσεων στην είσοδο. Παρέχεται κατά αυτόν τον τρόπο μια πρώτη εικόνα σχετικά με το αν το αρχικό πλήθος διαφορετικών συμμετεχόντων ανταποκρίνεται στην πραγματικότητα.

- Έπειτα, υπολογίζουμε έναν σημαντικό δείκτη σχετικά με τον τρόπο χρήσης της υπηρεσίας. Πρόκειται για το πλήθος (και στην συνέχεια το ποσοστό) των εισόδων της συναλλαγής που συμμετέχουν σε CoinJoin σε 2ο διαδοχικό γύρο. Για να επιτευχθεί αυτό, ελέγχουμε την προέλευση του κάθε UTXO εισόδου της συναλλαγής. Χρησιμοποιούμε δηλαδή την διεύθυνση απο την οποία προήλθε για την ανίχνευση της αντίστοιχης προηγούμενης συναλλαγής. Έπειτα, με την ευριστική ανίχνευσης των Wasabi CoinJoins ελέγχουμε αν η είσοδος μας είναι αποτέλεσμα προηγούμενου CoinJoin.

- Συνεχίζοντας, η ανάλυση μας κατευθύνεται στον έλεγχο των εξόδων της συναλλαγής. Συγκεκριμένα, παρέχουμε δεδομένα για τον αριθμό των εξόδων και για κάθε μια ανιχνεύουμε το ποσό στο οποίο αντιστοιχεί. Βρίσκουμε έτσι την έξοδο με την ποσότητα που εμφανίζεται περισσότερες φορές (ίση με το chunk size) και υπολογίζουμε έτσι το θεωρητικό σύνολο ανωνυμίας της συναλλαγής, δηλαδή το σύνολο των «καθαρών» εξόδων που είναι δυσδιάκριτες μεταξύ τους.

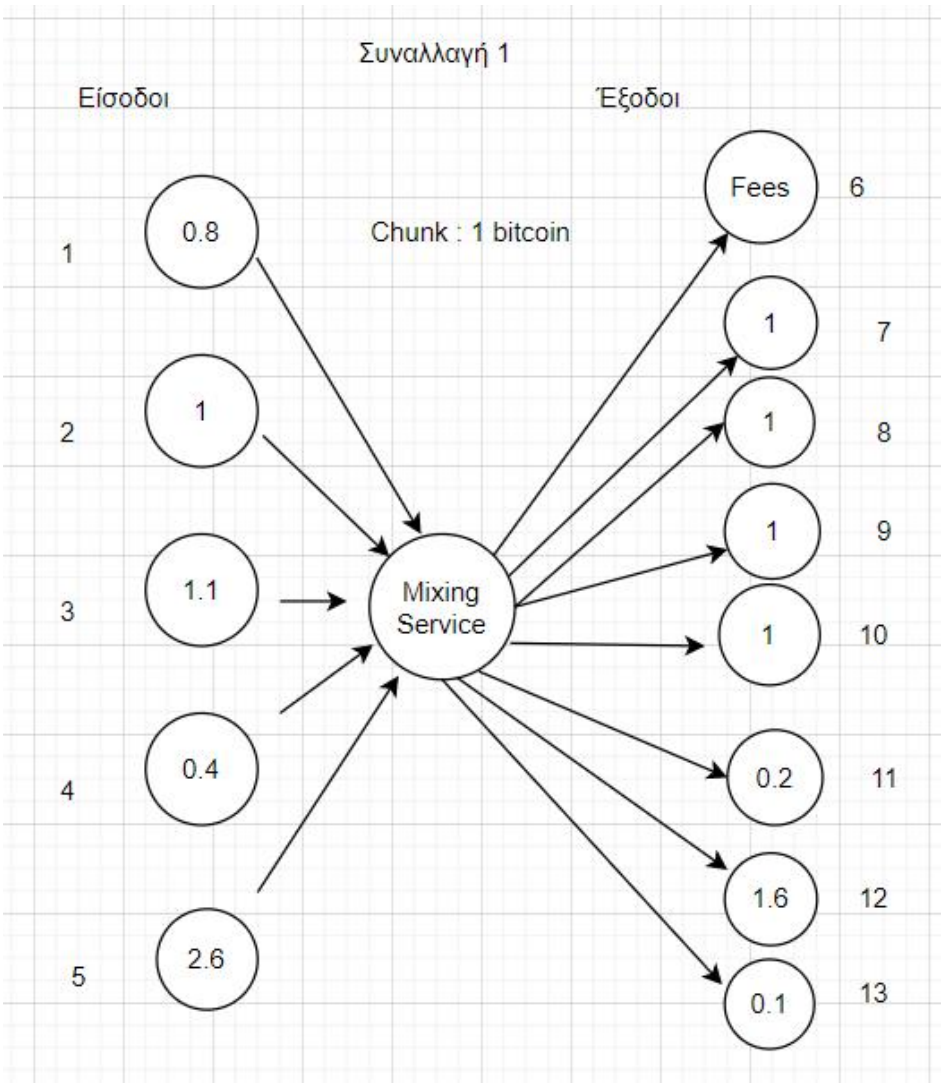
- Οι επόμενες μετρήσεις μας υπολογίζουν τον αριθμό και το ποσοστό των εξόδων που συμμετέχουν σε διαδοχικά CoinJoins, όπως αντίστοιχα κάνουμε και με τις εισόδους. Συγκεκριμένα, για κάθε μία απο τις εξόδους ελέγχουμε αν έχει χρησιμοποιηθεί σε μετέπειτα συναλλαγή. Όσες δεν έχουν χρησιμοποιηθεί τις σημειώνουμε ως «unspent» και για τις υπόλοιπες ελέγχουμε την συναλλαγή χρησιμοποίησης τούς. Η ανάλυση αυτή αφορά βέβαια μονάχα τις εξόδους με ποσότητα όσο η τιμή του chunk size και όχι τις εξόδους επιστροφής (που δεν θεωρείται πως συμμετέχουν στο CoinJoin).

- Τέλος, ο σημαντικότερος ίσως δείκτης που παρέχουμε αφορά τον έλεγχο για λανθασμένη χρησιμοποίηση των εξόδων CoinJoin. Ορίζουμε ως «λάθος μετά απο CoinJoin» την χρησιμοποίηση εξόδου CoinJoin σε συνδυασμό με κάποια διεύθυνση που συμμετείχε στον ίδιο γύρο ως είσοδος είτε ως έξοδος. Στο σχήμα 4.5 εξηγείται με παράδειγμα αυτή η περίπτωση. Ο έλεγχος αυτός έχει μεγάλη χρονική πολυπλοκότητα, αφού επιβάλλει την άντληση δεδομένων για την επόμενη συναλλαγή και τις διευθύνσεις που εμφανίζονται σε όλες τις εξόδους της τρέχουσας. Συγκεκριμένα, δημιουργούμε ένα σύνολο με όλες τις διευθύνσεις που εμφανίζονται ώς είσοδοι ή έξοδοι στην τρέχουσα συναλλαγή (έστω σύνολο A). Έπειτα, για κάθε διεύθυνση εξόδου (έστω π.χ διεύθυνση που συμβολίζεται με το γράμμα i) αντλούμε τα δεδομένα της επόμενης συναλλαγής στην οποία συμμετέχει. Έτσι, δημιουργούμε το αντίστοιχο σύνολο των διευθύνσεων εισόδου που εμφανίζονται σε αυτή τη συναλλαγή (έστω σύνολο B_i) και ελέγχουμε αν υπάρχει τομή μεταξύ των συνόλων A και B_i εκτός της διεύθυνσης i. Αν βρεθεί τέτοια τομή, σημειώνουμε την έξοδο και αυξάνουμε τον μετρητή λαθών της συναλλαγής. Επαναλαμβάνουμε την διαδικασία για κάθε έξοδο i (με αντίστοιχο σύνολο B_i). Σημειώνουμε πώς ο έλεγχος μας γίνεται σε «βάθος» 1 , δήλαδη αφορά μονάχα την πρώτη συναλλαγή χρησιμοποίησης του εκάστοτε UTXO μετά τη συμμετοχή του σε γύρο μίξης. Τα προηγμένα εργαλεία ανάλυσης αλυσίδας εκτελούν εξαντλητική αναζήτηση στο ιστορικό μεταφοράς του κάθε UTXO και εντοπίζουν τέτοιου είδους συνδέσεις ακόμα και αν απέχουν αρκετά «βήματα» στην αλυσίδα. Αυτός ο δείκτης παρ'όλα αυτά θα μας βοηθήσει να αποκτήσουμε μια καλή εικόνα του φαινομένου αφού ο αμεσότερος κίνδυνος απώλειας της ανωνυμίας είναι στις πρώτες συναλλαγές μετά την ολοκλήρωση της μίξης.

4.3.2 Αποτελέσματα

Εκτελέσαμε την ανάλυση για περισσότερες απο 1500 συναλλαγές του Wasabi CoinJoin και παρακάτω παρουσιάζουμε τα αποτελέσματα της μελέτης μας.

Παρατηρούμε πως οι συναλλαγές CoinJoin έχουν κατά μέσο όρο 75 εισόδους και 120 εξόδους. Η επαναχρησιμοποίηση των διευθύνσεων εισόδου είναι ιδιαίτερα μικρή (ποστοστό κάτω του 0.5% γεγονός σημαντικό για την ορθή χρήση του πρωτοκόλλου. Οι «καθαρές» έξοδοι (anonymity set) που παράγει κάθε συναλλαγή κατά μέσο όρο είναι 57 και το μέσο chunk size είναι 0.1 bitcoin. Ως προς την αξιολόγηση της χρήσης του μηχανισμού δίνουμε έμφαση στους δείκτες για τα διαδοχικά CoinJoins στην είσοδο (27%) και την έξοδο (25%) που δείχνει το ποσοστό των χρηστών που επιλέγουν την ενισχυμένη χρήση που προσφέρει η συμμετοχή σε διαδοχικά CoinJoins. Αρκεί να συλλογιστούμε πως αν ένας γύρος CoinJoin παρέχει σύνολο



Σχήμα 4.5: Στο εικονιζόμενο παράδειγμα συναλλαγής θεωρούμε πως όλες οι είσοδοι προέρχονται απο διαφορετικές διευθύνσεις. Θεωρούμε ως αναγνωριστικά των διευθύνσεων τους δείκτες που έχουμε σημειώσει. Οι καθαρές έξοδοι που παράγει ο γύρος μίξης μεταφέρονται στις διευθύνσεις 7-10. Άν κάποια απο τις διευθύνσεις 7-10 χρησιμοποιηθεί σε κάποια μετέπειτα συναλλαγή σε συνδυασμό με κάποια απο τις υπόλοιπες διευθύνσεις που εμφανίζονται στην συναλλαγή 1 (1-6 ή 11-13) τότε είναι δυνατή η σύνδεση τους και η ομαδοποίηση τους σε μια κοινή οντότητα.

ανωνυμίας για τα καθαρά νομίσματα της τάξεως του $\frac{1}{57}$ τότε με 2 γύρους προκύπτει:

$$\frac{1}{57^2} \approx \frac{1}{3250}$$

Ως πρός τα λάθη στην χρήση του CoinJoin, βρήκαμε πως περίπου 15% των εξόδων συσχετίζονται με διευθύνσεις που χρησιμοποιούνται στο ίδιο CoinJoin. Αυτό το ποσοστό φανερώνει χρήστες που ακυρώνουν την προσπάθεια ανωνυμίας που καταβάλλουν με την συμμετοχή στην διαδικασία και υπογραμμίζει τη σημασία εκπαίδευσης τους στη σωστή χρήση του πρωτοκόλλου.

Συνολικά, τα αποτελέσματα της ανάλυσης μας υποδηλώνουν ότι τα CoinJoins είναι αποτελεσματικά, αλλά υπάρχει περιθώριο βελτίωσης όσον αφορά τη μείωση των σφαλμάτων που οφείλονται στον ανθρώπινο παράγοντα. Αυτό φανερώνει την αδυναμία του πρωτοκόλλου να αποτελέσει συνολική λύση στο ζήτημα της ιδιωτικότητας. Για την ορθή χρήση του απαιτείται η εκπαίδευση των χρηστών στον τρόπο λειτουργίας του και στην γνώση των κινδύνων που δεν

εξαλείφονται με το «καθάρισμα» των νομισμάτων. Τέλος, για την παραγωγή καλύτερων αποτελεσμάτων επιβάλλεται επίσης η βελτιστοποίηση του ποσοστού των διαδοχικών συμμετοχών σε γύρους CoinJoin.

Sample count	Transaction inputs	Different input addresses	(Transaction inputs - Different input addresses) / Transaction inputs	Consecutive CoinJoins (before)	Consecutive CoinJoins (before) / Transaction inputs	Outputs	Denomination	Anonymity set	Consecutive CoinJoins (after)	Consecutive CoinJoins (after)/Anonymity set	Mistakes	Mistakes / Anonymity set	Unspent
1514	75.908	75.6	0.405	21.308	28.071	120.417	0.102	57.429	14.279	24.865	8.555	14.896	1.16

Σχήμα 4.6: Αποτελέσματα ανάλυσης CoinJoins του Wasabi Wallet

4.4 Έξοδοι μεταβλητής ποσότητας και η νέα βελτίωση του WabiSabi

Τον Ιούνιο του 2022 το Wasabi Wallet παρουσίασε την 2η έκδοση του [10] η οποία εισάγει το λογισμικό WabiSabi. Το WabiSabi παρ'ότι βασίζεται στο ZeroLink σηματοδοτεί σημαντικές αλλαγές και θεωρείται πως εν μέρη το αντικαθιστά. Σε αυτήν την έκδοση εκτελέστηκαν ποικίλες αλλαγές στο πορτοφόλι όπως αυτή της βελτίωσης της διεπαφής χρήστη (User Interface). Η μετάβαση απο το ZeroLink στο WabiSabi παρ'ότι είναι ακόμη πρόσφατη είναι βέβαιο πως θα επηρεάσει και το ζήτημα της ιδιωτικότητας. Συνεπώς σε αυτό το σημείο θεωρούμε ιδαίτερα χρήσιμο να αναφερθούμε σε αυτές τις αλλαγές.

Το WabiSabi χρησιμοποιεί αποδείξεις μηδενικής γνώσεις για την απόδειξη ορθότητας των δεσμεύσεων κατά την καταχώρηση εισόδων σε κάθε γύρο μίξης. Με αυτόν τον τρόπο ο κάθε χρήστης μπορεί να πείσει τον συντονιστή για την ιδιοκτησία της συνολικής αξίας που καταθέτει στη συναλλαγή, χωρίς να παρουσιάσει τα συγκεκριμένα UTXOs. Η προσπάθεια απόκρυψης της σχέσης των εισόδων ενισχύεται ακόμη περισσότερο με την εισαγωγή των «Keyed-Verification Anonymous Credentials» (KVACs) [90]. Πρόκειται για μια τεχνική που επιτρέπει στον συντονιστή να «σφραγίσει» και ύστερα να επαληθεύσει το σύνολο των UTXOs που καταθέτει ο εκάστοτε συμμετέχων με ανώνυμο τρόπο. Ενισχύονται έτσι οι τυφλές υπογραφές Chaum και αποκρύπτονται «περιττές» πληροφορές για τα σύνολα UTXOs που ανήκουν σε κάθε οντότητα.

Μια ακόμη μεγάλη διαφοροποίηση στη 2η έκδοση του Wasabi αφορά τις ποσότητες εξόδων. Καταργείται πλέον η ομοιομορφία των καθαρών εξόδων. Επιτυγχάνεται έτσι η μίξη μεγαλύτερων ποσών και η διάσπαση τους σε πολλές εξόδους τυχαίων τιμών, που αθροίζονται βέβαια στο συνολικό ποσό καταχώρησης του κάθε χρήστη. Για την αποτελεσματικότητα αυτής της μεθόδου το Wasabi Wallet χρησιμοποιεί πολλαπλές εισόδους απο τον κάθε χρήστη ώστε να αποφευχθεί η πιθανή σύνδεση αθροίσματος εξόδων με συγκεκριμένη είσοδο. Παράγονται επιπλέον πολλές έξοδοι για κάθε είσοδο ώστε γίνει ακόμα πιο δύσκολη η ιχνηλάτηση του εκάστοτε UTXO. Θεωρείται τέλος αναγκαιότητα η μίξη τους κάθε UTXO σε πολλαπλούς γύρους μίξης για την καλύτερη αντιμετώπιση ευριστικών μεθόδων.

Παρατηρούμε πως οι συγκεκριμένες αλλαγές μεγαλώνουν το σύνολο ανωνυμίας σε κάθε γύρο μίξης, αφού αντικαθίσταται ο ρόλος των διευθύνσεων επιστροφής με επιπλέον καθαρές εξόδους. Αυτή η επιλογή του Wasabi Wallet οφείλεται εν μέρη στην ανάγκη βελτώσης της χρηστικότητας του πορτοφολιού με την εξυπηρέτηση μεγαλύτερου εύρους τιμών εισόδων. Επιπλέον αποτρέπεται σε έναν βαθμό η ανίχνευση των συναλλαγών του πορτοφολιού στην αλυσίδα και η χρήση στοχευμένων ευριστικών κατάργησης της ανωνυμίας που προσφέρει. Στην περιγραφή του πρωτοκόλλου οι συγγραφείς αναφέρουν πως η νέα αυτή έκδοση δεν λύνει πλήρως τα προβλήματας των ευριστικών μεθόδων ανίχνευσης των συναλλαγών που οφείλονται σε μίξεις του Wasabi Wallet. Έχει συνεπώς ενδιαφέρον στο πλαίσιο μελλοντικής έρευνας να εξερευνηθεί η ύπαρξη αποτελεσματικής ευριστικής ανίχνευσης αυτών των συναλλαγών. Έτσι θα δοθεί ευκαιρία για περαιτέρω αξιολόγηση της ιδιωτικότητας τους και σύγκρισης του πρωτοκόλλου με την

προηγούμενη έκδοση του.

Τέλος παρατηρούμε πως η επίδραση της στατιστικής μελέτης που εκτελέσαμε δεν αλλάζει σημαντικά, αφού ο τρόπος χρήσης των καθαρών εξόδων και οι δυνατότητες που δίνονται στους χρήστες ως πρός την αξιοποίηση τους δεν μεταβλήθηκαν. Το πρωτόκολλο παραμένει ευάλωτο σε λάθη σε περίπτωση συνδυασμού διευθύνσεων που συμμετείχαν στον ίδιο γύρο μίξης (είτε ως είσοδοι είτε ως έξοδοι), όπως περιγράφτηκε στην προηγούμενη ενότητα. Η συστηματική μελέτη συναλλαγών παρ'όλα αυτά θα φανερώσει κατά πόσο η ελευθερία στη δυνατότητα ανομοιόμορφων εξόδων επηρεάζει ευγεργετικά τον δείκτη λανθασμένης χρήσης καθαρών νομισμάτων. Είναι σίγουρο πως η μαζική συμμετοχή των UTXOs των χρηστών σε γύρους μίξης είναι πλέον ευκολότερη. Μένει να φανεί αν το κόστος συμμετοχής σε μεγάλο πλήθος γύρων μίξης θα αποτελέσει ανασταλτικό παράγοντα στη μείωση των λαθών ανωνυμίας.

Κεφάλαιο 5

Συμπεράσματα

Κλείνοντας αυτή τη μελέτη κάνουμε μια επισκόπηση στην ανάλυση και τα συμπεράσματα μας για το ζήτημα της ιδιωτικότητας στο bitcoin.

Απο την πρώτη κιόλας περίοδο διάδοσης των κρυπτονομισμάτων έγινε αντιληπτό πως η ψευδώνυμη φύση του bitcoin δεν επαρκεί για την διασφάλιση της ανωνυμίας των συναλλασσόμενων μελών. Οι κίνδυνοι που απειλούν την ιδιωτικότητα είναι πολλοί και εντοπίζονται σε διαφορετικές πτυχές του τρόπου υλοποίησης του. Ως εκ τούτου αναλύθηκε το ζήτημα των ευριστικών μεθόδων ανάλυσης αλυσίδας. Πρόκειται για μεθόδους που στοχεύουν στην ομαδοποίηση διευθύνσεων ως προς την ιδιοκτησία τους και εκμεταλεύονται συνηθισμένους τρόπους συμπεριφοράς κατά τη τέλεση συναλλαγών. Οι κυριότερες ευριστικές μέθοδοι αφορούν τις διευθύνσεις των UTXOs που χρησιμοποιούνται συνδυαστικά ως είσοδοι σε συναλλαγές αλλά και εκείνες στις οποίες επιστρέφονται τα «ρέστα». Στην πρώτη περίπτωση γίνεται η υπόθεση πως οι είσοδοι ανήκουν στην ίδια οντότητα οπότε μπορούν να ομαδοποιηθούν. Αυτή η μέθοδος αποδείχθηκε πως έχει τεράστια αποτελεσματικότητα σε συναλλαγές με μικρό πλήθος εισόδων. Στη δεύτερη περίπτωση αναλύονται τα ποσά εξόδων και εξάγονται συμπεράσματα για την σχέση μεταξύ εισόδων και εξόδων της συναλλαγής. Κατά το μεγαλύτερο διάστημα της πορείας του κρυπτονομίσματος οι περισσότερες συναλλαγές είχαν μονάχα δύο εξόδους. Αρχικά μάλιστα η έξοδος για τα ρέστα επαναχρησιμοποιούνταν, οπότε και υπήρχε πλήρης διαφάνεια στη πορεία των εξόδων της συναλλαγής. Όσο «ωρίμαζε» η χρήση κρυπτονομισμάτων οι περισσότερες υλοποιήσεις πορτοφολιών λάμβαναν υπόψιν τους αυτό το πρόβλημα και έθεταν ως κανόνα την χρήση νέων διευθύνσεων σε κάθε εισερχόμενη συναλλαγή (όπως και για την επιστροφη υπολοίπου). Αυτό αποτέλεσε μια ακόμη ευριστική μέθοδο ομαδοποίησης διευθύνσεων που ανήκουν στην ίδια οντότητα μεταξύ των εξόδων της εκάστοτε συναλλαγής. Οι παραπάνω μέθοδοι είναι ιδιαίτερα απλές και αφορούν μονάχα την πληροφορία που δίνεται κατά τη τέλεση μια πληρωμής χωρίς την περαιτέρω συσχέτιση με προηγούμενες και επόμενες συναλλαγές. Τα σύγχρονα εργαλεία ανάλυσης αλυσίδας είναι ακόμη περισσότερο εξελιγμένα και ελέγχουν κάθε πιθανό σημάδι συσχέτισης UTXOs. Οι πληροφορίες που αξιοποιούν αφορούν επίσης τα μεταφερόμενα ποσά, τις χρονικές στιγμές τέλεσης των συναλλαγών και ασφαλώς το φαινόμενο της επαναχρησιμοποίησης διευθύνσεων. Λαμβάνεται επίσης υπόψιν το script που ορίζει τους κανόνες της συναλλαγής, το οποίο πολλές φορές φανερώνει στοιχεία για το πορτοφόλι απο το οποίο δημιουργήθηκε.

Το πρόβλημα τήρησης της ιδιωτικότητας αφορά επίσης τον τρόπο αξιοποιήσης των κρυπτονομισμάτων και τη χρήση υπηρεσιών που έχουν πρόσβαση σε προσωπικά δεδομένα. Εκεί υπάρχει σοβαρός κίνδυνος σύνδεσης πραγματικών οντοτήτων με διευθύνσεις και πλήρους κατάργησης της ιδιωτικότητας τους. Το φαινόμενο αυτό επεκτείνεται και σε οποιαδήποτε χρήση κρυπτονομισμάτων για πληρωμές ή εισπράξεις καθώς και στην διαδικτυακή επαφή με υπηρεσίες που σχετίζονται με το bitcoin. Σε αυτή τη κατηγορία ανήκουν τόσο τα online πορτοφόλια, οι συναλλακτικές υπηρεσίες αλλά και εφαρμογές αναζήτησης δεδομένων στο blockchain (συναλλαγών, blocks κτλ).

Στη συνέχεια η μελέτη μας δίνει έμφαση στις λύσεις που έχουν δοθεί με σκοπό ενίσχυση της ιδιωτικότητας.

Για την ανώνυμη χρήση του bitcoin είναι απαραίτητη η αποφυγή συσχέτισης διευθύνσεων, συναλλαγών ή οποιονδήποτε ακόμη πληροφοριών της αλυσίδας με προσωπικά δεδομένα. Για

την αγορά και την πώληση κρυπτονομισμάτων κατά αυτόν τον τρόπο υπάρχουν λύσεις όπως ανώνυμα bitcoin ATMs, υπηρεσίες ανταλλαγής νομισμάτων με μετρητά κ.α. Πρέπει ταυτόχρονα να αποφεύγονται υπηρεσίες που απαιτούν εγγραφή και να προτιμώνται εκείνες χωρίς ταυτοποίηση.

Τα πορτοφόλια που πολλές φορές εγκαθιστούν οι χρήστες στις συσκευές τους συγχρονίζουν τα δεδομένα τους ανά τακτά χρονικά διαστήματα. Κατά τη μεταφορά αυτών των δεδομένων θεωρείται ασφαλέστερη η χρήση πλήρους κόμβου, όπου λαμβάνονται καθολικά τα δεδομένα της αλυσίδας. Για την προσπάθεια εξάλειψης της διαρροής δεδομέων μέσω της διεύθυνσης IP των χρησιμοποιούμενων συσκευών, αρκετά πορτοφόλια ενεργούν στο δίκτυο Tor. Έτσι η δικτυακή κίνηση αποκρύπτεται και μειώνεται η πιθανότητα επιτυχούς παρακολούθησης της.

Η εργασία έπειτα κατευθύνεται στις μεθόδους καταπολέμησης των ευριστικών ιχνηλάτησης της αλυσίδας. Τα περισσότερα σύγχρονα πορτοφόλια παράγουν αυτόματα νέες διεύθυνσεις για τα ποσά επιστροφής ως υπόλοιπα συναλλαγών. Από εκεί και πέρα η τήρηση του κανόνα αποφυγής επαναχρησιμοποίσης διευθύνσεων για εισπράξεις και αποστολές νομισμάτων επαφίεται στον κάθε χρήστη. Ως πρός τη δημιουργία νέων διευθύσεων ο πιο διαδεδομένος τύπος πορτοφολιού είναι ο ιεραρχικά ντετερμινιστικός. Πρόκειται για ένα πρωτόκολλο που ξεκινάει κατά τη δημιουργία του κάθε πορτοφολιού με την παραγωγή 9-12 λέξεων. Αυτές οι λέξεις ταξινομούνται σε καθορισμένη σειρά και αποτελούν αναγνωριστικό του πορτοφολιού. Απο τον σπόρο επίσης παράγονται όλες οι διευθύνσεις του πορτοφολιού, σε δενδρική μορφή. Η μέθοδος αυτή δημιουργεί εξάρτηση όλων των διευθύνσεων (όπως και των κλειδιών τους) απο τον αρχικό σπόρο και επιτρέπει την ανάκτηση τους, αφού η παραγωγή κλειδιών είναι ντετερμινιστική (οπότε μπορεί να επαναληφθεί).

Στην συνέχεια η παρούσα μελέτη περιγράφει προτεινόμενες και λιγότερο διαδεδομένες μεθόδους ενίσχυσης της ανωνυμίας που παρουσιάζουν μεγάλο ενδιαφέρον. Σε αυτή τη κατηγορία ανήκουν οι μυστικές διευθύνσεις, οι υπογραφές δακτυλίου, οι εμπιστευτικές συναλλαγές, οι αποδείξεις μηδενικής γνώσης αλλά και η επίλυση του ζητήματος της ανωνυμίας με χρήση συναλλαγών «εκτός αλυσίδας». Οι μυστικές διευθύνσεις χρησιμοποιούν διευθύνσεις μιας χρήσης για την παραλαβή νομισμάτων και «κρύβουν» μέσω κρυπτογράφησης τους πραγματικούς παραλήπτες. Οι υπογραφές δακτυλίου επιχειρούν τη δημιουργία συνόλων ανωνυμίας για την απόκρυψη του πραγματικού υπογράφοντα. Έχουν αποκεντρωμένη φύση και είναι δοκιμασμένες σε κρυπτονομίσματα με εγγενή αυξημένη ιδιωτικότητα. Οι εμπιστευτικές συναλλαγές έπειτα, χρησιμοποιούνται στην δυνατότητα επικύρωσης δεδομένων ενώ παραμένουν κρυπτογραφημένα. Στο bitcoin η εφαρμογή τους αφορά την απόκρυψη των ποσών εισόδου σε συναλλαγές. Παρόμοια λειτουργικότητα έχουν επίσης οι αποδείξεις μηδενικής γνώσεις. Στοχεύουν στην ολοκλήρωση διαδικασιών επικύρωσης δεσμέυσεων με την παροχή όσο το δυνατόν λιγότερων πληροφοριών. Εφαρμόζονται σε πορτοφόλια όπως το Wasabi Wallet και άλλες υλοποιήσεις που στοχεύουν στην ενίσχυση της ιδιωτικότητας. Συνεχίζοντας, είναι αξιοσημείωτη η προσπάθεια απλοποίησης των scripts που ορίζουν τις συναλλαγές στο bitcoin. Η πρόσφατη ενσωμάτωση των υπογραφών Schnorr στο bitcoin ενοποίησε το σύνολο των υπογραφών της κάθε συναλλαγής μειώνοντας τα δεδομένα που εμφανίζονται στην αλυσίδα. Τα «Scriptless» scripts αποτελούν προτεινόμενη μέθοδο που βασίζεται στις υπογραφές Schnorr και επιχυρεί την απλοποίηση των scripts σε βαθμό που να εμφανίζονται μόνο οι δημόσιες διευθύνσεις και οι υπογραφές. Τέλος, στα επόμενα χρόνια αναμένεται η αύξηση της διάδοσης υλοποιήσεων μηχανισμών «εκτός αλυσίδας». Εκεί είναι ήδη διαθέσιμη η δυνατότητα τέλεσης συναλλαγών μικρών ποσών, οι οποίες δεν καταγράφονται αναλυτικά στην αλυσίδα. Η προσπάθεια καθιέρωσης αλλά και το ζήτημα αξιολόγησης της ιδιωτικότητας τους παρουσιάζουν μεγάλο ενδιαφέρον με πρώιμο ακόμη χαρακτήρα.

Στο τελευταίο μέρος της εργασίας δίνεται έμφαση στη μίξη νομισμάτων. Η κατασκευή συναλλαγών με μεγάλο πλήθος εισόδων με σκοπό τη δημιουργία μεγάλων συνόλων ανωνυμίας για τις εξόδους αποτελεί τον πιο αποτελεσματικό τρόπο ενίσχυσης της ιδιωτικότητας στο bitcoin. Για τον σκοπό αυτό έχουν δημιουργηθεί πολλές υπηρεσίες που συντονίζουν την συνεργασία χρηστών έναντι μικρού αντίτιμου απο τον κάθε χρήστη. Οι υλοποιήσεις αυτές ήταν αρχικά συγκεντρωτικές και δημιουργούσαν μεγάλους κινδύνους παραβίασης της ιδιωτικότητας και της ασφάλειας των συμμετεχόντων.

Τα τελευταία χρόνια έχουν δημιουργηθεί πορτοφόλια που αξιοποιούν την ιδέα της μίξης με πλήρως αποκεντρωμένο τρόπο. Η μέθοδος αυτή αναφέρεται ως CoinJoin. Στην παραδοσιακή μίξη νομισμάτων η υπηρεσία έχει τον πλήρη έλεγχο διαχείρισης των εισόδων, κατασκευής και αποστολής της τελικής συναλλαγής μίξης. Αντίθετα, στο CoinJoin η υπηρεσία έχει τον ρόλο της επικύρωσης των δεδομένων και της δημιουργία της ενιαίας συναλλαγής. Κάθε βήμα της διαδικασίας γίνεται με τρόπο ανώνυμο και οι συμμετέχοντες έχουν τον πλήρη έλεγχο των νομισμάτων τους. Για την αποστολή της συναλλαγής μίξης απαιτείται η ομόφωνη επαλήθευση της εγκυρότητας της. Υπάρχουν αρκετές διαθέσιμες υλοποιήσεις CoinJoin και εκείνη που ξεχωρίζει είναι η δημιουργία του πορτοφολιού Wasabi Wallet. Πρόκειται για ένα πορτοφόλι που κατασκευάστηκε με βασικό κίνητρο την τήρηση της ιδιωτικότητας των χρηστών του. Λειτουργεί αποκλειστικά μέσω του δικτύου Tor και ενισχύεται συνεχώς με τις πιο σύγχρονες τεχνικές ανωνυμοποίησης. Το πρωτόκολλο CoinJoin που υιοθέτησε το Wasabi Wallet ονομάστηκε Chaumian CoinJoin, αφού βασίζεται στις υπογραφές Chaum. Επιτρέπει την εισαγωγή UTXOs απο μεγάλο πλήθος χρηστών και δημιουργεί «καθαρές εξόδους» ίδιας ποσότητας. Το πλήθος των ίσων εξόδων ορίζει το σύνολο ανωνυμίας, δηλαδή το σύνολο των εξόδων που είναι δυσδιάκριτες μεταξύ τους.

Η αξιολόγηση της αποτελεσματικότητας του CoinJoin γίνεται με την μελέτη την παραγόντων που επιδρούν στη μεταβολή του θεωρητικού συνόλου ανωνυμίας. Για τον λόγο αυτό η εργασία μας αξιοποιεί την υπάρχουσα γνώση ανίχνευσης συναλλαγών CoinJoin. Δημιουργήσαμε ένα εργαλείο ανάλυσης συναλλαγών μίξης και αξιολογήσαμε 1500 συναλλαγές που εκτελέστηκαν με το Wasabi Wallet στο διάστημα 2018-2022. Η εφαρμογή ελέγχει τον τρόπο χρησιμοποίησης των καθαρών εξόδων και αποφαίνεται πως περίπου 15% εξ αυτών συνδέονται με διευθύνσεις που συμμετείχαν στον ίδιο γύρο μίξης. Ο έλεγχος μάλιστα αφορά μόνο την πρώτη συναλλαγη στην οποία χρησιμοποιείται το κάθε UTXO μετά την μίξη του. Είναι βέβαιο πως με «εξαντλητική» ανάλυση του ιστορικού μεταφοράς των νομισμάτων προκύπτει ακόμη μεγαλύτερο ποσοστό. Τα αποτελέσματα αυτά προκύπτουν παρότι το πορτοφόλι παρέχει βαθμολογία ανωνυμίας κάθε UTXO και προτρέπει το συνδυασμό καθαρών μονάχα εισόδων κατά τη τέλεση συναλλαγών. Για την αποφυγή αυτού του προβλήματος είναι σημαντικό να καθαρίζονται τακτικότερα στο σύνολο τους τα νομίσματα ενός πορτοφολιού. Κάθε έξοδος πρέπει να περνάει απο διαδοχικούς γύρους μίξης για να αποφευχθεί η σύνδεση τους κατά τη τέλεση συναλλαγών. Η συμμετοχή σε διαδοχικούς γύρους μίξεις μεγαλώνει εκθετικά το σύνολο ανωνυμίας του εκάστοτε UTXO και διασφαλίζει την αποτελεσματικότητα του πρωτοκόλλου. Η εφαρμογή μας υπολόγισε πως περίπου 26% των νομισμάτων λαμβάνουν μέρος σε διαδοχικό γύρο μίξης. Το ποσοστό αυτό είναι χρήζει βελτίωσης και δικαιολογεί τα λάθη που εμφανίστηκαν στην χρήση των νομισμάτων μετά τη μίξη τους.

Το Wasabi Wallet στα μέσα του 2022 προχώρησε σε σημαντικές αλλαγές της υλοποίησης CoinJoin που χρησιμοποιεί. Ενίσχυσε την τήρηση της ανωνυμίας κατά την επικοινωνία χρηστών και συντονιστή, περιορίζοντας τη γνώση του για τον συσχετισμό εισόδων απο κοινή οντότητα. Η σημαντικότερη αλλαγή που επιτελέστηκε είναι η κατάργηση της ισότητας των καθαρών ποσών εξόδου. Επέτρεψε την συμμετοχή στον ίδιο γύρο μίξης εισόδων με διαφορετικές ποσότητες. Διευκόλυνε έτσι σε μεγάλο βαθμό την εύρεση συμμετεχόντων για κάθε γύρο μίξης με σκοπό να αυξήσει τις διαδοχικές μίξεις και την γενικότερη συχνότητα τους. Για την αποφυγή σύνδεσης εισόδων με εξόδους με βάση τα ποσά, ο αλγόριθμος του πορτοφολιού χρησιμοποιεί κατά βάση πολλαπλές εισόδους απο τον κάθε συμμετέχοντα και παράγει πολλαπλές εξόδους διαμοιράζοντας το σύνολο των ποσών. Η αποτελεσματικότητα του πρωτοκόλλου βασίζεται πλέον σε ακόμη μεγαλύτερο βαθμό απο πριν στην συμμετοχή σε διαδοχικές μίξεις για την αποφυγή συνδέσεων εξόδων με εισόδους.

Καταλήγουμε πως το CoinJoin είναι η ευρύτερα χρησιμοποιούμενη μέθοδος ενίσχυσης της ανωνυμίας στο bitcoin. Το Wasabi Wallet παρέχει την πιο διαδεδομένη υλοποίηση του πρωτοκόλλου. Παρ'όλα αυτά υπάρχουν σημαντικά περιθώρια βελτίωσης ως πρός την αποφυγή μίξης «καθαρών» νομισμάτων με UTXOs που επιφέρουν εκ νέου σύνδεση με τον ιδιοκτήτη τους. Οι πρόσφατες αλλαγές στο πρωτόκολλο του πορτοφολιού δεν λύνουν το πρόβλημα άμεσα, συντείνουν όμως στην αύξηση της συχνότητας μίξης. Η ευριστική ανίχνευσης αυτών των συναλλαγών

στην αλυσίδα βασίζονταν εώς τώρα στο μεγάλο πλήθος εξόδων ίδιας ποσότητας. Για την μελλοντική επέκταση αυτής της έρευνας έχει ενδιαφέρον η αναζήτηση νέας μεθόδου ανίχνευσης των συναλλαγών μίξης με σκοπό την εκ νέου παραγωγή των δεικτών αποτελεσματικότητας. Τέλος, είναι σημαντικό να αξιολογηθεί η ανομοιομορφία των ποσών εξόδων στους γύρους μίξης, ώστε να ποσοτικοποιηθούν τα πλεονέκτηματα και οι κίνδυνοι που επιφέρει.

Αρκτικόλεξα

UTXO	Unspent Transaction Output
CT	Confidential Transaction
CSS	Cascading Style Sheet
HTML	HyperText Markup Language
JSON	JavaScript Object Notation
P2TR	Pay-to-Taproot
BIP32	Bitcoin Improvement Proposal 32
KVAC	Keyed-Verification Anonymous Credentials
ECDSA	Elliptic Curve Digital Signature Algorithm
zk-SNARK	zero-knowledge Succinct Non-Interactive Knowledge
ZKP	Zero-Knowledge Proof
ISP	Internet Service Provider
VPN	Virtual Private Network
ATM	Automated teller machine
KYC	Know Your Customer
IP	Internet Protocol
TOR	The Onion Router
API	Application Programming Interface
SSI	Self Sovereign Identity
DSA	Digital Signature Algorithm
RSA	Rivest–Shamir–Adleman
P2SH	Pay-to-Script-Hash
P2PKH	Pay-to-Public-Key-Hash

Απόδοση ξενόγλωσσων όρων

Απόδοση	Ξενόγλωσσος όρος
εξόρυξη	mining
πορτοφόλι	wallet
κρυπτονόμισμα	cryptocurrency
καθολικό/κατάστιχο	ledger
αλυσίδα	chain
μίξη	mixing
ανωνυμία	anonymity
έξυπνο συμβόλαιο	smart contract
ατομική ανταλλαγή	atomic swap
ομότιμο	peer-to-peer
σε σύνδεση	online
δείκτης κατακερματισμού	hash pointer
εγγραφή	record
συναλλαγή	transaction
δημόσιο κλειδί	public key
ιδιωτικό κλειδί	private key
ιχνηλάτηση	tracing
αποτύπωμα	fingerprint
παρτίδα	batch
διεύθυνση	address
διεύθυνση επιστροφής χρημάτων	change address
ομαδοποίηση	clustering
εξερευνητής αλυσίδας	blockchain explorer
ομάδα εξόρυξης	mining pool
ιεραρχικό ντετερμινιστικό πορτοφόλι	hierarchical deterministic wallet
έλεγχος νομισμάτων	coin control
κρυφή διεύθυνση	stealth address
υπογραφή δακτυλίου	ring signature
ομομορφική κρυπτογράφηση	homomorphic encryption
δέσμευση	commitment
πλευρική αλυσίδα	sidechain
απόδειξη μηδενικής γνώσης	zero-knowledge proof
δυαδικό δένδρο	binary tree
αξόδευτα	unspent
διαπιστευτήρια	credentials
εκτός αλυσίδας	off-chain
σύνολο ανωνυμίας	anonymity set
βαθμός ανωνυμίας	anonymity score
τυφλή υπογραφή	blind signature
ερώτημα	query
υπηρεσία	service

συντονιστής	coordinator
μετά-μίξης	post-mix
πρό-μίξης	pre-mix
τέλη	fees
ομάδα	cluster

Βιβλιογραφία

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Cryptography Mailing list at https://metzdowd.com*, 03 2009.

[2] S. Banupriya and K. Kottilingam, "An Analysis of Privacy Issues and Solutions in Public Blockchain (Bitcoin)," in *2021 2nd International Conference for Emerging Technology (INCET)*, pp. 1–7, IEEE, 2021.

[3] M. Alharby and A. v. Moorsel, "Blockchain Based Smart Contracts : A Systematic Mapping Study," in *Computer Science & Information Technology (CS & IT)*, pp. 125–140, Academy & Industry Research Collaboration Center (AIRCC), Aug. 2017.

[4] A. Pfitzmann and M. Hansen, "A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management," *Nordic journal of computing*, Aug. 2010.

[5] E. Androulaki, G. O. Karame, M. Roeschlin, T. Scherer, and S. Capkun, "Evaluating user privacy in bitcoin," in *International conference on financial cryptography and data security*, pp. 34–51, Springer, 2013.

[6] F. Reid and M. Harrigan, "An Analysis of Anonymity in the Bitcoin System," in *2011 IEEE Third Int'l Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third Int'l Conference on Social Computing*, (Boston, MA, USA), pp. 1318–1326, IEEE, Oct. 2011.

[7] D. Ron and A. Shamir, "Quantitative Analysis of the Full Bitcoin Transaction Graph," in *Financial Cryptography and Data Security*, vol. 7859, Berlin, Heidelberg: Springer Berlin Heidelberg, 2013.

[8] M. Spagnuolo, F. Maggi, and S. Zanero, "BitIodine: Extracting Intelligence from the Bitcoin Network," in *Financial Cryptography and Data Security* (N. Christin and R. Safavi-Naini, eds.), vol. 8437, pp. 457–468, Berlin, Heidelberg: Springer Berlin Heidelberg, 2014.

[9] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction.* USA: Princeton University Press, 2016.

[10] A. Ficsor, "Wabisabi: Centrally coordinated coinjoins with variable amounts," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pp. 571–587, ACM, 2019.

[11] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, "Blockchain," *Business & Information Systems Engineering*, vol. 59, pp. 183–187, June 2017.

[12] M. N. M. Bhutta, A. A. Khwaja, A. Nadeem, H. F. Ahmad, M. K. Khan, M. A. Hanif, H. Song, M. Alshamari, and Y. Cao, "A Survey on Blockchain Technology: Evolution, Architecture and Security," *IEEE Access*, vol. 9, pp. 61048–61073, 2021.

[13] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[14] J. Katz and Y. Lindell, *Introduction to Modern Cryptography, Second Edition*. Chapman n' Hall/CRC, 2nd ed., 2014.

[15] R. L. Rivest, A. Shamir, and L. M. Adleman, "Cryptographic communications system and method," *US Patent 4,405,829*, 1983.

[16] Electronic Frontier Foundation (EFF), "Deep dive on end-to-end encryption: How do public key encryption systems work?." `https://ssd.eff.org/module/deep-dive-end-end-encryption-how-do-public-key-encryption-systems-work`, 2021. Accessed on 4 March 2023.

[17] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm," *IEEE Transactions on Information Theory*, vol. 38, no. 2, pp. 388–398, 2001.

[18] National Institute of Standards and Technology (NIST), "Digital signature standard (dss)." `https://csrc.nist.gov/publications/detail/fips/186/4/final`, 2020. Accessed on 4 March 2023.

[19] L. Lai, T. Zhou, Z. Cai, Z. Liang, and H. Bai, "A Survey on Security Threats and Solutions of Bitcoin," *Journal of Cyber Security*, vol. 3, no. 1, pp. 29–44, 2021.

[20] C. Allen, "The path to self-sovereign identity." `http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html`, 2016. Accessed on 4 March 2023.

[21] S. Bistarelli, I. Mercanti, and F. Santini, "An analysis of non-standard transactions," *Frontiers in Blockchain*, vol. 4, p. 23, 2021.

[22] C. Alfieri, "Cryptocurrency and National Security," *International Journal on Criminology*, vol. 9, Feb. 2022.

[23] BitMEX, "Bitcoin Address Reuse Statistics." `https://blog.bitmex.com/bitcoin-address-re-use-statistics/`, 2018. Accessed on 4 March 2023.

[24] OXT Research, "Oxt." `https://oxt.me/`, 2023. Accessed on 4 March 2023.

[25] J. D. Nick, "Data-driven de-anonymization in bitcoin," in *Data-Driven De-Anonymization in Bitcoin*, 2015.

[26] S. Lee, C. Yoon, H. Kang, Y. Kim, Y. Kim, D. Han, S. Son, and S. Shin, "Cybercriminal Minds: An investigative study of cryptocurrency abuses in the Dark Web," in *Proceedings 2019 Network and Distributed System Security Symposium*, (San Diego, CA), Internet Society, 2019.

[27] S. Ghesmati, W. Fdhila, and E. Weippl, "Studying bitcoin privacy attacks and their impact on bitcoin-based identity methods," in *Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP)*, pp. 537–544, 2018.

[28] Check Bitcoin Address, "Check bitcoin address." `https://checkbitcoinaddress.com/`, 2023. Accessed on 4 March 2023.

[29] T. Neudecker and H. Hartenstein, "Could Network Information Facilitate Address Clustering in Bitcoin?," in *Financial Cryptography and Data Security*, vol. 10323, pp. 155–169, Cham: Springer International Publishing, 2017.

[30] M. Harrigan and C. Fretter, "The unreasonable effectiveness of address clustering," in *2016 Intl IEEE Conferences on Ubiquitous Intelligence &: Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld)*, IEEE, jul 2016.

[31] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage, "A fistful of bitcoins: characterizing payments among men with no names," in *Proceedings of the 2013 conference on Internet measurement conference*, (Barcelona Spain), pp. 127–140, ACM, Oct. 2013.

[32] X. Yue, X. Shu, X. Zhu, X. Du, Z. Yu, D. Papadopoulos, and S. Liu, "Bitextract: Interactive visualization for extracting bitcoin exchange intelligence," *IEEE Transactions on Visualization and Computer Graphics*, vol. 25, no. 1, pp. 162–171, 2019.

[33] Blockchain.com, "Blockchain.com explorer." `https://www.blockchain.com/explorer/`, 2023. Accessed on 4 March 2023.

[34] BitRef, "Bitref." `https://bitref.com/`, 2023. Accessed on 4 March 2023.

[35] Wallet Explorer, "Wallet explorer." `https://www.walletexplorer.com/`, 2023. Accessed on 4 March 2023.

[36] Chainalysis, "Chainalysis." `https://www.chainalysis.com/`, 2023. Accessed on 4 March 2023.

[37] F. Sabry, W. Labda, A. Erbad, H. Al Jawaheri, and Q. Malluhi, "Anonymity and privacy in bitcoin escrow trades," in *Proceedings of the 18th ACM Workshop on Privacy in the Electronic Society*, WPES'19, (New York, NY, USA), p. 211–220, Association for Computing Machinery, 2019.

[38] H. Yousaf, G. Kappos, and S. Meiklejohn, "Tracing transactions across cryptocurrency ledgers," in *Proceedings of the 28th USENIX Conference on Security Symposium*, SEC'19, (USA), p. 837–850, USENIX Association, 2019.

[39] ShapeShift, "Shapeshift." `https://shapeshift.com/`, 2023. Accessed on 4 March 2023.

[40] K. Little, "A crypto wallet can help keep your coins safe. here's how to decide if you need one." `https://time.com/nextadvisor/investing/cryptocurrency/best-bitcoin-cryptocurrency-wallet/`, 2021.

[41] A. Biryukov, D. Khovratovich, and I. Pustogarov, "Deanonymisation of clients in bitcoin p2p network," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pp. 15–29, 2014.

[42] A. Biryukov and S. Tikhomirov, "Deanonymization and linkability of cryptocurrency transactions based on network analysis," in *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*, pp. 172–184, 2019.

[43] Wikipedia, "Tor." `https://el.wikipedia.org/wiki/Tor`, 2023. Accessed on 4 March 2023.

[44] J. Crawford and Y. Guan, "Knowing your bitcoin customer: Money laundering in the bitcoin economy," in *2020 13th International Conference on Systematic Approaches to Digital Forensic Engineering (SADFE)*, pp. 38–45, 2020.

[45] Paxful, "Paxful." `https://paxful.com/el`, 2023. Accessed on 4 March 2023.

[46] R. Henry, A. Herzberg, and A. Kate, "Blockchain access privacy: Challenges and directions," *IEEE Security and Privacy*, vol. 16, no. 4, pp. 38–45, 2018.

[47] P. Ferguson and G. Huston, "What is a vpn?." `https://www.ietf.org/rfc/rfc2764.txt`, 2000. Accessed on 4 March 2023.

[48] B. Wiki, "Privacy - bitcoin wiki." `https://en.bitcoin.it/wiki/Privacy#Wallet_history_synchronization`, 2023. Accessed on 4 March 2023.

[49] B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, "Private information retrieval," *Proceedings of IEEE 36th Annual Foundations of Computer Science*, pp. 41–50, 1995.

[50] K. Qin, H. Hadass, A. Gervais, and J. Reardon, "Applying private information retrieval to lightweight bitcoin clients," in *2019 Crypto Valley Conference on Blockchain Technology (CVCBT)*, pp. 60–72, 2019.

[51] S. Cheng, Y. Gao, X. Li, Y. Du, Y. Du, and S. Hu, "Blockchain application in space information network security," in *Space Information Networks* (Q. Yu, ed.), (Singapore), pp. 3–9, Springer Singapore, 2019.

[52] Blockstream, "Blockstream satellite." `https://blockstream.com/satellite/`, 2023. Accessed on 4 March 2023.

[53] S. B. Venkatakrishnan, G. Fanti, and P. Viswanath, "Dandelion: Redesigning the bitcoin network for anonymity," in *2017 IEEE European Symposium on Security and Privacy (EuroS&P)*, pp. 309–326, IEEE, 2017.

[54] G. Maxwell, "Deterministic wallets." `https://bitcointalk.org/index.php?topic=19137`. Last Accessed on 01/2023.

[55] G. Gutoski and D. Stebila, "Hierarchical Deterministic Bitcoin Wallets that Tolerate Key Leakage," in *Financial Cryptography and Data Security* (R. Böhme and T. Okamoto, eds.), (Berlin, Heidelberg), pp. 497–504, Springer Berlin Heidelberg, 2015.

[56] Pieter Wuille, "BIP 32: Hierarchical deterministic wallets." `https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki`, 2012. Accessed: March 5, 2023.

[57] N. T. Courtois and R. Mercer, "Stealth address and key management techniques in blockchain systems," in *International Conference on Information Systems Security and Privacy*, 2017.

[58] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in *Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology*, ASIACRYPT '01, (Berlin, Heidelberg), p. 552–565, Springer-Verlag, 2001.

[59] Y. Liu, R. Li, X. Liu, J. Wang, C. Tang, and H. Kang, "Enhancing anonymity of bitcoin based on ring signature algorithm," in *2017 13th International Conference on Computational Intelligence and Security (CIS)*, pp. 317–321, 2017.

[60] Y. Liu, X. Liu, C. Tang, J. Wang, and L. Zhang, "Unlinkable coin mixing scheme for transaction privacy enhancement of bitcoin," *IEEE Access*, vol. 6, pp. 23261–23270, 2018.

[61] S. Noether, A. Mackenzie, and t. M. R. Lab, "Ring Confidential Transactions," *Ledger*, vol. 1, pp. 1–18, Dec. 2016.

[62] B. Bünz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, and G. Maxwell, "Bulletproofs: Short proofs for confidential transactions and more," in *2018 IEEE Symposium on Security and Privacy (SP)*, pp. 315–334, 2018.

[63] G. Maxwell, "Confidential transactions," *https://elementsproject.org/features/confidential-transactions/investigation*, 2015.

[64] T. P. Pedersen, "Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing," in *Advances in Cryptology — CRYPTO '91* (J. Feigenbaum, ed.), (Berlin, Heidelberg), pp. 129–140, Springer Berlin Heidelberg, 1992.

[65] L. Network, "The liquid network." `https://liquid.net/`. Last Accessed on 02/2023.

[66] A. M. Pinto, "An introduction to the use of zk-snarks in blockchains," *Journal of Open Innovation: Technology, Market, and Complexity*, 2019.

[67] Zcash, "Zcash - all coins are created equal.." `https://z.cash/`, 2021. Last Accessed on 02/2023.

[68] Paxful, "Bitcoin taproot upgrade: Everything you need to know," *Paxful University*, 2021.

[69] R. C. Merkle, *SECRECY, AUTHENTICATION, AND PUBLIC KEY SYSTEMS*. Stanford University, Stanford, CA, 1979.

[70] M. Szydlo, "Merkle Tree Traversal in Log Space and Time," in *Advances in Cryptology - EUROCRYPT 2004* (C. Cachin and J. L. Camenisch, eds.), (Berlin, Heidelberg), pp. 541–554, Springer Berlin Heidelberg, 2004.

[71] A. Poelstra, "Scriptless scripts," 2018. Presented at Layer 2 Summit Hosted by MIT DCI and Fidelity Labs.

[72] J. Poon and T. Dryja, "The bitcoin lightning network: Scalable off-chain instant payments," *arXiv preprint arXiv:1602.07982*, 2016.

[73] A. Narayanan, "Escrow protocols for cryptocurrencies: How to buy physical goods using bitcoin," in *Proceedings of the 2016 ACM Workshop on Blockchain, Cryptocurrencies and Contracts*, pp. 29–34, ACM, 2016.

[74] A. Greenberg, "The dark web's favorite cryptocurrency is getting a hardware wallet," *Wired*, August 2021.

[75] W. Wang, "Upbit is the seventh major crypto exchange hack of 2019," *CoinDesk*, November 2019.

[76] L. Valenta and B. Rowan, "Blindcoin: Blinded, accountable mixes for bitcoin," in *Financial Cryptography Workshops*, 2015.

[77] E. Heilman, L. Alshenibr, F. Baldimtsi, A. Scafuro, and S. Goldberg, "Tumblebit: An untrusted bitcoin-compatible anonymous payment hub." Cryptology ePrint Archive, Paper 2016/575, 2016.

[78] Blockchain.com, "Blockchain data api." `https://www.blockchain.com/explorer/api/blockchain_api`. Last Accessed on 03/2023.

[79] G. Maxwell, "Coinjoin: Bitcoin privacy for the real world." `https://bitcointalk.org/index.php?topic=279249.0`. Last Accessed on 02/2023.

[80] JoinMarket-Org, "Joinmarket-docs: High-level design." https://github.com/JoinMarket-Org/JoinMarket-Docs/blob/master/High-level-design.md, 2021. Last Accessed on 03/2023.

[81] S. Wallet, "Whirlpool." https://samouraiwallet.com/whirlpool, accessed 2023.

[82] nopara73, "Zerolink." GitHub repository, 2021.

[83] D. Chaum, *Blind Signature System*, pp. 153–153. Boston, MA: Springer US, 1984.

[84] kilerstorm, "Coin mixing using chaum's blind signatures." https://bitcointalk.org/index.php?topic=150681.0.

[85] nopara73, "Wasabivssamourai." https://github.com/nopara73/WasabiVsSamourai, 2021. Accessed: 2023-03-07.

[86] nopara73, "Dumplings." https://github.com/nopara73/Dumplings, Accessed March 2023.

[87] L. Wu, Y. Hu, Y. Zhou, H. Wang, X. Luo, Z. Wang, F. Zhang, and K. Ren, "Towards Understanding and Demystifying Bitcoin Mixing Services," in *Proceedings of the Web Conference 2021*, pp. 33–44, Apr. 2021.

[88] R. Stütz, J. Stockinger, B. Haslhofer, P. Moreno-Sanchez, and M. Maffei, "Adoption and actual privacy of decentralized coinjoin implementations in bitcoin," in *28th USENIX Security Symposium (USENIX Security 19)*, pp. 1169–1186, USENIX Association, 2019.

[89] GraphSense Team, "Graphsense." https://graphsense.info/, accessed 2023.

[90] M. Chase, S. Meiklejohn, and G. Zaverucha, "Algebraic macs and keyed-verification anonymous credentials," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, CCS '14, (New York, NY, USA), Association for Computing Machinery, 2014.