ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ

ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΗΜΟΚΡΙΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΡΑΚΗΣ
ΤΜΗΜΑ ΝΟΜΙΚΗΣ

ΔΙΙΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ

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

Διπλωματική Εργασία

της

Κωνσταντίνας Σοφίας Ράμια

Θεσσαλονίκη, 02/2022

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

Κωνσταντίνα Σοφία Ράμια

Πτυχίο Νομικής, Δημοκρίτειο Πανεπιστήμιο Θράκης, 2017

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΟ ΔΙΚΑΙΟ & ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέπων Καθηγητής
Κομνηνός Κόμνιος

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 25/02/2022

Κομνηνός Κόμνιος	Ευγενία Αλεξανδροπούλου-Αιγυπτιάδου	Μαρία Μυλώση

Κωνσταντίνα Σοφία Ράμια

Περίληψη

Η παρούσα διπλωματική εργασία αποτελεί μία έρευνα σχετικά με τη δυνατότητα συμμόρφωσης της τεχνολογίας blockchain με τις διατάξεις του Ευρωπαϊκού Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ). Στο πρώτο κεφάλαιο της εργασίας περιλαμβάνεται μία ανάλυση του τρόπου λειτουργίας της τεχνολογίας blockchain. Στο δεύτερο κεφάλαιο επιχειρείται μία συγκριτική προσέγγιση, με σκοπό τη διαπίστωση του κατά πόσο καθίσταται δυνατόν να εφαρμοστεί ο ΓΚΠΔ σε τεχνολογίες blockchain και σε ποιο βαθμό, αναγνωρίζοντας ταυτόχρονα τις «γκρίζες περιοχές» μεταξύ τους και μελετώντας τις εναλλακτικές λύσεις για τις περιπτώσεις όπου η συμμόρφωση καθίσταται αδύνατη. Σκοπός της παρούσης έρευνας είναι η ανάδειξη της σημασίας της προστασίας της ιδιωτικότητας σε ένα συνεχώς μεταβαλλόμενο τεχνολογικό περιβάλλον όπου αναπτύσσονται ολοένα και περισσότερες νέες τεχνολογίες. Ωστόσο, αξιοποιώντας τις δυνατότητες και τα εργαλεία που παρέχουν οι νέες αυτές τεχνολογίες, καθίσταται δυνατό να τις εντάξουμε στην καθημερινότητά μας με ασφάλεια και σεβασμό προς το δικαίωμα προστασίας της ιδιωτικής ζωής.

Λέξεις Κλειδιά: Blockchain, DLT, δεδομένα προσωπικού χαρακτήρα, ΓΚΠΔ, ιδιωτικότητα

Abstract

The present dissertation is a survey concerning the compatibility of blockchain technology with the European General Data Protection Regulation (GDPR). The first chapter includes an analysis of the way in which blockchain technology functions. In the second chapter, a comparative approach is attempted, in order to determine whether it is possible for blockchain technology to comply with the GDPR and to what extent, acknowledging at the same time the "grey areas" between them and examining alternative solutions for the cases that compliance is impossible. The aim of the survey is to underline the importance of privacy in a continuously changing technological environment where new technologies rise every day. Nevertheless, it is possible to integrate these technologies in our everyday life with security and respect of privacy, by utilizing their feasibilities and the tools they provide.

Keywords: Blockchain, DLT, personal data, GDPR, privacy

Περιεχόμενα

Εισαγωγή

Η συνεχής ανάπτυξη των Επιστημών Πληροφορίας μετατρέπει τις σύγχρονες κοινωνίες σε ψηφιακές. Το Διαδίκτυο των πραγμάτων (Internet of things)[1], έχει εδραιωθεί και έχει αποκτήσει μόνιμη θέση στην καθημερινότητα, καθιστώντας πλέον απαραίτητες τις υπηρεσίες του για ένα μεγάλο μέρος του πληθυσμού, ενώ όλο και περισσότερες πτυχές της καθημερινής ζωής τείνουν να ψηφιοποιούνται. Νέες, καινοτόμες τεχνολογίες δημιουργούνται συνεχώς, αυξάνοντας την ανάγκη για συλλογή δεδομένων, προκειμένου να υποστηριχθεί η λειτουργία τους. Για παράδειγμα, τα μαζικά δεδομένα είναι σύνολα δεδομένων που έχουν συλλεχθεί και είναι τόσο μεγάλα σε όγκο και περίπλοκα που απαιτούν νέες τεχνολογίες, όπως η τεχνητή νοημοσύνη, για την επεξεργασία τους. Τα δεδομένα προέρχονται από πολλές διαφορετικές πηγές. Συχνά είναι δεδομένα του ίδιου τύπου, για παράδειγμα, δεδομένα GPS που προέρχονται από εκατομμύρια κινητά τηλέφωνα και χρησιμοποιούνται για τον περιορισμό της κυκλοφοριακής συμφόρησης. Ωστόσο μπορούμε να έχουμε και συνδυασμούς τύπων, όπως στην περίπτωση συλλογής δεδομένων από μητρώα υγείας και εφαρμογές εξυπηρέτησης ασθενών. Η τεχνολογία επιτρέπει τη συλλογή αυτών των δεδομένων με υψηλές ταχύτητες, σε σχεδόν πραγματικό χρόνο, και την ανάλυση τους για τη απόκτηση νέων πληροφοριών. Τα μαζικά δεδομένα μπορούν να παραχθούν είτε από ανθρώπους, πχ. σε εφαρμογές για κινητά, στο διαδίκτυο, συμπεριλαμβανομένων των μέσων κοινωνικής δικτύωσης και των εμπορικών συναλλαγών, σε αρχεία ηλεκτρονικής διακυβέρνησης, είτε από μηχανήματα και να συλλεχθούν μέσω αισθητήρων σε αντικείμενα που συνδέονται με το διαδίκτυο των πραγμάτων, συμπεριλαμβανομένων έξυπνων αυτοκινήτων, εργοστασίων, GPS και δορυφόρων που συλλέγουν μετεωρολογικά δεδομένα κλπ[2]. (Παρομοίως, η τεχνητή νοημοσύνη αναφέρεται στην ικανότητα μιας μηχανής να αναπαράγει τις γνωστικές λειτουργίες ενός ανθρώπου, όπως είναι η μάθηση, ο σχεδιασμός και η δημιουργικότητα. Η τεχνητή νοημοσύνη καθιστά τις μηχανές ικανές να 'κατανοούν' το περιβάλλον τους, να επιλύουν προβλήματα και να δρουν προς την επίτευξη ενός συγκεκριμένου στόχου. Ο υπολογιστής λαμβάνει δεδομένα (ήδη έτοιμα ή συλλεγμένα μέσω αισθητήρων, π.χ. κάμερας), τα επεξεργάζεται και ανταποκρίνεται βάσει αυτών. Τα συστήματα τεχνητής νοημοσύνης είναι ικανά να προσαρμόζουν τη συμπεριφορά τους, σε ένα ορισμένα βαθμό, αναλύοντας τις συνέπειες προηγούμενων δράσεων και επιλύοντας προβλήματα με αυτονομία.[3]

Η ανωτέρω περιγραφόμενη συνεχιζόμενη τάση για ψηφιοποίηση του προσώπου, η ανάλυση, δηλαδή και καταχώριση του κάθε πολίτη σε αρχεία βάσει των δεδομένων που τον χαρακτηρίζουν, ενέχει σημαντικούς κινδύνους για τα θεμελιώδη

[1] Το Διαδίκτυο των πραγμάτων ή Ίντερνετ των πραγμάτων (Internet of Things) αποτελεί το δίκτυο επικοινωνίας πληθώρας συσκευών, οικιακών συσκευών, αυτοκινήτων καθώς και κάθε αντικειμένου που ενσωματώνει ηλεκτρονικά μέσα, λογισμικό, αισθητήρες και συνδεσιμότητα σε δίκτυο ώστε να επιτρέπεται η σύνδεση και η ανταλλαγή δεδομένων. Απλούστερα, η φιλοσοφία του IoT είναι η σύνδεση όλων των ηλεκτρονικών συσκευών μεταξύ τους (τοπικό δίκτυο) ή με δυνατότητα σύνδεσης στο διαδίκτυο.

[2] https://www.europarl.europa.eu/

[3] https://www.europarl.europa.eu/news/el/headlines/priorities/i-techniti-noimosuni-stin-ee/20200827STO85804/ti-einai-i-techniti-noimosuni-kai-pos-chrisimopoieitai

δικαιώματα του ανθρώπου, όπως το δικαίωμα στην ιδιωτική ζωή, εν γένει και πιο συγκεκριμένα το δικαίωμα στην προστασία των προσωπικών του δεδομένων. Μάλιστα, κατά μία άποψη, ενέχεται σοβαρός κίνδυνος μετατροπής του ανθρώπου σε αντικείμενο[4]. Για το λόγο αυτό, προέκυψε η ανάγκη ενός πλαισίου προστασίας του δικαιώματος στην ιδιωτικότητα, το οποίο κατά τη διάρκεια των ετών εξελίχθηκε παράλληλα με τις νέες ανάγκες που δημιούργησαν οι τεχνολογικές εξελίξεις. Η συζήτηση για τη δημιουργία ενός πλαισίου προστασίας της ιδιωτικής ζωής εν γένει και στην πορεία των προσωπικών δεδομένων, ξεκίνησε ήδη από τη δεκαετία του 1960. Στην πορεία θεσμοθετήθηκαν σημαντικά νομοθετήματα στον χώρο της Ευρωπαϊκής Ένωσης, όπως η ΕΣΔΑ, ο Χάρτης Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, η Σύμβαση 108/1981, τα οποία έθεσαν γερές βάσεις στην προστασία προσωπικών δεδομένων και συνέβαλλαν στην μετέπειτα θεσμοθέτηση του Γενικού Κανονισμού για την προστασία των προσωπικών δεδομένων (2016/679 ΕΕ), αλλιώς GDPR, ο οποίος αποτελεί σήμερα το βασικό νομοθέτημα αναφορικά με την προστασία προσωπικών δεδομένων.

Αντικείμενο της παρούσης εργασίας πρόκειται να αποτελέσει η επεξεργασία δεδομένων προσωπικού χαρακτήρα με τη χρήση μίας επίσης πρωτοποριακής τεχνολογίας, της τεχνολογίας blockchain. Το Blockchain είναι μία βάση δεδομένων στην οποία τα δεδομένα αποθηκεύονται και διανέμονται σε έναν μεγάλο αριθμό υπολογιστών. Όλες οι εγγραφές, που πραγματοποιούνται σε αυτό το μητρώο, ονομάζονται «συναλλαγές» και είναι ορατές από το σύνολο των υπολογιστών, ήδη από τη δημιουργία του. Το Blockchain δεν αποτελεί το ίδιο μία διαδικασία επεξεργασίας προσωπικών δεδομένων έχοντας έναν εξ ολοκλήρου διακριτό σκοπό, αλλά πρόκειται για μία τεχνολογία, που μπορεί να συνεισφέρει στην υποστήριξη διαφόρων μορφών επεξεργασίας. Το blockchain δεν αποτελεί απλά μία τεχνολογία, αλλά ένα συνδυασμό επιχειρησιακών αρχών, οικονομικών πρακτικών, θεωρίας παιγνίων, κρυπτογραφίας και επιστήμης υπολογιστών.

Βασική προβληματική της έρευνας, είναι το γεγονός ότι εξαιτίας ορισμένων χαρακτηριστικών και ιδιοτήτων της τεχνολογίας blockchain, που οφείλονται στην αρχιτεκτονικής της συγκεκριμένης τεχνολογίας, παρουσιάζονται σημεία ασυμβατότητας με το ως άνω αναφερθέν κύριο νομοθέτημα δικαίου προστασίας δεδομένων, τον Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ). Αυτό έχει ως αποτέλεσμα, όταν η τεχνολογία αυτή χρησιμοποιείται για την επεξεργασία δεδομένων προσωπικού χαρακτήρα ή όταν κατά τη χρήση της διενεργείται επεξεργασία δεδομένων προσωπικού χαρακτήρα, αφενός τα υποκείμενα των δεδομένων να είναι εκτεθειμένα σε ένα μεγάλο αριθμό κινδύνων αναφορικά με την ικανοποίηση των δικαιωμάτων τους, αφετέρου διάφοροι φορείς που λαμβάνουν μέρος σε ένα δίκτυο να έρχονται αντιμέτωποι με υποχρεώσεις στις οποίες αδυνατούν να ανταποκριθούν.

Στόχος της διπλωματικής εργασίας είναι η ανάδειξη της αναγκαιότητας προσαρμογής της τεχνολογίας blockchain στις υποχρεώσεις που θέτει ο ΓΚΠΔ, έτσι ώστε η επεξεργασία δεδομένων προσωπικού χαρακτήρα, με τη χρήση της συγκεκριμένης τεχνολογίας, να διεξάγεται με σεβασμό προς το θεμελιώδες δικαίωμα

[4] Χριστοδούλου Κ., Δίκαιο Προσωπικών Δεδομένων, Νομική βιβλιοθήκη, 2020, σελ. 2

του προστασίας της ιδιωτικής ζωής και το δικαίωμα της προστασίας των δεδομένων προσωπικού χαρακτήρα. Συνεπώς, πρέπει να εντοπισθούν και να καταγραφούν οι δυσκολίες συμμόρφωσης με τον Κανονισμό, ενώ παράλληλα πρέπει να αναζητηθούν λύσεις προκειμένου να ξεπεραστούν τα ζητήματα που τίθενται.

Στο πρώτο μέρος της παρούσας εργασίας περιλαμβάνεται μία ανάλυση της τεχνολογίας blockchain. Αναφέρεται ο ορισμός της και οι βασικές ιδιότητές της, οι διάφορες επιστήμες, τεχνολογίες και επιχειρησιακές πρακτικές που συνεργάζονται για την λειτουργία της, ο τρόπος διενέργειας συναλλαγών σε περιβάλλον blockchain, καθώς μερικά από τα δημοφιλέστερα blockchain που χρησιμοποιούνται σήμερα. Η μελέτη του τρόπου λειτουργίας της συγκεκριμένης τεχνολογίας καθώς και η ανάλυση των βασικών της ιδιοτήτων είναι ιδιαιτέρως σημαντικά, καθώς μέσα από αυτά εξάγονται συμπεράσματα σχετικά με τη συμμόρφωση η μη με τον ΓΚΠΔ.

Στο δεύτερο μέρος της εργασίας επιχειρείται μία συγκριτική ανάλυση των ιδιοτήτων και του τρόπου λειτουργίας της τεχνολογίας blockchain με τις θεμελιώδεις αρχές και τα δικαιώματα που παρέχει ο ΓΚΠΔ. Γίνεται προσπάθεια υπαγωγής των συμμετεχόντων σε ένα δίκτυο blockchain στις βασικές διατάξεις του Κανονισμού καθώς και μία προσπάθεια καταγραφής των σημείων ασυμβατότητας μεταξύ των δύο πλευρών. Επιπλέον, επιχειρείται η πρόταση εναλλακτικών λύσεων με τη χρήση συγκεκριμένων εργαλείων, αλλά και η πρόταση ολοκληρωμένων συστημάτων blockchain, συμμορφούμενων με τον ΓΚΠΔ, βάσει επιστημονικών ερευνών.

Τέλος, εξάγονται συμπεράσματα σχετικά με το βασικό ερώτημα της έρευνας, ήτοι με το αν και σε ποιο βαθμό είναι συμβατή μία τεχνολογία blockchain με τον ΓΚΠΔ καθώς και αν καθίσταται δυνατό να ξεπεραστούν τα όποια προβλήματα ανιχνεύτηκαν κατά τη διενέργεια της έρευνας.

Ι. ΜΕΡΟΣ ΠΡΩΤΟ - Η τεχνολογία blockchain

Τεχνολογία Κατανεμημένου Καθολικού (DLT)

Η τεχνολογία κατανεμημένου καθολικού είναι ένα εργαλείο για την καταγραφή της κυριότητας – θα μπορούσε να αναφέρεται για παράδειγμα στην κυριότητα χρήματος ή περιουσιακών στοιχείων, όπως τα ακίνητα. Σήμερα, όταν οι τράπεζες διενεργούν συναλλαγές – δηλ. όταν μεταβιβάζεται η κυριότητα χρήματος ή χρηματοοικονομικών περιουσιακών στοιχείων – χρησιμοποιούν κεντρικά συστήματα, τα οποία συχνά διαχειρίζονται οι κεντρικές τράπεζες. Οι τράπεζες καταγράφουν τις συναλλαγές τους σε τοπικές βάσεις δεδομένων, οι οποίες επικαιροποιούνται μετά την ολοκλήρωση της συναλλαγής στο κεντρικό σύστημα.

Το κατανεμημένο καθολικό, από την άλλη, είναι μια βάση δεδομένων για συναλλαγές που, αντί να αποθηκεύεται σε μια κεντρική τοποθεσία, διαμοιράζεται σε ένα δίκτυο πολλών υπολογιστών. Συνήθως, όλα τα μέλη του δικτύου μπορούν να διαβάζουν τις πληροφορίες και, ανάλογα με τις άδειες που τους έχουν δοθεί, να προσθέτουν στοιχεία.[5]

Ο πιο κοινός τύπος τεχνολογίας κατανεμημένου καθολικού ονομάζεται αλυσίδα συστοιχιών («blockchain»). Η ονομασία αυτή προέρχεται από το γεγονός ότι οι συναλλαγές ομαδοποιούνται προκειμένου να σχηματίσουν συστοιχίες («blocks») οι οποίες συνδέονται μεταξύ τους με χρονολογική σειρά σχηματίζοντας μια αλυσίδα («chain»). Η αλυσίδα προστατεύεται στο σύνολό της από σύνθετους μαθηματικούς αλγορίθμους με σκοπό να διασφαλίζεται η ακεραιότητα και η ασφάλεια των δεδομένων. Αυτή η αλυσίδα αποτελεί την ολοκληρωμένη καταγραφή όλων των συναλλαγών που περιλαμβάνονται στη βάση δεδομένων.

Τα τελευταία χρόνια, κυρίως στον οικονομικό τομέα, ο όρος DLT και blockchain ταυτίζονται. Στην πραγματικότητα όμως αυτό δεν είναι απολύτως ακριβές, καθώς το blockchain, όπως ήδη αναφέρθηκε, είναι ένας τύπος DLT. Τα DLT αποτελούν μία διαμοιραζόμενη βάση δεδομένων μεταξύ γνωστών και εγκεκριμένων συμμετεχόντων, ωστόσο, δεν απαιτούν τη χρήση κρυπτονομίσματος ούτε τη χρήση mining για τη διασφάλιση της ασφάλειας του συστήματος[6] .

Blockchain

Το blockchain είναι ένα peer-to-peer σύστημα συναλλαγών το οποίο λειτουργεί χωρίς την μεσολάβηση τρίτων μερών. Πρόκειται για ένα διαμοιραζόμενο, αποκεντρωμένο και ανοιχτό καθολικό, μία βάση δεδομένων συναλλαγών, σαν ένα λογιστικό βιβλίο. Τα δεδομένα και οι πληροφορίες του καθολικού αντιγράφονται σε ένα μεγάλο αριθμό κόμβων. Το καθολικό έχει την ιδιότητα append only και δεν μπορεί να αλλαχθεί ή να τροποποιηθεί, συνεπώς κάθε εγγραφή είναι μόνιμη ενώ κάθε νέα εγγραφή περιλαμβάνεται σε όλα τα αντίγραφα των βάσεων δεδομένων στους διαφορετικούς κόμβους. Δεν υπάρχει η ανάγκη τρίτων μερών, πχ τραπεζών, προκειμένου να επικυρώσουν τις συναλλαγές, καθώς είναι μια τεχνολογία

[5] https://www.ecb.europa.eu/explainers/tell-me-more/html/distributed_ledger_technology.el.html

[6] Mastering Blockchain : A deep dive into distributed ledgers, consensus protocols, smart contracts, DApps, cryptocurrencies, Ethereum, and more, 3rd Edition

σχεδιασμένη με τέτοιο τρόπο, ώστε να ενσαρκώνει την αληθινή έννοια ενός αποκεντρωμένου συστήματος.

Κάθε κόμβος του δικτύου διαθέτει ένα αντίγραφο της αλυσίδας των μπλοκ, στην οποία κάθε μπλοκ αποτελεί μία συλλογή συναλλαγών, εξ ου και το όνομα της τεχνολογίας (blockchain= chain of blocks=αλυσίδα από μπλοκ). Τα μπλοκ αποτελούνται από δύο κύρια μέρη. Το μέρος που περιλαμβάνει την κεφαλίδα περιλαμβάνει αναφορά στο προηγούμενο μπλοκ της αλυσίδας και πιο συγκεκριμένα περιλαμβάνει το hash (συνάρτηση κατακερματισμού) του προηγούμενου μπλοκ, εξασφαλίζοντας έτσι ότι δεν θα τροποποιηθεί καμία συναλλαγή στο προηγούμενο μπλοκ. Το δεύτερο μέρος του μπλοκ, αποτελεί το περιεχόμενο σώματος και περιλαμβάνει μία έγκυρη λίστα των συναλλαγών, τα ποσά τους, τις διευθύνσεις των συμμετεχόντων μερών και μερικές ακόμα λεπτομέρειες. Όλα τα δεδομένα που περιλαμβάνονται στα μπλοκ είναι αμετάβλητα και κάθε συναλλαγή είναι αμετάκλητη. Οποιαδήποτε αλλαγή σημαίνει νέα συναλλαγή και πρέπει να επικυρωθεί από όλους τους κόμβους. Κάθε κόμβος περιλαμβάνει αντίγραφο του blockchain.[7]

Συγκεντρωτικά και αποκεντρωμένα συστήματα

Συγκεντρωτικά κατανεμημένο σύστημα είναι ένα σύστημα στο οποίο υπάρχει ένας κύριος κόμβος υπεύθυνος να διαχωρίζει τις εργασίες και τα δεδομένα και να τα διαμοιράζει στους υπόλοιπους κόμβους. Ένα αποκεντρωμένα κατανεμημένο σύστημα, είναι ένα σύστημα στο οποίο δεν υπάρχει ένα κύριος κόμβος.

Οι όροι συγκεντρωτικό και αποκεντρωμένο σύστημα δεν είναι πάντα σαφείς. Αυτό συμβαίνει διότι δεν υπάρχουν συστήματα τα οποία είναι αποκλειστικά συγκεντρωτικά ή αποκεντρωμένα. Αντίθετα, υπάρχουν διαφορετικές οπτικές υπό τις οποίες εξετάζεται το ζήτημα. Αρχικά, ένα σύστημα μπορεί να είναι συγκεντρωτικό ή αποκεντρωμένο κατά μία τεχνική αρχιτεκτονική άποψη, κατά την οποία πρέπει να ληφθεί υπόψη πόσοι υπολογιστές ή κόμβοι χρησιμοποιούνται για την σχεδίαση του συστήματος. Υπάρχει, ωστόσο και η πολιτική αντίληψη η οποία καταδεικνύει πόσο έλεγχο ασκεί ένα άτομο ή μία ομάδα ανθρώπων ή ένας οργανισμός πάνω σε ένα σύστημα. Εάν οι υπολογιστές ενός συστήματος ελέγχονται, τότε πρόκειται για ένα συγκεντρωτικό σύστημα, ενώ αν δεν ασκείται κάποιος έλεγχος από συγκεκριμένο άτομο ή ομάδα ατόμων, τότε πρόκειται για αποκεντρωμένο σύστημα, κατά την έννοια αυτή. Τέλος, υπάρχει και η λογική αντίληψη, κατά την οποία ένα σύστημα μπορεί να είναι συγκεντρωτικό ή αποκεντρωμένο ανάλογα με το πώς φαίνεται ότι είναι. Έτσι, εάν ένα σύστημα «κοπεί στα δύο», εάν τα μέρη μπορούν να λειτουργήσουν σαν ανεξάρτητη μονάδα, πρόκειται για αποκεντρωμένο σύστημα, διαφορετικά πρόκειται για συγκεντρωτικό.

Το blockchain σχεδιάστηκε με τέτοιο τρόπο ώστε να επιτρέπει την αποκέντρωση, συνεπώς κατά την τεχνική αρχιτεκτονική άποψη είναι αποκεντρωτικό σύστημα. Επιπλέον, κανείς δεν ασκεί τον απόλυτο έλεγχο, είναι επομένως αποκεντρωτικό και κατά την πολιτική αντίληψη. Ωστόσο, υπάρχει μία συμφωνημένη

[7] Beginning Blockchain: A Beginner's Guide to Building Blockchain Solutions, Bikramaditya Singhal, Gautam Dhameja, and Priyansu Sekhar Panda, Apress, 2018

κατάσταση, και όλο το σύστημα συμπεριφέρεται ως ένας, μοναδικός, παγκόσμιος υπολογιστής, συνεπώς, μπορεί να χαρακτηριστεί συγκεντρωτικό κατά την λογική αντίληψη.

Τα συγκεντρωτικά συστήματα είναι εύκολο να σχεδιαστούν, να διατηρηθούν κι είναι έμπιστα. Διαθέτουν ωστόσο κάποιους περιορισμούς, όπως το γεγονός ότι έχουν ένα κεντρικό σημείο αποτυχίας, το οποίο τα καθιστά λιγότερο σταθερά, είναι ευάλωτα σε επιθέσεις, επομένως λιγότερο ασφαλή. Επίσης, η συγκέντρωση του ελέγχου σε ένα κεντρικό σημείο μπορεί να οδηγήσει σε αντιδεοντολογικές πρακτικές. Τέλος, η κλιμάκωση είναι δύσκολης στις περισσότερες περιπτώσεις.

Τα αποκεντρωμένα συστήματα δεν έχουν ένα κεντρικό σημείο ελέγχου, αντιθέτως κάθε κόμβος διαθέτει ισότιμη εξουσία. Παρόλο που τα συστήματα αυτά παρουσιάζουν δυσκολίες στο να σχεδιαστούν, να διατηρηθούν, να διοικηθούν, να εμπνεύσουν εμπιστοσύνη, δεν διαθέτουν τα μειονεκτήματα των συγκεντρωτικών συστημάτων. Προσφέρουν, αντιθέτως, μία σειρά πλεονεκτημάτων, όπως η σταθερότητα και η ανεκτικότητα σε λάθη, εξαιτίας του γεγονότος ότι δεν διαθέτουν ένα κεντρικό σημείο αποτυχίας, η μεγαλύτερη ασφάλεια και ανθεκτικότητα σε επιθέσεις και μεγαλύτερη δημοκρατικότητα, καθώς πρόκειται για συμμετρικά συστήματα με ισότιμη εξουσία σε όλους, συνεπώς είναι λιγότερο πιθανό να υπάρξουν αντιδεοντολογικές πρακτικές.

Δημόσια και ιδιωτικά Blockchain

Τα δημόσια Blockchain δεν ανήκουν σε κανέναν, είναι ανοιχτά στο κοινό κι οποιοσδήποτε μπορεί να συμμετάσχει, ως κόμβος, στη διαδικασία λήψης αποφάσεων. Όλοι οι χρήστες διατηρούν ένα αντίγραφο του καθολικού στους κόμβους τους κι χρησιμοποιούν ένα μηχανισμό consensus για να αποφασίσουν την τελική κατάσταση του καθολικού. Παράδειγμα δημόσιου blockchain είναι το bitcoin και το Ethereum.

Τα ιδιωτικά blockchain είναι ανοιχτά μόνο σε μία κοινοπραξία ή σε μία ομάδα ατόμων ή οργανισμών που έχουν αποφασίσει να μοιράζονται το καθολικό μεταξύ τους. Παραδείγματα ιδιωτικών blockchain είναι το Hyperledger και το Ripple.

Ημι-ιδιωτικά blockchain

Τα Ημι-ιδιωτικά blockchain είναι κατά το ήμισυ ιδιωτικά και κατά το ήμισυ δημόσια. Σε ένα ημι-ιδιωτικό blockchain, το ιδιωτικό μέρος ελέγχεται από μία ομάδα ατόμων, ενώ το δημόσιο μέρος είναι ανοιχτό για οποιονδήποτε. Αυτό το είδος blockchain, μπορεί επίσης να χαρακτηριστεί ως ημι-αποκεντρωτικό μοντέλο, το οποίο ελέγχεται από μία οντότητα αλλά ταυτόχρονα επιτρέπει σε πολλούς χρήστες να συμμετέχουν στο δίκτυο ακολουθώντας τις ανάλογες διαδικασίες.

Επίπεδα του blockchain

Δεν υπάρχει ομοφωνία ως προς το διαχωρισμό των περιεχομένων του blockchain σε επίπεδα, καθώς υπάρχουν πολλές αναπαραστάσεις των επιπέδων. Κατά μία άποψη τα επίπεδα είναι τα ακόλουθα:

i. Application layer

Σε αυτό το επίπεδο γίνεται η κωδικοποίηση των επιθυμητών λειτουργιών για τη δημιουργία εφαρμογών για τον τελικό χρήστη. Συνήθως περιλαμβάνει τεχνικό εξοπλισμό για την ανάπτυξη λογισμικού όπως client προγραμματιστικές δομές, scripting, APIs, κλπ.

ii. Execution layer

Στο επίπεδο αυτό, λαμβάνει χώρα η εκτέλεση των εντολών σε όλους του κόμβους του δικτύου, οι οποίες εντολές δίνονται από το application layer. Οι εντολές μπορεί να περιλαμβάνουν είτε απλές εντολές, είτε πιο σύνθετες όπως τα smart contracts (έξυπνα συμβόλαια). Σε κάθε περίπτωση, το πρόγραμμα ή το script πρέπει να εκτελεστεί για τη σωστή διεξαγωγή των συναλλαγών και όλοι οι κόμβοι πρέπει να το εκτελέσουν ανεξάρτητα.

Τα script που εκτελούνται στο bitcoin είναι συνήθως απλά, δεν είναι Turing complete και επιτρέπουν την εκτέλεση μερικών μόνο εντολών. Ωστόσο, το Ethereum και το Hyperledger επιτρέπουν πιο περίπλοκες εντολές.

iii. Semantic layer

Μία συναλλαγή, έγκυρη ή μη, περιέχει μια σειρά από εντολές που εκτελούνται στο execution layer, ωστόσο επιβεβαιώνεται στο sematic layer. Για παράδειγμα εάν πρόκειται για το bitcoin, σε αυτό το επίπεδο διαπιστώνεται κατά πόσο κάποιος έχει κάνει μία νόμιμη συναλλαγή, εάν πρόκειται για επίθεση διπλοξοδέματος ή εάν κάποιος νομιμοποιείται να πραγματοποιήσει τη συναλλαγή. Επιπλέον στο επίπεδο αυτό καθορίζεται το πώς συνδέονται μεταξύ τους τα blocks. Όπως ήδη αναφέρθηκε, κάθε block στην αλυσίδα περιλαμβάνει το hash του προηγούμενου block μέχρι το αρχικό block (genesis block). Σε αυτό το επίπεδο, λοιπόν, καθορίζεται η σύνδεση μεταξύ των blocks.

iv. Propagation layer

Σε αυτό το επίπεδο επιτυγχάνεται η peer-to-peer επικοινωνία μεταξύ των κόμβων, η οποία τους επιτρέπει να ανακαλύπτουν ο ένας τον άλλον, να μιλούν και να συγχρονίζονται με βάση την τρέχουσα κατάσταση του δικτύου. Έτσι, όταν ένας κόμβος επιθυμεί να προτείνει ένα έγκυρο block, αμέσως μεταδίδεται σε ολόκληρο το δίκτυο προκειμένου οι υπόλοιποι κόμβοι να συνεχίσουν την αλυσίδα, θεωρώντας αυτό ως το πιο πρόσφατο block. Συνεπώς, η μετάδοση των block στο δίκτυο γίνεται σε αυτό το επίπεδο, διασφαλίζοντας την σταθερότητα του δικτύου.

v. Consensus layer

Το επίπεδο αυτό είναι συνήθως η βάση για τα περισσότερα blockchain συστήματα. Ο βασικός σκοπός του είναι να επιτύχει πλήρη συμφωνία από όλους του κόμβους για μία σταθερή κατάσταση του καθολικού. Η ασφάλεια του blockchain επιβεβαιώνεται στο επίπεδο αυτό. Στο bitcoin και στο Ethereum το consensus (συναίνεση) επιτυγχάνεται μέσω μία τεχνικής η οποία ονομάζεται mining (εξόρυξη), χρησιμοποιώντας ένα μηχανισμό Proof of Work(PoW).[8]

[8] Beginning Blockchain: A Beginner's Guide to Building Blockchain Solutions, Bikramaditya Singhal, Gautam Dhameja, and Priyansu Sekhar Panda, Apress, 2018

Κρυπτογραφία

Η κρυπτογραφία διαφυλάσσει τις τρεις βασικές αρχές της ασφάλειας πληροφοριών: εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα[9]. Η εμπιστευτικότητα διασφαλίζει ότι οι πληροφορίες διαμοιράζονται μεταξύ των σωστών μερών και ότι οι ευαίσθητες πληροφορίες (για παράδειγμα ιατρικές πληροφορίες, οικονομικά δεδομένα κλπ.) διαμοιράζονται αποκλειστικά με την συναίνεση των συμμετεχόντων. Η ακεραιότητα διασφαλίζει ότι μόνο εξουσιοδοτημένα άτομα μπορούν να αλλάξουν τα δεδομένα και ότι οι αλλαγές δεν απειλούν την ακρίβεια ή την αυθεντικότητα των δεδομένων. Η αρχή αυτή είναι η πιο σχετική με τα blockchain εν γένει κι ειδικότερα με τα δημόσια blockchain. Η διαθεσιμότητα διασφαλίζει ότι οι εξουσιοδοτημένοι χρήστες έχουν στη διάθεσή τους τη χρήση των δεδομένων όταν τα χρειάζονται ή όταν τα θέλουν.

Ο τρόπος με τον οποίο λειτουργεί η κρυπτογραφία είναι ο εξής: οποιαδήποτε πληροφορία σε μορφή γραπτού μηνύματος, αριθμητικών δεδομένων, προγραμμάτων ονομάζεται αρχικό κείμενο, το οποίο πρόκειται να κρυπτογραφηθεί με τη χρήση ενός αλγόριθμου κρυπτογράφησης και ενός κλειδιού που παράγουν το κρυπτοκείμενο. Το κρυπτοκείμενο μεταδίδεται στον λήπτη, ο οποίος το αποκρυπτογραφεί χρησιμοποιώντας τον αλγόριθμο κρυπτογράφησης και το κλειδί. Υπάρχουν δύο συστήματα κρυπτογραφίας, η συμμετρική κρυπτογραφία και η ασύμμετρη κρυπτογραφία (κρυπτογραφία δημοσίου κλειδιού)[10].

Στην συμμετρική κρυπτογραφία χρησιμοποιείται κατά τη διαδικασία της κρυπτογράφησης ή αποκρυπτογράφησης ένα κοινό κλειδί[11]. Η ασφάλεια αυτών των αλγορίθμων βασίζεται στη μυστικότητα του κλειδιού. Τα συμμετρικά κρυπτοσυστήματα προϋποθέτουν την ανταλλαγή του κλειδιού μέσα από ένα ασφαλές κανάλι επικοινωνίας ή μέσα από την φυσική παρουσία των προσώπων. Αυτό το χαρακτηριστικό καθιστά δύσκολη την επικοινωνία μεταξύ απομακρυσμένων ατόμων. Τα στάδια της επικοινωνίας μεταξύ δύο χρηστών μέσω του συμμετρικού μοντέλου είναι τα ακόλουθα: 1. Οι χρήστες του συστήματος αποφασίζουν για ένα κλειδί το οποίο το επιλέγει τυχαία μέσα από τον κλειδοχώρο. 2. Ο πρώτος χρήστης αποστέλλει το κλειδί στον δεύτερο μέσα από ένα ασφαλές κανάλι. 3. Ο δεύτερος δημιουργεί ένα μήνυμα όπου τα σύμβολα m ανήκουν στον χώρο των μηνυμάτων. 4. Κρυπτογραφεί το μήνυμα με το κλειδί που έλαβε από τον πρώτο χρήστη και η παραγόμενη κρυπτοσυμβολοσειρά αποστέλλεται. 5. Ο πρώτος χρήστης λαμβάνει την κρυπτοσυμβολοσειρά και στη συνέχεια με το ίδιο κλειδί την αποκρυπτογραφεί και η έξοδος που παράγεται είναι το αρχικό μη κρυπτογραφημένο μήνυμα[12].

---

[9] Brenn Hill, Samanyu Chopra, Paul Valencourt.; Blockchain Quick Reference : A Guide to Exploring Decentralized Blockchain Application Development

[10] Beginning Blockchain: A Beginner's Guide to Building Blockchain Solutions, Bikramaditya Singhal, Gautam Dhameja, and Priyansu Sekhar Panda, Apress, 2018

[11] https://el.wikipedia.org/wiki/%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%AC%CF%86%CE%B7%CF%83%CE%B7_%CE%A3%CF%85%CE%BC%CE%BC%CE%B5%CF%84%CF%81%CE%B9%CE%BA%CE%BF%CF%8D_%CE%9A%CE%BB%CE%B5%CE%B9%CE%B4%CE%B9%CE%BF%CF%8D

[12] Beginning Blockchain: A Beginner's Guide to Building Blockchain Solutions, Bikramaditya Singhal, Gautam Dhameja, and Priyansu Sekhar Panda, Apress, 2018

Το σύστημα συμμετρικής κρυπτογραφίας περιλαμβάνει διάφορους αλγόριθμους οι οποίοι χωρίζονται σε κατηγορίες. Συνεπώς υπάρχουν οι κρυπτογραφικοί αλγόριθμοι δέσμης (block ciphers), οι οποίοι χωρίζουν το μήνυμα σε κομμάτια και κρυπτογραφούν κάθε ένα από τα κομμάτια αυτά χωριστά, όπως ο DES (Data encryption standard), 3DES, AES κλπ, οι αλγόριθμοι ροής (stream ciphers) οι οποίοι κρυπτογραφούν μία ροή μηνύματος (stream) χωρίς να τη διαχωρίζουν σε τμήματα, όπως οι RC4, FISH, SNOW, SEAL, A5/1 κλπ. και οι αλγόριθμοι αντικατάστασης (substitution ciphers), οι οποίοι αντιστοιχίζουν και στη συνέχεια αντικαθιστούν κάθε σύμβολο γράμμα του αρχικού μηνύματος με κάποιο άλλο γράμμα ή ακολουθία γραμμάτων, ενώ ο δέκτης λαμβάνοντας το μήνυμα για να το αποκρυπτογραφήσει ακολουθεί την ανάστροφη διαδικασία[13].

Τα συστήματα συμμετρικής κρυπτογραφίας αντιμετωπίζουν, ωστόσο και κάποιες προκλήσεις. Αρχικά, το κλειδί είναι απαραίτητο να διαμοιραστεί μεταξύ του αποστολέα και του παραλήπτη πριν από την επικοινωνία, γεγονός που δημιουργεί την ανάγκη ενός μηχανισμού ασφαλούς διαμοιρασμού κλειδιών. Ο αποστολέας και ο παραλήπτης, επειδή μοιράζονται το ίδιο κλειδί, πρέπει να εμπιστεύονται ο ένας τον άλλον, για να αποφεύγεται έτσι η παρεμβολή κάποιου κακόβουλου τρίτου στο σύστημα. Επιπλέον, ένα μεγάλο δίκτυο το οποίο θα αποτελείται από n κόμβους, απαιτεί τη διαχείριση μεγάλου αριθμού κλειδιών και συγκεκριμένα n(n-1)/2 ζευγάρια κλειδιών. Υπάρχει, επίσης, συνεχής ανάγκη αλλαγής των κλειδιών. Τέλος, για την ορθότερη διαχείριση των κλειδιών, συνήθως χρειάζεται ένας έμπιστος τρίτος, γεγονός που από μόνο αποτελεί σημαντικό ζήτημα.

Η ασύμμετρη κρυπτογραφία, ή όπως είναι γνωστή η κρυπτογραφία δημοσίου κλειδιού αποτελεί μία επαναστατική μέθοδο με την οποία λύνεται το ζήτημα του διαμοιρασμού κλειδιών της συμμετρικής κρυπτογραφίας, μέσω των ψηφιακών υπογραφών[14]. Η βασική ιδέα είναι ότι ο αποστολέας και ο παραλήπτης δεν μοιράζονται ένα κοινό μυστικό κλειδί όπως στην περίπτωση της κρυπτογράφησης συμμετρικού κλειδιού, αλλά διαθέτουν διαφορετικά κλειδιά για διαφορετικές λειτουργίες. Συγκεκριμένα κάθε χρήστης διαθέτει δύο κλειδιά κρυπτογράφησης: το ένα ονομάζεται ιδιωτικό κλειδί (private key) και το άλλο δημόσιο κλειδί (public key). Το ιδιωτικό κλειδί θα πρέπει ο κάθε χρήστης να το προφυλάσσει και να το κρατάει κρυφό, ενώ αντιθέτως το δημόσιο κλειδί μπορεί να το ανακοινώνει σε όλη τη διαδικτυακή κοινότητα ή σε συγκεκριμένους παραλήπτες. Υπάρχουν δε και ειδικοί εξυπηρετητές δημοσίων κλειδιών (public key servers) στους οποίους μπορεί κανείς να απευθυνθεί για να βρει το δημόσιο κλειδί του χρήστη που τον ενδιαφέρει ή να ανεβάσει το δικό του δημόσιο κλειδί για να είναι διαθέσιμο στο κοινό. Τα δύο αυτά κλειδιά (ιδιωτικό και δημόσιο) έχουν μαθηματική σχέση μεταξύ τους. Εάν το ένα χρησιμοποιηθεί για την κρυπτογράφηση κάποιου μηνύματος, τότε το άλλο χρησιμοποιείται για την αποκρυπτογράφηση αυτού. Η επιτυχία αυτού του είδους κρυπτογραφικών αλγορίθμων βασίζεται στο γεγονός ότι η γνώση του δημόσιου

[13] https://pithos.okeanos.grnet.gr/public/k5aKPf3nzomvLIPDbErBA6

[14] Beginning Blockchain: A Beginner's Guide to Building Blockchain Solutions, Bikramaditya Singhal, Gautam Dhameja, and Priyansu Sekhar Panda, Apress, 2018

κλειδιού κρυπτογράφησης δεν επιτρέπει με κανέναν τρόπο τον υπολογισμό του ιδιωτικού κλειδιού κρυπτογράφησης.

Ένας από τους σημαντικότερους αλγόριθμους ασύμμετρης κρυπτογραφίας είναι ο RSA, ο οποίος είναι ίσως ο πιο ευρέως διαδεδομένος αλγόριθμος κρυπτογράφησης.

Συναρτήσεις κατακερματισμού

Η συνάρτηση κατακερματισμού ή συνάρτηση κατατεμαχισμού, είναι μια μαθηματική συνάρτηση που δέχεται ως είσοδο κάποιο δεδομένο τυχαίου μεγέθους και επιστρέφει ένα ακέραιο σταθερού μεγέθους αναπαράστασης. Το μέγεθος αυτό μπορεί να είναι από 32bit μέχρι 256bit ή περισσότερα, ανάλογα με το λόγο χρήσης της συνάρτησης. Οι τιμές που επιστρέφει η συνάρτηση κατατεμαχισμού ονομάζονται τιμές κατατεμαχισμού (hash values), κώδικες κατατεμαχισμού (hash codes), αθροίσματα κατατεμαχισμού (hash sums) ή απλά τιμές κατατεμαχισμού (hashes). Οι τιμές αυτές θα πρέπει να είναι διαφορετικές για διαφορετική είσοδο, καθώς η κύρια χρησιμότητα αυτών των συναρτήσεων είναι να ταυτοποιούν τα δεδομένα. Μια εφαρμογή αυτή της ιδιότητας είναι στην υλοποίηση της δομής δεδομένων σύνολο όπου θα πρέπει να αποτρέπεται η προσθήκη στοιχείου που το σύνολο ήδη περιέχει. Σε αυτή την περίπτωση τιμές 32bit αρκούν, εκτός αν το σύνολο μπορεί να φτάσει υπερβολικά μεγάλο μέγεθος.[15]

Αυτό που κάνουν οι συναρτήσεις κατακερματισμού είναι να αντιστοιχίζουν το μήνυμα σε μια συμβολοσειρά προκαθορισμένου μεγέθους (message digests). Ο τελικός χρήστης που παραλαμβάνει ένα μήνυμα, μπορεί να το δώσει σαν όρισμα στην ίδια συνάρτηση και αν οι συμβολοσειρές (message digests) ταυτίζονται, τότε ξέρει ότι δεν υπήρξε αλλοίωση. Προκειμένου να θεωρηθεί μια συνάρτηση κατακερματισμού αποδεκτή για χρήση στην κρυπτογραφία πρέπει να πληροί συγκεκριμένες προϋποθέσεις: 1) Το κείμενο εισόδου μπορεί να έχει οποιδήποτε μέγεθος, ενώ η έξοδος πρέπει να είναι συγεκριμένου μήκους, 2)Το hash value πρέπει να μπορεί να υπολογισθεί για οποιοδήποτε κείμενο, 3) Η ίδια είσοδος με την ίδια συνάρτηση κατακερατισμού να παράγει την ίδια τιμή κάθε φορά, 4) Να είναι αδύνατο η τιμή hash να αντιστραφεί και να παραχθεί το μήνυμα και 5) Οποιαδήποτε αλλαγή στο μήνυμα πρέπει να επηρεάζει την έξοδο της συνάρτησης[16].

Μία από τις παλαιότερες συναρτήσεις κατακερματισμού είναι η MD4. Ανήκει στην οικογένεια MD(message digest). Άλλες συναρτήσεις της ίδιας οικογένειας είναι οι MD5 και MD6. Μία άλλη οικογένεια συναρτήσεων είναι οι SHA (Secure Hash Algorithm). Υπάρχουν τέσσερις αλγόριθμοι σε αυτή την οικογένεια οι SHA-0, SHA-1, SHA-2 και SHA-3.

Οι συναρτήσεις κατακερματισμού αποτελούν βασικό κομμάτι της δομής του blockchain. Μέσω του hashing το blockchain επιτυγχάνει τη διατήρηση της

[15] https://el.wikipedia.org/wiki/%CE%A3%CF%85%CE%BD%CE%AC%CF%81%CF%84%CE%B7%CF%83%CE%B7_%CE%BA%CE%B1%CF%84%CE%B1%CF%84%CE%B5%CE%BC%CE%B1%CF%87%CE%B9%CF%83%CE%BC%CE%BF%CF%8D

[16] Beginning Blockchain: A Beginner's Guide to Building Blockchain Solutions, Bikramaditya Singhal, Gautam Dhameja, and Priyansu Sekhar Panda, Apress, 2018

αποκέντρωσης και της σταθερότητας. Εφόσον υπάρχει μόνο ένα πιθανό αποτέλεσμα και είναι αδύνατο να δοθεί το ίδιο αποτέλεσμα με διαφορετική είσοδο, γίνεται η σύνδεση ενός μπλοκ με το προηγούμενό του (κάθε μπλοκ περιέχει το hash του προηγούμενου) και μπορεί έτσι να διασφαλιστεί ότι μία ή περισσότερες συναλλαγές είναι έγκυρες. Εκτός από την ασφάλεια και την ακεραιότητα, οι συναρτήσεις κατακερματισμού βοηθούν ώστε τα δεδομένα να κατανέμονται σε πίνακες hash, διευκολύνοντας και επιταχύνοντας έτσι την αναζήτησή τους. Έτσι, αντί για ολόκληρα δεδομένα, αν αναζητήσουμε βάσει του hash, εφόσον το hash value είναι πολύ μικρότερο σε μέγεθος από το δεδομένο, η αναζήτηση θα ολοκληρωθεί γρηγορότερα. Επίσης, στο bitcoin, οι συναρτήσεις κατακερματισμού χρησιμοποιούνται ως proof of work (PoW) αλγόριθμοι.

Θεωρία παιγνίων

Η θεωρία παιγνίων χρησιμοποιείται εδώ και πολλά έτη σε διάφορες καταστάσεις της πραγματικής ζωής για την επίλυση περίπλοκων προβλημάτων. Χρησιμοποιείται επίσης και σε πολλές εφαρμογές blockchain όπως το bitcoin. Επισήμως παρουσιάστηκε από τον John von Neumann στη μελέτη οικονομικών αποφάσεων. Αργότερα, έγινε πιο δημοφιλής από τον John Forbes Nash Jr λόγω της θεωρίας της «Ισορροπίας Nash»[17].

Η θεωρία παιγνίων εφαρμόζεται σε καταστάσεις όπου δύο ή περισσότερα μέρη καλούνται να λάβουν αποφάσεις χρησιμοποιώντας στρατηγική σκέψη. Ως «παίγνιο» μπορεί να οριστεί μία κατάσταση που περιλαμβάνει μία συσχετιζόμενη λογική επιλογή, δηλαδή μία επιλογή η οποία λαμβάνεται από τις διαθέσιμες οπτικές, όχι όμως με βάση τις επιλογές που διαθέτει μία πλευρά μόνο, αλλά με βάση τις επιλογές που κάνουν όλες οι συμμετέχουσες πλευρές. Πρόκειται, συνεπώς, για μελέτη στρατηγικών και επιλογή της κατάλληλης κίνησης, μελετώντας και καταλαβαίνοντας παράλληλα τη στρατηγική του αντιπάλου.

Μία από τις δημοφιλέστερες θεωρίες, όπως ήδη αναφέρθηκε, η οποία ομοιάζει με πολλές καταστάσεις της καθημερινής ζωής είναι η θεωρίας της «Ισορροπίας Nash (Nash Equilibrium). Σύμφωνα με τη θεωρία αυτή, σε κάθε «παιχνίδι» στο οποίο δεν υπάρχει συνεργασία μεταξύ των παικτών και στο οποίο οι παίκτες γνωρίζουν τις στρατηγικές των άλλων παικτών, υπάρχει τουλάχιστον ένα σημείο ισορροπίας στο οποίο όλοι οι παίκτες χρησιμοποιούν τις καλύτερες στρατηγικές του για να πετύχουν το μεγαλύτερο δυνατό κέρδος και καμία πλευρά δεν θα είχε όφελος από το να αλλάξει την στρατηγική της.

Ένα επίσης πολύ δημοφιλές πρόβλημα, το οποίο χρησιμοποιείται ευρέως για την επίλυση προβλημάτων στην επιστήμη υπολογιστών αλλά και στην καθημερινή ζωή, είναι το πρόβλημα των βυζαντινών στρατηγών. Πρόκειται για μία κατάσταση την οποία αντιμετωπίζει ο Βυζαντινός στρατός κατά την επίθεσή του σε κάποια πόλη. Ο στρατός απαρτίζεται από διαφορετικά τμήματα που ακολουθούν εντολές διαφορετικών στρατηγών τα οποία έχουν περικυκλώσει κάποια πόλη για να την

[17] Beginning Blockchain: A Beginner's Guide to Building Blockchain Solutions, Bikramaditya Singhal, Gautam Dhameja, and Priyansu Sekhar Panda, Apress, 2018

κατακτήσουν και, φυσικά, ο μόνος τρόπος για να ο επιτύχουν είναι εάν επιτεθούν στην πόλη ταυτόχρονα. Το πρόβλημα είναι ο τρόπος με τον οποίον θα επιτύχουν τη συναίνεση. Έτσι, είτε όλοι οι στρατηγοί πρέπει επιτεθούν είτε όλοι να υποχωρήσουν, διαφορετικά είναι αδύνατον να κερδίσουν τη μάχη. Με αυτά τα δεδομένα είναι φανερό ότι υπάρχουν πολλά και διαφορετικά σενάρια ως προς το πώς θα εξελιχθεί η επίθεση. Υπάρχει επίσης και η πιθανότητα να υπάρχει κάποιος προδότης μεταξύ των στρατηγών ο οποίος δεν θα εκτελέσει την εντολή που έλαβε, για παράδειγμα να επιτεθεί και θα μεταφέρει στο τάγμα του την αντίθετη εντολή. Επιπλέον, είναι πολύ μεγάλης σημασίας το ζήτημα της μεταφοράς των μηνυμάτων μεταξύ των στρατηγών, πως επιτυγχάνεται δηλαδή, η μεταξύ τους επικοινωνία. Έτσι, γεννώνται πολλά ερωτήματα: Αν υπάρχουν πολλοί προδότες; Αν αυτός που μεταφέρει τα μηνύματα σκοτωθεί ή δωροδοκηθεί από τον αντίπαλο; Πώς είναι δυνατόν να εντοπιστούν οι προδότες στρατηγοί; Ο τρόπος με τον οποίο είναι απαραίτητο οι στρατηγοί να φτάσουν σε μία κατάσταση συναίνεσης, ομοιάζει με τον τρόπο με τον οποίο φτάνουν σε συναίνεση οι κόμβοι ενός blockchain όσον αφορά την κατάσταση του καθολικού.[18]

Η αλυσίδα των block

Το blockchain αποτελεί μία δομή δεδομένων σε μορφή αλυσίδας από μπλοκ που είναι συνδεδεμένα μεταξύ τους. Ένα μπλοκ μπορεί να είναι μία συναλλαγή ή πολλές συναλλαγές. Το βασικό συστατικό της αλυσίδας είναι οι δείκτες κατακερματισμού (hash pointers). Πρόκειται για μία κρυπτογραφημένη συνάρτηση κατακερματισμού που δείχνει προς ένα άλλο μπλοκ, στο οποίο ο δείκτης κατακερματισμού είναι η συνάρτηση κατακερματισμού του συγκεκριμένου μπλοκ. Οι δείκτες κατακερματισμού δείχνουν προς το προηγούμενο μπλοκ (parent block) και αυτή η αλληλουχία συνεχίζεται μέχρι το πρώτο μπλοκ το οποίο ονομάζεται genesis block. Επίσης, κάθε νέο μπλοκ που προστίθεται στην αλυσίδα γίνεται το parent block του επόμενου μπλοκ που πρόκειται να προστεθεί. Με αυτόν το τρόπο σχεδιασμού του blockchain, με τους δείκτες κατακερματισμού να συνδέουν τα μπλοκ μέχρι το αρχικό μπλοκ, είναι αδύνατο τα δεδομένα που περιέχονται στα μπλοκ να επηρεαστούν ή να αλλοιωθούν, διότι αν κάποιος αλλάξει τα δεδομένα ενός μπλοκ τότε τα hash δε θα συμπίπτουν, όπως αναφέρθηκε και ανωτέρω. Επιπλέον θα ήταν αδύνατο κάποιος να αλλάξει το ίδιο το hash κάποιου μπλοκ, διότι αυτό προϋποθέτει να αλλαχθούν τα hash όλων των μπλοκ μέχρι το genesis block, πράγμα εξαιρετικά δύσκολο. Ακόμα και εάν αυτό επιτύχει, επειδή κάθε κόμβος στο δίκτυο διαθέτει αντίγραφα του καθολικού, θα υπήρχε και πάλι πρόβλημα επιβεβαίωσης των δεδομένων μεταξύ των κόμβων. Για να επιτύχει μία τέτοια επίθεση, θα έπρεπε κανείς να επέμβει σε όλα τα συστήματα και να αλλάξει τα hash ταυτόχρονα[19].

[18] Beginning Blockchain: A Beginner's Guide to Building Blockchain Solutions, Bikramaditya Singhal, Gautam Dhameja, and Priyansu Sekhar Panda, Apress, 2018

[19] Beginning Blockchain: A Beginner's Guide to Building Blockchain Solutions, Bikramaditya Singhal, Gautam Dhameja, and Priyansu Sekhar Panda, Apress, 2018

Με τη χρήση των δεικτών κατακερματισμού επιτυγχάνεται μεγάλη ασφάλεια για το σύστημα και ανθεκτικότητα σε αλλαγές και παρεμβολές στα δεδομένα που περιέχουν τα μπλοκ.

Δέντρα merkle

Τα δέντρα merkle, τα οποία πήραν το όνομά τους από τον εφευρέτη τους, τον Ralph Merkle, είναι δυαδικά δέντρα που αποτελούνται από δείκτες κατακερματισμού. Πρόκειται για ακόμα μία δομή δεδομένων που χρησιμοποιείται στα blockchain και ειδικότερα από το bitcoin. Τα δέντρα merkle αποτελούνται από συζευγμένα δεδομένα στα οποία χρησιμοποιείται ένα hash στο αποτέλεσμα των οποίων γίνεται ξανά hash. Η διαδικασία αυτή επαναλαμβάνεται μέχρι τη ρίζα του κόμβου, η οποία ονομάζεται ρίζα merkle. Σχηματικά απεικονίζεται ως ένα ανάποδο δέντρο, καθώς οι συναλλαγές αποτελούν τα «φύλλα» του δέντρου, στις οποίες εφαρμόζεται hash ανά ζεύγη, στο αποτέλεσμα των οποίων εφαρμόζεται ξανά hash, μέχρι τη κορυφή που είναι η ρίζα.

Όπως και οι δείκτες κατακερματισμού, έτσι και τα δέντρα merkle είναι ανθεκτικά σε οποιαδήποτε αλλαγή, καθώς αν επιχειρηθεί η τροποποίηση δεδομένων σε οποιοδήποτε επίπεδο του δέντρου, δεν θα ταιριάζει με τα hash που έχουν αποθηκευτεί στη ρίζα του δέντρου.

Προκειμένου να επιβεβαιωθεί εάν μία συναλλαγή ανήκει στο δέντρο merkle, δεν είναι απαραίτητο να ελεγχθούν όλες οι συναλλαγές. Αντιθέτως, ξεκινώντας από δύο συναλλαγές και υπολογίζοντας το hash τους, μπορεί να επιβεβαιωθεί αν αυτό ταιριάζει με το hash του parent hash. Στη συνέχεια, υπολογίζοντας το hash του parent hash και του ζεύγους του σε αυτό το επίπεδο, επιβεβαιώνεται αν ταιριάζει με το δικό τους parent hash και η διαδικασία αυτή συνεχίζεται μέχρι τη ρίζα, η οποία περιλαμβάνει τα hash όλων των συναλλαγών του δέντρου.

Τα δέντρα merkle παρέχουν ένα πολύ αποτελεσματικό τρόπο επιβεβαίωσης για το εάν μία συναλλαγή ανήκει σε κάποιο μπλοκ. Σε κάθε μπλοκ, εκτός από τα συστατικά που αναφέρθηκαν ανωτέρω, περιλαμβάνεται και η ρίζα merkle όλων των συναλλαγών του μπλοκ. Έτσι, εάν θέλουμε να επιβεβαιώσουμε εάν μία συναλλαγή ανήκει σε κάποιο μπλοκ, ελέγχουμε εάν το hash της συγκεκριμένη συναλλαγής περιλαμβάνεται στη ρίζα merkle. Εάν περιλαμβάνεται, επιβεβαιώνεται και η συναλλαγή.

Η χρήση των δέντρων merkle δεν περιορίζεται μόνο στα blockchain, αλλά είναι πολύ δημοφιλείς σε γνωστές εφαρμογές όπως τα BitTorrent, Cassandra-an, No SQL database, Apache Wave, κλπ.[20]

Συναλλαγές σε blockchain

Οι συναλλαγές σε ένα δίκτυο blockchain περνούν από τα εξής βήματα προκειμένου να συμπεριληφθούν στο καθολικό:

1) Κάθε νέα συναλλαγή μεταδίδεται στο δίκτυο για να ενημερωθούν όλοι οι

[20] Beginning Blockchain: A Beginner's Guide to Building Blockchain Solutions, Bikramaditya Singhal, Gautam Dhameja, and Priyansu Sekhar Panda, Apress, 2018

κόμβοι ότι η συναλλαγή έλαβε χώρα καθώς και το χρόνο κατά τον οποίο συνέβη.

2) Οι κόμβοι ελέγχουν την αυθεντικότητα της συναλλαγής προκειμένου να την επικυρώσουν ή να την απορρίψουν.
3) Οι κόμβοι ίσως στοιβάξουν κάποιες συναλλαγές σε γκρουπ μέσα σε μπλοκ για να τις μοιραστούν με το υπόλοιπο δίκτυο.
4) Οι κόμβοι συμφωνούν στην εγκυρότητα ή μη κάποιας συναλλαγής μέσω του consensus (συναίνεση). Υπάρχουν διάφοροι αλγόριθμοι συναίνεσης.
5) Τα μπλοκ προστίθενται το ένα μετά το άλλο με τη χρονική σειρά με την οποία φτάνουν και γίνονται μέρος της αλυσίδας.
6) Μόλις οι κόμβοι του δικτύου αποδεχτούν ένα μπλοκ κι αυτό γίνει μέρος της αλυσίδας, περιλαμβάνει το hash του μπλοκ που έγινε αποδεκτό αμέσως πριν από αυτό, επεκτείνοντας έτσι την αλυσίδα κατά ένα μπλοκ.[21]

Μηχανισμοί συναίνεσης (consensus)

Η χρησιμότητα και η σημαντικότητα των μηχανισμών consensus έγκειται στην πιθανότητα ύπαρξης κακόβουλων κόμβων που θα επικυρώσουν μη έγκυρες συναλλαγές. Μέσω των μηχανισμών αυτών, οι κόμβοι ελέγχουν και επιβεβαιώνουν ένα μπλοκ συναλλαγών που έχει προτείνει ένας άλλος κόμβος, έχοντας κι οι ίδιοι, όπως ήδη έχει αναφερθεί, ένα αντίγραφο του καθολικού, και εφόσον φτάσουν σε συναίνεση, αυτό προστίθεται στην αλυσίδα. Έτσι, το σύστημα παραμένει επίσης δυνατό και ανθεκτικό απέναντι σε κάθε είδους επιθέσεις. Οι μηχανισμοί συναίνεσης ποικίλουν ανάλογα με τις ανάγκες του κάθε συστήματος.

Proof of work - Απόδειξη εργασίας (PoW)

Η ιδέα πίσω από τον αλγόριθμο PoW είναι ότι πρέπει να γίνει κάποια συγκεκριμένη ποσότητα υπολογιστικής εργασίας, η οποία ονομάζεται εξόρυξη (mining), πριν ένας κόμβος προτείνει ένα μπλοκ συναλλαγών σε ολόκληρο το δίκτυο. Η απόδειξη εργασίας αποτελεί ένα κομμάτι δεδομένων που είναι δύσκολο να παραχθεί, διότι απαιτεί μεγάλη υπολογιστική δύναμη και χρόνο, είναι όμως εύκολο να επιβεβαιωθεί. Αρχικά χρησιμοποιήθηκε για την αποφυγή spam email. Αυτό που ουσιαστικά προσφέρει είναι ότι εάν υπάρχει ανάγκη για εξαιρετικά μεγάλη υπολογιστική εργασία προκειμένου να προταθεί ένα μπλοκ, τότε αφενός θα χρειαστεί πολύ χρόνος μέχρι να προταθεί ένα μπλοκ και αφετέρου, εάν ένας κόμβος προσπαθήσει να προτείνει μία ψεύτικη συναλλαγή, τότε η απόρριψη της συναλλαγής από τους άλλους κόμβους θα είναι πολύ δαπανηρή για τον ίδιο. Εάν δεν υπήρχε η απαίτηση συγκεκριμένης ποσότητας εργασίας πριν την πρόταση κάποιου μπλοκ, τότε οι κόμβοι θα μπορούσαν να προτείνουν συνεχώς συναλλαγές με την ελπίδα ότι κάποια από αυτές θα μπορούσε κάποια στιγμή να περάσει και να ενταχθεί στο καθολικό.

Για να είναι αποδοτικός ο αλγόριθμος PoW πρέπει να προσαρμόζεται κάθε φορά το επίπεδο της δυσκολίας της εργασίας, ώστε να υπάρχει έλεγχος του πόσο

[21] Beginning Blockchain: A Beginner's Guide to Building Blockchain Solutions, Bikramaditya Singhal, Gautam Dhameja, and Priyansu Sekhar Panda, Apress, 2018

γρήγορα παράγονται τα μπλοκ. Επίσης, εάν πολλοί κόμβοι ταυτόχρονα προσπαθούν να επιλύσουν ένα υπολογιστικό πρόβλημα, είναι δύσκολο να καθοριστεί ποιος το έλυσε πρώτος. Σε δημόσια blockchain, είναι σημαντικό οι κόμβοι που διαθέτουν την υπολογιστική τους δύναμη, να επιβραβεύονται όταν επιδεικνύουν τίμια συμπεριφορά και αποφεύγουν κακόβουλες ενέργειες, λόγω της δυνατότητας που υπάρχει να έχουν πολλαπλές ταυτότητας και να παραμένουν ανώνυμοι, αποφεύγοντας έτσι πιθανές επιπλήξεις για κακόβουλη συμπεριφορά, αλλάζοντας κάθε φορά την ταυτότητά τους.

Proof of stake

Πρόκειται για έναν ακόμη αλγόριθμο συναίνεσης, ο οποίος δεν επικεντρώνεται τόσο στην εξόρυξη, όσο στην επικύρωση μπλοκ συναλλαγών. Δεν υπάρχουν επιβραβεύσεις για τους miners λόγω παραγωγής νέων νομισμάτων, αλλά υπάρχουν μόνο τέλη συναλλαγών για τους επικυρωτές (validators). Στα συστήματα αυτά, οι επικυρωτές δεσμεύουν το μερίδιο τους για να μπορέσουν να λάβουν μέρος στην επικύρωση συναλλαγών. Η πιθανότητα για έναν επικυρωτή να δημιουργήσει ένα μπλοκ είναι ανάλογη με το μερίδιό του, δηλαδή όσο μεγαλύτερο είναι το μερίδιό του τόσο μεγαλύτερη είναι η πιθανότητα να επικυρώσει ένα νέο μπλοκ συναλλαγών. Συγκριτικά με τα συστήματα PoW, τα συστήματα PoS προσφέρουν μεγαλύτερη προστασία απέναντι σε επιθέσεις, ενώ απαιτεί πολύ μικρότερη κατανάλωση ηλεκτρικής ενέργειας.

Practical Byzantine Fault Tolerance (PBFT)

Όπως και ο PoS έτσι και ο PBFT αλγόριθμος δεν βασίζεται σε επιβραβεύσεις μέσω της εξόρυξης. Κάθε φορά που πραγματοποιείται μια συναλλαγή, επικυρώνεται μέσω μιας συγκεκριμένης διαδικασίας. Ειδικότερα, όταν οι κόμβοι λάβουν ένα αίτημα, διεξάγουν τη διαδικασία υπολογισμού βασιζόμενοι στα δικά τους αντίγραφα. Το αποτέλεσμα των υπολογισμών διαμοιράζεται σε όλους τους υπόλοιπους κόμβους στο σύστημα και έτσι κάθε κόμβος γνωρίζει τι υπολογισμούς έχουν κάνει οι υπόλοιποι. Συγκρίνοντας τα αποτελέσματα των δικών τους υπολογισμών με τα αποτελέσματα των υπολοίπων οι κόμβοι λαμβάνουν μία απόφαση για την τελική τιμή η οποία επίσης διαμοιράζεται σε όλους τους κόμβους και έτσι όλοι γνωρίζουν τις αποφάσεις των άλλων κόμβων. Σε αυτό το σημείο, έχοντας όλοι οι κόμβοι καταθέσει τις τελικές τους αποφάσεις, η τελικά συναίνεση επιτυγχάνεται μέσω πλειοψηφίας.[22]

Βασικές ιδιότητες των blockchain

Αμεταβλητότητα

Πρόκειται για μία από τις βασικότερες ιδιότητες των blockchain. Εφόσον μία συναλλαγή καταγραφεί, είναι αδύνατο να τροποποιηθεί. Με το πέρασμα του χρόνου

[22] Beginning Blockchain: A Beginner's Guide to Building Blockchain Solutions, Bikramaditya Singhal, Gautam Dhameja, and Priyansu Sekhar Panda, Apress, 2018

όλο και περισσότερα μπλοκ περιλαμβάνονται στην αλυσίδα με αποτέλεσμα η σταθερότητα να αυξάνεται αναλογικά και η σταθερότητά του, μέχρις ότου, τελικά, να γίνει πλήρως αμετάβλητο.

Ανθεκτικότητα σε παραχαράξεις

Ένα κατανεμημένο σύστημα όπου οι συναλλαγές είναι δημόσιες είναι επιρρεπές σε επιθέσεις παραχάραξης, ειδικά όταν οι συναλλαγές έχουν μεγάλη αξία. Τα συστήματα blockchain χρησιμοποιώντας κρυπτογραφικές συναρτήσεις κατακερματισμού και ψηφιακές υπογραφές, διασφαλίζουν την ασφάλεια και την προστασία απέναντι σε τέτοιου είδους επιθέσεις.

Δημοκρατικά

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. Οι συμμετέχοντες έχουν ίσα δικαιώματα και ο αποφάσεις λαμβάνονται μέσω διαδικασιών consensus.

Ανθεκτικότητα σε διπλοξόδεμα (double-spend)

Μία επίθεση διπλοξοδέματος συμβαίνει όταν κάποιος επιχειρεί να ξοδέψει το ίδιο ποσό σε περισσότερα άτομα. Στο bitcoin, η είσοδος σε μία συναλλαγή είναι έξοδος σε μία άλλη συναλλαγή όπου κάποιος έχει λάβει τουλάχιστον το ποσό το οποίο πληρώνει σε αυτή τη συναλλαγή. Συνεπώς, η ίδια είσοδος είναι αδύνατο να χρησιμοποιηθεί σε άλλη συναλλαγή.

Ο τρόπος με τον οποίο προστατεύεται ένα blockchain από τέτοιες επιθέσεις διπλοξοδέματος είναι η γνώση όλων των συναλλαγών που έχουν διεξαχθεί. Οι κόμβοι οι οποίος επικυρώνουν τις συναλλαγές, έχουν πρόσβαση σε ολόκληρο το καθολικό σε ολόκληρη την αλυσίδα μέχρι το genesis block. Έτσι, ελέγχεται αν μία συναλλαγή αποτελεί διπλοξόδεμα.

Συνεπής κατάσταση του καθολικού

Η συνέπεια και η σταθερότητα στο καθολικό διασφαλίζονται αφενός από όλες τις ιδιότητες που αναφέρθηκαν ανωτέρω κι αφετέρου από τους μηχανισμούς συναίνεσης που επίσης αναπτύχθηκαν.

Ανθεκτικότητα

Το δίκτυο πρέπει να είναι αρκετά ανθεκτικό ώστε να μπορεί να ξεπεράσει προβλήματα όπως πιθανές αστοχίες των κόμβων, τη μη διαθεσιμότητα κάποιων κόμβων σε μερικές περιπτώσεις, τις διακυμάνσεις του δικτύου και τις απορρίψεις πακέτων κλπ.

Ελεγξιμότητα

Ένα blockchain είναι από το σχεδιασμό του ελέγξιμο, καθώς αποτελεί μία αλυσίδα από μπλοκ που συνδέονται μεταξύ τους με συναρτήσεις κατακερματισμού, από το

τελευταίο μέχρι και το genesis block. Υπάρχει, ωστόσο, πάντα η ανάγκη για δυνατότητα συνεχής επιβεβαίωσης των συναλλαγών σε σύντομο χρονικό διάστημα.[23]

Bitcoin

Το bitcoin είναι ένα αποκεντρωμένο ψηφιακό νόμισμα το οποίο επιτρέπει άμεσες συναλλαγές μεταξύ οποιωνδήποτε ατόμων, οπουδήποτε στον πλανήτη. Το bitcoin χρησιμοποιεί peer-to-peer τεχνολογία για να λειτουργεί χωρίς κεντρική εξουσία, ενώ η διαχείριση των συναλλαγών και η έκδοση του «χρήματος» γίνονται συλλογικά από το δίκτυο.

Δημιουργήθηκε από ένα άγνωστο άτομο ή ομάδα ατόμων με το όνομα Satoshi Nakamoto και κυκλοφόρησε ως ανοιχτού κώδικα λογισμικό το 2009. Βασισμένο στην άποψη ότι «χρήμα» είναι οποιοδήποτε αντικείμενο ή οποιοδήποτε είδος αρχείου που χρησιμοποιείται σαν πληρωμή για αγαθά και υπηρεσίες, το bitcoin σχεδιάστηκε πάνω στην ιδέα της χρήσης κρυπτογραφίας για τη δημιουργία και την μεταφορά χρημάτων, αντί να βασίζεται στις κεντρικές αρχές ενός κράτους. Διαθέτει όλες ιδιότητες του συμβατικού νομίσματος καθώς είναι φορητό, ανθεκτικό, μπορεί να υποδιαιρεθεί, αναγνωρίζεται από κυβερνήσεις, είναι ανταλλάξιμο, δυσεύρετο και δύσκολο να παραχαραχθεί. Το Bitcoin έχει πολλές υποδιαιρέσεις, μεταξύ των οποίων η μικρότερη μονάδα μέτρησής του ονομάζεται satoshi (πήρε το όνομά της από το όνομα / ψευδώνυμο του δημιουργού του, Satoshi Nakamoto) και ισούται με 1/100.000.000 Bitcoin.

Τα bitcoin δημιουργούνται ως επιβράβευση για τη διαδικασία του mining. Κάθε συναλλαγή που γίνεται με Bitcoin περνάει από έλεγχο εγκυρότητας και έπειτα τοποθετείται σε ένα block μαζί με άλλες ολοκληρωμένες συναλλαγές. Κάθε φορά που δημιουργείται ένα νέο μπλοκ δημιουργείται αυτόματα και ένας αριθμός νέων Bitcoin τα οποία μοιράζονται σε αυτούς που θα έχουν λύσει τον αλγόριθμο ανάλογα με τη συνεισφορά του καθενός. Όσο μεγαλύτερο ποσοστό της συνολικής υπολογιστικής δύναμης διαθέσει κάποιος για τη λύση του αλγορίθμου τόσο μεγαλύτερο ποσοστό από τα καινούργια bitcoin που δημιουργούνται θα πάρει. Ο αριθμός των bitcoin που δημιουργούνται με κάθε νέο block μειώνεται πολύ ελαφρά κάθε φορά. Μέσα σε 4 χρόνια τα bitcoin που δημιουργούνται με κάθε νέο block πέφτουν στο μισό. Τα τελευταία bitcoin θα δημιουργηθούν το 2140. Τότε ο συνολικός αριθμός των bitcoin που υπάρχουν θα είναι 21 εκατομμύρια.

Οι συναλλαγές με bitcoin αποτελούνται από μία ή περισσότερες εισόδους και μία ή περισσότερες εξόδους. Όταν ένας χρήστης στέλνει bitcoins, καθορίζει μία διεύθυνση και το ποσό bitcoin που αποστέλλεται σε αυτή τη διεύθυνση είναι μία έξοδος. Για την αποφυγή διπλοξοδέματος κάθε είσοδος πρέπει να αναφέρεται σε μία προηγούμενη έξοδο στο blockchain. Η χρήση πολλαπλών εισόδων αντιστοιχεί στη χρήση πολλών νομισμάτων σε μία συναλλαγή με μετρητά. Εφόσον οι συναλλαγές μπορούν να έχουν πολλές εξόδους, οι χρήστες μπορούν να στείλουν bitcoins σε πολλούς παραλήπτες σε μία μόνο συναλλαγή. Όπως και στις συναλλαγές με μετρητά,

[23] Beginning Blockchain: A Beginner's Guide to Building Blockchain Solutions, Bikramaditya Singhal, Gautam Dhameja, and Priyansu Sekhar Panda, Apress, 2018

το άθροισμα των εισόδων (των νομισμάτων που χρησιμοποιήθηκαν για την πληρωμή), μπορεί να ξεπερνάει το ποσό των επιδιωκόμενων πληρωμών. Έτσι, σε αυτή την περίπτωση, χρησιμοποιείται μία επιπλέον έξοδος, η οποία επιστρέφει το υπολειπόμενο ποσό στον χρήστη που έκανε την πληρωμή. Οποιαδήποτε είσοδος Satoshi που δεν προορίζεται για τις εξόδους της συναλλαγής, γίνεται προμήθεια για τη συναλλαγή.

Για να χρησιμοποιήσει κανείς bitcoin, το μόνο που χρειάζεται είναι να εγκαταστήσει ένα πορτοφόλι bitcoin, και αμέσως θα αποκτήσει την πρώτη του διεύθυνση bitcoin ή διαφορετικά το δημόσιο κλειδί του. Σε συναλλαγές με bitcoin, είναι καλό να χρησιμοποιούνται περισσότερες από μία διευθύνσεις, διότι η πολλαπλή χρήση της ίδια διεύθυνσης μπορεί να βλάψει την ιδιωτικότητα και την εμπιστευτικότητα του χρήστη. Η πολλαπλή χρήση μίας διεύθυνσης σε πολλές συναλλαγές μπορεί εύκολα να οδηγήσει στην αποκάλυψη της ταυτότητας του χρήστη. Τα πορτοφόλια bitcoin είναι παρόμοια με αυτά που χρησιμοποιούνται στην πραγματική ζωή, με την άποψη ότι ο κάτοχός του έχει πρόσβαση σε αυτό και μπορεί να ξοδέψει όποτε επιθυμεί. Στον ψηφιακό κόσμο των bitcoin, τα πορτοφόλια ή οι τραπεζικοί λογαριασμού αντιπροσωπεύονται από τις διευθύνσεις.

Τα πλεονεκτήματα που προσφέρει το bitcoin στους χρήστες του μπορούν να συνοψιστούν ως εξής:

- Ταχύτητα Συναλλαγών/Διεθνής Φύση : Οι συναλλαγές σε bitcoin συμβαίνουν άμεσα και ανακοινώνονται ταυτόχρονα σε όλο το δίκτυο ανά τον πλανήτη. Αυτό δεν απαιτεί άλλες υποδομές πέρα από κάποια μορφή του δωρεάν λογισμικού σε υπολογιστή ή σε Smartphone, και σύνδεση στο διαδίκτυο.
- Εξαιρετικά Χαμηλό κόστος συναλλαγών : Το παρόν κόστος για κάθε συναλλαγή ανεξαρτήτως μεγέθους ανέρχεται περίπου στα 5 λεπτά του ευρώ, και είναι προαιρετικό, αν δεν υπάρχει βιασύνη επιβεβαίωσης της συναλλαγής. Σε ακόμα πιο σύνθετα δίκτυα υπό την σκέπη επί μέρους ελεγκτικών δικτύων το κόστος συναλλαγών/αγορών δύναται να προσεγγίσει πολύ χαμηλότερες τιμές. Το ποσό αυτό αποδίδεται αυτόματα στους χρήστες, που εκτελούν τους ελέγχους των συναλλαγών και την επιβεβαίωση της αντικειμενικότητάς του, ως αμοιβή για την επεξεργαστική ισχύ που επενδύουν στην προστασία του δικτύου από κακόβουλες επιθέσεις.
- Έλεγχος από το χρήστη/Προστασία από υφαρπαγή : Καθώς ο χρήστης είναι ο μόνος που έχει τη δυνατότητα να εκτελέσει συναλλαγές και εφόσον δεν έχει παραχωρήσει αυτό το δικαίωμα, και έχει προστατεύσει λογικά την πρόσβαση στα bitcoin του, είναι πρακτικά αδύνατο να κλαπούν ή να υφαρπαχτούν από τρίτους (εφόσον η κρυπτογράφηση δεν παραβιαστεί). Περαιτέρω προβλέψεις επιτρέπουν την δυνατότητα μεταφοράς τους μόνο υπό πολύ ορισμένες συνθήκες, όπως μόνο από ορισμένα προσυμφωνημένα μέρη ταυτόχρονα για την αποφυγή μονομερών εκθέσεων ή μόνο μετά από συγκεκριμένο χρόνο.
- Φορητότητα/αντίγραφα ασφαλείας : Ανεξάρτητα από το πλήθος τους, τα bitcoins και τα «πορτοφόλια» αποθήκευσης ή οι κωδικού πρόσβασης σε αυτά

είναι ουσιαστικά πάρα πολύ μικρά σε μέγεθος, και μπορούν να μεταφερθούν εύκολα, να καταγραφούν σε χαρτί, ακόμα και να απομνημονευτούν. Επίσης, κάτι αδύνατο για συμβατικές αξίες, μπορούν να αντιγραφούν ώστε να υπάρχουν αντίγραφα ασφαλείας σε περίπτωση καταστροφής των αρχικών. Βέβαια αν παραβιαστεί οποιοδήποτε από τα αντίγραφα, τα υπόλοιπα είναι επίσης παραβιασμένα.

- Διαφάνεια Συναλλαγών/Κανόνων : Όλες οι συναλλαγές που έχουν εκτελεστεί ποτέ στο δίκτυο είναι δημόσια διαθέσιμες και διαφανείς. Έτσι, οποιοσδήποτε μπορεί να εξετάσει οποιαδήποτε διεύθυνση και να δει τις προηγούμενες συναλλαγές που έχουν εκτελεστεί με αυτήν, το πλήθος των bitcoin που έχουν μετακινηθεί, όπως και το που έχουν σταλεί. Αυτό ισχύει για όλες τις συναλλαγές που έχουν εκτελεστεί ποτέ στο δίκτυο έως την πρώτη. Το ίδιο ακριβώς ισχύει για όλους τους κανόνες σύμφωνα με τους οποίους δουλεύει το λογισμικό και στο οποίο συναινούν οι χρήστες. Δεν υπάρχει κανένας κρυφός κανόνας μέσα στο λογισμικό, και δεν είναι δυνατόν να υπάρξει, καθώς οι χρήστες δεν θα το αποδέχονταν.

- Συναινετική Φύση χρήσης/αλλαγών : Η αλλαγή οιουδήποτε χαρακτηριστικού του λογισμικού ή των κανόνων του, έχει ουσιαστικά εφαρμογή μόνο όταν τις δεχτεί η κοινότητα που απαρτίζει το δίκτυο. Με αυτό τον τρόπο αποφεύγονται κακόβουλες αλλαγές που θα μπορούσαν να αλλάξουν θεμελιωδώς το λογισμικό (καθώς η πλειοψηφία των χρηστών θα τις αναγνωρίσει και δεν θα τις δεχτεί), αλλά και μεγάλη ευελιξία και ταχύτητα αντίδρασης σε περίπτωση εντοπισμού σφαλμάτων ή απρόβλεπτων αστοχιών κατά τη λειτουργία. Η ύπαρξη μιας παγκόσμιας, εξειδικευμένης και δραστήριας κοινότητας, που αντιμετωπίζει με επαγγελματισμό την ποιότητα του λογισμικού ενώ είναι απολύτως ανοιχτή σε σχόλια, εισηγήσεις και κριτική από όλα τα μέρη είναι ανεκτίμητη για την βιωσιμότητα του λογισμικού. Αντίστοιχου βελησνεκούς επιτυχημένα εγχειρήματα ανοιχτού λογισμικού αποτελούν το Linux όπως και το BitTorrent.

- Αποκεντρωμένη Φύση : Ένα από τα πιο σημαντικά χαρακτηριστικά του δικτύου, είναι η αποκεντρωμένη φύση του, που δεν απαιτεί καμία κεντρική αρχή ελέγχου ή επιβεβαίωσης. Κάθε κόμβος του δικτύου το ενισχύει περαιτέρω, αλλά αν προσβληθεί με κάποιο τρόπο, η λειτουργία του συνολικού δικτύου δεν επηρεάζεται ανάλογα. Η προσβολή ακόμα και πολύ μεγάλου μέρους των υπολογιστών που απαρτίζουν το δίκτυο δεν θα επηρέαζε σε σημαντικό βαθμό τη λειτουργία του. Ο μόνος τρόπος να σταματήσει να δουλεύει το δίκτυο είναι να αποκοπούν όλοι οι υπολογιστές του δικτύου μεταξύ τους, με δυο λόγια να κοπεί το διαδίκτυο σε όλο τον πλανήτη, κάτι που είναι πέρα από τις δυνάμεις οποιουδήποτε στην παρούσα. Ακόμα και τότε, με την επαναλειτουργία του διαδικτύου, το δίκτυο συνεχίζει ακριβώς εκεί που σταμάτησε. Ακόμα και μόνο ένας υπολογιστής να παραμείνει συνδεδεμένος που περιέχει το αρχείο της αλυσίδας των προηγούμενων συναλλαγών το δίκτυο λειτουργεί κανονικά.

- Υποδιαιρέσεις : Κάθε bitcoin είναι υποδιαιρέσιμο έως 8 δεκαδικά ψηφία (έως 0,00000001) που ονομάζονται Satoshi, επιτρέποντας μικρο-συναλλαγές που δεν είναι δυνατές με άλλα μέσα ή συμβατικά νομίσματα. Η προσθήκη περισσότερων ακόμα δεκαδικών επαφίεται στην συναίνεση του δικτύου αν αυτό χρειαστεί στο μέλλον.
- Μη αντιστρέψιμη φύση : Όλες οι συναλλαγές με bitcoin είναι τελικές και μη αντιστρέψιμες. Αυτό έχει το επιπλέον πλεονέκτημα προς όσους διαθέτουν προϊόντα για bitcoin ότι δεν είναι δυνατόν να ανακληθούν συναλλαγές όπως π.χ. είθισται στις απάτες με πιστωτικές κάρτες. Αυτό συνήθως δίνει επιπλέον κίνητρα σε επιχειρήσεις να προσφέρουν τα προϊόντα τους σε χαμηλότερες τιμές, εξαιτίας της άμεσης και αμετάκλητης πληρωμής. Από την άλλη, οι χρήστες που εκτελούν αγορές με bitcoin πρέπει να είναι προσεκτικοί στις επιλογές τους, καθώς ένας πάροχος προϊόντων ή υπηρεσιών που δεν έχει ιστορικό κινήσεων ή έμπιστη παρουσία στην αγορά μπορεί να μην είναι αυτό που δείχνει.
- Ιδιωτικότητα συναλλαγών : Κάθε χρήστης μπορεί να δημιουργήσει, μέσω του λογισμικού, σχεδόν απεριόριστο αριθμό διευθύνσεων μέσω τον οποίων να εκτελέσει τις συναλλαγές του. Αυτές οι διευθύνσεις είναι ψευδώνυμες, δεν έχουν δηλαδή κάποια άμεση σχέση με τα πραγματικά στοιχεία ή την τοποθεσία του χρήστη, παρόλο που έχουν αναγνωρίσιμα χαρακτηριστικά ώστε να εντοπίζονται από το δίκτυο. Με αυτό τον τρόπο μπορεί ο χρήστης να διατηρήσει την ιδιωτικότητά του απεμπλέκοντας τις συναλλαγές του από τα προσωπικά του στοιχεία. Αυτό δεν συνεπάγεται εξ' ορισμού ανωνυμία συναλλαγών καθώς όλες οι συναλλαγές δημοσιεύονται, και έστω και μία συναλλαγή να έχει γνωστό (δημόσιο) αποδέκτη, ίσως μπορεί να εξαχθεί από συμπληρωματικά στοιχεία η ταυτότητα του χρήστη. Αυτός είναι και ο κύριος λόγος για τον οποίο η χρήση bitcoins δεν ενδείκνυται για συναλλαγές παράνομων δραστηριοτήτων, ιδιαίτερα μεγάλης κλίμακας, καθώς το ίχνος των συναλλαγών όχι μόνο δεν διαγράφεται με το πέρασμα του χρόνου, αλλά παραμένει διαθέσιμο για εξέταση από όλους, για πάντα.[24]

Ethereum

Το Ethereum είναι ένα λογισμικό το οποίο εκτελείται σε ένα δίκτυο υπολογιστών και διασφαλίζει ότι τα δεδομένα και μικρά προγράμματα υπολογιστών που ονομάζονται έξυπνα συμβόλαια (smart contracts) αντιγράφονται και επεξεργάζονται σε όλους τους υπολογιστές του δικτύου, χωρίς ένα κεντρικό συντονιστή. Η ιδέα είναι δημιουργηθεί ένας ασταμάτητος, ανθεκτικός σε λογοκρισία, αυτάρκης, αποκεντρωμένος παγκόσμιος ηλεκτρονικός υπολογιστής.

Επεκτείνει τις εφαρμογές του blockchain του bitcoin, το οποίο επικυρώνει, αποθηκεύει και αντιγράφει δεδομένων συναλλαγών σε πολλούς υπολογιστές σε όλο τον κόσμο. Το Ethereum προχωράει ένα βήμα παραπέρα και εκτελεί επιπλέον κώδικα

[24] https://el.wikipedia.org/wiki/Bitcoin

ταυτόχρονα σε πολλούς υπολογιστές στον κόσμο. Αυτό που κάνει το bitcoin για διανεμημένη αποθήκευση δεδομένων, το κάνει και το Ethereum, προσθέτοντας και την υπολογιστική διαδικασία. Τα έξυπνα συμβόλαια εκτελούνται από τους συμμετέχοντες στους υπολογιστές τους χρησιμοποιώντας ένα είδος λειτουργικού συστήματος που ονομάζεται «Ethereum virtual machine».

Το Ethereum χρησιμοποιεί και αυτό blockchain , το οποίο αποτελείται από μπλοκ δεδομένων, δηλαδή συναλλαγές και έξυπνα συμβόλαια. Τα μπλοκ δημιουργούνται ή εξορύσσονται μέσω της διαδικασίας mining από κάποιους συμμετέχοντες και διαμοιράζονται στους υπόλοιπους οι οποίοι τα επικυρώνουν.

Το κυρίως δίκτυο του Ethereum είναι δημόσιο και καθένας μπορεί να το κατεβάσει ή να δημιουργήσει ένα λογισμικό για να συνδεθεί στο δίκτυο όπου μπορεί να δημιουργήσει επίσης συναλλαγές και έξυπνα συμβόλαια, να επικυρώσει και να κάνει mining τα μπλοκς, χωρίς να χρειάζεται να δημιουργήσει λογαριασμό ή να συμμετέχει ως οργανισμός[25].

Το Ethereum είναι μία δημόσια πλατφόρμα blockchain η οποία διαθέτει διαφορετική αρχιτεκτονική από αυτή του bitcoin. Διαθέτει ένα επίπεδο αφαίρεσης όπου οι συναλλαγές από διαφορετικές εφαρμογές γενικεύονται στον κώδικα του προγράμματος ο οποίος εκτελείται σε όλους τους κόμβους. Οι miners παράγουν Ether, ένα ανταλλάξιμο κρυπτονόμισμα, χάρη στο οποίο το δίκτυο παραμένει αυτάρκες. Οι εφαρμογές στην πλατφόρμα του Ethereum πληρώνουν προμήθειες συναλλαγών, τις οποίες λαμβάνουν οι miners ως επιβράβευση.

Το διαμοιραζόμενο καθολικό του Ethereum αποτελείται από μικρά αντικείμενα, τους «λογαριασμούς» οι οποίοι μπορούν να αλληλεπιδρούν μεταξύ τους μέσω ενός πλαισίου ανταλλαγής μηνυμάτων. Υπάρχουν δύο είδη λογαριασμών, οι εξωτερικοί λογαριασμοί, που ελέγχονται από ιδιωτικά κλειδιά και δεν σχετίζονται με κανενός είδους κώδικα και οι λογαριασμοί συμβάσεων, οι οποίοι ελέγχονται από τον δικό τους κώδικα, στην ουσία «ελέγχονται από τον εαυτό τους», από τον κώδικα που περιγράφεται στα έξυπνα συμβόλαιά τους.[26]

Όσον αφορά τα έξυπνα συμβόλαια, αυτά αποτελούν απλώς προγράμματα υπολογιστών και δεν έχουν καμία σχέση με νομικούς όρους. Ο κώδικάς τους, εφόσον αναπτυχθεί δεν είναι δυνατόν να τροποποιηθεί. Το αποτέλεσμα της εκτέλεσης ενός έξυπνου συμβολαίου είναι το ίδιο για όλους όσους το εκτελούν, δεδομένου του περιεχομένου της συναλλαγής που εκκίνησε την εκτέλεσή του και της κατάστασης του blockchain του Ethereum τη στιγμή της εκτέλεσης. Τα έξυπνα συμβόλαια λειτουργούν με πολύ περιορισμένο περιεχόμενο κατά την εκτέλεσή τους. Μπορούν να έχουν πρόσβαση στη δική τους κατάσταση, το περιεχόμενο της συναλλαγής που τα κάλεσε και μερικές πληροφορίες σχετικά με τα πιο πρόσφατα μπλοκ.[27]

Τα έξυπνα συμβόλαια μπορούν να χρησιμοποιηθούν για τη δημιουργία μεγάλης ποικιλίας αποκεντρωμένων εφαρμογών (DApps- Decentralized Applications), οι

[25] A Gentle Introduction to Ethereum Oct 2, 2016 - Antony Lewis
[26] Preethi Kasireddy, How does Ethereum work, anyway? Sept 27, 2017
[27] Andreas M. Antonopoulos, Gavin Wood, What is a Smart Contract? Nov 12, 2018

οποίες περιλαμβάνουν παιχνίδια, διαδικτυακά συστήματα εκλογών, οικονομικά αγαθά και πολλά άλλα ακόμη.[28]

ΙΙ. ΜΕΡΟΣ ΔΕΥΤΕΡΟ – Η συμβατότητα της τεχνολογίας blockchain με το Γενικό Κανονισμό Προστασίας Δεδομένων

Η προστασία προσωπικών δεδομένων ως θεμελιώδες δικαίωμα

Το δικαίωμα της προστασίας δεδομένων προσωπικού χαρακτήρα συνδέεται στενά με το δικαίωμα στην προστασία της ιδιωτικής ζωής, πρόκειται ωστόσο για διακριτά δικαιώματα. Αποσκοπούν αμφότερα στην προστασία παρόμοιων αξιών, δηλαδή της αυτονομίας και της ανθρώπινης αξιοπρέπειας των προσώπων, παρέχοντάς τους μια σφαίρα στην οποία μπορούν να αναπτύσσουν ελεύθερα την προσωπικότητά τους, να σκέφτονται και να διαμορφώνουν τις απόψεις τους. Αποτελούν, επομένως, βασικό προαπαιτούμενο για την άσκηση άλλων θεμελιωδών ελευθεριών, όπως της ελευθερίας της έκφρασης, της ελευθερίας του συνέρχεσθαι και του συνεταιρίζεσθαι και της θρησκευτικής ελευθερίας. Οι διαφορές τους εντοπίζονται τόσο στη διατύπωσή τους όσο και στο πεδίο εφαρμογής. Το δικαίωμα στον σεβασμό της ιδιωτικής ζωής συνίσταται σε γενική απαγόρευση των επεμβάσεων, με την επιφύλαξη ορισμένων κριτηρίων δημόσιου συμφέροντος τα οποία μπορούν να δικαιολογούν την επέμβαση σε ορισμένες περιπτώσεις. Η προστασία των δεδομένων προσωπικού χαρακτήρα γίνεται αντιληπτή ως σύγχρονο και ενεργό δικαίωμα , που απαιτεί την καθιέρωση ενός συστήματος ελέγχων και ισορροπιών για την προστασία των προσώπων κατά την επεξεργασία των δεδομένων προσωπικού χαρακτήρα που τα αφορούν. Η επεξεργασία πρέπει να είναι σύμφωνη προς τις βασικές συνιστώσες της προστασίας των δεδομένων προσωπικού χαρακτήρα, ιδίως την ανεξάρτητη εποπτεία και τον σεβασμό των δικαιωμάτων του υποκειμένου των δεδομένων[29].

Το δικαίωμα στον σεβασμό της ιδιωτική ζωής, εμφανίστηκε για πρώτη φορά στην Οικουμενική Διακήρυξη των Δικαιωμάτων του Ανθρώπου (ΟΔΔΑ), το έτος 1948, καθώς και στην Ευρωπαϊκή Σύμβαση των Δικαιωμάτων του Ανθρώπου (ΕΣΔΑ), το έτος 1950. Στην ΕΣΔΑ, ρητώς προβλέπεται ότι κάθε πρόσωπο έχει δικαίωμα στο σεβασμό της ιδιωτικής και οικογενειακής ζωής, της κατοικίας και της αλληλογραφίας του (άρθρο 8)[30]. Ωστόσο, εξαιτίας των εξελίξεων στο χώρο της Επιστήμης της Πληροφορίας, των ηλεκτρονικών υπολογιστών και του διαδικτύου, δημιουργήθηκε σύντομα η ανάγκη για θέσπιση κανόνων που θα διέπουν τη συλλογή και επεξεργασία

[28] https://docs.ethhub.io/ethereum-basics/what-is-ethereum/#what-are-smart-contracts-and-decentralized-applications

[29] Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων, Έκδοση 2018, σελ. 21

[30] ΕΣΔΑ, άρθρο 8

δεδομένων και οδήγησε στη δημιουργία μίας νέας έννοιας, του «δικαιώματος στην πληροφοριακή αυτοδιάθεση» ή «πληροφοριακή ιδιωτικότητα».

Συνεπώς, στο άρθρο 8 του Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, βλέπουμε να κατοχυρώνεται η προστασία των δεδομένων προσωπικού χαρακτήρα ως εξής: ««1. Κάθε πρόσωπο έχει δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν. 2. Η επεξεργασία αυτών των δεδομένων πρέπει να γίνεται νομίμως, για καθορισμένους σκοπούς και με βάση τη συγκατάθεση του ενδιαφερομένου ή για άλλους θεμιτούς λόγους που προβλέπονται από το νόμο. Κάθε πρόσωπο δικαιούται να έχει πρόσβαση στα συλλεγέντα δεδομένα που το αφορούν και να επιτυγχάνει τη διόρθωσή τους. 3. Ο σεβασμός των κανόνων αυτών υπόκειται στον έλεγχο ανεξάρτητης αρχής»[31].

Ομοίως, το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα περιλαμβάνεται, επίσης, στα δικαιώματα που προστατεύονται βάσει του άρθρου 8 της ΕΣΔΑ, στο οποίο κατοχυρώνεται το δικαίωμα στον σεβασμό της ιδιωτικής και οικογενειακής ζωής, της κατοικίας και της αλληλογραφίας και καθορίζονται οι προϋποθέσεις υπό τις οποίες επιτρέπονται περιορισμοί του εν λόγω δικαιώματος. Σύμφωνα με την νομολογία του Ευρωπαϊκού Δικαστηρίου Δικαιωμάτων του Ανθρώπου (ΕΔΔΑ), τα δικαιώματα που κατοχυρώνονται στο εν λόγω άρθρο δεν είναι απόλυτα δικαιώματα, αλλά υπόκεινται σε περιορισμούς όταν αλληλεπιδρούν με άλλα θεμελιώδη δικαιώματα, όπως η ελευθερία της έκφρασης και η πρόσβαση σε πληροφορίες. Στις αποφάσεις που έχει εκδώσει το ΕΔΔΑ, παρατηρείται μία προσπάθεια εξισορρόπησης των επιμέρους δικαιωμάτων, κρίνοντας και αξιολογώντας κάθε υπόθεση κατά περίπτωση.

Η προστασία δεδομένων προσωπικού χαρακτήρα προβλέπεται επίσης και στην Σύμβαση 108 (Σύμβαση για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα) του Συμβουλίου της Ευρώπης, η οποία άνοιξε προς υπογραφή το 1981. Η Σύμβαση 108 εφαρμόζεται σε κάθε επεξεργασία δεδομένων η οποία εκτελείται τόσο από τον ιδιωτικό, όσο και από τον δημόσιο τομέα, συμπεριλαμβανομένης της επεξεργασίας δεδομένων από τις δικαστικές αρχές και τις αρχές επιβολής του νόμου. Προστατεύει τα πρόσωπα από τις καταχρήσεις οι οποίες ενδέχεται να συνοδεύουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα και αποσκοπεί, ταυτόχρονα, στη ρύθμιση των διασυνοριακών ροών αυτών των δεδομένων. Όσον αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα, οι προβλεπόμενες στη Σύμβαση αρχές αφορούν, ιδίως, τη δίκαιη και νόμιμη συλλογή και αυτοματοποιημένη επεξεργασία, για συγκεκριμένους, θεμιτούς σκοπούς. Αυτό σημαίνει ότι τα δεδομένα δεν θα πρέπει να χρησιμοποιούνται για την επιδίωξη στόχων οι οποίοι δεν συνάδουν με τους σκοπούς αυτούς και δεν θα πρέπει να διατηρούνται για διάστημα μεγαλύτερο από το αναγκαίο. Οι αρχές αφορούν επίσης την ποιότητα των δεδομένων και ιδίως την ανάγκη να είναι κατάλληλα, συναφή και όχι υπερβολικά (αναλογικότητα), καθώς και ακριβή. Επιπροσθέτως της παροχής εγγυήσεων σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα και των υποχρεώσεων σε ό,τι αφορά την ασφάλεια των δεδομένων, η Σύμβαση απαγορεύει, απουσία κατάλληλων νομικών

[31] Χάρτης Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, άρθρο 8

εγγυήσεων, την επεξεργασία «ευαίσθητων» δεδομένων –όπως αυτών που αναφέρονται στη φυλή, στις πολιτικές πεποιθήσεις, στην υγεία, στη θρησκεία, στη σεξουαλική ζωή ή στο ποινικό μητρώο ενός προσώπου. Η Σύμβαση κατοχυρώνει επίσης το δικαίωμα του προσώπου να γνωρίζει ότι έχουν αποθηκευτεί πληροφορίες που το αφορούν και, εφόσον είναι αναγκαίο, να ζητεί τη διόρθωσή τους. Περιορισμοί των δικαιωμάτων που κατοχυρώνονται στη Σύμβαση μπορούν να τεθούν μόνον όταν διακυβεύεται υπέρτερο συμφέρον, όπως η εθνική ασφάλεια ή η εθνική άμυνα. Επιπλέον, η Σύμβαση προβλέπει την ελεύθερη ροή δεδομένων προσωπικού χαρακτήρα μεταξύ των συμβαλλόμενων μερών και επιβάλλει ορισμένους περιορισμούς στις ροές σε κράτη στα οποία η νομική ρύθμιση δεν προβλέπει ισοδύναμη προστασία.

Περεταίρω, η Συνθήκη για τη Λειτουργία της Ευρωπαϊκής Ένωσης, καθιερώνει με το άρθρο 16 νέα νομική βάση, η οποία παρέχει στην ΕΕ την αρμοδιότητα να νομοθετεί σε θέματα προστασίας δεδομένων: «1. Κάθε πρόσωπο έχει δικαίωμα προστασίας των δεδομένων προσωπικού χαρακτήρα που το αφορούν. 2. Το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο, αποφασίζοντας σύμφωνα με τη συνήθη νομοθετική διαδικασία, θεσπίζουν τους κανόνες σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης, καθώς και από τα κράτη μέλη κατά την άσκηση δραστηριοτήτων που εμπίπτουν στο πεδίο εφαρμογής του δικαίου της Ένωσης, και σχετικά με την ελεύθερη κυκλοφορία των δεδομένων αυτών. Η τήρηση των κανόνων αυτών υπόκειται στον έλεγχο ανεξάρτητων αρχών»[32]. Το άρθρο 16 της ΣΛΕΕ παρέχει πλέον αυτοτελή νομική βάση για μια σύγχρονη, συνολική προσέγγιση της προστασίας δεδομένων, η οποία καλύπτει όλα τα θέματα αρμοδιότητας της ΕΕ, συμπεριλαμβανομένης της αστυνομικής και δικαστικής συνεργασίας σε ποινικές υποθέσεις. Στο άρθρο 16 της ΣΛΕΕ διευκρινίζεται επίσης ότι η τήρηση των κανόνων περί προστασίας δεδομένων που εκδίδονται βάσει του εν λόγω άρθρου πρέπει να υπόκειται στον έλεγχο ανεξάρτητων εποπτικών αρχών. Το άρθρο 16 αποτέλεσε τη νομική βάση για την έγκριση της συνολικής μεταρρύθμισης των κανόνων περί προστασίας δεδομένων το 2016, δηλαδή του Γενικού Κανονισμού για την Προστασία Δεδομένων και της οδηγίας για την προστασία δεδομένων για τις αστυνομικές αρχές και τις αρχές ποινικής δικαιοσύνης.

Είναι η προστασία των δεδομένων προσωπικού χαρακτήρα απόλυτο δικαίωμα;

Το θεμελιώδες δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα βάσει του άρθρου 8 του Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, δεν είναι απόλυτο δικαίωμα, «αλλά πρέπει να λαμβάνεται υπόψη σε σχέση με τον ρόλο που επιτελεί στην κοινωνία»[33]. Επομένως, στο άρθρο 52 παράγραφος 1 του Χάρτη αναγνωρίζεται ότι επιτρέπεται η επιβολή περιορισμών στην άσκηση δικαιωμάτων, όπως των δικαιωμάτων που προβλέπονται στα άρθρα 7

[32] Συνθήκη για τη Λειτουργία της Ευρωπαϊκής Ένωσης, άρθρο 16
[33] Χάρτης Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, Άρθρο 8

και 8 του Χάρτη, υπό την προϋπόθεση ότι οι περιορισμοί αυτοί προβλέπονται από τον νόμο, σέβονται την ουσία των εν λόγω δικαιωμάτων και ελευθεριών και, τηρουμένης της αρχής της αναλογικότητας, είναι αναγκαίοι και ανταποκρίνονται πραγματικά σε στόχους γενικού συμφέροντος που αναγνωρίζει η ΕΕ ή στην ανάγκη προστασίας των δικαιωμάτων και ελευθεριών των τρίτων[34]. Ομοίως, στο σύστημα της ΕΣΔΑ, η προστασία των δεδομένων κατοχυρώνεται στο άρθρο 8 και η άσκηση του δικαιώματος αυτού μπορεί να περιορίζεται όταν είναι αναγκαίο για την επιδίωξη θεμιτού σκοπού[35].

Ένα από τα δικαιώματα που αλληλεπιδρά σε πολύ σημαντικό βαθμό με το δικαίωμα στην προστασία των δεδομένων είναι αυτό της ελευθερίας της έκφρασης. Η ελευθερία της έκφρασης κατοχυρώνεται στο άρθρο 11 του Χάρτη («Ελευθερία έκφρασης και πληροφόρησης»). Το δικαίωμα αυτό περιλαμβάνει την «ελευθερία γνώμης και την ελευθερία λήψης ή μετάδοσης πληροφοριών ή ιδεών, χωρίς την ανάμειξη δημοσίων αρχών και αδιακρίτως συνόρων». Σύμφωνα τόσο με το άρθρο 11 του Χάρτη όσο και με το άρθρο 10 της ΕΣΔΑ, η ελευθερία πληροφόρησης προστατεύει το δικαίωμα όχι μόνο της μετάδοσης αλλά και της λήψης πληροφοριών. Η σχέση μεταξύ της προστασίας των δεδομένων προσωπικού χαρακτήρα και της ελευθερίας της έκφρασης διέπεται από το άρθρο 85 του Γενικού Κανονισμού για την Προστασία Δεδομένων, με τίτλο «Επεξεργασία και ελευθερία έκφρασης και πληροφόρησης». Κατά το άρθρο αυτό, τα κράτη μέλη συμβιβάζουν το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα με το δικαίωμα στην ελευθερία της έκφρασης και πληροφόρησης. Ειδικότερα, εξαιρέσεις και παρεκκλίσεις από συγκεκριμένα κεφάλαια του Γενικού Κανονισμού για την Προστασία Δεδομένων προβλέπονται για δημοσιογραφικούς σκοπούς ή για σκοπούς πανεπιστημιακής, καλλιτεχνικής ή λογοτεχνικής έκφρασης, στο μέτρο που είναι αναγκαίες για τον συμβιβασμό του δικαιώματος στην προστασία των δεδομένων προσωπικού χαρακτήρα με την ελευθερία της έκφρασης και πληροφόρησης[36].

Περεταίρω, ο ΓΚΠΔ προκρίνει έναντι της προστασίας των προσωπικών δεδομένων και τα δικαστικώς επιδιώξιμα δικαιώματα άλλων και γενικότερα την απονομή δικαιοσύνης, το δημόσιο συμφέρον, το διευθυντικό εργοδοτικό δικαίωμα, εργασιακά, συνδικαλιστικά και κοινωνικοασφαλιστικά δικαιώματα, την εκκλησιαστική ζωή, την έρευνα και την υγεία. Ωστόσο, η νομιμοποίηση προς στάθμιση μεταξύ συνταγματικών και υπερνομοθετικών δικαιωμάτων έχει ως όριο την προστασία του πυρήνα των θεμελιωδών αυτών αξιών.

Ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR)

Από το 1995 έως το 2018, η κύρια νομική πράξη της Ευρωπαϊκής Ένωσης που αφορούσε την προστασία δεδομένων προσωπικού χαρακτήρα ήταν η οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου. Η Οδηγία για την προστασία δεδομένων θέσπισε ένα ολοκληρωμένο σύστημα για την προστασία

[34] Χάρτης Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, Άρθρο 52, παρ. 1
[35] ΕΣΔΑ, άρθρο 8
[36] Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων, Έκδοση 2018

δεδομένων στην ΕΕ, ωστόσο, όπως όλες οι οδηγίες, δεν είχε άμεση ισχύ στα κράτη μέλη και υπήρχε ανάγκη μεταφοράς της στην εθνική έννομη τάξη των κρατών μελών. Συνεπώς, η μεταφορά των διατάξεων της οδηγίας εναπόκειτο στη διακριτική ευχέρεια των νομοθετών του κάθε κράτους μέλους, δημιουργώντας έτσι σύγχυση λόγω του διαφορετικού τρόπου που επέλεξε κάθε κράτος μέλος να την μεταφέρει στην έννομη τάξη του. Αυτό είχε ως αποτέλεσμα τη θέσπιση διαφορετικών κανόνων, με ορισμούς και κανόνες που ερμηνεύτηκαν διαφορετικά από κάθε κράτος μέλος[37].

Έπειτα από πολυετείς συζητήσεις για τον εκσυγχρονισμό της νομοθεσίας προστασίας δεδομένων, οι οποίες ξεκίνησαν το 2009, δημοσιεύτηκε για πρώτη φορά το 2012 πρόταση κανονισμού, δίνοντας την εκκίνηση των διαδικασιών διαπραγμάτευσης μεταξύ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της Ευρωπαϊκής Ένωσης. Το 2016 δημοσιεύθηκε ο Γενικός Κανονισμός Προστασίας Δεδομένων (General Data Protection Regulation – GDPR), με άμεση εφαρμογή στις ευρωπαϊκές έννομες τάξεις, ο οποίος προέβλεπε διετή μεταβατική περίοδο. Με την εκκίνηση της πλήρους εφαρμογής του GDPR, στις 25-05-2018 καταργήθηκε η Οδηγία για την προστασία δεδομένων σηματοδοτώντας την έναρξη μίας νέας εποχής στην προστασία προσωπικών δεδομένων στον ευρωπαϊκό χώρο, θεσπίζοντας συνεκτικούς κανόνες σε όλη την ΕΕ και δημιουργώντας ένα περιβάλλον ασφάλειας δικαίου[38].

Ο ΓΚΠΔ διατήρησε τις βασικές αρχές και τα δικαιώματα του υποκειμένου των δεδομένων που προβλέποντο στην Οδηγία για την προστασία προσωπικών δεδομένων και θέσπισε, επιπλέον, νέες υποχρεώσεις για τους οργανισμούς, μεταξύ των οποίων η υποχρέωση εφαρμογής της προστασίας δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού, η υποχρέωση ορισμού υπευθύνου προστασίας δεδομένων σε κάποιες περιπτώσεις, το δικαίωμα στη φορητότητα και η υποχρέωση λογοδοσίας[39].

Συγκριτική μελέτη των διατάξεων του ΓΚΠΔ με τις ιδιότητες της τεχνολογίας blockchain

Στην πραγματικότητα, δεν υπάρχει μία μόνο εκδοχή της τεχνολογίας blockchain. Ο όρος αναφέρεται σε πολλές διαφορετικές μορφές διαμοιραζόμενου καθολικού που παρουσιάζουν μεγάλη ποικιλομορφία στα τεχνικά και οργανωτικά τους χαρακτηριστικά καθώς και μεγάλη πολυπλοκότητα. Συνεπώς, η συμβατότητα των διαφόρων blockchain με τον Κανονισμό μπορεί να αξιολογηθεί μόνο μέσω μιας περιπτωσιολογικής ανάλυσης, ανάλογα με τον τεχνικό σχεδιασμό και την οργάνωση κάθε σχετικής χρήσης της τεχνολογίας. Με λίγα λόγια, είναι αδύνατο να εξαχθεί το συμπέρασμα ότι κατά γενική ομολογία η τεχνολογία blockchain είναι ή όχι συμβατή με τον Κανονισμό. Ωστόσο, υπάρχει η δυνατότητα κάποιων γενικών παρατηρήσεων, όσον αφορά την μεταξύ τους αλληλεπίδραση.

---

[37] Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων , Έκδοση 2018, σελ. 35-36

[38] Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων , Έκδοση 2018, σελ. 36-37

[39] Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων , Έκδοση 2018, σελ. 37

Πεδίο εφαρμογής

Σύμφωνα με το άρθρο 2 του ΓΚΠΔ, ο κανονισμός εφαρμόζεται στην, εν όλω ή εν μέρει, αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, καθώς και στη μη αυτοματοποιημένη επεξεργασία τέτοιων δεδομένων τα οποία περιλαμβάνονται ή πρόκειται να περιληφθούν σε σύστημα αρχειοθέτησης[40]. Ο κανονισμός δεν εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα: α) στο πλαίσιο δραστηριότητας η οποία δεν εμπίπτει στο πεδίο εφαρμογής του δικαίου της Ένωσης, β) από τα κράτη μέλη κατά την άσκηση δραστηριοτήτων που εμπίπτουν στο πεδίο εφαρμογής του κεφαλαίου 2 του τίτλου V της ΣΕΕ, γ) από φυσικό πρόσωπο στο πλαίσιο αποκλειστικά προσωπικής ή οικιακής δραστηριότητας, δ) από αρμόδιες αρχές για τους σκοπούς της πρόληψης, της διερεύνησης, της ανίχνευσης ή της δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων, συμπεριλαμβανομένης της προστασίας και πρόληψης έναντι κινδύνων που απειλούν τη δημόσια ασφάλεια.

Γίνεται, επομένως, σαφές ότι θα πρέπει να πρόκειται για επεξεργασία μόνο προσωπικών δεδομένων και με σκοπό όχι αποκλειστικά οικιακό ή προσωπικό και μάλιστα κατά τέτοιον τρόπο, ώστε αυτά να περιλαμβάνονται ή να πρόκειται να περιληφθούν σε αρχείο (σύστημα αρχειοθέτησης). Υπό την έννοια αυτή, το πεδίο εφαρμογής του Κανονισμού προσδιορίζεται διττώς, καθ΄ύλην (ratio materiae) και καθ’ υποκείμενο (ratio personae)[41].

Η εξαίρεση του άρθρου 2, παρ. 2γ ΓΚΠΔ, που αφορά τη μη εφαρμογή του κανονισμού σε περίπτωση προσωπικής ή οικιακής χρήσης δεδομένων προσωπικού χαρακτήρα, είναι αμφίβολο εάν μπορεί να εφαρμοστεί, στην περίπτωση του blockchain. Αρχικά, αναφορικά με τα ιδιωτικά blockchain, η δραστηριότητα που ασκείται είναι εν γένει εμπορική ή επαγγελματική, συνεπώς δεν μπορεί να εμπίπτει στην εξαίρεση του άρθρου 2, ακόμα και αν η διάδοση των δεδομένων μπορεί να ελεγχθεί σε περίπτωση χρήσης αδειοδοτημένου blockchain. Στην περίπτωση δημοσίων ή μη αδειοδοτημένων blockchain, είναι αδύνατο να υπάρξει έλεγχος της διάδοσης των δεδομένων από το υποκείμενο των δεδομένων, ακόμα και αν το blockchain χρησιμοποιείται για αποκλειστικά ιδιωτικούς σκοπούς, καθώς η διάδοση των δεδομένων γίνεται σε αόριστο αριθμό χρηστών.

Περεταίρω, σύμφωνα με το άρθρο 3 του ΓΚΠΔ, ο Κανονισμός εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα όταν πληρούνται συγκεκριμένες προϋποθέσεις[42]. Αρχικά, ο Κανονισμός εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο των δραστηριοτήτων μιας εγκατάστασης ενός υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία στην Ένωση, ανεξάρτητα από το κατά πόσο η επεξεργασία πραγματοποιείται εντός της Ένωσης. Αυτό σημαίνει ότι όταν ένα φυσικό ή νομικό πρόσωπο, το οποίο θεωρείται υπεύθυνος επεξεργασίας ή εκτελών την επεξεργασία, είναι εγκατεστημένο στην Ευρωπαϊκή ένωση και επεξεργάζεται δεδομένα προσωπικού χαρακτήρα (είτε

[40] ΓΚΠΔ, άρθρο 2

[41] Κωνσταντίνος Ν. Χριστοδούλου, Δίκαιο προσωπικών δεδομένων, Το πεδίο εφαρμογής του δικαίου των προσωπικών δεδομένων, Νομική Βιβλιοθήκη, 2020, σελ. 23

[42] ΓΚΠΔ, άρθρο 3

αυτό γίνεται μέσω blockchain, είτε με τη χρήση άλλων μέσων), τότε εφαρμόζεται ο ΓΚΠΔ.

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα μέσω συστημάτων διαμοιραζόμενου καθολικού, είναι δυνατόν να θεωρείται υποκείμενη στον Γενικό Κανονισμό Προστασίας Δεδομένων, υπό την έννοια του εδαφικού κριτηρίου εφαρμογής του άρθρου 3 του κανονισμού. Αυτό μπορεί να συμβεί στην περίπτωση όπου ένας χειριστής blockchain παρέχει την υποδομή του, η οποία μπορεί να χαρακτηριστεί ως υπηρεσία, σε άτομα στην Ευρωπαϊκή Ένωση. Επιπλέον, όταν ένα άτομο που είναι εγκατεστημένο εκτός Ευρωπαϊκής Ένωσης, χρησιμοποιεί blockchain για να επεξεργαστεί δεδομένα προκειμένου να ελέγξει τη συμπεριφορά ατόμων που είναι εγκατεστημένα στην ΕΕ, τότε επίσης εφαρμόζεται ο Κανονισμός.

Για τον καθορισμό της Εποπτικής Αρχής Προστασίας Δεδομένων (DPA) που θα είναι αρμόδια για την εποπτεία επεξεργασίας δεδομένων που διενεργείται με blockchain, σύμφωνα με το άρθρο 56 ΓΚΠΔ, πρόκειται για την Αρχή της κύριας εγκατάστασης[43]. Στην παράγραφο 2 του ίδιου άρθρου, αναφέρεται επίσης ότι κάθε εποπτική αρχή είναι αρμόδια για την εξέταση υποβληθείσας καταγγελίας ή για την αντιμετώπιση ενδεχόμενης παραβίασης του παρόντος κανονισμού, εάν το αντικείμενο αφορά μόνο εγκατάσταση στο οικείο κράτος μέλος ή επηρεάζει ουσιαστικώς υποκείμενα των δεδομένων μόνο στο οικείο κράτος μέλος[44]. Αναφορικά με τα ιδιωτικά blockchain, η αρμόδια Αρχή είναι εκείνη συνήθως εκείνη της κύριας εγκατάστασης του υπεύθυνου επεξεργασίας, ο οποίος είναι το άτομο που έχει χορηγήσει την πρόσβαση σε κάποια συγκεκριμένη υποδομή DLT. Όσον αφορά τα δημόσια blockchain είναι δύσκολο να καθοριστεί μία κύρια εγκατάσταση, διότι ελλείπει μία κύρια οντότητα που να ελέγχει το καθολικό.

Η έννοια της επεξεργασίας προσωπικών δεδομένων κι η εφαρμογή της σε συστήματα blockchain

Ο ΓΚΠΔ ορίζει την επεξεργασία δεδομένων ως κάθε εργασία ή σειρά εργασιών που εφαρμόζεται σε προσωπικά δεδομένα, από το Δημόσιο ή νομικό πρόσωπο δημοσίου δικαίου ή ιδιωτικού δικαίου ή ένωση προσώπων ή φυσικό πρόσωπο, με ή χωρίς την χρήση αυτοματοποιημένων μεθόδων[45]. Ο κανονισμός περιλαμβάνει έναν ενδεικτικό κατάλογο των ανωτέρω εργασιών, ο οποίος περιλαμβάνει τη συλλογή, την καταχώρηση, την οργάνωση, την κατηγοριοποίηση, τη διάρθρωση, τη διατήρηση ή αποθήκευση σε οποιοδήποτε μέσο αποθήκευσης, την προσαρμογή ή μεταβολή, την ανάκτηση, την αναζήτηση πληροφοριών, τη χρήση, την κοινολόγηση με διαβίβαση, τη διάδοση ή κάθε άλλης μορφής διάθεση, τη συσχέτιση ή τον συνδυασμό, τον περιορισμό, τη διαγραφή – καταστροφή. Η υπαγωγή αυτή κάθε γνωστικής δραστηριότητας στην έννοια της επεξεργασίας τελεί υπό δύο όρους, να μην αφορά σκοπό οικιακό ή καθαρώς προσωπικό ή Εθνικής Αμύνης και να περιλαμβάνεται ή πρόκειται να περιληφθεί σε αρχείο.

[43] ΓΚΠΔ, άρθρο 56
[44] ΓΚΠΔ, άρθρο 56
[45] ΓΚΠΔ, άρθρο 4, περ. 2

Ειδοποιό γνώρισμα της επεξεργασίας αποτελεί ο σκοπός της. Ο σκοπός της επεξεργασίας είναι αυτός που ορίζει τα κατά το νόμο ανεκτά όριά της και για το λόγο αυτό πρέπει να γνωστοποιείται στο υποκείμενο μέσα σε εύλογο χρονικό διάστημα, εάν δε μεταβληθεί εκ των υστέρων, οφείλεται νέα ενημέρωση. Το ποιος είναι ο σκοπός της εργασίας ενδέχεται να μην έχει αποφασιστεί εξ αρχής ή ακόμη και να είναι αδύνατο να εξευρεθεί κατά το στάδιο της συλλογής των δεδομένων. Συνεπώς, ενδέχεται η επεξεργασία κατ' αρχάς να εξαιρείται από το πεδίο εφαρμογής του Κανονισμού αλλά όχι οριστικός και αμετακλήτως αφού δεν αποκλείεται ο αρχικός σκοπός να αλλάξει και να υπάγεται πλέον στο πεδίο εφαρμογής του Κανονισμού[46]. Το ΔΕΕ στην υπόθεση του Ευρωπαίου Επόπτη Προστασίας Δεδομένων (ΕΕΠΔ) κατά του Συμβουλίου της Ευρωπαϊκής Ένωσης[47], έκρινε ότι η διαβίβαση των δεδομένων PNR στη CBP συνιστά επεξεργασία που αφορά τη δημόσια ασφάλεια και τις δραστηριότητες του κράτους σε τομείς του ποινικού δικαίου. Κατά το Δικαστήριο, μολονότι τα δεδομένα PNR συλλέγονταν αρχικώς από τις αεροπορικές εταιρίες στο πλαίσιο δραστηριότητας διεπόμενης από το δίκαιο της Ένωσης, δηλαδή της πώλησης αεροπορικού εισιτηρίου που έδινε δικαίωμα για την παροχή υπηρεσιών, η επεξεργασία δεδομένων την οποία αφορούσε η απόφαση 2004/535, σχετικά με την ικανοποιητική προστασία των δεδομένων προσωπικού χαρακτήρα που περιλαμβάνονται στο φάκελο των επιβατών (Passenger Name Record) αεροπορικών μεταφορών ο οποίος διαβιβάζεται στο Bureau of Customs and Border Protection (Υπηρεσία Τελωνείων και Προστασίας των Συνόρων) των Ηνωμένων Πολιτειών της Αμερικής, είχε εντελώς διαφορετικό χαρακτήρα. Συγκεκριμένα, η απόφαση αυτή δεν αφορούσε επεξεργασία δεδομένων αναγκαία για την παροχή υπηρεσιών, αλλά επεξεργασία δεδομένων λογιζόμενη ως αναγκαία για την προάσπιση της δημόσιας ασφάλειας και για τους σκοπούς της επιβολής του νόμου. Συναφώς, το Δικαστήριο επισήμανε ότι το γεγονός ότι τα δεδομένα PNR είχαν συλλεγεί από ιδιωτικούς φορείς για εμπορικούς σκοπούς και ότι οι φορείς αυτοί οργάνωναν τη διαβίβασή τους σε τρίτο κράτος δεν σήμαινε ότι ήταν αδύνατο να θεωρηθεί η διαβίβαση ως επεξεργασία δεδομένων η οποία δεν εμπίπτει στο πεδίο εφαρμογής της οδηγίας 95/46/ΕΚ, η οποία βρισκόταν κατά το χρόνο αυτό σε ισχύ.

Περεταίρω το ΔΕΕ στην υπόθεση Lindqvist[48] διαπίστωσε ότι η μνεία, σε ιστοσελίδα του διαδικτύου, διαφόρων προσώπων και ο προσδιορισμός της ταυτότητάς τους είτε με το όνομά τους είτε με άλλα μέσα, για παράδειγμα με τον αριθμό τηλεφώνου τους ή με στοιχεία σχετικά με τις συνθήκες εργασίας τους και τις ασχολίες τους κατά τον ελεύθερό τους χρόνο, ισοδυναμούν με «αυτοματοποιημένη, εν όλω ή εν μέρει, επεξεργασία δεδομένων προσωπικού χαρακτήρα».

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα σε ένα σύστημα blockchain, συνίσταται στην αρχική προσθήκη δεδομένων σε ένα σύστημα κατανεμημένου καθολικού, την συνεχιζόμενη αποθήκευσή τους, καθώς και κάθε

[46] Χριστοδούλου Κ., Δίκαιο Προσωπικών Δεδομένων, Νομική βιβλιοθήκη, 2020, σελ. 39-40
[47] ΔΕΕ, C-317/04 και C-318/04, Απόφαση του Δικαστηρίου (τμήμα μείζονος συνθέσεως) της 30ής Μαΐου 2006
[48] ΔΕΕ, C-101/01, Bodil Lindqvist

περαιτέρω επεξεργασία, όπως κάθε είδους ανάλυση δεδομένων που χρησιμοποιούνται για την διαδικασία του consensus.

Δεδομένα σε blockchain

Όπως ήδη αναφέρθηκε στο κεφάλαιο Ι της παρούσας εργασίας, τα συστήματα DLT βασίζονται σε μία μέθοδο επαλήθευσης δύο βημάτων, χρησιμοποιώντας την ασύμμετρη κρυπτογραφία, ή κρυπτογραφία δημοσίου κλειδιού. Κάθε χρήστης διαθέτει ένα δημόσιο κλειδί, το οποίο μοιράζεται με τους υπόλοιπους χρήστες για να πραγματοποιήσουν συναλλαγές. Επιπλέον, κάθε χρήστης διαθέτει ένα ιδιωτικό κλειδί, το οποίο λειτουργεί κατά κάποιο τρόπο ως κωδικός και δεν πρέπει ποτέ να μοιράζεται με τους άλλους χρήστες. Και τα δύο κλειδιά συνδέονται με μία μαθηματική σχέση, με τη χρήση της οποίας το ιδιωτικό κλειδί αποκρυπτογραφεί δεδομένα που κρυπτογραφήθηκαν με το δημόσιο κλειδί. Τα δημόσια κλειδιά, κρύβουν συνεπώς την ταυτότητα του κάθε ατόμου, εκτός αν συνδέονται και με άλλα αναγνωριστικά. Το καθολικό αποθηκεύεται σε υπολογιστές, που ονομάζονται κόμβοι. Σε κάποια συστήματα, υπάρχει διαχωρισμός των κόμβων σε “πλήρεις (full)” και “ελαφρείς (lightweight)”. Σε πλήρεις κόμβους αποθηκεύεται ένα πλήρες αντίγραφο του καθολικού από το genesis block ενώ σε ελαφρείς αποθηκεύονται μόνο κάποια μέρη του καθολικού.

Σε συστήματα blockchain τα δεδομένα μπορούν να αποθηκευτούν με πολλές μορφές. Αρχικά είναι δυνατόν να αποθηκευτούν δεδομένα στο καθολικό, όπως λ.χ. ένα έγγραφο ή κάποια μορφή ψηφιακής τέχνης, ως απλό κείμενο. Ωστόσο, αυτό θα ήταν προβληματικό, γιατί σε μη αδειοδοτημένα blockchain οποιοσδήποτε μπορεί να αποκτήσει πρόσβαση σε αυτά τα δεδομένα, γεγονός που είναι αποφευκτέο από την οπτική της προστασίας της ιδιωτικότητας, ενώ επιπλέον, θα ήταν μια ακριβή λύση, εξαιτίας της περιορισμένης αποθηκευτικής δυνατότητας. Για τους λόγους αυτούς, τα δεδομένα κρυπτογραφούνται ή χρησιμοποιείται hashing πριν αποθηκευτούν στο καθολικό και δεν αποθηκεύονται ως απλό κείμενο. Στα περισσότερα συστήματα blockchain, υπάρχουν δύο είδη δεδομένων που περιλαμβάνονται στα block: 1) η επικεφαλίδα η οποία περιέχει τη χρονοσήμανση και την ταυτότητα της πηγής των δεδομένων, πχ μία διεύθυνση και το hash του προηγούμενου block και 2) το περιεχόμενο σώματος, δηλαδή μία λίστα με τις συναλλαγές.

Δεδομένα προσωπικού χαρακτήρα σε blockchain

Ως δεδομένα προσωπικού χαρακτήρα ή προσωπικά δεδομένα, νοούνται οι πληροφορίες που αφορούν ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο[49]. Στην έννοια των δεδομένων προσωπικού χαρακτήρα υπάγεται κάθε πληροφορία που αναφέρεται σε φυσικό πρόσωπο. Βασικό στοιχείο του προσωπικού δεδομένου είναι η σύνδεσή του με συγκεκριμένο πρόσωπο, έτσι ώστε να προκύπτει η ταυτότητα του τελευταίου είτε άμεσα, δηλαδή με αναφορά στο όνομά του, είτε έμμεσα δηλαδή με το συνδυασμό πρόσθετων πληροφοριών που χαρακτηρίζουν την υπόστασή του από

[49] ΓΚΠΔ άρθρο 4 περ. 1

άποψη φυσική, βιολογική, ψυχική, οικονομική, πολιτιστική, πολιτική ή κοινωνική[50]. Έτσι, προσωπικά δεδομένα μπορεί να είναι ο αριθμός δελτίου ταυτότητας, ο ΑΦΜ, ο ΑΜΚΑ, ο τηλεφωνικός αριθμός, η ηλεκτρονική διεύθυνση, το domain name ή ακόμη και η IP διεύθυνση του ηλεκτρονικού υπολογιστή, φωτογραφίες, ακτινογραφίες, τα δεδομένα γενετικής ταυτότητας, καταγεγραμμένες συνομιλίες κλπ. Μέχρι μία πληροφορία να συνδεθεί με συγκεκριμένο πρόσωπο δεν αποτελεί προσωπικό δεδομένο. Επίσης, όταν μια πληροφορία αποσυνδεθεί από ένα πρόσωπο, πχ. με ανωνυμοποίηση του δεδομένου κατά τέτοιο τρόπο ώστε να είναι αδύνατο κάποιος να συνδέσει το δεδομένο με το συγκεκριμένο υποκείμενο, παύει να είναι προσωπικό δεδομένο.

Το ΔΕΕ στην υπόθεση Patrick Breyer κατά Bundesrepublik Deutschland[51] κλήθηκε να αποφανθεί εάν η διεύθυνση IP που αποθηκεύεται από φορέα παροχής υπηρεσιών τηλεμέσων, όποτε κάποιος επισκέπτεται τον διαδικτυακό του τόπο αποτελεί ως προς εκείνον δεδομένο προσωπικού χαρακτήρα. Το Δικαστήριο επισήμανε καταρχάς ότι, για να χαρακτηριστεί ένα στοιχείο ως «δεδομένο προσωπικού χαρακτήρα» κατά το άρθρο 2, στοιχείο α΄, της οδηγίας 95/46/ΕΚ δεν απαιτείται όλες οι πληροφορίες που καθιστούν δυνατή την εξακρίβωση του εμπλεκόμενου προσώπου να βρίσκονται στη διάθεση ενός μόνον προσώπου. Το γεγονός ότι οι πρόσθετες πληροφορίες που απαιτούνται για την εξακρίβωση της ταυτότητας του χρήστη διαδικτυακού τόπου δεν βρίσκονται στη διάθεση του φορέα παροχής υπηρεσιών τηλεμέσων, αλλά του παρόχου υπηρεσιών πρόσβασης στο διαδίκτυο του χρήστη αυτού, δεν σημαίνει ότι οι δυναμικές διευθύνσεις IP που έχει αποθηκεύσει ο φορέας παροχής υπηρεσιών τηλεμέσων αποκλείεται να αποτελούν, ως προς αυτόν, δεδομένα προσωπικού χαρακτήρα κατά την έννοια του άρθρου 2, στοιχείο α΄, της οδηγίας 95/46/ΕΚ (σκέψεις 43, 44). Ως εκ τούτου, το Δικαστήριο διαπίστωσε ότι δυναμική διεύθυνση IP που αποθηκεύεται από τον φορέα παροχής υπηρεσιών τηλεμέσων κατά την επίσκεψη προσώπου σε διαδικτυακό τόπο τον οποίο ο εν λόγω φορέας καθιστά προσβάσιμο στο κοινό αποτελεί, ως προς τον φορέα αυτόν, δεδομένο προσωπικού χαρακτήρα κατά το άρθρο 2, στοιχείο α΄, της οδηγίας 95/46/ΕΚ, εφόσον έχει στη διάθεσή του νόμιμα μέσα που καθιστούν δυνατή την ταυτοποίηση του οικείου προσώπου χάρη στις πρόσθετες πληροφορίες τις οποίες έχει στη διάθεσή της, για τον τελευταίο, η εταιρία που του παρέχει υπηρεσίες πρόσβασης στο διαδίκτυο (σκέψη 49, σημείο 1 του διατακτικού).

Ο ΓΚΠΔ μπορεί να εφαρμοστεί μόνο σε δεδομένα τα οποία χαρακτηρίζονται ως δεδομένα προσωπικού χαρακτήρα. Τα ανώνυμα δεδομένα εκπίπτουν του πεδίου εφαρμογής του ΓΚΠΔ. Για να αποκλειστεί η υπαγωγή στο πεδίο εφαρμογής του Κανονισμού θα πρέπει όχι απλώς να μην συνδέονται οι πληροφορίες με κάποιο πρόσωπο, αλλά και να μην είναι δυνατή η σύνδεσή τους αυτή, δηλαδή να μην υφίσταται ούτε δυνατότητα επανονομαστικοποίησής τους[52]. Η διαδικασία ανωνυμοποίησης των δεδομένων σημαίνει ότι όλα τα αναγνωριστικά στοιχεία

[50] άρθρο 2 στοιχ. Α' Οδηγίας 95/46/ΕΚ

[51] ΔΕΕ, Υπόθεση C-582/14 Patrick Breyer κατά Bundesrepublik Deutschland

[52] Χριστοδούλου Κ., Δίκαιο προσωπικών δεδομένων, Νομική Βιβλιοθήκη, 2020, σελ. 27

απαλείφονται από ένα σύνολο δεδομένων προσωπικού χαρακτήρα έτσι ώστε το υποκείμενο των δεδομένων να μην είναι πλέον ταυτοποιήσιμο. Για να ανωνυμοποιηθούν τα δεδομένα, δεν πρέπει να παραμείνει στις πληροφορίες κανένα στοιχείο το οποίο θα μπορούσε να χρησιμοποιηθεί, με εύλογη προσπάθεια, για την εκ νέου εξακρίβωση της ταυτότητας του ενδιαφερόμενου προσώπου. Ωστόσο, τα ψευδωνυμοποιημένα δεδομένα παραμένουν δεδομένα προσωπικού χαρακτήρα, όσο καθίσταται δυνατόν να ταυτοποιηθεί κάποιο υποκείμενο, με τη χρήση κάποιου αναγνωριστικού. Στο άρθρο 4 του ΓΚΠΔ ορίζεται η ψευδωνυμοποίηση των δεδομένων ως η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο[53]. Ο ΓΚΠΔ αναγνωρίζει διάφορες χρήσεις της ψευδωνυμοποίησης ως κατάλληλου τεχνικού μέτρου για την ενίσχυση της προστασίας των δεδομένων, και αναφέρεται ιδιαιτέρως για τον σχεδιασμό και την ασφάλεια της επεξεργασίας δεδομένων. Η ψευδωνυμοποίηση αποτελεί επίσης κατάλληλη εγγύηση η οποία θα μπορούσε να χρησιμοποιηθεί για την επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπούς διαφορετικούς από εκείνους για τους οποίους αυτά συλλέχθηκαν αρχικά[54].

Δύο είδη δεδομένων σε συστήματα blockchain μπορούν να χαρακτηριστούν δεδομένα προσωπικού χαρακτήρα. Αυτά είναι τα δημόσια κλειδιά, που λειτουργούν ως αναγνωριστικά χρήστη και τα δεδομένα συναλλαγών.

Δεδομένα συναλλαγών

Τα δεδομένα που αποθηκεύονται στα blocks μπορεί να σχετίζονται με κάποιο ταυτοποιημένο ή ταυτοποίησιμο φυσικό πρόσωπο και μπορεί να είναι δεδομένα που αποκαλύπτουν κάποια συγκεκριμένη συμπεριφορά σε περιπτώσεις χρήσης Internet of Things, ψηφιακές ταυτότητες ή οικονομικά και ιατρικά δεδομένα. Τα δεδομένα αυτά τα οποία περιέχουν προσωπικές πληροφορίες διαχωρίζονται από άλλα δεδομένα, όπως τα προσωπικά κλειδιά και ανήκουν στην κατηγορία των δεδομένων συναλλαγών. Τα δεδομένα αυτά, όπως αναφέρθηκε, μπορούν να αποθηκεύονται με τρεις τρόπους: ως απλό κείμενο, σε κρυπτογραφημένη μορφή και με τη χρήση hash στην αλυσίδα των block.

Τα δεδομένα που αποθηκεύονται σε ένα blockchain ως απλό κείμενο, μπορούν να χαρακτηριστούν ως δεδομένα προσωπικού χαρακτήρα και εμπίπτουν στο πεδίο εφαρμογής του ΓΚΠΔ.

Τα κρυπτογραφημένα δεδομένα, μπορούν να γίνουν προσβάσιμα με τα κατάλληλα κλειδιά, συνεπώς δεν έχουν καταστεί πλήρως ανώνυμα. Μπορούν, για παράδειγμα, να συνδεθούν με ένα υποκείμενο δεδομένων σε περιπτώσεις που διενεργούνται συναλλαγές για αγαθά εκτός αλυσίδας ή τα κρυπτονομίσματα

[53] ΓΚΠΔ, άρθρο 4

[54] Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων , Έκδοση 2018

μετατρέπονται σε παραστατικό χρήμα. Η κρυπτογράφηση θεωρείται ως μέθοδος ψευδωνυμοποίησης, εφόσον το υποκείμενο των δεδομένων μπορεί εμμέσως να ταυτοποιηθεί με τέτοιο τρόπο ώστε να μην μπορεί να θεωρηθεί ως μέθοδος ανωνυμοποίησης. Εν κατακλείδι, τα δεδομένα που έχουν κρυπτογραφηθεί, εμπίπτουν στο πεδίο εφαρμογής του ΓΚΠΔ, ως δεδομένα προσωπικού χαρακτήρα.

Δεδομένα συναλλαγών στα οποία έχει εφαρμοστεί η μέθοδος hash, επίσης μπορούν να χαρακτηριστούν δεδομένα προσωπικού χαρακτήρα. Παρόλο που μία συνάρτηση κατακερματισμού είναι σχεδόν αδύνατο να αντιστραφεί, εξακολουθεί να παραμένει στο πεδίο εφαρμογής του Κανονισμού. Η ομάδα εργασίας του άρθρου 29 έχει υπάρξει απολύτως σαφής ότι αναγνωρίζει τις συναρτήσεις κατακερματισμού ως μία μέθοδο ψευδωνυμοποίησης. Ειδικότερα στην Γνώμη 05/2014 σχετικά με τις τεχνικές ανωνυμοποίησης αναφέρει : "...εάν το εύρος των τιμών εισόδου της συνάρτησης κατατεμαχισμού είναι γνωστό, οι τιμές μπορούν να αναπαραχθούν μέσω της συνάρτησης κατατεμαχισμού ώστε να προκύψει η ορθή τιμή για μια συγκεκριμένη καταχώριση. Για παράδειγμα, εάν σε ένα σύνολο δεδομένων εφαρμόστηκε η χρήση ψευδωνύμου με τον κατατεμαχισμό του εθνικού αριθμού αναγνώρισης, το στοιχείο αυτό μπορεί να προκύψει πολύ απλά με τον κατατεμαχισμό όλων των πιθανών τιμών εισόδου και τη σύγκριση κατόπιν του αποτελέσματος με τις αντίστοιχες τιμές στο σύνολο δεδομένων. Συνήθως, οι συναρτήσεις κατατεμαχισμού είναι σχεδιασμένες κατά τρόπο ώστε να υπολογίζονται με σχετικά μεγάλη ταχύτητα και υπόκεινται σε «επιθέσεις ωμής βίας». Μπορούν επίσης να δημιουργηθούν προϋπολογισμένοι πίνακες για τη μαζική αντιστροφή μεγάλου αριθμού τιμών τεμαχισμού. Η χρήση κρυπτογραφικής συνάρτησης κατατεμαχισμού (στην οποία μια τυχαία τιμή, γνωστή ως «salt», προστίθεται στο ιδιοχαρακτηριστικό που υποβάλλεται σε τεμαχισμό) μπορεί να μειώσει τις πιθανότητες να προκύψει η τιμή εισόδου, αλλά, παρόλα αυτά, ο υπολογισμός της αρχικής τιμής του ιδιοχαρακτηριστικού που κρύβεται πίσω από το αποτέλεσμα μιας κρυπτογραφικής συνάρτησης κατατεμαχισμού ενδέχεται να εξακολουθεί να είναι εφικτός με τη χρήση εύλογων μέσων"[55].

Το συμπέρασμα ότι τα δεδομένα συναλλαγών που αποθηκεύονται σε ένα blockchain μπορούν να εμπίπτουν στο πεδίο εφαρμογής του ΓΚΠΔ, μπορεί να καταρριφθεί στο μέλλον. Αρχικά, θεωρείται εφικτό ότι κάποιο στιγμή στο μέλλον, κάποιες κρυπτογραφικές μέθοδοι όπως η SHA-256 ή η διάδοχός της SHA-3 θα καταστούν ικανές να ανωνυμοποιούν πλήρως δεδομένα. Επιπλέον, αναπτύσσονται τεχνικές λύσεις έτσι ώστε τα δεδομένα να μην αποθηκεύονται απευθείας στο blockchain. Σύμφωνα με τον Buterin, η κρυπτογραφημένα ασφαλής συσκότιση είναι το "άγιο δισκοπότηρο" της ιδιωτικότητας στα blockchain, ωστόσο παραδέχεται ότι το εργαλείο αυτό δεν έχει αναπτυχθεί επαρκώς ώστε να χρησιμοποιηθεί[56]. Ωστόσο, υπάρχουν άλλες λύσεις που θα μπορούσαν να χρησιμοποιηθούν στη συγκεκριμένη περίπτωση. Αρχικά, τα δεδομένα προσωπικού χαρακτήρα θα μπορούσαν να αποθηκευτούν εκτός της αλυσίδας και να συνδέονται με το blockchain μόνο μέσω

[55] Ομάδα εργασίας άρθρου 29, Γνώμη 05/2014 σχετικά με τις τεχνικές ανωνυμοποίησης

[56] Vitalik Buterin, Privacy on the Blockchain *(Ethereum Blog, 15* January 2016), https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/

ενός δείκτη κατακερματισμού. Σε αυτό το σενάριο, τα δεδομένα καταγράφονται σε μία κρυπτογραφημένη και μορφοποιήσιμη βάση δεδομένων και όχι στο blockchain. Στην πραγματικότητα, αυτή τη στιγμή αναπτύσσονται τεχνικές λύσεις διαχείρισης και κυριαρχίας δεδομένων που συνδυάζουν blockchain και αποθήκευση εκτός αλυσίδας προκειμένου να δομηθεί μία πλατφόρμα διαχείρισης δεδομένων προσωπικού χαρακτήρα που επικεντρώνεται στην προστασία της ιδιωτικότητας. Τέτοιου είδους πειραματικά project αποτελούν τα Swarm[57], Storj[58] και Filecoin[59].

Δημόσια κλειδιά

Τα δημόσια κλειδιά είναι δεδομένα που δεν μπορούν να αποδοθούν σε κάποιο συγκεκριμένο υποκείμενο δεδομένων αν δεν συνδυαστούν πρώτα με συμπληρωματικές πληροφορίες, όπως ένα όνομα ή μία διεύθυνση. Έχει αποδειχθεί ότι σε συστήματα DLT, παρά τη χρήση ασύμμετρης κρυπτογραφίας, η ταυτοποίηση παραμένει δυνατή. Η σύνδεση δημοσίων κλειδιών με περαιτέρω πληροφορίες, επιτρέποντας έτσι την ταυτοποίηση, διευκολύνεται με διάφορους τρόπους, όπως με την εκούσια αποκάλυψη του δημοσίου κλειδιού από τους χρήστες προκειμένου να λάβουν κεφάλαια, με παράνομα μέσα ή σε περιπτώσεις όπου συγκεντρώνονται περαιτέρω πληροφορίες σύμφωνα με κανονισμούς, πχ. όταν εκτελούνται καθήκοντα σχετικά με την αντιμετώπιση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες[60]. Επιπλέον, στο blockchain του bitcoin, κρυπτογραφημένα δεδομένα έχουν αποδειχτεί ικανά να αποκαλύψουν ένα σύνολο πληροφοριών σχετικά με το χρήστη και την συναλλαγή που καθιστά δυνατό από τις συναλλαγές να ανιχνεύονται οι χρήστες[61]. Επίσης, ακαδημαϊκές έρευνες έχουν δείξει ότι τα δημόσια κλειδιά μπορούν να ανιχνευθούν από διευθύνσεις IP, βοηθώντας έτσι την ταυτοποποίηση[62].

Ο ΓΚΠΔ δεν αφήνει καμία αμφιβολία ως προς το ότι τα δεδομένα που μπορούν να αποδοθούν σε ένα φυσικό πρόσωπο με τη χρήση περαιτέρω πληροφοριών, μπορούν να θεωρηθούν δεδομένα προσωπικού χαρακτήρα. Για να καθοριστεί εάν ένα άτομο μπορεί να ταυτοποιηθεί μέσω ψευδωνυμοποιημένων δεδομένων, πρέπει να ληφθούν υπόψη όλα τα μέσα που είναι ευλόγως πιθανό να χρησιμοποιηθούν[63]. Δεδομένου ότι τα δημόσια κλειδιά χρησιμοποιούνται για ταυτοποιούν άτομα, καταλήγουμε στο συμπέρασμα ότι αποτελούν ένα μέσο που είναι ευλόγως πιθανό να χρησιμοποιηθεί. Το συμπέρασμα αυτό ενισχύεται από την νομολογία του ΔΕΕ(Δικαστήριο της Ευρωπαϊκής Ένωσης).Όπως και ανωτέρω

[57] https://www.ethswarm.org/
[58] https://www.storj.io/
[59] https://filecoin.io/
[60] Kelly Philipps Erb, 'IRS Tries Again To Make Coinbase Turn OverCustomer Account Data' Forbes (20 March 2017) IRS Tries Again To Make Coinbase Turn Over Customer Account Data (forbes.com)
[61] Fergal Reid and Martin Harrigan, 'An Analysis of Anonymity in the Bitcoin System', 2012 https://arxiv.org/abs/1107.4524
[62] Biryukov et al, 'Denanonymisation of Clients in Bitcoin P2P Network' (2014) https://arxiv.org/abs/1405.7418
[63] ΓΚΠΔ, αιτιολογική σκέψη 26

αναφέρθηκε, στην υπόθεση Patrick Breyer[64] εναντίον Γερμανίας, το ΔΕΕ αναγνώρισε τις δυναμικές IP διευθύνσεις ως προσωπικά δεδομένα.

Σε αντίθεση με τα δεδομένα συναλλαγών, τα δημόσια κλειδιά δεν μπορούν να μετακινηθούν εκτός αλυσίδας, καθώς αποτελούν αναπόσπαστα συστατικά της τεχνολογίας και ουσιώδες κομμάτι των μεταδεδομένων μίας συναλλαγής, τα οποία απαιτούνται για την επαλήθευσή της. Συνεπώς, λύσεις πιο προσφιλείς στον ΓΚΠΔ είναι πιο δύσκολο να βρεθούν.

Υποκείμενο Δεδομένων

Ως υποκείμενο δεδομένων και δικαιούχος της προστασίας του δικαίου της ιδιωτικής σφαίρας νοείται μόνο φυσικό πρόσωπο. Σε τεθνεώτες δεν αναγνωρίζονται προσωπικά δεδομένα, ενώ επίσης νομικά πρόσωπα δεν θεωρούνται υποκείμενα προσωπικών δεδομένων[65].

Σε ένα σύστημα blockchain, υποκείμενο δεδομένων μπορεί να θεωρηθεί οποιοδήποτε άτομο του οποίου μία τουλάχιστον κατηγορία των ανωτέρω ειδών δεδομένων, εισάγονται στο σύστημα και υφίστανται επεξεργασία.

Λογοδοσία και Υπεύθυνος επεξεργασίας δεδομένων σε Blockchain

Ο ΓΚΠΔ ορίζει τον υπεύθυνο επεξεργασίας δεδομένων ως το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα[66]. Ο κανονισμός έχει δομηθεί με βάση την αρχή ότι η ευθύνη και η λογοδοσία παραμένουν με τον υπεύθυνο επεξεργασίας, ο οποίος επιβαρύνεται με την πρακτική αποτελεσματικότητα του Ευρωπαϊκού δικαίου προστασίας δεδομένων. Ο υπεύθυνος επεξεργασίας υποχρεούται να λαμβάνει τα κατάλληλα μέτρα, τεχνικής και οργανωτικής φύσεως, έτσι ώστε να είναι σε θέση να αποδείξει ότι η επεξεργασία των δεδομένων γίνεται με βάση τις επιταγές του ΓΚΠΔ[67].

Σύμφωνα με την Ομάδα εργασίας του άρθρου 29[68], η ικανότητα να «καθορίζει τους στόχους και τον τρόπο....» μπορεί να πηγάζει από διάφορες νομικές ή/και πραγματικές περιστάσεις: μία ρητή νομική αρμοδιότητα, όταν ο νόμος διορίζει τον υπεύθυνο της επεξεργασίας ή απονέμει ένα καθήκον ή μία υποχρέωση συλλογής και επεξεργασίας ορισμένων δεδομένων· διατάξεις του κοινού δικαίου ή υφιστάμενοι παραδοσιακοί ρόλοι οι οποίοι συνεπάγονται κατά κανόνα ορισμένη ευθύνη εντός ορισμένων οργανισμών (για παράδειγμα, ο εργοδότης σε σχέση με τα δεδομένα των υπαλλήλων του)· πραγματικές περιστάσεις και άλλα στοιχεία (όπως συμβατικές σχέσεις, πραγματικός έλεγχος από ένα μέρος, προβολή έναντι των προσώπων στα οποία αναφέρονται τα δεδομένα κ.λπ.). Εάν δεν εφαρμόζεται καμία από τις κατηγορίες αυτές, ο διορισμός ενός υπευθύνου της επεξεργασίας πρέπει να

[64] ΔΕΕ, Υπόθεση C-582/14 Patrick Breyer κατά Bundesrepublik Deutschland
[65] ΓΚΠΔ, άρθρο 4, σημείο 1
[66] ΓΚΠΔ, άρθρο 4, σημείο 7
[67] ΓΚΠΔ άρθρο 24
[68] Ομάδα εργασίας άρθρου 29, Γνώμη 1/2010 σχετικά με τις έννοιες του υπεύθυνου της επεξεργασίας και τους εκτελούντες την επεξεργασία, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_el.pdf

θεωρείται «άκυρος». Πράγματι, ένας φορέας ο οποίος δεν διαθέτει ούτε νομική ούτε πραγματολογική επιρροή καθορισμού του τρόπου επεξεργασίας δεδομένων προσωπικού χαρακτήρα δεν μπορεί να θεωρηθεί υπεύθυνος της επεξεργασίας. Ο καθορισμός του «στόχου» της επεξεργασίας συνεπάγεται τον χαρακτηρισμό του (de facto) υπευθύνου της επεξεργασίας. Αντίθετα, ο καθορισμός του «τρόπου» της επεξεργασίας μπορεί να μεταβιβασθεί από τον υπεύθυνο της επεξεργασίας, όσον αφορά τεχνικά ή οργανωτικά ζητήματα. Ωστόσο, ουσιαστικά ζητήματα τα οποία είναι σημαντικά για την αξιολόγηση της νομιμότητας της επεξεργασίας –όπως τα δεδομένα που πρόκειται να υποβληθούν σε επεξεργασία, η διάρκεια της αποθήκευσης, η πρόσβαση κ.λπ.– πρέπει να καθορίζονται από τον υπεύθυνο της επεξεργασίας.

Περεταίρω, η ως άνω γνώμη αναλύει ότι προσωπική πτυχή του ορισμού παραπέμπει σε ευρύ φάσμα υποκειμένων, τα οποία μπορούν να διαδραματίσουν τον ρόλο του υπευθύνου της επεξεργασίας. Ωστόσο, στη στρατηγική οπτική της κατανομής αρμοδιοτήτων, είναι προτιμότερο να θεωρείται υπεύθυνος της επεξεργασίας η εταιρεία ή ο φορέας παρά ένα συγκεκριμένο πρόσωπο εντός της εταιρείας ή του φορέα. Η εταιρεία ή ο φορέας θα θεωρηθούν τελικά υπεύθυνοι για την επεξεργασία των δεδομένων και τις υποχρεώσεις που απορρέουν από τη νομοθεσία για την προστασία των δεδομένων, εκτός εάν υπάρχουν σαφή στοιχεία που υποδεικνύουν ότι υπεύθυνο είναι ένα φυσικό πρόσωπο, για παράδειγμα όταν ένα φυσικό πρόσωπο το οποίο εργάζεται σε μία εταιρεία ή έναν δημόσιο φορέα χρησιμοποιεί δεδομένα για δικούς του στόχους, εκτός των δραστηριοτήτων της εταιρείας.

Το ενδεχόμενο πολλαπλού ελέγχου λαμβάνει υπόψη τον αυξανόμενο αριθμό περιπτώσεων στις οποίες διαφορετικά μέρη ενεργούν ως υπεύθυνοι της επεξεργασίας. Η αξιολόγηση του κοινού αυτού ελέγχου πρέπει να αντικατοπτρίζει την αξιολόγηση του «ενιαίου» ελέγχου υιοθετώντας μία ουσιαστική και λειτουργική προσέγγιση, επικεντρωμένη στο κατά πόσον οι στόχοι και τα ουσιώδη στοιχεία του τρόπου καθορίζονται από περισσότερα του ενός μέρη. Η συμμετοχή των μερών στον καθορισμό των στόχων και του τρόπου επεξεργασίας στο πλαίσιο του κοινού ελέγχου μπορεί να προσλάβει διάφορες μορφές και δεν είναι υποχρεωτικό να είναι επιμερισμένη εξίσου. Στην ως άνω γνώμη παρέχονται πολλά παραδείγματα διάφορων ειδών και βαθμών κοινού ελέγχου. Διαφορετικοί βαθμοί ελέγχου μπορεί να συνεπάγονται διαφορετικούς βαθμούς αρμοδιότητας και ευθύνης, και, βεβαίως, δεν μπορεί να θεωρηθεί ότι υπάρχει «αλληλέγγυος και εις ολόκληρον» ευθύνη σε όλες τις περιπτώσεις. Επιπλέον, είναι πολύ πιθανό σε πολύπλοκα συστήματα με πολλαπλούς εμπλεκόμενους φορείς, η πρόσβαση στα δεδομένα προσωπικού χαρακτήρα και η άσκηση των δικαιωμάτων άλλων προσώπων στα οποία αναφέρονται τα δεδομένα να μπορεί να διασφαλισθεί επίσης σε διαφορετικά επίπεδα από διαφορετικούς φορείς[69].

Η πρόσφατη νομολογία προσφέρει μία πιο ευρεία προσέγγιση του ζητήματος του υπευθύνου επεξεργασίας και του από κοινού υπευθύνου επεξεργασίας. Στην

[69] Ομάδα εργασίας άρθρου 29, Γνώμη 1/2010 σχετικά με τις έννοιες του υπεύθυνου της επεξεργασίας και τους εκτελούντες την επεξεργασία, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_el.pdf

υπόθεση Wirtschaftsakademie Schleswig-Holstein[70] ένα ιδιωτικό εκπαιδευτικό ίδρυμα χρησιμοποίησε το Facebook για να δημιουργήσει μία fan-page. Όταν οι χρήστες επισκέπτονταν την σελίδα, ένα cookie τοποθετούνταν στους υπολογιστές τους χωρίς να ειδοποιηθούν ούτε από την Facebook ούτε από το σχολείο. Συνεπώς, η αρμόδια Αρχή Προστασίας Δεδομένων, διέταξε το σχολείο να απενεργοποιήσει την σελίδα. Στην απόφασή του το Δικαστήριο έκρινε ότι το εκπαιδευτικό ίδρυμα μπορούσε να χαρακτηριστεί από κοινού υπεύθυνος επεξεργασίας, θεωρώντας ότι "*ο διαχειριστής σελίδας στο Facebook, όπως είναι η Wirtschaftsakademie, συμμετέχει, μέσω της επιλογής των σχετικών ρυθμίσεων, η οποία αποτελεί συνάρτηση, μεταξύ άλλων, του κοινού-στόχου, καθώς και των σκοπών διαχειρίσεως ή προωθήσεως των δραστηριοτήτων του, στον καθορισμό των σκοπών και του τρόπου επεξεργασίας των δεδομένων προσωπικού χαρακτήρα των επισκεπτών της σελίδας που έχει δημιουργήσει. Για τον λόγο αυτό, ο διαχειριστής αυτός πρέπει, εν προκειμένω, να χαρακτηριστεί ως υπεύθυνος σε επίπεδο Ένωσης, από κοινού με την Facebook Ireland, για την επεξεργασία αυτή*".

Στην γνώμη του ο Γενικός Εισαγγελέας Bot[71] , δήλωσε ότι ο διαχειριστής μίας fan page υπόκειται στην αρχή που προβλέπει ότι τα προσωπικά δεδομένα των επισκεπτών της σελίδας του, θα υφίστανται επεξεργασία για τον σκοπό της σύνταξης στατιστικών επισκεψιμότητας. Αν και ένας διαχειριστής δεν είναι, φυσικά, ο σχεδιαστής των εργαλείων διορατικότητας του Facebook, θα συμμετέχει στον καθορισμό των σκοπών και των μέσων της επεξεργασίας δεδομένων των επισκεπτών της σελίδας. Επίσης τονίζει ότι η επεξεργασία των δεδομένων δεν θα συνέβαινε χωρίς την απόφαση του διαχειριστή της σελίδας να χρησιμοποιήσει αυτή την υπηρεσία.

Από αυτή την οπτική, μόνο η συμφωνία ενός φυσικού προσώπου ή μίας νομικής οντότητας για την επεξεργασία δεδομένων είναι επαρκής για να επηρεάσει τα μέσα και τους σκοπούς της επεξεργασίας και να χαρακτηριστεί υπεύθυνος επεξεργασίας. Αναλόγως, η άποψη αυτή του Γενικού Εισαγγελέα θα μπορούσε να υπονοήσει ότι οποιοσδήποτε που επιλέγει μία τεχνική υποδομή, όπως ένα Blockchain, για να επεξεργαστεί δεδομένα, θα μπορούσε να αποκτήσει την ιδιότητα του από κοινού υπευθύνου επεξεργασίας του συστήματος αυτού, ακόμα και αν ο έλεγχος που ασκεί στους σκοπούς της επεξεργασίας είναι περιορισμένος και ο έλεγχος που ασκεί σχετικά με τους τρόπους επεξεργασίας, είναι ήσσονος σημασίας.

Παρόμοια είναι η προσέγγιση του ζητήματος του από κοινού υπεύθυνου επεξεργασίας στην υπόθεση Jehovan todistajat[72], που αφορά την επεξεργασία δεδομένων από Μάρτυρες του Ιεχωβά κατά τη διαδικασία του κηρύγματος τους. Το Δικαστήριο έκρινε ότι χαρακτηρίζονται ως από κοινού υπεύθυνοι επεξεργασίας, ως φυσικά ή νομικά πρόσωπα που ασκούν επιρροή κατά την επεξεργασία δεδομένων,

[70] Case C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein κατά Wirtschaftsakademie Schleswig-Holstein GmbH, 05-06-2018, https://curia.europa.eu/juris/liste.jsf?num=C-210/16

[71] Opinion AG Bot in Case C-210/16 Wirtschafsakademie Schleswig-Holstein

[72] C-25/17, Jehovan todistajat, 10-07-2018, https://curia.europa.eu/juris/document/document.jsf?text=&docid=203822&pageIndex=0&doclang=EL&mode=lst&dir=&occ=first&part=1&cid=7408029

για δικούς τους σκοπούς και οι οποίοι συμμετέχουν, συνεπώς στον καθορισμό των σκοπών και των τρόπων επεξεργασίας.

Όμοια ήταν η κρίση του Δικαστηρίου και στην υπόθεση Fashion ID[73]. Η Fashion ID, γερμανική επιχείρηση η οποία πωλεί ενδύματα μέσω του διαδικτύου, ενσωμάτωσε στην ιστοσελίδα της την επιλογή «Μου αρέσει!» του Facebook. Η ενσωμάτωση αυτή έχει κατά τα φαινόμενα ως συνέπεια, όταν ένας χρήστης του διαδικτύου επισκέπτεται την ιστοσελίδα της Fashion ID, να διαβιβάζονται στη Facebook Ireland δεδομένα προσωπικού χαρακτήρα που τον αφορούν. Φαίνεται ότι η διαβίβαση αυτή γίνεται χωρίς ο εν λόγω χρήστης να το γνωρίζει και ανεξαρτήτως του αν είναι μέλος του Facebook ή αν έχει κάνει κλικ στην επιλογή «Μου αρέσει!». Η Verbraucherzentrale NRW, γερμανική μη κερδοσκοπική ένωση προστασίας των καταναλωτών, προσάπτει στη Fashion ID ότι διαβίβασε στη Facebook Ireland δεδομένα προσωπικού χαρακτήρα των επισκεπτών της ιστοσελίδας της, αφενός, χωρίς τη συγκατάθεσή τους και, αφετέρου, κατά παράβαση των υποχρεώσεων που προβλέπουν οι διατάξεις για την προστασία των δεδομένων προσωπικού χαρακτήρα. Το Oberlandesgericht Düsseldorf (ανώτερο περιφερειακό δικαστήριο Ντίσελντορφ, Γερμανία), το οποίο επιλήφθηκε της διαφοράς, ζήτησε από το Δικαστήριο να ερμηνεύσει διάφορες διατάξεις της προϊσχύουσας οδηγίας του 1995 για την προστασία των δεδομένων (η οποία έχει μεν εφαρμογή στην υπόθεση αυτή, αλλά καταργήθηκε και αντικαταστάθηκε από τον γενικό κανονισμό του 2016 για την προστασία των δεδομένων ο οποίος τέθηκε σε ισχύ στις 25 Μαΐου 2018). Το Δικαστήριο έκρινε ότι η Fashion ID μπορεί να θεωρηθεί υπεύθυνη, από κοινού με τη Facebook Ireland, για τις πράξεις συλλογής και ανακοίνωσης με διαβίβαση στη Facebook Ireland των επίμαχων δεδομένων, εφόσον μπορεί να γίνει δεκτό (βάσει του ελέγχου στον οποίο πρέπει να προβεί το Oberlandesgericht Düsseldorf) ότι η Fashion ID και η Facebook Ireland καθορίζουν από κοινού τους σκοπούς και τον τρόπο της επεξεργασίας ως προς τις πράξεις αυτές.

Λαμβάνοντας υπόψη την ευρεία ερμηνεία του (από κοινού) υπευθύνου επεξεργασίας, πολλοί φορείς σε ένα blockchain θα μπορούσαν να θεωρηθούν ως (από κοινού) υπεύθυνοι επεξεργασίας. Για να αναγνωριστούν οι φορείς που καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων σε μία συγκεκριμένη χρήση του blockchain, είναι σημαντικό να εξεταστεί ο λειτουργικός σχεδιασμός του blockchain.

Αρχικά, πρέπει να ερμηνευθούν «οι σκοποί» και ο «τρόπος» στα πλαίσια ενός blockchain συστήματος που επεξεργάζεται δεδομένα. Όσον αφορά τον τρόπο της επεξεργασίας δεδομένων, η πρώτη δυσκολία έγκειται στην οπτική που πρέπει να υιοθετηθεί. Στην υπολογιστική νέφους, οι πάροχοι νέφους θεωρείται ότι καθορίζουν τον τρόπο επεξεργασίας γιατί επιλέγουν το λογισμικό, το υλισμικό και τα κέντρα δεδομένων που θα χρησιμοποιηθούν. Ομοίως, τα μέρη που ασκούν επιρροή πάνω στο λογισμικό, το υλισμικό και τα κέντρα δεδομένων που θα χρησιμοποιηθούν για τη λειτουργία ενός blockchain, μπορούν να θεωρηθούν ως επιρροή ως προς τον τρόπο επεξεργασίας.

[73] C-40/17 Fashion ID GmbH & Co. KG κατά Verbraucherzentrale NRW eV, 29-07-2019, https://curia.europa.eu/juris/liste.jsf?num=C-40/17&language=EL

Καθώς τα blockchain αποτελούν διαμοιραζόμενες βάσεις δεδομένων σχεδιασμένα να ελέγχονται από διαφορετικά μέρη, πολλοί φορείς επηρεάζουν τον καθορισμό του τρόπου της επεξεργασίας. Όσον αφορά τα ιδιωτικά και αδειοδοτημένα blockchain, ο τρόπος συνήθως καθορίζεται από μία οντότητα (πχ μία εταιρία) ή μία ένωση από οντότητες. Στα δημόσια και μη αδειοδοτημένα blockchain οι διαχειριστικοί κανονισμοί επηρεάζουν τις λεπτομέρειες του τρόπου επεξεργασίας. Σε γενικές γραμμές, δεν υπάρχει μία συγκεκριμένη οντότητα που αποφασίζει σχετικά με το λειτουργικό, το υλισμικό και τα κέντρα δεδομένων. Αντιθέτως, αυτές οι αποφάσεις λαμβάνονται από πολλούς διαφορετικούς παράγοντες.

Αναφορικά με τους σκοπούς της επεξεργασίας, που αποτελούν το κυριότερο κριτήριο για την αξιολόγηση του κατά πόσο κάποιος είναι υπεύθυνος επεξεργασίας, μπορεί να απεικονισθεί με το παράδειγμα συναλλαγής ενός απλού κέρματος. Είναι προφανές ότι η μεταβίβαση της κυριότητας του κέρματος μέσω της συγκεκριμένης τεχνικής υποδομής είναι ο βασικός στόχος. Επιπλέον, μπορεί να θεωρηθεί ότι κάποιος που χρησιμοποιεί ένα σύστημα blockchain για τους ανωτέρω σκοπούς, το κάνει έχοντας ως δεύτερο στόχο τη διατήρηση ενός επ' αόριστον αναπτυσσόμενου καθολικού συναλλαγών που θα υπάρχει για πάντα εξαιτίας της ανθεκτικότητας που του προσδίδει η ιδιότητά του να αντιγράφεται.

Συνεπώς, πολλές διαφορετικές οντότητες θα μπορούσαν να είναι υπεύθυνοι ή από κοινού υπεύθυνοι επεξεργασίας δεδομένων σε ένα blockchain σύστημα. Ειδικότερα:

Πάροχοι εφαρμογών blockchain

Στις περιπτώσεις όπου το blockchain έχει σχεδιαστεί με τέτοιο τρόπο ώστε οι χρήστες να αλληλεπιδρούν απευθείας μεταξύ τους, όπως για παράδειγμα το blockchain του bitcoin, ο υπεύθυνος επεξεργασίας εντοπίζεται σε επίπεδο υποδομής του blockchain. Ωστόσο, με την εξέλιξη της τεχνολογίας και των επιχειρηματικών μοντέλων, έχουν δημιουργηθεί περιβάλλοντα που περιλαμβάνουν περισσότερα επίπεδα, όπως το επίπεδο εφαρμογής. Σε αυτές τις περιπτώσεις, εγείρεται το ερώτημα εάν οι νομικές οντότητες που καθορίζουν τον τρόπο και τους σκοπούς της επεξεργασίας μπορούν να χαρακτηριστούν υπεύθυνοι επεξεργασίας. Σύμφωνα με την Ομάδα εργασίας του άρθρου 29[74] και το ΕΣΠΔ[75], στην περίπτωση των μέσων κοινωνικής δικτύωσης, τα ίδια τα μέσα κοινωνικής δικτύωσης αποτελούν υπευθύνους επεξεργασίας, καθώς καθορίζουν τον τρόπο και τους σκοπούς της επεξεργασίας. Συνεπώς, οι πάροχοι εφαρμογών είναι υπεύθυνοι επεξεργασίας καθώς "αναπτύσσουν εφαρμογές που λειτουργούν επιπλέον εκείνων του παρόχου των υπηρεσιών κοινωνικής δικτύωσης και τις οποίες ο χρήστης αποφασίζει να χρησιμοποιήσει". Αυτό μπορεί πολύ εύκολα να παραλληλισθεί με τον τρόπο λειτουργίας εφαρμογών blockchain και καταδεικνύει ότι σε περιβάλλοντα με πολλαπλά επίπεδα είναι πιθανό να υπάρξουν πολυάριθμοι υπεύθυνοι επεξεργασίας

[74] Ομάδα εργασίας άρθρου 29, Γνώμη 5/2009 σχετικά με τις επιγραμμικές υπηρεσίες κοινωνικής δικτύωσης

[75] ΕΣΠΔ, Κατευθυντήριες γραμμές 8/2020 σχετικά με τη στόχευση χρηστών μέσων κοινωνικής δικτύωσης

ή και από κοινού υπεύθυνοι επεξεργασίας, όπου ο καθένας έχει την ευθύνη για διαφορετικά στοιχεία όσον αφορά τα δεδομένα που επεξεργάζονται. Όταν ένα υποκείμενο δεδομένων βασίζεται σε κάποιον ενδιάμεσο τρίτο, όπως για παράδειγμα έναν πάροχο πορτοφολιού κρυπτονομίσματος, τότε ο πάροχος μπορεί να θεωρηθεί επίσης υπεύθυνος επεξεργασίας, καθώς οι ενδιάμεσοι αυτοί μπορούν να παράγουν και να αποθηκεύουν δημόσια και ιδιωτικά κλειδιά και να μεταδίδουν υπογεγραμμένες συναλλαγές στο υπόλοιπο δίκτυο .

Επιπλέον, η γαλλική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, CNIL (Commission Nationale Informatique et Libertés), αναφορικά με τα έξυπνα συμβόλαια, τονίζει ότι ο προγραμματιστής που κατασκευάζει ένα λογισμικό μπορεί να είναι απλώς ένας εξωτερικός πάροχος. Ωστόσο, αν συμμετέχει ενεργά στην επεξεργασία των δεδομένων μπορεί να θεωρηθεί ως εκτελών την επεξεργασία ή και από κοινού υπεύθυνος, αναλόγως της συνεισφοράς του στον καθορισμό των σκοπών επεξεργασίας[76].

Συμπερασματικά, οι πάροχοι εφαρμογών blockchain, εφόσον συμμετέχουν στον καθορισμό των σκοπών και του τρόπου της επεξεργασίας, μπορούν να θεωρηθούν υπεύθυνοι ή από κοινού υπεύθυνοι επεξεργασίας.

Ιδιωτικά και μη αδειοδοτημένα blockchain

Όταν πρόκειται για ιδιωτικά blockchain, είναι πιθανό να εντοπιστεί μία κεντρική οντότητα, όπως για παράδειγμα μία εταιρία ή μία κοινοπραξία, που μπορεί να είναι ο υπεύθυνος επεξεργασίας δεδομένων, καθώς καθορίζει τον τρόπο και τους σκοπούς της επεξεργασίας. Ωστόσο, είναι πιθανό να εντοπιστούν και άλλοι από κοινού υπεύθυνοι, σύμφωνα με όσα αναφέρθηκαν ανωτέρω, οι οποίοι μπορεί να χρησιμοποιούν την υποδομή για διαφορετικούς, δικούς τους σκοπούς.

Ένα παράδειγμα θα μπορούσε να είναι το blockchain μιας κοινοπραξίας που έχει καθιερωθεί μεταξύ πολλών παραγόντων της ίδιας εφοδιαστικής αλυσίδας. Στην περίπτωση αυτή, το νομικό πρόσωπο που αποτελεί την κοινοπραξία είναι ένας υπεύθυνος επεξεργασίας δεδομένου ότι ασκεί σημαντικό έλεγχο αναφορικά με τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων. Επίσης, οι επιχειρήσεις που συμμετέχουν στην κοινοπραξία και χρησιμοποιούν τη συγκεκριμένη υποδομή για τους δικούς τους σκοπούς, επιτρέποντας στο σύστημα να επεξεργάζεται νέα δεδομένα, μπορούν επίσης να αποτελούν υπευθύνους επεξεργασίας.

Η CNIL έχει αναφερθεί στην περίπτωση αυτή, τονίζοντας ότι όταν μία ομάδα συλλογικά αποφασίζει να χρησιμοποιήσει ένα σύστημα διαμοιραζόμενου καθολικού για τους δικούς της σκοπούς, ο υπεύθυνος επεξεργασίας πρέπει να οριστεί εξ αρχής. Ειδικότερα δίνει δύο επιλογές: είτε τη δημιουργία ενός νέου νομικού προσώπου είτε τον καθορισμό ενός ήδη υπάρχοντος νομικού προσώπου ως υπεύθυνου επεξεργασίας. Στην περίπτωση που υπάρχουν περισσότεροι από κοινού υπεύθυνοι, οφείλουν σύμφωνα με το άρθρο 26 ΓΚΠΔ να συνάπτουν μεταξύ τους συμφωνία με την οποία θα καθορίζουν τα καθήκοντα και τις υποχρεώσεις τους. Με αυτό τον τρόπο ένα υποκείμενο δεδομένων θα είναι σε θέση να αναγνωρίζει τον υπεύθυνο

[76] https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf

επεξεργασίας και να επικοινωνήσει μαζί τους σε περίπτωση που θέλει να ασκήσει κάποιο από τα δικαιώματά του.

Δημόσια και μη αδειοδοτημένα blockchain

Όταν το υποκείμενο των δεδομένων εμπλέκεται απευθείας με το επίπεδο υποδομής του blockchain, τότε είναι απαραίτητο να καθοριστεί ο υπεύθυνος επεξεργασίας στο επίπεδο αυτό. Η ταυτότητα του υπευθύνου επεξεργασίας εξαρτάται από την οπτική που υιοθετείται. Αν προσεγγίσει κανείς το ζήτημα από μία μακρο-οικονομική οπτική, ο σκοπός της επεξεργασίας δεδομένων είναι "να παρασχεθεί η σχετική υπηρεσία", (πχ μια συναλλαγή bitcoin) συνεπώς τα μέσα της επεξεργασίας που σχετίζονται με το λογισμικό, χρησιμοποιούνται από τους κόμβους και τους miners (εξορύκτες). Από μία μικρο-οικονομική οπτική (πχ η ατομική συναλλαγή), ο σκοπός της επεξεργασίας είναι "να καταγραφεί μία συναλλαγή σε ένα blockchain" και συνεπώς ο τρόπος επεξεργασίας αφορά την επιλογή κάποιας πλατφόρμας blockchain[77].

Από όλα τα ανωτέρω συνάγεται ότι σε δημόσια και μη αδειοδοτημένα blockchain ο υπεύθυνος επεξεργασίας μπορεί να εντοπιστεί μεταξύ πολλών συμμετεχόντων, συνεπώς πρέπει να επιχειρηθεί μία κατά περίπτωση προσέγγιση του ζητήματος.

Προγραμματιστές

Αναφορικά με τους προγραμματιστές λογισμικών, αξίζει να σημειωθεί ότι όλα τα μέρη που συνεισφέρουν στην ίδρυση και τη διατήρηση ενός blockchain, είναι τα λιγότερο πιθανά να αποτελέσουν υπευθύνους επεξεργασίας. Οι προγραμματιστές μπορεί μεν να διαδραματίζουν κάποιο ρόλο στο σχεδιασμό του σχετικού λογισμικού όταν προτείνουν αναβαθμίσεις λογισμικού σε άλλους, ωστόσο δεν είναι αυτοί που αποφασίζουν εάν οι αναβαθμίσεις θα υιοθετηθούν ή όχι, ενώ επιπλέον η επιρροή τους όσον αφορά τον τρόπο της επεξεργασίας είναι πολύ περιορισμένη. Οι αναβαθμίσεις λογισμικού στην πραγματικότητα αποφασίζονται, ανάλογα πάντα με τη σχετική διοικητική δομή του blockchain, από τους miners, τους κόμβους ή από άλλους παράγοντες όπως πχ οι κάτοχοι κρυπτονομισμάτων. Ομοίως, οι προγραμματιστές έχουν περιορισμένο ρόλο στον καθορισμό των σκοπών της επεξεργασίας, καθώς σχεδόν ποτέ δεν καθιστούν μία υποδομή διαθέσιμη για χρήση σε άλλους έτσι ώστε να πραγματοποιήσουν τους δικούς του σκοπούς. Επομένως, οι προγραμματιστές είναι σχεδόν αδύνατο να θεωρηθούν υπεύθυνοι επεξεργασίας σύμφωνα με το άρθρο 26 του ΓΚΠΔ.

Miners

Οι miners είναι υπεύθυνοι για την προσθήκη πληροφοριών στο σύστημα, όταν χρησιμοποιείται σαν μέθοδος consensus ο αλγόριθμος proof-of-work. Οι miners εκτελούν τον αλγόριθμο και μπορούν να προσθέτουν δεδομένα στο διαμοιραζόμενο

[77] Bacon J et al (2018) 'Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers' 25 Richmond Journal of Law and Technology 1, 64

καθολικό και να αποθηκεύουν ένα αντίγραφο του καθολικού στους υπολογιστές τους. Στην πραγματικότητα, ασκούν μεγάλο έλεγχο αναφορικά με τον τρόπο επεξεργασίας, καθώς επιλέγουν ποια εκδοχή του πρωτοκόλλου θα εκτελέσουν. Ωστόσο, δεν ασκούν καμία επιρροή στους σκοπούς μίας συναλλαγής, επομένως δεν μπορούν να θεωρηθούν υπεύθυνοι επεξεργασίας. Στην ίδια κατεύθυνση, η CNIL κατέληξε στην κρίση ότι οι miners δεν μπορούν να είναι υπεύθυνοι επεξεργασίας[78].

Κόμβοι

Στη συνέχεια, αξίζει να εξεταστεί αν οι κόμβοι θα μπορούσαν να είναι υπεύθυνοι ή από κοινού υπεύθυνοι επεξεργασίας. Σύμφωνα με τον Michele Finck[79] οι κόμβοι , κατά γενική αρχή, δεν θα μπορούσαν να χαρακτηρισθούν ως "από κοινού υπεύθυνοι επεξεργασίας δεδομένων" σύμφωνα με το άρθρο 26, παρ. 1 του ΓΚΠΔ, καθώς δεν "καθορίζουν από κοινού τους σκοπούς και τους τρόπους της επεξεργασίας", διότι αυτό προϋποθέτει σαφή κατανομή των αρμοδιοτήτων, όπως αναφέρεται και στην αιτιολογική σκέψη 79 του Κανονισμού. Οι κόμβοι είναι ελεύθεροι να αποφασίζουν εάν θα συμμετέχουν στο μη αδειοδοτημενο καθολικό και με ποιο τρόπο (πχ εάν θα συμμετέχουν ως πλήρεις ή ελαφρείς κόμβοι). Επιπλέον, δεν καθορίζουν από κοινού την επιβολή των κανόνων, όπως απαιτείται από το άρθρο 26 του Κανονισμού, αντιθέτως το σύστημα διαμορφώνεται ανάλογα με την ανεξάρτητη συμπεριφορά των κόμβων. Καθώς ένα blockchain τροφοδοτείται από την αλληλεπίδραση των κόμβων, οι κόμβοι δεν καθορίζουν τη λειτουργικότητα της επεξεργασίας δεδομένων των άλλων κόμβων. Τα μη αδειοδοτούμενα blockchain συστήματα είναι διαμοιραζόμενα και αποκεντρωμένα peer-to-peer δίκτυα στα οποία μπορεί να συμμετέχει οποιοσδήποτε για να αποκτήσει διάδραση με άγνωστα ή μη έμπιστα τρίτα μέρη. Σε τέτοια συστήματα, είτε κανένας κόμβος δεν μπορεί να θεωρηθεί ως υπεύθυνος επεξεργασίας δεδομένων λόγω της έλλειψης ανεξάρτητου καθορισμού του τρόπου και των σκοπών της επεξεργασίας, είτε πιθανότερα, κάθε κόμβος θα μπορούσε να είναι ένας υπεύθυνος επεξεργασίας δεδομένων. Πράγματι, οι κόμβοι δεν υπόκεινται σε εξωτερικές εντολές, αποφασίζουν αυτόνομα εάν θα συμμετέχουν στην αλυσίδα ή όχι και επιδιώκουν τους δικούς σκοπούς. Συνεπώς, φαίνεται ότι στην περίπτωση αυτή, οι υποχρεώσεις του Κανονισμού θα επιβάρυναν κάθε κόμβο ξεχωριστά και τα υποκείμενα των δεδομένων θα μπορούσαν να διεκδικήσουν τα αιτήματά τους ανεξάρτητα, από κάθε κόμβο. Παράλληλα, αν λάβουμε ως δεδομένο ότι κάθε κόμβος είναι και ένας υπεύθυνος επεξεργασίας, αυτό θα μπορούσε να εγείρει σημαντικά ζητήματα. Ο ακριβής αριθμός, η τοποθεσία και η ταυτότητα των κόμβων σε ένα blockchain δεν μπορούν να καθοριστούν εύκολα. Ανάλογα με την οπτική που υιοθετείται κατά περίπτωση, οι κόμβοι λειτουργούν είτε ως παθητικοί παράγοντες που υπόκεινται σε οδηγίες λογισμικών που έχουν σχεδιαστεί από προγραμματιστές είτε ως ενεργοί συμμετέχοντες στην διαχείριση ενός blockchain. Επίσης, οι κόμβοι έχουν πρόσβαση μόνο στην κρυπτογραφημένη ή μετά από χρήση hash, εκδοχή των δεδομένων, μη έχοντας έτσι τη δυνατότητα να κάνουν αλλαγές. Επομένως, οι κόμβοι είναι αποκεντρωμένες οντότητες που δεν

[78] https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf
[79] Michele Finck, Blockchain Regulation and Governance in Europe, 2018

μπορούν να ανταποκριθούν στις απαιτήσεις του ΓΚΠΔ, καθώς η επιβολή των υποχρεώσεων στους κόμβους είναι εξαιρετικά δύσκολη. Για το blockchain του Bitcoin, υπάρχουν αυτή τη στιγμή περίπου 15139 κόμβοι σε όλο τον πλανήτη, από τους οποίους οι 1773 βρίσκονται στη Γερμανία, οι 1779 στις ΗΠΑ, ενώ στην Ελλάδα βρίσκονται 6 κόμβοι[80]. Το blockchain του Ethereum διαθέτει συνολικά 6048 κόμβους από τους οποίους 2557 στις ΗΠΑ, 811 στη Γερμανία, ενώ στη χώρα μας βρίσκονται 10[81]. Εάν κάποιος επιχειρούσε να απευθυνθεί σε κάθε έναν από αυτούς τους κόμβους, κάποιοι από τους οποίους υπάγονται σε διαφορετικές δικαιοδοσίες, αυτό θα δημιουργούσε δύο είδη προβλημάτων. Αρχικά, θα χρειαζόταν να επικοινωνήσει με ένα μεγάλο αριθμό κόμβων, οι οποίοι θα έπρεπε να υποχρεωθούν σε συμμόρφωση. Δεύτερον, αυτό μπορεί να οδηγούσε σε αναγκαστική διακοπή της λειτουργίας του λογισμικού του blockchain από όλους τους κόμβους, κάθε φορά που τα δικαιώματα που προβλέπονται από τον ΓΚΠΔ δεν μπορούν να ασκηθούν με εναλλακτικούς τρόπους. Η κατάληξη θα ήταν ένα ολόκληρο blockchain να σταματήσει τη λειτουργία του σε μία δικαιοδοσία, λόγω μη συμμόρφωσης με τα δικαιώματα ενός μοναδικού υποκειμένου δεδομένων, γεγονός που θα μπορούσε να θεωρηθεί ως δυσανάλογο. Επίσης θα ήταν ασαφές το πώς θα υπολογίζονταν τα πρόστιμα, δεδομένου ότι σύμφωνα με το άρθρο 83 του Κανονισμού αυτά υπολογίζονται βάσει του παγκόσμιου ετήσιου κύκλου εργασιών, ή το πώς οι κόμβοι θα κατέβαλαν τα ποσά των προστίμων[82].

Οι Martini και Weinzierl προτείνουν κάθε κόμβος που ξεκινά μία συναλλαγή και διαμοιράζει πληροφορίες στους άλλους κόμβους, ή που αποθηκεύει μία συναλλαγή στο δικό του αντίγραφο του καθολικού, να θεωρείται και ένας υπεύθυνος επεξεργασίας, δεδομένου ότι ο κόμβος επιδιώκει τους δικούς του σκοπούς, δηλαδή τη συμμετοχή στο δίκτυο. Με αυτό τον τρόπο ο κόμβος καταγράφει, ζητάει και αποθηκεύει δεδομένα και μπορεί να χρησιμοποιήσει τα δεδομένα που καταγράφονται στον κόμβο του[83].

Οι Bacon κλπ., θεωρούν ότι οι κόμβοι μπορούν να συγκριθούν με ένα σύστημα SWIFT, μία χρηματοοικονομική υπηρεσία η οποία διευκολύνει τις συναλλαγές οικονομικών ιδρυμάτων και επεξεργάζεται δεδομένα των πληρωτών και των αποδεκτών. Σύμφωνα με την Ομάδα εργασίας του άρθρου 29, το SWIFT μπορεί να αποτελέσει υπεύθυνο επεξεργασίας, καθώς ασκεί σημαντικό έλεγχο στην επεξεργασία δεδομένων και έχει εγκαθιδρύσει ένα κέντρο δεδομένο στις ΗΠΑ με σκοπό να διαβιβάζει δεδομένα στις αρχές των ΗΠΑ[84]. Με τον ίδιο τρόπο ένας κόμβος μπορεί να λειτουργήσει ως υπεύθυνος επεξεργασίας.

Την άποψη ότι οι κόμβοι μπορούν να αποτελέσουν από κοινού υπευθύνους επεξεργασίας, υιοθετούν οι Wirth C. και Kolain M., δεδομένου ότι έχουν κοινή

[80] https://bitnodes.io/
[81] https://www.ethernodes.org/
[82] Michele Finck, Blockchain Regulation and Governance in Europe, 2018
[83] Martini M and Weinzierl Q (2017), 'Die Blockchain-Technologie und das Recht auf Vergessenwerden' 17 *Neue Zeitschrift für Verwaltungsrecht* 1251, 1253
[84] Article 29 Working Party, Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) (WP 128) 01935/06/EN, 11

επιρροή και ελευθερία να επιλέξουν ένα συγκεκριμένο blockchain και μπορούν να τροποποιήσουν τους κανόνες του[85].

Οι Muhammad Al-Abdullah, Izzat Alsmadi, Ruwaida AlAbdullah and Bernie Farkas θεωρούν ότι ο ορισμός του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία εξαρτάται από την χρήση της τεχνολογίας blockchain ανά περίπτωση. Έτσι, εάν οι κόμβοι και οι miners, για παράδειγμα, επεξεργάζονται ελάχιστα τα δεδομένα για λογαριασμό των χρηστών σε ένα μη αδειοδοτημένο blockchain, τότε οι χρήστες θα είναι οι υπεύθυνοι επεξεργασίας ενώ οι κόμβοι και οι miners θα είναι εκτελούντες την επεξεργασία. Αυτό συμβαίνει διότι απλά εκτελούν παθητικά το λογισμικό, όπως στην περίπτωση του Bitcoin. Εάν, όμως, οι κόμβοι αποκτήσουν ένα πιο ενεργό ρόλο στην επεξεργασία των δεδομένων με βάση τους δικούς τους σκοπούς, τότε μπορούν να θεωρηθούν υπεύθυνοι επεξεργασίας, όπως στην περίπτωση του Dispatch Protocol[86].

Χρήστες

Όσον αφορά τους χρήστες ενός blockchain, αυτοί μπορεί να είναι φυσικά ή νομικά πρόσωπα τα οποία υπογράφουν και υποβάλλουν μία συναλλαγή στο blockchain. Οι χρήστες μπορούν να αποτελέσουν υπευθύνους επεξεργασίας στην περίπτωση όπου μία συναλλαγή γίνεται απευθείας από τον χρήστη, όταν αυτός απευθείας εγκαθιστά τον client που συνδέεται στο δίκτυο και στέλνει συναλλαγές σε άλλους κόμβους. Άλλη άποψη υποστηρίζει ότι οι χρήστες μπορούν να είναι υπεύθυνοι επεξεργασίας όσον αφορά τα δεδομένα που καταχωρούν στο καθολικό και εκτελούντες την επεξεργασία, όσον αφορά την αποθήκευση ενός πλήρους αντιγράφου του καθολικού στους υπολογιστές τους[87].

Η CNIL προτείνει όταν ο χρήστης είναι φυσικό πρόσωπο, να μην μπορεί να εφαρμοστεί ο ΓΚΠΔ, λόγω της εξαίρεσης του άρθρου 2 του Κανονισμού που αφορά την αποκλειστικά προσωπική ή οικιακή δραστηριότητα. Ωστόσο, η σκέψη αυτή δεν μπορεί να εφαρμοστεί όταν πρόκειται για δημόσια και μη αδειοδοτημένα blockchain, διότι τότε τα δεδομένα διαμοιράζονται με αόριστο αριθμό ατόμων. Η CNIL έχει επίσης αναγνωρίσει ότι όταν η εξαίρεση της προσωπικής ή οικιακής δραστηριότητας δεν μπορεί να εφαρμοστεί επειδή ο σκοπός της συναλλαγής είναι εμπορικός ή επαγγελματικός, οι χρήστες ενός blockchain μπορεί να είναι υπεύθυνοι επεξεργασίας. Θεωρεί ότι σε τέτοιες περιπτώσεις, οι χρήστες καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας, καθώς επιλέγουν να χρησιμοποιήσουν ένα

[85] Wirth C and Kolain M (2018), 'Privacy by BlockChain Design: A Blockchain-enabled GDPR-compliant Approach for Handling Personal Data' in Wolfgang Prinz and Peter Hoschka (eds) Proceedings of the 1st ERCIM Blockchain Workshop 2018, Reports of the European Society for Socially Embedded Technologies Privacy by BlockChain Design, 5 https://dl.eusset.eu/bitstream/20.500.12015/3159/1/blockchain2018_03.pdf

[86] Muhammad Al-Abdullah, Izzat Alsmadi, Ruwaida AlAbdullah and Bernie Farkas, Designing privacy-friendly data repositories: a framework for a blockchain that follows the GDPR, Digital Policy, Regulation And Governance

[87] European Parliament (27 November 2018), Report on Blockchain: a Forward-Looking Trade Policy (AB-0407/2018)

blockchain αντί μιας άλλης τεχνολογίας , ενώ καθορίζουν επίσης και τον μορφότυπο των δεδομένων [88].

Υπάρχει μία γενικότερη κοινή αποδοχή ότι οι χρήστες ενός blockchain θα θεωρηθούν, τουλάχιστον σε κάποιες περιπτώσεις, υπεύθυνοι επεξεργασίας δεδομένων. Διακρίνονται δύο περιπτώσεις επεξεργασίας, ανάλογα με το αν επεξεργάζονται δεδομένα άλλων χρηστών ή δικά τους.

Όσον αφορά την πρώτη περίπτωση, ένα άτομο που ξεκινάει, για παράδειγμα, μία συναλλαγή σε Bitcoin, θεωρείται υπεύθυνος επεξεργασίας των προσωπικών δεδομένων του μέρους από το οποίο αγοράζει ή στο οποίο πουλάει Bitcoin. Το άτομο αυτό καθορίζει τους σκοπούς της επεξεργασίας, την αγορά δηλαδή ή την πώληση Bitcoin, καθώς επίσης και τον τρόπο της επεξεργασίας, δηλαδή την επιλογή του blockchain του Bitcoin. Είναι δύσκολο να αγνοήσει κανείς τις αναλογίες μεταξύ των στοιχείων που περιγράφονται στην υπόθεση Wirtschaftsakademie Schleswig Holstein, όπως αναλύθηκε ανωτέρω, και κάποιων περιπτώσεων συστημάτων DLT. Όταν μία τράπεζα χρησιμοποιεί ένα σύστημα DLT για να διαχειρίζεται τα δεδομένα των πελατών της, είναι υπεύθυνος επεξεργασίας. Έτσι, ένας χρήστης, ακόμα και αν είναι φυσικό πρόσωπο, μπορεί να είναι υπεύθυνος επεξεργασίας, εφόσον επεξεργάζεται δεδομένα για τους δικούς του σκοπούς. Υπάρχει ωστόσο και η σκέψη ότι στην πραγματικότητα δεν υπάρχουν επιλογές ανάμεσα σε διάφορους παρόχους για κάποιον που επιθυμεί να πουλήσει ή να αγοράσει Bitcoin. Παρόλα αυτά, σύμφωνα με το σκεπτικό της ανωτέρω απόφασης, η ιδιότητα ενός χρήστη να επεξεργάζεται δεδομένα άλλων ατόμων, μπορεί να του προσδώσει την ιδιότητα του υπευθύνου επεξεργασίας. Ανάλογο είναι και το σκεπτικό της Ομάδας Εργασίας του άρθρου 29 στη Γνώμη υπ' αριθμ. 1/2010, όπου καταλήγει στο συμπέρασμα ότι ο χρήστης ενός μέσο κοινωνικής δικτύωσης είναι υπεύθυνος επεξεργασίας[89], αλλά και στη Γνώμη 5/2012, όπου αναφέρει ότι ο χρήστης υπολογιστικής νέφους (cloud computing) είναι ο υπεύθυνος επεξεργασίας των δεδομένων που υφίστανται επεξεργασία στο cloud, καθώς καθορίζει τον σκοπό της επεξεργασίας και αποφασίζει σχετικά με την ανάθεση της επεξεργασίας σε κάποιο εξωτερικό οργανισμό[90] . Με τον ίδιο τρόπο, όταν ένας τέτοιος οργανισμός επιλέγει ένα σύστημα DLT, θα έχει καθορίσει τον τρόπο της επεξεργασίας των προσωπικών δεδομένων, επιπροσθέτως των δικών του σκοπών επεξεργασίας και αναλόγως θα επιβαρύνεται με τις υποχρεώσεις του υπευθύνου επεξεργασίας.

Υπάρχει, ωστόσο και αντίλογος σχετικά με το κατά πόσο οι χρήστες μιας τεχνικής υποδομής ασκούν πραγματικά έλεγχο σχετικά με τους σκοπούς και τα μέσα της επεξεργασίας. Πράγματι, ο χρήστης ενός blockchain, για παράδειγμα του Bitcoin, καθορίζει μόνο το εάν μία συναλλαγή έχει δημιουργηθεί, προς ποιον και τι ποσό BTC θα μεταφερθεί. Ο σκοπός σε αυτή την περίπτωση είναι να μεταφερθούν Bitcoin και δεν μπορεί να αλλάξει από τον χρήστη. Επιπλέον ο χρήστης δεν ασκεί καμία επιρροή

[88] Commission Nationale Informatique et Libertés (September 2018), 'Premiers Éléments d'analyse de la CNIL : Blockchain

[89] Ομάδα εργασίας άρθρου 29, Γνώμη 1/2010 σχετικά με τις έννοιες του «υπευθύνου της επεξεργασίας» και του «εκτελούντος την επεξεργασία», https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_el.pdf

[90] Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing

ως προς το για πόσο καιρό θα αποθηκευτούν τα δεδομένα, ποια τρίτα μέρη θα αποκτήσουν πρόσβαση σε αυτά και πότε θα διαγραφούν[91].

Σχετικά με τη δεύτερη περίπτωση επεξεργασίας δεδομένων από χρήστες blockchain, όπως αναφέρθηκε, οι χρήστες δεν επεξεργάζονται μόνο δεδομένα άλλων ατόμων αλλά και τα δικά τους. Σύμφωνα με την CNIL, ένας χρήστης blockchain δεν μπορεί να θεωρηθεί υπεύθυνος επεξεργασίας, διότι υπάγεται στην εξαίρεση της οικιακής ή προσωπικής χρήσης. Ωστόσο, σύμφωνα με την πρόσφατη, ανωτέρω αναφερθείσα νομολογία, σε ένα δημόσιο και μη αδειοδοτημένο blockchain τα δεδομένα διαμοιράζονται σε αόριστο αριθμό ατόμων, ενώ σε ιδιωτικά blockchain δεν μπορεί επίσης να εφαρμοστεί η εξαίρεση, διότι ο σκοπός της επεξεργασίας παραμένει εμπορικός. Επιπλέον η εξαίρεση της οικιακής χρήσης δεν μπορεί να εφαρμοστεί σε κάποιον που χρησιμοποιεί ένα blockchain για αμιγώς προσωπικούς σκοπούς, καθώς η διάδοση στο δίκτυο δεν ελέγχεται από τον χρήστη. Οι χρήστες δεν αποφασίζουν ποιο πρωτόκολλο χρησιμοποιείται στο διαμοιραζόμενο καθολικό και δεν μπορούν να τροποποιήσουν τα δεδομένα που αποθηκεύονται στις αμετάβλητες βάσεις δεδομένων. Κατά τον M. Finck, εφόσον είναι αδύνατο να εφαρμοστεί η εξαίρεση της οικιακής χρήσης, τότε, με βάση το σκεπτικό της CNIL, το υποκείμενο των δεδομένων είναι ταυτόχρονα και υπεύθυνος επεξεργασίας, ως προς τα δικά του προσωπικά δεδομένα[92].

Υπάρχει λοιπόν ένα ανοιχτό ερώτημα σχετικά με το αν οι ιδιότητες του υποκειμένου των δεδομένων και του υπευθύνου επεξεργασίας μπορούν να συγκεντρωθούν στο ίδιο άτομο ταυτόχρονα και κατά πόσο αυτό θα ήταν συμβατό με τον ΓΚΠΔ. Με μία πρώτη ματιά, η ιδέα να είναι το υποκείμενο δεδομένων ταυτόχρονα και υπεύθυνος επεξεργασίας όσον αφορά τα δικά του προσωπικά δεδομένα, θα μπορούσε να θεωρηθεί ως σημάδι ενδυνάμωσης του υποκειμένου, με την έννοια ότι θα έχει την απόλυτη αυτοκυριαρχία πάνω στα δεδομένα του. Ωστόσο, με μία δεύτερη σκέψη, αυτό θα μπορούσε να οδηγήσει σε επεξεργασία δεδομένων με μικρότερη ευθύνη και λογοδοσία, καθώς το υποκείμενο των δεδομένων δεν είναι σε θέση να αντιλαμβάνεται την περιπλοκότητα της επεξεργασίας δεδομένων, ενώ μπορεί να επιβαρυνθεί με την ευθύνη αποφάσεων στην οποία δεν μπορεί να ανταποκριθεί.

Μπορούν οι υπεύθυνοι επεξεργασίας σε ένα blockchain να ανταποκριθούν στις υποχρεώσεις του ΓΚΠΔ;

Από όλα τα ανωτέρω συνάγεται το συμπέρασμα ότι σε blockchain, ο υπεύθυνος επεξεργασίας δεδομένων δεν μπορεί να καθοριστεί με ένα γενικευμένο τρόπο, αλλά μόνο εξετάζοντας την κάθε περίπτωση ξεχωριστά και λαμβάνοντας υπόψη τεχνικούς και συγκυριακούς παράγοντες. Σε ιδιωτικά και αδειοδοτημένα blockchain είναι, φυσικά, ευκολότερο να εντοπιστεί ο υπεύθυνος επεξεργασίας δεδομένων, αφού συνήθως υπάρχει ένα νομικό πρόσωπο που καθορίζει τους σκοπούς και τα μέσα της επεξεργασίας. Σε δημόσια και μη αδειοδοτημένα

[91] Buocz T et al, 2019, 'Bitcoin and the GDPR: Allocating Responsibility in Distributed Networks', Computer Law & Security Review

[92] Michele Finck, Cobwebs of control: the two imaginations of the data controller in EU law, International Data Privacy Law, 2021

blockchain, πολλοί συμμετέχοντες θα μπορούσαν να είναι υπεύθυνοι επεξεργασίας (κόμβοι, χρήστες κλπ.). Ωστόσο, κάποιοι από αυτούς, έχουν περιορισμένη επιρροή στους σκοπούς και τον τρόπο της επεξεργασίας, προκαλώντας έτσι πρόβλημα στη συμμόρφωση με τον ΓΚΠΔ, εξαιτίας του μειωμένου ελέγχου τους επάνω στα δεδομένα. Τα προβλήματα μπορεί να αφορούν την άσκηση των δικαιωμάτων των υποκείμενων των δεδομένων, όπως για παράδειγμα το δικαίωμα πρόσβασης, καθώς σε κάποιες περιπτώσεις ο συμμετέχων που θεωρείται ως υπεύθυνος επεξεργασίας μπορεί να έχει πρόσβαση μόνο σε κρυπτογραφημένα δεδομένα, ή το δικαίωμα διαγραφής, καθώς ο υπεύθυνος επεξεργασίας μπορεί να έχει περιορισμένη επιρροή πάνω στην επεξεργασία.

Η Ομάδα εργασίας του άρθρου 29 αναγνωρίζει ότι εξαιτίας των ραγδαίων τεχνολογικών εξελίξεων, ο καθορισμός του υπευθύνου επεξεργασίας γίνεται όλο και πιο δύσκολος. Για το λόγο αυτό, μπορούν να προβλεφθούν διαφορετικές περιπτώσεις υπευθύνων ή από κοινού υπευθύνων επεξεργασίας, στις οποίες υπάρχουν διάφοροι βαθμοί αυτονομίας και ευθυνών, εντοπίζοντας την ευθύνη των υπευθύνων επεξεργασίας με τέτοιο τρόπο, ώστε να επιτυγχάνεται στην πράξη η συμμόρφωση με τις επιταγές του Κανονισμού. «Εντοπίζοντας έτσι 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. Πράγματι, παράγοντες που δρουν ως από κοινού υπεύθυνοι επεξεργασίας, έχουν ένα συγκεκριμένο βαθμό ευελιξίας στο διαμοιρασμό και τον εντοπισμό της ευθύνης και των υποχρεώσεων μεταξύ τους, αρκεί να επιτυγχάνουν πλήρη συμμόρφωση[93].

Ομοίως και το ΕΣΠΔ, θεωρεί ότι 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. Ωστόσο, ανεξάρτητα από την υποχρέωση αυτή, τα υποκείμενα των δεδομένων μπορούν να επικοινωνούν με οποιονδήποτε από τους υπεύθυνους επεξεργασίας. Εν γένει, τα μέτρα και οι υποχρεώσεις που πρέπει να λαμβάνουν υπόψη τους οι από κοινού υπεύθυνοι επεξεργασίας όταν καθορίζουν τις επί μέρους ευθύνες τους περιλαμβάνουν επίσης: την ενσωμάτωση των θεμελιωδών αρχών του ΓΚΠΔ, τη νόμιμη βάση της επεξεργασίας, τα μέτρα ασφάλειας, την ενημέρωση των υποκειμένων και της αρμόδιας εποπτικής αρχής σε περίπτωση παραβίασης δεδομένων, την εκτίμηση αντικτύπου, τη χρήση εκτελούντος την επεξεργασία, τις διεθνείς διαβιβάσεις δεδομένων σε τρίτες χώρες, την συνεργασία με τα υποκείμενα των δεδομένων και τις εποπτικές αρχές[94].

[93] Γνώμη 1/2010 σχετικά με τις έννοιες του «υπευθύνου της επεξεργασίας» και του «εκτελούντος την επεξεργασία», https://ec.europa.eu/justice/article-29/documentation/opinion recommendation/files/2010/wp169_el.pdf

[94] EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR

Λαμβάνοντας, συνεπώς υπόψη τις λειτουργικές ιδιότητες της τεχνολογίας blockchain, καθίσταται εμφανές ότι η τήρηση των κανόνων λογοδοσίας όπως προβλέπεται στον ΓΚΠΔ, είναι εξαιρετικά δύσκολη, ιδιαιτέρως σε δημόσια και μη αδειοδοτημένα blockchain, όπου πολλοί από τους συμμετέχοντες στο δίκτυο μπορούν να θεωρηθούν ως από κοινού υπεύθυνοι επεξεργασίας δεδομένων.

Εκτελούντες την επεξεργασία σε blockchain

Ο εκτελών την επεξεργασία είναι το πρόσωπο το οποίο επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου επεξεργασίας. Οι δραστηριότητες που ανατίθενται στον εκτελούντα την επεξεργασία μπορεί να περιορίζονται σε πολύ συγκεκριμένο καθήκον ή πλαίσιο ή μπορεί να είναι αρκετά γενικές και συνολικές[95].

Εκτός από την περίπτωση της επεξεργασίας δεδομένων για λογαριασμό άλλων, οι εκτελούντες την επεξεργασία είναι οι ίδιοι υπεύθυνοι επεξεργασίας δεδομένων σε σχέση με την επεξεργασία που διενεργούν για δικούς τους σκοπούς, για παράδειγμα, για τη διαχείριση των υπαλλήλων, των πωλήσεων και των λογαριασμών τους.

Στη Γνώμη 1/2010 της Ομάδας εργασίας άρθρου 29 σχετικά με τις έννοιες του «υπευθύνου της επεξεργασίας» και του «εκτελούντος την επεξεργασία» [96], αναλύεται επίσης, η έννοια του εκτελούντος την επεξεργασία, του οποίου η ύπαρξη εξαρτάται από απόφαση που λαμβάνει ο υπεύθυνος της επεξεργασίας, ο οποίος μπορεί να αποφασίσει είτε να επεξεργάζεται τα δεδομένα εντός του οργανισμού του είτε να μμεταβιβάσει το σύνολο ή μέρος των δραστηριοτήτων επεξεργασίας σε εξωτερικό οργανισμό. Επομένως, δύο βασικές προϋποθέσεις για τον χαρακτηρισμό κάποιου ως εκτελούντος την επεξεργασία είναι αφενός να πρόκειται για χωριστή νομική οντότητα σε σχέση με τον υπεύθυνο της επεξεργασίας και, αφετέρου, να επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας. Η δραστηριότητα επεξεργασίας μπορεί να περιορίζεται σε ένα πολύ συγκεκριμένο καθήκον ή πλαίσιο, ή μπορεί να περιλαμβάνει κάποιον βαθμό διακριτικής ευχέρειας όσον αφορά την εξυπηρέτηση των συμφερόντων του υπευθύνου της επεξεργασίας, επιτρέποντας στον εκτελούντα την επεξεργασία να επιλέξει τα καταλληλότερα τεχνικά και οργανωτικά μέσα. Επιπλέον, ο ρόλος του εκτελούντος την επεξεργασία δεν απορρέει από τη φύση ενός παράγοντα που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα, αλλά από τις συγκεκριμένες δραστηριότητές του σε ένα συγκεκριμένο πλαίσιο και σε σχέση με συγκεκριμένα σύνολα δεδομένων ή εργασιών. Ορισμένα κριτήρια μπορεί να είναι χρήσιμα για τον καθορισμό του χαρακτηρισμού των διάφορων παραγόντων που συμμετέχουν στην επεξεργασία: το επίπεδο των προηγούμενων εντολών από τον υπεύθυνο της επεξεργασίας· η παρακολούθηση από τον υπεύθυνο της επεξεργασίας του επιπέδου της υπηρεσίας· η προβολή απέναντι στα πρόσωπα στα οποία αναφέρονται τα

[95] ΓΚΠΔ άρθρο 4 σημείο 8

[96] Γνώμη 1/2010 σχετικά με τις έννοιες του «υπευθύνου της επεξεργασίας» και του «εκτελούντος την επεξεργασία», https://ec.europa.eu/justice/article-29/documentation/opinion recommendation/files/2010/wp169_el.pdf

δεδομένα· η εμπειρογνωμοσύνη των μερών· η εξουσία αυτόνομης λήψης αποφάσεων που διαθέτουν τα διάφορα μέρη[97].

Για να καθοριστεί ποιος μπορεί να θεωρηθεί εκτελών την επεξεργασία, σύμφωνα με τον ΓΚΔΠ, σε ένα blockchain, απαιτείται, επίσης, μία περιπτωσιολογική προσέγγιση.

Σε κάποιες περιπτώσεις η ύπαρξη του εκτελούντος την επεξεργασία σε συστήματα blockchain, εντοπίζεται συνήθως όταν μία εταιρία ή μία δημόσια αρχή χρησιμοποιούν μία υποδομή blockchain που ανήκει σε κάποιον εξωτερικό πάροχο υπηρεσιών. Εάν η υποδομή χρησιμοποιείται σύμφωνα με τις επιθυμίες της εταιρίας ή της δημόσιας αρχής, καθορίζοντας έτσι τον τρόπο και τους σκοπούς της επεξεργασίας, τότε ο εξωτερικός πάροχος είναι απλώς εκτελών την επεξεργασία. Έτσι, παραδείγματα εκτελούντων την επεξεργασία μπορούν να είναι αποθήκες δεδομένων υπηρεσιών εξωτερικής ανάθεσης, πάροχοι cloud ή πάροχοι λογισμικού, πλατφόρμων ή υποδομής as a service (SaaS, PaaS, IaaS), πάροχοι υπηρεσιών διαδικτύου και εν γένει εταιρίες που προσφέρουν blockchain as a service (BaaS), πιθανότατα θα μπορούν να θεωρηθούν ως εκτελούντες την επεξεργασία.

Οι χρήστες του blockchain, μπορεί να είναι ταυτόχρονα και υπεύθυνοι επεξεργασίας, όσον αφορά τα προσωπικά δεδομένα που ανεβάζουν στο καθολικό, αλλά και εκτελούντες την επεξεργασία αναφορικά με την αποθήκευση ενός πλήρους αντιγράφου του καθολικού στους υπολογιστές τους[98].

Σύμφωνα με την CNIL, οι προγραμματιστές λογισμικού μπορεί να είναι επίσης εκτελούντες την επεξεργασία, ειδικά στην περίπτωση όπου ένας προγραμματιστής έξυπνου συμβολαίου επεξεργάζεται προσωπικά δεδομένα για λογαριασμό κάποιου υπευθύνου επεξεργασίας, προσφέροντας πχ, μία τεχνική λύση σε κάποια συγκεκριμένη εταιρία. Επιπλέον, σε περιπτώσεις που πολλές εταιρίες αποφασίζουν να εκτελέσουν από κοινού ένα blockchain για τις διαδικασίες επεξεργασίας τους, μπορούν να αποφασίσουν ότι μόνο μία εξ αυτών θα είναι ο υπεύθυνος επεξεργασίας, καθιστώντας αυτομάτως τους υπόλοιπους εκτελούντες την επεξεργασία[99].

Η απαίτηση για σύναψη σύμβασης μεταξύ υπευθύνου και εκτελούντος την επεξεργασία μπορεί να αποβεί περίπλοκη σε ένα δημόσιο και μη αδειοδοτημένο blockchain, δεδομένου του μεγάλου αριθμού των συμμετεχόντων (χρήστες, κόμβοι, miners), ειδικότερα εφόσον όλοι αυτοί οι παράγοντες δεν γνωρίζονται μεταξύ τους. Στην περίπτωση αυτή, σύμφωνα με τους Bacon J. κλπ, θα πρέπει, προκειμένου να υπάρχει συμμόρφωση με τις απαιτήσεις του Κανονισμού, κάθε φορά που κάποιος χρησιμοποιεί την εκάστοτε πλατφόρμα, να συμφωνήσει με συγκεκριμένους όρους και προϋποθέσεις που καθορίζουν τις υποχρεώσεις μεταξύ των μερών. Υπάρχει, βέβαια η δυσκολία ότι σε δημόσια και μη αδειοδοτημένα blockchain, οι προγραμματιστές είναι ίσως η μοναδική ομάδα που θα μπορούσε να το κάνει αυτό,

[97] Ομάδα εργασίας άρθρου 29, Γνώμη 1/2010 σχετικά με τις έννοιες του υπεύθυνου της επεξεργασίας και τους εκτελούντες την επεξεργασία, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_el.pdf

[98] Έκθεση σχετικά με την τεχνολογία blockchain: μια μακρόπνοη εμπορική πολιτική (2018/2085(INI) https://www.europarl.europa.eu/doceo/document/A-8-2018-0407_EL.pdf

[99] Commission Nationale Informatique et Libertés (September 2018), 'Premiers Éléments d'analyse de la CNIL : Blockchain

ωστόσο, σύμφωνα με όσα αναφέρθηκαν ανωτέρω, δεν θεωρούνται συνήθως ως υπεύθυνοι επεξεργασίας δεδομένων. Παρόλα αυτά, ίσως να αναπτύσσουν κίνητρα για να προωθήσουν τη χρήση της πλατφόρμας τους και να συνειδητοποιήσουν ότι σχεδιάζοντάς την με τέτοιο τρόπο ώστε να επιτρέπει τη συμμόρφωση, προσελκύει περισσότερους miners και χρήστες. Με αυτό τον τρόπο οι προγραμματιστές θα μπορούσαν να απαιτήσουν από τους κόμβους και τους miners να συμφωνήσουν με τους όρους και τις προϋποθέσεις, όταν κάνουν λήψη ή αναβάθμιση του λογισμικού. Αναφορικά με τους χρήστες οι οποίοι συνήθως δεν αλληλεπιδρούν άμεσα με το λογισμικό, γεγονός που θα μπορούσε να οδηγήσει σε μη αποδοχή των όρων, τρίτα μέρη, όπως πάροχοι πορτοφολιών, θα μπορούσαν να ζητήσουν από τους χρήστες να αποδεχτούν τους όρους και τις προϋποθέσεις κατά την εγγραφή τους[100].

Η εφαρμογή των θεμελιωδών αρχών της επεξεργασίας δεδομένων προσωπικού χαρακτήρα σε blockchain.

Εξετάζοντας τα επιμέρους στοιχεία των θεμελιωδών αρχών της επεξεργασίας δεδομένων, όπως περιγράφονται στο άρθρο 5 του ΓΚΠΔ, θα γίνει ανάλυση αναφορικά με τον τρόπο που συναντώνται όταν η τεχνολογία που επιλέγεται για την επεξεργασία δεδομένων είναι η τεχνολογία blockchain.

Νομιμότητα

Η επεξεργασία προσωπικών δεδομένων πρέπει να είναι σύννομη[101]. Αυτό σημαίνει ότι η επεξεργασία πρέπει να βασίζεται είτε στη συγκατάθεση του υποκειμένου των δεδομένων είτε σε άλλο νόμιμο λόγο που προβλέπεται στη νομοθεσία για την προστασία δεδομένων. Οι νόμιμοι λόγοι επεξεργασίας που προβλέπει ο ΓΚΠΔ είναι πέντε και αφορούν περιπτώσεις όπου οι επεξεργασία δεδομένων είναι αναγκαία για την εκτέλεση σύμβασης, για την εκπλήρωση καθήκοντος που εκτελείται κατά την άσκηση δημόσιας εξουσίας, για τη συμμόρφωση προς έννομη υποχρέωση, για τον σκοπό των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτοι ή για τη διασφάλιση των ζωτικών συμφερόντων του υποκειμένου των δεδομένων[102].

Αναφορικά με την συγκατάθεση που προβλέπεται στο άρθρο 6παρ. 1α του Κανονισμού[103] ως νόμιμη βάση επεξεργασίας δεδομένων προσωπικού χαρακτήρα, σε συστήματα blockchain, οι Bacon J. κλπ., προτείνουν ότι η συγκατάθεση που πρέπει να δίνεται για να επιτραπεί η επεξεργασία δεδομένων μέσω ενός DLT συστήματος μπορεί να γίνεται 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[104]. Ωστόσο, υπάρχουν κάποια ζητήματα σχετικά με την προσέγγιση αυτή. Αρχικά, το επιτρεπτό

[100] Bacon J et al (2018), 'Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers' Richmond Journal of Law and Technology

[101] ΓΚΠΔ, άρθρο 5 παρ.1 , στοιχείο α

[102] ΓΚΠΔ, άρθρο 6 παρ. 1

[103] ΓΚΠΔ, άρθρο 6 παρ. 1

[104] Bacon J et al (2018), 'Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers' Richmond Journal of Law and Technology 1, 73

της επεξεργασίας των προσωπικών δεδομένων, ακολουθεί το σύστημα opt-in, ήτοι η επεξεργασία των προσωπικών δεδομένων κατ' αρχήν απαγορεύεται, εκτός αν το ίδιο το υποκείμενο επιλέξει την εισαγωγή των δεδομένων του στην επεξεργασία[105]. Έτσι, ο ΓΚΠΔ απαιτεί η συγκατάθεση 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, δημιουργώντας έτσι ζητήματα συμμόρφωσης όταν πρόκειται για συγκατάθεση που «υπονοείται»[106]. Επιπλέον, ο Κανονισμός προβλέπει τη δυνατότητα του υποκειμένου να αποσύρει τη συγκατάθεσή του οποιαδήποτε στιγμή[107]. Όμως, 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. Συμπερασματικά, για να μπορέσει ένα blockchain να επεξεργάζεται δεδομένα νόμιμα, με βάσει το άρθρο 6 παρ. 1$^{\alpha}$ ΓΚΠΔ, πρέπει να εφαρμοστεί κάποιο εργαλείο που να επιτρέπει τη διακοπή της επεξεργασίας σε περίπτωση που το υποκείμενο επιθυμεί την άρση της συγκατάθεσης.

Επόμενη νόμιμη βάση επεξεργασίας δεδομένων είναι η εκτέλεση σύμβασης της οποίας το υποκείμενο είναι συμβαλλόμενο μέρος. Όταν ένας πάροχος υπηρεσιών όπως για παράδειγμα μια τράπεζα, χρησιμοποιεί τεχνολογία blockchain για την εκτέλεση συμβατικών της υποχρεώσεων απέναντι σε κάποιο πελάτη της, διαθέτει ακολούθως και νόμιμη βάση για την επεξεργασία δεδομένων τους. Συνεπώς, όταν ένα κατανεμημένο καθολικό χρησιμοποιείται στα πλαίσια υπαρχόντων επισήμων εμπορικών ή επαγγελματικών σκοπών, οι συμβατικές συμφωνίες μεταξύ των μερών μπορούν να αποτελούν νόμιμη βάση για την επεξεργασία των σχετικών δεδομένων προσωπικού χαρακτήρα όταν για την επεξεργασία αυτή γίνεται χρήση DLT . Επιπλέον παραδείγματα μπορούν να είναι η χρήση blockchain σε εφοδιαστική αλυσίδα ή για λογιστικούς σκοπούς μεταξύ πολλών παραγόντων.

Στη συνέχεια, στην παράγραφο 1γ του άρθρου 6 ΓΚΠΔ προβλέπεται ως νόμιμη βάση επεξεργασίας η συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας. Η επεξεργασία προσωπικών δεδομένων καθίσταται απαραίτητη σε περιπτώσεις όπως η συμμόρφωση με απαιτήσεις Know Your Customer και την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες. Έτσι, σε ένα σύστημα blockchain η διάταξη αυτή του Κανονισμού μπορεί να εφαρμόζεται σε συναλλαγές με κρυπτονομίσματα όπου απαιτείται συμμόρφωση με τις ανωτέρω αναφερθείσες απαιτήσεις ή σε περίπτωση που η επεξεργασία συγκεκριμένων μορφών προσωπικών δεδομένων απαιτούνται για τη συμμόρφωση με τις διατάξεις του φορολογικού δικαίου.

Στην παράγραφο 1δ και ε του ίδιου άρθρου αναφέρονται ως νόμιμες βάσεις επεξεργασίας η διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων

[105] Χριστοδούλου Κ., Δίκαιο Προσωπικών Δεδομένων, Νομική Βιβλιοθήκη, 2020, σελ. 71
[106] ΓΚΠΔ, άρθρο 4, περ. 11
[107] ΓΚΠΔ, άρθρο 7, παρ. 3

ή άλλου φυσικού προσώπου και η εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας. Οι περιπτώσεις αυτές είναι σχεδόν αδύνατον να υπάρξουν σε σχέση με τη χρήση blockchain για την επεξεργασία δεδομένων.

Τέλος, στην παράγραφο 2στ του άρθρου 6 ΓΚΠΔ προβλέπεται ως νόμιμη βάση η περίπτωση όπου η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί. Η εφαρμογή της διάταξης αυτής στην περίπτωση χρήσης blockchain είναι αρκετά δύσκολη. Για παράδειγμα, ένα άτομο που αγοράζει κρυπτονομίσματα μπορεί να θεωρηθεί ότι «λογικά αναμένει» ότι τα προσωπικά του δεδομένα θα υποστούν επεξεργασία που ξεφεύγει από την ίδια τη συναλλαγή. Στην πραγματικότητα όμως, το πιο πιθανό είναι ότι οι περισσότεροι χρήστες δεν γνωρίζουν ότι τα δημόσια κλειδιά τους, για παράδειγμα, αποτελούν προσωπικά δεδομένα και ότι η συναλλαγή μπορεί να αποκαλύψει πληροφορίες σχετικές με το υποκείμενο. Ωστόσο, σε ποιο βαθμό πρέπει το κριτήριο αυτό να λαμβάνεται υπόψη δεν είναι απολύτως ξεκάθαρο[108].

Αντικειμενικότητα

Κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα πρέπει να γίνεται κατά τρόπο αντικειμενικό[109]. Θα πρέπει να είναι σαφές για τα φυσικά πρόσωπα ότι δεδομένα προσωπικού χαρακτήρα που τα αφορούν συλλέγονται, χρησιμοποιούνται, λαμβάνονται υπόψη ή υποβάλλονται κατ' άλλο τρόπο σε επεξεργασία, καθώς και σε ποιο βαθμό τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται ή θα υποβληθούν σε επεξεργασία[110]. Η εφαρμογή της αρχής αυτής σε τεχνολογίες blockchain δεν φαίνεται να δημιουργεί σοβαρά προβλήματα συμμόρφωσης με τον Κανονισμό και συνεπώς δεν χρήζει περεταίρω ανάλυσης.

Διαφάνεια

Η αρχή της διαφάνειας απαιτεί οποιαδήποτε ενημέρωση που απευθύνεται στο κοινό ή στο υποκείμενο των δεδομένων να είναι συνοπτική, εύκολα προσβάσιμη και εύκολα κατανοητή και να χρησιμοποιείται σαφής και απλή διατύπωση και, επιπλέον, κατά περίπτωση, απεικόνιση[111]. Οι πληροφορίες αυτές θα μπορούσαν να παρέχονται σε ηλεκτρονική μορφή, για παράδειγμα, όταν απευθύνονται στο κοινό, μέσω ιστοσελίδας. Αυτό έχει ιδιαίτερη σημασία σε περιπτώσεις στις οποίες η πληθώρα των συμμετεχόντων και η πολυπλοκότητα των χρησιμοποιούμενων τεχνολογιών καθιστούν δύσκολο για το υποκείμενο των δεδομένων να γνωρίζει και

[108] Blockchain and the General Data Protection Regulation,Can distributed ledgers be squared with European data protection law?, Study, Panel for the Future of Science and Technology, European Parliamentary Research Service, Scientific Foresight Unit (STOA) PE 634.445 – July 2019

[109] ΓΚΠΔ, άρθρο 5 παρ.1 , στοιχείο α

[110] ΓΚΠΔ, Αιτιολ. Σκέψη 39

[111] ΓΚΠΔ, άρθρο 5 παρ. 1

να κατανοεί εάν, από ποιον και για ποιο σκοπό συλλέγονται δεδομένα προσωπικού χαρακτήρα που το αφορούν[112]. Θα πρέπει να γνωστοποιείται στα φυσικά πρόσωπα η ύπαρξη κινδύνων, κανόνων, εγγυήσεων και δικαιωμάτων σε σχέση με την επεξεργασία δεδομένων προσωπικού χαρακτήρα και πώς να ασκούν τα δικαιώματά τους σε σχέση με την επεξεργασία αυτή. Ιδίως, οι συγκεκριμένοι σκοποί της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα θα πρέπει να είναι σαφείς, νόμιμοι και προσδιορισμένοι κατά τον χρόνο συλλογής των δεδομένων προσωπικού χαρακτήρα[113].

Δεν φαίνεται να προκύπτουν σημαντικά ζητήματα όσον αφορά την αρχής της διαφάνειας όταν πρόκειται για την τεχνολογία blockchain, αρκεί να καθίσταται σαφές στα υποκείμενα των δεδομένων τι είδους δεδομένα θα υποστούν επεξεργασία και τι κίνδυνοι μπορεί να προκύψουν. Ωστόσο, επειδή κάθε σύστημα μπορεί να εμφανίζει μεγάλες διαφορές από τα υπόλοιπα, ίσως υπάρχουν διαφορετικοί κίνδυνοι σε κάθε περίπτωση τους οποίους το υποκείμενο πρέπει να γνωρίζει. Επίσης, δυσκολία συμμόρφωσης μπορεί να υπάρξει σε περιπτώσεις όπου συγκεκριμένες λειτουργικές ιδιότητες του συστήματος μπορεί να μην επιτρέπουν τον ξεκάθαρο ορισμό του υπευθύνου επεξεργασίας ή σε περιπτώσεις όπου δεν υπάρχει επικοινωνία μεταξύ του υπευθύνου επεξεργασίας και του υποκειμένου των δεδομένων, όπως για παράδειγμα σε έναν κόμβο που δεν έχει σχέση με τους υπόλοιπους του δικτύου και έχει πρόσβαση μόνο σε κρυπτογραφημένα δεδομένα.

Περιορισμός του σκοπού

Κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα πρέπει να εκτελείται για συγκεκριμένο, καλά καθορισμένο σκοπό και μόνο για πρόσθετους σκοπούς οι οποίοι είναι συμβατοί προς τον αρχικό[114]. Συνεπώς, είναι παράνομη και δε συμμορφώνεται με τις διατάξεις του Κανονισμού οποιαδήποτε επεξεργασία δεδομένων προσωπικού χαρακτήρα εκτελείται για μη καθορισμένους σκοπούς καθώς και οποιαδήποτε επεξεργασία με αόριστο σκοπό, με το σκεπτικό ότι τα δεδομένα θα είναι χρήσιμα κάποια στιγμή μελλοντικά.

Κάθε νέος σκοπός επεξεργασίας ασύμβατος με τον αρχικό πρέπει να διαθέτει νέα, δική του νομική βάση. Περεταίρω επεξεργασία δεδομένων δεν μπορεί να γίνεται με τρόπο μη αναμενόμενο ή ακατάλληλο ή κατά τρόπο στον οποίο ενδέχεται να εναντιωθεί το υποκείμενο των δεδομένων[115].

Η εφαρμογή της αρχής του περιορισμού του σκοπού σε περιπτώσεις όπου η επεξεργασία εκτελείται μέσω τεχνολογιών blockchain εγείρει ένα μεγάλο ερώτημα: η περεταίρω επεξεργασία δεδομένων που προστίθενται σε block μετά την εκτέλεση της συναλλαγής για την οποία αρχικά προστέθηκαν στο καθολικό, είναι συμβατή με ην αρχή του περιορισμού του σκοπού; Αν σκεφτεί κανείς την ιδιότητα append-only των blockchain (δηλαδή την ιδιότητα που έχουν μόνο να προσαρτώνται δεδομένα σε αυτά και όχι να τροποποιούνται ή να διαγράφονται), τα δεδομένα θα συνεχίσουν να

[112] ΓΚΠΔ, Αιτιολ. Σκέψη 58
[113] ΓΚΠΔ, Αιτιολ. Σκέψη 39
[114] ΓΚΠΔ, άρθρο 5, παρ. 1 στοιχ. 1
[115] Αιτιολογική έκθεση Εκσυγχρονισμένης Σύμβασης 108, σημείο 49

υφίστανται επεξεργασία επ' αόριστον εφόσον προστεθούν στο καθολικό. Για παράδειγμα, όταν χρησιμοποιούνται δεδομένα σε ένα blockchain για την εκτέλεση συναλλαγών με κρυπτονομίσματα, είτε πρόκειται για δημόσια κλειδιά είτε για δεδομένα συναλλαγών, τα δεδομένα θα συνεχίσουν 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. Έτσι ανακύπτει το ερώτημα εάν η αποθήκευση και η συμπερίληψη των δεδομένων σε άλλες συναλλαγές θεωρούνται μέρος του αρχικού σκοπού της επεξεργασίας ή εάν πρόκειται για ασυμβατότητα με την αρχή του περιορισμού του σκοπού.

Δεδομένου ότι οι συγκεκριμένοι σκοποί της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα θα πρέπει να είναι σαφείς, νόμιμοι και προσδιορισμένοι κατά τον χρόνο συλλογής των δεδομένων προσωπικού χαρακτήρα[116], 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.

Η Ομάδα Εργασίας του άρθρου 29, αναφέρει ότι η συμβατότητα μεταξύ του αρχικού σκοπού και της περεταίρω επεξεργασίας καθορίζεται λαμβάνοντας υπόψη τα εξής: τη σχέση μεταξύ του σκοπού για τον οποίο τα δεδομένα συλλέχθηκαν και του σκοπού για τον οποίο υποβλήθηκαν σε περεταίρω επεξεργασία, τα πλαίσια στα οποία τα δεδομένα συλλέχθηκαν και τις λογικές προσδοκίες που μπορεί να έχουν τα υποκείμενα των δεδομένων για την περεταίρω επεξεργασία, τη φύση των δεδομένων και τον αντίκτυπο της περεταίρω επεξεργασίας στα υποκείμενα και τις εγγυήσεις που παρέχει ο υπεύθυνος επεξεργασίας για να διασφαλίσει την αντικειμενικότητα της επεξεργασίας και να αποτρέψει δυσάρεστες συνέπειες των υποκειμένων των δεδομένων[117].

Ένα κρίσιμο ζήτημα είναι το εάν η περεταίρω επεξεργασία υπονοήθηκε με κάποιο τρόπο με τον αρχικό σκοπό της επεξεργασίας. Η ομάδα εργασίας του άρθρου 29[118] θεωρεί ως σχετικό παράγοντα το για ποιο λόγο θα πίστευε, ένα λογικό άτομο στη θέση του υποκειμένου ων δεδομένων, ότι συλλέγονται τα προσωπικά δεδομένα του. Λαμβάνοντας επίσης υπόψη τη σχέση μεταξύ του υποκειμένου και του υπευθύνου επεξεργασίας, θα μπορούσαμε να οδηγηθούμε στο συμπέρασμα ότι μπορεί να υπάρξουν περιπτώσεις όπου η περεταίρω επεξεργασία σε μία συναλλαγή σε blockchain μπορεί να καλύπτεται από την αρχή του περιορισμού του σκοπού.

Ελαχιστοποίηση των δεδομένων

Σε επεξεργασία υποβάλλονται μόνο τα δεδομένα που είναι κατάλληλα, συναφή και δεν είναι δυσανάλογα σε σχέση με τον σκοπό για τον οποίο συγκεντρώνονται ή

[116] ΓΚΠΔ, Αιτιολ. Σκέψη 39
[117] Article 29 Working Party, Opinion 03/2013 on purpose limitation (WP 203) 00569/13/EN
[118] Article 29 Working Party, Opinion 03/2013 on purpose limitation (WP 203) 00569/13/EN

υφίστανται περεταίρω επεξεργασία[119]. Σύμφωνα με τη συγκεκριμένη αρχή, πρέπει πάντα να επιλέγεται κάποια λύση η οποία να επιδιώκει την προστασία της ιδιωτικής ζωής, αποφεύγοντας, όταν είναι αυτό εφικτό, τη χρήση δεδομένων προσωπικού χαρακτήρα, ή επιλέγοντας μέτρα τα οποία μειώνουν την ικανότητα σύνδεσης δεδομένων με ένα συγκεκριμένο υποκείμενο δεδομένων (π.χ. με ψευδωνυμοποίηση).

Η εκσυγχρονισμένη Σύμβαση 108 περιέχει επιπλέον απαίτηση αναλογικότητας για την επεξεργασία προσωπικών δεδομένων σε σχέση με τον σκοπό που επιδιώκει. Ειδικότερα, ορίζει ότι τα δεδομένα προσωπικού χαρακτήρα τα οποία είναι κατάλληλα και συναφή, αλλά συνεπάγονται δυσανάλογη επέμβαση στα θεμελιώδη δικαιώματα και τις ελευθερίες που διακυβεύονται θα πρέπει να θεωρούνται υπερβολικά[120].

Σημαντική απόφαση που αφορά την αρχή της ελαχιστοποίησης των δεδομένων αποτελεί η απόφαση του ΔΕΕ γνωστή ως Digital Rights Ireland[121]. Στη συγκεκριμένη υπόθεση το ΔΕΕ έκρινε ότι η Οδηγία για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία στο πλαίσιο διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δικτύων για ενδεχόμενη διαβίβαση σε αρμόδιες αρχές για την καταπολέμηση σοβαρών ποινικών αδικημάτων, περιείχε μία άκρως προβληματική διάταξη που αφορούσε κάθε πρόσωπο και κάθε μέσο ηλεκτρονικής επικοινωνίας, καθώς και το σύνολο των δεδομένων κινήσεως άνευ ουδεμίας διαφοροποιήσεως, περιορισμού ή εξαιρέσεως σε σχέση προς το σκοπό της καταπολεμήσεως σοβαρών παραβιάσεων. Κατά το ΔΕΕ, τα δεδομένα που μπορούσαν να διατηρηθούν βάσει της οδηγίας παρείχαν, στο σύνολό τους, ακριβείς πληροφορίες σχετικά με φυσικά πρόσωπα. Επιπλέον, το ΔΕΕ εξέτασε τη σοβαρότητα της επέμβασης στα θεμελιώδη δικαιώματα του σεβασμού της ιδιωτικής ζωής και της προστασίας των δεδομένων προσωπικού χαρακτήρα. Έκρινε ότι η διατήρηση ανταποκρίνεται σε στόχο δημόσιου συμφέροντος, δηλαδή στην καταπολέμηση σοβαρού εγκλήματος και, συνεπώς, στη διαφύλαξη της δημόσιας ασφάλειας. Ωστόσο, το ΔΕΕ αποφάνθηκε ότι η έκδοση της οδηγίας συνιστούσε παραβίαση της αρχής της αναλογικότητας από τον νομοθέτη της ΕΕ. Παρότι η οδηγία μπορεί να είναι κατάλληλη για την επίτευξη του απαιτούμενου στόχου, «συνεπάγεται μια τεράστιας εκτάσεως και ιδιαιτέρως μεγάλης βαρύτητας στο πλαίσιο της έννομης τάξεως της Ένωσης επέμβαση σε αυτά τα θεμελιώδη δικαιώματα χωρίς η επέμβαση αυτή να οριοθετείται επακριβώς μέσω διατάξεων δυνάμενων να διασφαλίσουν ότι πράγματι περιορίζεται στον απολύτως αναγκαίο βαθμό».

Δύο χαρακτηριστικά των blockchain μπορούν να προκαλέσουν ζητήματα αναφορικά με την αρχή της ελαχιστοποίησης δεδομένων. Η συνεχώς αυξανόμενη φύση τέτοιου είδους βάσεων δεδομένων και συνεχιζόμενη αντιγραφή των δεδομένων, καθώς κάθε κόμβος αποθηκεύει ένα πλήρες αντίγραφό του καθολικού. Για να μπορέσουμε να απαντήσουμε σχετικά με το αν σε ένα blockchain μπορεί να εφαρμοστεί η αρχή της ελαχιστοποίησης των δεδομένων πρέπει να επανέλθει το

[119] ΓΚΠΔ, άρθρο 5, παρ.1,στοιχ. γ

[120] Αιτιολογική έκθεση, Εκσυγχρονισμένη Σύμβαση 108, σημείο 52

[121] ΔΕΕ, C-293/12 και C-594/12, Digital Rights Ireland Ltd κατά Minister for Communications, Marine and Natural Resources κλπ. και Karntner Landesregierung, 08-04-2014

ζήτημα της ερμηνείας της αρχή του περιορισμού του σκοπού. Εάν ο αρχικός σκοπός της επεξεργασίας περιλαμβάνει όχι μόνο την συναλλαγή αλλά και την περεταίρω επεξεργασία, τότε η συνεχιζόμενη αποθήκευση και η αντιγραφή των δεδομένων συμμορφώνεται πλήρως και με την αρχή του περιορισμού του σκοπού αλλά και με την αρχή της ελαχιστοποίησης των δεδομένων.

Ακρίβεια

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[122]. Η ακρίβεια των δεδομένων μπορεί ενίοτε να απαιτεί αυτά να μην επικαιροποιούνται και να καταγράφονται ως ιστορικά στιγμιότυπα. Σε αντίθετες περιπτώσεις, τα δεδομένα οφείλουν να επικαιροποιούνται, να ελέγχονται και να διορθώνονται προκειμένου να μην προκαλέσουν ζημία στα υποκείμενα. Σε κάθε περίπτωση, η υποχρέωση διασφάλισης της ακρίβειας, εξετάζεται υπό το πλαίσιο του σκοπού της επεξεργασίας των δεδομένων.

Τα blockchain διαθέτουν την ιδιότητα append-only, επιτρέπουν δηλαδή μόνο την προσάρτηση δεδομένων, ενώ συχνά είναι σχεδιασμένα να καθιστούν την διαγραφή και την τροποποίηση δεδομένων εξαιρετικά δύσκολη ή και αδύνατη, με σκοπό να προστατεύσουν την ακεραιότητα των δεδομένων και την εμπιστοσύνη στο δίκτυο. Καταφανώς, αυτό έρχεται σε αντίθεση με τις απαιτήσεις του Κανονισμού που προβλέπει ότι τα δεδομένα πρέπει να είναι ευμετάβλητα έτσι ώστε να επιτρέπουν τη διαγραφή ή τη διόρθωσή τους. Έτσι, όταν ένα πελάτης ζητά από κάποιο πάροχο υπηρεσιών που χρησιμοποιεί blockchain να διορθώσει πληροφορίες που βρίσκονται στο αρχείο του, έρχεται αντιμέτωπος με την μη αναστρεψιμότητα του blockchain.

Παρόλα αυτά, σε ιδιωτικά και/ή μη αδειοδοτημένα blockchain, τέτοια αιτήματα μπορούν να ικανοποιηθούν, αλλάζοντας την καταγραφή της συναλλαγής με τη χρήση ξανά hash στα μεταγενέστερα block, όταν αυτό υποστηρίζεται από τις τεχνικές και ρυθμιστικές λειτουργίες. Αντίστοιχες ενέργειες σε δημόσια και/ή μη αδειοδοτημένα blockchain είναι εξαιρετικά πιο δύσκολες καθώς κάθε κόμβος τροποποιεί το δικό του αντίγραφο του καθολικού. Ακόμα και στην περίπτωση που όλοι οι κόμβοι συμφωνούσαν να δημιουργήσουν μια νέα εκδοχή του blockchain σε περιοδικά διαστήματα, προκειμένου να μπορούν να δέχονται ανάλογα αιτήματα, αυτό το επίπεδο συντονισμού είναι σχεδόν αδύνατο να επιτευχθεί ανάμεσα σε πιθανόν χιλιάδες κόμβους[123].

Περιορισμός της περιόδου αποθήκευσης των δεδομένων

Τα δεδομένα προσωπικού χαρακτήρα διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας των δεδομένων προσωπικού

[122] ΓΚΠΔ, άρθρο 5 παρ. 1 στοιχ. δ

[123] Bacon J et al (2018), 'Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers' *Richmond Journal of Law and Technology*

χαρακτήρα. Μπορούν να αποθηκεύονται για μεγαλύτερα διαστήματα, εφόσον τα δεδομένα προσωπικού χαρακτήρα θα υποβάλλονται σε επεξεργασία μόνο για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς και εφόσον εφαρμόζονται τα κατάλληλα τεχνικά και οργανωτικά μέτρα που απαιτεί ο Κανονισμός για τη διασφάλιση των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων[124].

Τα δεδομένα προσωπικού χαρακτήρα πρέπει να διαγράφονται ή να ανωνυμοποιούνται όταν οι σκοποί που αφορούν την επεξεργασία τους έχουν εκπληρωθεί. Έτσι, ο υπεύθυνος επεξεργασίας θα πρέπει να ορίζει προθεσμίες για τη διαγραφή τους ή για την περιοδική επανεξέτασή τους, ώστε να διασφαλίζεται ότι τα δεδομένα δεν διατηρούνται περισσότερο από όσο είναι αναγκαίο[125].

Η υποχρέωση που επιβάλλει η συγκεκριμένη αρχή εγείρει το ερώτημα ΄πότε τα δεδομένα σε ένα blockchain θεωρούνται παρωχημένα΄. Μία ερμηνεία θα μπορούσε να είναι με την ολοκλήρωση της σχετικής συναλλαγής, ή ακόμα κα μετά τη συναλλαγή τα δεδομένα θα μπορούσαν να θεωρηθούν απαραίτητα για την περεταίρω επεξεργασία και συγκεκριμένα για την συνεχή αποθήκευση των δεδομένων στο καθολικό καθώς και για την επεξεργασία για την εκτέλεση του αλγόριθμου συναίνεσης. Όπως ήδη έχει αναφερθεί, τα δεδομένα σε ένα blockchain μπορούν να αφαιρεθούν μόνο σε έκτακτες περιπτώσεις, δημιουργώντας έτσι «ένταση» στη σχέση με τον Κανονισμό, καθώς όπως φαίνεται η αρχή του περιορισμού της περιόδου αποθήκευσης δεν μπορεί να εφαρμοστεί.

Ακεραιότητα και εμπιστευτικότητα

Τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια των δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων[126]. Ανάλογα με τις εκάστοτε συνθήκες, τα τεχνικά και οργανωτικά μέτρα που υποχρεούνται να λαμβάνουν οι υπεύθυνοι επεξεργασίας θα μπορούσαν να περιλάβουν την ψευδωνυμοποίηση, την κρυπτογράφηση, την τήρηση εγκεκριμένου κώδικα δεοντολογίας, ή εγκεκριμένου μηχανισμού πιστοποίησης ακόμη και η υποχρέωση επαγγελματικού απορρήτου. Κατά την εφαρμογή των μέτρων αυτών, ο υπεύθυνος επεξεργασίας οφείλει να λαμβάνει υπόψη διάφορα στοιχεία, όπως τη φύση και τον όγκο των δεδομένων που υποβάλλονται σε επεξεργασία, τις δυνητικές αρνητικές συνέπειες για τα υποκείμενα των δεδομένων και την αναγκαιότητα περιορισμένης πρόσβασης στα δεδομένα.

Η υποχρέωση συμμόρφωσης με την συγκεκριμένη αρχή, δεν θέτει ιδιαίτερα ζητήματα συμμόρφωσης όσον αφορά τα blockchain.

[124] ΓΚΠΔ, άρθρο 5, παρ. 1, στοιχ. ε
[125] ΓΚΠΔ, αιτιολογική Σκέψη 39
[126] ΓΚΠΔ, άρθρο 5,παρ.1 στοιχ. στ

Λογοδοσία

Ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και πρέπει να είναι σε θέση να αποδείξει τη συμμόρφωσή του προς τις αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα[127]. Ο τύπος των διαδικασιών και των μηχανισμών που θα χρησιμοποιήσει ο υπεύθυνος επεξεργασία προκειμένου να συμμορφώνεται προς τις παραπάνω αρχές, διαφέρει ανάλογα με τους κινδύνους που ενέχει η επεξεργασία και ανάλογα με τη φύση των δεδομένων. Η λογοδοσία ουσιαστικά συνίσταται στην υποχρέωση του υπευθύνου επεξεργασίας να θεσπίζει μέτρα τα οποία, υπό κανονικές συνθήκες, θα διασφαλίζουν την τήρηση των κανόνων προστασίας δεδομένων στο πλαίσιο των πράξεων επεξεργασίας και να διαθέτει τεκμηρίωση που να αποδεικνύει στα υποκείμενα των δεδομένων και στις εποπτικές αρχές τη λήψη μέτρων για την επίτευξη συμμόρφωσης προς τους κανόνες[128].

Οι διάφοροι τρόποι συμμόρφωσης προς της αρχές της επεξεργασίας δεδομένων προσωπικού χαρακτήρα αναφέρονται στον ΓΚΠΔ και μπορούν να περιλαμβάνουν την καταχώρηση των δραστηριοτήτων επεξεργασίας σε αρχεία και η διάθεση τους στην εποπτική αρχή[129], τον ορισμό του υπευθύνου προστασίας δεδομένων[130], την εκτίμηση αντικτύπου[131], προστασία δεδομένων από τον σχεδιασμό και εξ ορισμού[132], εφαρμογή ρυθμίσεων και διαδικασιών για την άσκηση των δικαιωμάτων του υποκειμένου των δεδομένων[133], την τήρηση εγκεκριμένου κώδικα δεοντολογίας ή μηχανισμού πιστοποίησης[134].

Παρόλο που η αρχή της λογοδοσίας του άρθρου 5 ρητά κατονομάζει τον υπεύθυνο επεξεργασίας, υπάρχουν διατάξεις που αφορούν τη συγκεκριμένη αρχή και καθορίζουν υποχρεώσεις για τον εκτελούντα την επεξεργασία. Έτσι, ο εκτελών την επεξεργασία, οφείλει επίσης να τηρεί αρχείο δραστηριοτήτων επεξεργασίας[135], να διασφαλίζει την εφαρμογή όλων των αναγκαίων μέτρων που αφορούν την ασφάλεια των δεδομένων, να συνδράμει τον υπεύθυνο επεξεργασίας σε κάποιες απαιτήσεις συμμόρφωσης[136].

Η υποχρέωση για λογοδοσία που βαρύνει τον υπεύθυνο επεξεργασίας δεδομένων αναφορικά με τη χρήση τεχνολογίας blockchain, αναλύθηκε ανωτέρω.

Τα δικαιώματα των υποκειμένων των δεδομένων και η ικανοποίησή τους σε περιβάλλον blockchain

Στα άρθρα 15 έως 22 του ΓΚΠΔ προβλέπονται τα δικαιώματα των υποκειμένων. Αναφορικά με την άσκησή τους όταν η επεξεργασία δεδομένων γίνεται με τη χρήση κάποιας τεχνολογίας blockchain, σε κάποιες περιπτώσεις αυτή γίνεται

[127] ΓΚΠΔ, άρθρο 5, παρ. 2
[128] Ομάδα εργασίας άρθρου 29, Γνώμη 3/2010 σχετικά με την αρχή της λογοδοσίας
[129] ΓΚΠΔ άρθρο 30
[130] ΓΚΠΔ, άρθρα 37-39
[131] ΓΚΠΔ, άρθρο 35
[132] ΓΚΠΔ, άρθρο 25
[133] ΓΚΠΔ, άρθρα 12, 24
[134] ΓΚΠΔ, άρθρα 40,42
[135] ΓΚΠΔ, άρθρα 30, 37
[136] ΓΚΠΔ, άρθρο 28, παρ.3

ανεπηρέαστα ενώ σε κάποιες άλλες εμφανίζονται ζητήματα είτε τεχνικής είτε νομικής φύσεως.

Δικαίωμα ενημέρωσης

Τα υποκείμενα των δεδομένων έχουν δικαίωμα να ενημερώνονται με ακρίβεια και σαφήνεια για τη συλλογή και χρήση (επεξεργασία) των προσωπικών τους δεδομένων. Το δικαίωμα αυτό διέπεται από μία από τις βασικές αρχές του ΓΚΠΔ, την αρχή της διαφάνειας[137]. Η ενημέρωση πρέπει να είναι συνοπτική, διαφανής, κατανοητή, εύκολα προσβάσιμη και διατυπωμένη σε απλή και σαφή γλώσσα.

Δικαίωμα πρόσβασης

Σύμφωνα με τον Κανονισμό[138], το υποκείμενο των δεδομένων έχει το δικαίωμα να λαμβάνει από τον υπεύθυνο επεξεργασίας επιβεβαίωση για το κατά πόσον ή όχι τα δεδομένα προσωπικού χαρακτήρα που το αφορούν υφίστανται επεξεργασία και, εάν συμβαίνει τούτο, το δικαίωμα πρόσβασης στα δεδομένα προσωπικού χαρακτήρα και στις ακόλουθες πληροφορίες:

α) τους σκοπούς της επεξεργασίας,

β) τις σχετικές κατηγορίες δεδομένων προσωπικού χαρακτήρα,

γ) τους αποδέκτες ή τις κατηγορίες αποδεκτών στους οποίους κοινολογήθηκαν ή πρόκειται να κοινολογηθούν τα δεδομένα προσωπικού χαρακτήρα, ιδίως τους αποδέκτες σε τρίτες χώρες ή διεθνείς οργανισμούς,

δ) εάν είναι δυνατόν, το χρονικό διάστημα για το οποίο θα αποθηκευτούν τα δεδομένα προσωπικού χαρακτήρα ή, όταν αυτό είναι αδύνατο, τα κριτήρια που καθορίζουν το εν λόγω διάστημα,

ε) την ύπαρξη δικαιώματος υποβολής αιτήματος στον υπεύθυνο επεξεργασίας για διόρθωση ή διαγραφή δεδομένων προσωπικού χαρακτήρα ή περιορισμό της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα που αφορά το υποκείμενο των δεδομένων ή δικαιώματος αντίταξης στην εν λόγω επεξεργασία,

στ) το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή,

ζ) όταν τα δεδομένα προσωπικού χαρακτήρα δεν συλλέγονται από το υποκείμενο των δεδομένων, κάθε διαθέσιμη πληροφορία σχετικά με την προέλευσή τους,

η) την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ, που προβλέπεται στο άρθρο 22 παράγραφοι 1 και 4 και, τουλάχιστον στις περιπτώσεις αυτές, σημαντικές πληροφορίες σχετικά με τη λογική που ακολουθείται, καθώς και τη σημασία και τις προβλεπόμενες συνέπειες της εν λόγω επεξεργασίας για το υποκείμενο των δεδομένων.

Σύμφωνα με τον Κανονισμό, όταν ένα υποκείμενο υποβάλει αίτημα πρόσβασης, ο υπεύθυνος επεξεργασίας οφείλει να αναζητήσει όλα τα αρχεία του,

[137] ΓΚΠΔ άρθρα 12-14

[138] ΓΚΠΔ, άρθρο 15

είτε ηλεκτρονικά είτε έντυπα, έτσι ώστε να μπορέσει να ικανοποιήσει το αίτημα[139]. Αντίστοιχα, όταν ένας υπεύθυνος επεξεργασίας χρησιμοποιεί κάποια τεχνολογία blockchain για την επεξεργασία δεδομένων, οφείλει να διεξάγει έρευνα στη βάση δεδομένων και να διαπιστώσει εάν περιλαμβάνονται πληροφορίες του συγκεκριμένου υποκειμένου που υπέβαλε το αίτημα. Δεδομένου ότι υπάρχουν οι κατάλληλοι οργανωτικοί μηχανισμοί που επιτρέπουν την αποτελεσματική επικοινωνία και τη διαχείριση δεδομένων σε ένα blockchain, δεν εντοπίζονται σημαντικά εμπόδια που θα απέκλειαν την ικανοποίηση ενός αιτήματος πρόσβασης.

Ωστόσο, σε ένα blockchain είναι πιθανό πολλοί παράγοντες να θεωρούνται υπεύθυνοι ή από κοινού υπεύθυνοι επεξεργασίας και κάποιοι από αυτούς ίσως να μην έχουν πλήρη πρόσβαση στα δεδομένα, όπως για παράδειγμα οι κόμβοι, οι οποίοι συνήθως βλέπουν μόνο κρυπτογραφημένα δεδομένα. Σε τέτοιες περιπτώσεις υπάρχουν δυσκολίες, καθώς οι υπεύθυνοι επεξεργασίας αδυνατούν να διακρίνουν πότε περιλαμβάνονται στο καθολικό προσωπικά δεδομένα του υποκειμένου που ασκεί το αίτημα και πότε όχι. Ανάλογες δυσκολίες προκύπτουν όταν ο υπεύθυνος επεξεργασίας οφείλει να παρέχει στα υποκείμενα ένα αντίγραφο των δεδομένων που υφίστανται επεξεργασία σύμφωνα με το άρθρο 15παρ. 3 του Κανονισμού. Συνεπώς, όταν κάποιος επιθυμεί να χρησιμοποιήσει τεχνολογία blockchain για την επεξεργασία δεδομένων, προκειμένου να βρίσκεται σε πλήρη συμμόρφωση με τον Κανονισμό, πρέπει να επιβεβαιωθεί ότι έχει προβεί στις κατάλληλες οργανωτικές ρυθμίσεις που θα επιτρέπουν την άσκηση του δικαιώματος πρόσβασης.

Δικαίωμα διόρθωσης

Τα υποκείμενα των δεδομένων έχουν δικαίωμα να ζητήσουν τη διόρθωση των δεδομένων τους, όταν αυτά είναι ανακριβή ή τη συμπλήρωση των δεδομένων τους, όταν αυτά είναι ελλιπή, μεταξύ άλλων μέσω συμπληρωματικής δήλωσης[140]. Τα δεδομένα θεωρούνται ανακριβή όταν αυτά είναι λανθασμένα, ενώ ελλιπή θεωρούνται όταν η απουσία δεδομένων μπορεί να οδηγήσει σε παραπλάνηση ή παρεξήγηση.

Οι δυσκολίες στην εκπλήρωση αιτημάτων διόρθωσης από τα υποκείμενα των δεδομένων αφορούν σε δύο ζητήματα: αφενός στην ιδιότητα των blockchain να είναι μη αναστρέψιμα (append only), όπως αναλύθηκε στην ενότητα σχετικά με την εφαρμογή της αρχής της ακρίβειας και αφετέρου στο γεγονός ότι το υποκείμενο των δεδομένων πρέπει να απευθυνθεί σε όλους τους πλήρεις κόμβους του δικτύου για την ικανοποίηση του αιτήματος γεγονός που είναι δύσκολο, αν όχι ακατόρθωτο, δεδομένου ότι κάποιοι κόμβοι μπορεί να μην είναι συνδεδεμένοι στο δίκτυο ή να έχουν αλλάξει τις διευθύνσεις δικτύου τους.

Σε ιδιωτικά blockchain, αιτήματα διόρθωσης μπορούν να ικανοποιηθούν με μια τροποποίηση στην καταγραφή της συναλλαγής με τη χρήση ξανά hash στα μεταγενέστερα block, όταν αυτό υποστηρίζεται από τις τεχνικές και ρυθμιστικές λειτουργίες. Αντίστοιχες ενέργειες σε δημόσια και/ή μη αδειοδοτημένα blockchain είναι εξαιρετικά πιο δύσκολες καθώς κάθε κόμβος τροποποιεί το δικό του αντίγραφο

[139] ΓΚΠΔ, άρθρο 15
[140] ΓΚΠΔ άρθρο 16

του καθολικού, δεδομένου ότι μπορεί να εντοπίσει τα σχετικά δεδομένα έτσι ώστε να τα διορθώσει, γεγονός εξαιρετικά δύσκολο όταν τα δεδομένα είναι κρυπτογραφημένα[141].

Το άρθρο 16 του ΓΚΠΔ προβλέπει επίσης τη δυνατότητα συμπλήρωσης ελλιπών δεδομένων μέσω συμπληρωματικής δήλωσης. Τέτοιου είδους αιτήματα θα μπορούσαν ευκολότερα να ικανοποιηθούν αναφορικά με τα διαμοιραζόμενα καθολικά, καθώς οποιοδήποτε μέρος έχει προσθέσει δεδομένα στο καθολικό, μπορεί να προσθέσει νέα δεδομένα τα οποία διορθώνουν τα παλαιότερα. Έχει διατυπωθεί η άποψη ότι αυτή η συμπληρωματική δήλωση μπορεί να λειτουργήσει ως ένα τρόπος διόρθωσης δεδομένων σε blockchain, δημοσιεύοντας μία καινούρια συναλλαγή η οποία θα περιέχει νέα ή διορθωμένα δεδομένα, χωρίς να υπάρχει έτσι η ανάγκη για ολική διαγραφή της προηγούμενης συναλλαγής.

Δικαίωμα διαγραφής

Το δικαίωμα διαγραφής («δικαίωμα στη λήθη») είναι το δικαίωμα να ζητά το υποκείμενο των δεδομένων τη διαγραφή των δεδομένων προσωπικού χαρακτήρα που το αφορούν, εφόσον δεν επιθυμεί πια αυτά τα δεδομένα να αποτελούν αντικείμενο επεξεργασίας και εφόσον δεν υφίσταται νόμιμος λόγος να τα κατέχει ο υπεύθυνος επεξεργασίας[142]. Το δικαίωμα του φυσικού προσώπου να ζητεί τη διαγραφή των δεδομένων προσωπικού χαρακτήρα που το αφορούν χωρίς αδικαιολόγητη καθυστέρηση ισχύει όταν:

• τα δεδομένα προσωπικού χαρακτήρα δεν είναι πλέον απαραίτητα για τους σκοπούς για τους οποίους συλλέχθηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία,

• το υποκείμενο των δεδομένων ανακαλεί τη συγκατάθεση επί της οποίας βασίζεται η επεξεργασία και δεν υπάρχει άλλη νομική βάση για την επεξεργασία,

• το υποκείμενο των δεδομένων αντιτίθεται στην επεξεργασία και δεν υπάρχουν επιτακτικοί και νόμιμοι λόγοι για την επεξεργασία,

• τα δεδομένα προσωπικού χαρακτήρα υποβλήθηκαν σε επεξεργασία παράνομα,

τα δεδομένα προσωπικού χαρακτήρα πρέπει να διαγραφούν ώστε να τηρηθεί νομική υποχρέωση βάσει του ενωσιακού δικαίου ή του δικαίου κράτους μέλους στην οποία υπόκειται ο υπεύθυνος επεξεργασίας,

• τα δεδομένα προσωπικού χαρακτήρα έχουν συλλεχθεί στο πλαίσιο της παροχής υπηρεσιών της κοινωνίας των πληροφοριών σε παιδιά βάσει του άρθρου 8 του ΓΚΠΔ.

Ωστόσο, δεν πρόκειται για ένα απόλυτο δικαίωμα, καθώς η περαιτέρω διατήρηση των δεδομένων προσωπικού χαρακτήρα θεωρείται σύννομη, όταν είναι αναγκαία, για λόγους όπως για την άσκηση του δικαιώματος ελευθερίας της έκφρασης και ενημέρωσης, όπως προαναφέρθηκε, ή για τη συμμόρφωση με νομική

[141] Blockchain and the General Data Protection Regulation,Can distributed ledgers be squared with European data protection law?, Study, Panel for the Future of Science and Technology, European Parliamentary Research Service, Scientific Foresight Unit (STOA) PE 634.445 – July 2019

[142] ΓΚΠΔ άρθρο 17

υποχρέωση, για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας, για λόγους δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας, για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς ή για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων.

Στις 13 Μαΐου 2014, το Δικαστήριο της Ευρωπαϊκής Ένωσης (ΔΕΕ), εξέδωσε μία απόφαση - σταθμό για την καθιέρωση και την αναγνώριση του δικαιώματος διαγραφής, γνωστή ως Google Spain[143]. Το ΔΕΕ κατέληξε στο συμπέρασμα, μεταξύ άλλων, ότι η Google, όταν πραγματοποιεί αναζήτηση στον Παγκόσμιο Ιστό σχετικά με πληροφορίες και ιστοσελίδες και όταν ευρετηριάζει περιεχόμενο για να παρέχει αποτελέσματα αναζήτησης, καθίσταται υπεύθυνος επεξεργασίας δεδομένων με τις ευθύνες και υποχρεώσεις που προβλέπονται στο δίκαιο της ΕΕ.

Μετά την έκδοση της απόφασης, η Ομάδα εργασίας του άρθρου 29 εξέδωσε κατευθυντήριες γραμμές σχετικά με την εφαρμογή της απόφασης του ΔΕΕ. Στις κατευθυντήριες γραμμές περιλαμβάνεται κατάλογος κοινών κριτηρίων για χρήση από τις εποπτικές αρχές, όταν χειρίζονται καταγγελίες που αφορούν αιτήματα διαγραφής φυσικών προσώπων, εξηγούνται οι συνέπειες του δικαιώματος διαγραφής και παρέχεται καθοδήγηση για την ως άνω στάθμιση δικαιωμάτων. Στις κατευθυντήριες γραμμές επαναλαμβάνεται ότι οι εκτιμήσεις πρέπει να πραγματοποιούνται κατά περίπτωση. Καθώς το δικαίωμα στη λήθη δεν είναι απόλυτο, το αποτέλεσμα σχετικού αιτήματος μπορεί να διαφέρει ανάλογα με την υπό κρίση υπόθεση. Αυτό επισημαίνεται επίσης στη νομολογία του ΔΕΕ μετά την υπόθεση που αφορούσε την Google. Ο κατάλογος των κοινών κριτηρίων αξιολόγησης, τον οποίο διαμόρφωσε η Ομάδα εργασίας του άρθρου 29, αποτελεί το πλαίσιο που οι Εθνικές Αρχές θα εφαρμόζουν κατά τις διαδικασίες λήψης αποφάσεων, αλλά και το οποίο μπορούν από κοινού να εμπλουτίσουν αξιοποιώντας την εμπειρία που θα αποκομίζουν με την πάροδο του χρόνου.

Τα κοινά κριτήρια αξιολόγησης είναι τα εξής: 1) Το αποτέλεσμα της αναζήτησης αφορά φυσικό πρόσωπο, δηλ. άτομο; Το αποτέλεσμα αναζήτησης εμφανίζεται με βάση το όνομα του υποκειμένου των δεδομένων; 2) Το υποκείμενο των δεδομένων διαδραματίζει ρόλο στη δημόσια ζωή; Είναι δημόσιο πρόσωπο; 3) Το υποκείμενο των δεδομένων είναι ανήλικος; 4) Τα δεδομένα είναι ακριβή; 5) Τα δεδομένα είναι συναφή κι όχι περισσότερα από όσα χρειάζονται; Αφορούν την επαγγελματική ζωή του υποκειμένου; Το αποτέλεσμα της αναζήτησης συνδέεται με πληροφορίες που φέρεται να συνιστούν ρητορική μίσους/συκοφαντία/δυσφήμιση ή ανάλογα αδικήματα στον τομέα της έκφρασης κατά του προσφεύγοντος; Τα δεδομένα αντικατοπτρίζουν προσωπική γνώμη ή φαίνεται να είναι επιβεβαιωμένο γεγονός; 6) Είναι ευαίσθητα προσωπικά δεδομένα σύμφωνα με το άρ. 8 της Οδηγίας 95/46/ΕΚ; 7) Είναι τα δεδομένα επικαιροποιημένα; Διατίθενται για χρονικό διάστημα μμεγαλύτερο από όσο απαιτείται για τον επιδιωκόμενο σκοπό; 8) Η επεξεργασία των δεδομένων προκαλεί ζημία στο υποκείμενο των δεδομένων; Η δημοσιοποίηση των

[143] C-131/12, Google Spain και Inc κατά Agencia Española de Protección De Datos (AEPD) και Mario Costeja González

δεδομένων έχει δυσανάλογες αρνητικές επιπτώσεις για την ιδιωτική ζωή του υποκειμένου των δεδομένων; 9) Το αποτέλεσμα της αναζήτησης συνδέεται με πληροφορίες που θέτουν το υποκείμενο των δεδομένων σε κίνδυνο; 10) Μέσα σε ποιό κείμενο δημοσιεύτηκαν τα δεδομένα; Τα δεδομένα δημοσιοποιήθηκαν οικειοθελώς και σκοπίμως από το ίδιο το υποκείμενο; Θα μπορούσε να υπάρξει εύλογη προσδοκία από το υποκείμενο ότι τα δεδομένα θα δημοσιοποιηθούν; 11) Το αρχικό κείμενο δημοσιεύθηκε στο πλαίσιο δημοσιογραφικών σκοπών; 12) Ο εκδότης των δεδομένων έχει τη νομική δύναμη ή τη νομική υποχρέωση να καθιστά τα προσωπικά δεδομένα διαθέσιμα στο κοινό; 13) Τα δεδομένα αφορούν σε ποινικό αδίκημα; Σύμφωνα με τις εν λόγω Κατευθυντήριες Γραμμές, τα κριτήρια αυτά θα πρέπει να εφαρμόζονται σύμφωνα με τις οικείες εθνικές νομοθετικές διατάξεις και κανένα μεμονωμένο κριτήριο δεν είναι από μόνο του καθοριστικής σημασίας. [144]

Η δυσκολία άσκησης του δικαιώματος διαγραφής σε ένα σύστημα blockchain έχει τονιστεί επανειλημμένως. Η μη αναστρεψιμότητα των blockchain καθιστά τη διαγραφή των δεδομένων εξαιρετικά δύσκολη, καθώς τα δίκτυα αυτά είναι σχεδιασμένα με τέτοιο τρόπο ώστε να κάνουν την μονόπλευρη τροποποίηση των δεδομένων δύσκολη, ενισχύοντας έτσι την εμπιστοσύνη στο δίκτυο. Για παράδειγμα, όταν ο αλγόριθμός που χρησιμοποιείται είναι ο proof-of-work, η πλειοψηφία των peer-to-peer κόμβων που είναι συνδεδεμένοι στο δίκτυο θα έπρεπε να επιβεβαιώσει ξανά την ορθότητα κάθε συναλλαγής που επηρεάζεται με κατεύθυνση προς τα πίσω, «γκρεμίζοντας» ένα τα block του blockchain για να τα ξαναστήσουν έπειτα από την αρχή, με κάθε συναλλαγή να πρέπει να διαμοιραστεί σε κάθε block, σε όλους τους υπάρχοντες κόμβους[145]. Επιπλέον, ακόμα και αν υπήρχαν οι κατάλληλοι τεχνικοί μηχανισμοί για να επιτευχθεί η διαγραφή δεδομένων από το blockchain, αυτό το εγχείρημα θα παρέμενε δύσκολο εξαιτίας οργανωτικών παραγόντων, καθώς θα έπρεπε όλοι οι κόμβοι να εφαρμόσουν τους μηχανισμούς αυτούς και να προσαρμόσουν τις αλλαγές αυτές επάνω στο δικό τους αντίγραφο του καθολικού. Έτσι, μία εταιρία που χρησιμοποιεί τεχνολογία blockchain, ικανοποιώντας το αίτημα διαγραφής του κάποιο υποκειμένου των δεδομένων, το πραγματοποιεί εις βάρος της σταθερότητας και ακεραιότητας του συστήματος, η οποία μπορεί να οδηγήσει σε διάρρηξη της αξιοπιστίας της και της εμπιστοσύνης των πελατών της προς αυτή[146].

Συμπερασματικά, η συμμόρφωση με το άρθρο 17 του Κανονισμού, σχετικά με το δικαίωμα διαγραφής, είναι εξαιρετικά δύσκολη, εξαιτίας παραγόντων τόσο τεχνικής όσο και οργανωτικής φύσεως. Για το λόγο αυτό έχουν προταθεί εναλλακτικοί τεχνικοί τρόποι για να επιτευχθεί η διαγραφή δεδομένων σε ένα blockchain. Αρχικά η CNIL πρότεινε η διαγραφή να επιτυγχάνεται με την καταστροφή του ιδιωτικού κλειδιού, γεγονός που θα καθιστούσε τα κρυπτογραφημένα δεδομένα μη προσβάσιμα. Η πρόταση αφορά ειδικότερα τη διαγραφή του μυστικού κλειδιού,

[144] Ομάδα εργασίας άρθρου 29, 14/EL WP 225 Κατευθυντήριες γραμμές σχετικά με την εφαρμογή της απόφασης του δικαστηρίου της Ευρωπαϊκής Ένωσης στην υπόθεση c-131/12, «google Spain και inc κατά agencia española de protección de datos (aepd) και Mario Costeja González».

[145] Berberich M and Steiner M (2016), 'Blockchain Technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers?' 2 *European Data Protection Law Review*

[146] Unal Tatar, Yasir Gokce , Brian Nussbaum, Law versus technology: Blockchain, GDPR, and tough tradeoffs, Computer law & security review 38 (2020), Science Direct

στο οποίο έχει εφαρμοστεί συνάρτηση κατακερματισμού μαζί με όλες τις πληροφορίες από άλλα συστήματα όπου ήταν αποθηκευμένο για επεξεργασία[147]. Άλλη πρόταση είναι η χρήση μεθόδων όπως επεξεργάσιμα blockchain που θα έχουν από το σχεδιασμό τους την ιδιότητα να ΄΄ξεχνούν΄΄, οι ΄΄chameleon hashes΄΄, και οι αποδείξεις μηδενικής γνώσης (zero knowledge proofs)[148]. Έχει γίνει επιπλέον και η πρόβλεψη ότι στο μέλλον θα γίνει χρήση αυτοματοποιημένων επιλογών αναστρεψιμότητας, όπως διορθωτικές λειτουργίες που θα μπορούν να επεμβαίνουν αυτόματα με τη χρήση έξυπνων συμβολαίων[149].

Ακόμα και με την ύπαρξη των ανωτέρω τεχνικών λειτουργιών, η συμμόρφωση με το άρθρο 17 του Κανονισμού δεν θα μπορούσε να επιτευχθεί χωρίς την κατάλληλη επικοινωνία και συνεργασία μεταξύ όλων των παραγόντων του δικτύου. Σύμφωνα με το άρθρο 17παρ. 2 : «Όταν ο υπεύθυνος επεξεργασίας έχει δημοσιοποιήσει τα δεδομένα προσωπικού χαρακτήρα και υποχρεούται σύμφωνα με την παράγραφο 1 να διαγράψει τα δεδομένα προσωπικού χαρακτήρα, ο υπεύθυνος επεξεργασίας, λαμβάνοντας υπόψη τη διαθέσιμη τεχνολογία και το κόστος εφαρμογής, λαμβάνει εύλογα μέτρα, συμπεριλαμβανομένων των τεχνικών μέτρων, για να ενημερώσει τους υπευθύνους επεξεργασίας που επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα, ότι το υποκείμενο των δεδομένων ζήτησε τη διαγραφή από αυτούς τους υπευθύνους επεξεργασίας τυχόν συνδέσμων με τα δεδομένα αυτά ή αντιγράφων ή αναπαραγωγών των εν λόγω δεδομένων προσωπικού χαρακτήρα». Αυτό σημαίνει ότι τα αιτούμενα προς διαγραφή δεδομένα πρέπει να διαγραφούν από όλους τους κόμβους του δικτύου για να θεωρείται ότι διαγράφηκαν. Συνεπώς, όταν ένας υπεύθυνος επεξεργασίας σε ένα blockchain λάβει ένα αίτημα διαγραφής, δεν αρκεί να διαγράψει τα δεδομένα, αλλά πρέπει να ενημερωθούν και οι υπόλοιποι υπεύθυνοι ή εκτελούντες την επεξεργασία οι οποίο πραγματοποιούν επεξεργασία στα ίδια δεδομένα.

Επιπλέον, καθώς τα blockchain είναι συστήματα που αποτελούνται από επίπεδα, όπως αναλυτικά αναφέρθηκαν ανωτέρω, υπάρχει η περίπτωση να εμφανίζονται πολλοί από κοινού υπεύθυνοι επεξεργασίας σε κάθε συναλλαγή, στους οποίους μπορούν τα υποκείμενα να απευθύνονται για τη διεκδίκηση των δικαιωμάτων τους. Στην υπόθεση Google Spain, όπως αναφέρθηκε ανωτέρω, το ΔΕΕ έκρινε ότι οι μηχανές αναζήτησης αποτελούν υπεύθυνους επεξεργασίας δεδομένων και ότι ένα υποκείμενο μπορεί να ζητήσει απευθείας από την μηχανή αναζήτησης την διαγραφή των δεδομένων του, χωρίς αυτά να έχουν διαγραφεί προηγουμένως από την εφημερίδα, στην οποία περιλαμβανόταν το επίμαχο άρθρο. Με τον ίδιο συλλογισμό, ένα υποκείμενο δεδομένων μπορεί να απευθυνθεί σε ενδιάμεσα μέρη

[147] Commission Nationale Informatique et Libertés (September 2018), *Premiers Éléments d'analyse de la CNIL :* Blockchain

[148] Ateniese G, Magri B, Venturi D and Andrade E (2017), 'Redactable Blockchain – or – Rewriting History in Bitcoin and Friends'

[149] Bacon J et al (2018), 'Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers' 25 *Richmond Journal of Law and Technology*

σε ένα σύστημα blockchain, όπως για παράδειγμα σε κάποιο blockexplorer, για να διαγράψει τα δεδομένα του από το αρχείο του[150].

Τέλος, ένα ζήτημα εξαιρετικά περίπλοκο, αποτελεί η εδαφική εφαρμογή του δικαιώματος διαγραφής. Με την απόφασή του στην υπόθεση Google v CNIL το ΔΕΕ έκρινε ότι ο φορέας εκμετάλλευσης μηχανής αναζήτησης ο οποίος κάνει δεκτή αίτηση του υποκειμένου των δεδομένων για διαγραφή συνδέσμων, ενδεχομένως κατόπιν εντολής εποπτικής ή δικαστικής αρχής κράτους μέλους, δεν υπέχει υποχρέωση από το δίκαιο της Ένωσης να προβεί στη διαγραφή αυτή ως προς το σύνολο των εκδοχών της μηχανής αναζήτησης που εκμεταλλεύεται[151]. Δεδομένου ότι ένα blockchain μπορεί να υπάγεται ταυτόχρονα σε πολλές διαφορετικές δικαιοδοσίες, εντός και εκτός Ευρωπαϊκής Ένωσης, η αναλογική εφαρμογή της απόφασης αυτής του ΔΕΕ μπορεί να οδηγήσει στο ενδεχόμενο τα δεδομένα ενός υποκειμένου να τυγχάνουν διαγραφής σε κάποια δικαιοδοσία ενώ σε κάποια άλλη όχι. Αυτό έρχεται, φυσικά, σε αντίθεση με τις τεχνικές και λειτουργικές ιδιότητες των blockchain, καθώς το διαμοιραζόμενο καθολικό αντιγράφεται και αποθηκεύεται σε όλους τους κόμβους ενώ δεν είναι δυνατή η μερική διαγραφή δεδομένων, πχ σε συγκεκριμένους μόνο κόμβους.

Δικαίωμα περιορισμού της επεξεργασίας

Τα υποκείμενα των δεδομένων διατηρούν το δικαίωμα να ζητήσουν από τον υπεύθυνο επεξεργασίας τον περιορισμό της επεξεργασίας, όταν ισχύει ένα από τα ακόλουθα[152]:

α) η ακρίβεια των δεδομένων προσωπικού χαρακτήρα αμφισβητείται από το υποκείμενο των δεδομένων, για χρονικό διάστημα που επιτρέπει στον υπεύθυνο επεξεργασίας να επαληθεύσει την ακρίβεια των δεδομένων προσωπικού χαρακτήρα,

β) η επεξεργασία είναι παράνομη και το υποκείμενο των δεδομένων αντιτάσσεται στη διαγραφή των δεδομένων προσωπικού χαρακτήρα και ζητεί, αντ' αυτής, τον περιορισμό της χρήσης τους,

γ) ο υπεύθυνος επεξεργασίας δεν χρειάζεται πλέον τα δεδομένα προσωπικού χαρακτήρα για τους σκοπούς της επεξεργασίας, αλλά τα δεδομένα αυτά απαιτούνται από το υποκείμενο των δεδομένων για τη θεμελίωση, την άσκηση ή την υποστήριξη νομικών αξιώσεων,

δ) το υποκείμενο των δεδομένων έχει αντιρρήσεις για την επεξεργασία σύμφωνα με το άρθρο 21 παράγραφος 1, εν αναμονή της επαλήθευσης του κατά πόσον οι νόμιμοι λόγοι του υπευθύνου επεξεργασίας υπερισχύουν έναντι των λόγων του υποκειμένου των δεδομένων.

---

[150] Blockchain and the General Data Protection Regulation,Can distributed ledgers be squared with European data protection law?, Study, Panel for the Future of Science and Technology, European Parliamentary Research Service, Scientific Foresight Unit (STOA) PE 634.445 – July 2019

[151] Case C-507/17 *Google v CNIL,* *https://curia.europa.eu/juris/document/document.jsf;jsessionid=DBFD45FB81C1CD1091FED6B3CDCA2933?text=&docid=218105&pageIndex=0&doclang=EL&mode=lst&dir=&occ=first&part=1&cid=626146*

[152] ΓΚΠΔ άρθρο 18

Αναφορικά με το δικαίωμα περιορισμού της επεξεργασίας και κατά πόσο μπορεί να εφαρμοστεί σε ένα δίκτυο blockchain, είναι να πιθανόν να εμφανιστούν προβλήματα συμμόρφωσης σε δύο περιπτώσεις. Αρχικά, συστήματα όπως τα blockchain είναι σχεδιασμένα έτσι ώστε να καθιστούν την παρέμβαση στην επεξεργασία των δεδομένων εξαιρετικά επιβαρυντική και δύσκολη, εξασφαλίζοντας έτσι την ακεραιότητα των δεδομένων και την εμπιστοσύνη στο δίκτυο. Ειδικά σε δημόσια και μη αδειοδοτημένα blockchain δεν υπάρχει κάποιος τρόπος να διακοπεί η επεξεργασία δεδομένων που περιέχονται σε κάποιο μπλοκ. Επιπλέον, υπάρχουν εμπόδια οργανωτικής φύσεως, όπως η πιθανότητα πολλοί από κοινού υπεύθυνοι επεξεργασίας να αναλάβουν να κάνουν μία τέτοια παρέμβαση στο δίκτυο. Ωστόσο, κάποιοι από τους υπευθύνους αυτούς, όπως οι κόμβοι ή κάποιοι χρήστες, μπορεί να μην έχουν την ικανότητα να παρέμβουν με τέτοιο τρόπο ώστε να επιτευχθεί ο περιορισμός της επεξεργασίας δεδομένων, εξαιτίας της περιορισμένης πρόσβασής τους στα δεδομένα.

Υποχρέωση γνωστοποίησης όσον αφορά τη διόρθωση ή τη διαγραφή δεδομένων προσωπικού χαρακτήρα ή τον περιορισμό της επεξεργασίας

Σύμφωνα με το άρθρο 19 του ΓΚΠΔ ο υπεύθυνος επεξεργασίας ανακοινώνει κάθε διόρθωση ή διαγραφή δεδομένων προσωπικού χαρακτήρα ή περιορισμό της επεξεργασίας των δεδομένων που διενεργείται σύμφωνα με το άρθρο 16, το άρθρο 17 παράγραφος 1 και το άρθρο 18 σε κάθε αποδέκτη στον οποίο γνωστοποιήθηκαν τα δεδομένα προσωπικού χαρακτήρα, εκτός εάν αυτό αποδεικνύεται ανέφικτο ή εάν συνεπάγεται δυσανάλογη προσπάθεια. Το ερώτημα που προκύπτει είναι το ποια μέρη θα μπορούσαν να θεωρηθούν ως αποδέκτες προσωπικών δεδομένων όταν χρησιμοποιείται μια τεχνολογία blockchain. Σε ιδιωτικά και/ή αδειοδοτημένα συστήματα συνήθως υπάρχει μία καταγραφή των μερών τα οποία έχουν πρόσβαση σε προσωπικά δεδομένα, συνεπώς είναι εύκολο οι υπεύθυνοι επεξεργασίας να επικοινωνήσουν μαζί τους και να ενημερώσουν για τέτοιου είδους δράσεις. Αντιθέτως, σε δημόσια ή/και μη αδειοδοτημένα blockchain είναι αδύνατον να υπάρχει γνώση σχετικά με το ποιος έχει αποκτήσει πρόσβαση στα δεδομένα, καθώς δεν απαιτείται ειδική άδεια για αυτό. Συνεπώς η συμμόρφωση με τη συγκεκριμένη υποχρέωση είναι μάλλον αδύνατη και πιθανότατα η περίπτωση αυτή υπάγεται στην εξαίρεση που προβλέπει το άρθρο εάν πρόκειται για ενέργεια ανέφικτη.

Δικαίωμα στη φορητότητα

Το υποκείμενο των δεδομένων έχει το δικαίωμα να λαμβάνει τα δεδομένα προσωπικού χαρακτήρα που το αφορούν, και τα οποία έχει παράσχει σε υπεύθυνο επεξεργασίας, σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα μορφότυπο, καθώς και το δικαίωμα να διαβιβάζει τα εν λόγω δεδομένα σε άλλον υπεύθυνο επεξεργασίας χωρίς αντίρρηση από τον υπεύθυνο επεξεργασίας στον οποίο παρασχέθηκαν τα δεδομένα προσωπικού χαρακτήρα, όταν: α) η

επεξεργασία βασίζεται σε συγκατάθεση ή σε σύμβαση και β) η επεξεργασία διενεργείται με αυτοματοποιημένα μέσα[153].

Και στην περίπτωση του δικαιώματος στη φορητότητα, τα προβλήματα εντοπίζονται στο γεγονός ότι μπορεί μεν πολλές οντότητες να θεωρούνται υπεύθυνοι επεξεργασίας σε ένα blockchain, ωστόσο, υπάρχει πάντα η πιθανότητα να έχουν περιορισμένη πρόσβαση σε δεδομένα. Έτσι, ένα κόμβος που θεωρείται υπεύθυνος επεξεργασίας και έχει πρόσβαση μόνο σε κρυπτογραφημένα δεδομένα, αδυνατεί να βρεθεί σε συμμόρφωση με το άρθρο 20 του ΓΚΠΔ, καθώς το δικαίωμα του υποκειμένου στη φορητότητα δεν μπορεί να ικανοποιηθεί.

Δικαίωμα εναντίωσης

Το δικαίωμα της εναντίωσης[154] συνίσταται στο δικαίωμα που έχει το φυσικό πρόσωπο (υποκείμενο των δεδομένων) να αντιτάσσεται, ανά πάσα στιγμή και για λόγους που σχετίζονται με την ιδιαίτερη κατάστασή του, στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που το αφορούν, η οποία βασίζεται στο άρθρο 6 παρ. 1 στοιχ. ε΄ ΓΚΠΔ (καθήκον που εκτελείται προς το δημόσιο συμφέρον) ή στ΄ (ύπαρξη εννόμου συμφέροντος), περιλαμβανομένης της κατάρτισης προφίλ βάσει των εν λόγω διατάξεων.

Στην περίπτωση που το υποκείμενο των δεδομένων εναντιωθεί στην επεξεργασία των προσωπικών του δεδομένων, ο υπεύθυνος επεξεργασίας οφείλει να σταματήσει την εν λόγω επεξεργασία εκτός και αν καταδείξει επιτακτικούς και νόμιμους λόγους για την επεξεργασία, οι οποίοι υπερισχύουν των συμφερόντων, των δικαιωμάτων και των ελευθεριών του υποκειμένου των δεδομένων ή για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων.

Για ακόμα μία φορά, η συμμόρφωση με το άρθρο 21 ΓΚΠΔ σε ένα blockchain εξαρτάται από το την πραγματική ικανότητα των υπευθύνων επεξεργασίας να επηρεάζουν την επεξεργασία των δεδομένων, εξαιτίας της περιορισμένης πρόσβασης που μπορεί να έχουν σε αυτά αλλά και από την ικανότητά τους να διακόπτουν την επεξεργασία όταν αυτή στηρίζεται σε αυτοματοποιημένα μέσα. Ένα σημαντικό σημείο στο άρθρο 21 του Κανονισμού είναι οι επιτακτικοί και νόμιμοι λόγοι που μπορεί να προβάλει ο υπεύθυνος επεξεργασίας στο υποκείμενο των δεδομένων. Ένας παράγοντας που θα μπορούσε να αποτελέσει επιτακτικό και νόμιμο λόγο άρνησης ικανοποίησης του δικαιώματος εναντίωσης όταν η επεξεργασία γίνεται με τη χρήση blockchain, είναι η υποχρέωση του εκάστοτε υπευθύνου επεξεργασίας να διατηρήσει την ακεραιότητα των δεδομένων και του συστήματος εν γένει καθώς και την εμπιστοσύνη στο δίκτυο[155].

[153] ΓΚΠΔ άρθρο 20

[154] ΓΚΠΔ άρθρο 21

[155] Blockchain and the General Data Protection Regulation,Can distributed ledgers be squared with European data protection law?, Study, Panel for the Future of Science and Technology, European Parliamentary Research Service, Scientific Foresight Unit (STOA) PE 634.445 – July 2019

Αυτοματοποιημένη ατομική λήψη αποφάσεων, περιλαμβανομένης της κατάρτισης προφίλ

Σύμφωνα με τον ΓΚΠΔ το υποκείμενο των δεδομένων έχει το δικαίωμα να μην υπόκειται σε απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας, συμπεριλαμβανομένης της κατάρτισης προφίλ, η οποία παράγει έννομα αποτελέσματα που το αφορούν ή το επηρεάζει σημαντικά με παρόμοιο τρόπο. Η προηγούμενη διάταξη δεν τυγχάνει εφαρμογής όταν η απόφαση: α) είναι αναγκαία για τη σύναψη ή την εκτέλεση σύμβασης μεταξύ του υποκειμένου των δεδομένων και του υπευθύνου επεξεργασίας των δεδομένων, β) επιτρέπεται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους στο οποίο υπόκειται ο υπεύθυνος επεξεργασίας και το οποίο προβλέπει επίσης κατάλληλα μέτρα για την προστασία των δικαιωμάτων, των ελευθεριών και των έννομων συμφερόντων του υποκειμένου των δεδομένων ή γ) βασίζεται στη ρητή συγκατάθεση του υποκειμένου των δεδομένων[156].

Στις περιπτώσεις που αναφέρονται στην παράγραφο 2 στοιχεία α) και γ) του άρθρου 22 ΓΚΠΔ, ο υπεύθυνος επεξεργασίας των δεδομένων εφαρμόζει κατάλληλα μέτρα για την προστασία των δικαιωμάτων, των ελευθεριών και των έννομων συμφερόντων του υποκειμένου των δεδομένων, τουλάχιστον του δικαιώματος εξασφάλισης ανθρώπινης παρέμβασης από την πλευρά του υπευθύνου επεξεργασίας, έκφρασης άποψης και αμφισβήτησης της απόφασης.

Οι αποφάσεις που αναφέρονται στην παράγραφο 2 δεν βασίζονται στις ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα που αναφέρονται στο άρθρο 9 παράγραφος 1, εκτός αν ισχύει το άρθρο 9 παράγραφος 2 στοιχείο α) ή ζ) και αν υφίστανται κατάλληλα μέτρα για την προστασία των δικαιωμάτων, των ελευθεριών και των έννομων συμφερόντων του υποκειμένου των δεδομένων.

Το άρθρο 22 του ΓΚΠΔ, έχει ιδιαίτερη σημασία στα πλαίσια χρήσης blockchain για την επεξεργασία δεδομένων, όταν η επεξεργασία αφορά την εκτέλεση έξυπνων συμβολαίων. Πρέπει, αρχικά, να καθοριστεί εάν ένα έξυπνο συμβόλαιο μπορεί να αποτελέσει απόφαση που λαμβάνεται με αυτοματοποιημένα μέσα και εάν η απόφαση αυτή παράγει έννομα αποτελέσματα για το υποκείμενο των δεδομένων ή διαφορετικά εάν το επηρεάζει σημαντικά, προκειμένου να διαπιστωθεί εάν επιτυγχάνεται συμμόρφωση με τη συγκεκριμένη διάταξη. Σύμφωνα με τον M. Finck, τα έξυπνα συμβόλαια, τουλάχιστον σε κάποιες περιπτώσεις, μπορούν να λαμβάνουν αποφάσεις με τη χρήση τεχνολογικών μέσω και χωρίς την ανθρώπινη παρέμβαση, για παράδειγμα με τη χρήση ενός μηχανισμού που βασίζεται σε μία σχέση εάν/τότε η οποία αρχικά σχεδιάστηκε από ανθρώπους αλλά εκτελείται από κάποια μηχανή. Περαιτέρω, τα έξυπνα συμβόλαια μπορεί σε κάποιες περιπτώσεις να παράγουν έννομα αποτελέσματα όπως για παράδειγμα σε περιπτώσεις που το συμβόλαιο καθορίζει εάν έχουν πληρωθεί ασφάλιστρα ή εάν έχει γίνει η πληρωμή για κάποιο αγαθό[157]. Συνεπώς, το δικαίωμα του υποκειμένου των δεδομένων να αρνηθεί την

[156] ΓΚΠΔ άρθρο 22

[157] Michèle Finck, Smart Contracts as a Form of Solely Automated Processing under the GDPR, Max Planck Institute for Innovation and Competition Research Paper No. 19-01, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3311370

λήψη απόφασης με αυτοματοποιημένα μέσα, μπορεί να εφαρμοστεί στην περίπτωση των έξυπνων συμβολαίων, εκτός εάν εμπίπτουν στις εξαιρέσεις που προβλέπονται στην παράγραφο 2 του ίδιου άρθρου. Για να μπορεί κάποια περίπτωση να υπαχθεί στην πρώτη εξαίρεση που αφορά τη σύναψη ή την εκτέλεση σύμβασης μεταξύ του υποκειμένου των δεδομένων και του υπευθύνου επεξεργασίας, πρέπει να εντοπιστεί ο υπεύθυνος επεξεργασίας δεδομένων. Αναφορικά με τη δεύτερη εξαίρεση, η οποία εφαρμόζεται όταν επιτρέπεται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους στο οποίο υπόκειται ο υπεύθυνος επεξεργασίας, δεν υπάρχει προς το παρόν κάποια νομοθεσία η οποία ρητώς να επιτρέπει την επεξεργασία προσωπικών δεδομένων με αυτοματοποιημένα μέσα σχετικά με τα έξυπνα συμβόλαια.

Εφαρμογή της προστασίας προσωπικών δεδομένων από το σχεδιασμό και εξ ορισμού σε blockchain

Προκειμένου ο υπεύθυνος επεξεργασίας να μπορεί να αποδείξει συμμόρφωση προς τον Κανονισμό, θα πρέπει να θεσπίζει εσωτερικές πολιτικές και να εφαρμόζει μέτρα τόσο κατά τη στιγμή του καθορισμού των μέσων επεξεργασίας όσο και κατά τη στιγμή της επεξεργασίας, ανταποκρινόμενος έτσι, μεταξύ άλλων, στις αρχές της προστασίας των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού (data protection by design and by default)[158].

Σύμφωνα με την αρχή της προστασίας των δεδομένων ήδη από τον σχεδιασμό, κατά τη στιγμή του σχεδιασμού των συστημάτων επεξεργασίας και του καθορισμού των μέσων επεξεργασίας, ο υπεύθυνος επεξεργασίας πρέπει να ενσωματώνει και να εφαρμόζει κατάλληλα μέτρα και να χρησιμοποιεί τεχνολογίες ενίσχυσης της ιδιωτικότητας, όπως ψευδωνυμοποίηση δεδομένων προσωπικού χαρακτήρα, το συντομότερο δυνατόν (δηλ. αντικατάσταση προσωπικά ταυτοποιήσιμων πληροφοριών με τεχνητά αναγνωριστικά στοιχεία), κρυπτογράφηση (κωδικοποίηση προσωπικών δεδομένων έτσι ώστε μόνο όσοι είναι εξουσιοδοτημένοι να μπορούν να τα διαβάζουν), ελαχιστοποίηση της επεξεργασίας των δεδομένων και ενσωμάτωση των απαραίτητων εγγυήσεων στην επεξεργασία, κατά τρόπο ώστε να πληρούνται οι απαιτήσεις του ΓΚΠΔ και να προστατεύονται τα δικαιώματα των υποκειμένων των δεδομένων[159]. Κατά την ανάπτυξη, τον σχεδιασμό, την επιλογή και τη χρήση εφαρμογών, υπηρεσιών και προϊόντων που βασίζονται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα ή όταν επεξεργάζονται δεδομένα προσωπικού χαρακτήρα για την εκπλήρωση του έργου τους, οι παραγωγοί προϊόντων, υπηρεσιών και εφαρμογών πρέπει να λαμβάνουν υπόψη τους το δικαίωμα προστασίας των δεδομένων, ώστε, συνεκτιμώντας τις τελευταίες εξελίξεις της τεχνολογίας, να διασφαλίζεται ότι οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία θα είναι σε θέση να εκπληρώνουν τις υποχρεώσεις τους όσον αφορά την προστασία των δεδομένων. Η ρύθμιση αυτή, μπορεί να αναγνωσθεί ως μία έκφανση της αναλογικότητας, ως επιταγή για μέτρα ανάλογα με το είδος των δεδομένων, την επεξεργασία και τους

[158] ΓΚΠΔ άρθρο 25, αιτιολογική σκέψη 78
[159] ΓΚΠΔ, άρθρο 25

κινδύνους. Η υποχρέωση για ενσωμάτωση της αρχής αυτής αναφέρεται σε όλο το φάσμα και σε όλο τον κύκλο ζωής των δεδομένων[160].

Σύμφωνα με την αρχή της προστασίας των δεδομένων εξ ορισμού, ο υπεύθυνος επεξεργασίας εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα για να διασφαλίζει ότι, εξ ορισμού, εξασφαλίζεται η ιδιωτικότητα και υφίστανται επεξεργασία μόνο τα δεδομένα προσωπικού χαρακτήρα που είναι απαραίτητα για τον εκάστοτε σκοπό της επεξεργασίας. Αυτή η υποχρέωση ισχύει για το εύρος των δεδομένων προσωπικού χαρακτήρα που συλλέγονται, τον βαθμό της επεξεργασίας τους, την περίοδο αποθήκευσης και την προσβασιμότητά τους. Ειδικότερα, τα εν λόγω μέτρα διασφαλίζουν ότι, εξ ορισμού, τα δεδομένα προσωπικού χαρακτήρα δεν καθίστανται προσβάσιμα, χωρίς την παρέμβαση φυσικού προσώπου, σε αόριστο αριθμό φυσικών προσώπων. Η χρησιμότητα τα αρχής της προστασίας των δεδομένων εξ ορισμού συνοψίστηκε από τον Ευρωπαίο Επίτροπο Προστασίας Δεδομένων: «αποσκοπεί στην προστασία του υποκειμένου των δεδομένων σε καταστάσεις όπου μπορεί να υπάρχει έλλειψη κατανόησης ή ελέγχου αναφορικά με την επεξεργασία των προσωπικών δεδομένων του, ιδίως σε τεχνολογικό πλαίσιο» [161]

Τέλος, ένα μέτρο το οποίο ανταποκρίνεται στις αρχές της προστασίας των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού είναι και η διαφάνεια όσον αφορά τις λειτουργίες και την επεξεργασία των δεδομένων προσωπικού χαρακτήρα, ώστε να μπορεί το υποκείμενο των δεδομένων να παρακολουθεί την επεξεργασία δεδομένων και να είναι σε θέση ο υπεύθυνος επεξεργασίας να δημιουργεί και να βελτιώνει τα χαρακτηριστικά ασφάλειας.

Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΔ) εξέδωσε κατευθυντήριες γραμμές που περιλαμβάνουν γενικές οδηγίες σχετικά με την υποχρέωση προστασίας των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού[162]. Οι κατευθυντήριες γραμμές περιλαμβάνουν οδηγίες σχετικά με την αποτελεσματική εφαρμογή των αρχών της προστασίας των δεδομένων που προβλέπονται στο άρθρο 5, απαριθμώντας κύρια στοιχεία σχεδιασμού και εξ ορισμού, καθώς και πρακτικές περιπτώσεις ως ενδεικτικά παραδείγματα. Ο υπεύθυνος επεξεργασίας πρέπει να εξετάζει την καταλληλόλητα των προτεινόμενων μέτρων στο πλαίσιο της εκάστοτε επεξεργασίας. Σε όλα τα στάδια σχεδιασμού των δραστηριοτήτων επεξεργασίας, συμπεριλαμβανομένων των προμηθειών, των διαγωνισμών, της εξωτερικής ανάθεσης, της ανάπτυξης, της υποστήριξης, της συντήρησης, των δοκιμών, της αποθήκευσης, της διαγραφής, κ.λπ., ο υπεύθυνος επεξεργασίας πρέπει να λαμβάνει υπόψη του και να εξετάζει τα διάφορα στοιχεία της προστασίας δεδομένων από το σχεδιασμό και εξ ορισμού, τα οποία επεξηγούνται με παραδείγματα στο παρόν κεφάλαιο στο πλαίσιο της εφαρμογής των αρχών. Οι υπεύθυνοι επεξεργασίας οφείλουν να εφαρμόζουν τις αρχές ώστε να επιτυγχάνεται η προστασία δεδομένων από το σχεδιασμό και εξ ορισμού. Στις εν λόγω αρχές περιλαμβάνονται: η διαφάνεια,

[160] Κοτσαλής Λεωνίδας, Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων, Νομική Βιβλιοθήκη, σελ.280

[161] EDPS, Opinion of 7 March 2012 on the data protection reform package, 7 March 2012

[162] ΕΣΠΔ, Κατευθυντήριες γραμμές 4/2019 σύμφωνα με το άρθρο 25 Προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού

η νομιμότητα, η αντικειμενικότητα, ο περιορισμός του σκοπού, η ελαχιστοποίηση των δεδομένων, η ακρίβεια, ο περιορισμός της περιόδου αποθήκευσης, η ακεραιότητα, η εμπιστευτικότητα και η λογοδοσία.

Στα πλαίσια της επεξεργασίας προσωπικών δεδομένων με τη χρήση τεχνολογίας blockchain, δύο είναι τα βασικότερα ζητήματα που αφορούν την εφαρμογή της συγκεκριμένης αρχής. Πρώτον, οποιοδήποτε χρησιμοποιεί κάποια τεχνολογία blockchain, οφείλει να είναι σε θέση να επιβεβαιώσει ότι οι τεχνικές της ιδιότητες επιτρέπουν τη συμμόρφωση με τον ΓΚΠΔ. Δεύτερον, οι υπεύθυνοι επεξεργασίας δεδομένων πρέπει να επιβεβαιώνουν ότι οι οργανωτικές λειτουργίες του blockchain είναι σε θέση να συμμορφώνονται με τον Κανονισμό, να περιλαμβάνουν δηλαδή, την ύπαρξη επαρκούς επικοινωνίας μεταξύ υποκειμένων των δεδομένων και υπευθύνων επεξεργασίας, αλλά και με πιθανούς άλλους από κοινού υπευθύνους επεξεργασίας.

Ωστόσο κάποιες ιδιότητες της τεχνολογίας blockchain δείχνουν να είναι ασύμβατες με την υποχρέωση για προστασία των δεδομένων από το σχεδιασμό και εξ ορισμού. Η αμεταβλητότητα και η αδυναμία παραβίασης του συστήματος είναι μεταξύ αυτών. Το γεγονός ότι είναι σχεδόν αδύνατον, όπως αναφέρθηκε, να αφαιρεθούν δεδομένα από το καθολικό χωρίς να διαλυθεί η ακεραιότητα του συστήματος, καθιστά ανεφάρμοστη την προστασία δεδομένων από τον σχεδιασμό και εξ ορισμού.

Επιπλέον, ένα ακόμα χαρακτηριστικό που θέτει σημαντικά προβλήματα στη συμμόρφωση με τη συγκεκριμένη υποχρέωση, είναι το γεγονός ότι τα δεδομένα αποθηκεύονται με τέτοιο τρόπο, ώστε οποιοσδήποτε να μπορεί να τεκμηριώσει κάθε συναλλαγή και την αντίστοιχη αξία της. Συνεπώς, οποιοσδήποτε έχει πρόσβαση στο σύστημα μπορεί να επιβεβαιώσει εάν οι συναλλαγές είναι έγκυρες. Αυτή η διαφανής και ανοιχτή στο κοινό φύση των blockchain φαίνεται να είναι προβληματική από άποψη προστασίας δεδομένων, καθώς σύμφωνα με το Κανονισμό, τα δεδομένα πρέπει να αποθηκεύονται με τέτοιο τρόπο ώστε να εξασφαλίζεται η εμπιστευτικότητα και η διαθεσιμότητα μεταξύ των μερών. Με άλλα λόγια, τα δεδομένα πρέπει να είναι διαθέσιμα μόνο σε άτομα που διαθέτουν τη σχετική άδεια. Συνεπώς, το γεγονός ότι το καθολικό ενός blockchain είναι ορατό και ανοιχτό σε όλους από το σχεδιασμό του, έρχεται σε αντίθεση με την υποχρέωση για προστασία των δεδομένων από το σχεδιασμό και εξ ορισμού που προβλέπει ο ΓΚΠΔ[163].

Προκειμένου να επιτυγχάνεται η συμμόρφωση με την συγκεκριμένη υποχρέωση, οι προγραμματιστές και οι αρχιτέκτονες συστημάτων πρέπει να αντιμετωπίζουν τις υποχρεώσεις του ΓΚΠΔ για αναγνώριση των μέσων και των σκοπών της επεξεργασίας καθώς και εφαρμόζουν τις απαραίτητες εγγυήσεις κατά το χρόνο κατασκευής του λογισμικού, ακολουθώντας συγκεκριμένες στρατηγικές. Οκτώ στρατηγικές προστασίας της ιδιωτικότητας από το σχεδιασμό, κατατάσσονται σε στρατηγικές που σχετίζονται με τα δεδομένα και στρατηγικές που σχετίζονται με την επεξεργασία. Οι στρατηγικές που σχετίζονται με τα δεδομένα είναι οι εξής:

[163] Unal Tatar, Yasir Gokce , Brian Nussbaum, Law versus technology: Blockchain, GDPR, and tough tradeoffs, Computer law & security review 38 (2020), Science Direct

Ελαχιστοποίηση: Η στρατηγική αυτή εξασφαλίζει ότι τα δεδομένα που συλλέγονται περιορίζονται μόνο σε ότι είναι απαραίτητο να χρησιμοποιηθεί, η οποία λειτουργεί με το να συλλέγει λιγότερα δεδομένα για τους χρήστες ή με το να συλλέγει δεδομένα για λιγότερους χρήστες. Σκοπός της είναι να μειώσει τον αντίκτυπο των παραβιάσεων ιδιωτικότητας. Για να επιτευχθεί η ελαχιστοποίηση οι κατασκευαστές blockchain πρέπει να επιλέγουν σε μία κατά περίπτωση βάση τις πληροφορίες που χρειάζονται για την επεξεργασία καθώς και το γιατί και το πώς οι πληροφορίες αυτές θα συλλεχθούν, θα αποθηκευτούν και θα τις επεξεργαστούν. Σε ένα blockchain όλα τα παραπάνω μπορούν να επιτευχθούν με την αποθήκευση δεδομένων εκτός αλυσίδας και αφήνοντας κάθε υποκείμενο των δεδομένων να κρατάει το δικό του ιδιωτικό κλειδί, γεγονός που σημαίνει ότι οι μόνες οντότητες που θα αποφασίζουν ποια δεδομένα θα υποβάλλονται σε επεξεργασία είναι οι χρήστες. Επίσης καμία άλλη οντότητα στο blockchain δε θα έχει πρόσβαση στα δεδομένα ούτε στην επεξεργασία των δεδομένων. Η τακτική για να κρυφτούν τέτοιες πληροφορίες συναλλαγών είναι η χρήση των state channels τα οποία μπορούν να κρύψουν τις συναλλαγές εκτός της αλυσίδας και να διαμοιραστούν μόνο την τελική κατάσταση του εγγράφου στο δημόσιο καθολικό. Διαφορετικά, εάν αυτή η λύση δεν είναι δυνατό να λειτουργήσει, υπάρχει και η δυνατότητα για μία λεπτομερή συμφωνία η οποία δίνει στους χρήστες ένα χάρτη σχετικά με το πώς τα δεδομένα υφίστανται επεξεργασία, ενώ παράλληλα ζητείται και η συγκατάθεσή τους όταν χρησιμοποιούν το σύστημα.

Διαχωρισμός: Η στρατηγική αυτή απαιτεί τον λογικό ή φυσικό διαχωρισμό των δεδομένων που πρόκειται να υποβληθούν σε επεξεργασία, έτσι ώστε να καθίσταται δύσκολο να συνδυαστούν ή να συσχετιστούν με τέτοιο τρόπο που να αποκαλύπτουν προσωπικές πληροφορίες σχετικά με το υποκείμενο των δεδομένων. Δύο τεχνικές λύσεις προτείνονται σχετικά με την επεξεργασία και τον διαμοιρασμό των δεδομένων στο blockchain. Η πρώτη είναι κατακερματιστούν τα αρχεία και τα κομμάτια τους να αποθηκευτούν σε διαφορετικούς κόμβους ώστε μόνο ο ιδιοκτήτης του αρχείου να γνωρίζει που βρίσκονται τα υπόλοιπα κομμάτια. Η άλλη λύση είναι να αποθηκευτούν τα αρχεία εκτός της αλυσίδας και οι χρήστες να είναι αυτοί που θα ελέγχουν ποιος αποκτά πρόσβαση στα αρχεία.

Περίληψη: η στρατηγική αυτή επικεντρώνεται στον περιορισμό του επιπέδου της λεπτομέρειας των πληροφοριών που αποθηκεύονται, η οποία στοχεύει στην μείωση του αντικτύπου των παραβιάσεων ιδιωτικότητας. Η στρατηγική αυτή βασίζεται στη σύνοψη ή στην ομαδοποίηση οποιασδήποτε αποθήκευσης, συλλογής ή άλλης λειτουργίας σε προσωπικά δεδομένα. Τεχνικές λύσεις που μπορούν να επιτρέψουν τη λειτουργία αυτής της στρατηγικής είναι η χρήση κυκλικών υπογραφών (ring signatures), αποδείξεων μηδενικής γνώσης (zero-knowledge proof), state channels και side chains.

Απόκρυψη: Καθώς τα αρχεία σε ένα blockchain βρίσκονται σε κρυπτογραφημένη μορφή, η στρατηγική απόκρυψης απαιτείται για τα δεδομένα κεφαλίδας, για παράδειγμα τις διευθύνσεις. Τεχνικές λύσεις που χρησιμοποιούνται για την απόκρυψη διευθύνσεων και δεδομένων συναλλαγών είναι οι κυκλικές υπογραφές, οι stealth addresses, κλειδιά μίας χρήσης και η προσθήκη θορύβου στα δεδομένα.

Οι στρατηγικές που αφορούν την επεξεργασία είναι οι εξής:

Πληροφόρηση: Η διαφάνεια ως προς το ποια δεδομένα υφίστανται επεξεργασία, για ποιο λόγο και με ποιο τρόπο, είναι ένας σημαντικός πυλώνας της προστασίας δεδομένων. Για το λόγο αυτό, η στρατηγική αυτή περιλαμβάνει τακτικές για να παρέχει μία λεπτομερή συμφωνία στον χρήστη και πολιτικές συστήματος για να εξηγήσει για ποιο λόγο και με ποιο τρόπο επεξεργάζονται τα δεδομένα καθώς και ποια δεδομένα υφίστανται επεξεργασία. Για να επιτευχθεί η στρατηγική αυτή περιλαμβάνει τακτικές όπως διαφανή σχεδιασμό και τεκμηριωμένο λογισμικό καθώς και ένα ενεργό σύστημα ειδοποίησης για παραβιάσεις δεδομένων.
Έλεγχος: Μία στρατηγική ελέγχου ενσωματώνει την δυνατότητα να δίνεται στα υποκείμενα των δεδομένων ο έλεγχος να επιλέγουν, να αναβαθμίζουν και να αποσύρουν προσωπικές τους πληροφορίες. Στόχος της είναι να ρυθμίζει πώς οι χρήστες θα αποφασίζουν εάν θα χρησιμοποιήσουν ένα σύστημα και τι είδους δεδομένα θα επεξεργαστεί το σύστημα αυτό. Στην περίπτωση που υπάρχουν αρχεία σε ένα blockchain, μπορεί να επιτευχθεί με την αποθήκευση δεδομένων εκτός της αλυσίδας και ορίζοντας του χρήστες ως τους μόνους κατόχους ιδιωτικών κλειδιών, δίνοντάς τους έτσι έλεγχο επάνω στα δεδομένα τους.
Επιβολή: Αυτή η στρατηγική δηλώνει ότι μία πολιτική ιδιωτικότητας είναι απαραίτητη για τη διαφύλαξη της δέσμευσης απέναντι στην προστασία των δεδομένων του χρήστη. Από τεχνική άποψη, η διαφύλαξη της ιδιωτικότητα των δεδομένων επιτυγχάνεται με την αποθήκευση των δεδομένων εκτός αλυσίδας και διαβεβαιώνοντας ότι τα ιδιωτικά κλειδιά βρίσκονται μόνο με τους κατόχους των δεδομένων.
Παρουσίαση: Η στρατηγική αυτή στοχεύει στο να διαφυλάσσει την διαθεσιμότητα αποδείξεων για έλεγχο, καταγραφές και αναφορές σχετικά με τις πολιτικές και τεχνικούς ελέγχους αναφορικά με τις προσωπικές πληροφορίες. Τα blockchain υιοθετούν τη στρατηγική αυτή μέσω της ιδιότητάς τους να είναι μη αναστρέψιμα. Το δημόσιο καθολικό μπορεί να λειτουργήσει ως καταγραφή ή αναφορά ελέγχου για να ενημερώσει το υποκείμενο των δεδομένων σχετικά με το τι συνέβη στα δεδομένα του[164].

Εκτίμηση αντικτύπου κατά τη χρήση τεχνολογίας blockchain

Σύμφωνα με το άρθρο 35 του ΓΚΠΔ όταν ένα είδος επεξεργασίας, ιδίως με χρήση νέων τεχνολογιών και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας διενεργεί, πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα[165]. Σε μία εκτίμηση μπορεί να εξετάζεται ένα σύνολο παρόμοιων πράξεων επεξεργασίας οι οποίες ενέχουν παρόμοιους υψηλούς κινδύνους. Το ερώτημα, λοιπόν, που ανακύπτει εδώ, είναι εάν η επεξεργασία δεδομένων με τη χρήση

[164] Muhammad Al-Abdullah, Izzat Alsmadi, Ruwaida AlAbdullah and Bernie Farkas, Designing privacy-friendly data repositories: a framework for a blockchain that follows the GDPR, Digital Policy, Regulation And Governance, VOL. 22 NO. 5/6 2020, pp. 389-411
[165] ΓΚΠΔ, άρθρο 35

τεχνολογίας blockchain, υπάγεται στις περιπτώσεις που επιφέρουν υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων και πρέπει, συνεπώς, να διενεργείται εκτίμηση αντικτύπου.

Η Ελληνική Αρχή Προστασίας Δεδομένων (ΑΠΔΠΧ), δυνάμει της υπ' αριθμ. 65/2018 απόφασής της, εξέδωσε κατάλογο με τα είδη των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση για διενέργεια εκτίμησης αντικτύπου. Στον κατάλογο αυτό, τα κριτήρια για την διενέργεια ΕΑΠΔ ομαδοποιούνται στις παρακάτω τρεις κατηγορίες: 1η κατηγορία: με βάση τα είδη και τους σκοπούς επεξεργασίας, 2η κατηγορία: με βάση το είδος των δεδομένων και/ή τις κατηγορίες των υποκειμένων και 3η κατηγορία: με βάση τα πρόσθετα χαρακτηριστικά και/ή τα χρησιμοποιούμενα μέσα της επεξεργασίας. Η διενέργεια ΕΑΠΔ κρίνεται υποχρεωτική όταν πληρούται τουλάχιστον ένα από τα κριτήρια της 1ης ή της 2ης κατηγορίας. Είναι επίσης υποχρεωτική όταν συντρέχει ένα τουλάχιστον κριτήριο ως προς την 3η κατηγορία και η επεξεργασία αφορά είδη και 1ης σκοπούς επεξεργασίας της κατηγορίας, ή/και είδη δεδομένων ή/και κατηγορίες υποκειμένων της 2ης κατηγορίας. Στην 3η κατηγορία περιλαμβάνεται η καινοτόμος χρήση ή εφαρμογή νέων τεχνολογιών ή οργανωτικών λύσεων, οι οποίες μπορεί να περιλαμβάνουν νέες μορφές συλλογής και χρήσης δεδομένων, με ενδεχόμενο υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων όπως, μεταξύ άλλων και τεχνολογίες δημόσια προσπελάσιμων blockchain που περιλαμβάνουν προσωπικά δεδομένα[166].

Επιπλέον, η Αρχή Προστασίας Δεδομένων του Ηνωμένου Βασιλείου, θεωρεί ότι πρέπει να διενεργείται εκτίμηση αντικτύπου οποτεδήποτε χρησιμοποιείται κάποια καινούρια τεχνολογία[167]. Ωστόσο, αν και η τεχνολογία blockchain χαρακτηρίζεται ως νέα, βασίζεται σε καινοτομίες που εμφανίστηκαν κάποιες δεκαετίες παλαιότερα.

Διασυνοριακή ροή δεδομένων και blockchain

Διασυνοριακή επεξεργασία είναι η επεξεργασία δεδομένων προσωπικού χαρακτήρα η οποία γίνεται στο πλαίσιο των δραστηριοτήτων διάφορων εγκαταστάσεων σε περισσότερα του ενός κράτη μέλη υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία στην Ένωση όπου ο υπεύθυνος επεξεργασίας ή ο εκτελών επεξεργασία είναι εγκατεστημένος σε περισσότερα του ενός κράτη μέλη ή η επεξεργασία δεδομένων προσωπικού χαρακτήρα η οποία γίνεται στο πλαίσιο των δραστηριοτήτων μίας μόνης εγκατάστασης υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία στην Ένωση αλλά που επηρεάζει ή ενδέχεται να επηρεάσει ουσιωδώς υποκείμενα των δεδομένων σε περισσότερα του ενός κράτη μέλη[168].

Ο ΓΚΠΔ προβλέπει ότι κάθε διαβίβαση δεδομένων προσωπικού χαρακτήρα τα οποία υποβάλλονται σε επεξεργασία ή προορίζονται να υποβληθούν σε επεξεργασία μετά από τη διαβίβασή τους σε τρίτη χώρα ή διεθνή οργανισμό πραγματοποιείται

[166] Απόφαση 65/2018, ΑΠΔΧ, https://www.dpa.gr/el/enimerwtiko/prakseisArxis/katalogos-me-ta-eidi-ton-praxeon-epexergasias-poy-ypokeintai-stin

[167] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

[168] ΓΚΠΔ άρθρο 4, περ. 23

μόνο εάν οι προϋποθέσεις που θεσπίζονται στον Κανονισμό τηρούνται από τον υπεύθυνο επεξεργασίας και τον εκτελούντα την επεξεργασία, μεταξύ άλλων για περαιτέρω διαβιβάσεις δεδομένων προσωπικού χαρακτήρα από την τρίτη χώρα ή τον διεθνή οργανισμό σε άλλη τρίτη χώρα ή άλλο διεθνή οργανισμό[169].

Όσον αφορά τη ροή δεδομένων μεταξύ κρατών μελών της Ευρωπαϊκής Ένωσης, το άρθρο 1 παρ. 3 του Κανονισμού ορίζει ότι η ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα εντός της Ένωσης δεν περιορίζεται ούτε απαγορεύεται για λόγους που σχετίζονται με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

Οι διαβιβάσεις δεδομένων σε τρίτες χώρες πραγματοποιούνται σύμφωνα με το Κανονισμό, με δύο τρόπους, είτε βάσει απόφασης επάρκειας της Ευρωπαϊκής Επιτροπής ή, απουσία απόφασης επάρκειας, όταν ο υπεύθυνος της επεξεργασίας ή ο εκτελών την επεξεργασία παρέχει κατάλληλες εγγυήσεις, συμπεριλαμβανομένων εκτελεστών δικαιωμάτων και ένδικων μέσων για το υποκείμενο των δεδομένων. Απουσία είτε απόφασης επάρκειας είτε κατάλληλων εγγυήσεων, ισχύουν διάφορες παρεκκλίσεις[170].

Η έρευνα της εφαρμογής των διατάξεων του Κανονισμού που αφορούν τη διασυνοριακή ροή δεδομένων σε συστήματα blockchain έχει ιδιαίτερη σημασία καθώς οι κόμβοι στους οποίους αποθηκεύεται το καθολικό μπορεί να υπάγονται σε διαφορετικές δικαιοδοσίες, εντός και εκτός Ευρωπαϊκής Ένωσης. Σε ένα αδειοδοτημένο δίκτυο οι τοποθεσίες των κόμβων μπορούν να ελεγχθούν, ενώ αντίθετα, σε μη αδειοδοτημένα δίκτυα, αυτό είναι αδύνατο καθώς οποιοσδήποτε μπορεί να αποκτήσει πρόσβαση στο δίκτυο χωρίς την ανάγκη ύπαρξης προηγούμενης άδειας από κάποιο κεντρικό παράγοντα.

Σε περιπτώσεις όπου υπάρχουν αποφάσεις επάρκειας αναφορικά με κάποια τρίτη χώρα, η ροή των δεδομένων μπορεί να συνεχιστεί ελεύθερα μεταξύ αυτών των δικαιοδοσιών ανεξάρτητα από το ποια τεχνολογία χρησιμοποιείται και στη συγκεκριμένη περίπτωση ανεξάρτητα από το αν χρησιμοποιείται blockchain ή όχι. Ομοίως, όταν δεν υπάρχει απόφαση επάρκειας, ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία μπορούν να μεταφέρουν δεδομένα σε τρίτες χώρες μόνο όταν μπορούν να προβάλλουν τις κατάλληλες εγγυήσεις, σύμφωνα με όσα προβλέπει ο Κανονισμός.

Υπάρχει τρόπος να ξεπεραστούν οι δυσκολίες συμμόρφωσης;

Παρά τις δυσκολίες και τις ασυμφωνίες που ανιχνεύτηκαν με την ανωτέρω μελέτη σχετικά με τη συμμόρφωση μίας τεχνολογίας blockchain με τον ΓΚΠΔ, έχουν εκφραστεί απόψεις που συνηγορούν υπέρ της δυνατότητας ύπαρξης μίας «χρυσής τομής».

Σύμφωνα με τους Unal Tatar, Yasir Gokce και Brian Nussbaum οι αντιθέσεις μεταξύ του Κανονισμού και της τεχνολογίας blockchain δεν είναι πάντα άλυτες[171].

---

[169] ΓΚΠΔ άρθρο 44

[170] ΓΚΠΔ άρθρα 45 και 46

[171] *Unal Tatar, Yasir Gokce , Brian Nussbaum, Law versus technology: Blockchain, GDPR, and tough tradeoffs, Computer law & security review 38 (2020) Science Direct*

Θεωρούν πως οι αντιθέσεις αυτές μπορούν να λυθούν αν επικεντρωθούμε στα κοινά σημεία μεταξύ τους και προσαρμόζοντας την τεχνολογία blockchain σύμφωνα με τις ανάγκες του νόμου περί προστασίας των δεδομένων προσωπικού χαρακτήρα. Υπάρχει ένας μεγάλος αριθμός αρχών προστασίας δεδομένων οι οποίες παρατηρούνται και στον Κανονισμό και στα blockchain. Δίνοντας έμφαση σε αυτό που και οι δύο πλευρές προσπαθούν να επιτύχουν είναι μία καλή αρχή για το συμβιβασμό τους. Ειδικότερα και οι δύο πλευρές μοιράζονται τον στόχο της ενδυνάμωσης της ιδιωτικότητας των δεδομένων και της ασφάλειας, ωστόσο διαφέρουν ως προς τον τρόπο που προσπαθούν να τον επιτύχουν. Για παράδειγμα η διαφάνεια, ο αυξημένος ατομικός έλεγχος των δεδομένων, η ελαχιστοποίηση των δεδομένων και κρυπτογραφία είναι βασικές αρχές της τεχνολογίας blockchain οι οποίες παρατίθενται σε πολλά άρθρα του ΓΚΠΔ.

Επίσης, ενώ από την μία πλευρά η αμεταβλητότητα του καθολικού ενός blockchain φαίνεται να είναι ασύμβατη με το δικαίωμα στη διαγραφή, από την άλλη πλευρά το ίδιο ακριβώς χαρακτηριστικό εναρμονίζεται απόλυτα με την υποχρέωση για προστασία από το σχεδιασμό και εξ ορισμού του άρθρου 25 του Κανονισμού. Η αμετάβλητη και αποκεντρωμένη φύση του συστήματος διαφυλάσσει την ακεραιότητα και ακρίβεια των αρχείων που αποθηκεύονται στο καθολικό ελαχιστοποιώντας έτσι τον κίνδυνο τα δεδομένα να τροποποιηθούν παρανόμως. Ομοίως, η ακεραιότητα και η ακρίβεια των δεδομένων ανήκουν στις θεμελιώδεις αρχές που πρέπει να λάβει κανείς υπόψη όταν σχεδιάζει και αναπτύσσει μία τεχνολογία, σύμφωνα με το άρθρο 25 του Κανονισμού.

Επιπλέον η τεχνολογία blockchain ενδυναμώνει του χρήστες σε ένα μεγάλο βαθμό και τους επιτρέπει να ασκούν ατομικό έλεγχο στα προσωπικά δεδομένα που αποθηκεύονται στη βάση δεδομένων του blockchain. Αυτό σημαίνει ότι μπορούν να αποφασίζουν εάν θα μοιραστούν τα δεδομένα τους και μάλιστα στο βαθμό που απαιτείται από την εκάστοτε συναλλαγή στο blockchain. Με άλλα λόγια μπορούν να περιορίσουν τα δεδομένα στην απαραίτητη ποσότητα που απαιτείται για κάποιο συγκεκριμένο σκοπό. Αυτός είναι και ο ορισμός της ελαχιστοποίησης των δεδομένων που προβλέπεται στο άρθρο 5 του ΓΚΠΔ. Η μοναδική πρόκληση είναι το γεγονός ότι όταν τα δεδομένα εισάγονται στο καθολικό δεν μπορούν να ανακληθούν ή να «ξεχαστούν» και όχι εξαιτίας ενός συγκεντρωτικά οργανωμένου συστήματος επιβολής κανόνων αλλά εξαιτίας αρχιτεκτονικών κανόνων που βασίζονται σε ένα ψηφιακά κατασκευασμένο περιβάλλον.

Τέλος, οι πληροφορίες αποθηκεύονται στο καθολικό με έναν ανώνυμο και διαφανή τρόπο. Οι χρήστες συναλλάσσονται στην ίδια βάση δεδομένων δεν μπορούν να δουν τα προσωπικά δεδομένα των άλλων χρηστών εκτός αν τους δοθεί το ιδιωτικό κλειδί. Ωστόσο, οι πληροφορίες που αποσπώνται από τα προσωπικά δεδομένα είναι ορατές σε αυτούς και η διαφάνεια αυτή εξαλείφει την ανάγκη ύπαρξης μιας ενδιάμεση αρχής την οποία οι χρήστες δεν θα είχαν άλλη επιλογή παρά να την εμπιστευτούν. Η ανωνυμοποίηση και η διαφάνεια είναι μεταξύ των ζητημάτων και εργαλείων που και η τεχνολογία blockchain και ο ΓΚΠΔ χρησιμοποιούν για να επιτύχουν την ιδιωτικότητα και την ασφάλεια των δεδομένων.

Αφού εστιάσαμε στα κοινά σημεία του Κανονισμού με την τεχνολογία blockchain, υπάρχει η ανάγκη για μια διαφορετική προσέγγιση αναφορικά με τα σημεία ασυμβατότητας μεταξύ τους. Από τις σημαντικότερες «γκρίζες ζώνες», όπως έχει αναλυθεί ανωτέρω είναι η αδυναμία διαγραφής των δεδομένων από ένα blockchain αλλά και η υποχρέωση μία κεντρικής οντότητας η οποία έχει την ευθύνη, όπως επιβάλλεται από τον Κανονισμό, η οποία είναι αδύνατο να εφαρμοστεί σε αποκεντρωμένα συστήματα blockchain. Παρόλα αυτά, σχεδόν όλες οι ασυμβατότητες μπορούν να ξεπεραστούν, με μία πρακτική προσέγγιση από τις σχετικές δημόσιες αρχές αναγνωρίζοντας τις ιδιαιτερότητες της τεχνολογίας blockchain και δίνοντας προτεραιότητα στα κοινά σημεία της τεχνολογίας και του Κανονισμού. Η τεχνολογία blockchain μπορεί να επανασχεδιαστεί και να προσαρμοστεί στις απαιτήσεις του ΓΚΠΔ με κάποιους συμβιβασμούς. Συνεπώς η βιομηχανία του blockchain και οι κατασκευαστές του πρέπει να έχουν μία καλή γνώση και κατανόηση των αρχών και των στόχων του Κανονισμού έτσι ώστε να προσθέσουν νέα χαρακτηριστικά και να προσαρμόζουν την τεχνολογία στις απαιτήσεις του Κανονισμού.

Προκειμένου να προσαρμοστεί η τεχνολογία blockchain με τις απαιτήσεις του δικαιώματος διαγραφής, οι κατασκευαστές πρέπει να καταλήξουν σε μία λύση που επιτρέπει τη διαγραφή προσωπικών δεδομένων από το καθολικό. Ωστόσο, αυτή η λύση πρέπει να μην είναι επιβλαβής αναφορικά με την ακεραιότητα της αλυσίδας, τα δεδομένα, δηλαδή, πρέπει να αφαιρούνται από το καθολικό χωρίς να επηρεάζεται η σταθερότητα του blockchain. Αυτό σημαίνει ότι πρέπει να παραμένουν άθικτες οι συναρτήσεις κατακερματισμού που συνδέουν τα μπλοκ, ενώ ταυτόχρονα επιτρέπουν τη διαγραφή δεδομένων από αυτά. Αυτή η αναθεωρήσιμη αρχιτεκτονική των blockchain μπορεί να βασιστεί σε chameleon hashes, οι οποίες επιτρέπουν αποτελεσματικά τον καθορισμό της σύγκρουσης της συνάρτησης κατακερματισμού, δεδομένης της ύπαρξης μιας μυστική πληροφορίας. Το πρωτότυπο σύστημα που αναπτύχθηκε από τους Ateniese κλπ, επιτρέπει την ύπαρξη κατόχου ενός μυστικού κλειδιού, ο οποίος μπορεί να είναι ένας miner, ενός κεντρικού ελεγκτή ή αρκετών αρχών που μοιράζονται το μυστικό κλειδί[172]. Η Accenture έχει δημιουργήσει μία καινούρια δυνατότητα που επιτρέπει στην τεχνολογία blockchain να είναι επεξεργάσιμη κάτω από ακραίες συνθήκες. Η δυνατότητα αυτή επιτρέπει στις επιχειρήσεις να επιλύουν ανθρώπινα λάθη, να εφαρμόζουν νόμιμες και ρυθμιστικές απαιτήσεις και να αντιμετωπίζουν κακόβουλα ζητήματα, διατηρώντας ταυτόχρονα τα κρυπτογραφικά χαρακτηριστικά[173].

Μία άλλη προσπάθεια συμμόρφωσης με τον Κανονισμό επιτυγχάνεται με τη διατήρηση δεδομένων σε αποθήκευση εκτός αλυσίδας. Με αυτή τη λύση τα δεδομένα πρέπει να αποκοπούν από κάθε άλλα δεδομένα συναλλαγής και να τοποθετηθούν σε ξεχωριστή αποθήκευση εκτός της αλυσίδας. Η αυθεντικότητα των δεδομένων μπορεί να διαφυλαχθεί με τη χρήση αντίστοιχων συναρτήσεων

[172] Giuseppe Ateniese, and others 'Redactable blockchain– or – rewriting history in bitcoin and friends' (IEEE European Sympo-sium on Security and Privacy, 2017

[173] https://www.accenture.com/gr-en/insight-editing-uneditable-blockchain

κατακερματισμού που αποθηκεύονται στο δίκτυο του blockchain[174]. Τα πρωτόκολλα μπορούν να δημιουργηθούν με τέτοιο τρόπο ώστε να επιτρέπεται η διαγραφή προσωπικών δεδομένων που έχουν αποθηκευτεί εκτός αλυσίδας, χωρίς να επηρεάζεται η σταθερότητα της αλυσίδας. Η διαγραφή των δεδομένων που έχουν αποθηκευτεί εκτός αλυσίδας θα καταστήσει το hash value της συνάρτησης κατακερματισμού άσκοπο. Ωστόσο, η λύση αυτή ανατρέπει τα πλεονεκτήματα της αποθήκευσης δεδομένων στο καθολικό με μη αναστρέψιμο, ασφαλή και διαφανή τρόπο, καθώς το blockchain μπορεί να εκτεθεί σε ευπάθειες της αποθήκευσης εκτός αλυσίδας και πιθανότατα στην ανάγκη ύπαρξης τρίτων μερών, ένα από τα κύρια πράγματα που προσπαθεί ν αποφύγει η τεχνολογία blockchain.

Έχει προταθεί η χρήση μίας κρυφής διεύθυνσης η οποία χρησιμοποιεί μία συναλλαγή "μίας χρήσεως" που βασίζεται σε κλειδιά "μίας χρήσεως" στα οποία έχει εφαρμοστεί hash. Για παράδειγμα, το κρυπτονόμισμα montero κρύβει τον παραλήπτη της συναλλαγής, δημιουργώντας μία καινούρια διεύθυνση και ένα μυστικό κλειδί. Η χρήση λογαριασμών μία χρήσης για συναλλαγές προβλέπει ότι κάθε συναλλαγή πρέπει να αδειάζει πλήρως έναν ή περισσότερους λογαριασμούς και να δημιουργεί ένα ή περισσότερους καινούριους λογαριασμούς[175].

Κρυπτογραφικές έρευνες έχουν αναπτύξει "αποδείξεις μηδενικής γνώσης" (zero-knowledge proofs) οι οποίες παρέχουν μία δυαδική αληθή/λανθασμένη απάντηση χωρίς να παρέχουν πρόσβαση στα υποκείμενα δεδομένα. Το κρυπτονόμισμα Zcash βασίζεται στη διαδικασία αυτή για να διασφαλίσει ότι, ακόμα και αν οι συναλλαγές γίνονται σε δημόσιο blockchain, οι λεπτομέρειές τους παραμένουν κρυφές[176].

Μία άλλη πιθανή λύση θα ήταν η 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. Αλγόριθμοι παρόμοιοι με αυτό το μοντέλο έχουν ήδη καθοριστεί για τα blockchain του Bitcoin και του Ethereum. Μάλιστα, η Ομάδα εργασίας του άρθρου 29, έχει ήδη αναγνωρίσει ότι, εφόσον έχουν δοθεί απαραίτητες εγγυήσεις, η προσθήκη θορύβου μπορεί να είναι μία αποδεκτή μέθοδος ανωνυμοποίησης δεδομένων[177].

Άλλες επιλογές που δοκιμάζονται περιλαμβάνουν κανάλια κατάστασης (state channels), τα οποία επιτρέπουν στους χρήστες να κάνουν πολλαπλές συναλλαγές σε ένα blockchain, χωρίς να τις συμπεριλαμβάνουν όλες στο blockchain. Σε ένα παραδοσιακό state channel μόνο δύο συναλλαγές προστίθενται στο blockchain, αλλά μεταξύ των συμμετεχόντων μπορεί να γίνει απεριόριστος αριθμός συναλλαγών[178]. Από την άλλη πλευρά οι κυκλικές υπογραφές (ring signatures), κρύβουν συναλλαγές

[174] Athena Bourka and Prokopios Drogkaris , 'Recommendations on Shaping Technology According to GDPR Provisions', ENISA 2018

[175] Stealth Address https://getmonero.org/resources/moneropedia/stealthaddress.html

[176] Zcash, 'What are zk-SNARKs?' https://z.cash/technology/zksnarks.html

[177] Γνώμη 05/2014, τεχνικές ανωνυμοποίησης

[178] https://www.talentica.com/blogs/state-channels-an-introduction-to-off-chain-transactions/#:~:text=A%20state%20channel%20is%20a,cryptographically%20provable%20on%20the%20blockchain.

μέσα σε άλλες συναλλαγές ενώνοντας μία μοναδική συναλλαγή με πολλαπλά ιδιωτικά κλειδιά ακόμα και αν ένα μόνο από αυτά ξεκίνησε την συναλλαγή. Η υπογραφή αποδεικνύει ότι ο υπογράφων έχει ένα ιδιωτικό κλειδί που αντιστοιχεί σε ένα άλλο από ένα συγκεκριμένο σετ δημοσίων κλειδιών, χωρίς να αποκαλύπτει όμως σε ποιο[179].

Η ανάγκη για έναν αναγνωρίσιμο υπεύθυνο επεξεργασίας δεδομένων για λόγους λογοδοσίας, δεν είναι τόσο μεγάλο πρόβλημα για εφαρμογές που χρησιμοποιούν blockchain ως backend, όπως τα έξυπνα συμβόλαια (π.χ. τα έξυπνα συμβόλαια του Ethereum). Εφόσον οι ιδιοκτήτες αυτών των εφαρμογών συλλέγουν τα προσωπικά δεδομένα και αποφασίζουν με ποιο τρόπο και με ποιες προϋποθέσεις θα επεξεργαστούν αυτά τα δεδομένα, μπορούν να θεωρηθούν ως υπεύθυνοι επεξεργασίας. Υπάρχουν επίσης και έξυπνα συμβόλαια που επιτρέπουν στους χρήστες την σε πραγματικό χρόνο επεξεργασία των δεδομένων χωρίς να είναι απαραίτητη η αποθήκευσή τους. Υποστηρίζεται ότι το χαρακτηριστικό αυτό αντιμετωπίζει το ζήτημα της ανάγκης ύπαρξης ενός αναγνωρίσιμου υπευθύνου επεξεργασίας, εφόσον η επεξεργασία λαμβάνει χώρα με επαρκώς κρυπτογραφημένο τρόπο. Ένα παράδειγμα αυτής της προσέγγισης είναι η εκτός αλυσίδας αποθήκευση των προσωπικών δεδομένων. Εάν τα δεδομένα που αποθηκεύονται εκτός της αλυσίδας δεν είναι μέρος του blockchain, η πλευρά που τα ελέγχει μπορεί να θεωρηθεί ως υπεύθυνος επεξεργασίας, εφόσον έχει τη δυνατότητα να καθορίζει τους σκοπούς και τα μέσα της επεξεργασίας.

Dynamic Consent Management Systems βασισμένα σε έξυπνα συμβόλαια

Τα Dynamic consent management συστήματα (DCM) είναι ένα καινοτόμο μέσο που έχουν ως στόχο τη μεγαλύτερη συμπερίληψη των ατόμων στη χρήση των προσωπικών τους πληροφοριών. Στοχεύουν επίσης στην αντιμετώπιση των περιορισμών που θέτει η έντυπη μορφή συγκατάθεσης και άλλες στατικές μέθοδοι συγκατάθεσης οι οποίες επιτρέπουν λιγότερες δυνατότητες και μικρότερη ευελιξία αναφορικά με τη δυνατότητα των ατόμων να καθορίζουν και να διαχειρίζονται τις προτιμήσεις συγκατάθεσής τους. Η βασική ιδέα των DCM είναι να επιστρέψουν τον έλεγχο στους χρήστες ώστε να διαχειρίζονται αποφασιστικά τη συγκατάθεσή τους στη συλλογή και χρήση των δεδομένων προσωπικού χαρακτήρα που τους αφορούν.

Τα συμβατικά DCM δεν μπορούν να προσφέρουν την απαιτούμενη από τον ΓΚΠΔ διαφάνεια, λογοδοσία, ασφάλεια και ιδιωτικότητα, καθώς βασίζονται σε έμπιστους τρίτους. Ωστόσο, διαθέτουν τη δυναμική για να αντιμετωπίσουν προκλήσεις διασυνοριακές, σε ποικίλους τομείς και προσκλήσεις που αφορούν το διαμοιρασμό δεδομένων μεγάλης κλίμακας.

Προκειμένου τα συστήματα αυτά να ανταποκρίνονται στις απαιτήσεις του Κανονισμού και να παρέχουν την απαραίτητη ασφάλεια και προστασία της ιδιωτικότητας, έχει προταθεί ένα DCM που βασίζεται στην αρχιτεκτονική των έξυπνων συμβολαίων και υποστηρίζεται από τεχνολογία blockchain με σκοπό την νόμιμη χρήση δεδομένων προσωπικού χαρακτήρα, που συμμορφώνεται με το

[179] https://www.getmonero.org/resources/moneropedia/ringsignatures.html

ΓΚΠΔ[180]. Το προτεινόμενο σύστημα θέτει στο επίκεντρο τον χρήστη και αξιοποιεί τα έξυπνα συμβόλαια για επιτρέψει στους χρήστες να αναλάβουν τον έλεγχο της συγκατάθεσής τους σχετικά με την συλλογή και χρήση των δεδομένων τους καθ' όλη τη διάρκεια του κύκλου ζωής των δεδομένων. Η συγκατάθεση μπορεί να δίνεται και να ελέγχεται από τους χρήστες με την ανίχνευση οποιασδήποτε καταγραφής στο blockchain. Οι χρήστες έχουν τη δυνατότητα να ειδοποιούνται σχετικά με ρήτρες στις συμφωνίες συγκατάθεσης και μπορούν να αποσύρουν τη σχετική συγκατάθεσή τους. Στο συγκεκριμένο σύστημα χρησιμοποιούνται αποκεντρωμένοι IPFS κόμβοι[181], για την αποθήκευση δεδομένων εκτός της αλυσίδας, ενώ παράλληλα το ιστορικό των συναλλαγών και τα δεδομένα καταγραφών εισόδου, αποθηκεύονται στο blockchain για να ενισχύεται η εμπιστοσύνη και να παραμένουν τα δεδομένα απαραβίαστα, να παρέχεται λογοδοσία και ιχνηλασιμότητα.

Ένα πρότυπο του συστήματος σχεδιάστηκε και εφαρμόστηκε στην πλατφόρμα blockchain του Quorum προκειμένου να διευκρινιστούν οι δυνατότητές του. Οι χρήστες μπορούν να εκφράζουν την συγκατάθεσή τους με πολλούς τρόπους, όπως συμπληρώνοντας μία φόρμα ή επιλέγοντας ένα κουτί σε κάποια ιστοσελίδα. Από την πλευρά τους, οι εκτελούντες την επεξεργασία ζητούν την συγκατάθεση σε κάποια συγκεκριμένο σύνολο δεδομένων, στέλνοντας το αίτημά τους, το οποίο το επεξεργάζεται το σύστημα και το καταγράφει στο blockchain, ενώ αμέσως μετά το υποκείμενο των δεδομένων ειδοποιείται για την επιτυχή εκτέλεση του. Το αίτημα συγκατάθεσης περιέχει τα αναγνωριστικά του υποκείμενου των δεδομένων και του αποστολέα του αιτήματος, τους σκοπούς, την περίοδο και τη νομική βάση για τη συλλογή και τη χρήση των δεδομένων. Αφού λάβει το αίτημα, το υποκείμενο των δεδομένων, αποφασίζει ελεύθερα εάν θα συμφωνήσει ή θα διαφωνήσει, στέλνοντας ένα αίτημα απάντησης στον αποστολέα του αιτήματος συγκατάθεσης. Η διαδικασία λήγει με τη δημιουργία ενός συμβολαίου συμφωνίας για συγκατάθεση που δημοσιεύεται στο blockchain κατόπιν επιτυχούς εκτέλεσης της συναλλαγής. Το υποκείμενο των δεδομένων μπορεί να ανακαλέσει την συγκατάθεση οποιαδήποτε στιγμή, όταν για παράδειγμα, ο λόγος για τον οποίο δόθηκε η συγκατάθεση δεν είναι πλέον έγκυρος ή όταν οι ρήτρες της συμφωνίας παραβιάζονται. Το υποκείμενο των δεδομένων ξεκινάει επιλέγοντας την ανάκληση της συγκατάθεσης και υποβάλλοντας ένα αίτημα για έγκριση στον αντίστοιχο υπεύθυνο επεξεργασίας (ή στους υπεύθυνους επεξεργασίας). Αφού ο αίτημα εγκριθεί, η συγκατάθεση ανακαλείται αλλάζοντας την κατάσταση της ως άκυρη αμέσως μετά την επιτυχή ολοκλήρωση της συναλλαγής. Για την άσκηση του δικαιώματος διαγραφής με τη χρήση έξυπνου συμβολαίου, οι χρήστες μπορούν να υποβάλλουν αίτημα διαγραφής των δεδομένων τους που έχουν αποθηκευτεί εκτός της αλυσίδας, όμως η καταγραφή αυτών των συναλλαγών παραμένει στο καθολικό.

Αναφορικά με την ασφάλεια και την προστασία της ιδιωτικότητας που παρέχει το σύστημα, αυτές βασίζονται και επεκτείνονται σε εξελιγμένα

[180] Merlec, M.M., Lee, Y.K., Hong, S.-P., In, H.P. A Smart Contract-Based Dynamic Consent Management System for Personal Data Usage under GDPR. Sensors 2021, 21, 7994, https://doi.org/10.3390/s21237994

[181] https://en.wikipedia.org/wiki/InterPlanetary_File_System

χαρακτηριστικά της αδειοδοτημένης πλατφόρμας blockchain του Quorum. Ο κώδικας που εφαρμόστηκε αναλύθηκε επιτυχώς και επιβεβαιώθηκε με τη χρήση εργαλείων επιβεβαίωσης ακριβούς ευαλωττότητας. Το σύστημα είναι ασφαλές αναφορικά με τις κοινώς γνωστές ευαλωττότητες.

Έρευνες συμβατών με τον ΓΚΠΔ blockchain

Πιστοποιητικό εμβολιασμού κατά της COVID-19 βασισμένο σε τεχνολογία blockchain

Σε πρόσφατη έρευνα παρουσιάστηκε το πλαίσιο για ένα συμβατό με τον ΓΚΠΔ πιστοποιητικό εμβολιασμού κατά της ασθένειας COVID-19, βασισμένο σε τεχνολογία blockchain, προκειμένου να διευκολυνθούν οι μετακινήσεις και τα ταξίδια, παρέχοντας ένα διεθνώς χρησιμοποιούμενο, προσβάσιμο και ισχυρό αποδεικτικό εμβολιασμού[182].

Ένα τέτοιο διαβατήριο έχει ως σκοπό να επιτρέπει στις τοπικές αρχές να επιβεβαιώνουν την κατάσταση εμβολιασμού ενός ταξιδιώτη. Αρχικά προβλέπεται η χρήση ενός αδειοδοτημένου blockchain το οποίο θα επιτρέπει συγκεκριμένες ενέργειες να γίνονται από συγκεκριμένους ταυτοποιήσιμους φορείς. Περιλαμβάνει επίσης τη χρήση έξυπνων συμβολαίων κάθε φορά που μία αρχή μετανάστευσης θέλει να επιβεβαιώσει τις λεπτομέρειες του εμβολιασμού. Το γενικότερο κατασκευαστικό πλαίσιο του blockchain αυτού βασίζεται στην ανάγκη κάθε πολίτης που πρόκειται να αποκτήσει ένα διαβατήριο εμβολιασμού για ταξιδιωτικούς σκοπούς, να πρέπει να καταχωρηθεί ως εμβολιασμένος στην τοπική υγειονομική αρχή. Μετά τον εμβολιασμό του, τα απαραίτητα δεδομένα καταγράφονται σε βάση δεδομένων εκτός της αλυσίδας. Σε κάθε πιθανό ταξιδιώτη δίνεται ένα κωδικός QR μαζί με το διαβατήριο, τον οποίο λαμβάνει και ηλεκτρονικά. Όταν ζητηθεί ο κωδικός μπορεί να σκαναριστεί για την επιβεβαίωση των λεπτομερειών του εμβολιασμού.

Αναφορικά με το δεδομένα που καταγράφονται και αποθηκεύονται εντός και εκτός αλυσίδας, κάθε αρχή διαθέτει διαφορετικά δικαιώματα πρόσβασης σε αυτά. Έτσι, οι αρχές μετανάστευσης έχουν δικαίωμα να διαβάσουν τις καταγραφές, ωστόσο οι αρχές εμβολιασμού έχουν την δυνατότητα να δημιουργήσουν να διαβάσουν και να διαγράψουν τις καταγραφές. Η δυνατότητα διαγραφής αφορά μόνο στα δεδομένα που αποθηκεύονται εκτός της αλυσίδας, όταν όμως εκτελείται μία τέτοια διαδικασία, θα γίνει και η αντίστοιχη λογική διαγραφή των δεδομένων που αποθηκεύονται στο blockchain.

Ανάλογα με τους κανονισμούς που ακολουθεί κάθε κράτος, οι πολίτες προτεραιοποιούνται και εμβολιάζονται, λαμβάνοντας ένα αναγνωριστικό εμβολιασμού (vaccination ID). Μόλις ο χρήστης λάβει το αναγνωριστικό οι προϋποθέσεις συγκατάθεσης εισάγονται με μορφή κώδικα σε ένα έξυπνο συμβόλαιο, το οποίο μπορεί να περιλαμβάνει και άλλους όρους όπως για παράδειγμα την περίοδο αποθήκευσης των δεδομένων. Τα δεδομένα του

[182] Haque, A.B.; Naqvi, B., Islam, A.K.M.N.; Hyrynsalmi, S., Towards a GDPR-Compliant Blockchain-Based COVID Vaccination Passport. Appl. Sci. 2021, 11, 6132., https://doi.org/10.3390/app11136132

εμβολιασμού μπορούν να διατηρηθούν όσο καιρό απαιτείται από τις υγειονομικές αρχές. Ο χρόνος διατήρησής τους πρέπει να συμπεριληφθεί στο έξυπνο συμβόλαιο.

Κατά τη διάρκεια του εμβολιασμού, αναγνωριστικές πληροφορίες του ατόμου όπως το όνομα, ο αριθμός διαβατηρίου, πληροφορίες επικοινωνίας κλπ., αποθηκεύονται εκτός της αλυσίδας. Αυτό ενισχύεται με απαραίτητα εργαλεία ελέγχου πρόσβασης για την ενίσχυση της ασφάλειας. Παρόλα αυτά ο υπεύθυνος επεξεργασίας στο κέντρο διενέργειας του εμβολιασμού αποθηκεύει στο blockchain δύο είδη δεδομένων, αφενός το hash του αναγνωριστικού του εμβολιασμού και του αριθμού διαβατηρίου και αφετέρου την ημερομηνία της κάθε δόσης.

Όταν ένας πολίτης ταξιδεύει παρουσιάζει τον κωδικό QR στο προσωπικό της αρχής μετανάστευσης. Με το σκανάρισμα του κωδικού, ανακτώνται οι σχετικές πληροφορίες εμβολιασμού μαζί με το hash, από την τοπική αποθήκη εκτός αλυσίδας. Το hash επιβεβαιώνεται με τη χρήση έξυπνου συμβολαίου το οποίο το συγκρίνει με αυτό που έχει αποθηκευτεί εντός του αδειοδοτημένου blockchain. Εάν αυτά ταιριάζουν, το blockchain επιστρέφει τις ημερομηνίες εμβολιασμού μαζί με την επιβεβαίωση.

Η προτεινόμενη από την έρευνα αρχιτεκτονική, χρησιμοποιεί έξυπνα συμβόλαια για την πρόσβαση στα δεδομένα εμβολιασμού. Οι ενδιαφερόμενες τοπικές αρχές μπορούν να ανακτήσουν τα δεδομένα αυτά με τη χρήση των έξυπνων συμβολαίων. Από άποψη συμμόρφωσης με τον Κανονισμό, και ο χρήστης και οι αρχές ενημερώνονται για την ανάκτηση των δεδομένων γεγονός που συμμορφώνεται με τις επιταγές του άρθρου 5 του Κανονισμού. Οι όροι συγκατάθεσης για την επεξεργασία των δεδομένων περιλαμβάνονται σε μορφή κώδικα στα έξυπνα συμβόλαια. Όταν ο εμβολιασθείς καταγράφεται από την αρχή εμβολιασμού, συλλέγεται και η συγκατάθεσή του. Έτσι επιτυγχάνεται και η συμμόρφωση με το άρθρο 7 του Κανονισμού που αφορά τις προϋποθέσεις συγκατάθεσης όπως έχουν αναφερθεί αναλυτικά σε προηγούμενο κεφάλαιο. Προβλέπεται επιπλέον και η δυνατότητα άσκησης των δικαιωμάτων στη διαγραφή και στη διόρθωση των δεδομένων. Οποτεδήποτε επιθυμεί ένας εμβολιασθείς μπορεί να απευθύνει σχετικό αίτημα προς τον υπεύθυνο επεξεργασίας, το οποίο ικανοποιείται. Αυτό επιτυγχάνεται με την αποθήκευση των αυθεντικών δεδομένων εκτός της αλυσίδας και αποθήκευση εντός της αλυσίδας των δεδομένων που αποδεικνύουν την ύπαρξή τους. Τα δεδομένα εκτός και εντός αλυσίδας συνδέονται μεταξύ τους με έναν σύνδεσμο. Κάθε φορά που ένας χρήστης ζητά τη διαγραφή τω δεδομένων του, ο σύνδεσμος αυτός καταστρέφεται προκαλώντας λογική διαγραφή. Μετά τη λογική διαγραφή, διαγράφονται επίσης και τα δεδομένα που αποθηκεύονται εκτός της αλυσίδας, με αποτέλεσμα να μην υπάρχει καμία πληροφορία ταυτοποίησης εκτός αλυσίδας. Παράλληλα στο blockchain, ούτως η άλλως αποθηκεύονται μόνο τα hash τα οποία είναι μη αναστρέψιμα και είναι αδύνατον να ανακτηθούν δεδομένα γνωρίζοντας το hash.

Τέλος, υπεύθυνοι επεξεργασίας δεδομένων στο συγκεκριμένο σύστημα μπορούν να είναι κάθε κόμβοι, ενώ σε κάποιες περιπτώσεις και οι miners όταν έχουν φτάσει την ανώτατη οικονομική κατάσταση. Εφόσον χρησιμοποιούνται έξυπνα

συμβόλαια, οι προγραμματιστές των συμβολαίων θεωρούνται ως εκτελούντες την επεξεργασία, όπως επίσης και οι miners που επικυρώνουν τα μπλοκ.

Πιστοποίηση και επαλήθευση ακαδημαϊκών πληροφοριών με ταυτόχρονη συμμόρφωση με τον ΓΚΠΔ, βασισμένη στην τεχνολογία blockchain.

Σε πρόσφατη μελέτη προτάθηκε, για την αντιμετώπιση της εμφάνισης πλαστών τίτλων σπουδών και πιστοποιητικών στην εκπαίδευση, η χρήση τεχνολογίας blockchain η οποία θα προσφέρει την έμπιστη καταγραφή και επιβεβαίωση των πληροφοριών, σεβόμενη ταυτόχρονα τις επιταγές του ΓΚΠΔ[183].

Το προτεινόμενο από την έρευνα μοντέλο μπορεί να εφαρμοστεί σε πολλές περιπτώσεις όπως η έκδοση πιστοποιητικών και διαχείριση των ακαδημαϊκών πληροφοριών, εγγραφή σε όλα τα είδη εκπαίδευσης (επίσημη και ανεπίσημη), παρακολούθηση της αξίας των ικανοτήτων, καταγραφή των αποκτηθεισών ακαδημαϊκών πιστωτικών μονάδων κλπ.

Το μοντέλο επίσης προστατεύει και κρατά τα προσωπικά δεδομένα ασφαλή, συμμορφούμενο με τον ΓΚΠΔ ακόμα και στην περίπτωση που ένα εκπαιδευτικό ίδρυμα εξαφανίζεται. Η πρόταση είναι κλιμακούμενη και έχει την ικανότητα να εφαρμόζεται ικανοποιητικά χρησιμοποιώντας τις διαθέσιμες τεχνολογίες, οι οποίες με τη σειρά τους, εγγυώνται τη δυναμική του εφαρμογή και βιωσιμότητα. Για την προστασία των προσωπικών ακαδημαϊκών δεδομένων, λαμβάνονται υπόψη οι επιταγές του άρθρου 6 του ΓΚΠΔ, που αφορούν τη νομιμότητα της επεξεργασίας των δεδομένων, όταν δεν μπορούν να εφαρμοστούν άλλοι νόμοι ή κανονισμοί. Για το λόγο αυτό, το προτεινόμενο σύστημα, δίνει στα υποκείμενα των δεδομένων τη δυνατότητα να ελέγχουν την πρόσβαση στα προσωπικά τους δεδομένα, να διαμοιράζονται μόνο ένα μικρό μέρος των δεδομένων τους ανάλογα με τα ενδιαφέροντά τους, να ειδοποιούνται όποτε τα δεδομένα υφίστανται επεξεργασία και να ανακτούν και να λαμβάνουν τα δεδομένα τους σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα μορφότυπο, σύμφωνα με το άρθρο 20 ΓΚΠΔ. Επιπλέον, υποστηρίζει την δυνατότητα λήψης και ανάκλησης αδειών προς κάποιο συγκεκριμένο φορέα, σύμφωνα με το άρθρο 7παρ. 3 ΓΚΠΔ, ενώ η δυνατότητα άσκησης του δικαιώματος διαγραφής λαμβάνεται επίσης υπόψη. Τέλος, εναρμονίζεται πλήρως με την υποχρέωση για προστασία των δεδομένων από το σχεδιασμό, σύμφωνα με το άρθρο 25 του ΓΚΠΔ.

Ο κυρίως σχεδιασμός του προτεινόμενου μοντέλου αποτελείται από ένα κυρίως blockchain και έναν ακαθόριστο αριθμό ιδιωτικών blockchain που είναι συνδεδεμένα στο κυρίως. Κάθε blockchain θα σχεδιαστεί από αναγνωρισμένα και εξουσιοδοτημένα εκπαιδευτικά ιδρύματα. Τα μέλη του κυρίως blockchain θα είναι οργανισμοί που σχετίζονται με τον τομέα της εκπαίδευσης σε εθνική και διεθνή κλίμακα, ενώ τα μέλη των διαφορετικών ιδιωτικών blockchain θα είναι τοπικά εκπαιδευτικά ιδρύματα. Παρόλα αυτά, οι εθνικοί και διεθνείς οργανισμοί μπορούν να είναι επίσης μέλη των ιδιωτικών blockchain με διαφορετικό ρόλο. Κάθε ένα από

[183] Delgado-von-Eitzen, C.; Anido-Rifón, L.; Fernández-Iglesias, M.J. Application of Blockchain in Education: GDPR-Compliant and Scalable Certification and Verification of Academic Information. Appl. Sci. **2021**, 11, 4537. https://doi.org/10.3390/app11104537

τα ιδιωτικά blockchain θα είναι ανεξάρτητα από τα υπόλοιπα και θα είναι αυτόνομα ανάλογα με γεωγραφικά, οικονομικά ή άλλα κριτήρια. Κάθε ένα από αυτά, θα στέλνει περιοδικά, συγκεκριμένες συναλλαγές στο κυρίως blockchain. Με αυτή την προσέγγιση, η απαιτητική διαδικασία της έκδοσης των ακαδημαϊκών πληροφοριών επιτυγχάνεται διαμοιράζοντάς την σε διαφορετικά ιδιωτικά blockchain και ακολουθώντας τα πιο σύγχρονα μοντέλα κλιμάκωσης στις τεχνολογίες blockchain (Polkadot, Ethereum, Hyperledger Fabric). Το μοντέλο που χρησιμοποιούν τα εκπαιδευτικά ιδρύματα αυτή τη στιγμή, περιλαμβάνει τη διαχείριση των δεδομένων από τα ίδια τα ιδρύματα, γεγονός που θα περίμενε κανείς ότι πρόκειται να αλλάξει. Ωστόσο, για λόγους συμμόρφωσης με τον ΓΚΠΔ, τα δεδομένα που εκδίδονται πρόκειται να αποθηκεύονται στις βάσεις δεδομένων των οργανισμών και όχι στη βάση δεδομένων του blockchain. Για την περίπτωση όπου κάποιο ίδρυμα διακόψει την λειτουργία του, προβλέπεται η δημιουργία ενός νέου ιδιωτικού blockchain από επιλεγμένους αναγνωρισμένους οργανισμούς που είναι συνδεδεμένοι σε ένα ιδιωτικό σύστημα IPFS, το οποίο θα αποθηκεύει τα ¨ορφανά¨ δεδομένα.

Η διαδικασία της έκδοσης ακαδημαϊκών πληροφοριών ξεκινάει όταν ένα ίδρυμα εκδίδει κάποιο δίπλωμα που περιέχει δεδομένα του κατόχου (όνομα, επίθετο, βαθμός, ημερομηνία κλπ.) με κάποια συγκεκριμένη δομή και με τη μορφή ενός δέντρου Merkle. Και το ίδρυμα και ο κάτοχος του τίτλου εκπροσωπούνται από λογαριασμούς blockchain. Όλες οι πληροφορίες του τίτλου καταγράφονται από το ίδρυμα στην ιδιωτική του βάση δεδομένων και κρυπτογραφούνται με ένα μυστικό κλειδί που γνωρίζουν μόνο το ίδρυμα και ο κάτοχος του τίτλου. Το ίδρυμα συνδέεται επίσης σε ένα ιδιωτικό blockchain και στέλνει μία συναλλαγή που περιλαμβάνει έναν δείκτη για την καταγραφή στην εσωτερική του βάση δεδομένων, την τοποθεσία του του σημείου πρόσβασης του server της βάσης δεδομένων (όνομα κεντρικού υπολογιστή και τη θύρα), τη ρίζα Merkle των πληροφοριών που κρυπτογραφήθηκαν μαζί με το ιδιωτικό κλειδί, την επιβεβαίωση ότι οι πληροφορίες είναι έγκυρες και μία λίστα με λογαριασμούς που μπορούν να έχουν πρόσβαση σε αυτές. Τα ανωτέρω δεδομένα καταγράφονται ως μία συναλλαγή. Ο εκδότης μεταδίδει, χρησιμοποιώντας ένα ασφαλές κανάλι, στον κάτοχο το ολοκληρωμένο πιστοποιητικό, το κρυπτογραφημένο δέντρο Merkle, την επιβεβαίωση και τη συναλλαγή. Το ίδρυμα πρέπει να καταγράψει κάθε ενέργεια σε ένα τοπικό αρχείο, στο οποίο πρέπει επίσης να γίνει hash και να αποσταλεί στο blockchain, για να μπορεί να εξασφαλίζεται η λογοδοσία σε κάθε περίπτωση τροποποίησης. Το ιδιωτικό έξυπνο συμβόλαιο είναι το μοναδικό σημείο εξωτερικής πρόσβασης στα αρχεία της τοπικής βάσης δεδομένων του ιδρύματος, το οποίο επιβεβαιώνει ότι ο λογαριασμός που ζητά πρόσβαση, έχει δικαίωμα να την αποκτήσει. Περιοδικώς, κάθε ιδιωτικό blockchain μεταδίδει στο κυρίως δίκτυο τις καταγεγραμμένες πληροφορίες οι οποίες χωρίζονται στο έξυπνο συμβόλαιο που περιλαμβάνει την κρυπτογραφημένη ρίζα Merkle καθώς και πληροφορίες ότι τα δεδομένα είναι έγκυρα και στις πληροφορίες που αφορούν η λίστα με τους λογαριασμούς που έχουν δικαίωμα πρόσβασης.

Σε περίπτωση που κάποιο ίδρυμα επιθυμεί να τροποποιήσει τα δεδομένα, πρέπει να το κάνει στην εσωτερική του βάση δεδομένων, να δημιουργήσει ένα νέο πιστοποιητικό και να κάνει μία νέα μετάδοση στο blockchain, το οποίο θα

δημιουργήσει μία νέα συναλλαγή. Η ίδια διαδικασία μπορεί να ακολουθηθεί και στην περίπτωση επιβεβαίωσης ή διαγραφής δεδομένων.

Το προτεινόμενο από την έρευνα σύστημα είναι σχεδιασμένο με βάση την αρχή για προστασία δεδομένων από τον σχεδιασμό και εξ ορισμού, συμμορφούμενο έτσι με τις επιταγές του ΓΚΠΔ. Χρησιμοποιώντας το σύστημα αυτό, το υποκείμενο των δεδομένων χορηγεί ρητώς τη συγκατάθεσή του η οποία καταγράφεται κάθε φορά που ένας κάτοχος μεταδίδει προς το ίδρυμα τον blockchain λογαριασμό του για να συνδεθεί με τις εκδοθείσες ακαδημαϊκές πληροφορίες. Αφού εκδοθούν οι πληροφορίες από το ίδρυμα, το υποκείμενο των δεδομένων έχει τη δυνατότητα να επιτρέψει ή να αποσύρει την πρόσβαση σε όλα ή σε συγκεκριμένα δεδομένα σε οποιοδήποτε τρίτο μέρος, απλώς προσθέτοντας ή διαγράφοντας τον λογαριασμό του σε ένα έξυπνο συμβόλαιο.

Ένα GDPR compliant IOV (Internet of Vehicles) σύστημα διαμοιρασμού πληροφοριών εντοπισμού που βασίζεται στην τεχνολογία blockchain.

Σε πρόσφατη έρευνα, προτάθηκε η χρήση ενός συστήματος για την ενσωμάτωση, συλλογή, αποθήκευση και διαχείριση πληροφοριών σχετικών με την κυκλοφορία οχημάτων, το οποίο βασίζεται στην τεχνολογία blockchain και στο IOV (Internet of Vehicles) και το οποίο είναι με τέτοιο τρόπο κατασκευασμένο ώστε να εξασφαλίζεται η συμμόρφωση με τον ΓΚΠΔ[184]. Το IOV (Διαδίκτυο των οχημάτων) είναι ένα δίκτυο οχημάτων εξοπλισμένων με αισθητήρες, λογισμικό και τεχνολογίες που διαμεσολαβούν με τα ανωτέρω με σκοπό τη διασύνδεση και την ανταλλαγή δεδομένων μέσω διαδικτύου[185].

Η ιδέα του προτεινόμενου συστήματος βασίζεται στο γεγονός ότι υπάρχουν πολλοί φορείς που ενδιαφέρονται για τη διαχείριση πληροφοριών σχετικά με τη συμπεριφορά των οχημάτων αλλά επιθυμούν να προστατευθούν από πιθανή συσχέτιση που πηγάζει από κατακράτηση δεδομένων. Η συγκεκριμένη πρόταση περιλαμβάνει τη χρήση ζευγών ασύμμετρων κλειδιών για την υπογραφή πληροφοριών, για τη δυνατότητα αυθεντικοποίησης και για να μπορούν να κρυπτογραφούν ευαίσθητες πληροφορίες και να επιτρέπουν την πρόσβαση μόνο σε όσους διαθέτουν δικαίωμα πρόσβασης ή σε δημόσιες αρχές όταν τους επιτρέπεται δυνάμει δικαστικής απόφασης, ή όταν υπάρχει άλλου είδους έννομο συμφέρον που προβλέπεται από το νόμο. Χρησιμοποιεί επίσης τεχνολογία blockchain για να εξασφαλίζει την ευθύνη, να εγγυάται και επιβεβαιώνει την μη δυνατότητα τροποποίησης των δεδομένων και να μειώνει τους κινδύνους και το κόστος προστασίας, χωρίς την αποκάλυψη πληροφοριών.

Οι ενδιαφερόμενοι φορείς που θα μπορούσαν να λάβουν μέρος είναι οι κατασκευαστές οχημάτων, οι ασφαλιστικές εταιρίες, οι ανάδοχοι έξυπνων οδικών δικτύων, οι χώροι στάθμευσης , οι οδηγοί και μία δημόσια αρχή για τη διαχείριση της πρόσβασης σε ευαίσθητα δεδομένα.

---

[184] Lelio Campanile1, Mauro Iacono, Fiammetta Marulli, Michele Mastroianni, Designing a GDPR compliant blockchain-based IoV distributed information tracking system, Information Processing and Management 58 (2021) 102511, Elsevier

[185] https://en.wikipedia.org/wiki/Internet_of_vehicles

Η συμμόρφωση του συστήματος με τον ΓΚΠΔ επιτυγχάνεται αναφορικά με την αρχή της νομιμότητας με το γεγονός ότι όλοι οι συμμετέχοντες που διατηρούν προσωπικά δεδομένα πρέπει να είναι γνωστοί στους χρήστες και συνεπώς όλοι πρέπει να αντιμετωπίζονται ως από κοινού υπεύθυνοι επεξεργασίας. Ο τύπος blockchain που ταιριάζει περισσότερο σε αυτή την υποχρέωση είναι τα ιδιωτικά και αδειοδοτημένα blockchain. Επιπλέον, για την συμμόρφωση με το δικαίωμα διόρθωσης και το δικαίωμα διαγραφής το προτεινόμενο σύστημα προβλέπει τη δυνατότητα τροποποίησης των δεδομένων με την προσθήκη ενός νέου block με ενημερωμένες πληροφορίες και τη δυνατότητα διαγραφής, με κρυπτογράφηση των block και διαγραφή των κλειδιών. Μόνο οι εξουσιοδοτημένοι από την δημόσια αρχή φορείς μπορούν να ενσωματώσουν νέο κόμβο στο blockchain. Επιπλέον, όλοι οι χρήστες πρέπει να αναγνωριστούν και να αυθεντικοποιηθούν από τουλάχιστον έναν συμμετέχοντα κόμβο και με βάση κάποια συγκεκριμένη διαδικασία που συμφωνείται από όλους τους συμμετέχοντες.

Συμπεράσματα- Επίλογος

Έπειτα από την ανωτέρω έρευνα, το ερώτημα «μπορεί μία τεχνολογία blockchain να συμμορφώνεται με τις επιταγές του ΓΚΠΔ;», εξακολουθεί να μην μπορεί να απαντηθεί με σαφήνεια. Ο λόγος είναι οι ποικίλες μορφές με τις οποίες μπορεί να εμφανίζεται μία τεχνολογία blockchain, καθώς και κάποια χαρακτηριστικά των τεχνολογιών αυτών που εκ των πραγμάτων έρχονται σε αντίθεση με τον Κανονισμό. Συμπερασματικά, λοιπόν, θα μπορούσαμε να πούμε ότι η συμμόρφωση με τις επιταγές του ΓΚΠΔ καθίσταται ευκολότερη όταν πρόκειται για ιδιωτικά και/ή αδειοδοτημένα blockchain, λόγω της ευκολίας εντοπισμού μίας κεντρικής οντότητας που θα μπορούσε να αναλάβει τις υποχρεώσεις του υπευθύνου επεξεργασίας. Δυσκολίες συμμόρφωσης, ωστόσο, εξακολουθούν να υπάρχουν σε με ορισμένες υποχρεώσεις του Κανονισμού, οι περισσότερες από τις οποίες αφορούν την ικανοποίηση δικαιωμάτων διαγραφής, διόρθωσης και πρόσβασης. Από την άλλη πλευρά, όταν πρόκειται για δημόσια και μη αδειοδοτημένα blockchain, τα εμπόδια εμφανίζονται αρκετά μεγαλύτερα. Μία από τις βασικές ιδιότητες της τεχνολογίας blockchain, η αποκέντρωση έρχεται σε πλήρη αντίθεση με μία από τις βασικές αρχές του ΓΚΠΔ, τη λογοδοσία. Ωστόσο, όπως αποδείχθηκε, υπάρχουν εναλλακτικές λύσεις, όπως η χρήση ειδικών εργαλείων και τεχνικών που μπορούν να δημιουργήσουν ένα πλαίσιο εντός του οποίου ένα σύστημα blockchain, είτε ιδιωτικό είτε δημόσιο, μπορεί να λειτουργεί με συμβατότητα προς τον Κανονισμό.

Η «φιλικότερη» ως προς και τις δύο πλευρές προσέγγιση, είναι κατά την άποψη της γράφουσας, η προσπάθεια εντοπισμού και αναγνώρισης των κοινών σημείων μεταξύ τους, καθώς υπάρχουν θεμελιώδεις αρχές και στις τεχνολογίες blockchain και στον ΓΚΠΔ που στοχεύουν στο ίδιο ακριβώς αποτέλεσμα, όπως για παράδειγμα η ασφάλεια και η αξιοπιστία των δεδομένων. Από την άλλη πλευρά, είναι εξίσου σημαντικό να γίνει προσπάθεια ώστε οι αντιθέσεις και οι «εντάσεις» μεταξύ των δύο πλευρών να μειώνονται. Αυτό μπορεί να επιτευχθεί αφενός από την

δημιουργία συστημάτων φιλικών προς τον ΓΚΠΔ, γεγονός το οποίο ήδη έχει ξεκινήσει να συμβαίνει και αφετέρου με την έκδοση κατευθυντήριων γραμμών από τα αρμόδια όργανα ώστε να εξειδικεύεται ο τρόπος εφαρμογής των διατάξεων του Κανονισμού στις εν λόγω τεχνολογίες, οι οποίες συνεχώς εξελίσσονται προσθέτοντας νέα δεδομένα. Η αξιοποίηση των κοινών στόχων και των δύο πλευρών σε συνδυασμό με την προσπάθεια προσαρμογής αμφότερων στις ιδιαίτερες απαιτήσεις της έτερης, μπορούν να δημιουργήσουν συνθήκες «αρμονικής συνύπαρξης» μεταξύ τους.

Σε κάθε περίπτωση, είναι σημαντικό και από την άποψη των τεχνολογικών εξελίξεων και από την άποψη της προστασίας της ιδιωτικής ζωής, να υπάρχει ένα πλαίσιο εντός του οποίου μπορεί να γίνει με ασφάλεια η χρήση οποιασδήποτε τεχνολογίας χωρίς να δημιουργούνται αισθήματα ανασφάλειας και φόβου. Ο όγκος των δεδομένων που διακινούνται μέσω διάφορων τεχνολογιών είναι πλέον εξαιρετικά μεγάλος και για το λόγο αυτό είναι σημαντικό να μην καταστεί ανεξέλεγκτος, με όποια επίπτωση μπορεί να έχει αυτό στους χρήστες τους.

Βιβλιογραφία – Αρθρογραφία

Αιτιολογική έκθεση Εκσυγχρονισμένης Σύμβασης 108

Αλεξανδροπούλου -Αιγυπτιάδου Ευγενία, Προσωπικά Δεδομένα, Νομική Βιβλιοθήκη, 2016

Απόφαση 38/2010 ΑΠΔΠΧ

Απόφαση 65/2018, ΑΠΔΧ

Γενικός Κανονισμός Προστασίας Δεδομένων

ΔΕΕ, C-101/01, Bodil Lindqvist

ΔΕΕ, C-293/12 και C-594/12, Digital Rights Ireland Ltd κατά Minister for Communications, Marine and Natural Resources κλπ. και Karntner Landesregierung, 08-04-2014

ΔΕΕ, C-317/04 και C-318/04, Απόφαση του Δικαστηρίου (τμήμα μείζονος συνθέσεως) της 30ής Μαΐου 2006

ΔΕΕ, Υπόθεση C-582/14 Patrick Breyer κατά Bundesrepublik Deutschland

Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων, Έκδοση 2018

Έκθεση σχετικά με την τεχνολογία blockchain: μια μακρόπνοη εμπορική πολιτική (2018/2085(INI)

Εκσυγχρονισμένη Σύμβαση 108

ΕΣΠΔ, Κατευθυντήριες γραμμές 4/2019 σύμφωνα με το άρθρο 25 Προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού

ΕΣΠΔ, Κατευθυντήριες γραμμές 8/2020 σχετικά με τη στόχευση χρηστών μέσων κοινωνικής δικτύωσης

Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπο

Ιγγλεζάκης Ιωάννης, Ο Γενικός Κανονισμός Προστασίας Δεδομένων, Interactive

Κοτσαλής Λεωνίδας, Κωνσταντίνος Μενουδάκος, Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων, Νομική διάσταση και πρακτική εφαρμογή, Νομική Βιβλιοθήκη, 2021

Οδηγία 95/46/ΕΚ

Ομάδα εργασίας άρθρου 29, 14/EL WP 225 Κατευθυντήριες γραμμές σχετικά με την εφαρμογή της απόφασης του δικαστηρίου της Ευρωπαϊκής Ένωσης στην υπόθεση c-131/12, «google Spain και inc κατά agencia española de protección de datos (aepd) και Mario Costeja González».

Ομάδα εργασίας άρθρου 29, Γνώμη 5/2009 σχετικά με τις επιγραμμικές υπηρεσίες κοινωνικής δικτύωσης

Ομάδα εργασίας άρθρου 29, Γνώμη 05/2014 σχετικά με τις τεχνικές ανωνυμοποίησης

Ομάδα εργασίας άρθρου 29, Γνώμη 1/2010 σχετικά με τις έννοιες του υπεύθυνου της επεξεργασίας και τους εκτελούντες την επεξεργασία

Ομάδα εργασίας άρθρου 29, Γνώμη 15/2011, ορισμός της συγκατάθεσης

Ομάδα εργασίας άρθρου 29, Γνώμη 3/2010 σχετικά με την αρχή της λογοδοσίας

Ομάδας εργασίας του άρθρου 29, Γνώμη 4/2007

Τιντζογλίδου Νόπη, Οδηγός εφαρμογής GDPR, Νομική Βιβλιοθήκη, 2020

Χάρτης Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης

Χριστοδούλου Κωνσταντίνος, Δίκαιο προσωπικών δεδομένων, Το πεδίο εφαρμογής του δικαίου των προσωπικών δεδομένων, Νομική Βιβλιοθήκη

Antonopoulos Andreas M., Gavin Wood, What is a Smart Contract? Nov 12, 2018

Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing

Article 29 Working Party, Opinion 03/2013 on purpose limitation (WP 203) 00569/13/EN

Article 29 Working Party, Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) (WP 128) 01935/06/EN, 11

Ateniese G, Magri B, Venturi D and Andrade E (2017), 'Redactable Blockchain – or – Rewriting History in Bitcoin and Friends'

Bacon J et al (2018) 'Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers' 25 Richmond Journal of Law and Technology 1, 64

Berberich M and Steiner M (2016), 'Blockchain Technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers?' 2 European Data Protection Law Review

Bikramaditya Singhal, Gautam Dhameja, and Priyansu Sekhar Panda, Beginning Blockchain: A Beginner's Guide to Building Blockchain Solutions, , Apress, 2018

Biryukov et al, 'Denanonymisation of Clients in Bitcoin P2P Network' (2014)

Blockchain and the General Data Protection Regulation,Can distributed ledgers be squared with European data protection law?, Study, Panel for the Future of Science and Technology, European Parliamentary Research Service, Scientific Foresight Unit (STOA) PE 634.445 – July 2019

Bourka Athena and Prokopios Drogkaris , 'Recommendations on Shaping Technology According to GDPR Provisions', ENISA 2018

Brenn Hill, Samanyu Chopra, Paul Valencourt.; Blockchain Quick Reference : A Guide to Exploring Decentralized Blockchain Application Development

Buocz T et al, 2019, 'Bitcoin and the GDPR: Allocating Responsibility in Distributed Networks', Computer Law & Security Review

C-131/12, Google Spain και Inc κατά Agencia Española de Protección De Datos (AEPD) και Mario Costeja González

C-25/17, Jehovan todistajat, 10-07-2018

C-362/14, Maximillian Schrems κατά Data Protection Commissioner, 6 Οκτωβρίου 2015

C-40/17 Fashion ID GmbH & Co. KG κατά Verbraucherzentrale NRW eV, 29-07-2019

C-582/14, Patrick Breyer κατά Bundesrepublik Deutschland, 19-10-2016

Case C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein κατά Wirtschaftsakademie Schleswig-Holstein GmbH, 05-06-2018

Case C-507/17 Google v CNIL

Commission Nationale Informatique et Libertés (September 2018), 'Premiers Éléments d'analyse de la CNIL : Blockchain

Delgado-von-Eitzen, C.; Anido-Rifón, L.; Fernández-Iglesias, M.J. Application of Blockchain in Education: GDPR-Compliant and Scalable Certification and Verification of Academic Information. Appl. Sci. 2021, 11, 4537

EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR

European Parliament (27 November 2018), Report on Blockchain: a Forward-Looking Trade Policy (AB-0407/2018)

Lewis Antony, A Gentle Introduction to Ethereum Oct 2, 2016

Διαδικτυακές πηγές

https://www.europarl.europa.eu/

https://www.europarl.europa.eu/news/el/headlines/priorities/i-techniti-noimosuni-stin-ee/20200827STO85804/ti-einai-i-techniti-noimosuni-kai-pos-chrisimopoieitai

https://www.ecb.europa.eu/explainers/tell-me more/html/distributed_ledger_technology.el.html

https://el.wikipedia.org/wiki/%CE%A3%CF%85%CE%BD%CE%AC%CF%81%CF%84%CE%B7%CF%83%CE%B7_%CE%BA%CE%B1%CF%84%CE%B1%CF%84%CE%B5%CE%BC%CE%B1%CF%87%CE%B9%CF%83%CE%BC%CE%BF%CF%8D

https://el.wikipedia.org/wiki/Bitcoin

https://docs.ethhub.io/ethereum-basics/what-is-ethereum/#what-are-smart-contracts-and-decentralized-applications

https://landscape.hyperledger.org/card-mode?project=hosted

https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/

https://www.ethswarm.org/

https://www.storj.io/

https://filecoin.io/

IRS Tries Again To Make Coinbase Turn Over Customer Account Data (forbes.com)

https://arxiv.org/abs/1107.4524

https://arxiv.org/abs/1 405.7418

https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:62014CJ0582&from=EN

https://getmonero.org/resources/moneropedia/stealthaddress.html

https://z.cash/technology/zksnarks.html

https://www.talentica.com/blogs/state-channels-an-introduction-to-off-chain-transactions/#:~:text=A%20state%20channel%20is%20a,cryptographically%20provable%20on%20the%20blockchain.

https://www.getmonero.org/resources/moneropedia/ringsignatures.html

https://www.accenture.com/gr-en/insight-editing-uneditable-blockchain

https://curia.europa.eu/juris/liste.jsf?num=C-210/16

https://curia.europa.eu/juris/document/document.jsf?text=&docid=203822&pageIndex=0&doclang=EL&mode=lst&dir=&occ=first&part=1&cid=7408029

https://curia.europa.eu/juris/liste.jsf?num=C-40/17&language=EL

https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf

https://dl.eusset.eu/bitstream/20.500.12015/3159/1/blockchain2018_03.pdf

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_el.pdf

https://www.europarl.europa.eu/doceo/document/A-8-2018-0407_EL.pdf

https://curia.europa.eu/juris/document/document.jsf;jsessionid=DBFD45FB81C1CD1091FED6B3CDCA2933?text=&docid=218105&pageIndex=0&doclang=EL&mode=lst&dir=&occ=first&part=1&cid=626146

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3311370

https://www.dpa.gr/el/enimerwtiko/prakseisArxis/katalogos-me-ta-eidi-ton-praxeon-epexergasias-poy-ypokeintai-stin

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

https://doi.org/10.3390/s21237994

https://en.wikipedia.org/wiki/InterPlanetary_File_System

https://doi.org/10.3390/app11136132

https://doi.org/10.3390/app11104537

https://en.wikipedia.org/wiki/Internet_of_vehicles

https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_el.pdf

https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf

https://edpb.europa.eu/system/files/2021-11/edpb_guidelines_082020_on_the_targeting_of_social_media_users_el_0.pdf

https://bitnodes.io/

https://www.ethernodes.org/

https://el.wikipedia.org/wiki/%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%AC%CF%86%CE%B7%CF%83%CE%B7_%CE%A3%CF%85%CE%BC%CE%BC%CE%B5%CF%84%CF%81%CE%B9%CE%BA%CE%BF%CF%8D_%CE%9A%CE%BB%CE%B5%CE%B9%CE%B4%CE%B9%CE%BF%CF%8D

https://pithos.okeanos.grnet.gr/public/k5aKPf3nzomvLIPDbErBA6