ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ -
ΔΗΜΟΚΡΙΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΡΑΚΗΣ
ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ – ΤΜΗΜΑ ΝΟΜΙΚΗΣ
Διιδρυματικό Πρόγραμμα Μεταπτυχιακών Σπουδών
Δίκαιο Και Πληροφορική

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ:
Η ΤΕΧΝΟΛΟΓΙΑ BLOCKCHAIN ΚΑΙ Η ΣΥΜΒΑΤΟΤΗΤΑ ΤΗΣ ΜΕ ΤΟΝ ΓΕΝΙΚΟ ΚΑΝΟΝΙΣΜΟ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Φοιτήτρια: Κωνσταντίνα Σοφία Ράμια, mli20042
Επιβλέπων Καθηγητής: Κομνηνός Κόμνιος

ΠΑΡΟΥΣΙΑΣΗ ΘΕΜΑΤΟΣ - ΣΤΟΧΟΙ

- Κατά τη λειτουργία της τεχνολογίας blockchain διεξάγεται επεξεργασία δεδομένων η οποία μπορεί να υπάγεται στις διατάξεις του Ευρωπαϊκού Κανονισμού Προστασίας Προσωπικών Δεδομένων (ΓΚΠΔ).
- Ερευνάται η δυνατότητα συμμόρφωσης μίας τεχνολογίας blockchain με τις επιταγές του ΓΚΠΔ, τι είδους δεδομένα υφίστανται επεξεργασία, ποια θεωρούνται δεδομένα προσωπικού χαρακτήρα και εάν η επεξεργασία τους είναι σύννομη.
- Εντοπίζονται σημεία ασυμβατότητας της τεχνολογίας blockchain με τον ΓΚΠΔ και προτείνονται εναλλακτικές λύσεις προκειμένου να ξεπεραστούν οι δυσκολίες συμμόρφωσης.

- ✓ Η ανάδειξη της αναγκαιότητας προσαρμογής της τεχνολογίας blockchain στις υποχρεώσεις που θέτει ο ΓΚΠΔ, έτσι ώστε η επεξεργασία των δεδομένων προσωπικού χαρακτήρα να διεξάγεται με σεβασμό προς το θεμελιώδες δικαίωμα της προστασίας της ιδιωτικής ζωής και της προστασίας των δεδομένων προσωπικού χαρακτήρα.
- ✓ Ο εντοπισμός και η καταγραφή των δυσκολιών συμμόρφωσης, και η πρόταση εναλλακτικών λύσεων.
- ✓ Η ανάδειξη της αναγκαιότητας για έκδοση κατευθυντήριων γραμμών από τα αρμόδια όργανα, ώστε να εξειδικεύεται ο τρόπος εφαρμογής των διατάξεων του Κανονισμού στις εν λόγω τεχνολογίες.

ΔΙΑΡΘΡΩΣΗ ΕΡΓΑΣΙΑΣ

Πρώτο μέρος:

- Ορισμός της τεχνολογίας blockchain.
- Ανάλυση των βασικών της ιδιοτήτων.
- Παρουσίαση του τρόπου λειτουργίας της, διενέργεια συναλλαγών, αλυσίδα των block,κρυπτογραφία, αλγόριθμοι συναίνεσης, θεωρία παιγνίων, hash functions, δέντρα merkle
- Bitcoin, Ethereum

Δεύτερο μέρος:

- Συγκριτική προσέγγιση του τρόπου λειτουργίας της τεχνολογίας blockchain με τις διατάξεις του ΓΚΠΔ.
- Εντοπισμός και ανάλυση σημείων ασυμβατότητας της τεχνολογίας με συγκεκριμένες διατάξεις του Κανονισμού.
- Έρευνα και καταγραφή των εναλλακτικών λύσεων και των τεχνολογικών εργαλείων που μπορούν να χρησιμοποιηθούν.
- Παρουσίαση ερευνητικών συστημάτων blockchain, συμμορφούμενων με τον ΓΚΠΔ.

ΚΥΡΙΩΣ ΜΕΡΟΣ- ΒΑΣΙΚΕΣ ΘΕΜΑΤΙΚΕΣ

Δεδομένα προσωπικού χαρακτήρα σε blockchain:

- Δεδομένα συναλλαγών (τα δεδομένα που αποθηκεύονται στα blocks είτε ως απλό κείμενο, είτε σε κρυπτογραφημένη μορφή είτε με τη χρήση hash).
- Δημόσια κλειδιά.

Επεξεργασία δεδομένων σε blockchain:

- Αρχική προσθήκη δεδομένων στο σύστημα.
- Συνεχιζόμενη αποθήκευση των δεδομένων.
- Κάθε περαιτέρω επεξεργασία, όπως κάθε είδους ανάλυση δεδομένων που χρησιμοποιούνται για την διαδικασία του consensus

Βασικές θεματικές

1η Δυσκολία συμμόρφωσης
Λογοδοσία vs Αποκέντρωση και Δημοκρατικότητα

- ✓ Θεμελιώδη αρχή του ΓΚΠΔ αποτελεί η ευθύνη του υπευθύνου επεξεργασίας είναι να είναι σε θέση να αποδείξει τη συμμόρφωσή του προς τις αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα (άρθρο 5, παρ. 2 ΓΚΠΔ)
- ✓ Σε ένα αποκεντρωμένο peer-to-peer σύστημα διασφαλίζεται η δημοκρατικότητα, δεν υπάρχει καμία ύπαρξη εντός του συστήματος η οποία έχει μεγαλύτερη εξουσία από τις υπόλοιπες.
- ✓ Σε ιδιωτικά και αδειοδοτημένα blockchain, είναι πιθανό να εντοπιστεί μία κεντρική οντότητα, που μπορεί να θεωρηθεί ως υπεύθυνος επεξεργασίας δεδομένων, καθώς καθορίζει τον τρόπο και τους σκοπούς της επεξεργασίας.
- ✓ Σε δημόσια και μη αδειοδοτημένα blockchain ο υπεύθυνος επεξεργασίας μπορεί να εντοπιστεί μεταξύ πολλών συμμετεχόντων (προγραμματιστές, κόμβοι, χρήστες του δικτύου, πάροχοι εφαρμογών).
- ✓ Πολλοί από τους συμμετέχοντες ενός δικτύου μπορεί να θεωρηθούν ως από κοινού υπεύθυνοι επεξεργασίας, όταν ασκούν επιρροή κατά την επεξεργασία δεδομένων, για δικούς τους σκοπούς και συμμετέχουν, συνεπώς, στον καθορισμό των σκοπών και των τρόπων επεξεργασίας.

Ζητήματα που δημιουργούνται:

- ➢ σε ένα blockchain δεν είναι εύκολο να εντοπιστεί ο υπεύθυνος επεξεργασίας.
- ➢ ένας συμμετέχων που θεωρείται υπεύθυνος επεξεργασίας μπορεί να έχει περιορισμένη επιρροή στους σκοπούς και τον τρόπο της επεξεργασίας, προκαλώντας έτσι πρόβλημα στη συμμόρφωση με τον ΓΚΠΔ, εξαιτίας του μειωμένου ελέγχου του επάνω στα δεδομένα.
- ➢ Ομοίως, μπορεί να έχει περιορισμένη πρόσβαση σε δεδομένα, αδυνατώντας έτσι να ικανοποιήσει τα δικαιώματα ενημέρωσης, πρόσβασης, φορητότητας, εναντίωσης και περιορισμού της επεξεργασίας των υποκειμένων (π.χ. οι κόμβοι έχουν πρόσβαση μόνο σε κρυπτογραφημένα δεδομένα).

1η Δυσκολία συμμόρφωσης
Λογοδοσία vs Αποκέντρωση

Τρόπος προσέγγισης της δυσκολίας

- Ομάδα εργασίας του άρθρου 29 (Γνώμη 1/2010): «Εντοπίζοντας την ευθύνη», όταν ένας υπεύθυνος επεξεργασίας δεν θα μπορεί να ελέγξει όλες τις διαδικασίες επεξεργασίας, θα πρέπει να επιβεβαιώσει ότι οι σχέσεις του με τους υπόλοιπους συμμετέχοντες του δικτύου είναι τέτοιες, ώστε οι διαδικασίες αυτές να μπορούν να καλυφθούν από τους υπόλοιπους.
- ΕΣΠΔ (Κατευθυντήριες γραμμές 7/2020): σε περίπτωση που υπάρχουν από κοινού υπεύθυνοι επεξεργασίας, αυτοί οφείλουν να καθορίσουν «ποιος θα κάνει τι», αποφασίζοντας μεταξύ τους ποιος θα αναλαμβάνει ποιες εργασίες με σκοπό να διασφαλίσουν ότι η επεξεργασία συμμορφώνεται με τις επιταγές του ΓΚΠΔ. Συνεπώς, πρέπει να γίνεται ξεκάθαρο ποιος θα είναι υπεύθυνος να απαντά στα αιτήματα των υποκειμένων των δεδομένων.

2η Δυσκολία συμμόρφωσης
Ελαχιστοποίηση δεδομένων -Περιορισμός του σκοπού/της περιόδου αποθήκευσης δεδομένων vs Αμεταβλητότητα των blockchain

- Εφόσον μία συναλλαγή καταγραφεί σε ένα blockchain, είναι αδύνατο να τροποποιηθεί.
- Τα δεδομένα σε ένα blockchain συνεχίζουν να υφίστανται επεξεργασία ακόμα και μετά την επιτυχή εκτέλεση της συναλλαγής, με την έννοια ότι θα παραμείνουν αποθηκευμένα στο καθολικό και θα υφίστανται επεξεργασία καθώς θα εκτελείται ο αλγόριθμος συναίνεσης.
- Η αποθήκευση και η συμπερίληψη των δεδομένων σε άλλες συναλλαγές θεωρούνται μέρος του αρχικού σκοπού της επεξεργασίας ή πρόκειται για ασυμβατότητα με τις αρχές του περιορισμού του σκοπού, του περιορισμού της περιόδου αποθήκευσης και της ελαχιστοποίησης δεδομένων;
- Σε περίπτωση που θεωρηθεί ότι πρόκειται για ασυμβατότητα, η διαγραφή τους ή η διακοπή της επεξεργασίας είναι αδύνατη εξαιτίας της αμεταβλητότητας των blockchain.

➢ Συνεπώς:

Οι υπεύθυνοι επεξεργασίας σε ένα blockchain οφείλουν να διευκρινίζουν στα υποκείμενα των δεδομένων ότι χρησιμοποιούν τη συγκεκριμένη τεχνολογία καθώς και τις επιπτώσεις, όπως δηλαδή το γεγονός ότι η επεξεργασία δεν θα περιοριστεί στην αρχική συναλλαγή αλλά τα προσωπικά δεδομένα θα υφίστανται επεξεργασία και μετά την ολοκλήρωσή της.

Βασικές θεματικές

3η Δυσκολία Συμμόρφωσης
Αρχή της ακρίβειας/Δικαιώματα διαγραφής, διόρθωσης vs Αμεταβλητότητα των blockchain

- Η αρχή της ακρίβειας των δεδομένων προβλέπει ότι τα δεδομένα προσωπικού χαρακτήρα είναι ακριβή και, όταν είναι αναγκαίο, επικαιροποιούνται. Πρέπει να λαμβάνονται όλα τα εύλογα μέτρα για την άμεση διαγραφή ή διόρθωση δεδομένων προσωπικού χαρακτήρα τα οποία είναι ανακριβή, σε σχέση με τους σκοπούς της επεξεργασίας.
- Εφόσον μία συναλλαγή καταγραφεί σε ένα blockchain, είναι αδύνατο να τροποποιηθεί, να διαγραφεί ή να διορθωθεί.
- Τα αιτούμενα προς διαγραφή ή διόρθωση δεδομένα πρέπει να διαγραφούν ή να διορθωθούν σε όλους τους κόμβους του δικτύου για να θεωρείται ότι διαγράφηκαν ή ότι διορθώθηκαν. Συνεπώς, όταν ένας υπεύθυνος επεξεργασίας σε ένα blockchain λάβει ένα τέτοιο αίτημα, δεν αρκεί να διαγράψει ή να διορθώσει τα δεδομένα, αλλά πρέπει να ενημερωθούν και οι υπόλοιποι υπεύθυνοι ή εκτελούντες την επεξεργασία οι οποίο πραγματοποιούν επεξεργασία στα ίδια δεδομένα.
- Ένα blockchain μπορεί να υπάγεται ταυτόχρονα σε πολλές διαφορετικές δικαιοδοσίες, εντός και εκτός Ευρωπαϊκής Ένωσης. Έτσι υπάρχει το ενδεχόμενο τα δεδομένα ενός υποκειμένου να τυγχάνουν διαγραφής σε κάποια δικαιοδοσία ενώ σε κάποια άλλη όχι. Ωστόσο, το διαμοιραζόμενο καθολικό αντιγράφεται και αποθηκεύεται σε όλους τους κόμβους ενώ δεν είναι δυνατή η μερική διαγραφή δεδομένων, πχ σε συγκεκριμένους μόνο κόμβους.

Εργαλεία που μπορούν να χρησιμοποιηθούν για τα δικαιώματα διαγραφής και διόρθωσης

- Επεξεργάσιμα blockchain που βασίζονται σε chameleon hashes
- Αποθήκευση δεδομένων εκτός αλυσίδας
- Λογαριασμοί μίας χρήσης (συναλλαγές και κλειδιά μίας χρήσης)
- Αποδείξεις μηδενικής γνώσης (zero-knowledge proofs, παρέχουν μία δυαδική αληθή/λανθασμένη απάντηση χωρίς να παρέχουν πρόσβαση στα υποκείμενα δεδομένα)
- Προσθήκη θορύβου στα δεδομένα (αρκετές συναλλαγές συγκεντρώνονται μαζί ώστε θα ήταν αδύνατο από το εξωτερικό τους να ανιχνευτούν οι ταυτότητες των αποστολέων και των παραληπτών των συναλλαγών)
- State channels (επιτρέπουν στους χρήστες να κάνουν πολλαπλές συναλλαγές σε ένα blockchain) και ring signatures (κρύβουν συναλλαγές μέσα σε άλλες συναλλαγές ενώνοντας μία μοναδική συναλλαγή με πολλαπλά ιδιωτικά κλειδιά ακόμα και αν ένα μόνο από αυτά ξεκίνησε την συναλλαγή)
- Διαγραφή ιδιωτικών κλειδιών (CNIL)

Ζητήματα συγκατάθεσης

- Προτείνεται η συγκατάθεση που πρέπει να δίνεται για να επιτραπεί η επεξεργασία δεδομένων μέσω ενός blockchain να παρέχεται όταν ένας χρήστης εγγράφεται σε μία διεύθυνση Bitcoin, θεωρώντας δεδομένο ότι έχει δώσει ανεπιφύλακτα τη συγκατάθεσή του για την επεξεργασία της διεύθυνσης με σκοπό τη διενέργεια συναλλαγών.
- Η συγκατάθεση πρέπει να παρέχεται με σαφή θετική ενέργεια η οποία να συνιστά ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει ένδειξη της συμφωνίας του υποκειμένου των δεδομένων υπέρ της επεξεργασίας των δεδομένων που το αφορούν. Δεν μπορεί η συγκατάθεση να «υπονοείται».
- Όταν κάποιο προσωπικό δεδομένο προστίθεται σε ένα block του blockchain θα συνεχίσει να υφίσταται επεξεργασία για όσο υπάρχει το καθολικό, δημιουργώντας έτσι την ανάγκη για νέα βάση για την επεξεργασία εάν το υποκείμενο επιθυμεί τη συνέχιση της επεξεργασίας των δεδομένων του, διαφορετικά η επεξεργασία θα πρέπει να διακοπεί.
- Πιθανή λύση στο συγκεκριμένο πρόβλημα μπορεί να η χρήση εργαλείων όπως τα Dynamic consent management συστήματα (DCM) που βασίζονται σε έξυπνα συμβόλαια.

Συμπεράσματα

- ✓ Το ερώτημα «μπορεί μία τεχνολογία blockchain να συμμορφώνεται με τις επιταγές του ΓΚΠΔ;» είναι αδύνατο να απαντηθεί με σαφήνεια, καθώς τα blockchain εμφανίζονται με ποικίλες μορφές, απαιτείται κατά περίπτωση προσέγγιση.
- ✓ Η συμμόρφωση με τον Κανονισμό είναι πιο εύκολη όταν αφορά σε ιδιωτικά και αδειοδοτημένα δίκτυα blockchain, ενώ καθίσταται δυσκολότερη σε δημόσια και μη αδειοδοτημένα δίκτυα.
- ✓ Για να επιτευχθεί η πλήρης συμμόρφωση, υπάρχει η ανάγκη προσαρμογής των blockchain στις υποχρεώσεις που προβλέπει ο ΓΚΠΔ, σχεδιάζοντας «φιλικά» προς τον Κανονισμό συστήματα και χρησιμοποιώντας τα διαθέσιμα τεχνολογικά εργαλεία.
- ✓ Υπάρχει επίσης η ανάγκη έκδοσης κατευθυντηρίων γραμμών από τα αρμόδια όργανα με τις οποίες θα εξειδικεύεται η εφαρμογή των διατάξεων του Κανονισμού στη συγκεκριμένη τεχνολογία.

Σας ευχαριστώ!