Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή
Στην Ασφάλεια Υπολογιστών και Δικτύων

Η χρήση της τεχνολογίας blockchain για την προστασία των προσωπικών δεδομένων και την ασφάλεια των διαδικτυακών χρηματοοικονομικών συναλλαγών (Fintech) σύμφωνα με τις απαιτήσεις του GDPR.

Αβραάμ Ζαχαρίου

Επιβλέπων Καθηγητής
Νικόλαος Σκλάβος

Απρίλιος 2020

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Η χρήση της τεχνολογίας blockchain για την προστασία των προσωπικών δεδομένων και την ασφάλεια των διαδικτυακών χρηματοοικονομικών συναλλαγών (Fintech) σύμφωνα με τις απαιτήσεις του GDPR.

Αβραάμ Ζαχαρίου

Επιβλέπων Καθηγητής
Αβραάμ Ζαχαρίου

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στην Ασφάλεια Υπολογιστών και Δικτύων

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Απρίλιος 2020

Περίληψη

Ο στόχος της παρούσας μεταπτυχιακής διατριβής είναι να εξεταστεί η δυνατότητα εφαρμογής της τεχνολογίας Blockchain σε διαδικτυακές χρηματοοικονομικές συναλλαγές (Fintech) για την προστασία των προσωπικών δεδομένων σύμφωνα με τις απαιτήσεις τουGDPR.

Αρχικά θα αναλυθεί το φαινόμενο της αντικατάστασης των συμβατικών χρηματοοικονομικών υπηρεσιών και λύσεων από την τεχνολογικές λύσεις τύπου Fintech. Θα γίνει αναφορά στην οικονομική διάσταση της επέκτασης τους και στις κανονιστικές υποχρεώσεις που έχει μια εταιρεία Fintech που δραστηροποιείται εντός της ΕΕ. Ακολούθως θα γίνει μια παρουσίαση της τεχνολογίας Blockchain, των τεχνολογιών από τις οποίες συνίσταται, των δυνατοτήτων της, των περιορισμών της, των εξελίξεων που έχουν σημειωθεί τα τελευταία χρόνια και την προοπτική της.

Στη συνέχεια θα αναλυθεί τι προβλέπει ο κανονισμός GDPR, τι επιπτώσεις έχει στις διαδικτυακές συναλλαγές, στην υποδομή ενός οργανισμού Fintech και ποιοι άλλοι κανονισμοί και οδηγίες της ΕΕ επηρεάζουν την λειτουργία τους.

Αφού αναλυθούν οι αλληλεπιδράσεις των Blockchain-Fintech-GDPR θα γίνει παρουσίαση των επικρατέστερων λύσεων που κυκλοφορούν. Στη συνέχεια θα παρουσιαστεί η λύση που απαντάει σε όλα τα ζητήματα που αναλύθηκαν προηγουμένως και τα πλεονεκτήματα και μειονεκτήματα της συγκεκριμένης εφαρμογής.

Καταλήγοντας θα εξαχθούν τα απαραίτητα συμπεράσματα από τα προαναφερόμενα.

Summary

The goal of this postgraduate thesis is to examine the applicability of Blockchain technology to online financial transactions (Fintech) for the protection of personal data in accordance with the requirements of the GDPR.

Initially the phenomenon of the replacement of conventional financial services and solutions by Fintech technology solutions will be analyzed. The economic dimension of their expansion and the regulatory obligations of a Fintech company which is active within the EU.

Afterwards there will be a presentation of the Blockchain technology, the technologies it is comprised of, its capabilities, its limitations, the developments that have occurred in recent years and the prospect of it

It will then analyze what the GDPR provides, what impact it has on online transactions, on the infrastructure of a fintech organization, and what other EU regulations and directives affect their operation.

Once the interactions of Blockchain-Fintech-GDPR have been analysed, the prevailing solutions that are circulating will be presented.

The solution that responds to all previously analyzed issues and the advantages and disadvantages of this application will then be presented.

In conclusion, the necessary conclusions will be drawn from the above.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω την οικογένεια μου για την ηθική συμπαράσταση της στην προσπάθεια ολοκλήρωσης της παρούσας διατριβής.

ΠΕΡΙΕΧΟΜΕΝΑ

Εισαγωγή

Ένα από τα μεγαλύτερα προβλήματα της επέκτασης του διαδικτύου σε κάθε πτυχή της ζωής μας είναι η προστασία των προσωπικών δεδομένων. Ακόμα πιο σημαντική είναι η προστασία των προσωπικών δεδομένων μας στον τομέα των χρηματοοικονομικών συναλλαγών μας με τη χρήση έξυπνων συσκευών και λογισμικών δια μέσου του διαδικτύου. Συνέπεια αυτής της πραγματικότητας είναι η υιοθέτηση πιο αυστηρής νομοθεσίας για την προστασία των προσωπικών δεδομένων όπως αυτή έχει εκφραστεί στην Ε.Ε. από τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR).

Οι προκλήσεις που προκύπτουν από την αυξανόμενη χρήση Fintech λύσεων για τις χρηματοοικονομικές συναλλαγές σε συνδυασμό με τις απαιτήσεις του GDPR, έχουν αυξήσει το επίπεδο της δυσκολίας για τις επιχειρήσεις. Θα μπορούσε η υιοθέτηση της τεχνολογίας blockchain να προσφέρει μια λύση που να ικανοποιεί όλες τις ανάγκες; Την ανάγκη για προστασία των προσωπικών δεδομένων, για ασφαλείς συναλλαγές, για μείωση του όγκου των δεδομένων, για συμμόρφωση με κανονισμούς και νομοθεσίες, για μείωση του λειτουργικού κόστους. Στην παρούσα διατριβή θα γίνει προσπάθεια να απαντηθεί το πιο πάνω ερώτημα.

Κεφάλαιο 1

Βιβλιογραφική επισκόπηση

1.1 Εισαγωγή

Το ερευνητικό θέμα της παρούσας διατριβής είναι η προστασία προσωπικών δεδομένων και η ασφάλεια διαδικτυακών χρηματοοικονομικών συναλλαγών (Fintech). Το ερευνητικό πρόβλημα είναι κατά πόσο η τεχνολογία blockchain μπορεί να επιλύσει το θέμα της προστασίας των προσωπικών δεδομένων και της ασφάλειας των διαδικτυακών χρηματοοικονομικών συναλλαγών (Fintech), τηρώντας ταυτόχρονα τις απαιτήσεις του GDPR.

Οι βασικές έννοιες είναι η τεχνολογία blockchain, τα προσωπικά δεδομένα, οι διαδικτυακές χρηματοοικονομικές συναλλαγές, το fintech και ο κανονισμός GDPR.

Τα ερευνητικά ερωτήματα που προκύπτουν από το θέμα της διατριβής είναι:

- Μπορεί η τεχνολογία blockchain να προστατέψει τα προσωπικά δεδομένα και πώς;
- Μπορεί η τεχνολογία blockchain να κάνει πιο ασφαλείς τις διαδικτυακές συναλλαγές, ουσιαστικά την χρηματοοικονομική τεχνολογία (Fintech) και πώς;
- Μπορούν να γίνουν τα παραπάνω ενώ ταυτόχρονα να τηρούνται οι απαιτήσεις του κανονισμού GDPR;

1.2 Βιβλιογραφική επισκόπηση

Σύμφωνα με το Investopedia η χρηματοοικονομική τεχνολογία (Fintech) χρησιμοποιείται για την περιγραφή νέων τεχνολογιών που επιδιώκουν να βελτιώσουν και να αυτοματοποιήσουν την παροχή και τη χρήση των χρηματοπιστωτικών υπηρεσιών [1]. Το Wikipedia από την

πλευρά του λέει ότι η χρηματοοικονομική τεχνολογία, συχνά συντομευμένη σε fintech, είναι η τεχνολογία και η καινοτομία που στοχεύει να ανταγωνιστεί τις παραδοσιακές χρηματοοικονομικές μεθόδους στην παροχή χρηματοοικονομικών υπηρεσιών [2]. Τέλος η ΕΚΤ (Ευρωπαϊκή Κεντρική Τράπεζα) αναφέρει ότι Fintech - συντομογραφία για τη χρηματοοικονομική τεχνολογία - είναι ένας γενικός όρος για κάθε είδους τεχνολογική καινοτομία που χρησιμοποιείται για την υποστήριξη ή την παροχή χρηματοπιστωτικών υπηρεσιών [3].

Το GDPR, είναι ο Γενικός Κανονισμός για την Προστασία Δεδομένων (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών [10].

Το Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα της Κύπρου αναφέρει ότι: «Προσωπικά δεδομένα σημαίνει κάθε πληροφορία που αναφέρεται σε άτομο που βρίσκεται στη ζωή εφόσον η πληροφορία αυτή τυγχάνει αυτοματοποιημένης επεξεργασίας (π.χ. στον ηλεκτρονικό υπολογιστή) ή διατηρείται σε ένα διαρθρωμένο αρχείο μη αυτοματοποιημένης μορφής (δηλ. σε ταξινομημένο φάκελο)[11].

Σύμφωνα με πρόσφατη μελέτη που πραγματοποιήθηκε για λογαριασμό του Ευρωπαϊκού Κοινοβουλίου από την Μονάδα Επιστημονικής Πρόβλεψης - Scientific Foresight Unit (STOA), το Blockchain ορίζεται σαν μια κοινόχρηστη και συγχρονισμένη ψηφιακή βάση δεδομένων που διατηρείται από έναν αλγόριθμο συναίνεσης και αποθηκεύεται σε πολλαπλούς κόμβους (υπολογιστές που αποθηκεύουν μια τοπική έκδοση της βάσης δεδομένων) [19].

Η έκθεση του Ιουλίου του 2019 της EBA (European Banking Authority) σχετικά με τις επιπτώσεις της Fintech στα επιχειρηματικά μοντέλα των οργανισμών πληρωμών και των οργανισμών ηλεκτρονικού χρήματος [6], επικεντρώνεται στις τρέχουσες τάσεις και τους παράγοντες που διαμορφώνουν τα επιχειρηματικά μοντέλα των ιδρυμάτων πληρωμών (PI) και των ιδρυμάτων ηλεκτρονικού χρήματος (EMI), συλλογικά και εναλλακτικά, οι διάφορες προσεγγίσεις τους για τη χρηματοοικονομική τεχνολογία (FinTech), συμπεριλαμβανομένης της αλληλεπίδρασής τους με τις εταιρείες BigTech,·το επίπεδο εφαρμογής καινοτόμων

τεχνολογιών και οι παρατηρούμενες αλλαγές στις στρατηγικές και τα επιχειρηματικά τους μοντέλα. Η έκθεση δεν ασχολείται με σενάρια για πιθανή μελλοντική ανάπτυξη. και βασίζεται σε πληροφορίες και δεδομένα που συλλέγονται από την EBA μέσω της διασύνδεσης της με την εποπτική κοινότητα και τον ευρύτερο κλάδο, συμπεριλαμβανομένων των ευρύτερων δραστηριοτήτων του EBA FinTech Knowledge Hub.

Το συμπέρασμα των ερευνών της έκθεσης είναι ότι το τοπίο των πληρωμών στην ΕΕ υφίσταται σημαντική μεταμόρφωση λόγω της εισαγωγής του PSD2 και των συνεχιζόμενων εξελίξεων στη χρηματοοικονομική τεχνολογία. Τα περισσότερα ιδρύματα προσαρμόζουν τα επιχειρηματικά τους μοντέλα για να αντιμετωπίσουν την ανταγωνιστική πίεση και να αγκαλιάσουν τις αλλαγές του PSD2, ενώ ορισμένα από αυτά μπορούν παράλληλα να ενστερνιστούν τον θετικό αντίκτυπο της FinTech. Μεσοπρόθεσμα και μακροπρόθεσμα, μια σειρά παραγόντων θα καθορίσουν τη μετατροπή των επιχειρηματικών μοντέλων των διαφόρων ιδρυμάτων: (i) η πρόοδος των επιχειρήσεων Open Banking και APIs, η οποία διευκολύνεται εν μέρει από την PSD2,(ii) το επίπεδο εφαρμογής καινοτόμων τεχνολογιών και (iii) τη δραστηριότητα των εταιρειών BigTech στους τομείς των χρηματοπιστωτικών υπηρεσιών.

Ενώ οι τρέχουσες αλλαγές στη χρηματοοικονομική τεχνολογία ενδέχεται να προσφέρουν ελπιδοφόρες ευκαιρίες τόσο στους παράγοντες της αγοράς όσο και στους πελάτες, ενέχουν επίσης νέους κινδύνους για τον τομέα των χρηματοπιστωτικών υπηρεσιών, οι οποίοι πρέπει να αξιολογηθούν προσεκτικά και να αντιμετωπιστούν. Το τοπίο των κινδύνων εξελίσσεται ως αποτέλεσμα της αυξανόμενης στροφής προς την ψηφιοποίηση, τις πολιτικές αβεβαιότητες και το κανονιστικό πλαίσιο. Οι επιπτώσεις της κοινοχρησίας δεδομένων, συμπεριλαμβανομένων των αντίστοιχων συμβατικών εγγυήσεων, ενδέχεται να αλλάξουν περαιτέρω το τρέχον ανταγωνιστικό τοπίο, ενώ η αλληλεπίδραση μεταξύ PSD2 και GDPR μπορεί να δημιουργήσει περαιτέρω προκλήσεις που πρέπει να αντιμετωπιστούν.

Η έκθεση του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών (Enisa) με τίτλο «Distributed Ledger Technology & Cybersecurity - Improving information security in the financial sector» του 2016 [24], είχε ως στόχο να παρέχει στους επαγγελματίες του χρηματοπιστωτικού τομέα τόσο σε επιχειρηματικούς όσο και σε τεχνολογικούς ρόλους μια

αξιολόγηση των διαφόρων οφελών και προκλήσεων που ενδέχεται να αντιμετωπίσουν τα ιδρύματά τους κατά την εφαρμογή ενός κατανεμημένου καθολικού DLT. Μερικές από τις βασικές προκλήσεις του Blockchain που προσδιορίζονται στην έκθεση είναι:

- Παραδοσιακές προκλήσεις, όπως: η διαχείριση κλειδιού, η κρυπτογραφία, η ιδιωτικότητα και η αναθεώρηση κώδικα.

- Τεχνολογικές προκλήσεις, όπως: η δημιουργία κλειδιών, η διαχείριση έξυπνων συμβολαίων και η δυνατότητα αέναης επέκτασης.

Η έκθεση αναφέρει προβλήματα ασφαλείας που σχετίζονται συγκεκριμένα με το DLT όπως: Consensus hijack (Attack 51%), εκμετάλλευση ευπαθειών των sidechains, εκμετάλλευση του κεντρικού ρόλου που έχει μία οντότητα σε ένα Permissioned Blockchain, Distributed Denial of Service attack, η διαχείριση του ψηφιακού πορτοφολιού, η επεκτασιμότητα του blockchain, η τυχών ευπάθεια του κώδικα των έξυπνων συμβολαίων, η επικοινωνία μεταξύ διαφορετικού τύπου DLT, η διασύνδεση διακυβέρνησης με το DLT και η συμμόρφωση με τις απαιτήσεις για AML/CFT/KYC.

Ο ENISA επίσης προτείνει ορθές πρακτικές για την αντιμετώπιση των ζητημάτων που εντοπίστηκαν, καθώς και για την εισαγωγή των βασικών εννοιών που θα πρέπει να γνωρίζουν οι υπεύθυνοι λήψης αποφάσεων κατά την προσέγγιση αυτής της τεχνολογίας. Μετά την επανεξέταση των υφιστάμενων προκλήσεων που συνδέονται με κατανεμημένα λογιστικά βιβλία, ορισμένες ορθές πρακτικές είναι οι εξής:

- Χρήση κλειδιών αποκατάστασης

- Χρήση πολλών υπογραφών για την εξουσιοδότηση και την επεξεργασία συναλλαγών

- Χρήση βιβλιοθήκης τυποποιημένων έξυπνων συμβολαίων

Στην έκθεση εντοπίζονται προκλήσεις που μπορεί να απαιτήσουν περαιτέρω ανάπτυξη, όπως:

- Εργαλεία καταπολέμησης του μαύρου χρήματος και της απάτης

- Διαλειτουργικότητα των πρωτοκόλλων Blockchain

• Νομικές διατάξεις και εργαλεία για την εφαρμογή της ιδιωτικής ζωής και το δικαίωμα στη λήθη.

Η δημοσίευση σε συνέδριο του IEEE των Woo Young Moon and Soo Dong Kim το 2016 [31] αναφέρει ότι η χρηματοοικονομική τεχνολογία αναδεικνύεται ως ένα νέο πρότυπο για την αποτελεσματικότερη παροχή χρηματοπιστωτικών υπηρεσιών, ενσωματώνοντας αποτελεσματικές τεχνολογίες πληροφορικής. Η πληρωμή είναι μια υπάρχουσα υπηρεσία χρηματοοικονομικής τεχνολογίας και υπάρχουν αρκετά συστήματα πληρωμών. Ωστόσο, υπάρχει υψηλός βαθμός ετερογένειας μεταξύ των συστημάτων πληρωμών όσον αφορά τη διαδικασία πληρωμής, τη μέθοδο διακανονισμού συναλλαγών και την ανάπτυξη λογισμικού. Συνεπώς, δεν μπορεί να πραγματοποιηθεί πληρωμή μεταξύ δύο διαφορετικών καθεστώτων/συστημάτων πληρωμών. Σε αυτό το έγγραφο, παρουσιάζεται μια διαδικασία διαμεσολάβησης πληρωμών για τη διαμεσολάβηση των δραστηριοτήτων πληρωμής μεταξύ δύο διαφορετικών συστημάτων και του λογισμικού της εφαρμογής. Η πλατφόρμα επιτρέπει συναλλαγές πληρωμών μεταξύ των διαθέσιμων συστημάτων πληρωμών που είναι διαθέσιμα, όπως το Samsung Pay και το Apple Pay. Παρουσιάζεται επίσης μια proof-of-concept εφαρμογή της πλατφόρμας ως έργο αξιολόγησης.

Η πλατφόρμα διαμεσολάβησης έχει ένα κοινό σύνολο λειτουργιών. Ωστόσο, υπάρχουν διάφορα ζητήματα σχεδιασμού και ανάπτυξης αυτών των λειτουργιών, όπως η διακριτικοποίηση (tokenization) και η εξουσιοδότηση. Επειδή είναι εξαιρετικά δύσκολο να ενταχθούν σε ένα δίκτυο πληρωμών. Η πλατφόρμα μπορεί να χρησιμοποιηθεί ως θεωρητική βάση για την οικοδόμηση διαφόρων λύσεων διαμεσολάβησης πληρωμών.

Η δημοσιοποίηση των Polyviou A., Velanas P., and Soldatos J., του 2019 [32] αναφέρει ότι ενώ το Blockchain χρησιμοποιήθηκε αρχικά ως το καθολικό δημόσιων συναλλαγών για κρυπτονομίσματα, έχει εξεταστεί για μια πληθώρα άλλων εφαρμογών, καθώς συμπυκνώνει μοναδικές ιδιότητες, συμπεριλαμβανομένης της αποκέντρωσης, της ασφάλειας, της διαφάνειας και της καταπολέμησης της αλλοίωσης. Οι ιδιότητες αυτές είναι ιδιαίτερα συμφέρουσες για ποικιλία σημαντικών θεμάτων που έχουν παρουσιαστεί στον χρηματοπιστωτικό τομέα. Ως αποτέλεσμα, η τεχνολογία blockchain έχει τη δυνατότητα να

φέρει επανάσταση στον χρηματοπιστωτικό κλάδο αλλάζοντας τον τρόπο με τον οποίο διεξάγονται διαφορετικές υπηρεσίες στον χρηματοπιστωτικό κλάδο. Σε αυτό το έγγραφο, σκιαγραφούνται πέντε διαφορετικές περιπτώσεις χρήσης του χρηματοπιστωτικού κλάδου που αναμένεται να μεταμορφωθούν ριζικά με τη χρήση της τεχνολογίας blockchain. Αυτές είναι:

- Know Your Customer (KYC) και Know Your Business (KYB)
- Βαθμολογία πιστωτικού ρίσκου (Credit Risk Scoring) για μικρομεσαίες επιχειρήσεις
- Διαχείριση προφίλ πελατών και εξατομίκευση προϊόντων
- Διαχείριση Ασφαλιστικών Απαιτήσεων
- Συνεργατική Ασφάλεια στην Αλυσίδα Χρηματοπιστωτικών Υπηρεσιών

Όπως λέει η εργασία οι θιασώτες του Blockchain πιστεύουν ότι αυτές οι περιπτώσεις χρήσης είναι πιθανό να γίνουν συνηθισμένες στον χρηματοπιστωτικό τομέα μέσα στην επόμενη δεκαετία. Παρουσιάζουν επίσης άλλες περιπτώσεις χρήσης στους τομείς της επενδυτικής τραπεζικής και των κινητών αξιών, οι οποίες εξυπηρετούνται ήδη πολύ καλά από την πλατφόρμα Corda/R3. Από την άλλη πλευρά, επισημαίνουν ότι υπάρχουν τεχνολογίες που υπερπροβλήθηκαν χωρίς αποτέλεσμα και το γεγονός ότι τα κρυπτονομίσματα (όπως το BitCoin) είναι μέχρι σήμερα οι μόνες εφαρμογές μεγάλης κλίμακας των blockchains. Προς το παρόν, οι εισηγμένες περιπτώσεις χρήσης blockchain παρέχουν γόνιμο έδαφος για τους καινοτόμους στον χρηματοπιστωτικό τομέα, συμπεριλαμβανομένων των επιχειρήσεων FinTech και InsurTech.

Το Συμβούλιο Χρηματοπιστωτικής Σταθερότητας (Financial Stability Board, FSB) με την έκθεση του για τις «Επιπτώσεις στη χρηματοπιστωτική σταθερότητα από τη Χρηματοοικονομική Τεχνολογία» του 2017 [33] απαντάει σε εποπτικά και ρυθμιστικά ζητήματα που αξίζουν την προσοχή των αρχών. Όπως επισημαίνεται, επί του παρόντος, οποιαδήποτε αξιολόγηση των επιπτώσεων της χρηματοοικονομικής τεχνολογίας στη χρηματοπιστωτική σταθερότητα αποτελεί πρόκληση δεδομένης της περιορισμένης διαθεσιμότητας επίσημων και ιδιωτικών δεδομένων. Θα είναι σημαντικό να ληφθεί υπόψη η σημαντικότητα και οι κίνδυνοι κατά την αξιολόγηση νέων τομέων. Θα είναι επίσης σημαντικό να κατανοήσουμε πώς αλλάζουν τα επιχειρηματικά μοντέλα των νεοσύστατων επιχειρήσεων και των κατεστημένων φορέων, καθώς και η δομή της αγοράς. Για να αντλήσει

τα εποπτικά και ρυθμιστικά ζητήματα της χρηματοοικονομικής τεχνολογίας, το FSB ανέπτυξε ένα πλαίσιο που καθορίζει το πεδίο των δραστηριοτήτων χρηματοοικονομικής τεχνολογίας και προσδιορίζει τα δυνητικά οφέλη και τους κινδύνους για τη χρηματοπιστωτική σταθερότητα. Παρέχει μια βάση επί της οποίας μπορεί να γίνει μελλοντική ανάλυση και παρακολούθηση.

Δεδομένου ότι οι περισσότερες δραστηριότητες χρηματοοικονομικής τεχνολογίας είναι επί του παρόντος μικρές σε σύγκριση με το συνολικό χρηματοπιστωτικό σύστημα, η ανάλυση επικεντρώνεται σε πιθανά οφέλη και κινδύνους. Ωστόσο, οι διεθνείς οργανισμοί και οι εθνικές αρχές θα πρέπει να εξετάσουν το ενδεχόμενο να λαμβάνουν υπόψη τη χρηματοοικονομική τεχνολογία στις υφιστάμενες εκτιμήσεις κινδύνου και στα ρυθμιστικά τους πλαίσια υπό το πρίσμα της ταχείας εξέλιξής της. Πολλές αρχές έχουν ήδη προβεί σε κανονιστικές αλλαγές για να προσαρμοστούν στις δραστηριότητες χρηματοοικονομικής τεχνολογίας.

Υπάρχουν σαφή οφέλη για μεγαλύτερη διεθνή συνεργασία, δεδομένων των κοινών και της παγκόσμιας διάστασης πολλών δραστηριοτήτων χρηματοοικονομικής τεχνολογίας. Η αυξημένη συνεργασία θα είναι ιδιαίτερα σημαντική για τον μετριασμό του κινδύνου κατακερματισμού ή απόκλισης στα ρυθμιστικά πλαίσια, η οποία θα μπορούσε να εμποδίσει την ανάπτυξη και τη διάδοση επωφελών καινοτομιών στις χρηματοπιστωτικές υπηρεσίες, και να περιορίσει την αποτελεσματικότητα των προσπαθειών για την προώθηση της χρηματοπιστωτικής σταθερότητας.

Με βάση τα πορίσματα της βιβλιογραφίας, τις συζητήσεις με ακαδημαϊκούς και τους συμμετέχοντες στη βιομηχανία, καθώς και τον απολογισμό των ρυθμιστικών προσεγγίσεων για τη χρηματοοικονομική τεχνολογία, το FSB καταλήγει στο συμπέρασμα ότι επί του παρόντος δεν υπάρχουν επιτακτικοί κίνδυνοι χρηματοπιστωτικής σταθερότητας από τις αναδυόμενες καινοτομίες της χρηματοοικονομικής τεχνολογίας. Η ανάλυση προσδιορίζει, ωστόσο, 10 ζητήματα που χρήζουν προσοχής των αρχών, εκ των οποίων τα τρία θεωρούνται προτεραιότητες για διεθνή συνεργασία. Η αντιμετώπιση αυτών των τομέων προτεραιότητας θεωρείται σημαντική για την προώθηση της χρηματοπιστωτικής σταθερότητας, την προώθηση της υπεύθυνης καινοτομίας και την πρόληψη τυχόν εκτροχιασμού των προσπαθειών των αρχών για την επίτευξη ενός χρηματοπιστωτικού συστήματος χωρίς αποκλεισμούς. Αν και πολλά από αυτά τα ζητήματα δεν είναι νέα, μπορεί να επιδεινωθούν

δεδομένης της ταχύτητας ανάπτυξης της χρηματοοικονομικής τεχνολογίας, των νέων μορφών διασύνδεσης και της αυξημένης εξάρτησης από τρίτους παρόχους υπηρεσιών.

Το ευρωπαϊκό κοινοβούλιο (Michèle Finck, 2019) δημοσίευσε μια μελέτη σχετικά με το Blockchain και τον γενικό κανονισμό για την προστασία των δεδομένων και το αν μπορεί να συμβαδίσει με την ευρωπαϊκή νομοθεσία για την προστασία των δεδομένων [34]. Σύμφωνα με τη μελέτη τα τελευταία χρόνια, έχει γίνει εκτενής συζήτηση για τις τεχνολογίες blockchain (ή τεχνολογία κατανεμημένου καθολικού – DLT) και τις δυνατότητές τους για την ενιαία ψηφιακή αγορά της Ευρωπαϊκής Ένωσης. Ένα επαναλαμβανόμενο επιχείρημα ήταν ότι αυτή η κατηγορία τεχνολογιών μπορεί, από τη φύση της, να μην είναι σε θέση να συμμορφωθεί με την ευρωπαϊκή νομοθεσία για την προστασία των δεδομένων, η οποία με τη σειρά της κινδυνεύει να καταπνίξει την ανάπτυξή εις βάρος του ευρωπαϊκού σχεδίου για την ενιαία ψηφιακή αγορά. Η μελέτη αναλύει τη σχέση μεταξύ blockchain και GDPR, έτσι ώστε να αναδείξει τις υπάρχουσες εντάσεις και να προωθήσει πιθανές λύσεις.

Όπως αναφέρεται παρατηρήθηκε ότι μπορούν να εντοπιστούν πολλά σημεία τριβής μεταξύ των blockchains και του GDPR. Σε γενικές γραμμές, μπορεί να σημειωθεί ότι αυτά οφείλονται σε δύο γενικούς παράγοντες. Πρώτον, ο GDPR στηρίζεται στην υπόθεση ότι σε σχέση με κάθε σημείο δεδομένων προσωπικού χαρακτήρα υπάρχει τουλάχιστον ένα φυσικό ή νομικό πρόσωπο –ο υπεύθυνος επεξεργασίας δεδομένων– το οποίο μπορεί να αντιμετωπίσει τα αιτήματα των υποκειμένων των δεδομένων για την επιβολή των δικαιωμάτων τους βάσει του GDPR. Τα Blockchains, ωστόσο, συχνά επιδιώκουν να επιτύχουν αποκέντρωση αντικαθιστώντας έναν κεντρικό χειριστή με πολλούς διαφορετικούς. Αυτό καθιστά πολύ δύσκολη την κατανομή της ευθύνης και της λογοδοσίας, ιδίως υπό το πρίσμα των ατελών περιγραφών της έννοιας του «κοινού ελέγχου» που υπάρχουν στον κανονισμό. Επιπλέον δυσκολία προκαλούν, πρόσφατες εξελίξεις στη νομολογία, όπου ο ορισμός των οντοτήτων που χαρακτηρίζονται ως από κοινού υπεύθυνοι επεξεργασίας μπορεί να είναι γεμάτος αβεβαιότητα. Δεύτερον, ο GDPR βασίζεται στην υπόθεση ότι τα δεδομένα μπορούν να τροποποιηθούν ή να διαγραφούν, όπου είναι απαραίτητο, για να συμμορφωθούν με νομικές απαιτήσεις όπως τα άρθρα 16 και 17 του GDPR. Τα Blockchains, ωστόσο, καθιστούν αυτές τις τροποποιήσεις των δεδομένων σκόπιμα δύσκολες, προκειμένου να διασφαλιστεί η ακεραιότητα των δεδομένων και να αυξηθεί η εμπιστοσύνη στο δίκτυο. Ο προσδιορισμός του

κατά πόσον η τεχνολογία κατανεμημένου καθολικού μπορεί, να είναι σε θέση να συμμορφωθεί με το άρθρο 17 του GDPR, δυσκολεύει από τον αβέβαιο ορισμό της «διαγραφής» στο ίδιο άρθρο.

Η μελέτη κατέληξε στο συμπέρασμα ότι μπορεί να είναι ευκολότερο για τα ιδιωτικά και με άδεια blockchains να συμμορφωθούν με αυτές τις νομικές απαιτήσεις, σε αντίθεση με τα ιδιωτικά και χωρίς άδεια blockchains. Ωστόσο, τονίστηκε επίσης ότι η συμβατότητα αυτών των πράξεων με τον κανονισμό μπορεί να αξιολογηθεί μόνο κατά περίπτωση. Πράγματι, τα blockchains είναι στην πραγματικότητα μια κατηγορία τεχνολογιών με διαφορετικά τεχνικά χαρακτηριστικά και ρυθμίσεις διακυβέρνησης. Αυτό σημαίνει ότι δεν είναι δυνατή η αξιολόγηση της συμβατότητας μεταξύ του «blockchain» και της νομοθεσίας της ΕΕ για την προστασία των δεδομένων. Αντίθετα, αυτή η μελέτη έχει προσπαθεί να χαρτογραφήσει διάφορους τομείς του GDPR με τα χαρακτηριστικά που γενικά μοιράζονται αυτή η κατηγορία τεχνολογιών, και να επιστήσει την προσοχή στο πώς αποχρώσεις στη διαμόρφωση blockchains »μπορεί να επηρεάσει την ικανότητά τους να συμμορφώνονται με τις σχετικές νομικές απαιτήσεις.

Το βασικό στοιχείο της μελέτης αυτής είναι ότι είναι αδύνατο να δηλώσουμε ότι τα blockchains είναι, στο σύνολό τους, είτε πλήρως συμβατά είτε μη συμμορφούμενα με τον GDPR. Αντιθέτως, κάθε συγκεκριμένη περίπτωση χρήσης πρέπει να εξετάζεται βάσει λεπτομερούς ανάλυσης κατά περίπτωση. Το δεύτερο βασικό στοιχείο που τονίζεται σε αυτή τη μελέτη είναι ότι η ασυμβατότητα μεταξύ πολλών βασικών χαρακτηριστικών της εγκατάστασης τεχνολογιών blockchain και ορισμένων στοιχείων της ευρωπαϊκής νομοθεσίας για την προστασία των δεδομένων, δεν θα πρέπει να αναγάγονται μόνο στα ιδιαίτερα χαρακτηριστικά του DLT. Αντιθέτως, η εξέταση αυτής της τεχνολογίας μέσω του φακού του GDPR αναδεικνύει επίσης σημαντικές εννοιολογικές αβεβαιότητες σε σχέση με τον Κανονισμό που έχουν σημασία που υπερβαίνει τα blockchain. Πράγματι, η ανάλυση κατέδειξε ότι η έλλειψη σαφήνειας όσον αφορά πολυάριθμες έννοιες που περιέχει ο GDPR καθιστά δύσκολο να προσδιοριστεί πώς θα πρέπει να εφαρμοστεί σε αυτήν την τεχνολογία, αλλά και σε άλλες. Αυτό συμβαίνει, για παράδειγμα, όσον αφορά την έννοια των ανώνυμων δεδομένων, τον ορισμό του υπευθύνου επεξεργασίας δεδομένων και την έννοια της «διαγραφής» βάσει του άρθρου 17 του GDPR. Μια περαιτέρω αποσαφήνιση αυτών των εννοιών θα ήταν σημαντική για τη δημιουργία μεγαλύτερης νομικής σαφήνειας για όσους

επιθυμούν να χρησιμοποιήσουν το DLT, αλλά και πέρα από αυτό να ενισχύσουν την ευρωπαϊκή οικονομία δεδομένων μέσω της αυξημένης σαφήνειας του δικαίου.

Η μελέτη, ωστόσο, τονίζει επίσης ότι τα blockchains μπορούν να προσφέρουν οφέλη από την άποψη της προστασίας των δεδομένων. Είναι σημαντικό ότι αυτό δεν συμβαίνει αυτόματα. Αντίθετα, τα blockchains πρέπει να σχεδιαστούν σκόπιμα για να γίνει αυτό. Σε αυτή την περίπτωση, μπορούν να προσφέρουν νέες μορφές διαχείρισης δεδομένων που παρέχουν οφέλη στην οικονομία που βασίζεται στα δεδομένα και να επιτρέπουν στα υποκείμενα των δεδομένων να έχουν μεγαλύτερο έλεγχο επί των δεδομένων προσωπικού χαρακτήρα που τους αφορούν.

Βάσει αυτών των παρατηρήσεων, η μελέτη διατύπωσε τρεις ευρείες συστάσεις πολιτικής, οι οποίες έχουν χωριστεί σε διάφορα στοιχεία. Πρώτον, προτάθηκε η παροχή κανονιστικών κατευθυντήριων γραμμών σχετικά με την ερμηνεία ορισμένων στοιχείων του GDPR όταν εφαρμόζεται στα blockchains, ώστε να δημιουργηθεί μεγαλύτερη σαφήνεια του δικαίου σε αυτόν τον τομέα. Δεύτερον, συνιστάται να ενθαρρύνονται και να υποστηρίζονται κώδικες δεοντολογίας και μηχανισμοί πιστοποίησης. Τρίτον, συνιστάται να διατίθεται χρηματοδότηση για διεπιστημονική έρευνα που θα διερευνά πώς οι λύσεις τεχνικού σχεδιασμού και διακυβέρνησης των blockchains θα μπορούσαν να προσαρμοστούν στις απαιτήσεις του GDPR και κατά πόσον μπορεί να είναι δυνατά πρωτόκολλα που συμμορφώνονται εκ σχεδιασμού.

Σε άρθρο του CNIL του 2018 για τη συμβατότητα του Blockchain με το GDPR σε σχέση με τα προσωπικά δεδομένα [19] αφού παρουσιάζεται περιληπτικά η τεχνολογία Blockchain και τα χαρακτηριστικά διαφόρων τύπων blockchain, αναφέρει πως μετά από ανάλυση το CNIL κατέληξε ότι το Blockchain κατέληξε ότι ενα blockchain μπορεί να περιέχει δύο κατηγορίες προσωπικών δεδομένων:

- τα αναγνωριστικά των συμμετεχόντων και των miners: κάθε συμμετέχων/miner έχει δημόσιο κλειδί, διασφαλίζοντας την ταυτοποίηση του εκδότη και του παραλήπτη μιας συναλλαγής·

- πρόσθετα στοιχεία μπορεί να περιέχονται "εντός" μιας συναλλαγής (π.χ. δίπλωμα, πράξη ιδιοκτησίας). Εάν τα δεδομένα αυτά αφορούν φυσικά πρόσωπα, ενδεχομένως άλλα από τους συμμετέχοντες, τα οποία ενδέχεται να αναγνωρίζονται άμεσα ή έμμεσα, τα δεδομένα αυτά θεωρούνται δεδομένα προσωπικού χαρακτήρα.

Με τη χρήση αυτής της διάκρισης, εφαρμόζεται η συνήθης ανάλυση του GDPR περί προσδιορισμού του υπευθύνου επεξεργασίας δεδομένων, επιβολής δικαιωμάτων, εφαρμογής κατάλληλων διασφαλίσεων, υποχρεώσεις ασφάλειας κ.λπ.

Η λύση που προτείνει το CNIL είναι ότι όσον αφορά το ρόλο των διαφόρων παραγόντων, σε πολλές περιπτώσεις, ο συμμετέχων (δηλαδή το πρόσωπο που αποφασίζει να καταχωρήσει δεδομένα σε ένα blockchain) μπορεί να θεωρηθεί ως υπεύθυνος επεξεργασίας δεδομένων, δεδομένου ότι ο συμμετέχων καθορίζει το σκοπό και τα μέσα επεξεργασίας δεδομένων. Όσον αφορά την άσκηση των δικαιωμάτων, ορισμένα δικαιώματα μπορούν να ασκηθούν αποτελεσματικά, όπως το δικαίωμα πρόσβασης και το δικαίωμα φορητότητας. Όσον αφορά το δικαίωμα διαγραφής, το δικαίωμα διόρθωσης και το δικαίωμα εναντίωσης στην επεξεργασία, η CNIL αναγνωρίζει την ύπαρξη τεχνολογικών λύσεων που πρέπει να αξιολογηθούν. Χωρίς να έχουν απολύτως πανομοιότυπα αποτελέσματα, οι λύσεις αυτές επιτρέπουν στα ενδιαφερόμενα μέρη να έρθουν πιο κοντά στις απαιτήσεις συμμόρφωσης του GDPR, ιδίως εμποδίζοντας την πρόσβαση στα δεδομένα ανάλογα με τη μορφή που έχει επιλεγεί (π.χ. δέσμευση, δακτυλικό αποτύπωμα που παράγεται από μια λειτουργία κατακερματισμού με κλειδί, κρυπτογράφηση κ.λπ.). Ως εκ τούτου, θα πρέπει να εξεταστεί η συμμόρφωσή τους με τον GDPR. Επιπλέον, γενικότερα, είναι σημαντικό να μην αποθηκεύονται τα προσωπικά δεδομένα σε μη κρυπτογραφημένο κείμενο σε ένα blockchain. Επιπλέον, οι αρχές που αφορούν την ασφάλεια των δεδομένων εξακολουθούν να ισχύουν πλήρως για τα blockchains.

Σε κάθε περίπτωση, η διενέργεια εκτίμησης επιπτώσεων για την προστασία των δεδομένων (DPIA) θα μπορούσε να επιτρέψει την ανάλυση της αναγκαιότητας και της αναλογικότητας του μηχανισμού και, όπου απαιτείται, να επιτρέψει τον εντοπισμό περιπτώσεων στις οποίες άλλες λύσεις μπορεί να είναι καταλληλότερες.

Στο άρθρο του A. Doychev στο Medium.com το 2019 [27] σχετικά με τις σχέσεις Blockchains, DLT και GDPR, αναφέρεται ότι όταν ο GDPR παρουσιάστηκε από την Ευρωπαϊκή Επιτροπή για πρώτη φορά το 2012, οι τεχνολογίες blockchain εξακολουθούσαν να μην ήταν τόσο δημοφιλείς και σαφώς, δεν ήταν το επίκεντρο του κανονισμού.

Όπως αναφέρει, τα συστήματα που βασίζονται στο Blockchain έχουν τη δυνατότητα να παρέχουν καλύτερη προστασία στα προσωπικά δεδομένα από τα παραδοσιακά συστήματα αποθήκευσης δεδομένων που θεωρούνται συμβατά με τον GDPR. Μερικά από τα χαρακτηριστικά της τεχνολογίας blockchain, όπως η ψευδωνυμοποίηση των προσωπικών πληροφοριών και το αποκεντρωμένο μοντέλο του δικτύου, παρέχουν καλύτερη προστασία από επιθέσεις και καθιστούν τα δεδομένα λιγότερο ευάλωτα σε καταχρήσεις/παραβιάσεις σε σύγκριση με το κεντρικά ελεγχόμενο μοντέλο δεδομένων.

Ωστόσο, όπως αναφέρεται, εάν το γράμμα του κανονισμού τηρηθεί αυστηρά, τα ανοικτά δημόσια blockchains έχουν μια σειρά από ζητήματα που σχετίζονται με τις απαιτήσεις του GDPR:

- Το πρωτόκολλο Bitcoin και τα δημόσια blockchains, γενικά, περιέχουν πληροφορίες που δεν είναι πραγματικά ανώνυμες. Αντιθέτως, είναι ψευδώνυμες, και ως εκ τούτου θεωρούνται προσωπικά δεδομένα και δεν είναι τεχνικά αδύνατο να συνδεθεί μια διεύθυνση bitcoin με ένα αναγνωρίσιμο φυσικό πρόσωπο.
- Η λογική και η ορολογία του GDPR, με την έννοια του "υποκειμένου των δεδομένων", του "υπευθύνου επεξεργασίας δεδομένων" και του "εκτελούντος την επεξεργασία δεδομένων", φαίνεται δύσκολο να εφαρμοστεί στα blockchains. Υπάρχει έλλειψη σαφήνειας ως προς το ποιος είναι ποιος στο blockchain και ποιες είναι οι υποχρεώσεις τους σύμφωνα με τον GDPR.
- Αλλά το πιο προβληματικό σημείο των δημόσιων blockchains σε σχέση με τον GDPR είναι η απαίτηση ότι το αντικείμενο δεδομένων έχει "το δικαίωμα να ξεχαστεί", πράγμα που σημαίνει ότι κάθε άτομο έχει το δικαίωμα να ζητήσει τη διαγραφή των προσωπικών του δεδομένων από τα πρακτικά. Η διαγραφή ή η τροποποίηση δεδομένων σχετικά με το blockchain είναι σχεδόν αδύνατη, καθώς τα δεδομένα έχουν ήδη μεταδοθεί σε όλους τους συμμετέχοντες στο δίκτυο. Επιπλέον, η διαγραφή μιας εγγραφής θα άλλαζε τον κατακερματισμό του αντίστοιχου μπλοκ που περιέχει τα δεδομένα και θα ακύρωνε όλα τα επακόλουθα μπλοκ.

Το άρθρο συμπεραίνει ότι τα τροποποιημένα DLT θα μπορούσαν να δώσουν απάντηση στο πρόβλημα της συμμόρφωσης με τις απαιτήσεις του GDPR λόγω της μεγαλύτερης σχεδιαστικής ευελιξίας που έχουν:

- Ενώ οποιοσδήποτε μπορεί να συμμετάσχει στο ανοιχτό δημόσιο blockchain, το DLT επιτρέπει λύσεις όπου η πρόσβαση στο δίκτυο είναι κατόπιν άδειας. Οι ρόλοι και οι ευθύνες των συμμετεχόντων σε ένα τέτοιο δίκτυο είναι πιο εύκολο να προσδιοριστούν και υπάρχει καλύτερη λογοδοσία όσον αφορά την προστασία των δεδομένων.
- Μια αρχιτεκτονική DLT θα μπορούσε να σχεδιαστεί έτσι ώστε τα δεδομένα συναλλαγών να μην μεταδίδονται σε ολόκληρο το δίκτυο. Αντίθετα, μόνο τα εμπλεκόμενα μέρη μπορούν να το λάβουν με βάση την «ανάγκη να γνωρίζουν». Μια τέτοια προσέγγιση επιτρέπει μικρότερο πολλαπλασιασμό δεδομένων σε σύγκριση με το παγκόσμιο μοντέλο εκπομπής.
- Ο μηχανισμός συναίνεσης στο DLT θα μπορούσε να βασίζεται στην επικύρωση συναλλαγών από συγκεκριμένους συμμετέχοντες, αντί για ολόκληρο το δίκτυο. Η διάδοση δεδομένων μειώνεται, παρέχοντας ένα πιο ασφαλές περιβάλλον. Ο μηχανισμός επαλήθευσης μπλοκ (mining), που καθιστά αδύνατη τη διαγραφή δεδομένων, αποφεύγεται εντελώς.

Η λύση που προτείνεται στο άρθρο είναι το Corda και αναφέρονται οι ιδιαιτερότητες του που το κάνουν συμβατό με τις απαιτήσεις του GDPR όπως: πρόσβαση κατόπιν αδείας, συναλλαγές σημείο-προς-σημείο που επαληθεύονται από ειδικούς συμμετέχοντες και το γεγονός ότι είναι ανοικτού κώδικα, μπορεί όποιος θέλει να το διαμορφώσει στις δικές του απαιτήσεις και να έχει την πλήρη ευθύνη σε σχέση με τις απαιτήσεις του GDPR.

Επιπλέον το Corda έχει κάποιες διαδικτυακές υπηρεσίες που σχεδιάστηκαν για να αυξήσουν την συμμορφωση προς το GDPR και την προστασία των προσωπικών δεδομένων. Αυτά είναι:

- Η υπηρεσία Doorman που συλλέγει πληροφορίες από χρήστες και χειριστές που συμμετέχουν στο επιχειρηματικό δίκτυο, συμπεριλαμβανομένων προσωπικών δεδομένων, όπως όνομα επαφής, αριθμός τηλεφώνου ή διεύθυνση email. Τα δεδομένα αποθηκεύονται σε μια ιδιωτική, ασφαλή βάση δεδομένων και δεν μεταδίδονται στο δίκτυο. Εάν ένα συμβαλλόμενο μέρος αποχωρήσει ή εκδιωχθεί από

το δίκτυο, τυχόν προσωπικά δεδομένα που ανήκουν σε αυτό το συμβαλλόμενο μέρος θα διαγραφούν, με την επιφύλαξη για τυχών ρυθμιστικούς κανόνες που επιβάλλουν την φύλαξη ή/και καταγραφή δεδομένων και υπό την προϋπόθεση ότι δεν υπάρχει επιχειρηματικός λόγος για την αποθήκευσή του. Ρυθμίζοντας αυτήν τη διαδικασία, το Corda συμμορφώνεται με την απαίτηση του GDPR για το "Δικαίωμα να ξεχασθεί" το υποκείμενο των δεδομένων και τη διαγραφή τη διαγραφή αυτών.

- Η υπηρεσία χαρτών δικτύου (network map service) επιτρέπει στους συμμετέχοντες να βρίσκουν και να επικοινωνούν μεταξύ τους μέσω του δικτύου. Δεν μοιράζονται προσωπικά δεδομένα μεταξύ των συμμετεχόντων στο δίκτυο ως μέρος αυτής της υπηρεσίας.
- Η υπηρεσία συμβολαιογράφου (Notary) παρέχει τη συναίνεση του δικτύου και εγγυάται τη μοναδικότητα και το τελικό αποτέλεσμα κάθε συναλλαγής. Επί του παρόντος, το Corda Network Foundation παρέχει μόνο μη επικυρωμένους συμβολαιογράφους που βλέπουν μόνο ένα υποσύνολο μιας συναλλαγής για να καθορίσουν την υλοποίηση και τη μοναδικότητά της. Δεν γίνεται επεξεργασία ή αποθήκευση προσωπικών δεδομένων από την υπηρεσία.
- Η υιοθέτηση πολιτικών σε σχέση με παραβίαση των δεδομένων για ενημέρωση μέσα σε 72 ώρες από τότε που έγινε αντιληπτή όλων των συμμετεχόντων, της επιβλέπουσας αρχής (αν κινδυνεύουν τα δικαιώματα και στοιχεία φυσικών προσώπων) και του διοικητικού συμβουλίου του Corda Network Foundation.

1.3 Συμπεράσματα

Από όσα παρουσιάστηκαν είναι προφανές ότι υπάρχει μεγάλο ερευνητικό, ακαδημαϊκό, επιχειρηματικό και νομοθετικό ενδιαφέρον σχετικά με τις δυνατότητες εφαρμογής της blockchain τεχνολογίας στον κλάδο Fintech και για την προστασία των προσωπικών δεδομένων στα πλαίσια του GDPR.

Η δυναμική του Fintech δημιουργεί μια πίεση για υιοθέτηση νέων τεχνολογιών και εναρμόνιση των νόμων και κανονισμών στις απαιτήσεις της νέας εποχής όπως φαίνεται από πλειάδα εποπτικών αρχών που έχουν ασχοληθεί με το φαινόμενο (FSB, EBA, ECB κ.α.). Τεχνολογίες όπως το blockchain δημιουργούν προσδοκίες για ενίσχυση του κλάδου λόγω της

καινοτομίας και των αλλαγών που φέρνουν. Εργασίες όπως αυτή των Woo Young Moon and Soo Dong Kim δείχνουν ότι είναι δυνατή η προσαρμογή της τεχνολογίας ώστε να εξυπηρετηθεί η βελτιστοποίηση των υπηρεσιών συναλλαγών. Κάτι ανάλογο επισημαίνουν οι Polyviou A., Velanas P., and Soldatos J αναφέροντας κάποια πεδία εφαρμογής και επισημαίνοντας παράλληλα, ότι εκτός του Bitcoin η τεχνολογία αυτή δεν έχει δοκιμαστεί σε μεγάλη κλίμακα.

Οι αλλαγές που επιφέρουν στο ρυθμιστικό τοπίο οι κανονισμοί GDPR και PSD2 δημιουργούν, νέες συνθήκες και απαιτήσεις αυξάνοντας σημαντικά το βαθμό δυσκολίας για την υιοθέτηση νέων τεχνολογιών. Όλα αυτά ενώ παράλληλα διαπιστώνονται κενά και αδυναμίες της νέας τεχνολογίας σε σχέση με την ασφάλεια και την προστασία των προσωπικών δεδομένων.

Η μελέτη του Michèle Finck για λογαριασμό του Ευρωπαϊκού Συμβουλίου κατέληξε ότι είναι αδύνατο να δηλώσουμε ότι τα blockchains είναι, στο σύνολό τους, είτε πλήρως συμβατά είτε μη συμμορφούμενα με τον GDPR. Αντιθέτως, κάθε συγκεκριμένη περίπτωση χρήσης πρέπει να εξετάζεται βάσει λεπτομερούς ανάλυσης κατά περίπτωση. Τα blockchains μπορούν να προσφέρουν οφέλη από την άποψη της προστασίας των δεδομένων, αλλά δεν συμβαίνει αυτόματα, πρέπει να σχεδιαστούν σκόπιμα για να γίνει αυτό. Το άρθρο του A. Doychev στο Medium.com απαντάει στα πιο πάνω ζητήματα χωρίς να υπεισέρχεται σε λεπτομέρειες.

Από τα πιο πάνω συμπεραίνεται ότι οι περισσότερες δημοσιεύσεις ασχολούνται με την μία ή την άλλη ή μερικό συνδυασμό των βασικών εννοιών του ερευνητικού θέματος. Πέρα από τις επιμέρους διαπιστώσεις ή γενικές λύσεις που προτείνονται δεν καλύπτονται όλες τις πτυχές του ερευνητικού προβλήματος. Για αυτό έχει ακαδημαϊκή αξία η περαιτέρω διερεύνηση , ειδικά από τη στιγμή που θα γίνει συνδυαστικά, σε μεγαλύτερο βάθος και με μεγαλύτερη εξειδίκευση όσον αφορά τη λύση που θα προταθεί. Στα πλαίσια της παρούσας μεταπτυχιακής διατριβής θα γίνει προσπάθεια να καλυφθεί όσο το δυνατόν περισσότερο το πιο πάνω κενό ερευνώντας τις αλληλεπιδράσεις blockchain-Fintech, blockchain-GDPR και Fintech-GDPR με γνώμονα τα προσωπικά δεδομένα και την ασφάλεια των συναλλαγών. Στη συνέχεια θα γίνει προσπάθεια να προταθεί μια όσο το δυνατόν πιο συγκεκριμένη λύση που να καλύπτει όλα τα ζητούμενα.

Κεφάλαιο 2

Fintech

2.1 Τι είναι

Fintech είναι η συντομογραφία των λέξεων «financial technology», στα ελληνικά: «χρηματοοικονομική τεχνολογία». Χρησιμοποιείται για να περιγράψει κάθε είδος τεχνολογικής εξέλιξης/εφαρμογής που χρησιμοποιείται για την στήριξη ή την παροχή χρηματοπιστωτικών υπηρεσιών.

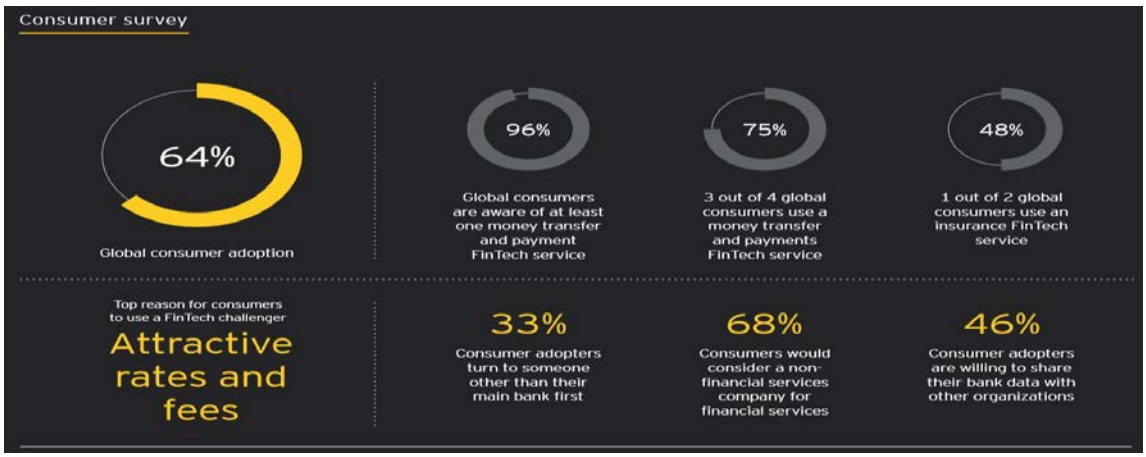
Σύμφωνα με το Investopedia «η financial technology (Fintech) χρησιμοποιείται για να περιγράψει κάθε νέα τεχνολογία που επιδιώκει να βελτιώσει και να αυτοματοποιήσει την παράδοση και τη χρήση των χρηματοοικονομικών υπηρεσιών. Στον πυρήνα της, η χρηματοοικονομική τεχνολογία χρησιμοποιείται για να βοηθήσει τις εταιρείες, τους ιδιοκτήτες επιχειρήσεων και τους καταναλωτές να διαχειρίζονται καλύτερα τις οικονομικές δραστηριότητές τους, τις διαδικασίες και τις ζωές τους αξιοποιώντας εξειδικευμένο λογισμικό και αλγόριθμους που χρησιμοποιούνται σε υπολογιστές και, όλο και περισσότερο, έξυπνα κινητά» [1].

Το Wikipedia αναφέρει ότι «μετά την αναθεώρηση περισσότερων από 200 επιστημονικών εγγράφων/εργασιών που αναφέρουν τον όρο "fintech", μια μελέτη

σχετικά με τον ορισμό της χρηματοοικονομικής τεχνολογίας κατέληξε στο συμπέρασμα ότι "fintech είναι ένας νέος χρηματοοικονομικός κλάδος που εφαρμόζει τεχνολογία για τη βελτίωση των χρηματοοικονομικών δραστηριοτήτων". Fintech είναι οι νέες εφαρμογές, διεργασίες, προϊόντα ή επιχειρηματικά μοντέλα στον τομέα των χρηματοοικονομικών υπηρεσιών, που αποτελούνται από μία ή περισσότερες συμπληρωματικές χρηματοοικονομικές υπηρεσίες και παρέχονται ως τελική διαδικασία μέσω του Διαδικτύου. Fintech μπορεί, επίσης, να θεωρηθεί ως «οποιεσδήποτε καινοτόμες ιδέες που βελτιώνουν τις διαδικασίες χρηματοοικονομικών υπηρεσιών προτείνοντας τεχνολογικές λύσεις σύμφωνα με διαφορετικές επιχειρηματικά καταστάσεις, ενώ οι ιδέες θα μπορούσαν επίσης να οδηγήσουν σε νέα επιχειρηματικά μοντέλα ή ακόμη και σε νέες επιχειρήσεις». Ο στόχος των εταιρειών «fintech», παλαιών και νέων, είναι η βελτίωση των χρηματοοικονομικών διεργασιών και η αύξηση της αυτοματοποίησης στη βιομηχανία» [2].

Η Ευρωπαϊκή Κεντρική Τράπεζα με τη σειρά της αναφέρει ότι «το Fintech αποτελεί έναν όρο για κάθε είδους τεχνολογική καινοτομία που χρησιμοποιείται για την υποστήριξη ή την παροχή χρηματοοικονομικών υπηρεσιών. Οδηγεί σε πολλές αλλαγές στον χρηματοπιστωτικό τομέα, οδηγώντας σε μια σειρά νέων επιχειρηματικών μοντέλων, εφαρμογών, διεργασιών και προϊόντων. Οι εταιρείες χρηματοοικονομικής τεχνολογίας βάζουν την τεχνολογική καινοτομία στον πυρήνα της επιχείρησής τους. Μπορεί να είναι ιδιαίτερα ενεργοί σε τομείς όπως οι υπηρεσίες πληρωμών, η βαθμολόγηση πίστωσης και οι αυτοματοποιημένες επενδυτικές συμβουλές, χρησιμοποιώντας τεχνητή νοημοσύνη, μεγάλα δεδομένα (big data) ή Blockchain.» [3]

Είναι προφανές ότι το fintech ή χρηματοοικονομική τεχνολογία ήρθε για να μείνει, είναι το μέλλον στον χρηματοοικονομικό τομέα. Έχει αλλάξει και θα αλλάξει ακόμα περισσότερο τον τρόπο που συναλλασσόμαστε.

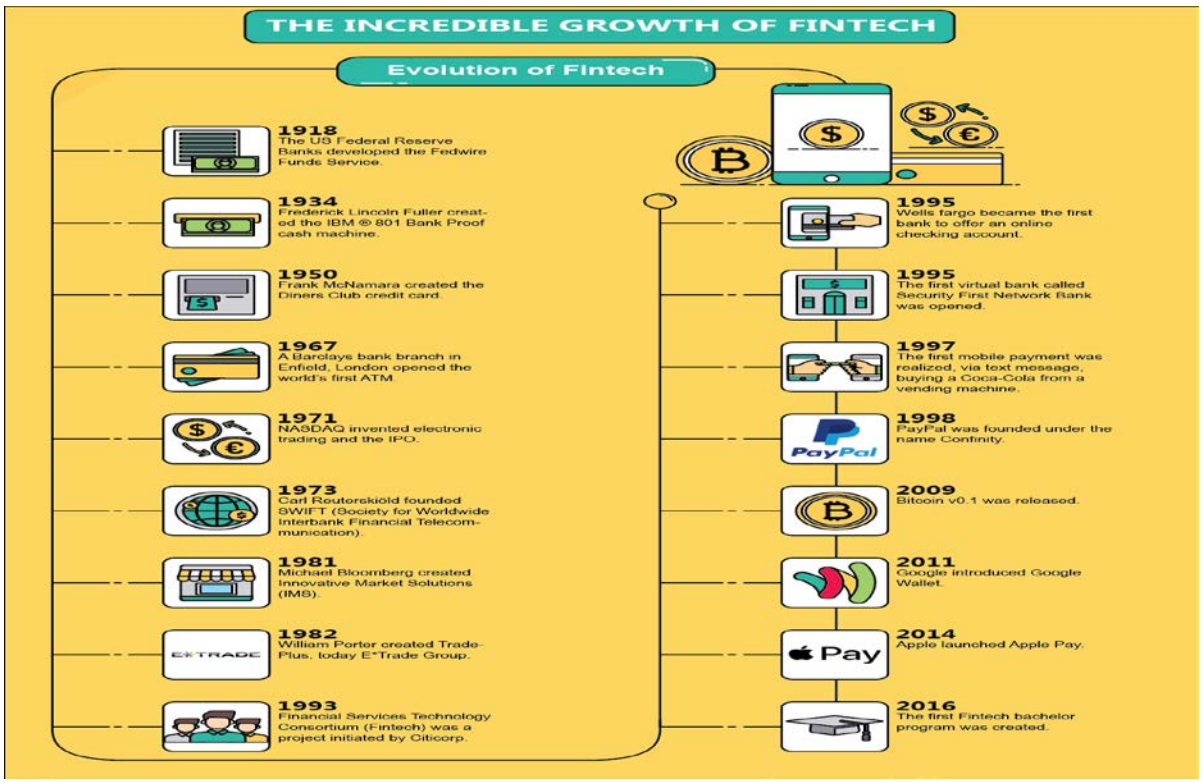


Εικόνα 1: Πηγή: ΕΥ, «Global FinTech Adoption Index 2019» σελ.5

2.2 Ιστορία και εξέλιξη του Fintech

Η «χρηματοοικονομική τεχνολογία», ή «fintech», αναφέρεται στη χρήση της τεχνολογίας για την παροχή χρηματοοικονομικών λύσεων. Ο όρος μπορεί να εντοπιστεί στις αρχές της δεκαετίας του 1990, και τώρα αναφέρεται σε μια πολύ ταχέως αναπτυσσόμενη βιομηχανία. Ωστόσο, μόνο από το 2014 ο τομέας έχει προσελκύσει τη εστιασμένη προσοχή των ρυθμιστικών αρχών, των συμμετεχόντων στη βιομηχανία, των καταναλωτών και των ακαδημαϊκών.[4]

Είναι σημαντικό να διακρίνουμε τρεις κύριες εποχές της εξέλιξης της χρηματοοικονομικής τεχνολογίας. Από περίπου το 1866 έως το 1967, ο κλάδος των χρηματοπιστωτικών υπηρεσιών παρέμεινε σε μεγάλο βαθμό αναλογικός, παρά το γεγονός ότι συνδεόταν στενά με την τεχνολογία. Την περίοδο αυτή την χαρακτηρίζουμε σαν Fintech 1.0. Από το 1967 έως το 2008, η χρηματοοικονομική ήταν όλο και πιο ψηφιοποιημένη λόγω της ανάπτυξης της ψηφιακής τεχνολογίας για τις επικοινωνίες και τις συναλλαγές. Η περίοδος αυτή χαρακτηρίζεται ως Fintech 2.0. Από το 2008, κατά την περίοδο που χαρακτηρίζονται ως Fintech 3.0, καινούργιες νεοφυείς (start-ups) επιχειρήσεις και καθιερωμένες εταιρείες τεχνολογίας έχουν αρχίσει να παράγουν χρηματοοικονομικά προϊόντα και υπηρεσίες απευθείας για τις επιχειρήσεις, το κοινό και τις τράπεζες[4].



Εικόνα 2: Πηγή: 16best.net, «The Incredible Growth of Fintech (Infographic)», 2017

2.2.1 Fintech .1.0

Από τα πρώτα στάδια, η χρηματοοικονομική και η τεχνολογία είναι αλληλένδετοι και αλληλοενισχυόμενοι κλάδοι. Η χρηματοοικονομική γεννήθηκε από την ανάγκη τα διοικητικά συστήματα να μεταβούν από τη φάση των ομάδων κυνηγών-συλλεκτών στη φάση των σταθερών γεωργικών κρατών. Τα χρήματα είναι μια τεχνολογία που επικυρώνει μεταβιβάσιμες αξίες, και η εμφάνιση πρώιμων τεχνολογιών υπολογισμού όπως ο άβακας διευκόλυναν σημαντικά τις χρηματοοικονομικές συναλλαγές. Η χρηματοοικονομική εξελίχθηκε παράλληλα με το εμπόριο και η διπλογραφική λογιστική εμφανίστηκε στα τέλη του Μεσαίωνα και της Αναγέννησης. Πολλοί ιστορικοί συμμερίζονται την άποψη ότι η Ευρωπαϊκή χρηματοοικονομική επανάσταση στα τέλη του 1600, η οποία περιελάμβανε κοινοπραξίες, ασφάλειες και τραπεζικές συναλλαγές, όλες με βάση τη διπλογραφική λογιστική, ήταν ουσιώδης για τη βιομηχανική επανάσταση. Έτσι, η σχέση μεταξύ της χρηματοοικονομικής και της τεχνολογία έθεσε τα θεμέλια για τη σύγχρονη περίοδο. Στα τέλη του 19ου αιώνα, τεχνολογίες όπως ο τηλέγραφός, ο σιδηρόδρομος και τα ατμόπλοια ενίσχυσαν τις χρηματοοικονομικές διασυνοριακές διασυνδέσεις. Στη συνέχεια, οι τεχνολογικές εξελίξεις μετά τον Πρώτο Παγκόσμιο Πόλεμο προχώρησαν ταχέως. Μέχρι εκείνη την περίοδο, είχε εγκαθιδρυθεί

ένα παγκόσμιο δίκτυο τέλεξ, το οποίο παρείχε την τηλεπικοινωνιακή βάση πάνω στην οποία θα αναπτυσσόταν το επόμενο στάδιο της χρηματοοικονομικής τεχνολογίας. [4]

2.2.2 Fintech 2.0 (1967 – 2008)

Στα τέλη της δεκαετίας του 1960 και της δεκαετίας του 1970, τα συστήματα ηλεκτρονικών πληρωμών είχαν ταχεία εξέλιξη. Το γραφείο διατραπεζικών υπολογιστών (Inter-Bank Computer Bureau) ιδρύθηκε στο Ηνωμένο Βασίλειο το 1968, αποτελώντας τη βάση των σημερινών Αυτόματων Υπηρεσιών Εκκαθάρισης των Τραπεζιτών (Bankers' Automated Clearing Services). Το σύστημα διατραπεζικών πληρωμών των ΗΠΑ ιδρύθηκε το 1970 και το Fedwire έγινε ηλεκτρονικό σύστημα στις αρχές της δεκαετίας του 1970. Αντικατοπτρίζοντας την ανάγκη διασύνδεσης των εγχώριων συστημάτων πληρωμών, η Κοινωνία των Παγκόσμιων Διατραπεζικών Χρηματοοικονομικών Τηλεπικοινωνιών ιδρύθηκε το 1973, με την κατάρρευση της Τράπεζας Χέρστατ να ακολουθεί το 1974, η οποία τόνισε τους κινδύνους από τις αυξημένες διεθνείς οικονομικές διασυνδέσεις. Αυτή η κρίση πυροδότησε την πρώτη μείζονα ρυθμιστική εστίαση στην χρηματοοικονομική τεχνολογία, με τη σύσταση της Επιτροπής Τραπεζικής Εποπτείας της Βασιλείας της Τράπεζας Διεθνών Διακανονισμών το 1975, η οποία οδηγεί σε μια σειρά διεθνών συμφωνιών ήπιας νομοθεσίας.

Το 1987, οι χρηματιστηριακές αγορές σε όλο τον κόσμο κατέρρευσαν την «Μαύρη Δευτέρα». Οι επιπτώσεις της κατάρρευσης ήταν ένας σαφής δείκτης ότι οι παγκόσμιες αγορές ήταν τεχνολογικά αλληλένδετες. Η αντίδραση οδήγησε στην εισαγωγή «διακοπτών κυκλώματος» για τον έλεγχο της ταχύτητας των μεταβολών των τιμών και οδήγησε τις ρυθμιστικές αρχές κινητών αξιών σε όλο τον κόσμο να δημιουργήσουν μηχανισμούς που υποστήριζαν την συνεργασία. Επιπλέον, η «Single European Act 1986», η Bing Bang χρηματοπιστωτική απελευθέρωση στο Ηνωμένο Βασίλειο το 1986 και η Συνθήκη του Μάαστριχτ του 1992, έθεσαν τις βάσεις για την πλήρη διασύνδεση των χρηματοπιστωτικών αγορών της ΕΕ μέχρι τις αρχές του 21ου αιώνα.

Οι πρόοδοι στα μέσα της δεκαετίας του 1990 τόνισαν τους αρχικούς κινδύνους σε σύνθετα μηχανογραφικά συστήματα διαχείρισης κινδύνων, με την κατάρρευση της Long-term Capital Management μετά τις χρηματοοικονομικές κρίσεις της Ασίας και της Ρωσίας του 1997 – 98. Ωστόσο, το επόμενο επίπεδο ανάπτυξης ξεκίνησε το 1995 όταν η Wells Fargo άρχισε να παρέχει ηλεκτρονικές τραπεζικές συναλλαγές στους καταναλωτές.

Μέχρι το 2001, οκτώ τράπεζες των ΗΠΑ είχαν τουλάχιστον 1.000.000 πελάτες στο διαδίκτυο. Στα τέλη της δεκαετίας του 1990, το διαδίκτυο παρείχε τη θεμελιώδη αλλαγή που κατέστησε εφικτό το Fintech 3.0 μια δεκαετία αργότερα. Η ηλεκτρονική τραπεζική και όλες οι εξελίξεις του Fintech 3.0 ήταν προϊόν της νέας εποχής του Διαδικτύου.

Η ρυθμιστική οπτική κατά τη διάρκεια του Fintech 2.0 ήταν ότι, ενώ η ηλεκτρονική τραπεζική ήταν μια ψηφιακή εκδοχή του παραδοσιακού μοντέλου, δημιούργησε νέους κινδύνους. Η τεχνολογία αφαίρεσε την ανάγκη να υπάρχουν οι καταθέτες σε ένα υποκατάστημα, και έτσι θα μπορούσε έμμεσα να διευκολύνει το ηλεκτρονικό bank run. Με τη σειρά της, η άμεση απόσυρση χρημάτων, θα μπορούσε να αυξήσει την πίεση σε ένα χρηματοπιστωτικό ίδρυμα. Οι ρυθμιστικές αρχές αναγνώρισαν επίσης ότι η ηλεκτρονική τραπεζική δημιουργεί νέους πιστωτικούς κινδύνους. Η προσδοκία ήταν επίσης ότι οι πάροχοι ηλεκτρονικής τραπεζικής θα ήταν εξουσιοδοτημένα χρηματοπιστωτικά ιδρύματα, που είναι συνήθως οι μόνες οντότητες που δικαιούνται να αυτοαποκαλούνται ως «τράπεζες». Ωστόσο, το Fintech 3.0 το άλλαξε αυτό [4].

2.2.3 Fintech 3.0 (2008 – σήμερα)

Ένας αριθμός παραγόντων συνδυάστηκε γύρω στο 2007 και 2008 για να παράσχει την απαιτούμενη ώθηση για το Fintech 3.0 στις ανεπτυγμένες χώρες. Εκείνη την περίοδο, η εικόνα των τραπεζών, ειδικά στο ΗΒ και στις ΗΠΑ, κλονίστηκε σοβαρά. Μια έρευνα του 2015 ανέφερε ότι οι Αμερικανοί εμπιστεύονται τις εταιρείες τεχνολογίας περισσότερο από τις τράπεζες για να χειριστούν τα οικονομικά τους. Τα ίδια φαινόμενα υπήρχαν στην Κίνα, όπου πάνω από 2000 (peer-to-peer) δανειοδοτικές πλατφόρμες λειτουργούν εκτός ενός σαφούς ρυθμιστικού πλαισίου και ωστόσο αυτό δεν αποθάρρυνε εκατομμύρια δανειστές και δανειολήπτες, λόγω του χαμηλότερου κόστους, καλύτερης απόδοσης και αυξημένης ευκολίας.

Οι κανονιστικές ρυθμίσεις μετά την οικονομική κρίση αύξησαν τις υποχρεώσεις και το κόστος συμμόρφωσης των τραπεζών και περιόρισαν τις πιστώσεις. Οι υποχρεώσεις κατά την οριοθέτηση και το αυξημένο ρυθμιστικό κεφάλαιο για τις τράπεζες άλλαξαν τα κίνητρα ή την ικανότητά τους να στηρίζονται σε δάνεια χαμηλής αξίας. Οι νέες απαιτήσεις για την προετοιμασία των σχεδίων ανάκαμψης και εξυγίανσης και τη διεξαγωγή προσομοιώσεων ακραίων καταστάσεων αύξησαν περαιτέρω το κόστος των τραπεζών. Το 2008 η παγκόσμια χρηματοπιστωτική κρίση είδε επίσης πολλούς οικονομικούς

επαγγελματίες να απολύονται και στη συνέχεια, να αναζητούν νέες δυνατότητες για τις δεξιότητές τους.

Επιπλέον, η Fintech 3.0 θα ήταν σχεδόν βέβαιο ότι δεν θα είχε προκύψει από την παγκόσμια χρηματοπιστωτική κρίση, αν η κρίση συνέβαινε πέντε χρόνια νωρίτερα. Δύο τεχνολογικές εξελίξεις απαιτούνταν να λάβουν χώρα για να προκύψει η διεπαφή των καταναλωτών και η διαλειτουργικότητα μεταξύ εφαρμογών και υπηρεσιών, και αυτές ήταν η έλευση των smartphone και η ανάπτυξη της εξειδίκευσης των διεπαφών προγραμματισμού εφαρμογών (API).

Οι κρίσιμες διαφορές στο Fintech 3.0 είναι οι εξής:

- πρώτον, ποιος παρέχει χρηματοπιστωτικές υπηρεσίες, με νεοσύστατες επιχειρήσεις και εταιρείες τεχνολογίας που υποκαθιστούν τις τράπεζες για την παροχή εξειδικευμένων υπηρεσιών στο κοινό, τις επιχειρήσεις και τις ίδιες τις τράπεζες.και

- δεύτερον, η ταχύτητα της ανάπτυξης. Σε πολλές αγορές, υπήρξε μια μετατόπιση της νοοτροπίας των πελατών όσον αφορά το ποιος έχει τους πόρους και τη νομιμότητα για την παροχή χρηματοοικονομικών υπηρεσιών, σε συνδυασμό με μια εντελώς νέα ταχύτητα εξέλιξης, ιδίως στις αναδυόμενες αγορές.

Ενώ η περαιτέρω ανάπτυξη της Fintech 3,0 στον Βορρά έχει σημαδευτεί από την παγκόσμια οικονομική κρίση, οι παράλληλες εξελίξεις στον Νότο οδηγούν σε ένα διαφορετικό τρόπο ανάπτυξης της τεχνολογίας. Αποκαλείται Fintech3.5. Ειδικότερα, οι Άρνερ, Μπαρμπέρης και Μπάκλεϊ προσδιορίζουν τις ακόλουθες υποστηρικτικές τάσεις:

1. Πολύ νέοι, ψηφιακά ενημερωμένοι πληθυσμοί που είναι εξοπλισμένοι με κινητές συσκευές.
2. Μια ταχέως αναπτυσσόμενη μεσαία τάξη (αν και αυτό ισχύει περισσότερο για ορισμένες αγορές από άλλες).
3. Αναποτελεσματικές παραδοσιακές κεφαλαιαγορές και χρηματοπιστωτικά ιδρύματα
4. Έλλειψη φυσικής υποδομής (δηλαδή Fintech 2.0),
5. Μια συμπεριφορική προδιάθεση προς την ευκολία παρά προς την εμπιστοσύνη.

6. Ένα τεράστιο κοινό χωρίς πρόσβαση σε χρηματοπιστωτικές υπηρεσίες ·
7. Λιγότερο αυστηρή προστασία των δεδομένων και ανταγωνισμός
8. Ένας δυναμικός ιδιωτικός τομέας με παίκτες πεινασμένους για νέες ευκαιρίες.
9. Ένας δημόσιος τομέας που υποδέχεται θετικά την μεταρρύθμιση της αγοράς και τη διαφοροποίηση που θα μπορούσε να οδηγήσει στην ανάπτυξη.

Οι δυνατότητες της Fintech 3.5 είναι τεράστιες, πάνω από 1,2 δισεκατομμύρια άνθρωποι δεν έχουν ακόμα τραπεζικό λογαριασμό, ενώ η πίστωση είναι πανάκριβη. Τον πρωταγωνιστικό ρόλο για την ανάπτυξη νέων fintech τεχνολογιών τον έχουν οι τηλεπικοινωνιακές εταιρείες.

2.2.4 Ο κλάδος της χρηματοοικονομικής τεχνολογίας σήμερα

Η χρηματοοικονομική τεχνολογία περιλαμβάνει σήμερα πέντε σημαντικούς τομείς:

- **Χρηματοδότηση και επενδύσεις:** η χρηματοοικονομική τεχνολογία εκτείνεται πέρα από εναλλακτικούς χρηματοδοτικούς μηχανισμούς, όπως η χορήγηση δανείων P2P, ώστε να συμπεριληφθεί η χρηματοδότηση μέσω της ίδιας της τεχνολογίας (π.χ. crowdfunding) και η χρήση της τεχνολογίας στις χρηματοπιστωτικές συναλλαγές, όπως οι αλγοριθμικές συναλλαγές. Η χρηματοοικονομική τεχνολογία συμμετέχει επίσης όλο και περισσότερο σε τομείς όπως οι ρομποτικές συμβουλευτικές υπηρεσίες.

- **Εσωτερικές χρηματοοικονομικές λειτουργίες και διαχείριση κινδύνων:** αυτές ήταν οι βασικές κινητήριες δυνάμεις των δαπανών IT από τα χρηματοπιστωτικά ιδρύματα, καθώς έχουν χτίσει καλύτερα συστήματα συμμόρφωσης. Για παράδειγμα, οι μηχανικοί υπολογιστών/πληροφορικής αποτελούν περίπου το ένα τρίτο του προσωπικού των 33.000 της Goldman Sachs.

- **Πληρωμές και υποδομές:** οι πληρωμές αποτέλεσαν έναν τομέα μεγάλης κανονιστικής προσοχής από τη δεκαετία του 1970, με αποτέλεσμα την ανάπτυξη τόσο εγχώριων όσο και διασυνοριακών συστημάτων ηλεκτρονικών πληρωμών. Ομοίως, οι υποδομές για την εμπορία αξιογράφων και τον διακανονισμό και τις συναλλαγές εξωχρηματιστηριακών παραγώγων είναι κεντρικές, και οι εταιρείες

πληροφορικής και τηλεπικοινωνιών αναζητούν ευκαιρίες για να παίξουν τον ρόλο του ενδιάμεσου στα παραδοσιακά ιδρύματα.

- **Ασφάλεια δεδομένων και δημιουργία εσόδων:** η ψηφιοποίηση του χρηματοπιστωτικού κλάδου σημαίνει ότι είναι ιδιαίτερα ευάλωτη στο έγκλημα στον κυβερνοχώρο και στην κατασκοπεία. Αυτό θα εξακολουθήσει να αποτελεί μείζονα ανησυχία για τις κυβερνήσεις, τους υπεύθυνους χάραξης πολιτικής, τις ρυθμιστικές αρχές, τους συμμετέχοντες στη βιομηχανία και τους πελάτες. Ωστόσο, η καινοτομία της χρηματοοικονομικής τεχνολογίας είναι σαφώς παρούσα στη χρήση «big data» για την ενίσχυση της αποδοτικότητας και της διαθεσιμότητας των χρηματοοικονομικών υπηρεσιών.

- **Διεπαφή (interface) καταναλωτή:** η διεπαφή καταναλωτή προσφέρει το μεγαλύτερο πεδίο ανταγωνισμού με τον παραδοσιακό χρηματοπιστωτικό σύστημα, καθώς οι εταιρείες τεχνολογίας μπορούν να αξιοποιήσουν τις προϋπάρχουσες βάσεις πελατών τους για την ανάπτυξη νέων χρηματοοικονομικών προϊόντων. Είναι ενδιαφέρον ότι στις αναπτυσσόμενες χώρες αυτό το φαινόμενο είναι πιο εμφανές.

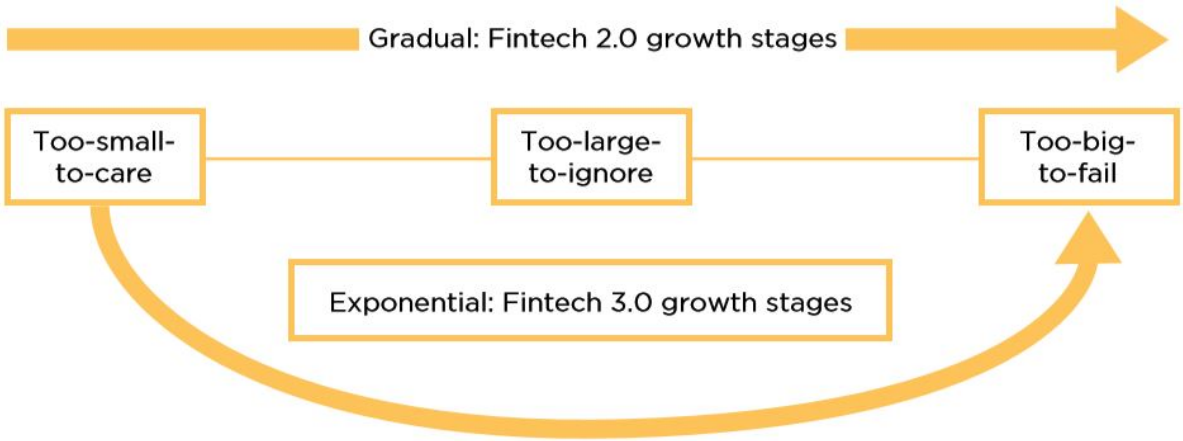
2.2.5 Ρυθμιστική εξέλιξη

Οι καθιερωμένοι χρηματοοικονομικοί φορείς, οι τεχνολογικές εταιρείες και οι ρυθμιστικές αρχές συνεργάζονται καλά για την ανάπτυξη κανονισμών μέσω διαβούλευσης με την αγορά, ωστόσο, νέοι Fintech 3.0 παίκτες εισέρχονται στη βιομηχανία χωρίς κουλτούρα χρηματοπιστωτικής συμμόρφωσης, και με περιορισμένη προϋπάρχουσα αλληλεπίδραση με τις ρυθμιστικές αρχές. Προς το παρόν, σε πολλές χώρες, υπάρχει αβεβαιότητα όσον αφορά τους νόμους και τις διαδικασίες που ισχύουν για τις νέες εταιρείες χρηματοοικονομικής τεχνολογίας.

Η τεχνολογία χρειάζεται χρόνο για να βρει την τελική χρήση και εφαρμογή της, και η αγορά μπορεί να χρειαστεί να κατασταλάξει πριν από την κανονιστική παρέμβαση. Η απόφαση για το πότε πρέπει να γίνει μια ρύθμιση μπορεί να είναι τόσο σημαντική όσο η απόφαση για το τι πρέπει να ρυθμιστεί. Υπάρχει δυνητικά μεγάλο όφελος οι ρυθμίσεις να μην επηρεάζουν την καινοτομία της αγοράς και να παραμένει τεχνολογικά ουδέτερη.

Στην πράξη, αυτό σημαίνει ότι οι ρυθμιστικές αρχές πρέπει να κατανοήσουν την εφαρμογή της τεχνολογίας.

Η απόφαση να επιτραπεί ή να απαγορευθεί μια τεχνολογία είναι ίσως καλύτερα να μην αφεθεί στις ρυθμιστικές αρχές, διότι μέχρι να χρησιμοποιηθεί ευρέως μια τεχνολογία, τέτοιοι κίνδυνοι είναι περιορισμένοι. Αντ' αυτού, μια προσέγγιση αναμονής επιτρέπει την εξέλιξη της τεχνολογίας και την ρυθμιστική αρχή να μάθει αν θα υιοθετηθεί η τεχνολογία και να αντλήσει ιστορικά δεδομένα σχετικά με τους κινδύνους. Παρόλα αυτά ένα μη παραδοσιακό χρηματοπιστωτικό ίδρυμα μπορεί να κινηθεί γρήγορα από το "too-small-to-care" σε " too-big-to-fail". Αυτή η εκθετική ανάπτυξη αποτελεί πρόκληση για τη σταδιακή ρύθμιση, διότι έχει παραλείψει τη φάση "πολύ-μεγάλη-για να αγνοηθεί" όταν οι ρυθμιστικές αρχές θα έχουν αρχίσει να ζητούν συμμόρφωση.



Εικόνα 3: Πηγή: researchgate.net, Ross Buckley, Douglas W. Arner, Janos Nathan Barberis, «150 Years of FinTech: An Evolutionary Analysis», 2016

2.2.6 Προσαρμογή των ρυθμιστικών μεθόδων στην ψηφιακή εποχή

Οι διαφορές μεταξύ της Fintech 2.0 και της Fintech 3.0 δημιουργούν ξεχωριστές προσδοκίες και ανάγκες για την εποπτεία του κλάδου. Για τις νεοφυής επιχειρήσεις, το υψηλό κόστος της κανονιστικής συμμόρφωσης δεν είναι συμβατό με το συνήθως «ελαφρύ» επιχειρηματικό μοντέλο τους. Συνήθως προτιμούν πιο ευέλικτες υποχρεώσεις συμμόρφωσης ενός κανονιστικού καθεστώτος που βασίζεται σε αρχές, βάσει του οποίου το πνεύμα ρυθμίσεως προτιμάται από την τυπολατρική εφαρμογή. Αντίθετα, τα αυστηρά κανονιστικά καθεστώτα δημιουργούν σαφείς κανόνες και διαδικασίες. Ωστόσο, η ευελιξία ενός μοντέλου που βασίζεται σε αρχές δημιουργεί κάποια αβεβαιότητα ως προς

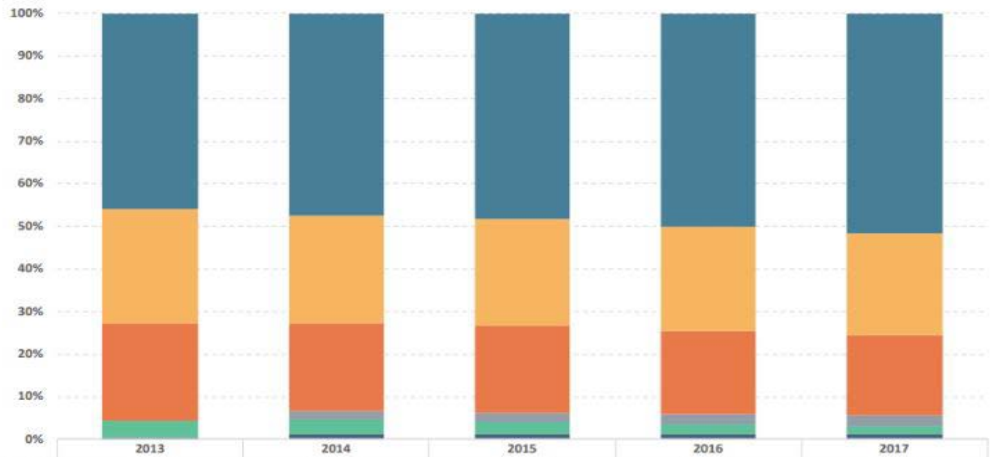
τις προσδοκίες συμμόρφωσης, και η καθαρότητα ενός μοντέλου που βασίζεται σε κανόνες μπορεί να περιορίσει το κίνητρο για να κάνει κάποιος περισσότερα.

Οι ρυθμιστικές υποχρεώσεις θα πρέπει να είναι δυναμικές ως προς την προσαρμογή στο μέγεθος και τη δραστηριότητα μιας επιχείρησης καθώς αναπτύσσεται. Στην περίπτωση των νεοφυών επιχειρήσεων, οι επενδυτές μπορεί να προτιμούν την κανονιστική βεβαιότητα του μοντέλου που βασίζεται σε κανόνες. Το υψηλότερο κόστος συμμόρφωσης μπορεί στη συνέχεια να εξισορροπηθεί με την αύξηση της ελκυστικότητας των νεοφυών εταιρειών προς τους επενδυτές. Ωστόσο, οι κανονιστικές προσεγγίσεις που βασίζονται σε κανόνες είναι πιθανότερο να δημιουργήσουν φραγμό στην είσοδο, και η Fintech 3.0 χρειάζεται επομένως ένα πλαίσιο τόσο ισορροπημένο όσο και δυναμικό.

2.3 Η επιρροή του Fintech στον χρηματοπιστωτικό τομέα στην ΕΕ.

Σύμφωνα με έρευνα της EBA (European Banking Authority) η παγκόσμια βιομηχανία πληρωμών αυξήθηκε σημαντικά τα τελευταία χρόνια, με 11% αυξημένες παγκόσμιες πληρωμές από 2016 σε 2017, οι οποίες επηρεάστηκαν θετικά από την επιταχυνόμενη μετάβαση από μετρητά σε ηλεκτρονικές και κινητές πληρωμές. Σύμφωνα με την Έκθεση για την Ψηφιακή Οικονομία και Κοινωνία του 2018, οι πολίτες της ΕΕ συμμετέχουν σε μια πλειάδα διαδικτυακών δραστηριοτήτων. Σημειώνεται η ανάπτυξη της χρήσης διαδικτυακών υπηρεσιών και η ανοδική τάση στο ηλεκτρονικό εμπόριο, με περίπου το 68% των χρηστών του Διαδικτύου της ΕΕ να ψωνίζουν στο διαδίκτυο το 2017. Ωστόσο, η ένταση του ηλεκτρονικού εμπορίου ποικίλλει σε μεγάλο βαθμό σε όλα τα κράτη μέλη της ΕΕ. Οι πτυχές της ιδιωτικής ζωής και της ασφάλειας κατά την πληρωμή στο διαδίκτυο αποτελούν το σημαντικότερο μέλημα για τους διαδικτυακούς αγοραστές.[5,6]

Σύμφωνα με την έκθεση τάσεων για τους καταναλωτές 2018/19, υπάρχει σταθερή αύξηση στη χρήση του ηλεκτρονικού χρήματος στην ΕΕ. Όσον αφορά τις μεθόδους πληρωμής, υπάρχει σημαντική αύξηση στις ανέπαφες πληρωμές που χρησιμοποιούν κάρτες ή εφαρμογές smartphone, με τη χρήση τεχνολογίας «προσέγγισης» – όπως η επικοινωνία κοντινού πεδίου (NFC), οι κωδικοί γρήγορης απόκρισης (QR) ή το Bluetooth – και τα τερματικά σημείων πώλησης που προσφέρουν ανέπαφες πληρωμές [5,6].



	2013	2014	2015	2016	2017
All cards except e-money function	46,248.5	50,355.3	55,806.5	62,215.8	69,198.4
Credit transfers	26,982.1	26,676.3	28,907.5	30,440.8	32,105.0
Direct debits	23,289.6	21,814.7	23,584.3	24,209.4	25,116.6
E-money purchase		2,097.0	2,388.2	2,843.4	3,417.6
Cheques	3,902.8	3,616.2	3,322.6	3,026.7	2,692.9
Other payment services	422.5	1,337.4	1,558.0	1,608.7	1,592.7

Εικόνα 4: Πηγή:EBA, "Impact of Fintech on payment institutions and e-money institutions business models" 2019

Η ευρύτερη ανάπτυξη της χρηματοοικονομικής τεχνολογίας επέφερε σημαντική αύξηση στη χρήση ψηφιακών και κινητών πορτοφολιών, τα οποία επί του παρόντος θεωρούνται ως μία από τις ταχύτερα αναπτυσσόμενες αγορές τεχνολογίας. Τα ψηφιακά πορτοφόλια εκτιμάται ότι έχουν προσθέσει περίπου 40δις δολάρια στα παγκόσμια έσοδα από τις πληρωμές το 2017. Η αυξανόμενη ενίσχυση του ρυθμού της διείσδυσης του διαδικτύου στην Ευρώπη, η οποία δημιούργησε ώριμες καταναλωτικές βάσεις για το ηλεκτρονικό εμπόριο σε ορισμένες περιοχές της ΕΕ, είχε θετικό αντίκτυπο στην Ευρωπαϊκή βιομηχανία ηλεκτρονικού εμπορίου, με αυξημένα έσοδα από το διασυνοριακό ηλεκτρονικό εμπόριο 13,2% το 2018 [5,6].

Εικόνα 5: Πηγή: Ευρωπαϊκή Αναφορά για το Ηλεκτρονικό Εμπόριο, Κύκλος εργασιών σε δις€ από το ηλεκτρονικό εμπόριο επιχειρήσεων προς καταναλωτές, 2018

Στην ΕΕ, οι άμεσες πληρωμές και η οδηγία για τις αναθεωρημένες υπηρεσίες πληρωμών (PSD2) δημιουργούν νέες ευκαιρίες, με νέους παίκτες να εισέρχονται στον τομέα των πληρωμών, χρησιμοποιώντας την τεχνολογία για τον επανασχεδιασμό παραδοσιακών δικτύων και επιχειρηματικών μοντέλων στις λιανικές και χονδρικές πληρωμές. Σύμφωνα με το μητρώο πληρωμών και τα ιδρύματα ηλεκτρονικού χρήματος της EBA, 961 Pis (payment institutions) και 297 EMIs (electronic money issuers) έχουν εγκριθεί ή καταχωρηθεί εντός της ΕΕ (στις 25 Μαΐου 2019). Νέες άδειες ελήφθησαν/επανεγκρίνονται μετά το PSD2, συμπεριλαμβανομένων οντοτήτων που δραστηριοποιούνται εκτός της ρυθμιστικής περιμέτρου, όπως οι εταιρείες τεχνολογίας και τηλεπικοινωνιών, οι οποίες αποφάσισαν να εισέλθουν στην περιοχή πληρωμών και ηλεκτρονικού χρήματος και έλαβαν άδεια PI ή EMI..[5,6]

Categories		**2017 services**	**2015 services**
Money Transfer and Payments	1	Online foreign exchange	Online foreign exchange
		Pay via cryptocurrency	
	2	Overseas remittances	Overseas remittances
	3	Online digital-only banks without branches	Nonbanks to transfer money
		Nonbanks to transfer money	
		Mobile phone payment at checkout	
Financial planning	4	Online budgeting and financial planning tools	Online budgeting and financial planning tool
Savings and investments	5	P2P platforms for high-interest investments	P2P platforms for high-interest investments
	6	Investments in equity crowdfunding platforms and rewards crowdfunding platforms	Investments in equity crowdfunding and rewards crowdfunding platforms
	7	Online investment advice and investment management	Online investment advice and investment management
	8	Online stockbroking	Online stockbroking and spreadbetting
		Spreadbetting	
Borrowing	9	Borrowing using P2P platforms	Borrowing using P2P platforms
		Borrowing using online short-term loan providers	
Insurance	10	Car insurance using telematics (black box) that monitor driver behavior	Car insurance using telematics (black box) that monitor driver behavior and health premium aggregators
		Insurance premium comparison sites	
		Activity-based health insurance that tracks your exercise	

Εικόνα 6: Κατηγορίες και υπηρεσίες Fintech, Πηγή: Karma Samir Sherif ,Mazen El-Masri, Karim Al-Yafi "The Digital Transformation of FinTech: Disruptions and Value Paths", Twenty-Third Pacific Asia Conference on Information Systems, China 2019

Τα επιχειρηματικά μοντέλα σε όλο τον τομέα των χρηματοπιστωτικών υπηρεσιών εξελίσσονται μαζί με την ψηφιακή μετάβαση, με την ανάπτυξη των ψηφιακών οικοσυστημάτων και την αυξανόμενη συνεργασία βασικών παραγόντων μέσω αλυσίδων υπηρεσιών ή εταιρικών συνεργασιών ή άλλων δομών. Επιπλέον, σύμφωνα με την Τράπεζα Διεθνών Διακανονισμών, οι δραστηριότητες χρηματοοικονομικών υπηρεσιών των επιχειρήσεων BigTech φαίνεται να αναπτύσσονται, ειδικά σε ορισμένες περιφέρειες, ιδίως σε πληρωμές, δανειοδότηση μικρών και μεσαίων επιχειρήσεων (SMEs) και άλλων συγκεκριμένων τμημάτων της αγοράς. Παρατηρήθηκε επίσης ότι, ενώ οι περισσότερες επιχειρήσεις BigTech ξεκινούν με τις πληρωμές, συχνά για να διευκολύνουν τη βασική τους επιχειρηματική δραστηριότητα (π.χ. ηλεκτρονική εμπορική ή διαφήμιση), υπάρχει σημαντική ποικιλομορφία στην αλληλουχία των επιχειρηματικών τομέων και του τρόπου με τον οποίο διεκπεραιώνουν τις υπηρεσίες πληρωμών. Στην Ευρώπη, όπου η κατεστημένη υποδομή πληρωμών με βάση τις τράπεζες είναι κυρίαρχη, οι καινοτόμες υπηρεσίες πληρωμών από τις εταιρείες BigTech (Google Pay, Amazon Pay, Apple Pay, Samsung Pay και πληρωμές στο Facebook Messenger) στηρίζονται σε υπάρχουσες δομές πληρωμών [5,6].

2.4 Ρυθμιστικό πεδίο και Fintech.

Δεν είναι μόνο η ανάπτυξη της χρηματοοικονομικής τεχνολογίας που επιτρέπει τη δραματική άνοδο των υπηρεσιών πληρωμών. Είναι επίσης το νέο ρυθμιστικό τοπίο, μετά την πρόσφατη εφαρμογή του PSD2 και του γενικού κανονισμού για την προστασία δεδομένων (GDPR), που αφορούν: την προστασία των δεδομένων, τον ασφαλή διαμοιρασμό δεδομένων, την ασφάλεια των πληρωμών και τη συγκατάθεση των πελατών. Ο συνδυασμός αυτών των δύο παρέχει τη νομική βάση και στοχεύει στην περαιτέρω ανάπτυξη μιας πιο ολοκληρωμένης εσωτερικής αγοράς ηλεκτρονικών πληρωμών εντός της ΕΕ, συμπεριλαμβανομένων για πρώτη φορά των απαιτήσεων ασφαλείας της ΕΕ, προκειμένου να γίνουν οι ηλεκτρονικές πληρωμές, όσο το δυνατόν ευκολότερες, αποδοτικότερο και ασφαλέστερες.

Με βάση έρευνα της ΕΒΑ, πάνω από το 85% των χρηματοπιστωτικών οργανισμών αναμένουν από τις εταιρείες BigTech να συμμετέχουν πιο ενεργά στις πληρωμές της ΕΕ

και στις επιχειρήσεις ηλεκτρονικού χρήματος στο εγγύς μέλλον, εισάγοντας και ενσωματώνοντας υπηρεσίες πληρωμών στις πλατφόρμες και τις εφαρμογές τους. Η πραγματικότητα είναι ότι οι εταιρείες BigTech μπορούν να αποτελέσουν σημαντική απειλή για τη βιωσιμότητα των επιχειρηματικών μοντέλων των υφιστάμενων χρηματοπιστωτικών οργανισμών, καθώς διαθέτουν σημαντική επενδυτική ικανότητα, τεχνολογικές γνώσεις και εμπειρογνωμοσύνη, όπως επίσης εμπειρία στην κλιμάκωση, για την παροχή μεγάλου όγκου υπηρεσιών με χαμηλότερο κόστος.

Επιπλέον, μεγάλος αριθμός χρηματοπιστωτικών οργανισμών έχουν ήδη ενστερνιστεί ή προσπαθούν ενεργά να ενστερνιστούν τις νέες υπηρεσίες που παρέχονται στο πλαίσιο του PSD2, δηλαδή: (i) υπηρεσίες πληροφοριών λογαριασμού (AIS) και (ii) υπηρεσίες εκκίνησης πληρωμών (PIS), εξετάζοντας την επέκταση των υπηρεσίες σε πελάτες. Η Ανοικτή Τραπεζική είναι το νέο ορόσημο της χρηματοοικονομικής τεχνολογίας.

Αυτές οι νέες υπηρεσίες φαίνεται να προσθέτουν προστιθέμενη αξία στις επιχειρήσεις των ιδρυμάτων, καθώς θα επιτρέπουν στους πελάτες να έχουν μια συγκεντρωτική προβολή των δεδομένων των υπηρεσιών λογαριασμού τους ή να χρησιμοποιούν εναλλακτικούς διαύλους πληρωμών, προς όφελος των διασυνοριακών υπηρεσιών. Με βάση την έρευνα της EBA του Μαρτίου 2019, τα περισσότερα ιδρύματα (77%) δεν παρέχουν ακόμη τις νέες υπηρεσίες στο πλαίσιο του PSD2, ενώ σήμερα το 12% των χρηματοοικονομικών οργανισμών που παρέχουν τόσο AIS όσο και PIs, 8% παρέχουν μόνο AIS και 3% μόνοPIs, αλλά σημαντικός αριθμός χρηματοπιστωτικών οργανισμών δήλωσαν ότι είχαν ήδη υποβάλει αίτηση για να παράσχουν μία ή και τις δύο από αυτές τις νέες υπηρεσίες στο πλαίσιο του PSD2 και σχεδιάζουν να χρησιμοποιούν δικαιώματα διαβατηρίου για την παροχή διασυνοριακών υπηρεσιών στο πλαίσιο της ελευθερίας παροχής υπηρεσιών ή την καθιέρωση τοπικής παρουσίας στα κράτη μέλη της ΕΕ.

Το σημείο που πρέπει να αντιμετωπιστεί είναι κατά πόσον το ρυθμιστικό πλαίσιο για τις ανοικτές τραπεζικές συναλλαγές (open-banking) παρέχει σημαντικές προκλήσεις στους νεοεισερχόμενους και τους μικρομεσαίου μεγέθους υφιστάμενους οργανισμούς, οι οποίοι μπορεί να εμποδιστούν από το να εισέλθουν στην αγορά και να αποφασίσουν να μην υιοθετήσουν τεχνολογική χρηματοπιστωτική καινοτομία ή αν οι κανονισμοί παρουσιάζουν μια τεράστια ευκαιρία για τις επιχειρήσεις BigTech και τους οργανισμούς που επενδύουν στην τεχνολογία τους για να αμφισβητήσουν τη θέση των τραπεζών και των πιστωτικών ιδρυμάτων στην αγορά.

2.4.1 PSD2

Το PSD2 είναι η Ευρωπαϊκή Οδηγία (ΕΕ) 2015/2366 που αφορά την ρύθμιση των υπηρεσιών πληρωμών στην Ευρωπαϊκή αγορά. Σκοπός της οδηγίας είναι η παροχή της νομικής βάσης για την περαιτέρω ανάπτυξη μιας ενοποιημένης εσωτερικής αγοράς για τις πληρωμές εντός της Ευρωπαϊκής Ένωσης, καθιστώντας τις εξίσου απλές, αποτελεσματικές, ασφαλείς και διαφανείς.[7]

Σύμφωνα με την Ευρωπαϊκή Επιτροπή, οι βασικοί στόχοι της PSD2's είναι:

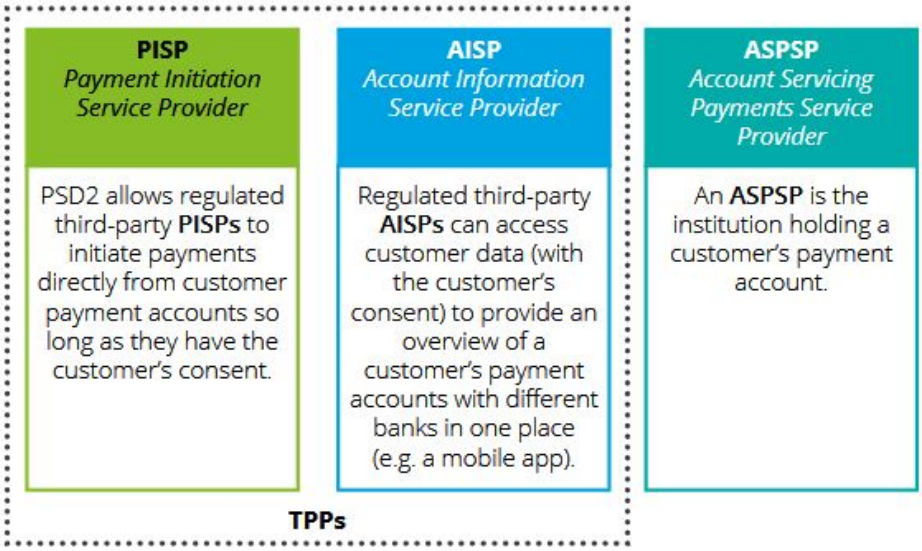
- η συμβολή σε μια πιο ολοκληρωμένη και αποδοτική αγορά ευρωπαϊκών πληρωμών
- να εξισορροπηθεί το επίπεδο ανταγωνισμού για τους παρόχους υπηρεσιών πληρωμών (συμπεριλαμβανομένων των νέων παικτών)
- να κάνει τις πληρωμές ασφαλέστερες και πιο ασφαλείς
- η προστασία των καταναλωτών
- η ενθάρρυνση χαμηλότερων τιμών για τις πληρωμές.[16]

Η Οδηγία 'PSD2' επιτρέπει την προσφορά υπηρεσιών πληρωμών τόσο σε καταναλωτές όσο και επιχειρήσεις, από Εταιρείες/Οργανισμούς που δεν είναι κατ' ανάγκην Τραπεζικά Ιδρύματα (Third Party Providers – TPPs), όπως:

- **Πάροχοι υπηρεσιών εκκίνησης πληρωμής (PISP):** Προσφέρουν τη δυνατότητα εκκίνησης μιας ηλεκτρονικής πληρωμής, κατόπιν οδηγιών του πληρωτή, από λογαριασμό του που τηρείται σε άλλο πάροχο υπηρεσιών πληρωμών (Τραπεζικό Ίδρυμα), παρέχοντας παράλληλα στους εμπόρους τη διαβεβαίωση για την εκκίνηση της πληρωμής, ούτως ώστε να αποδεσμεύονται τα αγαθά ή να παρέχονται οι υπηρεσίες χωρίς καθυστέρηση. Πάροχος υπηρεσιών εκκίνησης πληρωμής δυνατόν να είναι και κάποιο Τραπεζικό Ίδρυμα ή άλλος εξουσιοδοτημένος για το σκοπό αυτό Οργανισμός/Εταιρεία.

- **Πάροχοι υπηρεσιών πληροφοριών λογαριασμού (AISP):** Διαδικτυακή υπηρεσία η οποία παρέχει συγκεντρωτικές πληροφορίες σχετικά με ένα ή περισσότερους λογαριασμούς πληρωμών που τηρεί ο πελάτης με διάφορα Τραπεζικά Ιδρύματα, ώστε να έχει μια γενική εικόνα της οικονομικής του κατάστασης οποιαδήποτε χρονική στιγμή. Πάροχος υπηρεσιών πληροφοριών λογαριασμού δυνατό να είναι και κάποιο Τραπεζικό Ίδρυμα ή άλλος εξουσιοδοτημένος για το σκοπό αυτό Οργανισμός/Εταιρεία.

- **Πάροχοι υπηρεσιών πληρωμών εξυπηρέτησης λογαριασμού (ASPSP):** Τραπεζικά Ιδρύματα τα οποία παρέχουν και τηρούν τους λογαριασμούς πληρωμών των πελατών.[7]



Εικόνα 7: Πηγή: The Second Payment Services Directive (PSD2) – A briefing from Payments UK, Payments UK, July 2016.:

Το PSD2 δίνει τη δυνατότητα σε TPPs, με τη συγκατάθεση του ατόμου, να έχουν πρόσβαση στα στοιχεία του λογαριασμού του. Αυτά τα δεδομένα θα μπορούσαν να χρησιμοποιηθούν για την ανάλυση της συμπεριφοράς των δαπανών ή για την παροχή μιας επισκόπησης της οικονομικής κατάστασης με δεδομένα από πολλές διαφορετικές τράπεζες που παρουσιάζονται σε μία επισκόπηση. Ο πάροχος υπηρεσιών πληροφοριών λογαριασμού θα μπορούσε επίσης να περιλαμβάνει άλλους λογαριασμούς πληρωμών, όπως λογαριασμούς πιστωτικών καρτών και λογαριασμούς ενυπόθηκων δανείων, αλλά ακόμα δεν γνωρίζουμε εάν περιλαμβάνονται εμπορικοί λογαριασμοί. Μέχρι τώρα μόνο τα ίδια τα άτομα θα μπορούσαν να έχουν πρόσβαση στα δεδομένα τους επικοινωνώντας απευθείας με την τράπεζά τους, για παράδειγμα χρησιμοποιώντας μια ιστοσελίδα ή ακόμη και μια εφαρμογή για κινητές συσκευές που παρέχεται απευθείας από την τράπεζα.[8]

Ένα άμεσο αποτέλεσμα από την εφαρμογή του PSD2 είναι ότι είναι δυνατόν τα δεδομένα να μοιράζονται με διαφορετικό τρόπο από ό, τι πριν. Πλέον δύο νέου είδους πάροχοι θα είναι σε θέση να έχουν πρόσβαση στα στοιχεία του λογαριασμού του ατόμου και τις συναλλαγές του. Αυτό έχει ως αποτέλεσμα μεγαλύτερο βαθμό δυσκολίας σε σχέση με το πώς να διαχειριστεί και να εξασφαλίσει ένας οργανισμός υψηλό βαθμό ιδιωτικότητας.

Σύμφωνα με τα ρυθμιστικά τεχνικά πρότυπα, οι πάροχοι υπηρεσιών πληροφοριών λογαριασμού θα έχουν εγκατεστημένους κατάλληλους και αποτελεσματικούς μηχανισμούς που αποτρέπουν την πρόσβαση σε πληροφορίες χωρίς την ρητή συγκατάθεση του χρήστη/ιδιοκτήτη τους. Οι πάροχοι υπηρεσιών πληροφοριών λογαριασμού θα πρέπει επίσης να έχουν το δικαίωμα πρόσβασης σε πληροφορίες από λογαριασμούς πληρωμών κάθε φορά που ο χρήστης ζητεί ενεργά αυτές τις πληροφορίες ή έως και τέσσερις φορές (εκτός εάν συμφωνηθεί μεγαλύτερη συχνότητα) κατά τη διάρκεια μίας 24ωρης περιόδου με τη συγκατάθεση του χρήστη/ιδιοκτήτη.[8]

Τα ρυθμιστικά τεχνικά πρότυπα περιλαμβάνουν το πως πρέπει να υλοποιηθεί η ισχυρή ταυτοποίηση/αυθεντικοποίηση του χρήστη ,αλλά έχει αλλάξει η μορφή, από συγκεκριμένη σε μία πιο ευρεία για να επιτρέψει την ουδετερότητα της τεχνολογίας και των επιχειρηματικών μοντέλων. Τα πρότυπα τώρα περιλαμβάνουν μόνο ότι η ισχυρή ταυτοποίηση/αυθεντικοποίηση του χρήστη πρέπει να διασφαλίζεται με τρία στοιχεία (α) κάτι που μόνο ο χρήστης γνωρίζει, (β) κάτι που μόνο ο χρήστης κατέχει και (γ) κάτι που μόνο ο χρήστης είναι.[8]

Η ΕΒΑ υποστηρίζει ότι η προστασία των δεδομένων και η ιδιωτικότητα των δεδομένων είναι εκτός του πεδίου εφαρμογής των ρυθμιστικών τεχνικών προτύπων και, ως εκ τούτου, δεν μπορούν να αντιμετωπιστούν στα πλαίσια των εξειδικευμένων ρυθμιστικών τεχνικών προτύπων, ωστόσο τονίζεται ως σημαντική διαδικασία κατά την εφαρμογή τους. [8]. Αυτά προσδιορίζονται προστατεύονται με την εφαρμογή του GDPR (Γενικός Κανονισμός για την Προστασία των Δεδομένων).

Ενώ φαινομενικά το PSD2 είναι μια οδηγία εστιασμένη στις πληρωμές, ο μεγαλύτερος αντίκτυπος θα είναι αναμφισβήτητα το άνοιγμα των τραπεζικών δεδομένων των λογαριασμών των πελατών σε AISPs. Εάν οι ανεξάρτητοι AISPs αποκτήσουν σημαντική έλξη, οι τράπεζες ενδέχεται να χάσουν την αποκλειστικότητα της αλληλεπίδρασης με τους πελάτες τους και, επομένως, την κυρίαρχη σχέση μαζί τους. Αυτή η απειλή μπορεί να επιδεινωθεί περαιτέρω εάν ορισμένα TPPs επιλέξουν να ενεργούν ως υπηρεσίες AISPs και PISPs ταυτόχρονα, επιτρέποντας στους πελάτες να κάνουν πληρωμές από τους λογαριασμούς τους μέσω διασύνδεσης τρίτου μέρους.

Ωστόσο, οι εν λόγω πάροχοι θα πρέπει να αντιμετωπίσουν σύνθετα ζητήματα σχετικά με την προστασία των δεδομένων και την υπευθυνότητα. Ο γενικός κανονισμός της ΕΕ για

την προστασία δεδομένων (GDPR) απαιτεί από τους πελάτες να ενημερώνονται πλήρως, με σαφή, συνοπτικό και διαφανή τρόπο, για τον τρόπο με τον οποίο θα χρησιμοποιούνται τα προσωπικά τους δεδομένα και από ποιον. Οι πελάτες θα πρέπει να παρέχουν ρητή συγκατάθεση για τη χρήση των δεδομένων συναλλαγών τους.

Ο GDPR επιβάλλει ορισμένες νομικές υποχρεώσεις στους οργανισμούς για την προστασία αυτών των δεδομένων και για να διασφαλίσει την ακρίβεια και την πληρότητα τους. Οι πελάτες απολαμβάνουν επίσης πολλά πρόσθετα δικαιώματα, όπως η δυνατότητα ανάκλησης της συγκατάθεσης ανά πάσα στιγμή, να γνωρίζουν τι δεδομένα χρησιμοποιεί ένας οργανισμός και το να απαλείφονται οι πληροφορίες τους.

Καθώς η ανοικτή τραπεζική επιτρέπει την κοινή χρήση προσωπικών πληροφοριών μεταξύ οργανισμών, οι τράπεζες θα πρέπει να διασφαλίζουν ότι τα δεδομένα αυτά προστατεύονται όταν κοινοποιούνται σε άλλα μέρη και ότι η συγκατάθεση του πελάτη είναι σαφής και ενημερωμένη. Η μεγαλύτερη πρόσβαση τρίτων μερών αυξάνει τις οδούς μέσω των οποίων θα μπορούσε να διαπραχθεί κάποια απάτη, σε πολλές από τις οποίες οι τράπεζες δεν έχουν απαραιτήτως το ίδιο επίπεδο ελέγχου.

Οι AISPs και PISPs δεν θα μπορούν να χρησιμοποιούν δεδομένα που καταγράφονται κατά τη διαδικασία πληρωμής για να βελτιώσουν τα επιχειρηματικά τους μοντέλα. Αυτό συμβαίνει επειδή η νομοθεσία τους απαγορεύει να χρησιμοποιούν αυτά τα δεδομένα για σκοπούς άλλους από την παροχή των αντίστοιχων υπηρεσιών πληρωμών τους.[9]

Κεφάλαιο 3

GDPR

3.1-> Τι είναι το GDPR

Είναι ο Γενικός Κανονισμός για την Προστασία Δεδομένων (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών [10].

Σύμφωνα με τον ορισμό που δίνει ο Κανονισμός: «δεδομένα προσωπικού χαρακτήρα είναι κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου».

Το Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα της Κύπρου αναφέρει ότι: «Προσωπικά δεδομένα σημαίνει κάθε πληροφορία που αναφέρεται σε άτομο που βρίσκεται στη ζωή εφόσον η πληροφορία αυτή τυγχάνει αυτοματοποιημένης επεξεργασίας (π.χ. στον ηλεκτρονικό υπολογιστή) ή διατηρείται σε ένα διαρθρωμένο αρχείο μη αυτοματοποιημένης μορφής (δηλ. σε ταξινομημένο φάκελο). Για παράδειγμα προσωπικό δεδομένο είναι το ονοματεπώνυμο, η διεύθυνση, ο αριθμός τηλεφώνου, ο αριθμός πολιτικής ταυτότητας, ο αριθμός Κοινωνικών ασφαλίσεων, ο αριθμός λογαριασμού στην τράπεζα, η οικογενειακή κατάσταση, το επάγγελμα, η υγεία, η ερωτική ζωή, τα πολιτικά φρονήματα, οι θρησκευτικές πεποιθήσεις, η συμμετοχή σε ένωση, σωματείο ή συνδικαλιστική οργάνωση, οι ποινικές διώξεις ή καταδίκες, φωτογραφίες, δακτυλικά αποτυπώματα.»[11]

Επίσης το Γραφείο Επιτρόπου προσωπικών Δεδομένων αναφέρει ότι: «επεξεργασία προσωπικών δεδομένων» σημαίνει οποιαδήποτε εργασία πραγματοποιείται από οποιονδήποτε στο δημόσιο/ημικρατικό /ιδιωτικό τομέα αναφορικά με προσωπικά δεδομένα, όπως είναι για παράδειγμα η συλλογή, καταχώρηση/ αποθήκευση, χρήση, ανακοίνωση, διαβίβαση, διόρθωση και διαγραφή των δεδομένων.[11]

3.2 Τι προβλέπει ο νόμος

Ο Νέος Ευρωπαϊκός Κανονισμός GDPR 679/2016 αντικαθιστά την Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. Ο Κανονισμός ρυθμίζει τα δικαιώματα των φυσικών προσώπων σχετικά με:

- τα προσωπικά τους δεδομένα,

- την επεξεργασία των προσωπικών τους δεδομένων,

- την ελεύθερη και ανεμπόδιστη κυκλοφορία και μεταβίβαση των προσωπικών τους δεδομένων εντός των ορίων της Ευρωπαϊκής Ένωσης

- τις διαδικασίες διαβίβασης προσωπικών δεδομένων εκτός Ευρωπαϊκής Ένωσης.

Το GDPR αποτελείται από άρθρα που περιγράφουν τα δικαιώματα των ατόμων και τις απαιτήσεις των εκτελούντων επεξεργασία δεδομένων. Τα ακόλουθα είναι μια σύντομη περίληψη των δικαιωμάτων που χορηγούνται σε φυσικά πρόσωπα:

• Άρθρο 6: Νομιμότητα της επεξεργασίας. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα απαγορεύεται γενικά εάν δεν επιτρέπεται ρητά από το νόμο ή εάν τα επηρεαζόμενα πρόσωπα δεν έχουν συναινέσει στην επεξεργασία αυτών των δεδομένων.

• Άρθρο 7: Το δικαίωμα συγκατάθεσης. Το άτομο πρέπει να συναινεί στην συλλογή προσωπικών δεδομένων και μπορεί να ανακαλέσει την συγκατάθεση αυτή ανά πάσα στιγμή.

• Άρθρο 12: Το δικαίωμα να τίθενται ερωτήσεις σχετικά με τη χρήση δεδομένων προσωπικού χαρακτήρα και να ζητούνται και με ένδικα μέσα σε περίπτωση που οι ερωτήσεις δεν απαντώνται με σαφή, συνοπτικό και έγκαιρο τρόπο.

• Άρθρα 13 & 14: Το δικαίωμα να γνωρίζει κάποιος πώς χρησιμοποιούνται τα προσωπικά δεδομένα κατά τη στιγμή της συλλογής, το χρονικό διάστημα για το οποίο θα αποθηκευτούν και τα στοιχεία επικοινωνίας αυτού που τα συλλέγει.

• Άρθρο 15: Το δικαίωμα πρόσβασης στα δεδομένα προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία.

• Άρθρο 16: Το δικαίωμα διόρθωσης εσφαλμένων δεδομένων προσωπικού χαρακτήρα.

• Άρθρο 17: Το δικαίωμα διαγραφής των δεδομένων προσωπικού χαρακτήρα όταν δεν είναι πλέον αναγκαία για τους σκοπούς για τους οποίους συλλέχθηκαν και δεν υπάρχει νομική βάση για τη διατήρησή τους.

• Άρθρο 18: Το δικαίωμα περιορισμού της επεξεργασίας δεδομένων όταν τα δεδομένα είναι ανακριβή, η συλλογή τους παράνομη ή η επεξεργασία τους δεν απαιτείται πλέον.

• Άρθρο 19: Το μέρος που συλλέγει δεδομένα πρέπει να ενημερώσει όλους τους πρόσθετους εκτελούντες επεξεργασία δεδομένων, με τους οποίους μοιράζεται δεδομένα προσωπικού χαρακτήρα, να παύσουν την επεξεργασία δεδομένων που έχουν διορθωθεί ή διαγραφεί.

• Άρθρο 20: Το δικαίωμα λήψης των προσωπικών τους δεδομένων σε δομημένη, ευρέως χρησιμοποιούμενη, αναγνώσιμη από μηχάνημα μορφή την οποία μπορούν να μοιράζονται ελεύθερα με άλλους εκτελούντες επεξεργασία δεδομένων.

• Άρθρο 21: Το δικαίωμα ένστασης σε δεδομένα προσωπικού χαρακτήρα που χρησιμοποιούνται για τη δημιουργία προφίλ ή την προώθηση σε αυτούς.

• Άρθρο 22: Το δικαίωμα να μην υπόκεινται σε νομικά αποτελέσματα που βασίζονται αποκλειστικά στην αυτοματοποιημένη επεξεργασία δεδομένων.

• Άρθρο 25: Το δικαίωμα να αποθηκεύεται ο ελάχιστος όγκος δεδομένων, αναγκαίος, για την εκτέλεση των εργασιών των εκτελούντων επεξεργασία δεδομένων.

• Άρθρο 77: Το δικαίωμα υποβολής καταγγελίας κατά των μη συμμορφούμενων εκτελούντων επεξεργασία δεδομένων.

• Άρθρο 80: Το δικαίωμα να υπάρχει νόμιμος εκπρόσωπος για αγωγές κατά των εκτελούντων επεξεργασία δεδομένων.

Σύμφωνα με το άρθρο 4 του GDPR οι βασικές έννοιες του κανονισμού είναι [10]:

- **Προσωπικά Δεδομένα ή Δεδομένα Προσωπικού Χαρακτήρα:** Κάθε πληροφορία που αφορά ταυτοποιημένο, ή ταυτοποιήσιμο, φυσικό πρόσωπο («υποκείμενο των δεδομένων»). Παραδείγματα αποτελούν: όνομα, επώνυμο, αριθμός ταυτότητας, ΑΜΚΑ, ΑΦΜ, τηλέφωνο, ταχυδρομική και ηλεκτρονική διεύθυνση, διεύθυνση πρωτοκόλλου διαδικτύου (IP address), γεωχωρικά δεδομένα (GPS), δηλαδή στοιχεία που μπορούν να ταυτοποιήσουν ένα φυσικό πρόσωπο.

- **Υποκείμενο των Δεδομένων:** Πρόκειται για το φυσικό πρόσωπο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας.

- **Επεξεργασία δεδομένων:** Κάθε πράξη που πραγματοποιείται επί των προσωπικών δεδομένων, όπως συλλογή, καταχώριση, οργάνωση, αποθήκευση, μεταβολή, ανάκτηση, αναζήτηση πληροφοριών, χρήση, διαγραφή, καταστροφή κ.λπ.

- **Διασυνοριακή επεξεργασία:** Αφορά στην επεξεργασία δεδομένων προσωπικού χαρακτήρα η οποία γίνεται στο πλαίσιο των δραστηριοτήτων: α) διάφορων εγκαταστάσεων σε περισσότερα του ενός κράτη μέλη υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία στην ΕΕ, όπου ο υπεύθυνος επεξεργασίας ή ο εκτελών επεξεργασία είναι εγκατεστημένος σε περισσότερα του ενός κράτη μέλη και β) μίας μόνης εγκατάστασης υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία στην ΕΕ, αλλά που επηρεάζει ή ενδέχεται να επηρεάσει ουσιωδώς υποκείμενα των δεδομένων σε περισσότερα του ενός κράτη μέλη.

- **Υπεύθυνος Επεξεργασίας Δεδομένων:** Το φυσικό, ή νομικό, πρόσωπο, ή δημόσια αρχή/υπηρεσία, που καθορίζει τους σκοπούς και τον τρόπο της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα.

- **Εκτελών την Επεξεργασία:** Το φυσικό, ή νομικό, πρόσωπο, ή δημόσια αρχή / υπηρεσία, που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του Υπευθύνου Επεξεργασίας. Παραδείγματα Εκτελούντων την Επεξεργασία αποτελούν οι επιχειρήσεις ενημέρωσης οφειλετών και παροχής υπηρεσιών "cloud".

- **Αποδέκτης δεδομένων:** Το φυσικό, ή νομικό, πρόσωπο, ή δημόσια αρχή / υπηρεσία / άλλος φορέας, στον οποίο κοινολογούνται τα δεδομένα προσωπικού χαρακτήρα, είτε πρόκειται για τρίτον είτε όχι. Οι δημόσιες αρχές που ενδέχεται να λάβουν τέτοια δεδομένα στο πλαίσιο συγκεκριμένης έρευνας δεν θεωρούνται ως αποδέκτες. Η επεξεργασία των δεδομένων αυτών από τις εν λόγω δημόσιες αρχές πραγματοποιείται σύμφωνα με τους ισχύοντες κανόνες προστασίας των δεδομένων ανάλογα με τους σκοπούς της επεξεργασίας.

- **Υπεύθυνος Προστασίας Δεδομένων:** Ορίζεται από τον Υπεύθυνο Επεξεργασίας και τον Εκτελούντα την Επεξεργασία και συμμετέχει, δεόντως και εγκαίρως, σε όλα τα ζητήματα τα οποία σχετίζονται με την προστασία δεδομένων προσωπικού χαρακτήρα. Αποτελεί το πρόσωπο επικοινωνίας τόσο με τα υποκείμενα των δεδομένων όσο και με την εποπτική Αρχή.

- **Εκτίμηση Αντικτύπου σχετικά με την προστασία δεδομένων:** Όταν ένα είδος επεξεργασίας δεδομένων, 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 οφείλει να διενεργήσει, πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία προσωπικών δεδομένων.

- **Συγκατάθεση Υποκειμένου**: Κάθε ένδειξη βούλησης (ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει), με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν.

- **Παραβίαση Δεδομένων Προσωπικού Χαρακτήρα:** Παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας αποκάλυψη ή πρόσβαση δεδομένων προσωπικού χαρακτήρα, τα οποία διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία.

- **Εποπτική Αρχή Προστασίας Δεδομένων:** Πρόκειται για την ανεξάρτητη δημόσια Αρχή, καθ' ύλην αρμόδια για την εποπτεία εφαρμογής του Κανονισμού. Ο Κανονισμός ενθαρρύνει την επικοινωνία και συνεργασία μεταξύ των διάφορων Αρχών («μηχανισμός μιας στάσης»), ώστε να διασφαλίζεται ομοιογένεια στην αντιμετώπιση υποθέσεων διευρωπαϊκού ενδιαφέροντος και ασφάλεια δικαίου.

- **Επικεφαλής Εποπτική Αρχή:** Ορίζεται η Αρχή του κράτους-μέλους όπου βρίσκεται η «κύρια εγκατάσταση» (βλ. παρακάτω) του Υπευθύνου Επεξεργασίας.

- **Ενδιαφερόμενη Εποπτική Αρχή:** Ορίζεται η Αρχή, την οποία αφορά η επεξεργασία δεδομένων προσωπικού χαρακτήρα, όταν: α) ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία είναι εγκατεστημένος στο έδαφος του κράτους μέλους της εν λόγω εποπτικής αρχής, β) τα υποκείμενα των δεδομένων που διαμένουν στο κράτος μέλος της εν λόγω εποπτικής αρχής επηρεάζονται ή ενδέχεται να επηρεαστούν ουσιωδώς από την επεξεργασία, ή γ) έχει υποβληθεί καταγγελία στην εν λόγω εποπτική αρχή.

- **Κύρια Εγκατάσταση: Για τον Υπεύθυνο Επεξεργασίας:** Σε περίπτωση που έχει εγκαταστάσεις σε περισσότερα του ενός κράτη μέλη, πρόκειται για τον τόπο της κεντρικής του διοίκησης στην ΕΕ. Ωστόσο, εάν οι αποφάσεις, όσον αφορά στους σκοπούς και τα μέσα της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, λαμβάνονται σε άλλη εγκατάστασή του στην ΕΕ, και η εγκατάσταση αυτή έχει την εξουσία εφαρμογής των αποφάσεων αυτών, τότε πρόκειται για την εγκατάσταση στην οποία έλαβε αυτές τις αποφάσεις. **Για τον Εκτελούντα την Επεξεργασία:** Σε περίπτωση που έχει εγκαταστάσεις σε περισσότερα του ενός κράτη μέλη, πρόκειται για τον τόπο της κεντρικής του διοίκησης στην ΕΕ. Ωστόσο, εάν δεν έχει κεντρική διοίκηση στην ΕΕ, τότε πρόκειται για την εγκατάστασή του στην ΕΕ όπου εκτελούνται

οι κύριες δραστηριότητες επεξεργασίας στο πλαίσιο των δραστηριοτήτων εγκατάστασης του εκτελούντος την επεξεργασία.

- **Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων:** Απαρτίζεται από τον προϊστάμενο μίας εποπτικής Αρχής κάθε κράτους μέλους και από τον Ευρωπαίο Επόπτη Προστασίας Δεδομένων. Έχει ως στόχο να συμβάλλει στη συνεκτική εφαρμογή του Κανονισμού σε ολόκληρη την ΕΕ.

- **Μηχανισμός Συνεκτικότητας:** Ο μηχανισμός με βάση τον οποίο οι εποπτικές Αρχές συνεργάζονται μεταξύ τους, με κύριο στόχο τη συνεκτική εφαρμογή του Κανονισμού στο σύνολο της ΕΕ.

- **Κατάρτιση Προφίλ:** Περιλαμβάνει οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα που συνίσταται στη χρήση δεδομένων προσωπικού χαρακτήρα για την αξιολόγηση ορισμένων προσωπικών πτυχών ενός φυσικού προσώπου, ιδίως για την ανάλυση ή την πρόβλεψη πτυχών που αφορούν στην απόδοση στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις, τα ενδιαφέροντα, την αξιοπιστία, τη συμπεριφορά, τη θέση ή τις μετακινήσεις του εν λόγω φυσικού προσώπου.

- **Ψευδωνυμοποίηση:** Πρόκειται για την 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.

3.2.1 Βασικές αρχές

Σύμφωνα με το άρθρο 5 του Κανονισμού απαιτείται από τους Υπεύθυνους Επεξεργασίας και τους Εκτελούντες την επεξεργασία των προσωπικών δεδομένων, οι εξής βασικές αρχές:

Η αρχή της νόμιμης, αντικειμενικής και διαφανούς επεξεργασίας που επιβάλει την σύννομη, θεμιτή και με διαφανή τρόπο επεξεργασία αναφορικά με το υποκείμενο των δεδομένων. Η νομιμότητα της επεξεργασίας διασφαλίζεται, σύμφωνα με το άρθρο 6 του Κανονισμού, στις περιπτώσεις στις οποίες α) έχει ληφθεί η προηγούμενη συναίνεση του υποκειμένου στην επεξεργασία των δεδομένων του για έναν ή περισσότερους συγκεκριμένους σκοπούς, β) η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης ή για τη συμμόρφωση με έννομη υποχρέωση του Υπευθύνου Επεξεργασίας που απορρέει από άλλο κανόνα δικαίου, γ) η επεξεργασία είναι απαραίτητη για την διαφύλαξη ζωτικού συμφέροντος ή για την εκπλήρωση καθήκοντος προς το δημόσιο συμφέρον ή για την άσκηση δημόσιας εξουσίας ανατεθειμένης στον Υπεύθυνο Επεξεργασίας και τέλος, δ) η επεξεργασία είναι απαραίτητη για τους σκοπούς των εννόμων συμφερόντων που επιδιώκει ο Υπεύθυνος Επεξεργασίας εκτός αν υποκείμενο είναι παιδί, περίπτωση στην οποία υπερισχύει το έννομο συμφέρον προστασίας του παιδιού. Η διαφάνεια εξασφαλίζεται μέσω της παροχής κάθε πληροφορίας και ανακοίνωσης σχετικά με την επεξεργασία με συνοπτικό, διαφανή και κατανοητό τρόπο και σε εύκολα προσβάσιμη μορφή. Για την παροχή πληροφόρησης ή την διατύπωση της ανακοίνωσης, ιδίως εάν πρόκειται για ενημέρωση ανηλίκων, πρέπει να γίνεται χρήση σαφούς και απλής διατύπωσης. Η πληροφορία πρέπει να δίνεται στο υποκείμενο των δικαιωμάτων εντός προθεσμίας ενός μήνα από την παραλαβή του σχετικού αιτήματός του(με δυνατότητα παράτασης για δύο μήνες) ενώ στην περίπτωση που η παροχή της πληροφορίας δεν είναι εφικτή, ο Υπεύθυνος επεξεργασίας οφείλει να ενημερώσει το υποκείμενο για την αδυναμία αυτή καθώς και να το πληροφορήσει για τη δυνατότητα υποβολής καταγγελίας στην αρμόδια εποπτική αρχή και για τη δυνατότητα άσκησης δικαστικής προσφυγής.

Η αρχή του σκοπού που εκπληρώνεται όταν η συλλογή και η επεξεργασία γίνονται με στόχο σαφή και καθορισμένο που δεν επιτρέπει την υποβολή των δεδομένων σε περαιτέρω επεξεργασία. Μόνη επιτρεπτή εξαίρεση συνιστά η περαιτέρω επεξεργασία για σκοπούς αρχειοθέτησης που εξυπηρετούν το δημόσιο συμφέρον ή για σκοπούς

επιστημονικής ή ιστορικής έρευνας, ή στατιστικούς σκοπούς υπό τον όρο ότι οι χρησιμοποιούμενες μέθοδοι αποκλείουν την ταυτοποίηση των υποκειμένων των δεδομένων και παρέχουν τις κατάλληλες εγγυήσεις για την προστασία των δεδομένων τους.

Η αρχή ελαχιστοποίησης των δεδομένων η οποία πρέπει να εφαρμόζεται τόσο στον όγκο των δεδομένων όσο και στη διάρκεια τήρησης αυτών και βάσει της οποίας τα δεδομένα που τηρούνται πρέπει να είναι κατάλληλα, συναφή και περιορισμένα στα απολύτως απαραίτητα αναφορικά με τους σκοπούς για τους οποίους εκτελείται η επεξεργασία.

Η αρχή της ακρίβειας σύμφωνα με την οποία τα δεδομένα θα πρέπει να είναι ακριβή και, όταν είναι αναγκαίο, να επικαιροποιούνται ενώ το υποκείμενο θα πρέπει να έχει επαρκή ενημέρωση ως προς τα προσωπικά του δεδομένα τα οποία υφίστανται επεξεργασία. Παράλληλα, 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.

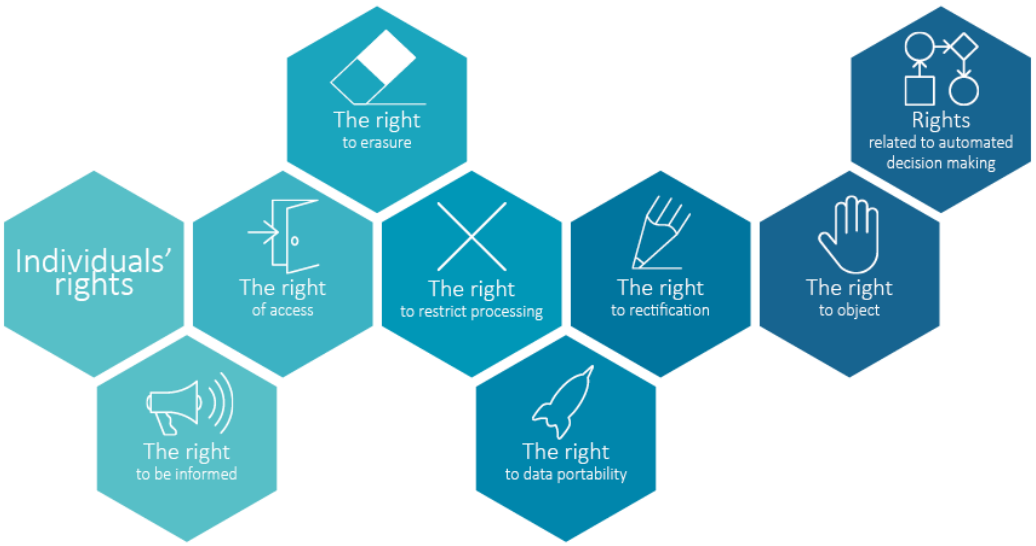
Η αρχή του περιορισμού της περιόδου αποθήκευσης, δηλαδή την τήρηση των αρχείων των δεδομένων για όσο διάστημα χρειάζεται για την επίτευξη του σκοπού της επεξεργασίας. Εξαίρεση προβλέπεται στην περίπτωση κατά την οποία η επεξεργασία γίνεται για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς και λαμβάνονται τα κατάλληλα οργανωτικά μέτρα για τη διασφάλιση των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων.

Η αρχή της ακεραιότητας και εμπιστευτικότητας που καλεί για την υποβολή των δεδομένων σε επεξεργασία κατά τρόπο ώστε να 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.

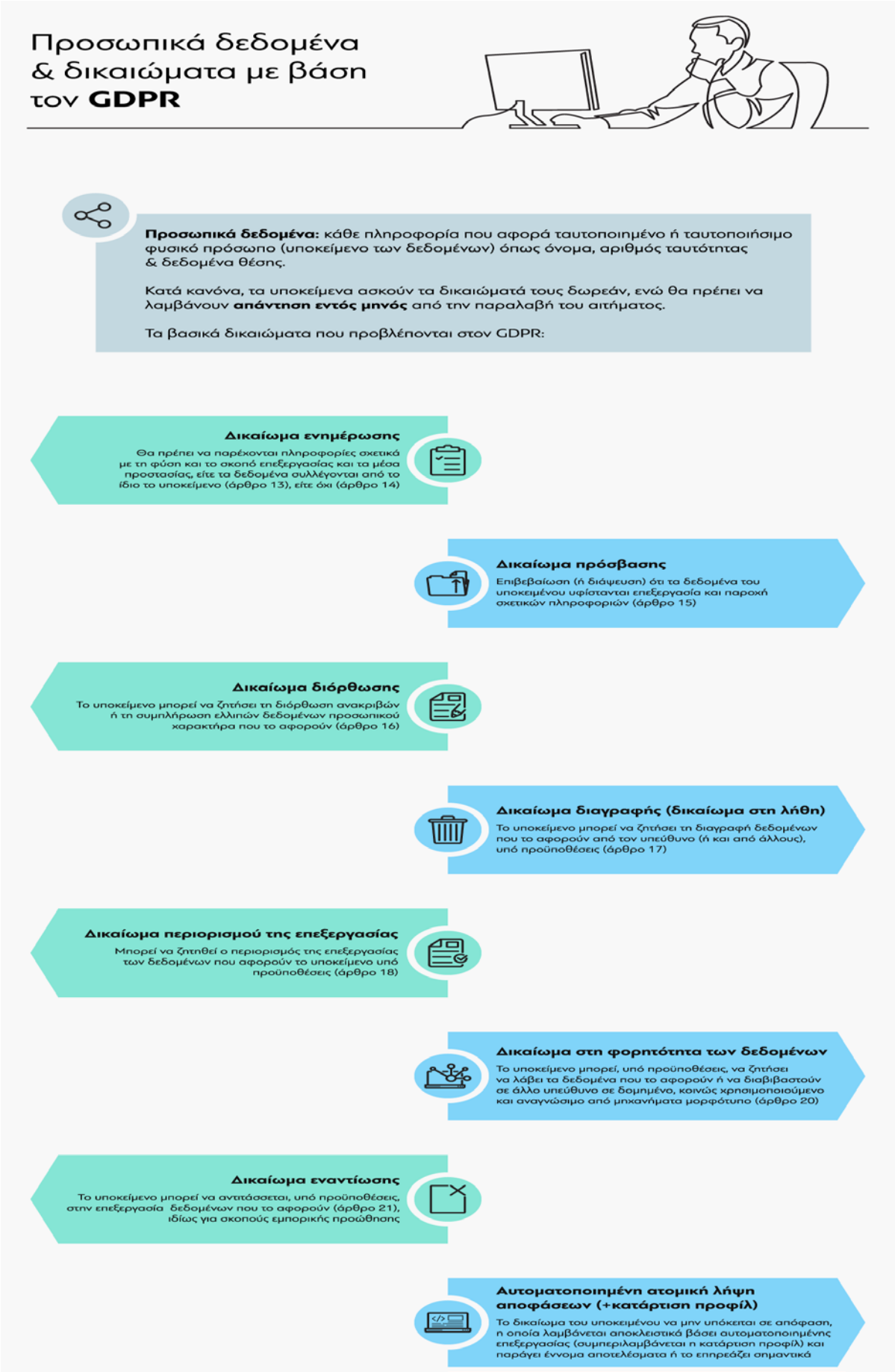
Η αρχή της αναλογικότητας που επιβάλλει να υπάρχει συνάφεια ανάμεσα στα δεδομένα που τηρούνται και στο σκοπό για τον οποίο αυτά συλλέγονται, καθώς και να είναι τα δεδομένα αυτά πρόσφορα και αναγκαία για την εκπλήρωση του σκοπού αυτού.

Με τον τρόπο αυτό, η αρχή της αναλογικότητας οδηγεί πρακτικά στην ελαχιστοποίηση των τηρούμενων δεδομένων, αφού το πιθανότερο είναι πως οι προϋποθέσεις αυτές δεν ισχύουν για το σύνολο των δεδομένων που συλλέγονται από τον Υπεύθυνο Επεξεργασίας ή τον Εκτελούντα την Επεξεργασία.

Τέλος, **η αρχή της λογοδοσίας** υπό την οποία ο Υπεύθυνος Επεξεργασίας και ο εκτελών την επεξεργασία φέρουν την ευθύνη να αποδείξουν όχι μόνο την συμμόρφωση στις υποχρεώσεις που θέτει ο Κανονισμός αλλά και την ετοιμότητά τους να συμμορφωθούν. Οι υποχρεώσεις τους δεν είναι προκαθορισμένες και σταθερές αλλά διαμορφώνονται ανάλογα με τον κίνδυνο που ενδέχεται να προκύψει από την επεξεργασία, όπως ο κίνδυνος αυτός εκτιμάται ήδη πριν την έναρξη της επεξεργασίας, βάσει της Εκτίμησης Αντικτύπου σχετικά με την προστασία των δεδομένων. [12]



Εικόνα 8: Πηγή: europeanprogress.gr



Εικόνα 9: Πηγή: lawspot.gr, «Προσωπικά δεδομένα: Τα δικαιώματα των πολιτών με βάση τον GDPR (infographic)», Μάϊος 2018.

3.2.2 Οργανωτικές απαιτήσεις

Σύμφωνα με τον GDPR, θα πρέπει να εφαρμοστεί ένα ευρύ φάσμα μέτρων, προκειμένου να διασφαλιστεί ότι θα μειωθεί ο κίνδυνος παραβίασης του Κανονισμού και προκειμένου να μπορεί ο οργανισμός να αποδείξει ότι έλαβε όλα τα απαραίτητα μέτρα για την προστασία των προσωπικών δεδομένων υπό τη διαχείριση του.

Μεταξύ των αναγκαίων μέτρων λογοδοσίας είναι: η αξιολόγηση των επιπτώσεων των προσωπικών δεδομένων, ο έλεγχος, η αξιολόγηση της πολιτικής, η διατήρηση αρχείων δραστηριότητας και (ενδεχομένως) ο διορισμός υπεύθυνου προστασίας δεδομένων (DPO-Data Privacy Officer). Σε ορισμένες περιπτώσεις, ο GDPR εισάγει την υποχρέωση διορισμού ενός υπευθύνου προστασίας δεδομένων (DPO). Για τη συγκεκριμένη θέση, οι οργανισμοί θα πρέπει να ορίσουν ένα μέλος του προσωπικού ή έναν εξωτερικό σύμβουλο. Οι εθνικές αρχές προστασίας δεδομένων αναμένεται να παράσχουν σχετική καθοδήγηση σχετικά με το ποιος θα πρέπει να προβεί στη συγκεκριμένη διαδικασία.

Ο DPO θα είναι υπεύθυνος για την παρακολούθηση της συμμόρφωσης με τον GDPR, θα ενημερώνει για τις υποχρεώσεις του οργανισμού, θα παράσχει συμβουλές σχετικά με το πότε και πώς θα πρέπει να διεξαχθεί αξιολόγηση των επιπτώσεων της διαχείρισης των προσωπικών δεδομένων και θα αποτελεί το άτομο στο οποίο θα απευθύνονται τόσο οι εθνικές αρχές προστασίας δεδομένων, όσο και οι ιδιώτες.

Η υπηρεσία μίας στάσης, επιτρέπει σε έναν οργανισμό που δραστηριοποιείται σε αρκετές χώρες της ΕΕ να συνδιαλλαγεί με μία μόνο εθνική αρχή προστασίας δεδομένων, αν και σε ορισμένες περιπτώσεις, οι κανόνες για τον προσδιορισμό του ποια αρχή θα πρέπει να αναλάβει αυτόν τον ρόλο, είναι αρκετά πολύπλοκες.[13]

3.2.3 Διαδικασίες GDPR

Ο GDPR προβλέπει κάποιες διαδικασίες/πολιτικές ανάλογα με διάφορα σενάρια και καταστάσεις, όπως:

- **Η παραβίαση δεδομένων:** που ορίζεται ως "παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, μη εξουσιοδοτημένη αποκάλυψη ή πρόσβαση σε προσωπικά δεδομένα που

διαβιβάζονται, αποθηκεύονται ή επεξεργάζονται με οποιονδήποτε τρόπο". Εάν τα προσωπικά δεδομένα έχουν παραβιαστεί, ανεξάρτητα από το αν έχει προκληθεί βλάβη στο άτομο, θα πρέπει να ενημερωθεί η εθνική αρχή προστασίας δεδομένων αμέσως, ή το αργότερο 72 ώρες μετά την ανακάλυψη του συμβάντος. Εάν έχουν εφαρμοστεί τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την προστασία των δεδομένων προσωπικού χαρακτήρα, όπως για παράδειγμα την κρυπτογράφησή τους, απαλλάσσεστε από την υποχρέωση γνωστοποίησης.

- **Η προστασία δεδομένων από το στάδιο του σχεδιασμού:** Κάθε νέα διαδικασία ή προϊόν θα πρέπει να σχεδιάζεται λαμβάνοντας υπόψη τις απαιτήσεις προστασίας των προσωπικών δεδομένων. Αυτή η προσέγγιση, ενώ προηγουμένως αποτελούσε βέλτιστη πρακτική, πλέον είναι ρητή απαίτηση.
- **Η εκτίμηση των επιπτώσεων της ιδιωτικής ζωής (privacy impact assessment -PIA):** έχει ως στόχο τον εντοπισμό και την ελαχιστοποίηση των κινδύνων μη συμμόρφωσης. Το PIA στο πλαίσιο του GDPR καθίσταται επίσημη απαίτηση. Οι ελεγκτές πρέπει να διασφαλίσουν ότι έχει καθοριστεί ο παράγοντας PIA σε οποιαδήποτε δραστηριότητα επεξεργασίας "υψηλού κινδύνου".
- **Οι διεθνείς μεταφορές δεδομένων (ενδοεταιρικά ή σε εξωτερικούς φορείς):** Εάν ο οργανισμός δραστηριοποιείται διεθνώς, οι κανόνες και οι διαδικασίες για τη μεταφορά δεδομένων σε χώρες εκτός δικαιοδοσίας της ΕΕ θα αποτελέσουν έναν σημαντικό παράγοντα, καθώς οι κυρώσεις για τη μη συμμόρφωση ή τη μεταφορά των δεδομένων σε δικαιοδοσίες που δεν αναγνωρίζονται (από την Ευρωπαϊκή Επιτροπή) ως έχουσες επαρκή νομοθεσία για την προστασία δεδομένων θα είναι πολύ πιο αυστηρές κάτω από τον νέο Κανονισμό GDPR.
- **Η ευαισθητοποίηση των εργαζομένων για την ασφάλεια των δεδομένων:** Πρέπει να ενημερωθούν οι υπάλληλοι σχετικά με την ανάγκη συμμόρφωσης με τον GDPR. Θα πρέπει να γίνει μια αναθεώρηση των διαδικασιών και ίσως να απαιτηθεί εκπαίδευση του προσωπικού.
- **Η λογοδοσία:** Ο GDPR καθιστά τους αρμόδιους ελεγκτές (πρόσωπα ή οργανισμοί που, αποκλειστικά ή συλλογικά, καθορίζουν τους σκοπούς και τα μέσα της επεξεργασίας των προσωπικών δεδομένων) υπεύθυνους για την απόδειξη της συμμόρφωσης με τις αρχές προστασίας δεδομένων. Είναι απαραίτητη η υιοθέτηση σαφών πολιτικών, οι οποίες σε περίπτωση ελέγχου να μπορεί να αποδειχθεί ότι πληρούν τα απαιτούμενα πρότυπα. Επιπλέον, θα πρέπει να έχει διασφαλισθεί ότι το προσωπικό είναι εκπαιδευμένο, κατανοεί τις υποχρεώσεις

του και είναι έτοιμο να το αποδείξει ανά πάσα στιγμή, όταν απαιτηθεί κάτι τέτοιο από την εθνική αρχή προστασίας δεδομένων.

- **Η παραβίαση των δεδομένων:** Θα πρέπει να προετοιμαστεί ο οργανισμός κατάλληλα για την πιθανότητα παραβίασης της ασφάλειας των δεδομένων (που ορίζεται ως "παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, μη εξουσιοδοτημένη αποκάλυψη ή πρόσβαση σε προσωπικά δεδομένα που διαβιβάζονται, αποθηκεύονται ή επεξεργάζονται με οποιονδήποτε τρόπο") θέτοντας σαφείς πολιτικές και δοκιμασμένες διαδικασίες, έτσι ώστε να διασφαλιστεί ότι θα μπορεί να αντιδράσει και να γνωστοποιήσει κάθε παραβίαση δεδομένων, όπου απαιτείται. Κυρώσεις ενδέχεται να επιφέρει τόσο η αποτυχία της αναφοράς παράβασης προσωπικών δεδομένων, όσο και η ίδια η παράβαση.
- **Η διασφάλιση των δικαιωμάτων των δεδομένων υποκειμένου:** Ο GDPR ενισχύει τα δικαιώματα που έχουν τα υποκείμενα των οποίων τα προσωπικά δεδομένα διαχειριζόμαστε., όπως: α) η ενίσχυση των δικαιωμάτων των ατόμων, με υποχρέωση του οργανισμού να επιτρέπει πρόσβαση στα προσωπικά του δεδομένα εντός συγκεκριμένου χρονικού διαστήματος, β) δικαίωμα στη λήθη, δηλαδή της διαγραφής των δεδομένων ενός ατόμου από τους υπεύθυνους επεξεργασίας κατόπιν αιτήματος του, χωρίς καθυστέρηση, γ) το δικαίωμα των υποκειμένων να μην υπόκειται σε αποφάσεις που βασίζονται σε προσωπικά προφίλ. Ως προφίλ ορίζεται «κάθε μορφή αυτοματοποιημένης επεξεργασίας των δεδομένων προσωπικού χαρακτήρα που περιλαμβάνει τη χρήση των προσωπικών δεδομένων για την αξιολόγηση ορισμένων πτυχών της προσωπικότητάς σε ένα φυσικό πρόσωπο, ιδίως για την ανάλυση ή την πρόβλεψη στοιχείων που αφορούν στην απόδοση του φυσικού προσώπου στην εργασία, την οικονομική κατάσταση , την υγεία, τις προσωπικές προτιμήσεις, τα ενδιαφέροντα, την αξιοπιστία, τη συμπεριφορά, τη θέση ή την κίνηση», δ) δικαίωμα στη φορητότητα των δεδομένων, το οποίο υπερβαίνει το δικαίωμα στην απαίτηση της παροχής των προσωπικών δεδομένων τους σε μια ευρέως χρησιμοποιούμενη ηλεκτρονική μορφή. Συγκεκριμένα, απαιτείται από τον ελεγκτή να παρέχει τις σχετικές πληροφορίες σε μια δομημένη, κοινή και αναγνώσιμη από μηχανή μορφή. Ωστόσο, ισχύει μόνο για τα προσωπικά δεδομένα που υποβάλλονται σε επεξεργασία με αυτοματοποιημένα μέσα, ε) το δικαίωμα περιορισμών συγκεκριμένων διεργασιών, όπως επίσης και το δικαίωμα αντίρρησης στην

υποβολή των δεδομένων προσωπικού χαρακτήρα σε επεξεργασία για σκοπούς απευθείας εμπορικής προώθησης. Μόλις ένα άτομο αρνηθεί, τα στοιχεία του δεν θα πρέπει να υποβάλλονται σε επεξεργασία για άμεση εμπορική προώθηση περαιτέρω και τα στοιχεία επικοινωνίας του ατόμου θα πρέπει να προστεθούν σε ένα τοπικό προς διαγραφή αρχείο. Οι οργανισμοί πρέπει να ενημερώνουν τον κόσμο σχετικά με το δικαίωμα να αρνηθούν την επεξεργασία των δεδομένων τους με τρόπο που να είναι σαφές και ξεχωριστό από άλλα στοιχεία τα οποία πρέπει επίσης να παρέχουν σε αυτούς.

- **Η επικοινωνία σχετικά με τα δεδομένα προσωπικού χαρακτήρα:** Θα πρέπει να επανεξετασθεί η διαδικασία λήψης συγκατάθεσης των ατόμων και αυτή να προέρχεται από θετική/ενεργητική ένδειξη συμφωνίας για τα δεδομένα προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία. Παραχωρείται, επίσης, το δικαίωμα περιορισμών συγκεκριμένων διεργασιών, όπως επίσης και το δικαίωμα αντίρρησης στην υποβολή των δεδομένων προσωπικού χαρακτήρα σε επεξεργασία για σκοπούς απευθείας εμπορικής προώθησης. Τέλος θα πρέπει να δηλώνονται προς τα υποκείμενα των δεδομένων στοιχεία όπως η νομική βάση για την επεξεργασία των δεδομένων τους, οι περιίοδοι διατήρησης των δεδομένων και το δικαίωμά τους να διαμαρτυρηθούν στην εθνική αρχή προστασίας δεδομένων, εάν θεωρούν ότι υπάρχει κάποιο πρόβλημα με το τρόπο που χειρίζονται τα δεδομένα τους.
- **Η ασφάλεια των δεδομένων:** Ο GDPR καθορίζει κανόνες ασφάλειας των δεδομένων παρόμοιους με εκείνους της ισχύουσας οδηγίας, στους οποίους συμπεριλαμβάνονται: η δικαιοσύνη, η νομιμότητα και η διαφάνεια, ο περιορισμός του σκοπού, η ελαχιστοποίηση και η ποιότητα των δεδομένων, η ασφάλεια, η ακεραιότητα και η εμπιστευτικότητα. Θα πρέπει να διασφαλιστεί ότι τα προσωπικά δεδομένα υποβάλλονται σε επεξεργασία κατά τρόπο που να κατοχυρώνει την ασφάλειά τους, συμπεριλαμβανομένης της προστασίας από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και από τυχαία απώλεια, καταστροφή ή φθορά: «Ο οργανισμός και οποιοσδήποτε τρίτος πάροχος υπηρεσιών θα πρέπει να εφαρμόσει τα κατάλληλα τεχνικά και οργανωτικά μέτρα, για να εξασφαλιστεί επίπεδο ασφάλειας ανάλογο προς τον κίνδυνο». Ο κανονισμός προτείνει μια σειρά από μέτρα ασφαλείας τα οποία μπορούν να χρησιμοποιηθούν για την επίτευξη της προστασίας των δεδομένων, συμπεριλαμβανομένων των: ψευδή ταυτότητα και κρυπτογράφηση των δεδομένων προσωπικού χαρακτήρα.

- **Η τεκμηρίωση δεδομένων, η νομική βάση και ο έλεγχος:** Θα πρέπει ένας οργανισμός να μπορεί να τεκμηριώσει τι προσωπικά δεδομένα κατέχει, από πού προήλθαν και με ποιους τα μοιράζεται. Εάν έχει ανακριβή δεδομένα προσωπικού χαρακτήρα και τα έχει μοιραστεί με κάποιον άλλον οργανισμό ο GDPR απαιτεί να του επισημανθεί η ανακρίβεια, έτσι ώστε να μπορεί να διορθώσει τα δικά του αρχεία. Για να γίνει αυτό μπορεί να απαιτηθεί έλεγχος των πληροφοριών σε ολόκληρη τον οργανισμό ή σε συγκεκριμένες επιχειρηματικές περιοχές. Αυτό θα σας βοηθήσει επίσης να συμμορφωθείτε με την αρχή της λογοδοσίας του GDPR. Επίσης θα πρέπει να εξεταστεί πώς πραγματοποιείται η επεξεργασία των δεδομένων προσωπικού χαρακτήρα και να προσδιοριστεί η νομική βάση επί της οποίας θα πραγματοποιηθούν και θα τεκμηριωθούν αυτές οι διαδικασίες. Αυτό είναι απαραίτητο διότι τα δικαιώματα κάποιων ατόμων θα τροποποιηθούν από τον GDPR ανάλογα με τη νομική βάση για την επεξεργασία των προσωπικών τους δεδομένων.[13]

3.2.4 Τεχνικές απαιτήσεις GDPR

Οι εντολές του GDPR προκειμένου να διασφαλιστεί μια ολοκληρωμένη λύση που προστατεύει το χρήστη ή το υποκείμενο των δεδομένων και περιορίζει τις επιχειρήσεις, μπορούν να συνοψιστούν στα ακόλουθα σημεία:

• **Διαθεσιμότητα:** Ο χρήστης θα πρέπει πάντα να έχει πρόσβαση στα δεδομένα του, ανεξάρτητα από το αν αποθηκεύονται τοπικά ή εξ αποστάσεως. Τα δεδομένα πρέπει να προστατεύονται από διαρροές ή επιθέσεις, επειδή επηρεάζουν τη διαθεσιμότητα.

• **Πληρότητα:** Θα πρέπει να καταγράφονται τα δεδομένα και κάθε γεγονός σχετικά με τη συλλογή και την επεξεργασία τους.

• **Εμπιστευτικότητα:** Μόνο τα μέρη που συμμετέχουν στην ανταλλαγή δεδομένων θα πρέπει να μπορούν να βλέπουν λεπτομέρειες της εν λόγω συναλλαγής.

• **Ορθότητα:** Θα πρέπει να εξασφαλίζεται η ακρίβεια των δεδομένων που καταγράφονται.

• **Αμετάβλητη:** Δεν θα πρέπει να υπάρχει δυνατότητα αλλαγής ιστορικών καταγραφών.

• **Ακεραιότητα:** Το περιεχόμενο του χώρου αποθήκευσης δεδομένων θα πρέπει να προστατεύεται από κακόβουλες ή ακούσιες αλλαγές.

• **Διαλειτουργικότητα:** Οι χρήστες θα πρέπει να μπορούν να συνδυάζουν δεδομένα που προέρχονται από διάφορες πηγές.

• **Μη αποκήρυξη:** Η αλληλεπίδραση με οποιαδήποτε δεδομένα δεν πρέπει να είναι δυνατόν να την αρνηθεί κάποιος σε μεταγενέστερα χρονικά σημεία.

• **Διόρθωση & Διαγραφή:** Οι χρήστες πρέπει να μπορούν να αλλάζουν ή να σβήνουν τα προσωπικά τους δεδομένα. Πρέπει επίσης να είναι σε θέση να προβαίνουν σε διορθώσεις εσφαλμένων δεδομένων.

• **Ιχνηλασιμότητα:** Οποιαδήποτε εμφάνιση δεδομένων επεξεργασίας πρέπει να είναι ανιχνεύσιμη και να συνδέεται με προηγούμενες εμφανίσεις επεξεργασίας των εν λόγω δεδομένων.

3.2.5 Κυρώσεις GDPR

Ο Κανονισμός προβλέπει ενιαίες, εξαιρετικά αυστηρές διοικητικές κυρώσεις. Η μόνη διακριτική ευχέρεια που καταλείπει στους εθνικούς νομοθέτες αφορά στη δυνατότητα που δίνει στους εθνικούς νομοθέτες για θέσπιση ποινικών κυρώσεων. Προβλέπεται 2% πρόστιμο για διοικητικές/ γραφειοκρατικές παραλείψεις ενώ για υπαίτιες παραβάσεις προβλέπεται η δυνατότητα επιβολής προστίμου ίσου με το 4% του ετήσιου παγκόσμιου τζίρου της επιχείρησης ή 20εκατομμύρια ευρώ.

Διοικητικά πρόστιμα μπορούν να επιβληθούν για ευρύ φάσμα παραβάσεων. Το άρθρο 83 του κανονισμού προβλέπει εναρμονισμένη προσέγγιση όσον αφορά τις παραβάσεις υποχρεώσεων που απαριθμούνται ρητά στις παραγράφους 4-6. Σύμφωνα με το δίκαιο των κρατών μελών, η εφαρμογή του άρθρου 83 μπορεί να επεκταθεί στις δημόσιες αρχές και τους φορείς που έχουν συσταθεί στο εν λόγω κράτος μέλος. Ο κανονισμός προβλέπει την αξιολόγηση κάθε περίπτωσης ξεχωριστά και η εποπτική αρχή είναι υπεύθυνη για την επιλογή του/των πιο κατάλληλου/-ων μέτρου/-ων.

Τα πρόστιμα είναι σημαντικό εργαλείο το οποίο θα πρέπει να χρησιμοποιούν οι εποπτικές αρχές όποτε το απαιτούν οι περιστάσεις. Οι εποπτικές αρχές ενθαρρύνονται να ακολουθούν σταθμισμένη και ισορροπημένη προσέγγιση κατά τη χρήση διορθωτικών μέτρων, προκειμένου να αντιμετωπίσουν την παράβαση κατά τρόπο αποτελεσματικό και αποτρεπτικό αλλά και αναλογικό. Σκοπός είναι να μη θεωρούνται τα πρόστιμα ύστατο μέτρο ή να αποφεύγεται η επιβολή τους, αλλά και να μη χρησιμοποιούνται κατά τρόπο που θα μείωνε την αποτελεσματικότητά τους ως εργαλείου.

Στο άρθρο 83 παράγραφος 2 παρατίθεται κατάλογος κριτηρίων που αναμένεται να χρησιμοποιούνται από τις εποπτικές αρχές κατά την αξιολόγηση του κατά πόσο θα πρέπει να επιβληθεί πρόστιμο και του ποσού του προστίμου. Τα κριτήρια αυτά είναι: α) η φύση, η βαρύτητα και η διάρκεια της παράβασης, β) ο δόλος ή η αμέλεια που προκάλεσε την παράβαση, δ) ο βαθμός ευθύνης του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, λαμβάνοντας υπόψη τα τεχνικά και οργανωτικά μέτρα που εφαρμόζουν δυνάμει των άρθρων 25 και 32, ε) τυχόν σχετικές προηγούμενες παραβάσεις του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, στ) ο βαθμός συνεργασίας με την αρχή ελέγχου για την επανόρθωση της παράβασης και τον περιορισμό των πιθανών δυσμενών επιπτώσεών της, ζ) οι κατηγορίες δεδομένων προσωπικού χαρακτήρα που επηρεάζει η παράβαση, η) ο τρόπος με τον οποίο η εποπτική αρχή πληροφορήθηκε την παράβαση, ειδικότερα εάν και κατά πόσο ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία κοινοποίησε την παράβαση, θ) σε περίπτωση που διατάχθηκε προηγουμένως η λήψη των μέτρων που αναφέρονται στο άρθρο 58 παράγραφος 2 κατά του εμπλεκόμενου υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία σχετικά με το ίδιο αντικείμενο, η συμμόρφωση με τα εν λόγω μέτρα, ι) η τήρηση εγκεκριμένων κωδίκων δεοντολογίας σύμφωνα με το άρθρο 40 ή εγκεκριμένων μηχανισμών πιστοποίησης σύμφωνα με το άρθρο 42, ια) κάθε άλλο επιβαρυντικό ή ελαφρυντικό στοιχείο που προκύπτει από τις περιστάσεις της συγκεκριμένης περίπτωσης, όπως τα οικονομικά οφέλη που αποκομιστήκαν ή ζημιών που αποφεύχθηκαν, άμεσα ή έμμεσα, από την παράβαση.[12]

3.3 Τι απαιτεί η προσαρμογή με το GDPR

Ο κανονισμός GDPR αφορά όλους τους οργανισμούς και επιχειρήσεις του ιδιωτικού και δημοσίου τομέα με έδρα εντός και εκτός Ε.Ε., που με οποιοδήποτε τρόπο συλλέγουν, επεξεργάζονται και αποθηκεύουν δεδομένα προσωπικού χαρακτήρα πελατών, προμηθευτών, συνεργατών και εργαζόμενων. Ανάλογα με την ιδιότητα του κάθε εμπλεκόμενου υπάρχουν διάφορες απαιτήσεις από τον κανονισμό. Ακολουθεί παρουσίαση των απαιτήσεων που αφορούν και τους χρηματοπιστωτικούς οργανισμούς.

3.3.1 Από διαχειριστές δεδομένων και παραγωγούς

Ακολουθεί μια σύντομη περίληψη των υποχρεώσεων που περιλαμβάνει ο GDPR για τους εκτελούντες επεξεργασία δεδομένων:

• Άρθρο 24: Πρέπει να είναι σε θέση να αποδείξει ότι κάθε επεξεργασία και χειρισμός είναι μέσα στα πλαίσια του κανονισμού.

• Άρθρο 28: Πρέπει να ενημερώνει τους κατόχους δεδομένων όταν τα δεδομένα θα μοιράζονται με άλλους εκτελούντες επεξεργασία.

• Άρθρο 29: Πρέπει να επεξεργάζεται τα εξουσιοδοτημένα δεδομένα μόνο για εξουσιοδοτημένους σκοπούς.

• Άρθρο 30: Πρέπει να τηρεί αρχείο όλων των δραστηριοτήτων επεξεργασίας δεδομένων. Η εγγραφή πρέπει να περιλαμβάνει ποιος το επεξεργάστηκε, τι υποβλήθηκε σε επεξεργασία, πού υποβλήθηκε σε επεξεργασία ή μεταφέρθηκε, πότε θα διαγραφεί, και τα μέτρα ασφαλείας που εφαρμόζονταν όταν έγινε.

• Άρθρο 32: Πρέπει να προστατεύουν τα δεδομένα με τη χρήση ψευδωνυμοποίησης και κρυπτογράφησης. Πρέπει να εξασφαλίζουν ότι τα μέτρα αυτά ελέγχονται τακτικά και μπορούν να ανακάμψουν σε περίπτωση αστοχιών.

• Άρθρο 33: Πρέπει να ενημερώνει τους ιδιοκτήτες των δεδομένων και άλλους εκτελούντες επεξεργασία δεδομένων σε περίπτωση παραβίασης, εντός 72 ωρών από την ώρα που έλαβαν γνώση της παραβίασης.

• Άρθρο 37: Πρέπει να διορίζει υπεύθυνο προστασίας δεδομένων (DPO).

• Άρθρο 50: Η διαβίβαση δεδομένων πρέπει να γίνεται μόνο προς χώρες που έχουν κριθεί ότι έχουν επαρκείς νόμους προστασίας δεδομένων.

Ο GDPR απαιτεί από τους υπευθύνους επεξεργασίας δεδομένων να υλοποιήσουν την προστασία των δεδομένων εκ σχεδιασμού και εξ ορισμού στην επεξεργασία των δεδομένων τους. Αυτό σημαίνει ότι κάθε υπεύθυνος επεξεργασίας δεδομένων πρέπει να ελέγχει εάν η απαίτηση αυτή ικανοποιείται επαρκώς. Αυτό σημαίνει να βεβαιωθεί ότι έχουν επιλεγεί οι κατάλληλες προρυθμίσεις σύμφωνα με την αρχή «πρώτα η προστασία των δεδομένων». Σε περίπτωση που τα προϊόντα, οι υπηρεσίες ή οι εφαρμογές που χρησιμοποιούνται δεν επιτρέπουν προεπιλεγμένες ρυθμίσεις φιλικές για την προστασία των δεδομένων, ο υπεύθυνος επεξεργασίας θα πρέπει να διαβιβάζει την απαίτηση αυτή στους παραγωγούς ή στους εκτελούντες την επεξεργασία δεδομένων. Ενδέχεται να είναι σκόπιμο να διατυπωθεί ο όρος «προστασία των δεδομένων εκ σχεδιασμού και εξ ορισμού» σε οποιεσδήποτε διαδικασίες σύναψης συμβάσεων και να χρησιμοποιηθεί αυτό το κριτήριο για την επιλογή των κατάλληλων προϊόντων, υπηρεσιών ή εφαρμογών. Είναι σαφές ότι οι κοινές δράσεις των ελεγκτών (π.χ. σε συγκεκριμένους τομείς της οικονομίας ή στο δημόσιο τομέα) μπορούν να έχουν ισχυρότερο αντίκτυπο στους παραγωγούς, ενώ παράλληλα να είναι πιο οικονομικά βιώσιμες για τους ελεγκτές. Οι υπεύθυνοι επεξεργασίας δεδομένων θα πρέπει να κάνουν τις έννοιες «εκ σχεδιασμού» και «εξ ορισμού» βασικά δομικά στοιχεία των διαδικασιών επεξεργασίας δεδομένων και να επενδύουν σε σχετικές υλοποιήσεις βέλτιστων πρακτικών.

Οι παραγωγοί δεν είναι επηρεαζόμενοι άμεσα από τον GDPR, αλλά εάν τα προϊόντα, οι υπηρεσίες και οι εφαρμογές τους μπορούν να χρησιμοποιηθούν για επεξεργασία προσωπικών δεδομένων στην Ευρώπη, συνίσταται να εκπληρώσουν την απαίτηση "προστασίας δεδομένων εκ σχεδιασμού και εξ ορισμού" και να καταγράψουν τον τρόπο εφαρμογής της. Αυτή η τεκμηρίωση μπορεί να παραδοθεί στους υπευθύνους επεξεργασίας δεδομένων, ώστε να μπορούν να την προσθέσουν στα έγγραφα λογοδοσίας τους και, ως εκ τούτου, να είναι βέβαιοι ότι πληρούν την απαίτηση του GDPR.

Μια υποδειγματική υλοποίηση, συμπεριλαμβανομένων των συνοδευτικών πληροφοριών, μπορεί να αποτελέσει ανταγωνιστικό πλεονέκτημα για τα προϊόντα, τις υπηρεσίες και τις εφαρμογές. Η ενσωμάτωση και η αλληλεπίδραση με τις προεπιλογές ασφαλείας είναι επίσης σημαντική.

Οι παραγωγοί θα πρέπει επίσης να επενδύσουν στη διδασκαλία και την παροχή συμβουλών στην ομάδα ανάπτυξης, για την προστασία των δεδομένων εκ κατασκευής και εξ ορισμού. Η αναπτυξιακή διαδικασία θα πρέπει να λαμβάνει υπόψη τις αρχές προστασίας δεδομένων καθ' όλη τη διάρκεια της διαδικασίας. Για τις προεπιλεγμένες ρυθμίσεις, οι αποφάσεις χρειάζονται κατάλληλη συλλογιστική και αιτιολόγηση που θα πρέπει να τεκμηριώνονται. Σε συγκεκριμένα στάδια της διαδικασίας ανάπτυξης θα μπορούσε να γίνουν έλεγχοι για τις κατάλληλες προρυθμίσεις, ενώ, στη φάση των δοκιμών (testing) θα πρέπει να ελέγχουν επιμελώς και αυτές τις πτυχές.

Επιπλέον, θα μπορούσαν να προβλεφθούν ειδικά εργαλεία προστασίας που θα βοηθούν τους χρήστες ή τους υπευθύνους επεξεργασίας δεδομένων να αλλάξουν τις προρυθμίσεις που δεν είναι φιλικές προς την προστασία των δεδομένων πριν από τη χρήση. Για τους χρήστες, αυτό θα μπορούσε να είναι μια προσέγγιση προστασίας do-it yourself, ενώ, για τους υπευθύνους επεξεργασίας δεδομένων θα τους επιτρέψει να εκπληρώσουν καλύτερα την αρχή της προστασίας των δεδομένων από προεπιλογή. Επίσης, κατά τη χρήση ενός προϊόντος, μιας υπηρεσίας ή μιας εφαρμογής, συγκεκριμένα εργαλεία μπορούν να υποστηρίξουν το φιλτράρισμα των προσωπικών δεδομένων ή το κλείδωμα οποιασδήποτε υπερβολική επεξεργασίας τους στο βαθμό που απαιτείται.

Οι παραγωγοί προϊόντων, υπηρεσιών και εφαρμογών θα πρέπει να απέχουν από τη χρήση προτύπων σχεδιασμού που μπορούν να οδηγήσουν τους χρήστες σε επιλογές που δεν είναι φιλικές προς την ιδιωτικότητα. Αντιθέτως, θα πρέπει να ενσωματώσουν την ασφάλεια, καθώς και την προστασία των δεδομένων εκ σχεδιασμού και εξ’ ορισμού στα επιχειρηματικά τους μοντέλα και να παρέχουν επαρκή καθοδήγηση και υποστήριξη στους υπευθύνους επεξεργασίας δεδομένων και στους τελικούς χρήστες.[14]

3.3.2 Τι είναι τα default settings

Κατά τη διαδικασία κατασκευής συστημάτων πληροφορικής ή υπηρεσιών πληροφορικής, οι προγραμματιστές πρέπει να αποφασίσουν για τους πιθανούς τρόπους

υλοποίησης της επιθυμητής λειτουργικότητας. Για το σκοπό αυτό, ορισμένες λειτουργίες είναι ενσωματωμένες, δηλαδή δεν μπορούν να ρυθμιστούν ή να τροποποιηθούν μετά τη δημιουργία του συστήματος/υπηρεσίας. Για άλλες λειτουργίες, εξαρτάται από τη διαμόρφωση (configuration), δηλαδή τις προδιαγραφές των σχετικών ρυθμίσεων (settings) του συστήματος, ανεξάρτητα από το αν αυτές οι λειτουργίες ενεργοποιούνται ή όχι και ποιες παράμετροι χρησιμοποιούνται. Αυτή η διαμόρφωση μπορεί να προσαρμοστεί σύμφωνα με τις ανάγκες των χρηστών. Για παράδειγμα, οι ίδιοι οι τελικοί χρήστες μπορούν να ορίσουν τις επιθυμητές ρυθμίσεις και ενδεχομένως να τις αλλάξουν με την πάροδο του χρόνου ή μια εταιρεία μπορεί να επιβάλει την κατάλληλη ρύθμιση παραμέτρων για τα συστήματα πληροφορικής όλων των εργαζομένων πριν από τη φάση παράδοσης του συστήματος.

Όσον αφορά τις διαμορφώσιμες λειτουργίες, οι προγραμματιστές πρέπει να καθορίσουν ποια από αυτές θα πρέπει να προρυθμιστούν, δηλαδή να οριστούν συγκεκριμένες τιμές, οι οποίες αντιπροσωπεύουν την προεπιλεγμένη συμπεριφορά του συστήματος σε περίπτωση που κανείς δεν αλλάξει αυτές τις ρυθμίσεις. Εναλλακτικά, μπορεί να μη γίνει προεπιλογή οποιασδήποτε διαμόρφωσης. π.χ. κατά την εγκατάσταση του συστήματος ή της υπηρεσίας πληροφορικής, οι χρήστες (ή οι τοπικοί διαχειριστές) θα μπορούσαν να ερωτηθούν για τις επιλογές τους, ρυθμίζοντας έτσι το σύστημα σύμφωνα με τις ανάγκες τους.

Για το σκοπό αυτό, η προεπιλογή σε ένα σύστημα IT ή υπηρεσία αναφέρεται σε μια προρυθμισμένη ή προκαθορισμένη τιμή που έχει αντιστοιχισθεί σε μια παραμετροποιήσιμη ρύθμιση αυτού του συστήματος ή υπηρεσίας. Αυτή η ρύθμιση δεν θα αλλάξει χωρίς την παρέμβαση του χρήστη. Μπορεί να ποικίλει από μία επιλογή μέχρι πολλαπλές επιλογές σχετικά με την ίδια λειτουργία, οι οποίες όλες μαζί αποτελούν τις λεγόμενες "προεπιλεγμένες ρυθμίσεις" (default settings). Επιπλέον, μπορεί να σχετίζεται με τη λειτουργικότητα του βασικού συστήματος ή την παροχή συμπληρωματικών ή πρόσθετων λειτουργιών του συστήματος.

Οι προεπιλογές διέπουν μεγάλο μέρος της καθημερινής χρήσης των συστημάτων και υπηρεσιών πληροφορικής, το οποίο μπορεί να είναι ή όχι εμφανές στους χρήστες. Για παράδειγμα, οι προεπιλεγμένες ρυθμίσεις για τη λειτουργία δικτύου, την εμφάνιση του συστήματος, τις επιλογές δημιουργίας αντιγράφων ασφαλείας, το πρόγραμμα περιήγησης στο Internet, είναι μόνο μερικές τυπικές περιπτώσεις, οι οποίες ισχύουν για

όλους τους τύπους λειτουργικών συστημάτων IT. Οι προεπιλεγμένες τιμές συχνά προδιαμορφώνονται σε πολλές ηλεκτρονικές φόρμες, όταν ζητείται από τους χρήστες να παρέχουν πληροφορίες (π.χ. προεπιλογές για την επιλογή χώρας ή γλώσσας). Οι προεπιλογές ασφαλείας καθορίζουν τις βασικές ιδιότητες ασφαλείας που παρέχει μια υπηρεσία ή μια εφαρμογή (π.χ. όσον αφορά την πρόσβαση στους πόρους ενός υπολογιστή ή στην αποθήκευση πληροφοριών). Οι προεπιλογές ιδιωτικότητας καθορίζουν τον προεπιλεγμένο τρόπο με τον οποίο μια εφαρμογή ή μια συσκευή επεξεργάζεται τα προσωπικά δεδομένα του χρήστη της (π.χ. όσον αφορά την πρόσβαση σε δεδομένα επικοινωνίας, τη χρήση κάμερας ή μικροφώνου, τα δεδομένα τοποθεσίας κ.λπ.).

Κάθε φορά που καταχωρείται μια προεπιλογή, η αλληλεπίδραση του χρήστη ελαχιστοποιείται. Ως εκ τούτου, οι προεπιλογές είναι απαραίτητες προκειμένου να καταστεί δυνατή η ομαλή λειτουργία των συστημάτων και υπηρεσιών χωρίς να επιβαρύνει τους χρήστες με ένα πλήθος ερωτήσεων και επιλογών να κάνουν. Ταυτόχρονα, η χρήση προεπιλογών μπορεί να αυξήσει τα σφάλματα από την πλευρά των χρηστών, δηλαδή εάν οι προεπιλογές δεν έχουν επιλεγεί κατάλληλα ή εάν οι χρήστες δεν είναι επαρκώς ενημερωμένοι. Για το λόγο αυτό, η δυνατότητα αλλαγής των προεπιλογών είναι μια απαραίτητη απαίτηση που συνοδεύει την προσφορά της προεπιλεγμένης επιλογής στην πρώτη θέση. Σε ορισμένες περιπτώσεις, μπορεί ακόμη και να χρειαστεί να αλλάξετε τις προεπιλογές κατά την πρώτη χρήση (π.χ. προεπιλεγμένο κωδικό πρόσβασης στη ρύθμιση παραμέτρων ενός διακομιστή). Σε όλες τις περιπτώσεις, η διαθεσιμότητα πληροφοριών σχετικά με τις προεπιλογές είναι υψίστης σημασίας για τη σωστή χρήση της πλήρους λειτουργικότητας ενός συστήματος ή μιας υπηρεσίας.[14]

3.3.3 Τα κριτήρια για τα default settings

Ο υπεύθυνος επεξεργασίας δεδομένων είναι ο υπεύθυνος για την προεπιλεγμένη ρύθμιση. Πρέπει να εφαρμόσει τα κατάλληλα τεχνικά και οργανωτικά μέτρα για να διασφαλίσει ότι, εξ ορισμού, υποβάλλονται σε επεξεργασία μόνο τα δεδομένα προσωπικού χαρακτήρα, τα οποία είναι αναγκαία για κάθε συγκεκριμένο σκοπό της επεξεργασίας.

Για το σκοπό αυτό, όσον αφορά την απαίτηση «προστασία δεδομένων εξ ορισμού», γίνεται αναφορά στις αρχές της δεσμευτικής χρήσης, της ελαχιστοποίησης των δεδομένων και του περιορισμού της αποθήκευσης. Αντικατοπτρίζονται σε τέσσερα κριτήρια του άρθρου 25 παράγραφος 2 του GDPR που θα πρέπει να χρησιμοποιούνται από τους υπευθύνους επεξεργασίας κατά τον καθορισμό των προεπιλογών:

Κριτήριο 1: Ελάχιστη ποσότητα δεδομένων προσωπικού χαρακτήρα: Η ποσότητα των δεδομένων προσωπικού χαρακτήρα πρέπει να είναι η ελάχιστη δυνατή για τον εκάστοτε σκοπό.

Κριτήριο 2: Ελάχιστη έκταση της επεξεργασίας δεδομένων προσωπικού χαρακτήρα:

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα θα πρέπει να ελαχιστοποιείται ανάλογα με κάθε συγκεκριμένο σκοπό, π.χ. περιορισμός του κατά πόσον θα αποθηκεύονται τα δεδομένα, του εάν και πώς αναλύονται τα δεδομένα μία ή περισσότερες φορές, του εάν τα δεδομένα μεταφέρονται σε άλλους αποδέκτες, του εάν πρόκειται για τα δεδομένα που συνδέονται με άλλες πληροφορίες, π.χ. για σκοπούς δημιουργίας προφίλ (άρθρο 21 του GDPR).

Κριτήριο 3: Ελάχιστη περίοδος αποθήκευσης των δεδομένων προσωπικού χαρακτήρα:

Η περίοδος αποθήκευσης δεδομένων προσωπικού χαρακτήρα από τον υπεύθυνο επεξεργασίας διαδραματίζει σημαντικό ρόλο. Όσον αφορά τον σκοπό αυτό, πρέπει να επιλεγεί ο ελάχιστος χρόνος αποθήκευσης των δεδομένων προσωπικού χαρακτήρα. Αυτό θα μπορούσε να σημαίνει ότι δεν υπάρχει καθόλου αποθήκευση, ή υπάρχει ανωνυμοποίηση ή διαγραφή το συντομότερο δυνατόν.

Κριτήριο 4: Ελάχιστη προσβασιμότητα των δεδομένων προσωπικού χαρακτήρα:

Σε σχέση με την προσβασιμότητα το άρθρο 25 παράγραφος 2 του GDPR αντιμετωπίζει την πιθανή πρόσβαση από οποιαδήποτε οντότητα (άτομα όπως άλλοι χρήστες, οργανισμοί όπως ο υπεύθυνος επεξεργασίας δεδομένων ή οι κυβερνητικές αρχές, μηχανήματα όπως οι μηχανές αναζήτησης ή οι διακομιστές cloud). Η προσβασιμότητα εξαρτάται από το πού αποθηκεύονται ή υποβάλλονται σε επεξεργασία τα δεδομένα, τον τρόπο με τον οποίο η πρόσβαση περιορίζεται από εκχωρημένα δικαιώματα πρόσβασης, εάν τα δεδομένα αποθηκεύονται ή υποβάλλονται σε επεξεργασία σε καθαρό κείμενο ή σε κρυπτογραφημένη μορφή και ποιος θα μπορούσε να αποκρυπτογραφήσει τα δεδομένα. Επίσης εξετάζει ποιοι είναι οι παραλήπτες των δεδομένων και αν αντίγραφα, συμπεριλαμβανομένων των αρχείων που δεν έχουν διαγραφεί με ασφάλεια, ενδέχεται να υπάρχουν και να έχουν πρόσβαση σε αυτά τρίτοι. Η θέση αποθήκευσης και επεξεργασίας

είναι σημαντική για τον προσδιορισμό της προσβασιμότητας, π.χ. η διαφορά μεταξύ μιας τοπικής επεξεργασίας σε μια συσκευή από την πλευρά του χρήστη και της κεντρικής επεξεργασίας σε ένα σύννεφο ή σε διακομιστές από την πλευρά του ελεγκτή δεδομένων. Ο περιορισμός της προσβασιμότητας σημαίνει επίσης περιορισμό της αποθήκευσης σε δικαιοδοσίες όπου ο νόμος επιτρέπει την πρόσβαση των κυβερνήσεων χωρίς επαρκείς εγγυήσεις για την προστασία των προσωπικών δεδομένων. Επίσης κατά την αναμετάδοση προσωπικών δεδομένων το εύρος θα πρέπει να περιορίζεται όσο το δυνατόν περισσότερο αναφορικά με το σκοπό για την αποτροπή της μη εξουσιοδοτημένης πρόσβασης. [14,15]

.

Κεφάλαιο 4

Blockchain

4.1 Τι είναι

Σύμφωνα με πρόσφατη μελέτη που πραγματοποιήθηκε για λογαριασμό του Ευρωπαϊκού Κοινοβουλίου από την Μονάδα Επιστημονικής Πρόβλεψης - Scientific Foresight Unit (STOA), το Blockchain ορίζεται σαν μια κοινόχρηστη και συγχρονισμένη ψηφιακή βάση δεδομένων που διατηρείται από έναν αλγόριθμο συναίνεσης και αποθηκεύεται σε πολλαπλούς κόμβους (υπολογιστές που αποθηκεύουν μια τοπική έκδοση της βάσης δεδομένων). Τα Blockchain έχουν σχεδιαστεί για να επιτυγχάνουν ανθεκτικότητα μέσω της αναπαραγωγής, πράγμα που σημαίνει ότι υπάρχουν συχνά πολλά μέρη που εμπλέκονται στη συντήρηση αυτών των βάσεων δεδομένων. Κάθε κόμβος αποθηκεύει ένα ολοκληρωμένο αντίγραφο της βάσης δεδομένων και μπορεί να ενημερώσει ανεξάρτητα τη βάση δεδομένων. Στα συστήματα αυτά, τα δεδομένα συλλέγονται, αποθηκεύονται και υποβάλλονται σε επεξεργασία με αποκεντρωμένο τρόπο. Επιπλέον, τα Blockchains είναι «λογιστικά» βιβλία-καθολικά που μόνο μπορούν να προστεθούν δεδομένα, και δεν αφαιρούνται παρά μόνο σε έκτακτες περιστάσεις. Είναι σημαντικό να σημειωθεί ότι blockchain είναι ένας τεχνολογικός κλάδος. Δεν υπάρχει μία εκδοχή αυτής της τεχνολογίας. Αντιθέτως, ο όρος αναφέρεται σε πολλές διαφορετικές μορφές κατανεμημένων βάσεων δεδομένων που παρουσιάζουν μεγάλη διακύμανση στις τεχνικές ρυθμίσεις και τις διευθετήσεις διακυβέρνησης και την πολυπλοκότητα τους.

Από την πλευρά του το CNIL (Commission Nationale de l'Informatique et des Libertés) αναφέρει ότι «Ένα blockchain είναι μια βάση δεδομένων στην οποία τα δεδομένα αποθηκεύονται και διανέμονται σε μεγάλο αριθμό υπολογιστών και στο οποίο όλες οι εγγραφές, που ονομάζονται "συναλλαγές", είναι ορατές σε όλους τους χρήστες. Ένα blockchain δεν είναι, από μόνο του, μια λειτουργία επεξεργασίας δεδομένων με το δικό της σκοπό: είναι μια τεχνολογία που μπορεί να χρησιμεύσει σε ένα ευρύ φάσμα εργασιών επεξεργασίας.» [16]

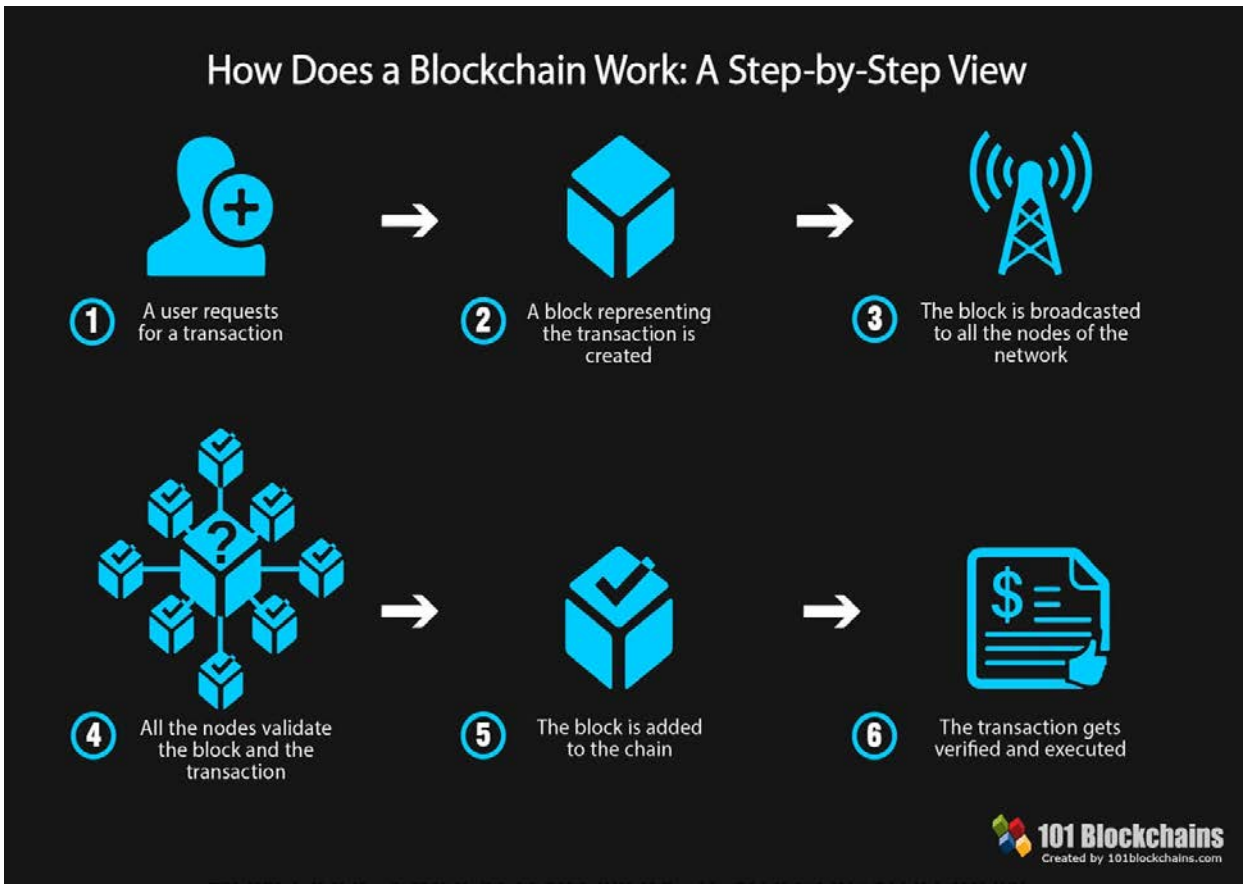
Ένας πιο γενικός ορισμός είναι αυτός του Don & Alex Tapscott, συγγραφέα του βιβλίου «Η Επανάσταση του Blockchain» (2016): «Το blockchain είναι ένα αδιάφθορο ψηφιακό λογιστικό βιβλίο για οικονομικές συναλλαγές, που μπορεί να προγραμματιστεί να καταγράφει όχι μόνο οικονομικές συναλλαγές αλλά ουσιαστικά οτιδήποτε έχει αξία.»[17]

4.1.1 Ιστορική διαδρομή

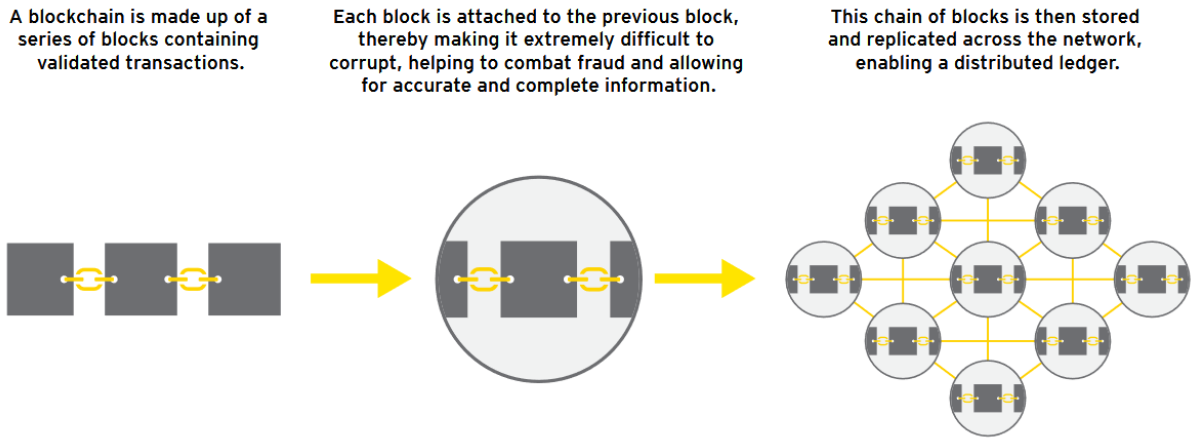
Τον Οκτώβριο του 2008, ο Satoshi Nakamoto (ψευδώνυμο) δημοσίευσε ένα έγγραφο στην λίστα αλληλογραφίας κρυπτογράφησης στο metzdowd.com, περιγράφοντας το ψηφιακό νόμισμα του Bitcoin. Είχε τον τίτλο "Bitcoin: ένα peer-to-peer ηλεκτρονικό σύστημα μετρητών". Τον Ιανουάριο του 2009, ο Νακαμότο κυκλοφόρησε το πρώτο λογισμικό Bitcoin που εκκίνησε το δίκτυο και τις πρώτες μονάδες του κρυπτονομίσματος Bitcoin, που ονομαζονταν bitcoins. Ο Σατόσι Νακαμότο, κυκλοφόρησε την έκδοση 0.1 του λογισμικού Bitcoin στο Sourceforge στις 9 Ιανουαρίου 2009.

Ο Νακαμότο ισχυρίστηκε ότι οι εργασίες για την συγγραφή του κώδικα ξεκίνησαν το 2007. Ο Νακαμότο γνώριζε ότι λόγω της φύσης του, ο βασικός σχεδιασμός θα έπρεπε να είναι σε θέση να υποστηρίξει ένα ευρύ φάσμα τύπων συναλλαγών. Η λύση που εφαρμόστηκε, επέτρεψε ειδικούς κώδικες και πεδία δεδομένων από την αρχή μέσω της χρήσης ενός predicative script.

Ο Νακαμότο δημιούργησε μια ιστοσελίδα με το όνομα domain: bitcoin.org και συνέχισε να συνεργάζεται με άλλους προγραμματιστές στο λογισμικό Bitcoin μέχρι τα μέσα του 2010. Περίπου αυτήν την χρονική περίοδο, παρέδωσε τον έλεγχο του αποθετηρίου του πηγαίου κώδικα και το κλειδί συναγερμού του δικτύου στον Gavin Andresen, μετέφερε αρκετούς σχετικά domains σε διάφορα εξέχοντα μέλη της κοινότητας Bitcoin, και σταμάτησε την εμπλοκή του στο έργο. Μέχρι λίγο πριν την απουσία και την παράδοσή του, ο Νακαμότο έκανε όλες τις τροποποιήσεις στον πηγαίο κώδικα. [17,18]



Εικόνα 10: Πηγή: 101blockchains.com, «*Πώς δουλεύει ένα Blockchain: Βήμα προς Βήμα*», 13 Ιουλίου 2018.



Εικόνα 11: Πηγή: Ernst & Young, "Blockchain-How this technology could impact the CFO" "Distributed ledger structure", 2017

4.1.2 Δομή

Τα blockchain καθορίζονται από τις ακόλουθες ιδιότητες:

- **διαφάνεια:** όλοι οι συμμετέχοντες μπορούν να δουν όλα τα δεδομένα που καταγράφονται

- **κοινή χρήση και αποκέντρωση:** πολλά αντίγραφα του blockchain συνυπάρχουν σε διαφορετικούς υπολογιστές.

- **μη αναστρέψιμη:** μόλις καταγραφούν τα δεδομένα, δεν μπορεί να τροποποιηθούν ή να αφαιρεθούν, και

- **αποδιαμεσολάβηση:** όλες οι αποφάσεις λαμβάνονται με συναίνεση μεταξύ των συμμετεχόντων, χωρίς κεντρικό διαμεσολαβητή.

Στην πράξη, υπάρχουν διάφοροι τύποι blockchain, οι οποίοι χρησιμοποιούν διαφορετικά επίπεδα δικαιωμάτων για διαφορετικές κατηγορίες συμμετεχόντων:

1. Τα **δημόσια blockchain** είναι προσβάσιμα σε όλους, οπουδήποτε στον κόσμο. Οποιοσδήποτε μπορεί να καταγράψει μια συναλλαγή, να συμμετάσχει στην επικύρωση των μπλοκ ή να αποκτήσει πρόσβαση σε ένα αντίγραφό τους.

2. Τα **εμπιστευτικά blockchain** έχουν κανόνες που καθορίζουν ποιος μπορεί να συμμετάσχει στη διαδικασία επικύρωσης ή ακόμη και να καταχωρήσει συναλλαγές. Μπορούν, ανάλογα με την περίπτωση, να είναι προσβάσιμα σε όλους ή να περιορίζονται

3. Τα **"ιδιωτικά" blockchain** ελέγχονται από έναν μοναδικό χρήστη που μόνο επιβλέπει τη συμμετοχή και την επικύρωση. Σύμφωνα με ορισμένους εμπειρογνώμονες, αυτές οι παράμετροι δεν σέβονται τις παραδοσιακές ιδιότητες των blockchain, όπως η αποκέντρωση και η κοινή επικύρωση.

Υπάρχουν τριών ειδών δρώντες που αλληλεπιδρούν με τα blockchain:

- Οι **accessors** (έχοντες πρόσβαση), οι οποίοι έχουν το δικαίωμα να διαβάσουν και να κρατήσουν ένα αντίγραφο της αλυσίδας.

- Οι **participants** (συμμετέχοντες) που έχουν το δικαίωμα να κάνουν εγγραφές (δηλ. να κάνουν μια συναλλαγή για την οποία ζητούν επικύρωση)

- Οι **miners** («μεταλλωρύχοι») που επικυρώνουν μια συναλλαγή και δημιουργούν μπλοκ εφαρμόζοντας τους κανόνες του blockchain για να έχουν "αποδοχή" από την κοινότητα.[19]

4.1.3 Double Spending

Η τεχνολογία blockchain εξασφαλίζει την εξάλειψη του προβλήματος διπλής χρήσης (double-spending), με τη βοήθεια κρυπτογραφίας δημόσιου κλειδιού, σύμφωνα με την οποία κάθε παράγοντας παίρνει ένα ιδιωτικό κλειδί (διατηρείται κρυφό σαν κωδικός πρόσβασης) και ένα δημόσιο κλειδί που μοιράζεται με όλους τους άλλους παράγοντες. Μια συναλλαγή ξεκινά όταν ο μελλοντικός κάτοχος των κερμάτων ή ψηφιακών διακριτικών (digital tokens) στέλνει το δημόσιο κλειδί του στον αρχικό ιδιοκτήτη. Τα κέρματα/tokens μεταφέρονται με την ψηφιακή υπογραφή ενός hash. Τα δημόσια κλειδιά είναι διευθύνσεις που δημιουργούνται κρυπτογραφικά αποθηκευμένες στο Blockchain. Κάθε κέρμα/token συνδέεται με μια διεύθυνση, και μια συναλλαγή στην κρυπτο-οικονομία είναι απλά μια μεταφορά/ανταλλαγή νομισμάτων από τη μία διεύθυνση στην άλλη. Το εντυπωσιακό χαρακτηριστικό του blockchain είναι ότι τα δημόσια κλειδιά δεν είναι ποτέ συνδεδεμένα με μια πραγματική ταυτότητα. Οι συναλλαγές, αν και ανιχνεύσιμες, ενεργοποιούνται χωρίς να αποκαλύπτουν την ταυτότητα κάποιου. Αυτή είναι μια σημαντική διαφορά με τις συναλλαγές σε νομίσματα που, με εξαίρεση τις (μη ανιχνεύσιμες) συναλλαγές τοις μετρητοίς, σχετίζονται με συγκεκριμένους οικονομικούς παράγοντες που διαθέτουν νομική οντότητα (είτε φυσική είτε νομική).

4.1.4 Payment Finality

Σε έναν κόσμο με παραστατικό χρήμα (fiat money), το αμετάκλητο της πληρωμής (payment finality) γίνεται αντιληπτό σε σχέση με το τραπεζικό χρήμα εντός μιας

τριγωνικής δομής πληρωμή που περιλαμβάνει έναν πληρωτή, έναν δικαιούχο και μια τράπεζα που ενεργεί ως «μεσάζον». Αυτός ο "μεσάζον" είναι στην πραγματικότητα το αξιόπιστο τρίτο μέρος που απαιτείται σε όλες τις πληρωμές μέχρι την έλευση των κρυπτονομισμάτων. Ωστόσο, τα τελευταία είναι αναξιόπιστα πρωτόκολλα που απαλλάχτηκαν από το αξιόπιστο τρίτο μέρος. Η έννοια που αποδίδεται στην αμετάκλητη πληρωμή σε μια κρυπτο-οικονομία διαφέρει από αυτήν που αποδίδεται στο παραδοσιακό τραπεζικό σύστημα: μια συναλλαγή είναι οριστική μόλις συμπεριληφθεί στο blockchain, μια και έτσι καθίσταται ταυτόχρονα επαληθεύσιμη από πολλές πηγές.

4.1.5 Miners

Το blockchain είναι μια αλυσίδα εγγραφών συναλλαγών που ένα υποσύνολο συμμετεχόντων στο δίκτυο (γνωστό και ως «miners») εμπλουτίζει με την επίλυση δύσκολων υπολογιστικών προβλημάτων. Οι «miners» σκληρά (και ανώνυμα) ανταγωνίζονται στο δίκτυο για να λύσουν το μαθηματικό πρόβλημα με τον πιο αποτελεσματικό τρόπο, προσθέτοντας έτσι το επόμενο μπλοκ στο Blockchain. Η ανταμοιβή για το μπλοκ (δηλαδή κέρματα που έχουν πρόσφατα δημιουργηθεί) αποστέλλονται στη δημόσια διεύθυνση του «miner». Αν ο «miner»θέλει να ξοδέψει αυτά τα νομίσματα, πρέπει να υπογράψει με το αντίστοιχο ιδιωτικό κλειδί. Όταν αυξάνεται η δύναμη εξόρυξης σε όλο το σύστημα, το ίδιο κάνει και η δυσκολία των υπολογιστικών προβλημάτων που απαιτούνται για να εξορύξεις ένα νέο μπλοκ. Αυτό το επίπεδο δυσκολίας προσαρμόζεται για να κρατήσει σταθερό το ρυθμό δημιουργίας νέων μπλοκ, περίπου στα δέκα λεπτά.

4.1.6 Κρυπτογραφία

Το blockchain βασίζεται εκτενώς σε hash και λειτουργίες hash. Το hash (output) είναι το αποτέλεσμα ενός μετασχηματισμού των αρχικών πληροφοριών (input). Μια λειτουργία hash είναι ένας μαθηματικός αλγόριθμος που εισάγονται κάποια δεδομένα και τα μετατρέπει σε μια τιμή hash. Μια κρυπτογραφική λειτουργία hash χαρακτηρίζεται από την ακραία δυσκολία του να αναστραφεί, με άλλα λόγια, για να δημιουργηθούν ξανά τα δεδομένα εισόδου από την τιμή hash μόνο.

Η λειτουργία proof-of-work (απόδειξη εργασίας) βρίσκεται στην καρδιά της δημιουργίας μπλοκ στο πρωτόκολλο Bitcoin. Κρυπτογραφικά proof-of-work απαιτούνται για την αποδοχή νέων μπλοκ. Για την επαλήθευση των συναλλαγών, και τον υπολογισμό του proof-of-work, το Bitcoin βασίζεται σε μια κρυπτογραφική λειτουργία hash, που ονομάζεται διπλός SHA256 αλγόριθμος hash. Ο αλγόριθμος SHA256 (Ασφαλής Αλγόριθμος Κατακερματισμού 256-bit) χρησιμοποιείται για κρυπτογραφική ασφάλεια. Οι αλγόριθμοι κρυπτογραφικού κατακερματισμού παράγουν μη αναστρέψιμους και μοναδικούς κατακερματισμούς. Όσο μεγαλύτερος είναι ο αριθμός των πιθανών κατακερματισμών, τόσο μικρότερη είναι η πιθανότητα δημιουργίας του ίδιου κατακερματισμού από δύο τιμές. Για να είναι έγκυρο ένα μπλοκ, πρέπει να γίνει κατακερματισμός σε τιμή μικρότερη από τον τρέχοντα στόχο. Κάθε νέο μπλοκ που παράγεται αναγνωρίζει ότι έχει γίνει έργο κατά τη δημιουργία του. Η proof-of-stake είναι μια προτεινόμενη εναλλακτική λύση για την proof-of-work που έχει ήδη υλοποιηθεί για ορισμένα νομίσματα (εκτός από το Bitcoin), ενώ άλλα στηρίζονται σε ένα υβριδικό πρωτόκολλο. Αντί να διαχωρίζονται τα μπλοκ αναλογικά με τους σχετικούς ρυθμούς κατακερματισμού των miners (δηλ. την ισχύ εξόρυξης), τα πρωτόκολλα «proof of stake» προκύπτουν διαιρώντας τα μπλοκ αναλογικά με τον τρέχοντα πλούτο των miners (π.χ. πόσα κέρματα έχουν). Η proof-of-stake έχει ορισμένα διακριτά πλεονεκτήματα σε σχέση με την proof-of-work (μη περιττό πρωτόκολλο, μειωμένη πιθανότητα επίθεσης 51%, δυνητικά ταχύτερων αλυσίδων, κλπ.).

4.1.7 Smart Contracts

Ένα «έξυπνο συμβόλαιο» (smart contract) είναι μια αυτο-επιβαλλόμενη συμφωνία ενσωματωμένη στον κώδικα υπολογιστή που διαχειρίζεται ένα blockchain. Ο κώδικας περιλαμβάνει ένα σύνολο κανόνων σύμφωνα με τους οποίους τα μέρη του εν λόγω «έξυπνου συμβολαίου» συμφωνούν να αλληλοεπιδρούν μεταξύ τους. Εάν και όταν πληρούνται οι προκαθορισμένοι κανόνες, η συμφωνία εφαρμόζεται αυτόματα. Τα «έξυπνα συμβόλαια» παρέχουν μηχανισμούς για την αποτελεσματική διαχείριση διακεκριμένων στοιχείων (assets) και των δικαιωμάτων πρόσβασης μεταξύ δύο ή περισσοτέρων μερών. Μπορεί κανείς να το σκεφτεί σαν ένα κρυπτογραφικό κουτί που ξεκλειδώνει την αξία ή την πρόσβαση, αν και όταν πληρούνται συγκεκριμένες προκαθορισμένες συνθήκες. Οι υποκείμενες τιμές και τα δικαιώματα πρόσβασης που διαχειρίζονται αποθηκεύονται σε ένα blockchain, το οποίο είναι ένα διαφανές,

κοινόχρηστο καθολικό, όπου προστατεύονται από διαγραφή, αλλοίωση και αναθεώρηση. Ως εκ τούτου, τα «έξυπνα συμβόλαια» παρέχουν έναν δημόσιο και επαληθεύσιμο τρόπο ενσωμάτωσης των κανόνων διακυβέρνησης και της επιχειρηματικής λογικής σε μερικές γραμμές κώδικα, οι οποίες μπορούν να ελεγχθούν και να επιβληθούν από την πλειοψηφική συναίνεση ενός δικτύου P2P.[19,20]

4.2 Blockchain και εφαρμογές

Η τεχνολογία blockchain βρίσκει εφαρμογή σε πολλούς τομείς, ενώ συνέχεια ανακαλύπτονται νέοι τρόποι που μπορεί να χρησιμοποιηθεί για να διευκολύνει τη ζωή μας. Μερικοί από αυτούς είναι οι εξής:

- Έξυπνα συμβόλαια τύπου Ethereum ή πιο πολύπλοκα.

Εικόνα 12: Πηγή: PricewaterhouseCoopers, «*Έξυπνα συμβόλαια, -απλά προς πολύπλοκα*», 2016.

- Peer to peer πληρωμές μέσω κρυπτονομισμάτων και όχι μόνο, όπως το OpenBazzar που είναι ένα ανοικτού κώδικα Ebay χωρίς προμήθειες και διαμεσολαβητές.
- Crowd funding ή συλλογική χρηματοδότηση τύπου Kickstarter ή Gofundme μέσω έξυπνων συμβολαίων και blockchain.
- Governance ή διακυβέρνηση, που θα προσφέρει διαφάνεια σε διαδικασίες όπως οι εκλογές ή οι εταιρικές αποφάσεις ή η χρηματοδότηση κομμάτων κλπ.
- Η επιβεβαίωση της αυθεντικότητας/προέλευσης προϊόντων και αγαθών μέσω ενός συστήματος καταγραφής της πορείας του, τύπου blockchain.
- Η προστασία των πνευματικών δεδομένων μέσω έξυπνων συμβολαίων που θα επιτρέπουν τη χρήση αφού προηγηθεί πληρωμή.
- Η καταχώρηση τίτλου γης και ιδιοκτησίας που θα είναι προσβάσιμος σε όλους χωρίς να υπάρχει φόβος πλαστογραφίας ή/και άλλης απάτης.
- Οι συναλλαγές μετοχών peer to peer μέσω έξυπνων συμβολαίων που θα εκτελούνται άμεσα και χωρίς την μεσολάβηση μεσαζόντων κ.α. [19,20]

Κεφάλαιο 5

Η συνύπαρξη Blockchain-Fintech-GDPR

5.1 Fintech και Blockchain

Καθώς οι χρηματοπιστωτικές υπηρεσίες κινούνται προς την ψηφιοποίηση, τα χρηματοπιστωτικά ιδρύματα θα πρέπει να λειτουργούν με χαμηλότερο κόστος, γραμμές πληρωμών μεγάλου όγκου για την εξυπηρέτηση των λιανικών δραστηριοτήτων τους, ενώ θα πρέπει να καλύπτουν παράλληλα την αυξανόμενη ζήτηση για ασφάλεια και κινητικότητα. Υπάρχουν επίσης αυξανόμενες απαιτήσεις για αποτελεσματικότητα και διαφάνεια από θεσμικούς αντισυμβαλλομένους και τις χρηματοπιστωτικές ρυθμιστικές αρχές, σχετικά με τις επιχειρηματικές και τεχνολογικές διαδικασίες.

5.1.1 Πώς το blockchain ευνοεί το Fintech

Οι κύριοι παράγοντες πίσω από την υιοθέτηση της τεχνολογίας κατανεμημένου καθολικού, blockchain, είναι:

- Μείωση κόστους - Η ευκαιρία τα χρηματοπιστωτικά ιδρύματα να αποσυνδέσουν τα συστήματα παλαιού τύπου και να μειώσουν τα επίπεδα που απαιτούνται για την κοινή χρήση δεδομένων. Εξασφαλίζοντας ότι τα δεδομένα είναι εγγενώς σε ψηφιακή μορφή και διαμοιράζονται στο σημείο της συναλλαγής, ο χρόνος συμφιλίωσης μπορεί επίσης να μειωθεί δραστικά.

- Διαχείριση κινδύνων - Η ικανότητα πρόβλεψης και αποφυγής της υπερεπέκτασης των υποχρεώσεων ενός ιδρύματος. Παρέχοντας ένα τυποποιημένο πλαίσιο για την καταγραφή ακόμη και πολύπλοκων συναλλαγών, όπως τα

παράγωγα, τα χρηματοπιστωτικά ιδρύματα μπορούν να διευκολύνουν πολύ τη διαχείριση των κινδύνων και των θέσεών τους σε πραγματικό χρόνο.

- Κανονιστική συμμόρφωση - Η συμμόρφωση με τις απαιτήσεις διαφόρων νομοθετικών συνόλων, καθώς και η διενέργεια μόνο εγκεκριμένων συναλλαγών μπορούν να αυτοματοποιηθούν σε μεγάλο βαθμό.

Οι τεχνολογίες κατανεμημένου καθολικού μπορεί να επιτρέψουν στα ιδρύματα να ενσωματώσουν τους κανόνες λειτουργίας τους εντός κώδικα. Από την άποψη της διακυβέρνησης, αυτό σημαίνει ότι οι επιχειρηματικές λειτουργίες των κανονιστικών, ελεγκτικών και εσωτερικών ελέγχων μπορούν να ενσωματωθούν στο σύστημα συναλλαγών. Για παράδειγμα:

Αλλαγές κανονισμών. Η τεχνολογία κατανεμημένου καθολικού θα μπορούσε να βοηθήσει τα χρηματοπιστωτικά ιδρύματα και τις ρυθμιστικές αρχές με τέτοιο τρόπο ώστε μόλις ένας νέος κανονισμός κωδικοποιηθεί στο κατανεμημένο καθολικό να διαμοιράζεται σε όλους, χωρίς να απαιτείται τεχνική αλλαγή από τους αντισυμβαλλομένους.

Έλεγχους. Οι έλεγχοι δείχνουν κυρίως την κατάσταση ενός συγκεκριμένου συστήματος ή οργανισμού σε ένα δεδομένο χρονικό σημείο. Η τεχνολογία κατανεμημένου καθολικού θα μπορούσε να επιτρέψει τη συνεχή παρακολούθηση.

Επιχειρηματική λογική. Στην κλίμακα ενός μεμονωμένου χρηματοπιστωτικού ιδρύματος, η επιχειρηματική λογική μπορεί να προγραμματιστεί σε έξυπνες συμβάσεις (smart contracts), απλοποιώντας σημαντικά τις δραστηριότητες back-office, ιδίως όσον αφορά τη συμφωνία δεδομένων και τη διευθέτηση περιουσιακών στοιχείων ή κεφαλαίων. Με τη θέσπιση κοινού πρωτοκόλλου για τις συναλλαγές και τους διακανονισμούς, τα χρηματοπιστωτικά ιδρύματα μπορούν να κινηθούν προς διακανονισμούς σε σχεδόν πραγματικό χρόνο. Εάν όλες οι χρηματοπιστωτικές συναλλαγές καταγράφονται σε ρυθμιζόμενα λογιστικά βιβλία, ενδέχεται να είναι δυνατή η εφαρμογή κανονισμών προληπτικής εποπτείας. Για παράδειγμα, αυτό θα μπορούσε να περιορίσει αυτόματα νέες συναλλαγές που κάνουν τον ισολογισμό ενός ιδρύματος να ξεφύγει από τις παραμέτρους διαχείρισης κινδύνου που εκδίδονται από τις ρυθμιστικές αρχές στη δικαιοδοσία των οποίων υπόκεινται τα χρηματοπιστωτικά ιδρύματα.

Μειώση της ανάγκης για εσωτερική παρακολούθηση. Με την υποστήριξη των συναλλαγών Blockchain που τώρα θα διεξάγονται και θα διευθετούνται από το λογισμικό και όχι από το προσωπικό. Η απαίτηση για τακτικούς ελέγχους δεδομένων θα παραμείνει, ώστε να διασφαλίζεται ότι η έξυπνη σύμβαση έχει εκτελεστεί όπως προβλέπεται.

Επίτευξη συναίνεσης σε ένα αβέβαιο περιβάλλον. Η φύση του κατανεμημένου καθολικού επιτρέπει την επίτευξη συναίνεσης για μια συγκεκριμένη συναλλαγή, ακόμα και όταν δεν μπορείτε να εμπιστεύεστε τους αντισυμβαλλομένους στο δίκτυο. [19]

5.1.2 Οι τεχνικές προκλήσεις του blockchain στο Fintech

Η χρήση ενός κατανεμημένου καθολικού συνεπάγεται ότι τα δεδομένα μοιράζονται μεταξύ όλων των αντισυμβαλλομένων στο δίκτυο. Από τη μία πλευρά, αυτό θα μπορούσε ενδεχομένως να έχει αρνητικό αντίκτυπο στην εμπιστευτικότητα·ενώ από την άλλη, έχει θετικό αντίκτυπο στη διαθεσιμότητα με πολλούς κόμβους που συμμετέχουν στο Blockchain, καθιστώντας το πιο ανθεκτικό.

Είναι πολύ σημαντικό να προστατεύονται τα ιδιωτικά κλειδιά πρόσβασης σε ένα blockchain γιατί οι ενέργειες που λαμβάνουν χώρα στη μηχανή π.χ. ενός χάκερ, όπως οι απόπειρες αποκρυπτογράφησης αρχείων ή η αναπαραγωγή ιδιωτικού κλειδιού, δεν υπόκεινται ελέγχους ή καταγραφή που επιβάλλονται από το διακομιστή (server) όπως σε άλλες βάσεις δεδομένων και εκτελούνται χωρίς να μπορεί κανείς άλλος να το καταλάβει.

Σε αντίθεση με τα παραδοσιακά συστήματα, όπου ένας διαχειριστής διακομιστή ήταν σε θέση να παρακολουθεί τις προσπάθειες για να παραβιαστεί ένας λογαριασμός χρήστη ή πελάτη, οι κακόβουλοι χρήστες μπορούν να συνεχίσουν να προσπαθούν απεριόριστα να αποκρυπτογραφήσουν ή να αναπαράγουν ένα ιδιωτικό κλειδί από κρυπτογραφημένα δεδομένα ενός συγκεκριμένου καθολικού. Με το Blockchain, δεν υπάρχει τρόπος να γνωρίζουμε ότι αυτό συμβαίνει μέχρι να πετύχει ο χάκερ.

Οι περισσότερες υλοποιήσεις blockchain βασίζονται στα κρυπτογραφικά δημόσια και ιδιωτικά κλειδιά για να λειτουργήσουν. Η κύρια πρόκληση που σχετίζεται με την κρυπτογράφηση είναι ότι πρέπει να ακολουθούνται αυστηρές πολιτικές και διαδικασίες κατά τη διαχείριση κλειδιών, συμπεριλαμβανομένων των ατόμων, των διαδικασιών και της τεχνολογίας.

Συνήθως, ο χρήστης δημιουργεί τα ιδιωτικά και δημόσια κλειδιά χρησιμοποιώντας λογισμικό, όπως το λογισμικό-πελάτη blockchain, ή άλλο διαθέσιμο λογισμικό. Έχει ήδη αποδειχθεί, ότι ορισμένα προγράμματα δημιουργούν κλειδιά που είναι αδύναμα. Υπάρχουν επίσης τεκμηριωμένες προσπάθειες να διαδοθούν σκόπιμα αποδυναμωμένες γεννήτριες τυχαίων αριθμών, από τις οποίες μπορεί να παραχθεί ένα περιορισμένο φάσμα πιθανών τιμών. Τα κλειδιά που παράγονται μέσω των συγκεκριμένων γεννητριών τυχαίων αριθμών θα μπορούσαν να «σπάσουν» ευκολότερα.

Η κβαντική πληροφορική αποτελεί απειλή για την αξιοπιστία της ασύμμετρης κρυπτογραφίας. Αν και δεν αποτελεί άμεση απειλή, θα πρέπει ασφαλώς να ληφθεί υπόψη για μια λύση ανθεκτική στο μέλλον. Δημοφιλείς αλγόριθμοι ασφαλείας που χρησιμοποιούνται για την εξασφάλιση πληροφοριών μέσω μιας περίπλοκης πρόκλησης (λογικό ή μαθηματικό πρόβλημα/υπολογισμό), μπορούν τώρα να επιλυθούν σε μικρότερο χρονικό διάστημα μέσω της χρήσης κβαντικού υπολογιστή.

Σε ένα καθολικό με ελεύθερη πρόσβαση, όλοι οι αντισυμβαλλόμενοι μπορούν να κάνουν λήψη του καθολικού, πράγμα που σημαίνει ότι ενδέχεται να μπορούν να εξερευνήσουν ολόκληρο το ιστορικό των συναλλαγών, συμπεριλαμβανομένων εκείνων στις οποίες δεν ήταν μέλη. Το "δικαίωμα στη λήθη" όπου οι πληροφορίες πρέπει να αφαιρεθούν από ένα καθολικό είναι δύσκολο να υλοποιηθεί. Συνήθως, πολλοί αντισυμβαλλόμενοι έχουν τα δεδομένα από το καθολικό και θα ήταν δύσκολο να αποδειχθεί ότι όλα τα δεδομένα έχουν διαγραφεί.

Επιπλέον, υπάρχει μια πρόκληση σε σχέση με τα έξυπνα συμβόλαια που μπορούν να έχουν πρόσβαση στα δεδομένα προκειμένου να επεξεργάζονται συναλλαγές. Από την στιγμή που αυτό είναι δυνατό, υπάρχει πιθανότητα να διαρρεύσουν πληροφορίες σχετικά με το τι είναι υπό επεξεργασία. Με αυτόν τον τρόπο, η προστασία της

ιδιωτικότητας μπορεί να παραβιαστεί. Επίσης δεν αποκλείεται να υπάρχουν άγνωστα τρωτά σημεία στον κώδικα του διανεμημένου καθολικού που εφαρμόζεται στην κάθε περίπτωση [19]

5.1.3 Ψηφιακή ταυτότητα και fintech

Ως «ψηφιακή ταυτότητα» νοούνται οι πληροφορίες που χρησιμοποιούνται για την εκπροσώπηση μιας οντότητας σε ένα σύστημα πληροφοριών. Ο σκοπός του συστήματος πληροφοριών καθορίζει ποια από τα χαρακτηριστικά που περιγράφουν μια οντότητα χρησιμοποιούνται για την ταυτότητα. Από την άποψη αυτή, είναι σημαντικό να θεωρηθεί ότι μια οντότητα περιλαμβάνει πρόσωπα (φυσικά ή νομικά), αντικείμενα (πληροφορίες, συστήματα ή συσκευές) ή μια ομάδα αυτών των επιμέρους οντοτήτων. Επιπλέον, τα χαρακτηριστικά θα μπορούσαν να είναι ετερογενή, για παράδειγμα όνομα, αριθμό τηλεφώνου και εκπαιδευτικό υπόβαθρο για φυσικά πρόσωπα ή, όσον αφορά μια νομική οντότητα, δήλωση που θα πιστοποιεί την οικονομική της κατάσταση ή το αποτέλεσμα των επαληθεύσεων των δεδομένων σε μια διαδικασία δέουσας επιμέλειας ως προς τον πελάτη (customer Due Diligence, CDD).

Όσον αφορά το CDD, τα θεσμικά όργανα πρέπει να συμμορφώνονται με την Οδηγία (ΕΕ) 2018/843 για την πρόληψη της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και τη χρηματοδότηση της τρομοκρατίας, όπως μεταφέρεται στην εθνική τους νομοθεσία. Η οδηγία απαιτεί από τα ιδρύματα να αξιολογούν τους κινδύνους νομιμοποίησης εσόδων από παράνομες δραστηριότητες και χρηματοδότησης της τρομοκρατίας που συνδέονται με τις επιχειρήσεις και τους πελάτες τους και να θέτουν σε εφαρμογή πολιτικές και διαδικασίες σε επίπεδο ομίλου για τον μετριασμό αυτών των κινδύνων. Για να επιτευχθεί αυτό, τα ιδρύματα υποχρεούνται να ανταλλάσσουν πληροφορίες με τα υποκαταστήματά τους και τις θυγατρικές τους εντός της ΕΕ και τρίτων χωρών, στο βαθμό που επιτρέπεται από την τοπική νομοθεσία.

Επί του παρόντος, μια σειρά λύσεων ψηφιακής ταυτότητας που ενεργοποιούνται από το DLT βρίσκονται υπό συζήτηση στην αγορά. Σε γενικές γραμμές, οι λύσεις αυτές βασίζονται σε i) ένα DLT που αποθηκεύει την απόδειξη των δημόσιων κλειδιών των ταυτοτήτων και την απόδειξη των δεδομένων και των βεβαιώσεων·ii) εξωτερική

αποθήκευση δεδομένων όπου βρίσκονται δεδομένα και έγγραφα iii) αίτηση τελικού χρήστη για τον έλεγχο της ταυτότητας και iv) έξυπνα συμβόλαια που ενορχηστρώνουν τη διαδικασία.

Ορισμένα ιδρύματα διερευνούν επί του παρόντος τη δυνατότητα κοινοποίησης επαληθευμένων δεδομένων πελατών σε άλλο ίδρυμα μέσω της χρήσης DLT, προκειμένου να αποφευχθεί η επανάληψη των προσπαθειών και να ενισχυθεί η εμπειρία των πελατών τους, καθιστώντας τη διαδικασία ένταξης/εγγραφής πιο βολική για αυτά σε σύγκριση με τις παραδοσιακές διαδικασίες, για παράδειγμα, όταν ο πελάτης υποχρεούται να είναι παρών φυσικά κατά τη στιγμή της επαλήθευσης ταυτότητας. Λόγω πιθανών ζητημάτων συμμόρφωσης που προκύπτουν από τη χρήση προσωπικών δεδομένων, τα ιδρύματα περιορίζουν το πεδίο χρήσης για να μοιράζονται μόνο δεδομένα CDD και να επαληθεύουν τα αποτελέσματα των εταιρικών πελατών.

Όταν δεν υπάρχουν καταχωρημένα τα στοιχεία ενός πελάτη στα πλαίσια του «γνώριζε τον πελάτη σου» (Know Your Customer, KYC), γίνεται από το εκάστοτε ίδρυμα ταυτοποίηση και επαλήθευση των στοιχείων που προσκομίζονται. Μετά την επαλήθευση των πληροφοριών που λαμβάνει από τους πελάτες, το ίδρυμα αποθηκεύει την ψηφιακή έκδοση των σχετικών εγγράφων και πληροφοριών που λαμβάνονται στην εσωτερική βάση δεδομένων του. Τα κατακερματισμένα (hashed) έγγραφα και τα αποδεικτικά στοιχεία του αποτελέσματος της διαδικασίας επαλήθευσης (επαληθευμένα ή απορριφθέντα) θα μπορούσαν να αποθηκευτούν στο DLT.

Δεδομένου ότι το αποτέλεσμα της επαλήθευσης συνδέεται με την ψηφιακή ταυτότητα του πελάτη, ο πελάτης μπορεί να το αποκαλύψει μαζί με την ψηφιακή έκδοση των εγγράφων σε μεταγενέστερες διαδικασίες κατά την εγγραφή του. Τα ιδρύματα μπορούν να εμπιστεύονται τα έγγραφα εάν τα hash τους είναι τα ίδια με αυτά του κατανεμημένου καθολικού. Στο πλαίσιο αυτό, ο αποδέκτης της βεβαίωσης μπορεί να επαληθεύσει την ακεραιότητά της βάσει του ποιος την εξέδωσε και του κατά πόσον είναι αξιόπιστος για τους σκοπούς του (π.χ. ανάλογα με το ποιος είναι ο εκδότης ή εάν η βεβαίωση είναι πρόσφατη). Αυτό θα μπορούσε να επιτρέψει την απλούστευση της διαδικασίας επαλήθευσης της γνησιότητας των εγγράφων και, κατά συνέπεια, να μειώσει το σχετικό κόστος και χρόνο.

Επιπλέον, η τεχνολογία αυτή έχει τη δυνατότητα να αλλάξει ριζικά τον τρόπο με τον οποίο οι πελάτες έχουν πρόσβαση σε χρηματοπιστωτικές υπηρεσίες στο διαδίκτυο, καθώς θα επέτρεπε τη χρήση μιας ενιαίας ψηφιακής ταυτότητας, καθιστώντας την πιο βολική. Θα επέτρεπε επίσης στους πελάτες να παρουσιάζουν ψηφιακά έγγραφα και βεβαιώσεις αντί να μεταφέρουν φυσικά έγγραφα σε υποκατάστημα. Επιπλέον, οι πληροφορίες των πελατών θα μπορούσαν να ενημερώνονται σε ένα μόνο μέρος και το ίδρυμα θα μπορούσε να λάβει μια ειδοποίηση όταν αλλάξει, η οποία ενεργοποιείται από μια έξυπνη σύμβαση που είναι αποθηκευμένη στο DLT. Ωστόσο, μπορεί να υπάρχουν φορές που η ψηφιακή ταυτότητα που είναι αποθηκευμένη στο καθολικό ενδέχεται να μην επαρκεί για την κάλυψη των απαιτήσεων CDD των συμμετεχόντων ιδρυμάτων και ενδέχεται να απαιτούνται πρόσθετα έγγραφα ή πληροφορίες για τον μετριασμό του κινδύνου που συνδέεται με τον πελάτη, π.χ. προσωπικά δεδομένα και πληροφορίες που σχετίζονται με τον πραγματικό δικαιούχο (φυσικό πρόσωπο) του εταιρικού πελάτη.[21,22]

5.1.4 Οι ρυθμιστικές προκλήσεις του blockchain στο Fintech

Η ραγδαία ανάπτυξη της χρηματοοικονομικής τεχνολογίας (Fintech) τα τελευταία χρόνια έχει δημιουργήσει σημαντικές προκλήσεις σε σχέση με τις αυξημένες ρυθμιστικές ανάγκες που υπάρχουν στον χρηματοπιστωτικό κλάδο.

Η τεχνολογία FinTech παρουσιάζει επίσης ευκαιρίες αλλά και προκλήσεις όσον αφορά τη συμμόρφωση προς τις ρυθμιστικές διατάξεις και την εποπτεία. Μπορεί να διευκολύνει, να εκσυγχρονίσει και να αυτοματοποιήσει τη συμμόρφωση και την υποβολή σχετικών στοιχείων και να βελτιώσει την εποπτεία. Οι πάροχοι υπηρεσιών μπορούν να παρέχουν σε ρυθμιζόμενες οντότητες υπηρεσίες συμμόρφωσης βασισμένες στην τεχνολογία FinTech, η ευθύνη, ωστόσο, για την εκπλήρωση των υποχρεώσεων των ρυθμιζόμενων οντοτήτων εξακολουθεί να ανήκει στις ίδιες. Για παράδειγμα, οι οντότητες που υπόκεινται σε απαιτήσεις δέουσας επιμέλειας ως προς τον πελάτη βάσει του ρυθμιστικού πλαισίου για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες

δραστηριότητες δεν επιτρέπεται να αναθέτουν την ευθύνη για την εκπλήρωση των υποχρεώσεων αυτών σε εξωτερικούς παρόχους υπηρεσιών.[22]

Ο γενικός κανονισμός για την προστασία των δεδομένων (GDPR) και η οδηγία κατά της νομιμοποίησης εσόδων από παράνομες δραστηριότητες παρέχουν θεμελιώδεις εγγυήσεις για την προστασία των δεδομένων προσωπικού χαρακτήρα και της ακεραιότητας του χρηματοπιστωτικού συστήματος της ΕΕ κατά της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και της χρηματοδότησης της τρομοκρατίας. Μια χρηματοπιστωτική αγορά της ΕΕ με τεχνολογικές δυνατότητες απαιτεί την πλήρη συμμόρφωση με τις εν λόγω θεμελιώδεις εγγυήσεις. Οι κίνδυνοι του κυβερνοχώρου υπονομεύουν την εμπιστοσύνη και συνιστούν απειλή για τη σταθερότητα του χρηματοπιστωτικού συστήματος.

Η τεχνολογική καινοτομία οδήγησε στην εμφάνιση νέων ειδών χρηματοπιστωτικών περιουσιακών στοιχείων, όπως τα κρυπτοπεριουσιακά στοιχεία (crypto-assets). Τα κρυπτοπεριουσιακά στοιχεία και η τεχνολογία blockchain στην οποία βασίζονται υπόσχονται πολλά για τις χρηματοπιστωτικές αγορές και υποδομές. Η χρήση τους, όμως, ενέχει και κινδύνους, όπως προκύπτει από την έντονη μεταβλητότητα των κρυπτοπεριουσιακών στοιχείων, τα φαινόμενα απάτης, τις λειτουργικές αδυναμίες και τις ευπάθειες των ανταλλακτηρίων κρυπτοπεριουσιακών στοιχείων.

Η χρήση DLT (Distributed ledger technology) και έξυπνων συμβολαίων για τη χρηματοδότηση του εμπορίου ενέχει διάφορους κινδύνους από προληπτική άποψη. Δυνητικοί νομικοί κίνδυνοι και κίνδυνοι συμμόρφωσης θα μπορούσαν να προκύψουν από διάφορους παράγοντες, όπως οι αβεβαιότητες γύρω από το εφαρμοστέο δίκαιο, η ασαφής και αβέβαιη νομική αξία των έξυπνων συμβάσεων και η έλλειψη σαφούς ισχύουσας δικαιοδοσίας, καθώς οι κόμβοι DLT θα μπορούσαν να βρίσκονται σε διαφορετικές δικαιοδοσίες των οποίων οι νόμοι ενδέχεται να έρχονται σε σύγκρουση μεταξύ τους. Για παράδειγμα, μια σύμβαση με ψηφιακή υπογραφή ενδέχεται να μην είναι εκτελεστή σε όλες τις δικαιοδοσίες. Είναι σημαντικό να καθοριστεί η εφαρμοστέα δικαιοδοσία, σε περίπτωση σύγκρουσης, και οι μηχανισμοί επίλυσης διαφορών, όταν ανακύπτει διαφορά. Επιπλέον, η πιθανή απουσία κεντρικού μέρους για τη διακυβέρνηση

της πλατφόρμας και την ανάληψη ευθύνης θα μπορούσε να δημιουργήσει πρόσθετες προκλήσεις στη συνολική διακυβέρνηση και διαχείριση του μοντέλου.

Ενδέχεται να προκύψουν πιθανά ζητήματα συμμόρφωσης με τους σχετικούς κανονισμούς, για παράδειγμα σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα, εάν αποκαλυφθούν ευαίσθητες προσωπικές πληροφορίες·σχετικά με τους νόμους περί ανταγωνισμού, ιδίως όταν προσχωρούμε σε κοινοπραξίες ή σε AML/CFT (anti-money laundering/counter terrorist financing). Όσον αφορά ειδικότερα τον κανονισμό AML/CFT, δεδομένου ότι η τεχνολογία αυτή επιτρέπει δυνητικά λιγότερη φυσική ανάλυση της τεκμηρίωσης, η DLT θα μπορούσε να οδηγήσει σε καταχρήσεις για σκοπούς νομιμοποίησης εσόδων από παράνομες δραστηριότητες και χρηματοδότησης της τρομοκρατίας. Η μη συμμόρφωση με αυτούς τους κανονισμούς θα μπορούσε να επιφέρει μεγάλα πρόστιμα, με σημαντικό οικονομικό αντίκτυπο και πιθανές συνέπειες στη φήμη.

Η συνολική διακυβέρνηση του κατανεμημένου καθολικού, όπως ποιος επιτρέπεται να συμμετέχει στο καθολικό και ο ρόλος κάθε συμμετέχοντος, πώς θα προχωρήσει εάν ένα μέλος χάσει το ιδιωτικό του κλειδί ή εάν ή ένα μέλος θα μπορούσε να αποβληθεί από την πλατφόρμα λόγω μη συμμόρφωσης με τους κανόνες που τη διέπουν, θα μπορούσε να δημιουργήσει σημαντικές προκλήσεις για όλα τα συμμετέχοντα ιδρύματα. Η έλλειψη επαρκούς διακυβέρνησης θα μπορούσε να έχει αρνητικό αντίκτυπο που θα οδηγούσε σε λειτουργικούς κινδύνους και κινδύνους φήμης.

Η εξάρτηση από τρίτους θα μπορούσε να αυξηθεί, δεδομένου ότι το DLT και άλλα συστήματα γύρω από την πλατφόρμα θα παρέχονταν γενικά από παρόχους υπηρεσιών ICT (Information and Communications Technology). Κίνδυνος συγκέντρωσης μπορεί επίσης να προκύψει εάν πολλά ιδρύματα βασίζονται στον ίδιο πάροχο, υλοποίηση ή κοινοπραξία, που οδηγούν σε ευρύτερες ανησυχίες, δηλαδή τη δημιουργία ενός πιθανού ενιαίου σημείου αποτυχίας.

Θα μπορούσε να προκύψει πιθανός αντίκτυπος στον κίνδυνο ασφάλειας των ICT, διότι, αν και τα δεδομένα αναπαράγονται σε διαφορετικούς υπολογιστές, υπονομεύοντας τη δυνατότητα τροποποίησης του καθολικού, θα μπορούσε επίσης να συνεπάγεται

περισσότερους κόμβους που χρειάζονται προστασία, ο καθένας με διαφορετικό επίπεδο ασφάλειας. Επιπλέον, τα ποσά που εμπλέκονται στις εμπορικές συναλλαγές θα μπορούσαν να δώσουν κίνητρα για εσωτερική ή εξωτερική απάτη, μεταξύ άλλων και στο επίπεδο του οργανωμένου εγκλήματος.

Ένας εισβολέας θα μπορούσε να εκμεταλλευτεί μια ευπάθεια στον πιο αδύναμο κόμβο για να κλέψει το ιδιωτικό του κλειδί, να πλαστογραφήσει έναν κόμβο ή να αποκτήσει πρόσβαση σε ευαίσθητα δεδομένα προσώπων ή εταιρειών, ειδικά όταν τα δεδομένα αποθηκεύονται σε απλό κείμενο. Ακόμη και στις περιπτώσεις όπου αποθηκεύονται κρυπτογραφημένα δεδομένα, θα μπορούσε να υπάρξει συσχέτιση των συναλλαγών όταν πραγματοποιούνται με τη χρήση του ίδιου δημόσιου κλειδιού. Επιπλέον, όταν τα έξυπνα συμβόλαια πρέπει να στείλουν ή να ανακτήσουν εξωτερικά δεδομένα, βασίζονται σε εξωτερικές υπηρεσίες, οι οποίες θα μπορούσαν επίσης να δεχτούν επίθεση ή να μην είναι διαθέσιμες.

Ο κώδικας υπολογιστή διανέμεται σε όλο το DLT και η διόρθωση ενός σφάλματος σε κάθε κόμβο γίνεται πρόκληση, επηρεάζοντας τον κίνδυνο αλλαγής της ICT. Το να κρατηθούν όλοι οι κόμβοι ενημερωμένοι με την τελευταία έκδοση του λογισμικού και να γίνει έλεγχος των αλλαγών είναι πιο περίπλοκο από ό, τι σε ένα κεντρικό σύστημα.

Ενώ το DLT θεωρείται γενικά πιο ανθεκτικό από τα παραδοσιακά συστήματα χάρη στον διανεμημένο χαρακτήρα του, θα μπορούσε επίσης να δημιουργήσει κινδύνους διαθεσιμότητας και συνέχειας των ICTs, οι οποίοι προκαλούνται από την κακόβουλη κατάρρευση κόμβων ή δικτύων, οι οποίοι θα μπορούσαν να το εμποδίσουν να επικυρώσει και να μοιραστεί συναλλαγές. Επιπλέον, τα λειτουργικά σφάλματα μπορεί να επιδεινωθούν από το γεγονός ότι τα σφάλματα στα δεδομένα ή τον κώδικα υπολογιστή θα μπορούσαν να μεταδοθούν γρήγορα σε ολόκληρο το DLT.

Στο σενάριο όπου οι συναλλαγές εμπορικής χρηματοδότησης τρέχουν μέσω της χρήσης του DLT, τα ιδρύματα θα μπορούσαν να πιεστούν να μειώσουν τις αμοιβές και τις προμήθειες για το συνάλλαγμα, με συνεπώς πιθανό αντίκτυπο στον επιχειρηματικό κίνδυνο. [22, 23]

5.2 Blockchain και GDPR

Παρά το γεγονός ότι η συμβατότητα μεταξύ της τεχνολογίας blockchain και του GDPR μπορεί να προσδιοριστεί επακριβώς μόνο κατά περίπτωση, με βάση αντίστοιχους τεχνικούς και άλλους παράγοντες , η γενική σχέση τους προκειμένου να συνδυαστούν εντός του νομικού πλαισίου, θα παρουσιαστούν ακολούθως.

5.2.1 Εδαφικό πεδίο εφαρμογής

Αν και ο GDPR είναι κομμάτι του δικαίου της ΕΕ, η εφαρμογή του δεν σταματά στα σύνορα της Ευρωπαϊκής Ένωσης. Το άρθρο 3 του GDPR προβλέπει ότι ο GDPR εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα όταν πληρούνται ορισμένες απαιτήσεις. Πρώτον, όταν η επεξεργασία δεδομένων προσωπικού χαρακτήρα πραγματοποιείται «στο πλαίσιο των δραστηριοτήτων εγκατάστασης υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία στην Ένωση, ανεξάρτητα από το αν η επεξεργασία πραγματοποιείται στην Ένωση ή όχι.». Αυτό σημαίνει ότι όταν ένα φυσικό ή νομικό πρόσωπο που χαρακτηρίζεται ως υπεύθυνος επεξεργασίας δεδομένων ή εκτελών την επεξεργασία δεδομένων στο πλαίσιο του GDPR και επεξεργάζεται δεδομένα προσωπικού χαρακτήρα (μέσω blockchains ή άλλων μέσων), το ευρωπαϊκό πλαίσιο προστασίας δεδομένων εφαρμόζεται στην εν λόγω επεξεργασία. Ο κανονισμός εφαρμόζεται επίσης όταν τα δεδομένα προσωπικού χαρακτήρα αφορούν πρόσωπα που έχουν την έδρα τους στην ΕΕ, ακόμη και όταν ο υπεύθυνος επεξεργασίας δεδομένων και ο εκτελών την επεξεργασία δεδομένων δεν είναι εγκατεστημένοι στην Ένωση.

Κατά συνέπεια, υπάρχουν πολλές περιπτώσεις όπου η επεξεργασία δεδομένων προσωπικού χαρακτήρα μέσω blockchains εμπίπτει στο εδαφικό πεδίο εφαρμογής του GDPR. Αυτό συμβαίνει όταν το φυσικό ή νομικό πρόσωπο που είναι υπεύθυνο για την συγκεκριμένη χρήση είναι εγκατεστημένο στην ΕΕ και βασίζονται σε blockchains για την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Ωστόσο, ακόμη και όταν αυτό δεν συμβαίνει, η επεξεργασία δεδομένων προσωπικού χαρακτήρα βάσει distributed ledger θα υπόκειται πολλές φορές στις ευρωπαϊκές απαιτήσεις προστασίας δεδομένων, όπως όταν ένα φυσικό ή νομικό πρόσωπο προσφέρει αγαθά ή υπηρεσίες σε υποκείμενα των δεδομένων στην ΕΕ. Όταν κάποιος που έχει την έδρα του εκτός της ΕΕ και χρησιμοποιεί το blockchain για την επεξεργασία προσωπικών δεδομένα στο πλαίσιο της

παρακολούθησης της συμπεριφοράς των ατόμων με έδρα την ΕΕ, ο κανονισμός ισχύει εξίσου.

Για να καθοριστεί ποια αρχή προστασίας δεδομένων (ΑΠΔ) έχει αρμοδιότητα σε σχέση με μια συγκεκριμένη δραστηριότητα επεξεργασίας, το άρθρο 56 του GDPR προβλέπει ότι είναι αυτή «της κύριας εγκατάστασης (establishment). Όσον αφορά τα ιδιωτικά ή/και τα με έγκριση blockchains, η αρμόδια ΑΠΔ θα προκύψει, από την κύρια εγκατάσταση του υπευθύνου επεξεργασίας δεδομένων, η οποία συνήθως θα είναι το νομικό πρόσωπο που λειτουργεί ή έχει συνάψει πρόσβαση σε συγκεκριμένη υποδομή Distributed Ledger. Για τα δημόσια και ανοικτά blockchain μπορεί να είναι δύσκολο να προσδιοριστεί «η κύρια εγκατάσταση» από τη στιγμή που δεν υπάρχει μία νομική οντότητα που να κυβερνά το συγκεκριμένο έργο. Η ισχύουσα νομολογία υποδηλώνει ότι, υπό τις συνθήκες αυτές, πρέπει να υιοθετηθεί μια λειτουργική προσέγγιση για να καθοριστεί, που ασκήθηκε η σχετική δραστηριότητα για την εν λόγω επεξεργασία.[24]

5.2.2 Υλικό πεδίο εφαρμογής

Σύμφωνα με το άρθρο 2 παράγραφος 1 του GDPR, ο κανονισμός εφαρμόζεται «στην επεξεργασία δεδομένων προσωπικού χαρακτήρα εν όλω ή εν μέρει με αυτοματοποιημένα μέσα και στην επεξεργασία εκτός από αυτοματοποιημένα μέσα, δεδομένων προσωπικού χαρακτήρα που αποτελούν μέρος συστήματος αρχειοθέτησης ή προορίζονται να αποτελέσουν μέρος ενός συστήματος αρχειοθέτησης. Η επεξεργασία δεδομένων μέσω blockchain χαρακτηρίζεται ως επεξεργασία δεδομένων «με αυτοματοποιημένα μέσα».

Όσον αφορά τα blockchains, αυτή η πολύ ευρεία κατανόηση του τι μετράει ως επεξεργασία δεδομένων συνεπάγεται ότι η αρχική προσθήκη προσωπικών δεδομένων σε ένα κατανεμημένο καθολικό, η συνεχής αποθήκευσή του και οποιαδήποτε περαιτέρω επεξεργασία (όπως για οποιαδήποτε μορφή ανάλυσης δεδομένων αλλά και επίτευξη συναίνεσης σχετικά με την τρέχουσα κατάσταση του δικτύου) πιθανότατα συνιστά επεξεργασία δεδομένων προσωπικού χαρακτήρα σύμφωνα με το άρθρο 4 παράγραφος 2 του GDPR.

Υπάρχει, ωστόσο, μια σημαντική εξαίρεση στο ευρύ πεδίο εφαρμογής του GDPR. Όταν η επεξεργασία δεδομένων προσωπικού χαρακτήρα συνιστά αμιγώς ιδιωτική υπόθεση, προστατεύεται από την εφαρμογή του συστήματος προστασίας δεδομένων της ΕΕ.

Σύμφωνα με το άρθρο 2, παράγραφος 2, στοιχείο γ΄, του GDPR, ο κανονισμός δεν εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα από φυσικό πρόσωπο που λαμβάνει χώρα «στο πλαίσιο αμιγώς προσωπικής ή οικιακής δραστηριότητας». Κατά συνέπεια, όταν η επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι αμιγώς προσωπική το δίκαιο της ΕΕ δεν παρεμβαίνει. Η δυσκολία έγκειται στο διαχωρισμό μεταξύ του τι είναι καθαρά προσωπικό και τι όχι.

Ως εκ τούτου, φαίνεται αμφίβολο κατά πόσον η εξαίρεση του νοικοκυριού μπορεί να εφαρμοστεί στην επεξεργασία προσωπικών δεδομένων μέσω blockchains. Πρώτον, η εξάρτηση από ιδιωτικές ή/και με έγκριση βάσεις δεδομένων γενικά συμβαίνει σε ένα πλαίσιο που είναι εμπορικό ή επαγγελματικό και, κατά συνέπεια, υπολείπεται του όρου που αναφέρεται στο άρθρο 2 παράγραφος 2 στοιχείο γ) του GDPR σχετικά με τη φύση της δραστηριότητας (παρόλο που το πεδίο της διάδοσης ελέγχεται όταν χρησιμοποιείται ένα blockchain που απαιτεί έγκριση). Δεύτερον, ένα δημόσιο και χωρίς άδεια blockchain μπορεί να χρησιμοποιηθεί για καθαρά ιδιωτικούς σκοπούς, αλλά εξ ορισμού το πεδίο της διάδοσης των δεδομένων αυτών δεν μπορεί να ελεγχθεί από το υποκείμενο των δεδομένων.

Αξίζει να σημειωθεί ότι ακόμη και όταν ισχύει η απαλλαγή για τα νοικοκυριά, η σχετική επεξεργασία δεδομένων προσωπικού χαρακτήρα δεν εξαιρείται εξ ολοκλήρου από το πεδίο εφαρμογής του GDPR. Σύμφωνα με την αιτιολογική σκέψη (Recital) 18, ο GDPR εφαρμόζεται «στους υπευθύνους επεξεργασίας ή στους εκτελούντες την επεξεργασία που παρέχουν τα μέσα για την επεξεργασία δεδομένων προσωπικού χαρακτήρα για τις εν λόγω προσωπικές ή οικιακές δραστηριότητες».[24]

5.2.3 Προσωπικά και ανώνυμα δεδομένα

Ο κανονισμός διαχωρίζει τα δεδομένα προσωπικού χαρακτήρα με τα μη προσωπικά δεδομένα και έχει εφαρμογή μόνο στα πρώτα. Σύμφωνα με την αιτιολογική σκέψη (Recital) 26 του GDPR, ο κανονισμός πράγματι δεν εφαρμόζεται στα ανώνυμα δεδομένα. Στην πραγματικότητα υπάρχουν δεδομένα που είναι σαφώς προσωπικά, δεδομένα που είναι σαφώς ανώνυμα και αρκετά που είναι κάτι ενδιάμεσο. Τα δεδομένα προσωπικού χαρακτήρα είναι μόνο τα δεδομένα που αφορούν ένα φυσικό πρόσωπο. Ως πλαίσιο θεμελιωδών δικαιωμάτων, ο GDPR δεν εφαρμόζεται συνεπώς στα νομικά πρόσωπα.

Το άρθρο 4 παράγραφος 5 του GDPR που εισάγει την έννοια της ψευδωνυμοποίησης που ορίζεται ως η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα προσωπικού χαρακτήρα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω πρόσθετες πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι τα δεδομένα προσωπικού χαρακτήρα δεν αποδίδονται σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο. Στον GDPR αναφέρεται ρητώς ότι τα ψευδωνυμοποιημένα δεδομένα δεν πρέπει να θεωρούνται ανώνυμα. Πράγματι, ο GDPR ενθαρρύνει ρητά την ψευδωνυμοποίηση ως μέτρο διαχείρισης κινδύνου και μπορεί να θεωρηθεί σαν απόδειξη συμμόρφωσης με το άρθρο 5 και την εξ' ορισμού και εκ σχεδιασμού προστασία των προσωπικών δεδομένων.

Είναι σημαντικό να θυμόμαστε ότι, σύμφωνα με την αιτιολογική σκέψη (Recital) 30, τα υποκείμενα των δεδομένων μπορούν να «συνδέονται με on-line αναγνωριστικά που παρέχονται από τις συσκευές, τις εφαρμογές, τα εργαλεία και τα πρωτόκολλά τους, όπως διευθύνσεις διαδικτυακού πρωτοκόλλου, αναγνωριστικά cookies ή άλλα αναγνωριστικά, όπως ετικέτες αναγνώρισης ραδιο-συχνότητας.» Ενώ τα αναγνωριστικά αυτά στοιχεία έχουν ψευδώνυμο χαρακτήρα, μπορούν, ωστόσο, να επιτρέπουν την έμμεση ταυτοποίηση του υποκειμένου των δεδομένων, καθώς αφήνουν ίχνη τα οποία «ιδίως όταν συνδυάζονται με μοναδικά αναγνωριστικά στοιχεία και άλλα πληροφορίες που λαμβάνονται από τους διακομιστές, μπορούν να χρησιμοποιηθούν για τη δημιουργία προφίλ των φυσικών προσώπων και την αναγνώρισή τους». Τα δημόσια κλειδιά που λειτουργούν ως αναγνωριστικά στα blockchains μπορούν να χαρακτηριστούν ως τέτοιο αναγνωριστικό και ως εκ τούτου χαρακτηρίζονται ως δεδομένα προσωπικού χαρακτήρα.

Το σχετικό κριτήριο για να καθοριστεί αν τα δεδομένα είναι δεδομένα προσωπικού χαρακτήρα είναι το κριτήριο της ταυτοποίησης. Το προοίμιο του GDPR παρέχει επιπλέον κατάλογο στοιχείων που πρέπει να λαμβάνονται υπόψη για τον προσδιορισμό της πιθανότητας ταυτότητας με όλα τα ευλόγως πιθανά να χρησιμοποιηθούν. Σε αυτά περιλαμβάνονται όλοι οι αντικειμενικοί παράγοντες, όπως το κόστος και το χρονικό διάστημα που απαιτείται για την ταυτοποίηση, λαμβάνοντας υπόψη τη διαθέσιμη τεχνολογία κατά τη στιγμή της επεξεργασίας και τις τεχνολογικές εξελίξεις.[24]

5.2.4 Δικαίωμα στη λήθη

Σύμφωνα με την Ομάδα Εργασίας του Άρθρου 29 (Article 29 Working Party), πρέπει να εξεταστούν τρία διαφορετικά κριτήρια για να καθοριστεί αν η αποταυτοποίηση είναι «μη αναστρέψιμη» ή «μόνιμη ως διαγραφή» και συγκεκριμένα αν i) είναι ακόμη δυνατό να ταυτοποιηθεί ένα άτομο, ii) εξακολουθεί να είναι δυνατή η σύνδεση αρχείων σχετικών με ένα άτομο και iii) κατά πόσον οι πληροφορίες που αφορούν ένα άτομο μπορούν ακόμη να προκύψουν. Όταν η απάντηση στα τρία αυτά ερωτήματα είναι αρνητική, τα δεδομένα μπορούν να θεωρηθούν ανώνυμα.

Το ξεδιάλεγμα (singling out) αναφέρεται στη «δυνατότητα απομόνωσης ορισμένων ή όλων των εγγραφών που προσδιορίζουν ένα άτομο στο σύνολο δεδομένων». Η δυνατότητα σύνδεσης (linkability) δηλώνει τον κίνδυνο που δημιουργείται όταν τουλάχιστον δύο σύνολα δεδομένων περιέχουν πληροφορίες σχετικά με το ίδιο υποκείμενο δεδομένων. Τέλος, η εξαγωγή συμπερασμάτων/στοιχείων (inference) είναι η δυνατότητα να συναχθεί, με σημαντική πιθανότητα, η τιμή ενός χαρακτηριστικού από τις τιμές ενός συνόλου άλλων χαρακτηριστικών.

Επιπλέον, η αυξανόμενη πληθώρα δεδομένων διευκολύνει την αποανωνυμοποίηση των δεδομένων μέσω του συνδυασμού διαφορετικών συνόλων δεδομένων. Είναι συχνά εύκολο να εντοπιστούν τα υποκείμενα των δεδομένων βάσει δήθεν ανώνυμων δεδομένων. Τα ψευδώνυμα δεδομένα σε ένα blockchain μπορούν, καταρχήν, να συσχετισθούν με ένα αναγνωρισμένο ή αναγνωρίσιμο φυσικό προσωπικό μέσω του ξεδιαλέγματος, της εξαγωγής συμπερασμάτων ή της συνάφειας.

Τα blockchains είναι λογιστικά βιβλία μόνο για εισαγωγή εγγραφών από τα οποία τα δεδομένα δεν μπορούν εύκολα να διαγραφούν μετά την προσθήκη τους. Μπορεί να υπάρχουν περιπτώσεις χρήσης blockchain που απαιτούν το καθολικό να χρησιμοποιείται μόνο για ένα συγκεκριμένο χρονικό διάστημα, όπως ένα οικονομικό έτος. Στην περίπτωση αυτή, οι τεχνικές εξελίξεις θα πρέπει να αξιολογούνται μόνο για το εν λόγω χρονικό διάστημα. Ωστόσο, άλλες περιπτώσεις χρήσης blockchain βασίζονται στην υπόθεση ότι η υποδομή θα χρησιμεύσει ως ένα διαρκές αρχείο των συναλλαγών, πράγμα που σημαίνει ότι η προβλεπόμενη χρονική περίοδος χρήσης είναι αόριστη. Είναι, ωστόσο, αδύνατο να προβλεφθούν εξελίξεις στην επεξεργασία και ανάλυση δεδομένων μέχρι το τέλος του χρόνου, καθώς αναμφισβήτητα καθίσταται δυνατή κάτι. Συνεπώς, μπορεί να

γίνει το επιχείρημα ότι, όταν προστίθενται δεδομένα σε ένα blockchain που έχει σχεδιαστεί για να χρησιμοποιηθεί για ένα χρονικό πλαίσιο που υπερβαίνει την εύλογη ανάλυση, τα δεδομένα θα πρέπει να θεωρούνται δεδομένα προσωπικού χαρακτήρα, καθώς δεν μπορεί εύλογα να θεωρηθεί ότι η ταυτοποίηση παραμένει απίθανη στο μέλλον.

5.2.5 Προβλήματα εφαρμογής Blockchain σε σχέση με το GDPR

Τα χαρακτηριστικά του Blockchain δεν είναι πάντα συμβατά με τις υποχρεώσεις που απορρέουν από τον GDPR. Για παράδειγμα το πλαίσιο των υποχρεώσεων που απορρέουν από την ιδιωτικότητα εκ σχεδιασμού (άρθρο 25), ο υπεύθυνος επεξεργασίας πρέπει να σκεφτεί εκ των προτέρων την καταλληλόλητα αυτής της τεχνολογίας σε σχέση με τη δυνατότητα επεξεργασίας της. Ένα blockchain δεν είναι απαραίτητα η πιο κατάλληλη τεχνολογία για την επεξεργασία όλων των δεδομένων. Μπορεί να αποτελέσει πηγή δυσκολιών για τους υπευθύνους επεξεργασίας δεδομένων όσον αφορά τη συμμόρφωση με τις υποχρεώσεις που έχει ορίσει ο GDPR. Για παράδειγμα, οι μεταφορές δεδομένων εκτός της Ευρωπαϊκής Ένωσης (ΕΕ) μπορεί να είναι ιδιαίτερα προβληματικές, ιδίως στην περίπτωση των δημόσιων blockchains.

Όπως είναι γνωστό, όλες οι συναλλαγές στο blockchain περιλαμβάνουν: α) αίτημα επικύρωσης της συναλλαγής (και συνεπώς δυνητικά προσωπικών δεδομένων) να αποστέλλεται σε όλους τους miners της αλυσίδας και β) μια ενημέρωση στο blockchain με την οποία προστίθεται ένα νέο μπλοκ στην αλυσίδα για όλους τους συμμετέχοντες. Ωστόσο, είτε πρόκειται για miners ή όχι, οι συμμετέχοντες μπορούν να βρίσκονται σε χώρες εκτός ΕΕ, που δημιουργεί ερωτηματικά με το κατά πόσον ικανοποιείται η υποχρέωση σε σχέση με μεταφορές δεδομένων εκτός ΕΕ.

Ενώ οι κατάλληλες διασφαλίσεις για μια μεταφορά εκτός της ΕΕ μπορούν να χρησιμοποιηθούν σε ένα blockchain που απαιτεί έγκριση, όπως τυποποιημένες συμβατικές ρήτρες, δεσμευτικοί εταιρικοί κανόνες, κώδικες δεοντολογίας ή ακόμη και μηχανισμούς πιστοποίησης, που είναι πιο δύσκολο να εφαρμοστούν σε ένα δημόσιο blockchain, δεδομένου ότι ο υπεύθυνος επεξεργασίας δεδομένων δεν έχει κανέναν έλεγχο πάνω στη θέση των miners.

Ακόμα ένα από τα χαρακτηριστικά των blockchains είναι ότι τα δεδομένα που καταχωρούνται σε αυτά δεν μπορούν να τροποποιηθούν ή να διαγραφούν τεχνικά. Μόλις

ένα μπλοκ στο οποίο καταγράφεται μια συναλλαγή έχει γίνει αποδεκτό από την πλειοψηφία των συμμετεχόντων, η συναλλαγή αυτή δεν μπορεί πλέον να τροποποιηθεί στην πράξη.

Όπως είναι γνωστό κάθε συμμετέχων στο blockchain έχει ένα αναγνωριστικό που αποτελείται από μια σειρά αλφαριθμητικών χαρακτήρων που φαίνονται τυχαίοι και οι οποίοι αποτελούν το δημόσιο κλειδί για το λογαριασμό του συμμετέχοντα. Αυτό το δημόσιο κλειδί συνδέεται με ένα ιδιωτικό κλειδί, γνωστό μόνο από τον συμμετέχοντα. Η ίδια η αρχιτεκτονική των blockchains σημαίνει ότι αυτά τα αναγνωριστικά είναι πάντα ορατά, καθώς είναι απαραίτητα για τη σωστή λειτουργία του. Εκτός από τα αναγνωριστικά των συμμετεχόντων, τα πρόσθετα δεδομένα που αποθηκεύονται στο blockchain μπορεί να περιέχουν προσωπικά δεδομένα, τα οποία μπορούν δυνητικά να σχετίζονται με άτομα εκτός των συμμετεχόντων και των miners, πράγμα που έρχεται σε αντίθεση με το άρθρο 25 του GDRP.

Σύμφωνα με το CNIL (Commission nationale de l'informatique et des libertés) τα προσωπικά δεδομένα θα πρέπει να καταχωρούνται στο blockchain κατά προτίμηση με τη μορφή μιας «δέσμευσης» (commitment scheme), που είναι ένας κρυπτογραφικός μηχανισμός που επιτρέπει το «πάγωμα» των δεδομένων με ένα τρόπο που να είναι ταυτόχρονα δυνατό να αποδειχθεί ότι είναι παγωμένα και αδύνατο να βρεθούν ή αναγνωριστούν με τη χρήση αυτής της δέσμευσης. Εάν αυτό δεν είναι δυνατό, μπορεί κανείς να καταχωρήσει τα δεδομένα με τη μορφή hash που δημιουργείται με τη χρήση συνάρτησης κατακερματισμού (hash) με κλειδί ή, τουλάχιστον, με μια μορφή κρυπτογράφησης που να εξασφαλίζει υψηλό επίπεδο εμπιστευτικότητας.

Εάν δικαιολογείται από τον σκοπό της επεξεργασίας και εάν μια εκτίμηση επιπτώσεων στην προστασία των δεδομένων (data protection impact assesment, DPIA) έχει αποδείξει ότι οι εναπομένοντες κίνδυνοι είναι αποδεκτοί, τα δεδομένα προσωπικού χαρακτήρα μπορούν κατ' εξαίρεση να αποθηκεύονται στο blockchain, χωρίς κρυπτογράφηση.

Σε σχέση με τις απαιτήσεις του GDPR στο blockchain, το δικαίωμα πληροφόρησης των υποκειμένων των δεδομένων δεν είναι προβληματικό. Ο υπεύθυνος επεξεργασίας πρέπει να παρέχει πληροφορίες που να είναι εύκολα προσβάσιμες και να διατυπώνονται με σαφείς όρους στο υποκείμενο των δεδομένων πριν υποβάλει τα δεδομένα προσωπικού χαρακτήρα στους miners για επικύρωση. Το ίδιο ισχύει και για το δικαίωμα πρόσβασης

και το δικαίωμα φορητότητας. Η άσκηση αυτών των δικαιωμάτων είναι συμβατή με τις τεχνικές ιδιότητες των blockchains.

Ταυτόχρονα φαίνεται να είναι τεχνικά αδύνατο να γίνει δεκτό το αίτημα διαγραφής που υποβάλλεται από ένα υποκείμενο δεδομένων όταν τα δεδομένα καταχωρούνται σε ένα blockchain. Ωστόσο, όταν τα δεδομένα που καταγράφονται στο blockchain είναι με τη μορφή «δέσμευσης», ή ενός hash που δημιουργείται από μια λειτουργία hash με κλειδί ή ενός κρυπτοκειμένου που λαμβάνεται μέσω αλγορίθμων και κλειδιών "τελευταίας τεχνολογίας", ο υπεύθυνος επεξεργασίας δεδομένων μπορεί να κάνει τα δεδομένα πρακτικά απρόσιτα και, ως εκ τούτου, να προσεγγίσει το αποτέλεσμα της διαγραφής δεδομένων.

Οι μαθηματικές ιδιότητες ορισμένων συστημάτων «δέσμευσης» μπορούν να εξασφαλίσουν ότι, μετά τη διαγραφή των στοιχείων που επιτρέπουν την επαλήθευσή τους, δεν θα είναι πλέον δυνατό να αποδειχθεί ή να επαληθευτεί ποιες πληροφορίες έχουν «δεσμευτεί». Ως εκ τούτου, η ίδια η «δέσμευση» δεν θα αποτελούσε πλέον κανένα κίνδυνο από την άποψη της εμπιστευτικότητας. Οι πληροφορίες θα πρέπει επίσης να διαγραφούν σε άλλα συστήματα όπου έχουν αποθηκευτεί για επεξεργασία.

Ένα άλλο παράδειγμα είναι η διαγραφή του μυστικού κλειδιού της λειτουργίας hash με κλειδί, το οποίο θα είχε παρόμοια αποτελέσματα. Η απόδειξη ή η επαλήθευση των πληροφοριών που έχουν κατακερματιστεί (γίνει hashed) δεν θα είναι πλέον δυνατή. Στην πράξη, ο κατακερματισμός (hash) δεν θα αποτελούσε πλέον κίνδυνο εμπιστευτικότητας.

Εξαιρουμένης της συγκεκριμένης περίπτωσης ορισμένων συστημάτων «δέσμευσς», οι λύσεις αυτές δεν οδηγούν, με απόλυτο τρόπο, σε διαγραφή των δεδομένων, στο βαθμό που τα δεδομένα εξακολουθούν να υπάρχουν στο blockchain. Παρόλα αυτά επιτρέπουν στα υποκείμενα των δεδομένων να πλησιάσουν περισσότερο σε μια αποτελεσματική άσκηση του δικαιώματός τους περί διαγραφής/λήθης. Θα πρέπει να αξιολογείται κάθε φορά η ισοδυναμία τους σε σχέση με τις απαιτήσεις του GDPR.

Είναι τεχνικά αδύνατο να γίνει δεκτό το αίτημα διόρθωσης ή διαγραφής από ένα υποκείμενο των δεδομένων όταν καταγράφονται μη κρυπτογραφημένα ή κατακερματοποιημένα (hashed) δεδομένα σε ένα blockchain. Ως εκ τούτου, συνιστάται

έντονα να μην καταχωρούνται τα προσωπικά δεδομένα σε μη κρυπτογραφημένο κείμενο σε ένα blockchain.

Όσον αφορά το δικαίωμα διόρθωσης, η αδυναμία τροποποίησης των δεδομένων σε ένα μπλοκ πρέπει να έχει ως αποτέλεσμα ο υπεύθυνος επεξεργασίας δεδομένων να εισάγει τα επικαιροποιημένα δεδομένα σε νέο μπλοκ. Πράγματι, μια μεταγενέστερη συναλλαγή μπορεί να ακυρώσει μια αρχική συναλλαγή, παρόλο που η πρώτη συναλλαγή θα εξακολουθεί να εμφανίζεται στην αλυσίδα. Οι ίδιες λύσεις με εκείνες που εφαρμόζονται μετά από αίτηση διαγραφής δεδομένων προσωπικού χαρακτήρα θα μπορούσαν να εφαρμοστούν σε εσφαλμένα δεδομένα όταν τα δεδομένα αυτά απαιτούν διαγραφή.

Φαίνεται ότι μια αποκλειστικά αυτοματοποιημένη απόφαση που απορρέει από ένα έξυπνο συμβόλαιο είναι αναγκαία για την εκτέλεσή της, δεδομένου ότι επιτρέπει την εκπλήρωση της ίδιας της ουσίας του συμβολαίου (δηλαδή, του λόγου για τον οποίο τα μέρη συνήψαν το συμβόλαιο). Όσον αφορά τα κατάλληλα μέτρα για τη διασφάλιση των δικαιωμάτων και ελευθεριών και των έννομων συμφερόντων του υποκειμένου των δεδομένων, το υποκείμενο των δεδομένων θα πρέπει να είναι σε θέση να αποκτήσει ανθρώπινη παρέμβαση, να εκφράζει την άποψή του και να αμφισβητεί την απόφαση μετά την εκτέλεση της έξυπνης σύμβασης. Ως εκ τούτου, ο υπεύθυνος επεξεργασίας θα πρέπει να παρέχει τη δυνατότητα ανθρώπινης παρέμβασης που θα επιτρέπει στο υποκείμενο των δεδομένων να αμφισβητήσει την απόφαση, ακόμη και αν η σύμβαση έχει ήδη εκτελεστεί, και ανεξάρτητα από το τι έχει καταχωρηθεί στο blockchain. [19]

5.3 Πιθανή χρήση blockchain σε Fintech

Από τα προηγούμενα κεφάλαια είναι προφανείς η μεγάλες δυνατότητες που έχει η τεχνολογία blockchain ή ευρύτερα τα distributed ledger για εφαρμογή σε όλους τους κλάδους της οικονομίας και τις εκφάνσεις της κοινωνικής ζωής. Ειδικότερα όσον αφορά τον χρηματοπιστωτικό κλάδο οι δυνατότητες είναι ανεξάντλητες. Καθημερινά βγαίνουν νέες εφαρμογές/τεχνολογίες που αφορούν DLT,για χρήση σε Fintech επιχειρήσεις ή στον ευρύτερο χρηματοπιστωτικό τομέα. Αυτές μπορεί να είναι είτε ανοικτού κώδικα, είτε εμπορικές, είτε ακαδημαϊκές μέσα από την έρευνα. Η λίστα είναι ανεξάντλητη, για αυτό θα γίνει αναφορά σε μερικές από τις πιο δημοφιλείς και καθιερωμένες.

5.3.1 Bitcoin

Το κύριο κρυπτονόμισμα με βάση την κεφαλαιοποίηση του στην αγορά και η πιο ευρέως γνωστή εφαρμογή της έννοιας blockchain, το Bitcoin λειτουργεί χωρίς καμία κεντρική αρχή από το 2009. Υπάρχουν πλέον πάνω από 15 εκατομμύρια bitcoins, με κεφαλαιοποίηση αγοράς κοντά στα 8δις ευρώ (ανάλογα με την εκάστοτε ισοτιμία).

Το Bitcoin περιέχει μια πολύ βασική γλώσσα scripting, που ονομάζεται Script, που πραγματοποιεί απλά έξυπνα συμβόλαια. Το σενάριο δεν υποστηρίζει βρόχους και λειτουργεί κυρίως ως εργαλείο για την τοποθέτηση παραμέτρων σχετικά με το πώς μπορούν να δαπανηθούν bitcoins μόλις φτάσουν στον προορισμό τους.

Το Bitcoin χρησιμοποιεί ένα κατανεμημένο καθολικό συναλλαγών από το οποίο είναι δυνατό να υπολογιστεί το σύνολο μη αναλωμένων συναλλαγών (Unspent Transaction Output) ή UTxO. Από μια πιο πρακτική πλευρά, αυτό σημαίνει ότι οι διευθύνσεις των πορτοφολιών που εκτίθενται δημόσια (δηλαδή μοναδικά αναγνωριστικά) δεν είναι απλώς συνδέσεις με ένα καθορισμένο ποσό ή περιουσιακό στοιχείο. Αντιθέτως, είναι ο πιο πρόσφατος σύνδεσμος σε μια δημόσια επαληθεύσιμη ιστορική διαδρομή συναλλαγών που τελειώνει σε αυτή τη διεύθυνση.

Ανοικτά δίκτυα όπως το Bitcoin πρέπει να επιτρέπουν έναν απεριόριστο αριθμό συμμετεχόντων. Η πρόκληση που προκύπτει για μεγάλο αριθμό μερών που δεν γνωρίζονται μεταξύ τους και δεν μπορούν να εμπιστευτούν το ένα το άλλο, είναι το να καταλήξουν σε συμφωνία σχετικά με την αλήθεια μιας συγκεκριμένης συναλλαγής. Το Bitcoin λύνει αυτό το πρόβλημα με τη χρήση ενός αλγορίθμου απόδειξης εργασίας. Για να θεωρηθούν έγκυρα τα μηνύματα, πρέπει να συμπιεστούν σε ένα μπλοκ δεδομένων, το οποίο προσαρτάται σε μια υπάρχουσα βάση δεδομένων. Αυτή η έννοια της επικύρωσης ενός συνόλου μηνυμάτων αναφέρεται ως εξόρυξη (mining). Στους miners δίνεται οικονομικό κίνητρο για να συντηρούν το σύστημα. Οι miners που υποβάλλουν επιτυχώς το επόμενο μπλοκ λαμβάνουν μια ανταμοιβή, εκφρασμένη στο κρυπτο-διακριτικό που συνδέεται με το συγκεκριμένο Blockchain.

Για να λειτουργήσει το σύστημα, οι συμμετέχοντες πρέπει να είναι σε θέση να εξακριβώσουν ότι οι πληροφορίες που τους έχουν παρουσιαστεί είναι αληθείς. Επιπλέον, θα πρέπει να υπάρχει αντικίνητρο για ανέντιμους παράγοντες να παραβιάσουν το

σύστημα. Η απόδειξη της λειτουργίας της εργασίας καθιστά απίθανο για δύο μέρη να καταλήξουν σε έγκυρο συμπέρασμα ταυτόχρονα. Ωστόσο, παραμένει μια πιθανότητα. Όταν συμβεί αυτό, μπορεί να αναπτυχθεί μία διχάλα στο Blockchain με δύο ξεχωριστές αλυσίδες να αναπτύσσονται. Για να σταματήσουν και για να εξασφαλιστεί ότι υπάρχει μόνο μία αλυσίδα, οι πελάτες δέχονται τη μεγαλύτερη αλυσίδα πάνω από όλες τις άλλες.

Το ζήτημα που προκύπτει με ένα κατανεμημένο καθολικό το να εγγυηθεί ότι, καθώς το σύνολο δεδομένων εξελίσσεται με την πάροδο του χρόνου, τα παλαιότερα δεδομένα δεν υπόκεινται σε τροποποίηση. Για να αποφευχθεί αυτό, όλα τα προηγούμενα μπλοκ στο σύστημα περιλαμβάνονται στο hash για το πιο πρόσφατο μπλοκ. Αυτό αναφέρεται ως απόδειξη Merkle. Η εφαρμογή Bitcoin διαθέτει μια αλυσίδα μπλοκ. Κάθε μπλοκ περιέχει μια κεφαλίδα μπλοκ με 6 στοιχεία:

Έκδοση μπλοκ - Καθορίζει την έκδοση του Blockchain για την οποία δημιουργείται το λογισμικό εξόρυξης.

Hash της κεφαλίδας του προηγούμενου μπλοκ - Μια κατακερματισμένη έκδοση της προηγούμενης κεφαλίδας μπλοκ.

Hash του Merkle Root (Συναλλαγές σε μπλοκ) – Ένα hash όλων των συναλλαγών/μηνυμάτων στο τρέχον μπλοκ.

Χρονική σήμανση - Ο χρόνος δημοσίευσης του μπλοκ.

Bits - Ένας αριθμός 256-bit που λειτουργεί ως στόχος για τους miners να παράγουν ένα hash κάτω από την τιμή του, προκειμένου να δημιουργηθεί ένα έγκυρο μπλοκ.

Nonce - Ένας τυχαίος αριθμός που επιτρέπει διαφορετικά αποτελέσματα hash για ένα μπλοκ σε κάθε προσπάθεια.

Προκειμένου να παραχθεί ένα μπλοκ, οι miners επιλέγουν ένα σύνολο συναλλαγών για να επικυρώσουν και να τους κάνουν hash χρησιμοποιώντας έναν αλγόριθμο SHA-256. Εάν το hash που προκύπτει είναι μικρότερος αριθμός από τα Bit, τότε θεωρείται έγκυρη λύση και μεταδίδεται στο υπόλοιπο δίκτυο. Εάν δεν είναι, το nonce αλλάζει για κάθε τρέξιμο του hash μέχρι να βρεθεί ένα αποτέλεσμα με χαμηλότερη τιμή από τα bits.

Ο αλγόριθμος που χρησιμοποιείται για την απόδειξη της εργασίας απαιτεί από την οντότητα που εκτελεί τον υπολογισμό να συνεισφέρει υπολογιστική ισχύ. Η πιθανότητα υποβολής της έγκυρης λύσης σε ένα μπλοκ είναι ανάλογη με τη συνολική ποσότητα υπολογιστικής ισχύος που συνεισφέρει ο χρήστης κατά τη διάρκεια του χρονικού παραθύρου που είναι απαραίτητο για την εύρεση του πιο πρόσφατου έγκυρου μπλοκ.. Ωστόσο, ένα από τα κύρια ελαττώματά του έγκειται στο γεγονός ότι καταναλώνει μεγάλη ποσότητα ενέργειας. Η πρώτη ακούσια συνέπεια είναι ότι αυτό δημιουργεί μια ώθηση προς την υπερσυγκέντρωση/κεντροποίηση της ικανότητας εξόρυξης λόγω των οικονομιών κλίμακας που πρέπει να επιτευχθούν στον τομέα του υλικού και ηλεκτρικής ενέργειας.[24]

5.3.2 Ethereum

Το Ethereum ιδρύθηκε το 2013 και ξεκίνησε το 2015 μετά από μια επιτυχημένη καμπάνια crowdfunding που συγκέντρωσε πάνω από 18 εκατομμύρια δολάρια σε Bitcoin. Μέχρι σήμερα υπάρχουν πάνω από 80 εκατ. Ether σε κυκλοφορία με κεφαλαιοποίηση πάνω από 1 δις ευρώ.

Το Ethereum προσφέρει το ίδιο φάσμα υπολογιστικών ικανοτήτων με τα υπάρχοντα συστήματα του πραγματικού κόσμου, και ιδίως με βρόχους υποστήριξης και τις υπό όρους δηλώσεις. Ο εγγενής σχεδιασμός του συστήματος σημαίνει ότι ο κώδικας των έξυπνων συμβολαίων και η εκτέλεσή του είναι ανοικτά για επανεξέταση από όλα τα μέρη. Το Ether είναι ένας τρόπος πληρωμής που γίνεται από τους πελάτες της πλατφόρμας προς τα μηχανήματα εκτέλεσης των ζητούμενων εργασιών.

Έχουν αναπτυχθεί διάφορες γλώσσες για την υποστήριξη των έξυπνων συμβολαίων. Η εικονική μηχανή του Ethereum τρέχει σε byte κώδικα, η οποία μπορεί τώρα να συνταχθεί από πολλές παραδοσιακές γλώσσες, συμπεριλαμβανομένων Javascript και C++. Η Solidity είναι μια νέα γλώσσα υψηλού επιπέδου που αναπτύχθηκε ειδικά για τα συμβόλαια του Ethereum, είναι παρόμοια με javascript, σχεδιάστηκε με στόχο να κάνει πολύπλοκα έξυπνα συμβόλαια όσο το δυνατόν πιο εύκολο να γραφτούν.

Ενώ τα μπλοκ του Bitcoin περιέχουν μηνύματα συναλλαγών, τα μπλοκ του Ethereum περιέχουν μηνύματα που αντιπροσωπεύουν υπολογιστικά βήματα της εκτέλεσης ενός έξυπνου συμβολαίου. Ο υπολογισμός αυτός χρηματοδοτείται από υπομονάδες αιθέρα,

που συνήθως αναφέρονται ως "αέριο". Όλα τα τέλη εκτέλεσης καταβάλλονται από την οντότητα που εκδίδει την οδηγία και περιλαμβάνονται στις ανταμοιβές εξόρυξης για το συγκεκριμένο μπλοκ. Τα μπλοκ στην αλυσίδα Ethereum επικυρώνονται επί του παρόντος και με τη χρήση ενός αλγορίθμου απόδειξης εργασίας. Ωστόσο, βρίσκεται στη διαδικασία μετάβασης σε αλγόριθμο τύπου Proof of Stake.[24]

5.3.3 Ripple

Ήδη χρησιμοποιείται από διάφορα χρηματοπιστωτικά ιδρύματα. Το Ripple παρέχει ένα peer to peer σύστημα για τις τράπεζες σε αγορές συναλλάγματος (FX) για να συναλλάσσονται μεταξύ τους. Το παγκόσμιο καθολικό αναπαράγεται από χιλιάδες συμμετέχοντες. Οι συναλλαγές FX πραγματοποιούνται μέσω ενός κατανεμημένου βιβλίου παραγγελιών, όπου όλες οι προσφορές και οι απαιτήσεις καταγράφονται και εκτελούνται. Το Ripple βασίζεται στην έννοια των "πυλών" (gateways). Ως εκ τούτου, για να μετακινήσει ένας χρήστης το υπόλοιπο του fiat (δηλαδή τα υπόλοιπα λογαριασμών που εκφράζονται σε νομίσματα που εκδίδονται από το κράτος, όπως EUR, GBP κ.λπ.) έξω από το δίκτυο Ripple, θα πρέπει να ζητήσει διακανονισμό από την οντότητα που εξέδωσε αρχικά το υπόλοιπο αυτό στο δίκτυο. Ως εκ τούτου, το Ripple εξακολουθεί να περιέχει ένα βαθμό κινδύνου αντισυμβαλλομένου, μια και οι χρήστες υποχρεούνται να εμπιστεύονται ότι θα είναι σε θέση να λάβουν μια αποτελεσματική διευθέτηση των κεφαλαίων τους.[24]

5.3.4 Hyperledger

Η μεγάλη ποικιλία των εφαρμογών για την τεχνολογία κατανεμημένου καθολικού σημαίνει επίσης ότι υπάρχει μεγάλες των δυνατότητες βελτιστοποίησης που μπορεί να γίνουν, μια και ορισμένα πρωτόκολλα μπορεί να είναι πιο κατάλληλα για ορισμένες περιπτώσεις, ανάλογα με το ποιος τα κατασκευάζει και για ποιον λόγο. Η αναγνώριση αυτού του δεδομένου έχει οδηγήσει στην ανάπτυξη του Hyperledger, το οποίο αναπτύσσεται από μια κοινοπραξία χρηματοπιστωτικών επιχειρήσεων και τεχνολογίας, όπου ηγείται το ίδρυμα Linux. Το Hyperledger επικεντρώνεται στην ανάπτυξη ενός προτύπου για κατανεμημένα λογιστικά βιβλία που θα επιτρέψει ξεχωριστά λογιστικά

βιβλία για να επικοινωνούν μεταξύ τους χωρίς να χρειάζεται κατά παραγγελία API. Από την άποψη της ασφάλειας, το Hyperledger χρησιμοποιεί δύο τύπους πιστοποιητικών:

- Πιστοποιητικά εγγραφής: Ελέγχει την πρόσβαση των συμμετεχόντων στο δίκτυο

- Πιστοποιητικά συναλλαγών μίας χρήσης: Περιορίζει τη δυνατότητα προώθησης ανεπιθύμητων συναλλαγών.

Το Hyperledger αναφέρεται σε αυτό το κοινό πρότυπο το Fabric, και σχεδιάστηκε ώστε τα έξυπνα συμβόλαια να είναι εγγράψιμα σε αυτή την πλατφόρμα σε οποιαδήποτε κοινή γλώσσα προγραμματισμού. Ο στόχος είναι να παραχθεί ένα εντελώς αρθρωτό σύστημα που θα επιτρέπει τα πάντα - από την κρυπτογραφία που χρησιμοποιείται μέχρι το υποκείμενο πρωτόκολλο συναίνεσης - να είναι εύκολα παραμετροποιήσιμα και να αναπτύσσονται με όσο το δυνατόν λιγότερη προσπάθεια. Ο βασικός παράγοντας της σπονδυλωτής προσέγγισης του Hyperledger είναι να επιτρέψει στις επιχειρήσεις που συμμετέχουν να καθορίσουν το πρωτόκολλο συναίνεσης που θα χρησιμοποιήσουν, ακολουθώντας τις επιχειρηματικές τους ανάγκες.[24]

5.3.5 Corda

Η Corda είναι ένα κατανεμημένο καθολικό για συμβάσεις προσαρμοσμένες για χρήση από χρηματοπιστωτικά ιδρύματα. Επανεξετάζει μια σειρά από τα υποτιθέμενα απαιτούμενα συστατικά του σχεδιασμού τους. Οι συναλλαγές/συμφωνίες είναι ορατές μόνο στα μέρη που πρέπει να τις δουν, συμπεριλαμβανομένης μιας καθορισμένης ρυθμιστικής αρχής. Σε αυτό το πλαίσιο, η ρυθμιστική αρχή θα μπορούσε να είναι μια αρχή όπως η Ευρωπαϊκή Αρχή Τραπεζών (ΕΒΑ) ή ένας φορέας του κλάδου που καθορίζει ένα σύνολο προτύπων που οι συμμετέχοντες στην αγορά υποχρεούνται να τηρούν. Το Corda δεν έχει κρυπτονόμισμα, καθώς μόνο τα μέρη που μετέχουν είναι επίσης οι επικυρωτές της συμφωνίας που λαμβάνει χώρα, με πολλαπλούς μηχανισμούς συναίνεσης που εν δυνάμει μπορούν να χρησιμοποιηθούν.

Η Corda έχει ως στόχο να παρέχει ένα παγκόσμιο κατανεμημένο καθολικό, όπου οι συναλλαγές χρησιμεύουν ως έγκυρα και δεσμευτικά γεγονότα για την αποδέσμευση συμβατικών υποχρεώσεων στους αντισυμβαλλομένους. Για το σκοπό αυτό, η συμπεριφορά του συστήματος σχεδιάζεται σε κώδικα και υποστηρίζεται από νομικό

πλαίσιο που περιγράφει τις υποχρεώσεις των συμμετεχόντων. Η Corda έχει σχεδιαστεί για να επιτρέπει ορισμένες χρηματοπιστωτικές συναλλαγές, συμπεριλαμβανομένης της δυνατότητας των χρηματοπιστωτικών ιδρυμάτων να εκδίδουν ψηφιακό νόμισμα fiat σε αντισυμβαλλομένους. Με τη σειρά τους, αυτά τα κεφάλαια που βασίζονται στο Blockchain μπορούν να χρησιμοποιηθούν για συναλλαγές και διακανονισμούς. [24, 25]

Είναι ένα παγκόσμιο δίκτυο με κάποιες αξιοσημείωτες διαφορές από το ανοικτό δημόσιο blockchain:

- Η πρόσβαση στο δίκτυο του Corda απαιτεί άδεια.

- Οι πληροφορίες συναλλαγών σχετικά με τις ροές στο Corda είναι από σημείο σε σημείο, και η συναίνεση βασίζεται στην επικύρωση των συναλλαγών από συμμετέχοντες στο δίκτυο που ονομάζονται συμβολαιογράφοι, αποφεύγοντας έτσι την "Απόδειξη της εργασίας" (Proof of Work), ή εμποδίζοντας το “mining”, που χρησιμοποιούνται στα αρχικά blockchains.

- Πρόκειται για ένα έργο ανοικτού κώδικα, όπου ο καθένας μπορεί να κάνει ένα επιχειρηματικό δίκτυο και να εφαρμόσει το δικό του σχεδιασμό, αναλαμβάνοντας την ευθύνη για τη συμμόρφωση του GDPR.

Για να διευκολυνθεί η εφαρμογή της πλατφόρμας, οι προγραμματιστές της Corda έχουν αναπτύξει το Δίκτυο Corda — ένα δημόσιο δίκτυο κόμβων που λειτουργεί/ελέγχεται από τους συμμετέχοντες στο δίκτυο. Προορίζεται να υποστηρίξει πολλά υποδίκτυα κόμβων, με τα δικά τους συντονιστικά μέρη και κανόνες για την συμμετοχή και τη χρήση. Όπως και το Διαδίκτυο, το δίκτυο Corda παρέχει τις υπηρεσίες ραχοκοκαλιάς για τη διασυνδεσιμότητα και υψηλής ταχύτητας ροή συναλλαγών.

Οι υπηρεσίες δικτύου της Corda έχουν σχεδιαστεί για να συμμορφώνονται με την ιδιωτικότητα των δεδομένων και τον GDPR:

- Η **υπηρεσία Doorman** (Doorman service) συλλέγει πληροφορίες από χρήστες και φορείς που συμμετέχουν στο επιχειρηματικό δίκτυο, συμπεριλαμβανομένων προσωπικών δεδομένων, όπως όνομα επαφής, αριθμό τηλεφώνου ή διεύθυνση ηλεκτρονικού ταχυδρομείου. Τα δεδομένα αποθηκεύονται σε μια ιδιωτική, ασφαλή

βάση δεδομένων και δεν μεταδίδονται στο δίκτυο. Εάν ένα μέρος βγει εκτός του δικτύου, τα προσωπικά δεδομένα που του ανήκουν θα διαγραφούν, με την επιφύλαξη των κανόνων κράτησης αρχείων και υπό την προϋπόθεση ότι δεν υπάρχει επιχειρηματικός λόγος για την αποθήκευσή τους. Με τη θέσπιση αυτής της διαδικασίας, το Corda συμμορφώνεται με την απαίτηση του GDPR για το «Δικαίωμα στη λήθη» του υποκειμένου των δεδομένων και της διαγραφής δεδομένων.

- Η **υπηρεσία χάρτη δικτύου** (Network Map Service) επιτρέπει στους συμμετέχοντες να βρίσκουν και να επικοινωνούν μεταξύ τους μέσω του δικτύου. Δεν κοινοποιούνται προσωπικά δεδομένα στους συμμετέχοντες στο δίκτυο ως μέρος αυτής της υπηρεσίας.

- Η **συμβολαιογραφική υπηρεσία** (Notary Service) παρέχει τη συναίνεση του δικτύου και εγγυάται τη μοναδικότητα και την οριστικότητα κάθε συναλλαγής. Προς το παρόν, το Corda Network Foundation παρέχει μόνο μη επικυρωμένους συμβολαιογράφους που βλέπουν μόνο ένα υποσύνολο μιας συναλλαγής για να προσδιορίσουν την παραγγελία και τη μοναδικότητά της. Δεν υποβάλλονται σε επεξεργασία ή αποθηκεύονται προσωπικά δεδομένα από την υπηρεσία αυτή.

Η Corda έχει ένα σύνολο διαδικασιών σε περίπτωση παραβίασης δεδομένων:

1. Ο χειριστής του Corda Network Foundation ενημερώνει τα επηρεαζόμενα μέρη σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα εντός 72 ωρών από την ώρα που έγινε αντιληπτή η παραβίαση.

2. Μια εποπτική αρχή ενημερώνεται εάν υπάρχει κίνδυνος για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.

3. Ο χειριστής θα ειδοποιήσει το Συμβούλιο του Corda Network Foundation άμεσα.[25]

Τα δίκτυα Corda είναι με έγκριση. Κάθε μέρος στο δίκτυο έχει μια γνωστή ταυτότητα που χρησιμοποιούν κατά την επικοινωνία με τους αντισυμβαλλομένους, και η πρόσβαση στο δίκτυο ελέγχεται από έναν «θυρωρό». Αυτό έχει αρκετά οφέλη όπως:

- Οι ανώνυμοι συμμετέχοντες είναι ακατάλληλοι για τα περισσότερα σενάρια που αφορούν ρυθμιζόμενα χρηματοπιστωτικά ιδρύματα.

- Η γνώση της ταυτότητας των αντισυμβαλλομένων σας επιτρέπει την επίλυση διενέξεων εκτός καθολικού με τη χρήση υπαρχόντων νομικών συστημάτων.

- Οι επιθέσεις Σίμπιλ (sybil attack: δημιουργία πληθώρας ψεύτικων ταυτοτήτων για να αποκτήσεις αυξημένη επιρροή σε ένα δίκτυο) αποτρέπονται χωρίς τη χρήση δαπανηρών μηχανισμών, όπως η απόδειξη της εργασίας (Proof of Work)

Στο Corda, κάθε μήνυμα απευθύνεται σε συγκεκριμένο αντισυμβαλλόμενο και δεν φαίνεται από κανένα τρίτο μέρος που δεν εμπλέκεται. Ο προγραμματιστής έχει τον πλήρη έλεγχο των μηνυμάτων που αποστέλλονται, σε ποιον και με ποια σειρά. Ως αποτέλεσμα, τα δεδομένα κοινοποιούνται μόνο σε need-to-know βάση. Για να αποτρέψουμε τις διπλές δαπάνες σε αυτό το σύστημα, απασχολούμε «συμβολαιογράφους» ως εναλλακτική λύση στην απόδειξη της εργασίας.

Το Corda χρησιμοποιεί επίσης πολλές άλλες τεχνικές για τη μεγιστοποίηση της ιδιωτικότητας στο δίκτυο:

Αποκρυπτογραφήσεις συναλλαγών: Οι συναλλαγές είναι δομημένες με τρόπο που τους επιτρέπει να υπογράφονται ψηφιακά χωρίς να αποκαλύπτουν τα περιεχόμενα της συναλλαγής. Αυτό επιτυγχάνεται χρησιμοποιώντας μια δομή δεδομένων που ονομάζεται Δέντρο Merkle.

Τυχαιοποίηση κλειδιού: Τα μέρη μιας συναλλαγής αναγνωρίζονται μόνο από τα δημόσια κλειδιά τους και δημιουργούνται νέα ζεύγη κλειδιών για κάθε συναλλαγή. Ως εκ τούτου, ένας θεατής δεν μπορεί να προσδιορίσει ποια μέρη συμμετείχαν σε μια δεδομένη συναλλαγή.

Το Corda χρησιμοποιεί ένα μοντέλο UTXO (έξοδος μη αναλωμένων συναλλαγών). Κάθε συναλλαγή καταναλώνει ένα σύνολο υπαρχουσών καταστάσεων για την παραγωγή ενός συνόλου νέων καταστάσεων. Το κύριο πλεονέκτημα του μοντέλου UTXO είναι ότι οι συναλλαγές με διαφορετικές εισροές μπορούν να εφαρμοστούν παράλληλα, αυξάνοντας κατά πολύ τις πιθανές συναλλαγές του δικτύου ανά δευτερόλεπτο. Στο μοντέλο τύπου

λογαριασμού, ο αριθμός των συναλλαγών ανά δευτερόλεπτο περιορίζεται από το γεγονός ότι οι ενημερώσεις σε ένα συγκεκριμένο αντικείμενο πρέπει να εφαρμόζονται διαδοχικά.

Τα χρηματοπιστωτικά ιδρύματα χρειάζονται τη δυνατότητα επίλυσης διαφορών χρησιμοποιώντας το παραδοσιακό νομικό σύστημα, όπου απαιτείται. Το Corda έχει σχεδιαστεί για να το καταστήσει αυτό δυνατό με το να:

- Έχει δικαιώματα δικτύων, πράγμα που σημαίνει ότι οι συμμετέχοντες γνωρίζουν με ποιον συναλλάσσονται σε κάθε συναλλαγή.

- Όλα τα συμβόλαια φτιαγμένα με κώδικα θα πρέπει να περιλαμβάνουν μια σύνδεση LegalProseReference με το νομικό έγγραφο που περιγράφει την προβλεπόμενη συμπεριφορά της σύμβασης, η οποία μπορεί να προβληθεί για την επίλυση διενέξεων

Όπου είναι δυνατόν, η Corda επαναχρησιμοποιεί τις υπάρχουσες τεχνολογίες για να κάνει την πλατφόρμα πιο ισχυρή συνολικά. Για παράδειγμα, η Corda επαναχρησιμοποιεί Java, SQL και υπάρχουσες υλοποιήσεις ουράς μηνυμάτων.[25]

5.3.6 Κενά ασφαλείας

Για να αποκομίσουν τα οφέλη της τεχνολογίας blockchain, οι εταιρείες πρέπει να εισαγάγουν νέες εφαρμογές λογισμικού καθώς και νέα υποδομή πληροφορικής, όπως, διακομιστές, βάσεις δεδομένων, συνδέσεις δικτύου κ.λπ. Και εδώ είναι που μπορούν να εμφανιστούν κίνδυνοι.

Οι έξυπνες συμβάσεις (smart contracts) είναι σύνολα επιχειρηματικής λογικής που υλοποιούνται με τη μορφή προγραμματισμού. Οι έξυπνες συμβάσεις «ενεργοποιούν» μια επιχειρηματική συναλλαγή εάν πληρούνται οι απαιτούμενες επιχειρηματικές προϋποθέσεις (καταγράφονται επίσης στο blockchain). Για παράδειγμα, τα μέρη μπορούν να συμφωνήσουν σχετικά με την παράδοση αγαθών και υπηρεσιών ή συγκεκριμένους όρους βάσει των οποίων τα κεφάλαια μπορούν να αποδεσμευθούν αυτόματα ή να επιβληθούν χρεώσεις ποινής. Οι έξυπνες συμβάσεις πρέπει να λειτουργούν ως τεκμηριωμένες, να συμπεριφέρονται ντετερμινιστικά και να μην περιέχουν αδήλωτες λειτουργίες.

Υπάρχουν ειδικές πτυχές του blockchain για την ανάπτυξη τόσο των εφαρμογών όσο και των έξυπνων συμβάσεων που πρέπει να λάβει υπόψη ένας προγραμματιστής, και οι οποίες μπορεί επίσης να υπόκεινται σε κακόβουλους χειρισμούς.

Οι χρηματοοικονομικοί οργανισμοί βλέπουν το DLT ως μέσο μείωσης του κόστους συναλλαγών, απόκτησης πελατών που υποστηρίζονται από κρυπτογράφηση και της βελτίωσης της διαφάνειας και της δυνατότητας ελέγχου. Επιδιώκουν ενεργά την έρευνα και ανάπτυξη του τομέα και προσπαθούν να μεγιστοποιήσουν τα οφέλη της χρήσης του blockchain. Στην επιθυμία να εκμεταλλευτούν όσο το δυνατόν περισσότερο την τεχνολογία, είναι ζωτικής σημασίας να εφαρμοστεί κάθε κομμάτι του οικοσυστήματος με ασφαλή τρόπο. Μερικά από τα προβλήματα ασφαλείας που συναντούμε είναι:

α. Λάθη στον κώδικα των έξυπνων συμβολαίων μπορούν να οδηγήσουν σε μη ντετερμινιστική συμπεριφορά των κόμβων και σε πλήρη απαξίωση των δεδομένων.

β. Ελαττώματα ασφαλείας στην υποδομή δικτύου μπορούν να αξιοποιηθούν από προηγμένες επίμονες απειλές προκειμένου να αντλήσουν ευαίσθητα εμπορικά δεδομένα

γ. Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα μέσω των εφαρμογών blockchain μπορεί να οδηγήσει σε χειραγώγηση δεδομένων και να θέσει σε κίνδυνο διάφορες οντότητες.

δ. Η μη ντετερμινιστική συμπεριφορά των έξυπνων συμβάσεων παράγει ασυνεπή αποτελέσματα στην επιχειρηματική διαδικασία.

ε. Τα ελαττώματα ασφαλείας σε τερματικές συσκευές που μπορούν να καταστήσουν ευάλωτα σε επιθέσεις τα εταιρικά δίκτυα των συμμετεχόντων μερών.

στ. Ανεπαρκής έλεγχος ταυτότητας χρήστη σε εφαρμογές blockchain μπορεί να οδηγήσει σε μη εξουσιοδοτημένες οικονομικές συναλλαγές.

ζ. Λάθος ή κακόβουλοι χειρισμοί στον κώδικα μπορεί να προκαλέσουν ασυνάρτητη συμπεριφορά κόμβων και απρόβλεπτα αποτελέσματα, ενώ η εσφαλμένη ρύθμιση παραμέτρων μπορεί να οδηγήσει σε χειραγώγηση δεδομένων και μη εγκεκριμένες συναλλαγές.

Το μεγαλύτερο ζήτημα με τις διαδικασίες που βασίζονται στο blockchain είναι ότι μόλις ξεκινήσουν, είναι πολύ δύσκολο να τροποποιηθούν εάν υπάρχουν λειτουργικά προβλήματα. Γι' αυτό είναι εξαιρετικά σημαντικό να δοκιμαστεί πλήρως η λύση blockchain πριν την εφαρμογή.

Πολύ γνωστή περίπτωση αποτελεί το Ethereum DAO hack που είναι ένα παράδειγμα του τρόπου με τον οποίο οι συμμετέχοντες σε ένα κατανεμημένο καθολικό μπορούν, με συναίνεση, να ξεπεράσουν σημαντικά γεγονότα ασφαλείας. Ωστόσο, αυτό εισάγει επίσης τη δυνατότητα επαναφοράς των συναλλαγών του παρελθόντος, ένα ζήτημα που θα σήμαινε ότι οι συμμετέχοντες που συναλλάσσονται μετά την επίθεση θα δουν τις συναλλαγές τους ουσιαστικά να έχουν ακυρωθεί. Αυτό έχει οδηγήσει στο διαχωρισμό του Ethereum σε 2 μέρη όπου το αποκαλούμενο "EthereumClassic" δεν αναγνωρίζει την αναστροφή της επίθεσης που έγινε ως έγκυρη.

Επίσης ο ανοικτός τρόπος με τον οποίο λειτουργεί το δίκτυο Ripple επέτρεψε, την ανάπτυξη τρωτών σημείων. Ερευνητές στο Πανεπιστήμιο Purdue έχουν διαπιστώσει ότι, αν και ο πυρήνας του δικτύου παραμένει εξαιρετικά ρευστός, η δομή επιτρέπει επιθέσεις σε ορισμένους κόμβους εντός του δικτύου που δύναται να ακρωτηριάσουν την πρόσβαση ορισμένων χρηστών στα κεφάλαια τους. Στην πραγματικότητα, περίπου 50.000 ψηφιακά πορτοφόλια μπορεί να είναι σε άμεσο κίνδυνο, αν μια τέτοια επίθεση επρόκειτο να συμβεί [35].

Το Bitcoin λόγω της οικονομικής σημασίας που έχει αποτελεί μεγαλύτερο στόχο και έχουν βρεθεί κάποια κενά ασφαλείας που το αφορούν άμεσα ή έμμεσα. Τα σημαντικότερα είναι τα ευάλωτα ψηφιακά πορτοφόλια, η ταυτόχρονη επίθεση χάκερ σε μεγάλα ανταλλακτήρια, οι επιθέσεις Distributed Denial of Service (DDoS), οι συντονισμένες επιθέσεις με στόχο το double spending (διπλή χρέωση) και επιθέσεις τύπου 51% όπου όταν κάποιος ελέγχει μεγάλο κομμάτι των miners μπορεί να δράσει συντονισμένα και να χειραγωγήσει συναλλαγές. Αυτά τα κενά ασφαλείας και η όσο το δυνατόν καλύτερη αντιμετώπιση τους, είναι μεταξύ των λόγων που οδήγησαν στην προτεινόμενη λύση που θα ακολουθήσει.

5.4 Προτεινόμενη λύση

Η χρησιμοποίηση της τεχνολογίας blockchain ή παραλλαγών της τύπου distributed ledger σε fintech εφαρμογές τηρώντας παράλληλα τις απαιτήσεις κανονισμών όπως ο GDPR ή το PSD2, αποτελούν ζητούμενο για μεγάλο κομμάτι του χρηματοπιστωτικού κλάδου. Ακολούθως θα γίνει μια προσπάθεια να προταθεί μια συγκεκριμένη λύση που θα καλύπτει όσο το δυνατόν περισσότερο τις απαιτήσεις.

5.4.1 Είδος blockchain

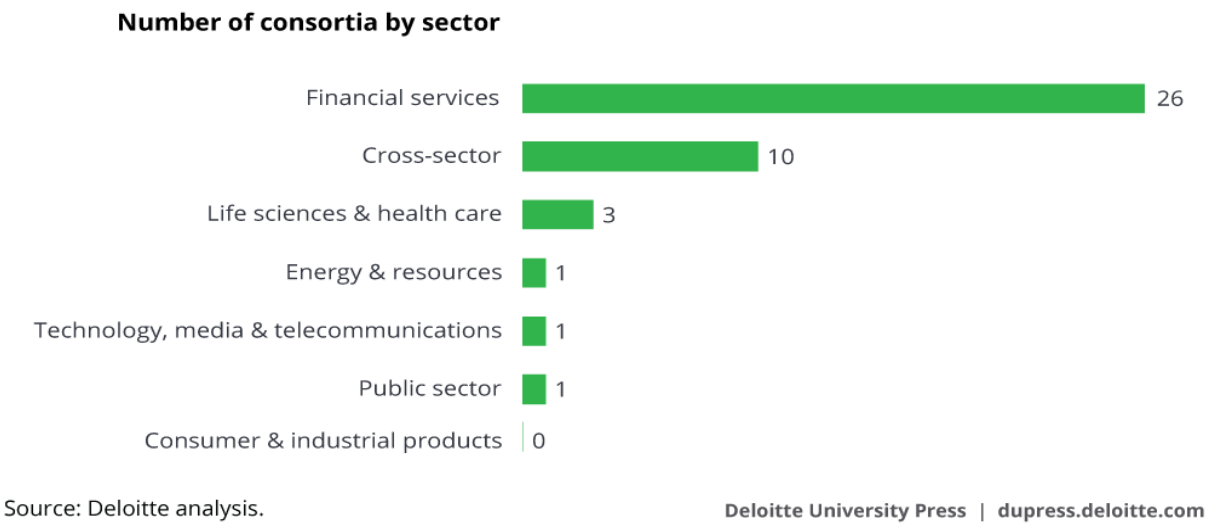
Καταρχήν θα πρέπει να αποφασιστεί τι είδους ledger θα χρησιμοποιηθεί. Με δεδομένες τις ιδιαιτερότητες του χρηματοπιστωτικού κλάδου η πιο ενδεδειγμένη λύση φαίνεται να είναι αυτή των «consortium blockchains» ή κοινοπραξιών blockchain.

Τα κατανεμημένα λογιστικά βιβλία είναι εργαλεία ροής εργασίας μεταξύ επιχειρήσεων (B2B), γεγονός που συνεπάγεται ότι το blockchain ουσιαστικά απαιτεί συνεργασία— για τον καθορισμό προτύπων, την ανάπτυξη υποδομών και την εκτέλεση συναλλαγών. Αυτές οι κοινοπραξίες (consortiums) είναι ο μηχανισμός μέσω του οποίου συνεργάζονται εταιρείες, ρυθμιστικές αρχές και κυβερνήσεις που ενδιαφέρονται για το blockchain.

Υπάρχουν δύο τύποι κοινοπραξιών blockchain: οι εστιασμένες στις επιχειρήσεις και οι εστιασμένες στην τεχνολογία. Οι κοινοπραξίες που επικεντρώνονται στις επιχειρήσεις στοχεύουν στη δημιουργία και τη λειτουργία επιχειρηματικών πλατφορμών που βασίζονται στο blockchain για την επίλυση ενός συγκεκριμένου επιχειρηματικού προβλήματος. Οι κοινοπραξίες που επικεντρώνονται στην τεχνολογία επιδιώκουν να αναπτύξουν επαναχρησιμοποιήσιμες πλατφόρμες blockchain με βάση τεχνικά πρότυπα.

Ορισμένες κοινοπραξίες καλύπτουν και τους δύο τύπους δραστηριοτήτων. Ένα παράδειγμα είναι η R3, η κοινοπραξία του οποίου περιλαμβάνει περισσότερα από 200 από τα μεγαλύτερα χρηματοπιστωτικά ιδρύματα, ρυθμιστικές αρχές και κεντρικές τράπεζες στον κόσμο. Στην συγκεκριμένη κοινοπραξία ανήκει η πλατφόρμα Corda.

Ο χρηματοπιστωτικός τομέας κυριαρχεί στη δημιουργία κοινοπραξιών blockchain.



Εικόνα 13: Πηγή: Deloitte analysis, «*Αριθμός κοινοπραξιών ανά κλάδο*», 2018.

Οι λόγοι που προτιμώνται είναι η χρηματοδότηση που μοιράζεται, η συμμετοχή μεγάλων εταιρειών του κλάδου, η ηγεσία ορισμένων εταιρειών με εμπειρία και η σωστή διακυβέρνηση που βοηθάει στην επίτευξη κοινών στόχων.

Από την πλειάδα των consortium blockchains που υπάρχουν θα επιλεγεί το Corda, που όπως έχει αναφερθεί προηγουμένως, περιέχει εγγενή συμμόρφωση με τον GDPR, ενώ το στηρίζουν και συμμετέχουν σε αυτό πληθώρα μεγάλων χρηματοπιστωτικών οργανισμών. [26, 27]

5.4.2 Αρχιτεκτονική της εφαρμογής

Ένα δίκτυο Corda είναι ένα ομότιμο δίκτυο κόμβων. Κάθε κόμβος αντιπροσωπεύει μια νομική οντότητα και κάθε ένας εκτελεί το λογισμικό Corda.

Όλη η επικοινωνία μεταξύ κόμβων είναι από σημείο σε σημείο και κρυπτογραφείται με ασφάλεια επιπέδου μεταφοράς. Αυτό σημαίνει ότι τα δεδομένα κοινοποιούνται μόνο αν είναι ανάγκη. Δεν υπάρχουν παγκόσμιες μεταδόσεις.

Κάθε κόμβος έχει μία και μοναδική γνωστή ταυτότητα. Η ταυτότητα του κόμβου χρησιμοποιείται για την αντιπροσώπευση του κόμβου στις συναλλαγές. Η υπηρεσία χάρτη δικτύου (network map service) αντιστοιχίζει κάθε γνωστή ταυτότητα κόμβου σε μια διεύθυνση IP. Αυτές οι διευθύνσεις IP χρησιμοποιούνται για την ανταλλαγή μηνυμάτων μεταξύ των κόμβων.

Οι κόμβοι μπορούν επίσης να δημιουργήσουν εμπιστευτικές ταυτότητες για μεμονωμένες συναλλαγές. Η αλυσίδα πιστοποιητικών που συνδέει μια εμπιστευτική ταυτότητα με μια γνωστή ταυτότητα κόμβου ή πραγματική νομική ταυτότητα διανέμεται μόνο όπου και όταν είναι απαραίτητο. Εάν χρησιμοποιούνται εμπιστευτικές ταυτότητες, αυτό εξασφαλίζει ότι ακόμα και αν ένας εισβολέας αποκτήσει πρόσβαση σε μια μη κρυπτογραφημένη συναλλαγή, δεν μπορεί να αναγνωρίσει τους συμμετέχοντες της συναλλαγής χωρίς πρόσθετες πληροφορίες.

Οι κόμβοι Corda ανακαλύπτουν ο ένας τον άλλον μέσω μιας υπηρεσίας χάρτη δικτύου. Αυτή η υπηρεσία λειτουργεί ως τηλεφωνικός κατάλογος, ο οποίος δημοσιεύει μια λίστα ομότιμων κόμβων που περιλαμβάνει μεταδεδομένα σχετικά με το ποιοι είναι και ποιες υπηρεσίες μπορούν να προσφέρουν.

Σε αντίθεση με το παραδοσιακό blockchain, τα δίκτυα του Corda είναι ημι-ιδιωτικά. Για να συμμετάσχει σε ένα δίκτυο, ένας κόμβος πρέπει να αποκτήσει ένα πιστοποιητικό από τον χειριστή του δικτύου. Αυτό το πιστοποιητικό αντιστοιχίζει μια γνωστή ταυτότητα κόμβου σε:

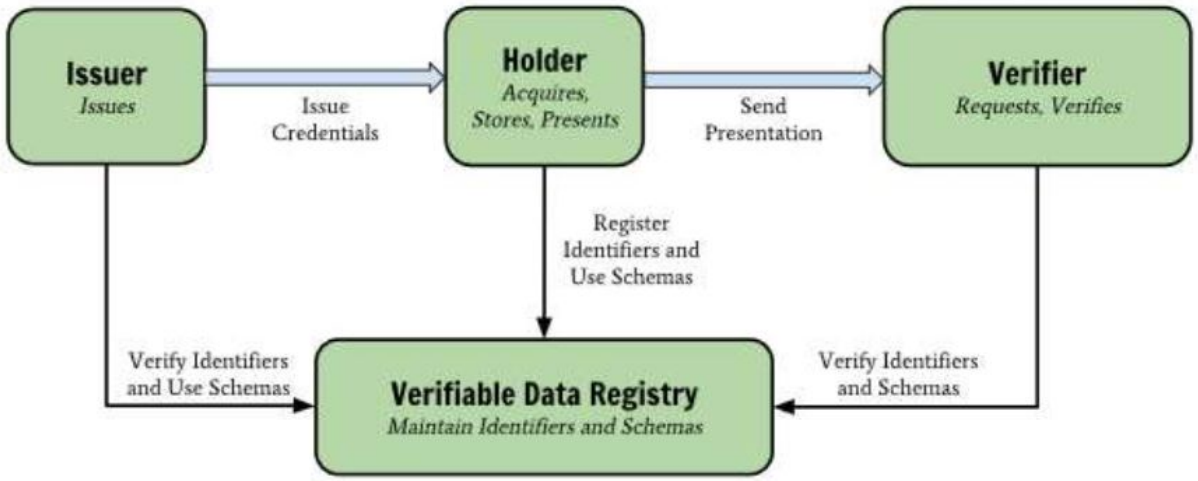
- Μια πραγματική νομική ταυτότητα

- Ένα δημόσιο κλειδί

Ο χειριστής δικτύου επιβάλλει κανόνες σχετικά με τις πληροφορίες που πρέπει να παρέχουν οι κόμβοι και τις διαδικασίες γνώριζε-τον πελάτη σου (KYC) που πρέπει να ολοκληρώσουν πριν από τη χορήγηση αυτού του πιστοποιητικού.

Σημαντικό ρόλο σε σχέση με την προστασία των προσωπικών δεδομένων και το KYC, παίζει η υιοθέτηση μέσω του Cordentity της αυτοκυρίαρχης (self-sovereign) ψηφιακής ταυτότητας που στηρίζεται πάνω σε δύο έννοιες/τεχνολογίες τα DIDs (Decentralized Identifiers) και τα ABCs (Attribute Based Credential ή Verifiable Claims). Σε αυτό το πλαίσιο, σημαίνει ότι τα διαπιστευτήρια (ψηφιακά υπογεγραμμένες αξιώσεις ή σύνολο χαρακτηριστικών) αποθηκεύονται απευθείας από τον κάτοχο της ταυτότητας και μοιράζονται μόνο εάν είναι απαραίτητο να γνωρίζει κάποιος. Αυτά τα διαπιστευτήρια υπογράφονται κρυπτογραφικά από γνωστές οντότητες (π.χ. Αστυνομία, Νοσοκομείο, Πανεπιστήμιο, Τράπεζα κ.λπ.) που είναι έγκυροι φορείς στον τομέα τους. Με αυτό τον

τρόπο μπορούμε να συνδυάσουμε τις υπάρχουσες αρχές και τις "αξιόπιστες πηγές" (που έχουν δημόσια DID) με έναν πολύ ευέλικτο, κλιμακούμενο και ασφαλή τρόπο ανταλλαγής πληροφοριών. Η προσέγγιση αυτή είναι επίσης συμβατή με τον GDPR και επιτρέπει πολλές λειτουργίες που χρειάζονται προσωπικά αναγνωρίσιμες πληροφορίες (Personally Identifiable Information, PII) που διαφορετικά θα ήταν πολύ δύσκολο να εφαρμοστούν.[27]



Εικόνα 14: Πηγή: Europa.eu, «eIDAS - *The DID / SSI approach to identity and Verifiable claims*», Μάιος 2019.

Στο Corda, δεν υπάρχει ένας κεντρικός χώρος αποθήκευσης δεδομένων. Αντίθετα, κάθε κόμβος διατηρεί τη δική του βάση δεδομένων για τα γεγονότα που γνωρίζει. Τα γεγονότα που ένας κόμβος γνωρίζει είναι αυτά με τα οποία εμπλέκεται. Το αποτέλεσμα αυτής της σχεδίασης είναι ότι κάθε ομότιμο μέρος βλέπει μόνο ένα υποσύνολο γεγονότων στο καθολικό και κανένα ομότιμο μέρος δε γνωρίζει το καθολικό στο σύνολό του. Το Corda Ledger είναι μια υποκειμενική κατασκευή από την άποψη κάθε ομότιμου μέρους.

Στο Corda, δεν υπάρχει κεντρικό ή γενικό καθολικό που να λειτουργεί σαν εκπρόσωπος για λογαριασμό όλων των κόμβων του δικτύου. Αντίθετα, κάθε κόμβος στο δίκτυο διατηρεί τη δική του θυρίδα αποθήκευσης που περιέχει όλα τα γνωστά σε αυτόν γεγονότα, μια ιδιωτική βάση δεδομένων.

Μια «κατάσταση» είναι ένα αμετάβλητο αντικείμενο που αντιπροσωπεύει ένα γεγονός γνωστό από έναν ή περισσότερους κόμβους Corda σε μια συγκεκριμένη χρονική στιγμή. Οι καταστάσεις μπορούν να περιέχουν αυθαίρετα δεδομένα, τα οποία τους επιτρέπουν να αντιπροσωπεύουν γεγονότα κάθε είδους (π.χ. μετοχές, ομόλογα, δάνεια, στοιχεία KYC,

πληροφορίες ταυτότητας κλπ). Εκτός από οποιαδήποτε πληροφορία σχετικά με το ίδιο το γεγονός, η κατάσταση περιέχει επίσης μια αναφορά στο συμβόλαιο που διέπει την εξέλιξη της κατάστασης με την πάροδο του χρόνου.

Δεδομένου ότι οι καταστάσεις είναι αμετάβλητες, δεν μπορούν να τροποποιηθούν άμεσα ώστε να αντικατοπτρίζουν μια αλλαγή στην κατάσταση του κόσμου. Αντίθετα, ο κύκλος ζωής ενός κοινού γεγονότος με την πάροδο του χρόνου αντιπροσωπεύεται από μια ακολουθία κατάστασης. Όταν μία κατάσταση πρέπει να ενημερωθεί, δημιουργούμε μια νέα έκδοση της κατάστασης που αντιπροσωπεύει τη νέα κατάσταση του κόσμου, και χαρακτηρίζουμε την υπάρχουσα κατάσταση ως ιστορική. Αυτή η αλληλουχία αντικατάστασης των καταστάσεων μας δίνει μια πλήρη εικόνα της εξέλιξης του κοινού γεγονότος με την πάροδο του χρόνου.

Κάθε κόμβος στο δίκτυο διατηρεί μια θυρίδα αποθήκευσης - μια βάση δεδομένων όπου παρακολουθεί όλες τις τρέχουσες και ιστορικές καταστάσεις που γνωρίζει, και την οποία θεωρεί ότι είναι σχετική με τον εαυτό του.

Το Corda χρησιμοποιεί ένα UTXO (unspent transaction output) μοντέλο όπου κάθε κατάσταση στο καθολικό είναι αμετάβλητη. Το καθολικό εξελίσσεται με την πάροδο του χρόνου με το να εφαρμόζει τις συναλλαγές. Οι συναλλαγές ενημερώνουν το καθολικό χαρακτηρίζοντας μηδέν ή περισσότερες υπάρχουσες καταστάσεις καθολικού ως ιστορικές (input) και παράγωντας μηδενικές ή περισσότερες νέες καταστάσεις καθολικού (output). Οι συναλλαγές αντιπροσωπεύουν μία μόνο σύνδεση στις ακολουθίες καταστάσεων. Μια συναλλαγή μπορεί να περιέχει οποιονδήποτε αριθμό εισροών, εκροών και αναφορών οποιουδήποτε τύπου:

- Μπορούν να περιλαμβάνουν πολλούς διαφορετικούς τύπους καταστάσεων (οι καταστάσεις μπορούν να αντιπροσωπεύσουν, π.χ., μετρητά ή ομόλογα)

- Μπορούν να είναι εκδόσεις (έχουν μηδενικές εισροές) ή έξοδοι (έχουν μηδενικές εκροές)

- Μπορούν να συγχωνεύσουν ή να χωρίσουν τα ανταλλάξιμα περιουσιακά στοιχεία (να συνδυάσουν μία κατάσταση €2 και μία κατάσταση €5 σε μία κατάσταση μετρητών €7)

Οι συναλλαγές είναι ατομικές. Είτε όλες οι προτεινόμενες αλλαγές της συναλλαγής γίνονται δεκτές, ή καμία δε γίνεται δεκτή. Υπάρχουν δύο βασικοί τύποι συναλλαγών: Οι συναλλαγές συμβολαιογραφικής αλλαγής (που χρησιμοποιούνται για την συμβολαιογραφική αλλαγή μιας κατάστασης), και οι γενικές συναλλαγές (που χρησιμοποιούνται για οτιδήποτε άλλο).

Αρχικά, μια συναλλαγή είναι απλώς μια πρόταση για την ενημέρωση του καθολικού. Αντιπροσωπεύει την μελλοντική κατάσταση του καθολικού που επιθυμούν οι δημιουργοί της συναλλαγής. Για να γίνει πραγματικότητα, η συναλλαγή πρέπει να λάβει υπογραφές από όλους τους απαιτούμενους υπογράφοντες. Κάθε απαιτούμενος υπογράφων προσαρτά την υπογραφή του στη συναλλαγή για να υποδείξει ότι εγκρίνει την πρόταση. Εάν συγκεντρωθούν όλες οι απαιτούμενες υπογραφές, η συναλλαγή μετατρέπεται σε δεσμευμένη. Αυτό σημαίνει ότι οι εισροές της συναλλαγής μαρκάρονται ως ιστορικές και δεν μπορούν να χρησιμοποιηθούν σε μελλοντικές συναλλαγές και ότι οι εκροές της συναλλαγής γίνονται μέρος της τρέχουσας κατάστασης του καθολικού.

Κάθε απαιτούμενος υπογράφων θα πρέπει να υπογράφει τη συναλλαγή μόνο εάν ισχύουν οι ακόλουθες δύο προϋποθέσεις:

> **Εγκυρότητα συναλλαγής:** Τόσο για την προτεινόμενη συναλλαγή όσο και για κάθε συναλλαγή στην αλυσίδα συναλλαγών που δημιούργησε τις εισροές της τρέχουσας προτεινόμενης συναλλαγής: α) η συναλλαγή υπογράφεται ψηφιακά από όλα τα απαιτούμενα μέρη και β) η συναλλαγή είναι συμβατικά έγκυρη
>
> **Μοναδικότητα συναλλαγής:** Δεν υπάρχει άλλη δεσμευμένη συναλλαγή που να έχει καταναλώσει οποιαδήποτε από τις εισροές στην προτεινόμενη συναλλαγή.

Εάν η συναλλαγή συγκεντρώσει όλες τις απαιτούμενες υπογραφές, αλλά οι προηγούμενες συνθήκες δεν ισχύουν, οι εκροές της συναλλαγής δεν θα είναι έγκυρες και δεν θα γίνονται δεκτές ως εισροές σε επόμενες συναλλαγές. Τα συμβόλαια για τις καταστάσεις αναφοράς δεν εκτελούνται για τη συναλλαγή που τις περιέχει.

Εκτός από τις καταστάσεις εισροών και τις καταστάσεις εκροών, οι συναλλαγές περιέχουν:

Εντολές (μας επιτρέπουν να δηλώσουμε την πρόθεση της συναλλαγής, επηρεάζοντας τον τρόπο ελέγχου της εγκυρότητας της συναλλαγής)

Συνημμένα (μεγάλα κομμάτια δεδομένων που μπορούν να επαναχρησιμοποιηθούν σε πολλές διαφορετικές συναλλαγές)

Time-Window (χρονικό διάστημα κατά το οποίο μπορεί να πραγματοποιηθεί η συναλλαγή)

Notary (παρέχει το σημείο οριστικότητας στο σύστημα)

Η ισχύς του συμβολαίου ορίζεται ως εξής:

1) Κάθε κατάσταση συναλλαγής καθορίζει ένα τύπο συμβολαίου

2) Ένα συμβόλαιο λαμβάνει μια συναλλαγή ως εισροή και δηλώνει εάν η συναλλαγή θεωρείται έγκυρη με βάση τους κανόνες του συμβολαίου

3) Μια συναλλαγή είναι έγκυρη μόνο εάν το συμβόλαιο κάθε κατάστασης εισροής και κάθε κατάστασης εκροής τη θεωρεί έγκυρη.

Μια συναλλαγή που δεν είναι συμβατικά έγκυρη, δεν είναι έγκυρη πρόταση για την ενημέρωση του καθολικού και επομένως δεν μπορεί ποτέ να υποβληθεί στο καθολικό. Με τον τρόπο αυτό, τα συμβόλαια επιβάλλουν κανόνες για την εξέλιξη των καταστάσεων με την πάροδο του χρόνου, οι οποίοι είναι ανεξάρτητοι από την προθυμία των απαιτούμενων υπογραφόντων να υπογράψουν μια δεδομένη συναλλαγή.

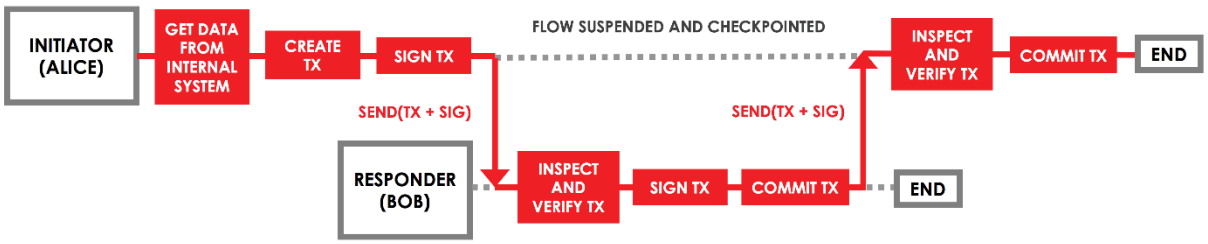
Η επαλήθευση των συναλλαγών πρέπει να είναι ντετερμινιστική – ένα συμβόλαιο θα πρέπει είτε πάντα να αποδέχεται είτε πάντα να απορρίπτει μια δεδομένη συναλλαγή. Αυτή είναι μια απαραίτητη προϋπόθεση για να εξασφαλιστεί ότι όλοι οι ομότιμοι συμμετέχοντες στο δίκτυο επιτυγχάνουν συναίνεση σχετικά με την εγκυρότητα μιας δεδομένης ενημέρωσης του καθολικού.

Δεδομένου ότι ένα συμβόλαιο δεν έχει πρόσβαση σε πληροφορίες από τον έξω κόσμο, μπορεί να ελέγξει μόνο τη συναλλαγή για εσωτερική ισχύ. Επομένως, οι ομότιμοι συμμετέχοντες θα πρέπει να ελέγχουν το περιεχόμενο μιας συναλλαγής πριν την

υπογράψουν, ακόμα και αν η συναλλαγή είναι συμβατικά έγκυρη, για να δουν αν συμφωνούν με την προτεινόμενη ενημέρωση του καθολικού.

Κάθε συμβόλαιο αναφέρεται επίσης σε ένα νομικό πεζό έγγραφο που αναφέρει τους κανόνες που διέπουν την εξέλιξη της κατάστασης με την πάροδο του χρόνου με τρόπο συμβατό με τα παραδοσιακά νομικά συστήματα. Το έγγραφο αυτό μπορεί να χρησιμοποιηθεί σε περίπτωση νομικών διαφορών.

Τα δίκτυα Corda χρησιμοποιούν μηνύματα από σημείο σε σημείο αντί για μια καθολική μετάδοση. Αυτό σημαίνει ότι ο συντονισμός μιας ενημέρωσης του καθολικού απαιτεί από τους συμμετέχοντες στο δίκτυο να καθορίζουν ακριβώς ποιες πληροφορίες πρέπει να αποσταλούν, σε ποιους αντισυμβαλλομένους και με ποια σειρά. Αντί να χρειάζεται να καθοριστούν αυτά τα βήματα με μη αυτόματο τρόπο, το Corda αυτοματοποιεί τη διαδικασία χρησιμοποιώντας ροές. Μια ροή είναι μια ακολουθία βημάτων που υποδεικνύει σε έναν κόμβο τον τρόπο επίτευξης μιας συγκεκριμένης ενημερωμένης του καθολικού, όπως η έκδοση ενός περιουσιακού στοιχείου ή η διευθέτηση μιας συναλλαγής.



Εικόνα 15: Πηγή: Corda.net, «*Αλληλουχία βημάτων ροής για την ενημέρωση του καθολικού*», 2020.

Οι κόμβοι επικοινωνούν με διαβίβαση μηνυμάτων μεταξύ ροών. Κάθε κόμβος έχει μηδενικές ή περισσότερες ροές που έχουν καταχωρηθεί για να ανταποκρίνονται σε μηνύματα από μία άλλη ροή. Το Corda παρέχει μια βιβλιοθήκη ροών για το χειρισμό κοινών εργασιών. Το πλαίσιο ροών επιτρέπει στους κόμβους να έχουν πολλές ροές ενεργές ταυτόχρονα.

Συναίνεση εγκυρότητας είναι η διαδικασία ελέγχου ότι ισχύουν οι ακόλουθες προϋποθέσεις τόσο για την προτεινόμενη συναλλαγή όσο και για κάθε συναλλαγή στην αλυσίδα συναλλαγών που παρήγαγε τις εισροές στην προτεινόμενη συναλλαγή:

- Η συναλλαγή γίνεται αποδεκτή από τα συμβόλαια κάθε κατάστασης εισροών και εκροών

- Η συναλλαγή έχει όλες τις απαιτούμενες υπογραφές

Δεν αρκεί να επαληθεύεται η ίδια η προτεινόμενη συναλλαγή. Πρέπει επίσης να επαληθεύσουμε κάθε συναλλαγή στην αλυσίδα συναλλαγών που οδήγησε στη δημιουργία των εισροών στην προτεινόμενη συναλλαγή. Αυτό είναι γνωστό ως “walking the chain”, περπατώντας την αλυσίδα.

Η συναίνεση μοναδικότητας είναι η απαίτηση ότι καμία από τις εισροές σε μια προτεινόμενη συναλλαγή δεν έχει ήδη καταναλωθεί σε άλλη συναλλαγή. Εάν μία ή περισσότερες από τις εισροές έχουν ήδη καταναλωθεί σε άλλη συναλλαγή, αυτό είναι γνωστό ως διπλή δαπάνη και η πρόταση συναλλαγής θεωρείται άκυρη. Η συναίνεση μοναδικότητας παρέχεται από τους συμβολαιογράφους.

Ένα συμπλέγμα συμβολαιογράφων είναι μια υπηρεσία δικτύου που παρέχει συναίνεση μοναδικότητας, βεβαιώνοντας ότι, για μια δεδομένη συναλλαγή, δεν έχει ήδη υπογράψει άλλες συναλλαγές που καταναλώνουν οποιαδήποτε από τις καταστάσεις εισαγωγής της προτεινόμενης συναλλαγής.

Το Corda έχει "pluggable" συναίνεση, επιτρέποντας συμπλέγματα συμβολαιογράφων να επιλέξουν έναν αλγόριθμο συναίνεσης με βάση τις απαιτήσεις τους όσον αφορά την ιδιωτικότητα, την επεκτασιμότητα, την συμβατότητα με το νομικό σύστημα και την αλγοριθμική ευελιξία.

Τα συμβολαιογραφικά συμπλέγματα μπορεί να διαφέρουν ως προς:

Τη δομή - ένα συμβολαιογραφικό σύμπλεγμα μπορεί να είναι ένας κόμβος, αρκετοί κόμβοι αμοιβαία εμπιστοσύνης ή αρκετοί αμοιβαία δύσπιστοι κόμβοι

Αλγόριθμος συναίνεσης - ένα συμβολαιογραφικό σύμπλεγμα μπορεί να επιλέξει να εκτελέσει έναν αλγόριθμο υψηλής ταχύτητας, υψηλής εμπιστοσύνης όπως το RAFT, έναν αλγόριθμο χαμηλής ταχύτητας, χαμηλής εμπιστοσύνης όπως το BFT, ή οποιονδήποτε άλλο αλγόριθμο συναίνεσης επιλέξει.

Ένα συμβολαιογραφικό σύμπλεγμα πρέπει επίσης να αποφασίσει εάν θα παράσχει ή όχι συναίνεση εγκυρότητας επικυρώνοντας κάθε συναλλαγή πριν από τη διάπραξή της. Κατά τη λήψη αυτής της απόφασης, αντιμετωπίζει την ακόλουθη αντιστάθμιση:

> Εάν μια συναλλαγή δεν ελέγχεται για εγκυρότητα (μη επικυρών συμβολαιογράφος), δημιουργεί τον κίνδυνο επιθέσεων τύπου "denial of state", όπου ένας κόμβος δημιουργεί εν γνώσει του μια μη έγκυρη συναλλαγή που καταναλώνει κάποιο σύνολο υπαρχουσών καταστάσεων και την στέλνει στο συμβολαιογράφο, με αποτέλεσμα οι καταστάσεις να επισημαίνονται ως καταναλωθείσες.
>
> Εάν η συναλλαγή ελεγχθεί για εγκυρότητα (επικυρών συμβολαιογράφος), ο συμβολαιογράφος θα πρέπει να δει το πλήρες περιεχόμενο της συναλλαγής και τις εξαρτήσεις της. Αυτό διαρρέει δυνητικά ιδιωτικά δεδομένα στο συμβολαιογραφικό σύμπλεγμα.

Στην περίπτωση του μη επικυρωμένου μοντέλου, το μοντέλο ελεγχόμενης διανομής δεδομένων της Corda σημαίνει ότι οι πληροφορίες στις μη αναλωθείσες καταστάσεις δεν διαμοιράζονται ευρέως. Επιπλέον, το με έγκριση δίκτυο της Corda σημαίνει ότι το συμβολαιογραφικό σύμπλεγμα μπορεί να αποθηκεύσει την ταυτότητα του μέρους που δημιούργησε τη συναλλαγή “denial of state”, επιτρέποντας την επίλυση της επίθεσης εκτός καθολικού.

Στην περίπτωση του μοντέλου επικύρωσης, η χρήση ανώνυμων δημόσιων κλειδιών που δημιουργήθηκαν πρόσφατα αντί για νομικές ταυτότητες για την αναγνώριση των μερών σε μια συναλλαγή περιορίζει τις πληροφορίες που βλέπει το συμβολαιογραφικό σύμπλεγμα.

Transaction components	Validating	Non-validating
Input states	Fully visible	References only [1]
Output states	Fully visible	Hidden
Commands (with signer identities)	Fully visible	Hidden
Attachments	Fully visible	Hidden
Time window	Fully visible	Fully visible
Notary identity	Fully visible	Fully visible
Signatures	Fully visible	Hidden
Network parameters	Fully visible	Fully visible

Εικόνα 16: Πηγή: Corda.net, «Σύνοψη των συγκεκριμένων στοιχείων συναλλαγής που πρέπει να αποκαλύπτονται σε κάθε τύπο συμβολαιογράφου », 2020.

Κάθε δίκτυο Corda μπορεί να έχει πολλαπλά συμπλέγματα συμβολαιογράφων, με το καθένα δυνητικά να τρέχει ένα διαφορετικό αλγόριθμο συναίνεσης. Αυτό παρέχει διάφορα οφέλη:

Προστασία προσωπικών δεδομένων - μπορούμε να έχουμε συμπλέγματα συμβολαιογράφων τόσο που επικυρώνουν όσο που δεν επικυρώνουν στο ίδιο δίκτυο, με το καθένα να τρέχει ένα διαφορετικό αλγόριθμο. Αυτό επιτρέπει στους κόμβους να επιλέγουν το προτιμώμενο σύμπλεγμα συμβολαιογράφων ανά συναλλαγή.

Εξισορρόπηση φορτίου - η κατανομή του φορτίου συναλλαγής σε πολλά συμπλέγματα συμβολαιογράφων επιτρέπει υψηλότερη διεκπεραίωση συναλλαγών για την πλατφόρμα συνολικά.

Χαμηλή λανθάνουσα κατάσταση - ο λανθάνων χρόνος μπορεί να ελαχιστοποιηθεί με την επιλογή ενός συμπλέγματος συμβολαιογράφων που βρίσκεται πιο κοντά, φυσικά, στα μέρη που συναλλάσσονται.

Η θυρίδα αποθήκευσης περιέχει δεδομένα που εξάγονται από το καθολικό που θεωρείται ότι σχετίζονται με τον κάτοχο του κόμβου, αποθηκευμένα με ένα σχεσιακό μοντέλο μπορούν εύκολα να αναζητηθούν και να εργαστεί κάποιος με αυτά. Το θησαυροφυλάκιο παρακολουθεί τόσο τις καταστάσεις που δεν καταναλώνονται όσο και τις καταστάσεις που καταναλώνονται:

Οι μη αναλωμένες (ή μη δαπανηθέντες) καταστάσεις αντιπροσωπεύουν ανταλλάξιμες/μετρήσιμες καταστάσεις που είναι διαθέσιμες για δαπάνες (συμπεριλαμβανομένων συναλλαγών "προς τον εαυτό") και γραμμικές καταστάσεις που είναι διαθέσιμες για εξέλιξη (π.χ. ως απάντηση σε ένα γεγονός κύκλου ζωής σε μια συμφωνία) ή για μεταφορά σε άλλο μέρος.

Οι καταστάσεις που αναλώθηκαν (ή δαπανήθηκαν) αντιπροσωπεύουν αμετάβλητη κατάσταση του καθολικού για τον σκοπό της αναφοράς συναλλαγών, του ελέγχου και της αρχειοθέτησης, συμπεριλαμβανομένης της δυνατότητας εκτέλεσης συνδυασμών με δεδομένα ιδιωτικού είδους (όπως σημειώσεις πελατών).

Όπως και με ένα πορτοφόλι κρυπτονομισμάτων, η θυρίδα αποθήκευσης του Corda μπορεί να δημιουργήσει συναλλαγές που στέλνουν αξία (π.χ. μεταφορά κατάστασης) σε κάποιον άλλο συνδυάζοντας ανταλλάξιμες καταστάσεις και ενδεχομένως προσθέτοντας μια εκροή αλλαγής που κάνει τις τιμές να ισορροπούν (αυτή η διαδικασία συνήθως αναφέρεται ως «επιλογή νομίσματος»). Οι δαπάνες της θυρίδας αποθήκευσης διασφαλίζουν ότι οι συναλλαγές τηρούν τους κανόνες της ανταλλαξιμότητας, προκειμένου να διασφαλιστεί ότι ο εκδότης και τα δεδομένα αναφοράς διατηρούνται καθώς τα περιουσιακά στοιχεία περνούν από χέρι σε χέρι.

Μια δυνατότητα που ονομάζεται «μαλακό κλείδωμα» παρέχει τη δυνατότητα αυτόματης ή ρητής δέσμευσης καταστάσεων για την αποτροπή πολλαπλών συναλλαγών εντός του ίδιου κόμβου, να προσπαθήσουν ταυτόχρονη χρήση του ίδιου αποτελέσματος. Ενώ αυτό το σενάριο θα μπορούσε τελικά να ανιχνευθεί από έναν συμβολαιογράφο, το «μαλακό κλείδωμα» παρέχει έναν μηχανισμό έγκαιρης ανίχνευσης για τέτοια αδικαιολόγητα και άκυρα σενάρια.

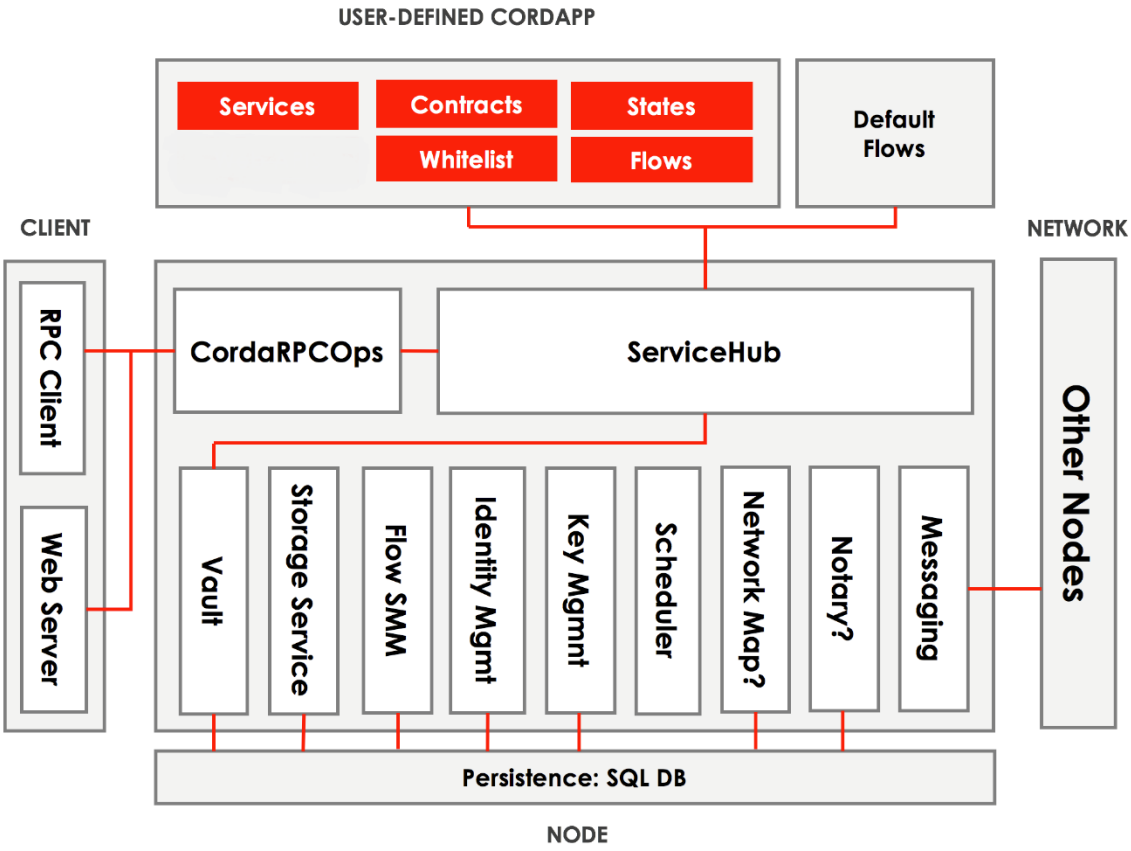
Ένας «συμβολαιογράφος» ενεργεί επίσης ως αρχή χρονικής σήμανσης, επαληθεύοντας ότι μια συναλλαγή πραγματοποιήθηκε κατά τη διάρκεια ενός συγκεκριμένου χρονικού παραθύρου πριν την συμβολαιογράφηση της. Για να έχει νόημα ένα χρονικό περιθώριο, οι συνέπειές του πρέπει να είναι δεσμευτικές για το μέρος που το ζητεί. Οι χρόνοι στις συναλλαγές καθορίζονται ως χρονικά παράθυρα, όχι ως απόλυτοι χρόνοι. Σε ένα κατανεμημένο σύστημα δεν μπορεί ποτέ να υπάρξει "αληθινός χρόνος", μόνο μια προσέγγιση του.

Σε πολλές περιπτώσεις, η συμβατική ισχύς μιας συναλλαγής εξαρτάται από ορισμένα εξωτερικά στοιχεία, όπως η τρέχουσα συναλλαγματική ισοτιμία. Τα Oracles είναι υπηρεσίες δικτύου που, κατόπιν αιτήματος, παρέχουν εντολές που συμπυκνώνουν ένα συγκεκριμένο γεγονός (π.χ. τη συναλλαγματική ισοτιμία τη χρονική στιγμή x) και παραθέτουν το oracle ως απαιτούμενο υπογράφοντα.

Εάν ένας κόμβος επιθυμεί να χρησιμοποιήσει ένα δεδομένο γεγονός σε μια συναλλαγή, ζητούν μια εντολή που επιβεβαιώνει αυτό το γεγονός από το oracle. Εάν το oracle θεωρεί το γεγονός αληθινό, στέλνουν πίσω την απαιτούμενη εντολή. Στη συνέχεια, ο κόμβος περιλαμβάνει την εντολή στη συναλλαγή τους και το oracle θα υπογράψει τη συναλλαγή για να επιβεβαιώσει ότι το γεγονός είναι αληθές.

Για λόγους προστασίας προσωπικών δεδομένων, το oracle δεν απαιτεί πρόσβαση σε κάθε μέρος της συναλλαγής και οι μόνες πληροφορίες που χρειάζεται να δει είναι οι ενσωματωμένες, που σχετίζονται με το oracle, εντολές. Θα πρέπει επίσης να παρέχουν εγγυήσεις ότι όλες οι εντολές που απαιτούν υπογραφή από το συγκεκριμένο oracle θα πρέπει να είναι ορατές στην οντότητα oracle, αλλά όχι στις υπόλοιπες.

Ο κόμβος Corda είναι ένα περιβάλλον χρόνου εκτέλεσης JVM με μοναδική ταυτότητα στο δίκτυο που φιλοξενεί υπηρεσίες Corda και CorDapps.



Εικόνα 17: Πηγή: Corda.net, «Εσωτερική αρχιτεκτονική ενός κόμβου », 2020.

Τα βασικά στοιχεία της αρχιτεκτονικής είναι:

- Ένα έμμονο επίπεδο (persistence layer) για την αποθήκευση δεδομένων
- Μια διασύνδεση δικτύου (network interface) για αλληλεπίδραση με άλλους κόμβους
- Μια διασύνδεση RPC για αλληλεπίδραση με τον κάτοχο του κόμβου
- Ένας κόμβος εξυπηρέτησης (service hub) για να επιτρέπεται στις ροές του κόμβου να καλούν τις άλλες υπηρεσίες του κόμβου
-Μια διασύνδεση cordapp και υπηρεσία παροχής για την επέκταση του κόμβου με την εγκατάσταση των CorDapps

Το στρώμα εμμονής έχει δύο μέρη:

Τη **θυρίδα αποθήκευσης**, όπου ο κόμβος αποθηκεύει οποιεσδήποτε σχετικές τρέχουσες και ιστορικές καταστάσεις

Η **υπηρεσία αποθήκευσης**, όπου αποθηκεύει συναλλαγές, συνημμένα και σημεία ελέγχου ροής

Η παροχή οποιωνδήποτε πρόσθετων δεδομένων συναλλαγής στο oracle θα αποτελούσε διαρροή απορρήτου. Για να το καταπολεμήσουμε, χρησιμοποιούμε την έννοια των φιλτραρισμένων συναλλαγών, στην οποία ο προτείνων τη συναλλαγή χρησιμοποιεί μια ένθετη προσέγγιση δέντρου Merkle για να "αποκόψει" οποιαδήποτε τμήματα της συναλλαγής που ο oracle/συμβολαιογράφος δεν χρειάζεται να δουν πριν το παρουσιάσει σε αυτούς για υπογραφή. Ένα δέντρο Merkle είναι ένας γνωστός κρυπτογραφικός συνδυασμός που χρησιμοποιείται συνήθως για την παροχή αποδείξεων συμπερίληψης και ακεραιότητας δεδομένων. Τα δέντρα Merkle χρησιμοποιούνται ευρέως σε ομότιμα δίκτυα, συστήματα blockchain και git.[28, 29]

5.4.3 Τα πλεονεκτήματα της εφαρμογής

Από την ανάλυση της αρχιτεκτονικής της συγκεκριμένης εφαρμογής, γίνεται αντιληπτό ότι προκύπτουν κάποια οφέλη από την υιοθέτηση της συγκεκριμένης υλοποίησης. Ακολούθως θα γίνει μια παρουσίαση των βασικότερων και κυρίως αυτών που απαντούν στα ζητούμενα της διατριβή.

Το Corda δεν έχει περιττή παγκόσμια ανταλλαγή δεδομένων όπως το τυπικό blockchain, που το κάνει συμβατό με την απαίτηση του GDPR για περιορισμό του διαμοιρασμού των δεδομένων εντός ΕΕ. Σε συνδυασμό με τη δυνατότητα του συστήματος για σχεδιασμό, δημιουργία και λειτουργία κόμβων αποκλειστικά εντός ΕΕ, επιλύεται ένα βασικό πρόβλημα της τεχνολογίας blockchain σε σχέση με το GDPR.

Στο Corda μόνο τα μέρη που έχουν νόμιμη ανάγκη να γνωρίζουν μπορούν να δουν τα δεδομένα μέσα στο πλαίσιο μιας συμφωνίας. Αυτό το χαρακτηριστικό το διαφοροποιεί σε σχέση με το κλασσικό blockchain, όπου οι συναλλαγές κοινοποιούνται σε όλους τους μετέχοντες, έστω και αν τα στοιχεία της ταυτότητας τους είναι hashed. Ουσιαστικά, κατευθύνει τη ροή εργασιών μεταξύ εταιρειών χωρίς να υπάρχει κεντρικός ελεγκτής ενώ ταυτόχρονα επιτυγχάνει συναίνεση μεταξύ των επιχειρήσεων σε επίπεδο επιμέρους συμφωνιών και όχι στο επίπεδο του συστήματος.

Παράλληλα οι συναλλαγές στο Corda επικυρώνονται από τα μέρη της συναλλαγής και όχι από μια ευρύτερη ομάδα μη συνδεδεμένων επικυρωτών (validators), όπως οι miners στο Bitcoin και άλλα blockchain. Επίσης η χρησιμοποίηση ειδικών μηχανισμών του συστήματος όπως τα notary (συμβολαιογράφοι) και oracle που μπορούν να εμπλακούν

στην επικύρωση των συναλλαγών εφόσον τηρούνται κάποιες προσυμφωνημένες συνθήκες/όροι αυξάνουν τη χρηστικότητα του συστήματος. Πέρα από τη μείωση του κινδύνου για διαρροή/υποκλοπή δεδομένων, δίνεται η δυνατότητα για καλύτερη χρήση των έξυπνων συμβολαίων. Η μείωση της ανάγκης χρήσης αξιόπιστων μεσαζόντων, ειδικά στον χρηματοπιστωτικό τομέα, μειώνει το κόστος και τον χρόνο υλοποίησης των συναλλαγών.

Ένα ακόμα πρόβλημα σε σχέση με το GDPR που έχει η τεχνολογία blockchain και στο οποίο απαντάει το Corda είναι η συναίνεση (consensus) για επεξεργασία και αποθήκευση δεδομένων. Υπάρχουν αρκετοί μηχανισμοί και δικλείδες ασφαλείας εκ σχεδιασμού, ενώ το σύστημα επιτρέπει την υιοθέτηση ή σχεδιασμό ακόμα πιο αυστηρών διαδικασιών και μέτρων ανάλογα με τις ανάγκες και επιθυμίες των εταιρειών. Σε αυτό βοηθάει ότι βάσει σχεδιασμού το Corda αποθηκεύει τα ευαίσθητα προσωπικά δεδομένα εκτός δικτύου.

Επιπλέον οι δυνατότητες που δίνει το Corda με την υιοθέτηση της ψηφιακής αυτοκυρίαρχης ταυτότητας (self-sovereign digital identity) σε σχέση με το KYC και την προστασία των προσωπικών δεδομένων είναι τεράστιες. Η κρυπτογράφηση των δεδομένων σε όλο το εύρος του δικτύου και η ελαχιστοποίηση χρήσης του αποκεντρωμένου πλαισίου, απλοποιούν την πρόσβαση σε επαληθευμένη ταυτότητα. Βελτιώνει τις διαδικασίες βεβαίωσης καθ' όλη τη διάρκεια του κύκλου ζωής της ψηφιακής ταυτότητας, ενώ οι χρήστες μπορούν να διαχειρίζονται και να παρακολουθούν ποιοι οργανισμοί μπορούν να έχουν πρόσβαση στα δεδομένα τους. Με αυτόν τον τρόπο καταφέρνει να εξυπηρετεί σε σημαντικό βαθμό τις απαιτήσεις του GDPR, του PSD2 και των ρυθμιστικών αρχών.

Παράλληλα ο σχεδιασμός της Corda επιτρέπει τη δημιουργία και λειτουργία κόμβων ρυθμιστικών και εποπτικών παρατηρητών καλύπτοντας τις εποπτικές απαιτήσεις σε σχέση με ξέπλυμα μαύρου χρήματος, χρηματοδότησης της τρομοκρατίας κ.α.. Με τη βοήθεια της ψηφιακής ταυτότητας και άλλων τεχνολογιών αυτό μπορεί να γίνει χωρίς να υπάρχει σύγκρουση με απαιτήσεις του GDPR.

Στο Corda υπάρχει ευθεία σχέση μεταξύ των γραπτών νομικών εγγράφων σε απλή γλώσσα και του κώδικα των έξυπνων συμβολαίων. Αυτό χρησιμεύει ιδιαίτερα τους χρηματοπιστωτικούς οργανισμούς, λόγω πιο αυστηρού πλαισίου αποδοχής κινδύνου που δεν τους επιτρέπει να εμπλακούν σε οποιαδήποτε συναλλαγή χωρίς την ύπαρξη

νομικά δεσμευτικής συμφωνίας. Η σύνδεση με τα έξυπνα συμβόλαια επιτρέπει να υπάρχει αυτό χωρίς όμως να υπάρχει αυξημένο κόστος και καθυστερήσεις με την εμπλοκή νομικών και άλλων μεσαζόντων.

Ακόμα ένα πλεονέκτημα του Corda είναι ότι είναι χτισμένο πάνω σε ευρέως διαδεδομένη γλώσσα προγραμματισμού (π.χ.Java, JVM) ενώ ταυτόχρονα επιτρέπει την ανάπτυξη εφαρμογών που αυξάνουν την ευχρηστία του σε σχέση με συγκεκριμένες απαιτήσεις διαφόρων κάδων ή μεμονωμένων επιχειρήσεων.

Τέλος η απουσία δικού του κρυπτονομίσματος για χρήση στις συναλλαγές αυξάνει την ευχρηστία, ενώ ταυτόχρονα μειώνει τους κινδύνους (οικονομικούς και ηθικούς) που θα δημιουργούσε η ύπαρξη του.

5.4.4 Τα μειονεκτήματα της εφαρμογής

Η τεχνολογία πίσω από το Corda και την κοινοπραξία R3 που το στηρίζει και δημιούργησε πολλοί ισχυρίζονται ότι δεν είναι blockchain. Η R3 πήρε την υπάρχουσα τεχνολογία των distributed ledger, την εξέλιξε και την προσάρμοσε στις απαιτήσεις των περίπου 200 εταιρειών που μετέχουν στην κοινοπραξία και όχι μόνο. Αυτό έχει δημιουργήσει μία διαμάχη στην επιστημονική και τεχνολογική κοινότητα για το κατά πόσο είναι πραγματικά blockchain η συγκεκριμένη εφαρμογή.

Παρά το γεγονός ότι οι απαιτήσεις του GDPR ικανοποιούνται σε μεγάλο βαθμό, δεν ικανοποιούνται απόλυτα. Καταρχήν ακόμα και αν οι κόμβοι βρίσκονται εντός ΕΕ υπάρχει πρόβλημα σχετικά με το ποια Αρχή Προστασίας Δεδομένων θα είναι αρμόδια. Αν θεωρήσουμε ότι αυτό θα κριθεί ανάλογα με το που βρίσκεται ο σέρβερ που φυλάσσονται τα ευαίσθητα προσωπικά δεδομένα εκτός δικτύου Corda, δημιουργούνται νέα προβλήματα.

Τόσο σε σχέση με το GDPR, όσο σε σχέση με άλλες ρυθμιστικές και ελεγκτικές αρχές η έννοια της αυτοκυρίαρχης ψηφιακής ταυτότητας δεν έχει ακόμα υιοθετηθεί επαρκώς παρά την ύπαρξη του Κανονισμού eIDAS, No 910/2014 για την ψηφιακή ταυτότητα. Η τεχνολογία είναι πιο μπροστά από το νομικό καθεστώς και κυρίως τις δυνατότητες των ρυθμιστικών-ελεγκτικών αρχών. Τυχόν παράκαμψη αυτής της τεχνολογίας δημιουργεί δυνητικά πρόβλημα στο βαθμό συμμόρφωσης της εφαρμογής στις απαιτήσεις του GDPR.

Το Corda, επίσης, παρουσιάζει δύο αδυναμίες σε επίπεδο σχεδιασμού που δημιουργούν ένα ζήτημα σχετικά με προστασία των δεδομένων και ένα σε σχέση με την ασφάλεια του δικτύου. Οι συμβολαιογράφοι (notaries) που επικυρώνουν το περιεχόμενο των συναλλαγών πριν από την επίτευξη συναίνεσης ονομάζονται συμβολαιογράφοι επικύρωσης. Προς το παρόν, ένας επικυρωτικός συμβολαιογράφος μπορεί να επικυρώσει μια συναλλαγή μόνο όταν είναι σε θέση να παρατηρήσει το πλήρες περιεχόμενο της συναλλαγής. Επίσης πρέπει να είναι σε θέση να παρατηρεί τις εξαρτήσεις των συναλλαγών, δηλαδή ολόκληρο το ιστορικό της συναλλαγής μέχρι το σημείο έκδοσης του περιουσιακού στοιχείου. Η δυνατότητα να δει κάποιος το πλήρες περιεχόμενο μιας συναλλαγής θα μπορούσε ενδεχομένως να είναι ένα ζήτημα ιδιωτικότητας, δεδομένου ότι μια συναλλαγή μπορεί να περιέχει ευαίσθητα προσωπικά δεδομένα του πελάτη με αποτέλεσμα να δημιουργηθεί πρόβλημα συμμόρφωσης με το GDPR. Επίσης μπορούν να εξαχθούν εκμεταλλεύσιμα οικονομικά στοιχεία από το ιστορικό και τον όγκο των δεδομένων της συναλλαγής που θα αποτελούσε σοβαρό λειτουργικό κίνδυνο για τον εκάστοτε χρηματοπιστωτικό οργανισμό.[30]

Σε αντίθεση με τους συμβολαιογράφους επικύρωσης, οι μη επικυρωτικοί συμβολαιογράφοι μπορούν να παρατηρήσουν περιορισμένο αριθμό πληροφοριών συναλλαγών. Ένας μη επικυρωτικός συμβολαιογράφος αποθηκεύει έναν ταξινομημένο κατάλογο των αναλωμένων καταστάσεων. Από τη στιγμή που μια συναλλαγή αποστέλλεται σε μη επικυρωτικό συμβολαιογράφο, επαληθεύει εάν η κατάσταση στην οποία αναφέρεται η συναλλαγή έχει δαπανηθεί. Εάν η κατάσταση δεν έχει δαπανηθεί, ενημερώνεται η ταξινομημένη λίστα. Επίσης, οποιαδήποτε συναλλαγή επιχειρήσει να τη δαπανήσει από αυτό το σημείο και μετά, απορρίπτεται.. Είναι σημαντικό να σημειωθεί ότι οι μη επικυρωτικοί συμβολαιογράφοι δεν επαληθεύουν υπογραφές. Αν και η αποκάλυψη περιορισμένων πληροφοριών αντιμετωπίζει το πρόβλημα της ιδιωτικότητας που υπάρχει με τους συμβολαιογράφους επικύρωσης, επιτρέπει επί του παρόντος την επίθεση τύπου denial of state. Για να γίνει αυτό πρέπει να υπάρχουν δύο προϋποθέσεις. Πρώτον, ο κακόβουλος δράστης πρέπει να έχει πρόσβαση στο δίκτυο του Corda και δεύτερον, πρέπει να γνωρίζει τις λεπτομέρειες μιας υπάρχουσας κατάστασης. Κάτω από αυτές τις υποθέσεις ένας κακόβουλος δράστης μπορεί να εκτελέσει μια επίθεση denial of state. Ο κακόβουλος δράστης μπορεί να εκτελέσει την επίθεση δημιουργώντας και υπογράφοντας μια συναλλαγή με το ιδιωτικό του κλειδί. Οι μη επικυρωτικοί συμβολαιογράφοι δεν επαληθεύουν υπογραφές, αλλά επαληθεύουν εάν η κατάσταση

μπορεί να καταναλωθεί. Το αποτέλεσμα αυτής της επίθεσης είναι να μην μπορεί να καταναλωθεί η συγκεκριμένη κατάσταση και άρα ο ιδιοκτήτης του περιουσιακού στοιχείου που αντιπροσωπεύει να μην μπορεί να το χρησιμοποιήσει. Ο ιδιοκτήτης δεν γνωρίζει ότι μια κατάσταση έχει ξοδευτεί μέχρι να προσπαθήσει να την χρησιμοποιήσει, που σημαίνει ότι μπορεί να περάσει μεγάλο χρονικό διάστημα μέχρι να γίνει αντιληπτή η επίθεση [30].

Τέλος η συμμόρφωση με το PSD2 για τη διασύνδεση και πρόσβαση στα οικονομικά δεδομένα των πελατών μέσω API (application programming interface) νέων παρόχων χρηματοπιστωτικών υπηρεσιών, θα μπορούσε να δημιουργήσει προβλήματα συμβατότητας των δεδομένων και κατά συνέπεια ασφάλειας.

Κεφάλαιο 6

Συμπεράσματα

Η τεχνολογία blockchain με την εξέλιξη της έχει δημιουργήσει μια δυναμική που δεν αφήνει αδιάφορο κανέναν κλάδο της οικονομίας, πόσο μάλλον τον χρηματοπιστωτικό κλάδο. Είναι, ίσως, ο πρώτος κλάδος που επηρεάζεται από τις εξελίξεις που φέρνει η υιοθέτηση αυτής της τεχνολογίας. Οι περιορισμοί και οι δεσμεύσεις που επιβάλουν κανονισμοί και νόμοι όπως το GDPR ή το PSD2 αυξάνουν το βαθμό δυσκολίας για την εκμετάλλευση των δυνατοτήτων αυτής της τεχνολογίας.

Στα προηγούμενα κεφάλαια έγινε προσπάθεια να αναλυθούν τα δεδομένα και να προταθεί μια συγκεκριμένη λύση-εφαρμογή που να καλύπτει στο μεγαλύτερο δυνατό βαθμό τα ζητούμενα. Ακολουθεί η παρουσίαση των συμπερασμάτων που εξήχθησαν από τα όσα έχουν προηγηθεί.

6.1 Συμπεράσματα

Η τεχνολογία blockchain ήρθε για να μείνει. Οι επενδύσεις που έχουν γίνει και γίνονται σε διάφορες εφαρμογές της είναι τεράστιες. Ακόμα και αν η τεχνολογία δεν είναι στην αρχική μορφή που έγινε γνωστή μέσω του Bitcoin, τα οφέλη που προσφέρει στην ασφάλεια και την μείωση του χρόνου και κόστους οποιουδήποτε είδους ηλεκτρονικών αλληλεπιδράσεων δεν μπορούν να αγνοηθούν. Μια και ακόμα είμαστε σε πολύ πρώιμο στάδιο της ανάπτυξης της τεχνολογίας, παρουσιάζονται αρκετές «παιδικές ασθένειες». Όσο η έρευνα προχωράει και η προσπάθεια να προσαρμοστεί στις απαιτήσεις της αγοράς και των οργανισμών που χρηματοδοτούν την έρευνα και ανάπτυξη της, θα μειώνονται τα προβλήματα.

Απαντώντας στο τρίτο ερευνητικό ερώτημα, όπως φάνηκε από τα προηγούμενα κεφάλαια, οι απαιτήσεις του χρηματοπιστωτικού τομέα σε συνδυασμό με τις ρυθμιστικές και κανονιστικές απαιτήσεις (GDPR, PSD2 κ.α.), δεν μπορούν να καλυφθούν από την αρχική μορφή του blockchain. Ειδικά τα ανοικτού τύπου χωρίς έγκριση (permissionless) κατανεμημένα καθολικά έρχονται σε ευθεία αντίθεση με αρκετές απαιτήσεις του κανονισμού GDPR, όπως και ρυθμιστικών απαιτήσεων για το ξέπλυμα μαύρου χρήματος.

Απαντώντας και στο δεύτερο ερευνητικό ερώτημα η προσέγγιση που φαίνεται να επικρατεί στον χρηματοπιστωτικό κλάδο είναι τροποποιημένο DLT (Distributed Ledger Technology) που απαιτεί έγκριση (permissioned) που αναπτύσσονται από κοινοπραξίες εταιρειών του κλάδου και όχι μόνο. Αν και θα μπορούσαν να χρησιμοποιήσουν ιδιωτικά blockchain για να καλύψουν τις απαιτήσεις του GDPR, θα ακυρώνονταν σε μεγάλο βαθμό τα οφέλη του χαμηλότερου κόστους, ενώ δημιουργούνται προβλήματα εφαρμογής σε σχέση με το PSD2. Η δημιουργία κοινοπραξιών βοηθάει στο διαμοιρασμό του κόστους για την έρευνα και την ανάπτυξη κοινών λύσεων. Το μεγάλο κίνητρο για τον χρηματοπιστωτικό κλάδο σε σχέση με την υιοθέτηση της τεχνολογίας κατανεμημένου καθολικού DLT είναι η μείωση αν όχι εξάλειψη των μεσαζόντων.

Είναι προφανές ότι ακόμα και λύσεις όπως το Corda που δημιουργήθηκε με σαφή προσανατολισμό στον χρηματοπιστωτικό τομέα, δεν είναι πλήρεις. Υπάρχουν ακόμα ερωτηματικά για το κατά πόσο πληρούν το σύνολο των απαιτήσεων της νομοθεσίας, αλλά και τις πολύ υψηλές απαιτήσεις ασφάλειας που έχουν οι εταιρείες του κλάδου. Σε συνδυασμό με την πίεση που ασκείται από εταιρείες από άλλους κλάδους που πλέον έχουν δικαίωμα να προσφέρουν χρηματοπιστωτικές υπηρεσίες, το τοπίο δυσκολεύει.

Οι λεγόμενες «Big Tech» εταιρείες έχουν τη δυνατότητα να προσφέρουν υπηρεσίες με πολύ μικρότερο κόστος χωρίς να χρειάζεται να ανακαλύψουν τον τροχό όσον αφορά την τεχνολογία που θα χρησιμοποιήσουν. Το συγκριτικό πλεονέκτημα που έχουν στον τεχνολογικό τομέα με τεράστιες δυνατότητες διαχείρισης μεγάλου όγκου δεδομένα (big data analytics) σε συνδυασμό με τις απαιτήσεις του PSD2 για διαμοιρασμό των οικονομικών στοιχείων, δημιουργούν υπαρξιακό κίνδυνο για τις παραδοσιακές εταιρείες του κλάδου (π.χ. τράπεζες). Η υιοθέτηση τεχνολογιών fintech και ο συνδυασμός τους με τεχνολογίες διανεμημένου καθολικού DLT, είναι η πλέον δημοφιλής λύση για να κρατήσουν σημαντικό μερίδιο της αγοράς μειώνοντας το κόστος των υπηρεσιών τους και προσφέροντας ταχύτερες υπηρεσίες.

Πέρα από την όποια υστέρηση της τεχνολογίας, μεγάλο πρόβλημα αποτελεί το νομικό-κανονιστικό καθεστώς που διέπει τον κλάδο. Πολλές φορές οι κανονισμοί δυσχεραίνουν την υιοθέτηση καινοτόμων τεχνολογικών λύσεων είτε γιατί η νομοθεσία δεν είχε προβλέψει τις αλλαγές που αυτές μπορεί να επιφέρουν, είτε γιατί οι ελεγκτικοί μηχανισμοί προσαρμόζονται στα νέα δεδομένα με πολύ αργούς ρυθμούς.

Ειδικότερα σε σχέση με το GDPR, παρά το γεγονός ότι αποτελεί τεράστιο βήμα για την προστασία των προσωπικών δεδομένων, είναι προφανές ότι θα πρέπει όσο η τεχνολογία εξελίσσεται να προσαρμόζεται και ο κανονισμός. Όταν ξεκίνησε να σχεδιάζεται ο κανονισμός έννοιες όπως η αυτοκυρίαρχη ψηφιακή ταυτότητα ήταν άγνωστες, ενώ το blockchain και τα DLT ήταν σε βρεφικό στάδιο. Θα πρέπει παράλληλα με την τεχνολογία να εξελίσσεται και η νομοθεσία ή να προβλέπει τις διαφοροποιήσεις που μπορούν να προκύψουν.

Όσον αφορά το πρώτο ερευνητικό ερώτημα σε σχέση με τα προσωπικά δεδομένα η λύση που προσφέρει το Blockchain και ειδικά το Corda είναι ίσως η μοναδική που συνδυάζει

την ανωνυμία εκ σχεδιασμού με την μείωση του χρόνου για τη διεκπεραίωση μιας συναλλαγής. Μπορεί να υπάρχουν άλλες τεχνολογίες που να είναι πιο ασφαλείς ή πιο γρήγορες, αλλά δύσκολα συνδυάζουν και τα δύο εξ΄ ορισμού και εκ' σχεδιασμού. Οι όποιες αδυναμίες σε σχέση με τις απαιτήσεις του GDPR ή του PSD2 και των κανονιστικών/ρυθμιστικών απαιτήσεων του χρηματοπιστωτικού κλάδου, μπορούν να απαντηθούν όσο η τεχνολογία εξελίσσεται.

Η τακτική της ΕΕ να δημιουργεί πολύπλοκα ρυθμιστικά πλαίσια για κάθε έκφανση της κοινωνικής και οικονομικής ζωής, πολλές φορές έχει τα αντίθετα από τα επιδιωκόμενα αποτελέσματα. Αν το αποτέλεσμα του αυξημένου κόστους και χρόνου που απαιτείται από τους παραδοσιακούς χρηματοπιστωτικούς οργανισμούς οδηγήσει στην κυριαρχία των μεγάλων τεχνολογικών εταιρειών, ο ζημιωμένος θα είναι ο πολίτης. Ήδη κυριαρχούν στις υπόλοιπες εκφάνσεις της ψηφιακής δραστηριότητας/ζωής, συλλέγοντας τεράστιο όγκο δεδομένων για όλους. Αν γίνουν ολιγοπώλιο και στις χρηματοπιστωτικές υπηρεσίες, όσο και να συμμορφώνονται με τις ρυθμιστικές απαιτήσεις αυτό μακροπρόθεσμα θα δημιουργήσει μεγαλύτερα προβλήματα.

Τέλος μεγάλο ερωτηματικό για οποιαδήποτε τεχνολογία συμπεριλαμβάνει κρυπτογραφία αποτελεί η έλευση των κβαντικών επεξεργαστών. Κανείς δεν μπορεί να εγγυηθεί ότι με τις δυνατότητες που θα προκύψουν, θα αντέξει οποιαδήποτε σημερινή τεχνολογία κρυπτογραφίας και ειδικά η ασύμμετρη που εφαρμόζεται στο blockchain. Πέρα από τα όποια σημερινά προβλήματα πρέπει να ξεπεραστούν, θα πρέπει να είμαστε έτοιμοι για τις προκλήσεις του μέλλοντος. Χωρίς αποτελεσματική κρυπτογραφία δεν μπορούν να υπάρξουν ασφαλείς συναλλαγές, προσωπικά δεδομένα, κατανεμημένα καθολικά, ανάπτυξη του fintech.

Παραπομπές/Βιβλιογραφία

Παραπομπές

[1] Kagan, Julia. "Financial Technology – Fintech Definition." Investopedia. Accessed November 21, 2019. https://www.investopedia.com/terms/f/fintech.asp.

[2] "Financial Technology." In Wikipedia, November 15, 2019. https://en.wikipedia.org/w/index.php?title=Financial_technology&oldid=926326366.

[3] E. C. Bank, "Τι είναι οι τράπεζες χρηματοοικονομικής τεχνολογίας (fintech) και πώς επηρεάζουν τις χρηματοπιστωτικές υπηρεσίες;," European Central Bank - Banking Supervision. [Online]. Available: https://www.bankingsupervision.europa.eu/about/ssmexplained/html/fintech.el.html.

[4] R. Buckley, D. Arner, and J. Barberis, "150 Years of FinTech: An Evolutionary Analysis," JASSA - The FINSIA Journal of Applied Finance, Jan. 2016.

[5] O. C.-U. Piattelli, "EBA Report highlights the impact of FinTech on payment services and electronic money business models | Lexology." [Online]. Available: https://www.lexology.com/library/detail.aspx?g=ddbabb7e-4f95-4757-bf01-3ba9132b1efe

[6] EBA REPORT ON THE IMPACT OF FINTECH ON PAYMENT INSTITUTIONS' AND E-MONEY INSTITUTIONS' BUSINESS MODELS, July 2019, https://eba.europa.eu/sites/default/documents/files/documents/10180/2551996/32ff1cbb-a6c3-4a01-94f2-4d129386fa0a/EBA%20thematic%20report%20on%20the%20impact%20of%20FinTech%20on%20PIs%27%20and%20EMIs%27%20business%20models.pdf?retry=1

[7] "Ευρωπαϊκή Οδηγία σχετικά με τις υπηρεσίες πληρωμών (PSD2)." [Online]. Available: https://www.bankofcyprus.com.cy/home-gr/bank_gr/forms_gr/PSD-gr/

[8] European Banking Authority (2017). Consultation Paper RTS Final Report. [ONLINE] https://www.eba.europa.eu/documents/10180/1761863/Final+draft+RTS+on+SCA+and+CSC+under+PSD2+ %28EBA-RTS-2017-02%29.pdf

[9] Deloitte, "Open banking and PSD2," p. 36,2019, https://www2.deloitte.com/content/dam/Deloitte/cz/Documents/financial-services/cz-open-banking-and-psd2.pdf

[10] «ΚΑΝΟΝΙΣΜΌΣ (ΕΕ) 2016/679 ΤΟΥ ΕΥΡΩΠΑΪΚΟΎ ΚΟΙΝΟΒΟΥΛΊΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΊΟΥ της 27ης Απριλίου 2016» [Online]. Available: https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:32016R0679&from=EL

[11] "Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα." [Online]. Available: http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/page0a_gr/page0a_gr?OpenDocument&ExpandSection=3%2C2#_Section3.

[12] Ομάδα Εργασίας ΣΕΒ «Προστασία Προσωπικών Δεδομένων», "Ο νέος Γενικός Κανονισμός για την Προστασία Δεδομένων(GDPR)Εφαρμογή και προκλήσεις για τις επιχειρήσεις στην εποχή της ψηφιοποίησης", Αθήνα, 2018, http://www.sev.org.gr/Uploads/Documents/51628/meleti_sev_GDPR_final.pdf

[13] "Πως ο GDPR θα επηρεάσει την πολιτική προστασίας των δεδομένων σας," Eset GR. [Online]. Available: https://encryption.eset.com/gdpr-compliance

[14] A. Bourka, P. Drogkaris, European Union, and Agency for Network and Information Security, "Recommendations on shaping technology according to GDPR provisions: exploring the notion of data protection by default." 2018.

[15] ΟΜΑΔΑ ΕΡΓΑΣΙΑΣ ΤΟΥ ΑΡΘΡΟΥ 29 ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ, «Κατευθυντήριες γραμμές για την εφαρμογή και τον καθορισμό διοικητικών προστίμων για τους σκοπούς του κανονισμού 2016/679», 2017
https://www.dpa.gr/pls/portal/docs/PAGE/APDPX/GDPR/FILES%20GDPR/WP253_EL.PDF

[16] Θανάσης Δαβαλάς, newdream.gr. "Τι είναι η τεχνολογία Blockchain. Πλήρης Οδηγός." Dreamweaver.Gr (blog), March 6, 2018. https://www.dreamweaver.gr/blockchain.php.

[17] "Satoshi Nakamoto." In Wikipedia, November 14, 2019.
https://en.wikipedia.org/w/index.php?title=Satoshi_Nakamoto&oldid=926098841.

[18] BlockchainHub. "Smart Contracts." Accessed November 22, 2019. https://blockchainhub.net/smart-contracts/.

[19] "Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data | CNIL." [Online]. Available: https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data

[20] Marta Piekarska, Michael Lodder, Zachary Larson, and Kaliya Young, "When GDPR becomes real, and Blockchain is no longer Fairy Dust," 2018.

[21] E. Politou, E. Alepis, and C. Patsakis, "Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions," Journal of Cybersecurity, vol. 4, no. 1, Jan. 2018,

[22] Ευρωπαϊκή Επιτροπή, «Σχέδιο δράσης για τη χρηματοοικονομική τεχνολογία: Για έναν πιο ανταγωνιστικό και καινοτόμο ευρωπαϊκό χρηματοπιστωτικό τομέα», 2018, https://eur-lex.europa.eu/resource.html?uri=cellar:6793c578-22e6-11e8-ac73-01aa75ed71a1.0018.02/DOC_1&format=PDF

[23] EBA, "REPORT ON PRUDENTIAL RISKS AND OPPORTUNITIES ARISING FOR INSTITUTIONS FROM FINTECH", 2018,
https://eba.europa.eu/sites/default/documents/files/documents/10180/2270909/02c7859f-576e-421e-b243-a145c0eaa131/Report%20on%20prudential%20risks%20and%20opportunities%20arising%20for%20institutions%20from%20FinTech.pdf

[24] "Distributed Ledger Technology & Cybersecurity - Improving information security in the financial sector — ENISA." [Online]. Available: https://www.enisa.europa.eu/publications/blockchain-security

[25] Mike Hearn, Richard Gendal Brown, "Corda: A distributed ledger", 2019, https://www.r3.com/wp-content/uploads/2019/08/corda-technical-whitepaper-August-29-2019.pdf

[26] Peter Gratzke, David Schatsky, and Eric Piscini, "Banding together for blockchain", Deloitte University Press, 2017, https://www2.deloitte.com/us/en/insights/focus/signals-for-strategists/emergence-of-blockchain-consortia.html

[27] A. Doychev, "The Complicated Relationship of Blockchains, DLT and GDPR," Medium, Sep. 02, 2019. https://medium.com/industria-tech/https-medium-com-industria-tech-the-complicated-relationship-of-blockchains-2888c04b3e9b.

[28] R3, Corda,"Welcome to Corda !" Jan. 08, 2020. https://docs.corda.net/docs/corda-os/4.4.html

[29] "Meet Cordentity!," Corda, Jan. 18, 2019. https://www.corda.net/blog/meet-cordentity/

[30] T. Koens, S. King, C. van Wijk, and A. Koren, "*Solutions for the Corda Security and Privacy Trade-off: Having Your Cake and Eating It,*" p. 10, 2019.

[31] Woo Young Moon and Soo Dong Kim, *"A Payment Mediation Platform for heterogeneous FinTech schemes"* in 2016 IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), Xi'an, China, 2016, pp. 511–516.

[32] Polyviou A., Velanas P., and Soldatos J., "*Blockchain Technology: Financial Sector Applications Beyond Cryptocurrencies,*" Proceedings, vol. 28, no. 1, p. 7, Oct. 2019.

[33] Financial Stability Board (FSB), "*Financial Stability Implications from FinTech: Supervisory and Regulatory Issues that Merit Authorities' Attention*," p. 65, 2017

[34] M. Finck, European Parliament, and Directorate-General for Parliamentary Research Services, Blockchain and the general data protection regulation: Can distributed ledgers be squared with European data protection law. 2019. https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf

[35]N. Reiff, "What is the Biggest Security Threat to Ripple Cryptocurrency?," Investopedia. https://www.investopedia.com/news/what-biggest-security-threat-ripple-cryptocurrency/ (accessed Jun. 05, 2020).

Βιβλιογραφία

N. B. Truong, K. Sun, G. M. Lee and Y. Guo, "GDPR-Compliant Personal Data Management: A Blockchain-Based Solution," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 1746-1761, 2020.

T. Swanson, "'There have been a few different start-ups trying to create basically their own blockchains with specific use-cases. In our view we feel that kind of defeats the purpose of having a network itself because it just recreates silos.'3," p. 3.

Ameer Rosic, "17 Blockchain Applications That Are Transforming Society," Blockgeeks, 07-Mar-2017. [Online]. Available: https://blockgeeks.com/guides/blockchain-applications/.

G. Karamanolis, "Ασχολήσου με το fintech! Οι δύο ευκαιρίες στην Ελλάδα και στην Κύπρο.," Medium, 26-Aug-2018. [Online]. Available: https://medium.com/the-crowdpolicy-collection/m%CE%B7%CE%BD-%CF%87%CE%AC%CE%BD%CE%B5%CE%B9%CF%82-%CE%B5%CF%85%CE%BA%CE%B1%CE%B9%CF%81%CE%AF%CE%B5%CF%82-%CE%B1%CF%83%CF%87%CE%BF%CE%BB%CE%AE%CF%83%CE%BF%CF%85-%CE%BC%CE%B5-%CF%84%CE%BF-fintech-637dd32817

"Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα." [Online]. Available: http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/762DC741383135AEC22582480036C631?OpenDocument.

"Ευρωπαϊκή Οδηγία σχετικά με τις υπηρεσίες πληρωμών (PSD2)." [Online]. Available: https://www.bankofcyprus.com.cy/home-gr/bank_gr/forms_gr/PSD-gr/.

"Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ, vol. 119. 2016. https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016R0679&from=EL

"Σε ποιους εφαρμόζεται η νομοθεσία περί προστασίας των δεδομένων;," Ευρωπαϊκή Επιτροπή - European Commission. [Online]. Available: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/who-does-data-protection-law-apply_el.

M. Raikwar, S. Mazumdar, S. Ruj, S. Sen Gupta, A. Chattopadhyay, and K.-Y. Lam, "A Blockchain Framework for Insurance Processes," in 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris, 2018, pp. 1–4.

M. Banerjee, J. Lee, and K.-K. R. Choo, "A blockchain future to Internet of Things security: A position paper," Digital Communications and Networks, Oct. 2017.

Silvan Jongerius, TechGDPR, "A primer to GDPR, blockchain, and the Seven Foundational Principles of Privacy by Design. .pdf.", 2018, https://techgdpr.com/wp-content/uploads/2018/12/PbD-GDPR-Blockchain-SilvanJongerius-v1.2.pdf

13th November 2018, "A question of compatibility: blockchain and the GDPR," FinTech Futures. [Online]. Available: https://www.fintechfutures.com/2018/11/a-question-of-compatibility-blockchain-and-the-gdpr/

D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, "A review on consensus algorithm of blockchain," in 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Banff, AB, 2017, pp. 2567–2572.

X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," Future Generation Computer Systems, Aug. 2017.

W. (Derek) Du, S. L. Pan, D. E. Leidner, and W. Ying, "Affordances, experimentation and actualization of FinTech: A blockchain implementation study," The Journal of Strategic Information Systems, Nov. 2018.

A. J. Diaz-Honrubia et al., "An Overview of the CUREX Platform," in 2019 IEEE 32nd International Symposium on Computer-Based Medical Systems (CBMS), Cordoba, Spain, 2019, pp. 162–167.

M. H. Miraz and D. C. Donald, "Application of Blockchain in Booking and Registration Systems of Securities Exchanges," in 2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE), Southend, United Kingdom, 2018, pp. 35–40.

G. Karame and E. Androulaki, Bitcoin and Blockchain Security. Norwood, MA: Artech House, 2016.

Π. Γιαλούρης, "Bitcoin: Η καινοτομία του κρυπτονομίσματος - Κίνδυνοι και ευκαιρίες στο σύγχρονο επιχειρηματικό περιβάλλον," Sep. 2017.

Σ. Χαριζάνης, "Blockchain - Αποκεντρωμένο Σύστημα Πιστοποίησης Συναλλαγών," Sep. 2017.

Hayes Adam and Tasca Paolo, "Blockchain and Crypto-currencies," The FinTech Book, Mar. 2016.

"Blockchain and Cryptocurrency," Breaking Digital Gridlock, Feb. 2018.

"Blockchain and GDPR: Can they Live under One Roof?," OpenLedger Insights, 23-May-2019. .

M. Slaughter, "Blockchain and the GDPR: reconcilable differences?," p. 5.

M. Finck, European Parliament, and Directorate-General for Parliamentary Research Services, Blockchain and the general data protection regulation: Can distributed ledgers be squared with European data protection law. 2019.

L. W. Cong and Z. He, "Blockchain Disruption and Smart Contracts," The Review of Financial Studies, vol. 32, no. 5, pp. 1754–1797, May 2019.

Hasib Anwar, “Blockchain GDPR Paradox: Rising Conflict Between Law and Technology?”, 2018, [Online]. Available: https://101blockchains.com/blockchain-gdpr/

S. Ølnes, J. Ubacht, and M. Janssen, “Blockchain in government: Benefits and implications of distributed ledger technology for information sharing,” Government Information Quarterly, vol. 34, no. 3, pp. 355–364, Sep. 2017.

P. Treleaven, R. G. Brown, and D. Yang, “Blockchain Technology in Finance,” Computer, vol. 50, no. 9, pp. 14–17, 2017.

M. Crosby, “BlockChain Technology: Beyond Bitcoin,” no. 2, p. 16, 2016.

I. Eyal, “Blockchain Technology: Transforming Libertarian Cryptocurrency Dreams to Finance and Banking Realities,” Computer, vol. 50, no. 9, pp. 38–49, 2017.

P.-W. Chen, B.-S. Jiang, and C.-H. Wang, “Blockchain-based payment collection supervision system using pervasive Bitcoin digital wallet,” in 2017 IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Rome, 2017, pp. 139–146.

N. Kshetri, “Blockchain’s roles in strengthening cybersecurity and protecting privacy,” Telecommunications Policy, vol. 41, no. 10, pp. 1027–1038, Nov. 2017.

Morgen E. Peck, “Blockchains How They Work And Why They’ll Change The World - IEEE Spectrum,” IEEE Spectrum: Technology, Engineering, and Science News. [Online]. Available: https://spectrum.ieee.org/computing/networks/blockchains-how-they-work-and-why-theyll-change-the-world.

Van Lier Ben, “Can Cyber-Physical Systems Reliably Collaborate within a Blockchain?” Metaphilosophy, vol. 48, no. 5, pp. 698–711, Oct. 2017.

B. B. Klinger, “Compliance with Data Protection Regulations by Applying the Blockchain Technology,” in The RegTech Book, 1st ed., J. Barberis, D. W. Arner, and R. P. Buckley, Eds. Wiley, 2019.

Bartłomiej Klinger, “Compliance with Data Protection Regulations by Applying the Blockchain Technology - The RegTech Book - Wiley Online Library.” [Online]. Available: https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781119362197.ch46.

H. Neng, “Construction of High-Availability Bank System in Virtualized Environments,” in 2017 IEEE Second International Conference on Data Science in Cyberspace (DSC), Shenzhen, China, 2017, pp. 561–568.

Maull Roger, Godsiff Phil, Mulligan Catherine, Brown Alan, and Kewell Beth, “Distributed ledger technology: Applications and implications,” Strategic Change, vol. 26, no. 5, pp. 481–489, Sep. 2017.

D. A. Freund, “Economic incentives and Blockchain security,” Journal of Securities Operations & Custody, vol. 10, no. 1, pp. 67–76, Jan. 2018.

J. Villasenor, “Ensuring Cybersecurity In Fintech: Key Trends And Solutions,” Forbes. [Online]. Available: https://www.forbes.com/sites/johnvillasenor/2016/08/25/ensuring-cybersecurity-in-fintech-key-trends-and-solutions/

H. C. Lim, “Enterprises and Future Disruptive Technological Innovations: Exploring Blockchain Ledger Description Framework (BLDF) for the Design and Development of Blockchain Use Cases,” in Advances in Information and Communication, 2020, pp. 533–540.

“European Commission - PRESS RELEASES - Press release - Questions and Answers – General Data Protection Regulation.” [Online]. Available: https://europa.eu/rapid/press-release_MEMO-18-387_en.htm.

Aafaf Ouaddah, Anas Abou Elkalam, Abdellah Ait Ouahman, “FairAccess: a new Blockchain-based access control framework for the Internet of Things - Ouaddah - 2016 - Security and Communication Networks - Wiley Online Library.” [Online]. Available: https://onlinelibrary.wiley.com/doi/10.1002/sec.1748.

T.-C. Chang and Y.-L. Chen, “Fintech Puzzle: The Case of Bitcoin,” in 2018 Portland International Conference on Management of Engineering and Technology (PICMET), Honolulu, HI, 2018, pp. 1–6.

White Gareth R.T., “Future applications of blockchain in business and management: A Delphi study,” Strategic Change, vol. 26, no. 5, pp. 439–451, Sep. 2017.

M.-L. Marsal-Llacuna, “Future living framework: Is blockchain the next enabling network?,” Technological Forecasting and Social Change, vol. 128, pp. 226–234, Mar. 2018.

Alex Don, “GDPR & FinTechs: A Competitive Advantage?,” Deloitte United Kingdom. [Online]. Available: https://www2.deloitte.com/uk/en/pages/financial-services/articles/is-gdpr-a-competitive-advantage-for-fintechs.html.

“General Data Protection Regulation (GDPR) – Official Legal Text,” General Data Protection Regulation (GDPR). [Online]. Available: https://gdpr-info.eu/.

N. Al-Zaben, M. M. Hassan Onik, J. Yang, N.-Y. Lee, and C.-S. Kim, “General Data Protection Regulation Complied Blockchain Architecture for Personally Identifiable Information Management,” in 2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE), Southend, United Kingdom, 2018, pp. 77–82.

B. D. Journal, “Here’s how GDPR and the blockchain can coexist,” The Next Web, 26-Jul-2018. [Online]. Available: https://thenextweb.com/syndication/2018/07/26/gdpr-blockchain-cryptocurrency/

C. DeCusatis, M. Zimmermann, and A. Sager, “Identity-based network security for commercial blockchain services,” in 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), 2018, pp. 474–477.

D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, “The Blockchain as a Decentralized Security Framework [Future Directions],” IEEE Consumer Electron. Mag., vol. 7, no. 2, pp. 18–21, Mar. 2018.

M. El-Masri, K. Al-Yafi, and K. S. Sherif, “The Digital Transformation of FinTech: Disruptions and Value Paths,” p. 14, 2019.

R. Adams, G. Parry, P. Godsiff, and P. Ward, “The future of money and further applications of the blockchain,” Strategic Change, vol. 26, no. 5, pp. 417–422, Sep. 2017.

Y. Zhao and B. Duncan, “The Impact of Crypto-Currency Risks on the Use of Blockchain for Cloud Security and Privacy,” in 2018 International Conference on High Performance Computing & Simulation (HPCS), Orleans, 2018, pp. 677–684.

G. Dusil and D. Cerny, “The Next Evolution in Funding Innovation,” in 2018 International Joint Conference on Neural Networks (IJCNN), Rio de Janeiro, 2018, pp. 1–4.

V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, and V. Santamaria, “To Blockchain or Not to Blockchain: That Is the Question,” IT Prof., vol. 20, no. 2, pp. 62–74, Mar. 2018.

G. W. Peters and E. Panayi, “Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money,” in Banking Beyond Banks and Money, Springer, Cham, 2016, pp. 239–278.

Jesse Yli-Huumo, Deokyoon Ko, Sujin Choi, Sooyong Park, Kari Smolander, “Where Is Current Research on Blockchain Technology?—A Systematic Review.” [Online]. Available: http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0163477.