Πανεπιστήμιο Πειραιώς
Σχολή Τεχνολογιών Πληροφορικής και Επικοινωνιών
Τμήμα Ψηφιακών Συστημάτων

Ιδιωτικότητα σε Blockchain

Μελέτη προβλημάτων Ιδιωτικότητας
σε βάσεις δεδομένων Blockchain
σε θεωρητικό και πρακτικό επίπεδο

Θεοφάνης Τριανταφύλλης
E17150
fanis_30fillis@outlook.com

Επιβλέπων Καθηγητής:
Στέφανος Γκρίτζαλης, Καθηγητής

Ιδιωτικότητα Στο Διαδίκτυο

Απρίλιος 2021

Περιεχόμενα

Κεφάλαιο 0

Εισαγωγή

Η τεχνολογία Blockchain παρουσιάστηκε το 2008 από τον Satoshi Nakatomo [1] και πλέον είναι μια πολυσυζητημένη τεχνολογία αποθήκευσης δεδομένων. Σήμερα χρησιμοποιείται κατά κόρον στα κρυπτονομίσματα αλλά οι ιδιότητες που έχει την κάνουν ιδανική τεχνολογία για χρήση σε πολλά άλλα πεδία.

Στόχος αυτής της εργασίας είναι να αναλύσει τα προβλήματα που αντιμετωπίζουν οι βάσεις δεδομένων Blockchain όσο αφορά την ιδιωτικότητα σε θεωρητικό επίπεδο και σε πρακτικό εξετάζοντας μερικές εφαρμογές των Blockchain.

Στο πρώτο μέρος αναφέρονται οι έννοιες και γνώσεις που χρειάζονται για την κατανόηση των επόμενων κεφαλαίων.
Στο πρώτο κεφάλαιο παρουσιάζονται συνοπτικά οι κρυπτογραφικές γνώσεις που χρειάζονται για να κατανοηθεί η Blockchain και ορισμένοι τρόποι προστασίας της ιδιωτικότητας.
Στο δεύτερο κεφάλαιο παρουσιάζεται η τεχνολογία των Blockchain και παρουσιάζεται η χρήση τους στο Bitcoin, στο Ethereum και στο Monero.

Στο τρίτο κεφάλαιο γίνεται μια σύντομη αναφορά στον ορισμό της ιδιωτικότητας, τα προσωπικά δεδομένα και στον Γενικό Κανονισμό Προστασίας Δεδομένων.

Στο μέρος δεύτερο ελέγχεται η τεχνολογία Blockchain για πιθανά προβλήματα με την ιδιωτικότητα και εξετάζονται τα προβλήματα με τον κανονισμό GDPR.

Στο τέταρτο κεφάλαιο αναλύονται τα προβλήματα της ιδιωτικότητας σε μια βάση δεδομένων Blockchain.

Στο πέμπτο κεφάλαιο αναλύεται η σχέση και τα πιθανά σημεία τριβής μεταξύ των Blockchain και του κανονισμού GDPR.

Μέρος Ι

Γνωστικό Υπόβαθρο

Κεφάλαιο 1

Κρυπτογραφία

Η τεχνολογία Blockchain χρησιμοποιεί ορισμένες κρυπτογραφικές έννοιες για την λειτουργία της, γι' αυτό είναι απαραίτητη μια επιφανειακή γνώση αυτών των εννοιών ώστε να κατανοηθεί η τεχνολογία Blockchain.

Οι έννοιες που παρουσιάζονται στο κεφάλαιο είναι η κρυπτογραφία δημοσίου κλειδιού, οι συναρτήσεις κατακερματισμού και οι συναρτήσεις κατακερματισμού χαμαιλέοντα, οι ψηφιακές υπογραφές, οι ανώνυμες υπογραφές, οι αποδείξεις μηδενικής γνώσης και τα πρωτόκολλα τίμιας εναλλαγής.

1.1 Κρυπτογραφία Δημοσίου Κλειδιού

Στη κρυπτογραφία δημοσίου κλειδιού χρειαζόμαστε δύο κλειδιά για να κάνουμε κρυπτογράφηση και αποκρυπτογράφηση, το δημόσιο και το ιδιωτικό. Ότι κρυπτογραφείτε με το δημόσιο κλειδί αποκρυπτογραφείται με το ιδιωτικό και ότι κρυπτογραφείτε με το ιδιωτικό αποκρυπτογραφείτε με το δημόσιο. Θέλουμε όλοι να γνωρίζουν το δημόσιο κλειδί και πρέπει μόνο ο κάτοχος να γνωρίζει το ιδιωτικό κλειδί, αυτό επιτρέπει να υποθέσουμε ότι όταν ένα αντικείμενο, όπως ένα κείμενο, είναι κρυπτογραφημένο με το ιδιωτικό κλειδί μιας οντότητας τότε αυτό το έχει κάνει η συγκεκριμένη οντότητα[2]. Παραδείγματα τέτοιων κρυπτοσυστημάτων είναι τα κρυπτοσυστήματα ελλειπτικών καμπυλών [3] και το κρυπτοσύστημα RSA [4].

1.2 Συναρτήσεις Σύναψης

Οι Συναρτήσεις Σύνοψης (Hash Functions) δέχονται μια είσοδο και παράγουν μια έξοδο, η έξοδος θα είναι ένας αριθμός ιδανικά μοναδικά συνδεδεμένος με την είσοδο, όμως λόγο ότι έχουν πεπερασμένο αριθμό εξόδων και σχεδόν άπειρο αριθμό εισόδων δεν είναι απίθανο να βρεθούν δύο αντικείμενα με το ίδιο Hash, πρέπει να είναι υπολογιστικά αδύνατο να βρεθούν δύο είσοδοι που έχουν ως αποτέλεσμα την ίδια έξοδο, διαφορετικά δεν θεωρείτε ασφαλής η συνάρτηση. Επίσης οι συναρτήσεις αυτές πρέπει είναι μη αναστρέψιμες, δηλαδή δεν μπορεί κάποιος έχοντας το αποτέλεσμα μόνο να φτάσει στο αρχικό κείμενο [2]. Τέτοιες συναρτήσεις είναι η MD5 [5] και ο SHA-256 [6].

1.2.1 Συναρτήσεις Σύνοψης Χαμαιλέοντα

Οι συναρτήσεις σύνοψης χαμαιλέοντα είναι συναρτήσεις σύνοψης που έχουν μια κρυφή συνάρτηση κερκόπορτας (trapdoor function) που επιτρέπει την αποδοτική εύρεση συγκρούσεων τιμών εισόδου [7].

1.3 Ψηφιακές Υπογραφές

Οι ψηφιακές υπογραφές χρησιμοποιούν την κρυπτογραφία δημοσίου κλειδιού και τις συναρτήσεις Hash για να υπογράψει μια οντότητα ένα αντικείμενο, όπως ένα έγγραφο, η υπογραφή αυτή έχει την ίδια χρησιμότητα με μια φυσική υπογραφή ενός ατόμου. Επίσης εγγυάται ότι το αντικείμενο έχει υπογραφεί με τη μορφή που έχει από αυτή την οντότητα και δεν έχει γίνει τροποποίηση από κάποιον κακόβουλο. Για να δημιουργηθεί μια ψηφιακή υπογραφή ο υπογράφων παίρνει την Hash ενός αντικειμένου και την κρυπτογραφεί με το ιδιωτικό του κλειδί, όποιος θέλει να επιβεβαιώσει την υπογραφή αποκρυπτογραφεί την Hash με το δημόσιο κλειδί της υπογράφουσας οντότητας και ελέγχει το Hash του αντικειμένου που έχει υπογράψει [2].

1.3.1 Τυφλές Υπογραφές

Στην κρυπτογραφία η τυφλές υπογραφές είναι υπογραφές αντικειμένων που έχουν γίνει με τέτοιο τρόπο ώστε ο υπογραφών να μην γνωρίζει το αντικείμενο που υπογράφει, δηλαδή ο αποστολέας στέλνει στην οντότητα ένα αντικείμενο με μια συνιστώσα τύφλωσης, ο υπογράφων το υπογραφεί χωρίς να ξέρει το τι είναι το έγγραφο και χωρίς να γνωρίζει την συνιστώσα τύφλωσης, και όταν το στείλει στον αποστολέα ο αποστολέας μπορεί να αφαιρέσει την συνιστώσα τύφλωσης και να πάρει το αρχικό μήνυμα υπογεγραμμένο [2].

1.4 Ομομορφική Κρυπτογραφία

Κρυπτογραφία με ομομορφία είναι ένα είδος κρυπτογραφίας που επιτρέπει την μεταβολή του κρυπτοκειμένου μέσω κάποιων υπολογισμών που έχουν ως αποτέλεσμα την αλλαγή του αρχικού κειμένου χωρίς να χρειάζεται να αποκρυπτογραφηθεί και να κρυπτογραφηθεί ξανά [8].

1.4.1 Συστήματα Δεσμεύσεων

Τα συστήματα δεσμεύσεων χρησιμοποιούνται για την δέσμευση μίας οντότητας για μια τιμή. Για παράδειγμα αν η Αλίκη και ο Βασίλης παίζουν κορώνα γράμματα και η Αλίκη θέλει να αποδείξει στον Βασίλη ότι επέλεξε τη κορώνα πρέπει να πάρει την τιμή της κορώνας και μία συνιστώσα, τις περνά από μια συνάρτηση σύνοψης και αποστείλει το αποτέλεσμα στο Βασίλη. Όταν γίνει η ρίψη του νομίσματος τότε η Αλίκη μπορεί να αποδείξει ότι επέλεξε την κορώνα αποστέλλοντας την πρόβλεψη της και την συνιστώσα στον Βασίλη για να επιβεβαιώσει ότι λέει την αλήθεια [9].

1.4.2 Δεσμεύσεις Pedersen

Οι δεσμεύσεις Pedersen είναι σαν τις κανονικές δεσμεύσεις μόνο που έχουν την προσθετική ομομορφική ιδιότητα, δηλαδή αν έχουμε δεσμεύσεις $C(a)$ και $C(b)$ τότε λόγω της ομομορφικής τους ιδιότητας μπορούμε να υπολογίσουμε $C(a) + C(b) = C(a + b)$ [9].

Κεφάλαιο 2

Blockchain

Σε αυτό το κεφάλαιο εξηγείται η τεχνολογία Blockchain καθώς και αναφέρονται μερικές υλοποιήσεις των Blockchain ενδεικτικά.

2.1 Ομότιμα Δίκτυα - Peer to Peer Networks

Η τεχνολογία Blockchain χρησιμοποιεί τα δίκτυα peer to peer για την υποδομή της βάσης δεδομένων και της επεξεργασίας που χρειάζεται. Αυτά τα δίκτυα είναι επίπεδα δίκτυα, δηλαδή δεν υπάρχει ιεραρχία κόμβων ούτε κεντρικός εξυπηρετητής. Οι κόμβοι έχουν κατανεμημένους πόρους για να ολοκληρώσουν ένα σκοπό με κατανεμημένο τρόπο [10], επίσης είναι πολύ κλιμακώσιμα [11]. Όλοι οι κόμβοι του συστήματος μπορούν να μάθουν τις διευθύνσεις των υπόλοιπων κόμβων και να ελέγξουν τις επικοινωνίες τους με άλλους κόμβους, επίσης οι κόμβοι είναι αυτόνομοι και κατά συνέπεια δεν είναι όλοι έμπιστοι.

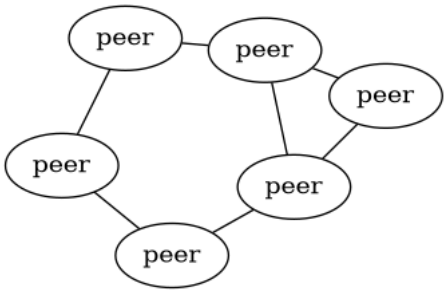


Figure 2.1: Τοπολογία ενός ομότιμου δικτύου

2.2 Τεχνολογία Blockchain

Η τεχνολογία Blockchain είναι, με πολύ απλά λόγια, μια μη μεταβαλλόμενη κατανεμημένη βάση δεδομένων, προτάθηκε αρχικά το 2008 από τον Satoshi Nakatomo στο έγγραφο Bitcoin: A Peer to Peer Electronic Cash System, όπου προτείνει το κρυπτονόμισμα Bitcoin που βασίζεται στο Blockchain [1]. Η Blockchain χρησιμοποιείται για να αποσιωπήσει την μη εξουσιοδοτημένη μεταβολή, επίσης γίνεται χρονική επισήμανση των δεδομένων και δημιουργείτε ένας ισχυρός δεσμός μεταξύ των κομματιών της αλυσίδας [12].

2.2.1 Κατανεμημένη Συμφωνία

Η κατανεμημένη συμφωνία είναι μια μέθοδος για να συμφωνήσουν όλοι οι κόμβοι του δικτύου για ποιο θα είναι το επόμενο τμήμα των Blockchain. Η σωστή λειτουργία της μεθόδου αυτής είναι ζωτικής σημασίας στη σωστή λειτουργία του Blockchain, μερικοί τρόποι για να επιτευχθεί η κατανεμημένη συμφωνία είναι [13]:

- Proof of Work
- Proof of Stake
- Proof of Importance

2.2.2 Πως Δουλεύει το Blockchain

Το Blockchain αποτελείτε από χρονικά επισημασμένα κομμάτια δεδομένων που είναι συνδεδεμένα μεταξύ τους μέσω ενός πολύπλοκου συνδέσμου. Όταν ένας κόμβος λαμβάνει εγγραφές, τις προσθέτει σε ένα τμήμα, υπολογίζει τον πολύπλοκο σύνδεσμο με το προηγούμενο κομμάτι και το δημοσιοποιεί. Αν οι υπόλοιποι κόμβοι συμφωνήσουν με βάση κάποιον αλγόριθμο κατανεμημένης συμφωνίας ότι το κομμάτι είναι νόμιμο τότε μπαίνει στην αλυσίδα. Μετά από αυτό τα δεδομένα στην Blockchain δεν μεταβάλλονται [14].

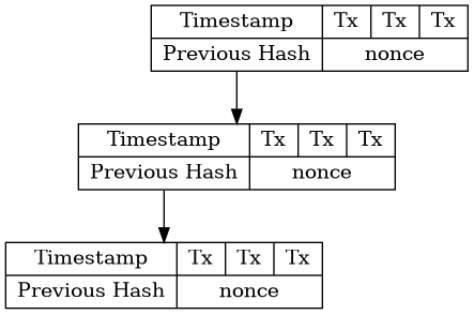


Figure 2.2: Μορφή ενός blockchain

2.2.3 Περιγραφή του Bitcoin Blockchain

Το Blockchain του κρυπτονομίσματος Bitcoin χρησιμοποιείται για να αποθηκεύει όλες τις συναλλαγές που γίνονται με το κρυπτονόμισμα ώστε να μην είναι δυνατό για κάποιον να διπλοξοδέψει ένα νόμισμα. Μια συναλλαγή αποτελείται από την ψηφιακή υπογραφή του τωρινού κατόχου του νομίσματος στη hash της προηγούμενης συναλλαγής και το δημόσιο κλειδί του επόμενου κατόχου, έτσι επιβεβαιώνεται η θέληση του κατόχου να κάνει την συναλλαγή. Αυτό σημαίνει ότι όλοι όσοι έχουν το Blockchain του Bitcoin μπορούν να δουν όλες τις συναλλαγές μεταξύ των οντοτήτων. Τα κομμάτια δεδομένων που αποθηκεύονται στους κόμβους έχουν συναλλαγές, το hash του προηγούμενου κομματιού, μια χρονική επισήμανση και ένα νούμερο nonce (number only used once) που αλλάζει για να πληρεί μερικά κριτήρια ως απόδειξη εργασίας (Proof of Work) [1], όπου όπου είναι ο τρόπος για να επιτευχθεί κατανεμημένη συμφωνία. Όταν ένας κόμβος έχει ολοκληρώσει τον υπολογισμό του κομματιού το δημοσιεύει σε άλλους κόμβους που το ελέγχουν για προσπάθειες διπλοξοδέματος, αν δεν υπάρχει τότε αρχίζουν να δουλεύουν στο επόμενο τμήμα της αλυσίδας.
Οι κόμβοι σε μια τέτοια Blockchain χωρίζονται σε κόμβους που λαμβάνουν εξωτερικές συνδέσεις (εξυπηρετητές) και σε κόμβους που δεν δέχονται συνδέσεις (πελάτες). Ανεξάρτητα από το αν ένας κόμβος είναι πελάτης ή εξυπηρετητής πρέπει να συνδέεται με τουλάχιστον 8 κόμβους ανά πάσα

στιγμή, στην περίπτωση που είναι πελάτης αυτοί οι κόμβοι λέγονται κόμβοι εσόδου (entry nodes) [15].

Μοντέλο Μη Σπαταλημένης Συναλλαγής

Σε αυτό το μοντέλο το υπόλοιπο ενός χρήστη είναι μια λίστα από συναλλαγές που έχει λάβει αλλά δεν έχει ξοδέψει ακόμη, το άθροισμα αυτών είναι το υπόλοιπο του λογαριασμού. Για να υπάρξει μια συναλλαγή πρέπει η κάθε είσοδος από ένα άτομο να είναι υπογεγραμμένη από τον ιδιοκτήτη και μη ξοδεμένη, αν υπάρχουν πολλές είσοδοι τότε όλες να είναι σωστά υπογεγραμμένες επίσης πρέπει ο αριθμός των εισόδων είναι ίσος ή μεγαλύτερος από τον αριθμό των εξόδων [16].
Ένα προτέρημα αυτού του μοντέλου είναι το πιθανώς υψηλό επίπεδο ιδιωτικότητας, καθώς επιτρέπει σε έναν χρήστη να έχει πολλούς λογαριασμούς χωρίς να υπάρχει σύνδεση μεταξύ τους, όμως υπάρχουν και αρνητικά όπως όταν ένας χρήστης έχει 10 Bitcoin στον λογαριασμό του και θέλει να στείλει 5 σε κάποιον πρέπει μετά το τέλος της συναλλαγής να κάνει μια πληρωμή 5 Bitcoin στον εαυτό του, αυτό μπορεί να διαρρεύσει πληροφορία σε κάποιον παρατηρητή [16].

2.2.4 Περιγραφή του Ethereum Blockchain

Το Blockchain του Ethereum έχει αρκετές ομοιότητες με το Blockchain του Bitcoin αλλά δεν είναι εντελώς όμοια, πέρα από τις συναλλαγές που αποθηκεύονται στο Blockchain υπάρχει η δυνατότητα για εκτέλεση προγραμμάτων στην Blockchain μέσω του EthereumVM που επιτρέπει την δημιουργία έξυπνων συμβολαίων και κατανεμημένων εφαρμογών [17]. Μια μεγάλη διαφορά μεταξύ του Bitcoin και του Ethereum είναι ο τρόπος που διαχειρίζονται τους λογαριασμούς των χρηστών, ενώ στο Bitcoin ο υπολογισμός του υπολοίπου ενός χρήστη γίνεται κοιτώντας τις συναλλαγές του στο Ethereum γίνεται με λογαριασμό, που είναι πιο απλός τρόπος αλλά λιγότερο ασφαλής [16].

Μοντέλο Βασισμένο σε Λογαριασμούς Επιγραμμικών Συναλλαγών

Αυτό το μοντέλο χρησιμοποιείται στο Ethereum για την διαχείρηση συναλλαγών των χρηστών, είναι πιο απλό από το μοντέλο του Bitcoin αλλά λιγότερο ασφαλές [16].

Ο κάθε λογαριασμος Ethereum έχει μια διεύθυνση 20 bytes (160 bit δημοσίου κλειδιού) και έχει 4 πεδία [17]:

- Ο αριθμός nonce (number only used once) που είναι ένας μετρητής των συναλλαγών.
- Το υπόλοιπο του λογαριασμού
- Ο κώδικας συμβολαίων, αν υπάρχει
- Ο αποθηκευτικός χώρος του λογαριασμού

Υπάρχουν δύο τύποι λογαριασμών, οι εξωτερικοί που ελέγχονται από ιδιωτικό κλειδί και λογαριασμούς συμβολαίων που ελέγχονται από τον κώδικα συμβολαίων τους [17].

2.2.5 Περιγραφή του Monero Blockchain

Το Monero είναι ένα κρυπτονόμισμα που έχει ώς αρχές την Ιδιωτικότητα, την Ασφάλεια, την Αποκέντρωση και να είναι ανταλλάξιμο [18, 19]. Οι σκοποί της Ιδιωτικότητας και της ασφάλειας επιτυγχάνονται χρησιμοποιώντας διάφορες τεχνικές βελτίωσης ιδιωτικότητας, όπως η απόκρυψη του αποστολέα, του παραλήπτη και του ποσού που αποστάλθηκε ενώ ταυτόχρονα παράγει διαβεβαιώσεις για την εγκυρότητα των συναλλαγών [19].

Το Monero χρησιμοποιεί δύο δημόσια και δύο ιδιωτικά κλειδιά για κάθε χρήστη. Για να λάβει χρήματα ένας χρήστης δημιουργεί μια διεύθυνση από τα δημόσια κλειδιά και όταν κάποιος θέλει να μεταφέρει χρήματα σε αυτόν τον χρήστη θα εισάγει μια νέα εγγραφή στη βάση δεδομένων την οποία μπορεί να δει και να ξοδέψει μόνο ο παραλήπτης με τα ιδιωτικά του κλειδιά [19]. Οι συναλλαγές αποθηκεύονται ως δεσμεύσεις Pedersen για να αποκρύψουν το ποσό.

Το Monero χρησιμοποιεί την απόδειξη μέσω εργασίας για την εισαγωγή νέων τμημάτων στην αλυσίδα [18].

2.2.6 Είδη Blockchain

Μπορούν να υπάρχουν πολλές διαφορετικές χρήσεις Blockchain για πολλές διαφορετικές ανάγκες, γιαυτό ορίζονται κάποια είδη ανάλογα με την προσβασιμότητα στα δεδομένα[20, 21]:

- Δημόσια
  Είναι δημοσίως διαθέσιμη, όλοι έχουν πρόσβαση στα δεδομένα που είναι στη βάση δεδομένων
- Ιδιωτική
  Την διαχειρίζεται ένας φορέας που είναι υπεύθυνος για την λειτουργία της.
- Κοινοτική
  Είναι διαθέσιμη σε μια ομάδα από φορείς οι οποίοι μπορεί να έχουν κοινά ενδιαφέρονται και έχουν όλοι οι φορείς πρόσβαση στη βάση δεδομένων.
- Υβριδική
  Είναι συνδυασμός οποιονδήποτε δύο από τα πάνω.

Επίσης γίνεται διαχωρισμός με βάση την εξουσιοδότηση που χρειάζεται για τη συμμετοχή στο Blockchain:

- Χωρίς εξουσιοδότηση
  Οποιοσδήποτε μπορεί να συμμετέχει στη Blockchain, δηλαδή να επεξεργάζεται και να βλέπει τα δεδομένα.
- Με Εξουσιοδότηση
  Πρέπει κάποιος να έχει εξουσιοδότηση για να συμμετέχει, είτε για να δει τα δεδομένα είτε για να έχει ενεργό ρόλο στη Blockchain.
- Υβριδικές
  Συνδυασμός των δύο παραπάνω, για παράδειγμα μπορεί να επιτρέπεται να είναι δημοσίως προσβάσιμη η βάση δεδομένων αλλά να μπορούν να συμμετέχουν μόνο εξουσιοδοτημένοι κόμβοι.

Κεφάλαιο 3

Ιδιωτικότητα και Προσωπικά Δεδομένα

Σε αυτό το κεφάλαιο γίνεται μια σύντομη αναφορά στον ορισμό της ιδιωτικότητας και περιγράφονται οι κύριοι ορισμοί και τα κύρια σημεία του Γενικού Κανονισμού Προστασίας Δεδομένων.

3.1 Ιδιωτικότητα

Η ιδιωτικότητα πλέον είναι ένα ανθρώπινο δικαίωμα, έχει χαρακτηριστεί ως απαραίτητο για την δημοκρατία, την κοινωνία και την ελευθερία ενός ατόμου. Δεν είναι όμως εύκολος ο προσδιορισμός της έννοιας της λέξης [22].

Το Blockchain είναι μια βάση δεδομένων στην οποία αποθηκεύονται δεδομένα μικρού όγκου. Επειδή το μοντέλο αυτό εφαρμόζεται καλύτερα σε δεδομένα που έχουν μορφή συναλλαγών [23] ορίζουμε δύο περιπτώσεις ιδιωτικότητας, την ιδιωτικότητα των οντοτήτων και την ιδιωτικότητα των δεδομένων.

Ιδιωτικότητα Οντοτήτων ονομάζουμε την μη συνδεσιμότητα μεταξύ οντότητας και εγγραφής στη βάση δεδομένων. Όταν έχουμε ιδιωτικότητα οντοτήτων δεν μπορεί κάποιος επιτιθέμενος να συνδέσει εγγραφή με οντότητα.

Ιδιωτικότητα Δεδομένων ονομάζουμε το να μην μπορεί κάποιος να διαβάσει το περιεχόμενο των εγγραφών που υπάρχουν στην Blockchain. Ουσιαστικά είναι η εμπιστευτικότητα των δεδομένων που αποθηκεύονται.

Στην ιδανική περίπτωση θα έχουμε ιδιωτικότητα οντοτήτων και την ιδιωτικότητα των δεδομένων.

3.2 Προσωπικά Δεδομένα και Γενικός Κανονισμός Προστασίας Δεδομένων

Ο Κανονισμός 2016/679 (GDPR) της Ευρωπαϊκής Ένωσης ψηφίστηκε το 2016 από το Ευρωπαϊκό Κοινοβούλιο και τέθηκε σε ισχύ το 2018, αφορά την προστασία προσωπικών δεδομένων των Ευρω-

παίων πολιτών και για να θεσπιστεί ένα κοινό πλαίσιο για όλες τις χώρες της Ευρωπαϊκής Ένωσης.

Ο Γενικός Κανονισμός Προστασίας Δεδομένων εφαρμόζεται πάνω στα προσωπικά δεδομένα, δηλαδή ο ορισμός των προσωπικών δεδομένων ορίζει την λειτουργία του κανονισμού [24].
Το άρθρο 4 του κανονισμού ορίζει τα προσωπικά δεδομένα ως δεδομένα που μπορεί να οδηγήσουν σε ταυτοποίηση, τέτοια δεδομένα δεν είναι μόνο το ονοματεπώνυμο ή πληροφορίες για εμάς αλλά οποιαδήποτε δεδομένα που μπορούν να χρησιμοποιηθούν έμμεσα ή άμεσα για να ταυτοποιήσουν ένα υποκείμενο, όπως η διεύθυνση IP. Επίσης υπάρχει το ενδεχόμενο να αποκαλυφθεί η ταυτότητα ενός υποκειμένου από την πρόσμιξη πολλών δεδομένων που από μόνα τους δεν βάζουν σε κίνδυνο την ταυτότητα ενός ατόμου. Ενδέχεται κάποια δεδομένα να είναι προσωπικά ανάλογα με τον σκοπό του υπεύθυνου των δεδομένων, επίσης ακόμα και τα αναληθή δεδομένα είναι προσωπικά δεδομένα.

3.2.1 Ψευδωνυμοποίηση των Δεδομένων

Η ψευδωνυμοποίηση σύμφωνα με το άρθρο 4 του κώδικα GDPR είναι η επεξεργασία των προσωπικών δεδομένων με τέτοιο τρόπο ώστε να είναι αδύνατη η σύνδεση με μια οντότητα χωρίς επιπλέον πληροφορίες, δεδομένου ότι οι πληροφορίες αυτές κρατούνται ξεχωριστά από τα δεδομένα. Σύμφωνα με την Ομάδα του ΄Αρθρου 29 η ψευδωνυμοποίηση κάνει την συνδεσιμότητα δεδομένων και οντότητας πιο δύσκολη και όχι αδύνατη, κατά συνέπεια τα ψευδωνυμοποιημένα δεδομένα πρέπει να θεωρούνται προσωπικά δεδομένα [25]. Το GDPR θεωρεί την ψευδωνυμοποίηση των δεδομένων ως μια τεχνική για την διαχείριση του κινδύνου και στο ΄Αρθρο 5 του κανονισμού θεωρεί την ψευδωνυμοποίηση ως πειστήριο της συμμόρφωσης του υπευθύνου των δεδομένων με τον κανονισμό.

3.2.2 Ανωνυμοποίηση των Δεδομένων

Μετά από την σωστή ανωνυμοποίηση των δεδομένων τα δεδομένα δεν μπορούν να συνδεθούν με μια οντότητα με κανέναν τρόπο και κατά συνέπεια δεν εφαρμόζεται το GDPR σε αυτά καθώς δεν συνδέονται με μια οντότητα. Η μετατροπή των δεδομένων σε ανώνυμα δεν είναι μια απλή διαδικασία καθώς πρέπει να τροποποιηθούν τα δεδομένα ώστε να είναι αδύνατη η σύνδεση τους ανάλογα με τις μεθόδους που ενδέχεται να χρησιμοποιηθούν, αυτό σημαίνει ότι ανωνυμοποιημένα δεδομένα ενδέχεται να είναι δυνατή η σύνδεση τους με ένα πρόσωπο αλλά πρέπει και η διαδικασία να μην είναι αναστρέψιμη [26].

3.3 Οντότητες στην Επεξεργασία Δεδομένων

Η νομοθεσία ορίζει τέσσερις οντότητες, το υποκείμενο των δεδομένων, τον υπεύθυνο επεξεργασίας, τον εκτελών την επεξεργασία και την τρίτη οντότητα. Οι πιο σημαντικές είναι ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία. Το υποκείμενο των δεδομένων είναι η οντότητα που παραχωρεί τα δεδομένα και η τρίτη οντότητα είναι μια οντότητα που λαμβάνει τα δεδομένα από τον υπεύθυνο αλλά δεν τα επεξεργάζεται.

Υπεύθυνος Επεξεργασίας

Είναι η οντότητα που κρατάτε νομικά υπεύθυνη για την συμμόρφωση με τον κανονισμό. Έχει την υποχρέωση να λαμβάνει μέτρα για να προστατεύσει τα δεδομένα, τόσο σε τεχνολογικό όσο και σε οργανωτικό επίπεδο. Πρέπει να ξέρει τι δεδομένα επεξεργάζεται ο φορέας και τι επεξεργασία

κάνει. Επίσης σε περίπτωση προβλήματος με τα δεδομένα είναι νομικά υποχρεωμένος να πληροφορήσει τα υποκείμενα των δεδομένων [24]. Επιτρέπεται να υπάρχουν περισσότεροι από ένας υπεύθυνοι επεξεργασίας [24].

Εκτελών της Επεξεργασίας

Είναι η οντότητα που εκτελεί την επεξεργασία με βάση τις οδηγίες που έχει λάβει από τον υπεύθυνο της επεξεργασίας. Επίσης δέχεται οδηγίες για την ασφάλεια των δεδομένων που επεξεργάζεται και είναι υποχρεωμένος να ακολουθεί το GDPR ανεξάρτητα από τις οδηγίες του υπευθύνου.

3.4 Αρχές της Επεξεργασίας

Οι αρχές του κανονισμού ορίζονται στο άρθρο 5 και αποτελούν ίσως το σημαντικότερο κομμάτι του κανονισμού. Καθορίζουν το πως πρέπει να γίνει η επεξεργασία ώστε να ακολουθεί το νομικό πλαίσιο και να σέβεται την ιδιωτικότητα των χρηστών. Οι αρχές της επεξεργασίας που πρέπει να ακολουθεί ένας φορές που επεξεργάζεται προσωπικά δεδομένα είναι:

- Νομιμότητα της Επεξεργασίας
  Αρχικά η επεξεργασία που πρόκειται να γίνει πρέπει να είναι νόμιμη, δηλαδή όταν βασίζεται σε μια από τις βάσεις νομιμότητας επεξεργασίας που καθορίζονται στο άρθρο 6 του κανονισμού και όταν τηρεί τις αρχές του κανονισμού σχετικά με την επεξεργασία [27].
- Ο σκοπός επεξεργασίας
  Ο σκοπός επεξεργασίας πρέπει να είναι νόμιμος, καλά και καθαρά καθορισμένος στο υποκείμενο των δεδομένων, επίσης τα δεδομένα που αποκτούνται για την εκπλήρωση αυτού του σκοπού πρέπει να χρησιμοποιούνται αποκλειστικά γι' αυτόν το σκοπό.
- Ελαχιστοποίηση των Δεδομένων
  Αυτή η αρχή καθορίζει ότι τα δεδομένα που συλλέγονται πρέπει να ανταποκρίνονται στον σκοπό που θα εκπληρώσουν, δεν επιτρέπεται να ζητηθούν περισσότερα δεδομένα απ' όσα είναι απαραίτητα για την επίτευξη του εκάστοτε σκοπού.
- Εγκυρότητα των δεδομένων
  Τα δεδομένα πρέπει να είναι έγκυρα και όταν χρειάζεται να ενημερώνονται. Αυτό σημαίνει ότι τα υποκείμενα έχουν το δικαίωμα να ζητήσουν την διόρθωση των δεδομένων αν παρατηρήσουν ασυνέχεια [26].
- Ακεραιότητα και Εμπιστευτικότητα
  Τα προσωπικά δεδομένα πρέπει να επεξεργάζονται με τρόπο που διασφαλίζει την ασφάλεια τους [26].

Δικαιώματα των Υποκειμένων

Από τις παραπάνω αρχές προέρχονται ορισμένα δικαιώματα των υποκειμένων των δεδομένων [26]:

- Δικαίωμα της Διόρθωσης
  Αν το υποκείμενο διαπιστώσει ασυνέχεια στα δεδομένα της τότε έχει το δικαίωμα να ζητήσει διόρθωση των δεδομένων.
- Δικαίωμα της Διαγραφής
  Όταν τα δεδομένα δεν είναι χρήσιμα για τον σκοπό που συλλέχθηκαν τότε πρέπει να διαγράφονται.

- Δικαίωμα της Πρόσβασης
  Τα υποκείμενα έχουν το δικαίωμα να ζητήσουν τα δεδομένα τα οποία έχει στην κατοχή του ο υπεύθυνος της επεξεργασίας.
- Δικαιώματα σχετικά με την αυτοματοποιημένη επεξεργασία
  Αυτά τα δεδομένα αφορούν την δημιουργία προφίλ των υποκειμένων και το ενδεχόμενο να υπάρξουν νομικές επιπτώσεις στο υποκείμενο.

3.5 Νομική Βάση της Επεξεργασίας

Για να πραγματοποιηθεί επεξεργασία δεδομένων πρέπει αυτή να στηρίζεται σε κάποια νομική βάση. Οι βάσεις της επεξεργασίας σύμφωνα με το άρθρο 6 του κανονισμού GDPR είναι:

- Συναίνεση
  Για την επεξεργασία των δεδομένων απαιτείται η συναίνεση του υποκειμένου των δεδομένων.
- Λόγω Συμβολαίου
- Λόγω Νομικών Υποχρεώσεων
- Αν είναι Ζωτικής Σημασίας του υποκειμένου ή άλλης φυσικής οντότητας
- Δημόσιο Συμφέρων
- Έννομο Συμφέρων του Υπευθύνου δεδομένων ή τρίτης οντότητας

Μέρος ΙΙ

Έλεγχος Προβλημάτων των Blockchain

Κεφάλαιο 4

Προβλήματα Ιδιωτικότητας Blockchain

Σε αυτό το κεφάλαιο παρουσιάζονται τα γενικά προβλήματα ιδιωτικότητας των Blockchain και τους πιθανούς τρόπους για να επιλυθούν.

4.1 Μελέτη της Monero Blockchain

Το ψηφιακό νόμισμα Monero εγγυάται την ασφάλεια και την ιδιωτικότητα των οντοτήτων που πραγματοποιούν τις συναλλαγές, λόγω αυτού αξίζει να γίνει αναφορά σχετικά με τους τρόπους που προσπαθεί να επιτύχει τους σκοπούς. Όπως θα φανεί η ιδιωτικότητα των οντοτήτων και των δεδομένων είναι στενά συνδεδεμένες. Γι' αυτό αξίζει να αναλυθεί η λειτουργία του.

4.1.1 Ιδιωτικότητα Οντοτήτων

Ένας από τους στόχους του Monero είναι να διασφαλίσει την ιδιωτικότητα των οντοτήτων, αυτό γίνεται κυρίως με την απόκρυψη των διευθύνσεων.

Διευθύνσεις

Αρχικά κάθε χρήστης του Monero έχει δύο ζευγάρια κλειδιών, το κλειδί της επίβλεψης (view key), που χρησιμοποιείται από έναν χρήστης για να δει το υπόλοιπο του, και το κλειδί του ξοδέματος (spend key) που χρησιμοποιείται για να ξοδέψει τα χρήματα που έχει [9].
Όταν ένας χρήστης θέλει να λάβει χρήματα στέλνει την διεύθυνση του στον αποστολέα ο οποίος εφαρμόζει ένα πρωτόκολλο ανταλλαγής κλειδιών σαν το Diffie Hellman και δημιουργεί μια προσωρινή διεύθυνση για κάθε έξοδο της συναλλαγής, έτσι είναι αδύνατο να βρεθεί μια δημόσια διεύθυνση από έναν επιτιθέμενο [9]. Αρχικά για να γίνει μια συναλλαγή ο αποστολέας πρέπει να ξέρει την δημόσια διεύθυνση του παραλήπτη. Μια συναλλαγή ακολουθεί τα βήματα [9]:

1. Ο αποστολέας δημιουργεί ένα τυχαίο αριθμό r και υπολογίζει την μοναδική διεύθυνση $K^o = H_n * (r * K_B^v) * G + K_B^s$
2. Η μοναδική διεύθυνση τίθεται ως ο παραλήπτης της συναλλαγής και μπαίνει στο δίκτυο
3. Ο παραλήπτης χρησιμοποιώντας τις $r*G$ και K^o μπορεί να υπολογίσει το $K_B^v * r * G = r * K_B^v$. Μετά από αυτό μπορεί να υπολογίσει το $K_B^s = K^o - H_n * (r * K_B^v) * G$. Αν το $K_B^s = K_B^s$ γνωρίζει ότι απευθύνεται σε αυτόν. Το k_B^v είναι το ιδιωτικό κλειδί ελέγχου του παραλήπτη και όποιος το έχει μπορεί να δει όλες του τις συναλλαγές

4. Τα κλειδιά της συναλλαγής είναι
   $K^o = H_n * (r * K_B^v) * G + K_B^s = (H_n(r * K_B^v) + k_B^s) * G$
   $k^o = H_n * (r * K_B^v) + K_B^s$

Το μόνο που χρειάζεται για να ξοδέψει ο αποστολέας το ποσό πρέπει να υπογράψει ένα μήνυμα με το κλειδί K^o. Το κλειδί k_B^s απαιτείται για την απόδειξη της ιδιοκτησίας του ποσού που έλαβε. Ο αποστολέας δεν μπορεί να καταλάβει αν ο παραλήπτης έχει ξοδέψει το ποσό χωρίς το κλειδί k^o που έχει μόνο ο παραλήπτης.
Στη περίπτωση πολλών εξόδων από μια συναλλαγή η κάθε έξοδος έχει ένα δείκτη ώστε τα κλειδιά της κάθε μίας εξόδου να είναι διαφορετικά.

Υποδιευθύνσεις

Ένας χρήστης Monero μπορεί να έχει υποδιευθύνσεις από κάθε διεύθυνση όταν δεν θέλει να δώσει την κύρια του διεύθυνση, τα χρήματα που αποστέλλονται σε μια υποδιεύθυνση μπορούν να ξοδευτούν με τα κλειδιά της κύριας διεύθυνσης [9].

Υπογραφές Δακτυλίου

Οι υπογραφές δακτυλίου αναφέρονται στην εισαγωγή 4.2.2, εδώ θα αναλυθεί η χρήση τους στο Monero.

Όταν μια οντότητα θέλει να κάνει μια συναλλαγή τότε επιλέγει μερικά τυχαία δημόσια κλειδιά, που δεν ανήκουν στην οντότητα, και πολυπλέκει τα δημόσια τους κλειδιά για εκτροπή τυχών παρατηρητών, έτσι το δίκτυο μπορεί να δει ότι ένα από τις εξόδους ξοδεύεται αλλά δεν ξέρει πια οντότητα ξοδεύει [19].

Αναγνωριστικά Συναλλαγών

Τα αναγνωριστικά των συναλλαγών δεν είναι απαραίτητο να υπάρχουν σε μια συναλλαγή αλλά υπάρχουν αν το ζητήσει ο παραλήπτης. Τα αναγνωριστικά μπορεί να είναι αποκρυπτογραφημένα στη Blockchain (clear text) αλλά αυτό αποτελεί κίνδυνο ιδιωτικότητας, γι'αυτό είναι δυνατό να ενσωματωθεί το αναγνωριστικό συναλλαγής στις διευθύνσεις των χρηστών και να δοθούν αυτές οι διευθύνσεις.

Το Πρωτόκολλο Dandelion++

Αυτή η τεχνική αφορά τον τρόπο με τον οποίο ανακοινώνονται οι συναλλαγές στο δίκτυο και έχει ως σκοπό την βελτίωση της ανωνυμίας των οντοτήτων που συμμετέχουν. Το πρωτόκολλο αυτό έχει δύο φάσεις: την φάση stem και την φάση fluff [28].

Στη φάση stem ένας κόμβος επιλέγει τυχαία δύο κόμβους στους οποίους είναι συνδεδεμένο, όταν χρειάζεται να ανακοινώσει μια συναλλαγή επιλέγει τυχαία έναν από τους δύο και στέλνει την συναλλαγή σε αυτόν.

Στη φάση fluff ένας κόμβος που δέχεται μια συναλλαγή την αποστέλλει σε όλες του τις εξερχόμενες συνδέσεις.

Ένας κόμβος κάθε λίγα λεπτά επιλέγει αν θα στέλνει δεδομένα με τρόπο stem ή fluff.

Αυτή η τεχνική εξασφαλίζει ότι ένας επιτιθέμενος δεν μπορεί να ακούσει για ανακοινώσεις καθώς ο αριθμός των ανακοινώσεων που έχουν γίνει πριν φτάσει στον επιτιθέμενο είναι άγνωστος.

4.1.2 Ιδιωτικότητα Δεδομένων

Ο κύριος τρόπος για την απόκρυψη των δεδομένων μιας συναλλαγής είναι οι Ring Confidential Transactions (RingCT).

Ring Confidential Transactions

Αυτή η τεχνολογία είναι ένας κρυπτογραφικός τρόπος για την απόκρυψη των ποσών που ανταλλάζονται ενώ ταυτόχρονα επιτρέπει σε έναν χρήστη να αποδείξει ότι έχει αρκετά χρήματα για μια συναλλαγή χωρίς να αποκαλύψει το συνολικό ποσό που διαθέτει. Αυτό το καθιστούν δυνατό οι δεσμεύσεις Pedersen και οι αποδείξεις εύρους [19].
Οι αποδείξεις εύρους είναι μια μέθοδος για να αποδειχθεί ότι το ποσό που έχει δεσμευτεί ένας χρήστης είναι μεγαλύτερο του μηδέν και μικρότερο από έναν συγκεκριμένο αριθμό [19].

4.2 Ιδιωτικότητα στα Υποκείμενα Δεδομένων σε Blockchain

Η ιδιωτικότητα των υποκειμένων των δεδομένων σημαίνει να μην υπάρχει συνδεσιμότητα μεταξύ φυσικών οντοτήτων και εγγραφών στην βάση δεδομένων, αν τα δεδομένα της βάσης δεδομένων είναι δημοσίως διαθέσιμα όπως σε αυτές των Bitcoin και Ethereum τότε η ιδιωτικότητα των οντοτήτων είναι απαραίτητη για να μην γνωρίζει ο καθένας το ιστορικό μιας οντότητας.

4.2.1 Επιθέσεις Σύνδεσης Φυσικών Οντοτήτων και Ψευδωνύμων

Τέτοιες επιθέσεις έχουν ως σκοπό την σύνδεση οντοτήτων και ψευδωνύμων σε Blockchains. Σε Blockchains που δεν παρέχουν εμπιστευτικότητα των δεδομένων πρέπει να παρέχουν ισχυρές τεχνικές για την μη συνδεσιμότητα οντοτήτων και δεδομένων για να διατηρήσουν την ιδιωτικότητα.

Σύνδεση οντοτήτων και διευθύνσεων στο δίκτυο Bitcoin

Μια τέτοια επίθεση περιγράφεται στο [15], όπου οι επιτιθέμενοι αρχικά συλλέγουν μια λίστα των διευθύνσεων των κόμβων (εξυπηρετητών και πελατών) που από αυτή τη λίστα επιλέγουν κάποιους για να κάνουν την επίθεση. Έπειτα για τους πελάτες σε αυτή τη λίστα βρίσκονται οι κόμβοι εισόδου που χρησιμοποιούν, αξίζει να σημειωθεί ότι για να γίνει η σύνδεση χρειάζεται να βρεθούν 3 κόμβοι εισόδου ενός πελάτη. Μετά ο επιτιθέμενος αντιστοιχεί συναλλαγές με τους κόμβους εισόδου και ελέγχει αν η διευθύνσεις των εξυπηρετητών Bitcoin είναι μέσα σε αυτές που επέλεξε για την επίθεση τότε έχει ζευγάρι διεύθυνσης και συναλλαγής. Αυτή η επίθεση έχει ποσοστό επιτυχίας από 10% έως 60% ανάλογα με το πόσο διακριτική θέλει να είναι η επιτιθέμενη.

Επίθεση στην Ανωνυμία του Monero

Πρόσφατα υπήρχε μια αποτυχημένη προσπάθεια επίθεσης τύπου Sybil στην ανωνυμία του Monero [29, 30].
Ο επιτιθέμενος εκτέλεσε κάποιους κόμβους στο δίκτυο και προσπάθησε να καταγράψει τις διευθύνσεις IP χρησιμοποιώντας μια ευπάθεια που ενίσχυε τις πιθανότητες να πετύχει την επίθεση του, λόγω της χρήσης του Dandelion++ η επίθεση ήταν αποτυχημένη. Αναφέρεται όμως και ότι αν ο

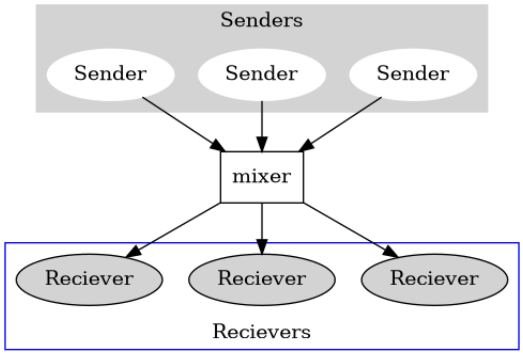
επιτιθέμενος είναι πιο ικανός και έχει καλύτερη χρηματοδότηση ενδέχεται η επίθεση να επιτύχει. Για αποφυγή τέτοιων επιθέσεων συνιστάτε η χρήση τεχνολογιών ανωνυμοποίησης όπως το Tor.

4.2.2 Τεχνικές Διασφάλισης Ιδιωτικότητας σε Blockchain

Οι τεχνικές διασφάλισης ιδιωτικότητας χρησιμοποιούνται για να βελτιώσουν την ανωνυμία των υποκειμένων των δεδομένων στις Blockchains.

Mixers

Οι Mixers είναι ένα εργαλείο που χρησιμοποιείται για να αποτρέψει την συνδεσιμότητα μεταξύ αποστολέα και παραλήπτη μιας συναλλαγής [31]. Σε κρυπτονομίσματα όπως το Bitcoin μεταφέρει νομίσματα από πολλές διευθύνσεις προς πολλές διευθύνσεις και μετά αποδίδει τα νομίσματα στους χρήστες ώστε να κάνει δύσκολη την ιχνιλάτηση τους από κάποιον επιτυθέμενο [32].



Ανώνυμες Υπογραφές

Οι ανώνυμες υπογραφές είναι υπογραφές σχεδιασμένες για να διατηρούν την ανωνυμία του υπογραφών, υπάρχουν υπογραφές συνόλων και υπογραφές δακτυλίου [33].

Οι Υπογραφές Συνόλων (Group Signatures) ουσιαστικά επιτρέπουν σε οποιαδήποτε μέλη ενός συνόλου να υπογράψουν ένα μήνυμα για όλο το σύνολο χρησιμοποιόντας το μυστικό του κλειδί. Αυτή η διαδικασία δεν φανερώνει κάτι σχετικά με το ποιο άτομο από το σύνολο έβαλε την υπογραφή, το σύνολο χρειάζεται έναν διαχειριστή για να διαχειρίζεται τα μέλη και να επιλύει τις διαφορές [33], αν χρειαστεί μπορεί να βρεθεί ο ακριβώς υπογραφών από τον διαχειριστή.

Οι Υπογραφές Δακτυλίου (Ring Signature) όπου πάλι έχουμε ένα σύνολο από το οποίο κάποια μπορεί να υπογράψει ένα έγγραφό αλλά οι διαφορές του με τις υπογραφές συνόλου είναι ότι η πραγματική ταυτότητα του υπογραφών δεν μπορεί να βρεθεί και οποιοιδήποτε χρήστες μπορούν να κάνουν ένα σύνολο [33].

4.3 Ιδιωτικότητα στα Δεδομένα των Blockchain

Τα περιεχόμενα στην Blockchain είναι δημοσίως προσβάσιμα γιατί είναι κατανεμημένη αρχιτεκτονική και όλοι έχουν ένα αντίγραφο των δεδομένων, αυτό σημαίνει ότι όλοι μπορούν να δουν τα δεδομένα. Για να υπάρξει ανωνυμία πρέπει να υπάρχει κρυπτογράφηση των δεδομένων ή κάποιος άλλος τρόπος όπως η αποθήκευση των hash των αντικειμένων και την αποθήκευση των δεδομένων

σε μια βάση δεδομένων εκτός της Blockchain. Κάτι τέτοιο όμως είναι αδύνατο στις Blockchain των Bitcoin, Ethereum και άλλων που βασίζονται στο να ελέγχεται το περιεχόμενο των δεδομένων για την ορθή λειτουργία τους.

4.4 Συμπεράσματα

Από τα παραπάνω μπορούμε να δούμε ότι απαιτούνται επιπλέον τεχνικές για την διασφάλιση της ανωνυμίας των οντοτήτων και της εμπιστευτικότητας των δεδομένων για να σχεδιαστεί μια Blockchain που προστατεύει την ιδιωτικότητα των ατόμων που συμμετέχουν.

4.4.1 Εμπιστευτικότητα μέσω Κρυπτογραφία

Η κρυπτογράφηση των δεδομένων είναι ένας τρόπος για να διασφαλιστεί η εμπιστευτικότητα τους. Κάτι τέτοιο γίνεται στο Monero με το RingCT με τις δεσμεύσεις Pedersen.

Η ομομορφική ιδιότητα (1.4) είναι πολύ χρήσιμη για την διασφάλιση της ιδιωτικότητας καθώς επιτρέπει να γίνουν πράξεις πάνω σε κρυπτογραφημένα δεδομένα χωρίς να αποκρυπτογραφηθούν. Αυτή η κρυπτογραφία μπορεί να παρέχει ιδιωτικότητα των δεδομένων σε μια Blockchain χωρίς να προκαλούνται προβλήματα στη λειτουργία της [33].

Κεφάλαιο 5

Blockchain και GDPR

Σε αυτό το κεφάλαιο αναφέρονται τα σημεία που μπορεί να υπάρξουν προβλήματα μιας Blockchain σχετικά με τον νόμο GDPR, πιθανές τους λύσεις και εξετάζονται υπάρχουσες Blockchain ως προς την συνοχή με την νομοθεσία.

5.1 Ρόλοι στο GDPR

Σε αυτή τη ενότητα θα ερευνηθούν οι ρόλοι του GDPR στις Blockchain και πιθανά προβλήματα καθορισμού. Η εύρεση των κατάλληλων υπευθύνων είναι ζωτικής σημασίας για την συμμόρφωση με τον κανονισμό.

5.1.1 Ποιος είναι ο Υπεύθυνος Επεξεργασίας σε Blockchain

Ο ρόλος του υπεύθυνου επεξεργασίας είναι ο πιο σημαντικός ρόλος γιατί ο υπεύθυνος σιγουρεύει ότι η βάση δεδομένων είναι συμβατή με τον κανονισμό και καθορίζει την επεξεργασία που θα γίνει στα δεδομένα.

Ιδιωτικές Blockchain

Σε Blockchains που είναι ιδιωτικές συνήθως υπάρχει ένας φορέας που αποφασίζει τα μέσα και τους σκοπούς επεξεργασίας, σε αυτές τις περιπτώσεις είναι ο υπεύθυνος των δεδομένων, όμως ενδέχεται να υπάρχουν κοινοί υπεύθυνοι σε μερικές περιπτώσεις [24]. Στην περίπτωση πολλών υπεύθυνων πρέπει να επιλεχθούν σωστά οι αρμοδιότητες του καθενός σύμφωνα με το ΄Αρθο 26 του GDPR [24].

Δημόσιες Blockchain

Στις δημόσιες Blockchains δεν είναι εύκολη υπόθεση η επιλογή του υπεύθυνου επεξεργασίας εξ' αιτίας του τρόπου λειτουργίας μιας τέτοιας Blockchain και της έλλειψης κεντρικής οντότητας.

Οι Προγραμματιστές της Blockchain είναι υπεύθυνοι για την υλοποίηση της βάσης δεδομένων, όμως συνήθως δεν είναι υπεύθυνοι για την κατεύθυνση που κατευθύνεται η βάση δεδομένων, η οποία βασίζεται στη δομή της Blockchain [24]. Γι' αυτό δεν πρέπει να θεωρούνται ελεγκτές [24, 26].

Οι κόμβοι Εξόρυξης είναι υπεύθυνοι της εισαγωγής δεδομένων σε Blockchain που έχουν πρωτόκολλο κατανεμημένης συμφωνίας με απόδειξη εργασίας [24]. Στην νεφοϋπολογιστική υπεύθυνος επεξεργασίας θεωρείται ο πάροχος των υποδομών καθώς αυτός παρέχει το λογισμικό, υλικό και τα κέντρα δεδομένων που χρησιμοποιούνται [24, 34]. Αναλογικά θα μπορούσε κάποιος να υποστηρίξει πως ως υπεύθυνοι πρέπει να οριστούν οι κάτοχοι των κόμβων εξόρυξης στο δίκτυο, καθώς κατεβάζοντας και εκτελώντας το πρόγραμμα σε δικό τους υλικό αποφασίζουν τον σκοπό και τα μέσα της επεξεργασίας [24, 26]. Όμως ελέγχουν τον σκοπό και τα μέσα της επεξεργασίας καθώς απλά εκτελούν το πρόγραμμα για το πιθανό κέρδος που μπορεί να έχουν [26].

Οι κόμβοι του δικτύου αποθηκεύουν πλήρες ή μερικώς την βάση δεδομένων και επικυρώνουν νέα τμήματα της Blockchain, όταν ένας κόμβος εξόρυξης υπολογίσει το hash ενός τμήματος τότε το λαμβάνουν οι κόμβοι και υπολογίζουν την σύνοψη για να επιβεβαιώσουν το τμήμα [24]. Υπάρχει η άποψη ότι οι κόμβοι μπορούν να οριστούν ως συνυπεύθυνοι των δεδομένων καθώς έχουν ίση ελευθερία και επιρροή στην επεξεργασία δεδομένων για να διαλέξουν ένα δίκτυο Blockchain.

Υπάρχουν πολλά μέρη που επηρεάζουν τα μέσα της επεξεργασίας, στις δημόσιες βάσεις δεδομένων οι ιδιοκτήτες των κόμβων επιλέγουν το υλικό που θα χρησιμοποιήσουν και οι προγραμματιστές αποφασίζουν τις αλλαγές που θα γίνουν στο λογισμικό [24]. Δεν υπάρχει καθαρή απάντηση στο ποιος θα πρέπει να είναι ο Υπεύθυνος Επεξεργασίας των δημοσίων Blockchains[26].

5.1.2 Ποιος Είναι ο Εκτελών την Επεξεργασία

Εδώ πάλι στις ιδιωτικές Blockchain που απαιτούν άδεια για την συμμετοχή δεν υπάρχει πρόβλημα με την επιλογή του Εκτελών καθώς υπάρχει η έμπιστη τρίτη οντότητα που ελέγχει τα δεδομένα.

Στις δημόσιες Blockchains υπάρχει πάλι πρόβλημα. Αρχικά για να οριστεί ο Εκτελών επεξεργασίας πρέπει να οριστεί ο Υπεύθυνος επεξεργασίας. Αν υποθέσουμε την ύπαρξη ενός Υπεύθυνου πάλι δεν μπορεί να οριστεί ένας Εκτελών την Επεξεργασία. Μια λύση θα ήταν να οριστούν οι ιδιοκτήτες των κόμβων ως εκτελών την επεξεργασία, αλλά και πάλι υπάρχουν .

5.2 Προσωπικά δεδομένα

Σε πολλές Blockchain τα δεδομένα εισάγονται από τα υποκείμενα των δεδομένων και δεν συλλέγεται από τον υπεύθυνο επεξεργασίας. Έτσι τα υποκείμενα έχουν τα ίδια τον έλεγχο των δεδομένων που θα αποθηκευτούν.
Το GDPR γράφηκε για την προστασία προσωπικών δεδομένων, όμως τα Blockchain μπορεί να αποθηκεύουν hash ευαίσθητων δεδομένων τα οποία δεν είναι ξεκάθαρο αν είναι ή όχι προσωπικά δεδομένα [26]. Σε αυτή την περίπτωση καλό είναι να υποθέσουμε ότι είναι προσωπικά δεδομένα και να ληφθούν οι κατάλληλες μέθοδοι για την προστασία τους.

5.2.1 Ακεραιότητα και Εμπιστευτικότητα Δεδομένων

Ένα από τα δικαιώματα των υποκειμένων είναι η ακεραιότητα και η εμπιστευτικότητα των δεδομένων. Η τεχνολογία Blockchain είναι σχεδιασμένη για να διασφαλίζει την ακεραιότητα των δεδομένων όμως δεν ισχύει κάτι τέτοιο για την εμπιστευτικότητα των δεδομένων όπως φάνηκε νωρίτερα 4.3.
Εφαρμογές όπως το Bitcoin δεν έχουν εμπιστευτικότητα των δεδομένων [1], άλλες εφαρμογές όπως το Monero υπάρχουν τεχνικές για την εμπιστευτικότητα των δεδομένων που αποθηκεύονται [19].

Από αυτά μπορούμε να συμπεράνουμε ότι δεν υπάρχει πρόβλημα με την ακεραιότητα και την εμπιστευτικότητα των δεδομένων εφόσον η Blockchain σχεδιαστεί σωστά.

5.3 Δικαιώματα Υποκειμένων

Σε αυτή την ενότητα θα ελέγξουμε το πως διατηρεί μια Blockchain τα δικαιώματα των υποκειμένων σύμφωνα με τον κανονισμό GDPR.

5.3.1 Διαγραφή Δεδομένων

Λόγω ότι του τρόπου λειτουργίας των Blockchain όπως προτάθηκε αρχικά είναι αδύνατη η διαγραφή οποιονδήποτε δεδομένων που είναι αποθηκευμένα χωρίς να αναιρεθεί ένα κομμάτι της εργασίας που έχει γίνει, παρόλα αυτά υπάρχουν τεχνολογίες που μπορούν να επιτύχουν την διαγραφή. Ένα πρόβλημα πηγάζει από το γεγονός ότι σύμφωνα με το GDPR πρέπει να διαγράφονται τα δεδομένα όταν δεν χρησιμοποιούνται, άλλο ένα πρόβλημα διαγραφής δεδομένων είναι ότι το υποκείμενο των δεδομένων έχει το δικαίωμα να αποσύρει την συναίνεση του οποτεδήποτε θέλει.

Πιθανές Μέθοδοι για Διαγραφή Δεδομένων

Έχουν βρεθεί μερικές λύσεις για το πρόβλημα της διαγραφής δεδομένων από την βάση δεδομένων, κάποιες από αυτές είναι οι παρακάτω.
Μια λύση θα ήταν να γίνει ένα παρακλάδι στην Blockchain από το σημείο που πρέπει να διαγραφούν τα δεδομένα, αυτό όμως μπορεί να απαιτεί τεράστια επεξεργαστική ισχύ ανάλογα με την χρονική στιγμή των δεδομένων που πρέπει να διαγραφούν, κατά συνέπεια αυτή η μέθοδος δεν είναι αξιόπιστη.

Τον σκοπό να κάνουν την διαγραφή δεδομένων δυνατή έχουν τα Reductuble Blockchains [7] που επιτρέπουν την διαγραφή δεδομένων με την χρήση συναρτήσεων κατακερματισμού χαμαιλέοντα, δηλαδή συναρτήσεις κατακερματισμού που έχουν μια παγίδα (trapdoor) που κάνει υπολογιστικά εύκολο τον υπολογισμό συγκρούσεων έτσι ώστε όταν υπάρχει ανάγκη για να γίνει διαγραφή δεδομένων απλά να αλλάξουν με τέτοιον τρόπο που δεν αλλάζει το αποτέλεσμα της συνάρτησης σύνοψης [7].

Μια άλλη έννοια είναι το κλάδεμα, αλλά αφορά μόνο τοπικά αντίγραφα και όχι ολόκληρη την Blockchain. Γίνεται διαγραφή ορισμένων κομματιών και όχι της Blockchain από ένα σημείο και πίσω [35].

Επίσης μπορεί να γίνεται έλεγχος κατά την εισαγωγή των δεδομένων ώστε να αποτραπεί η εισαγωγή δεδομένων που δεν θα πρέπει να είναι στη βάση δεδομένων. Για παράδειγμα δεν έχουν λόγο να είναι αποθηκευμένες οι εικόνες στο Bitcoin [36].

5.3.2 Διόρθωση των Δεδομένων

Η διόρθωση των δεδομένων είναι τροποποίηση των δεδομένων ώστε να διορθωθούν ατέλειες. Η τροποποίηση μπορεί να γίνει με την διαγραφή των δεδομένων σε ένα προγενέστερο στάδιο της βάσης δεδομένων και την επανεισαγωγή τους τροποποιημένα σε αργότερο σημείο.

5.3.3 Δικαίωμα της Πρόσβασης

Οι χρήστες έχουν το δικαίωμα να ζητήσουν αντίγραφο από τα δεδομένα που έχουν σε μια βάση δεδομένων από τον υπεύθυνο των δεδομένων που, όπως είδαμε νωρίτερα δεν είναι εύκολο να προσδιοριστεί σε μια τέτοια βάση δεδομένων. Ανεξάρτητα για το αν μιλάμε για δημόσια ή ιδιωτική Blockchain κάτι τέτοιο μπορεί να γίνει δεδομένου ενός διαχωριστικού χαρακτηριστικού των υποκειμένων, που στην περίπτωση του Bitcoin είναι το δημόσιο κλειδί του χρήστη.

5.4 Μελέτη Υπάρχοντων Blockchain

Σε αυτή την ενότητα ελέγχουμε Blockchains που υπάρχουν για να δούμε κατά πόσο εφαρμόζουν τον κανονισμό GDPR.

5.4.1 Bitcoin Blockchain

Εδώ θα μελετηθεί το κρυπτονόμισμα Bitcoin για την συμμόρφωση και πιθανά προβλήματα με τον κανονισμό GDPR.

Επιλογή Υπεύθυνου Δεδομένων και Εκτελών την Επεξεργασία

Αρχικά η Bitcoin Blockchain δεν έχει ορίσει Υπεύθυνο των δεδομένων και Εκτελών την επεξεργασία, άρα έρχεται σε αντίφαση με τον κανονισμό GDPR, φυσικά όπως φάνηκε παραπάνω το πρόβλημα στην επιλογή υπεύθυνου και εκτελών την επεξεργασία δεν έχει λυθεί ακόμα.

Δικαιώματα Υποκειμένων

Τα δικαιώματα των υποκειμένων είναι:

- Διαγραφή Δεδομένων
  Τα δεδομένα που αποθηκεύονται στη Blockchain του Bitcoin είναι συναλλαγές που ενδέχεται να υπάρχει λόγος για την αποθήκευση τους επ' αόριστον.
  Στο Bitcoin υπάρχει η δυνατότητα να εγγραφούν δεδομένα άσχετα με τον σκοπό της βάσης δεδομένων που δεν θα έπρεπε να υπάρχουν αλλά είναι ακόμα και σήμερα διαθέσιμα στη βάση δεδομένων [37].
- Διόρθωση
  Η μεταβολή των δεδομένων μετά την εισαγωγή τους στο Bitcoin δεν είναι δυνατή, άρα δεν είναι δυνατή η διόρθωση τους.
- Πρόσβαση
  Οι χρήστες έχουν άμεση πρόσβαση στα δεδομένα τους στη βάση δεδομένων.
- Αυτοματοποιημένη Επεξεργασία
  Στο Bitcoin δεν γίνεται αυτοματοποιημένη επεξεργασία με τρόπο που μπορεί να βλάψει νομικά ένα άτομο.

Προσωπικά Δεδομένα

Τα δεδομένα που αποθηκεύονται στο Bitcoin είναι συναλλαγές των χρηστών με τα δημόσια κλειδιά τους τα οποία θεωρούνται ψευδωνυμοποιημένα προσωπικά δεδομένα [24].

Οι απαιτήσεις που υπάρχουν από το GDPR σχετικά με τα προσωπικά δεδομένα είναι η εμπιστευτικότητα και η ακεραιότητα τους.

Το Bitcoin εξασφαλίζει την ακεραιότητα των δεδομένων χρησιμοποιώντας την Blockchain αλλά δεν υπάρχει εμπιστευτικότητα στα δεδομένα που αποθηκεύονται, δηλαδή μπορεί να τα δει και να τα επεξεργαστεί ο καθένας.

5.4.2 Monero Blockchain

Σε ότι αφορά την συμμόρφωση με το GDPR η Monero δεν είναι πολύ διαφορετικό αλλά είναι σχεδιασμένο με σκοπό την διασφάλιση της Ιδιωτικότητας.

Επιλογή Υπεύθυνου Δεδομένων και Εκτελών την Επεξεργασία

Όπως και στο Bitcoin το Monero δεν έχει υπεύθυνο επεξεργασίας ούτε εκτελών την επεξεργασία. Για να γίνει αυτό πρέπει να οριστούν αυτές οι οντότητες.

Δικαιώματα Υποκειμένων

Τα δικαιώματα των υποκειμένων είναι:

- Διαγραφή Δεδομένων
  Δεν υπάρχει η δυνατότητα της διαγραφής των δεδομένων αλλά λόγω ότι αποθηκεύονται τα δεδομένα μόνο των συναλλαγών πρέπει να διατηρηθούν επ' αορίστων.
- Διόρθωση
  Η μεταβολή των δεδομένων δεν είναι δυνατή μετά από την εισαγωγή τους.
- Πρόσβαση
  Οι χρήστες έχουν άμεση πρόσβαση στα δεδομένα τους στη βάση δεδομένων.
- Αυτοματοποιημένη Επεξεργασία
  Δεν γίνεται αυτοματοποιημένη επεξεργασία με τρόπο που μπορεί να βλάψει νομικά ένα άτομο.

Προσωπικά Δεδομένα

Πάλι εδώ αποθηκεύονται συναλλαγές με δημόσια κλειδιά άρα είναι προσωπικά δεδομένα.

Οι απαιτήσεις που υπάρχουν από το GDPR σχετικά με τα προσωπικά δεδομένα είναι η εμπιστευτικότητα και η ακεραιότητα τους.

Εδώ σε αντίθεση με το Bitcoin υπάρχουν τεχνικές για την ακεραιότητα αλλά και για την εμπιστευτικότητα των δεδομένων που αποθηκεύονται στη βάση δεδομένων. Άρα από άποψη προσωπικών δεδομένων είναι συμβατή με το GDPR.

5.5 Συμπεράσματα

Η τεχνολογία Blockchain έχει εμφανέστατα προβλήματα όταν πρόκειται με τον GDPR, όμως αυτό δεν σημαίνει ότι είναι ασυμβίβαστα. Υπάρχουν μόνο εφαρμογές της Blockchain που είναι νόμιμες ή παράνομες με βάση τον GDPR.
Για να γίνει μια εφαρμογή που χρησιμοποιεί μια βάση δεδομένων Blockchain συμβατή με τον κανονισμό GDPR πρέπει να σχεδιαστεί με προσεκτικό τρόπο λόγω των ιδιαιτεροτήτων που υπάρχουν.

Συντομογραφίες - Ακρωνύμια

GDPR	General Data Protection Regulation
ΓΚΠΔ	Γενικός Κανονισμός Προστασίας Δεδομένων
ΕΕ	Ευρωπαϊκή Ένωση

Αντιστοίχηση Ελληνικών και Αγγλικών Όρων

Συναρτήσεις Σύνοψης	Hash Functions
Σύνοψη Μηνύματος	Message Digest
Έξυπνα Συμβόλαια	Smart Contracts
Γενικός Κανονισμός Προστασίας Δεδομένων	General Data Protection Regulation
Τμήμα	Block
Ομότιμα	Peer to Peer
Ανωνυμία	Anonymity
Ιχνυλάτηση	Tracking
Επιγραμμικο	Online
Παγίδα	Trapdoor

Αναφορές

[1] Satoshi Nakamoto. “Bitcoin: A Peer-to-Peer Electronic Cash System”. In: *Cryptography Mailing list at https://metzdowd.com* (Mar. 2009).

[2] Mike Burmester, Στέφανος Γκρίτζαλης, Σωκράτης Κάτσικας και Βασίλειος Χρυσικόπουλος. *Σύγχρωνη Κρυπτογραφία Θεωρία και Εφαρμογές*. Παπασωτηρίου, 2011.

[3] Victor S. Miller. “Use of Elliptic Curves in Cryptography”. In: *Advances in Cryptology — CRYPTO ’85 Proceedings*. Ed. by Hugh C. Williams. Berlin, Heidelberg: Springer Berlin Heidelberg, 1986, pp. 417–426. ISBN: 978-3-540-39799-1.

[4] Ronald L. Rivest, Adi Shamir, and Leonard Adleman. *Cryptographic communications system and method*. Sept. 1983.

[5] R. Rivest. *The MD5 Message-Digest Algorithm*. RFC 1321. RFC Editor, Apr. 1992. URL: https://www.rfc-editor.org/rfc/rfc1321.txt.

[6] *Secure Hash Standard (SHS)*. 2015.

[7] G. Ateniese, B. Magri, D. Venturi, and E. Andrade. “Redactable Blockchain – or – Rewriting History in Bitcoin and Friends”. In: *2017 IEEE European Symposium on Security and Privacy (EuroS P)*. 2017, pp. 111–126. DOI: 10.1109/EuroSP.2017.37.

[8] Elisa Bertino Xun Yi Russell Paulet. *Homomorphic Encryption and Applications*. Springer International Publishing, 2014.

[9] Sarang Noether Koe Kurt M. Alonso. *Zero to Monero: Second Edition*. 2020.

[10] Adriana Iamnitchi, Paolo Trunfio, Jonathan Ledlie, and Florian Schintke. “Peer-to-Peer Computing”. In: Aug. 2010, pp. 444–445. ISBN: 978-3-642-15276-4. DOI: 10.1007/978-3-642-15277-1_42.

[11] George Coulouris, Jean Dollimore, Tim Kindberg, and Gordon Blair. *Distributed Systems: Concepts and Design Edition 5*. Pearson, 2012.

[12] Oleksandr Oksiiuk and Iryna Dmyrieva. “Security and privacy issues of blockchain technology”. In: Feb. 2020, pp. 1–5. DOI: 10.1109/TCSET49122.2020.235489.

[13] Julian Debus. “Consensus methods in blockchain systems”. In: *Frankfurt School of Finance & Management, Blockchain Center, Tech. Rep* (2017).

[14] Michael Nofer, Peter Gomber, Oliver Hinz, and Dirk Schiereck. “Blockchain”. In: *Business & Information Systems Engineering* 59 (Mar. 2017). DOI: 10.1007/s12599-017-0467-3.

[15] Alex Biryukov, Dmitry Khovratovich, and Ivan Pustogarov. “Deanonymisation of Clients in Bitcoin P2P Network”. In: *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. CCS ’14. Scottsdale, Arizona, USA: Association for Computing Machinery, 2014, pp. 15–29. ISBN: 9781450329576. DOI: 10.1145/2660267.2660379. URL: https://doi.org/10.1145/2660267.2660379.

[16] Rui Zhang, Rui Xue, and Ling Liu. “Security and Privacy on Blockchain”. In: *ACM Computing Surveys (CSUR)* 52 (2019), pp. 1–34.

[17] Vitalik Buterin. “Ethereum Whitepaper”. In: (2013). URL: https://ethereum.org/en/whitepaper/.

[18] *About Monero*. URL: https://www.getmonero.org/resources/about/.

[19] Serhack. *Mastering Monero The future of private transactions*. 2018.

[20] Mahendra Shrivas and Dr Yeboah. “The Disruptive Blockchain: Types, Platforms and Applications”. In: Dec. 2018. DOI: 10.21522/TIJAR.2014.SE.19.02.Art003.

[21] I.-C Lin and T.-C Liao. “A survey of blockchain security issues and challenges”. In: *International Journal of Network Security* 19 (Sept. 2017), pp. 653–659. DOI: 10.6633/IJNS.201709.19(5).01.

[22] Daniel J Solove. “Understanding privacy”. In: (2008).

[23] Dylan Yaga, Peter Mell, Nik Roby, and Karen Scarfone. *Blockchain Technology Overview*. en. Oct. 2018. DOI: https://doi.org/10.6028/NIST.IR.8202.

[24] “Blockchain and the General Data Protection Regulation”. In: (2018). URL: https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2019)634445.

[25] ARTICLE 29 DATA PROTECTION WORKING PARTY. “Opinion 05/2014 on Anonymisation Techniques”. In: (2014). URL: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

[26] Ken Timsit Tom Lyons Ludovic Courcelas. “Blockchain and the GDPR”. In: (2018).

[27] Λίλιαν Μήτρου. *Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων*. Εκδόσεις Σάκκουλα Α.Ε., 2017.

[28] *How Dandelion++ Keeps Monero’s Transaction Origins Private*. 2020. URL: https://localmonero.co/nojs/knowledge/monero-dandelion.

[29] Tobi Loba. *An Attempt by Attacker to Breach Monero (XMR) Users’ Privacy Failed*. 2020. URL: https://heraldsheets.com/attempt-by-attacker-to-breach-monero-xmr-users-privacy-failed/.

[30] Riccardo Spagni. *Recently, a largely incompetent attacker bumbled their way through a Sybil attack against Monero, trying to correlate transactions to the IP address of the node that broadcast it. Whilst novel in that it is the 1st Sybil attack of this sort, it was also quite ineffective*. URL: https://threadreaderapp.com/thread/1326130648491417602.html.

[31] Qi Feng, Debiao He, Sherali Zeadally, Khurram Khan, and Neeraj Kumar. “A survey on privacy protection in blockchain system”. In: *Journal of Network and Computer Applications* 126 (Nov. 2018). DOI: 10.1016/j.jnca.2018.10.020.

[32] Simon Barber, Xavier Boyen, Elaine Shi, and Ersin Uzun. “Bitter to Better — How to Make Bitcoin a Better Currency”. In: *Financial Cryptography and Data Security*. Ed. by Angelos D. Keromytis. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 399–414. ISBN: 978-3-642-32946-3.

[33] Rui Zhang, Rui Xue, and Ling Liu. “Security and privacy on blockchain”. In: *ACM Computing Surveys (CSUR)* 52.3 (2019), pp. 1–34.

[34] W. Kuan Hon, Christopher Millard, and Ian Walden. “Who is Responsible for ’Personal Data’ in Cloud Computing? The Cloud of Unknowing, Part 2”. In: (2014).

[35] Martin Florian, Sophie Beaucamp, Sebastian A. Henningsen, and Björn Scheuermann. “Erasing Data from Blockchain Nodes”. In: *CoRR* abs/1904.08901 (2019). arXiv: 1904.08901. URL: http://arxiv.org/abs/1904.08901.

[36] Roman Matzutt, Martin Henze, Jan Ziegeldorf, Jens Hiller, and Klaus Wehrle. “Thwarting Unwanted Blockchain Content Insertion”. In: Apr. 2018. DOI: 10.1109/IC2E.2018.00070.

[37] *Why distributed ledger technology must adapt to an imperfect world*. URL: https://www.accenture.com/_acnmedia/pdf-33/accenture-editing-uneditable-blockchain.pdf.