ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΗΛΕΚΤΡΙΚΩΝ ΒΙΟΜΗΧΑΝΙΚΩΝ ΔΙΑΤΑΞΕΩΝ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΑΠΟΦΑΣΕΩΝ

Ανάλυση τεχνολογίας Blockchain για την υλοποίηση πληροφοριακού συστήματος διαχείρισης ευαίσθητων ιατρικών δεδομένων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Ιωάννης Παναγόπουλος

Επιβλέπων : Δημήτριος Ασκούνης
Καθηγητής Ε.Μ.Π.

Αθήνα, Οκτώβριος 2019

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΗΛΕΚΤΡΙΚΩΝ ΒΙΟΜΗΧΑΝΙΚΩΝ ΔΙΑΤΑΞΕΩΝ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΑΠΟΦΑΣΕΩΝ

Ανάλυση τεχνολογίας Blockchain για την υλοποίηση πληροφοριακού συστήματος διαχείρισης ευαίσθητων ιατρικών δεδομένων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Ιωάννης Παναγόπουλος

Επιβλέπων : Δημήτριος Ασκούνης
Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 3η Οκτωβρίου 2019.

.....	.....	.....
Δημήτριος Ασκούνης	Ιωάννης Ψαρράς	Χρυσόστομος Δούκας
Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.	Αν. Καθηγητής Ε.Μ.Π.

Αθήνα, Οκτώβριος 2019

.....

Ιωάννης Παναγόπουλος

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

Ευχαριστίες

Η εκπόνηση της παρούσας διπλωματικής εργασίας έγινε κατά το ακαδημαϊκό έτος 2018 – 2019 στον τομέα Ηλεκτρικών Βιομηχανικών Διατάξεων και Συστημάτων Αποφάσεων της Σχολής Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Εθνικού Μετσόβιου Πολυτεχνείου, στα πλαίσια των ερευνητικών δραστηριοτήτων του Εργαστηρίου Συστημάτων Αποφάσεων και Διοίκησης.

Υπεύθυνος για τη διπλωματική εργασία ήταν ο Καθηγητής κ. Δημήτριος Ασκούνης, τον οποίο θα ήθελα να ευχαριστήσω για την ανάθεση της, καθώς και για την ευκαιρία που μου δόθηκε να ασχοληθώ με ένα τόσο ενδιαφέρον θέμα.

Θα ήθελα επίσης να ευχαριστήσω τον κ. Χρήστο Κοντζίνο, υποψήφιο διδάκτορα του εργαστηρίου Συστημάτων Αποφάσεων, για την άψογη συνεργασία που είχαμε και τη συνεχή του καθοδήγηση καθ' όλη τη διάρκεια εκπόνησης της παρούσας διπλωματικής εργασίας. Θα ήθελα να ευχαριστήσω επίσης την οικογένειά μου για την στήριξη που μου παρείχε σε όλη τη διάρκεια των σπουδών μου.

Τέλος απευθύνω θερμές ευχαριστίες σε όλο το διδακτικό προσωπικό του Εθνικού Μετσόβιου Πολυτεχνείου για τις γνώσεις που μου παρείχαν όλα αυτά τα χρόνια

Αθήνα, Οκτώβριος 2019

Ιωάννης Παναγόπουλος

Περίληψη

Σκοπός αυτής της εργασίας είναι η περιγραφή, η κατανόηση και η ανάλυση της τεχνολογίας Blockchain καθώς και η σύνδεσή της με τη διαχείριση των ευαίσθητων ιατρικών δεδομένων.

Στο πλαίσιο της διπλωματικής διευκρινίζεται τι είναι ο Ηλεκτρονικός Φάκελος Υγείας, περιγράφονται τα χαρακτηριστικά του, το περιεχόμενό του, η χρησιμότητά του για ασθενείς και γιατρούς και αναφέρονται τα πλεονεκτήματα και τα μειονεκτήματά του. Αναλύεται επίσης το νομοθετικό πλαίσιο που προστατεύει τα ευαίσθητα προσωπικά και θεμελιώδη δεδομένα των ασθενών σε ευρωπαϊκό και πανελλαδικό επίπεδο.

Εκτενέστερη ανάλυση γίνεται στον τρόπο με τον οποίο θα μπορούσε η τεχνολογία Blockchain να διαχειριστεί την ιατρική πληροφορία ούτως ώστε να αξιοποιηθούν πλήρως οι δυνατότητες των ιατρικών δεδομένων. Επιπλέον, παρουσιάζονται και αναλύονται εφαρμογές που δραστηριοποιούνται στον τομέα της υγειονομικής περίθαλψης και τέλος, περιγράφονται πιθανά σενάρια χρήσης μιας Blockchain εφαρμογής στον τομέα της υγείας και προσδιορίζονται οι λειτουργικές της απαιτήσεις.

Λέξεις κλειδιά : Blochchain, Ethereum, Ηλεκτονικός Φάκελος Υγείας, GDPR, έξυπνα συμβόλαια, επεκτασιμότητα, εφαρμογές υγείας, ιατρικά δεδομένα

Abstract

The purpose of this work is to describe, understand and analyze Blockchain technology and its association with the management of sensitive medical data.

It specifies what the Electronic Health Record is, describes its features, its content, its usefulness to patients and doctors and describes its advantages and disadvantages. It also analyzes the legal framework that protects sensitive personal and fundamental patient data at European and national level.

More detailed analysis is performed on how Blockchain technology could manage medical information in order to fully exploit its potential. Applications in the field of healthcare are presented and analyzed. Finally, possible use cases are described for using a Blockchain application in the healthcare domain along with its potential functional requirements.

Keywords: Blochchain, Ethereum, Electronic Health Record, smart contracts, scalability, health applications, medical data

Πίνακας Περιεχομένων

Ευρετήριο Εικόνων

Ακρωνύμια

Ακρωνύμιο	**Μετάφραση**
ΗΦΥ	Ηλεκτρονικός Φάκελος Υγείας
ΗΙΦΑ	Ηλεκτρονικός Ιατρικός Φάκελος Ασθενούς
ΗΙΦ	Ηλεκτρονικός Ιατρικός Φάκελος
ΗΥ	Ηλεκτρονικό Υπολογιστή
ΦΠΑ	Φόρος Προστιθέμενης Αξίας
ΕΕ	Ευρωπαϊκή Ένωση
ΕΚΤ	Ευρωπαϊκή Κεντρική Τράπεζα
ΣΛΕΕ	Συνθήκη Λειτουργίας Ευρωπαϊκής Ένωσης
ΕΣΔΑ	Ευρωπαϊκή Σύμβαση Δικαιωμάτων
ΣτΕ	Συμβούλιο της Επικρατείας
ΕΟΧ	Ευρωπαϊκού Οικονομικού Χώρου
ΕΚ	Ευρωπαϊκή Κοινότητα
ΑΠΔΠΧ	Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
ΥΠΔ	Υπεύθυνος Προστασίας Δεδομένων
IOM	Institute of Medicine
CPR	Computer-based Patient Record
SOAP	Subjective Objective Assessment Plan
GDPR	General Data Protection Regulation
ICO	Initial Coin Offering
P2P	peer-to-peer
CNIL	Commission Nationale de l'Informatique et des Libertes
DPO	Data Protection Officer
DPIA	Data Protection Impact Assessment
ROT	Redundant Obsolete Trivial
ROI	Return On Investment
Dapp	Decentralized Application
DAO	Decentralized Autonomous Organization
DAC	Decentralized Autonomous Corporation
IoT	Internet of Things
EVM	Ethereum Virtual Machine
API	Application Programming Interface
UI	User Interface
EMR	Electronic Medical Record
EHR	Electronic Health Record
EHRs	Electronic Health Records
HIPAA	Health Insurance Portability and Accountability Act)
RPC	Remote Procedural Call
AI	Artificial Intelligence
CRUD	Create Read Update Delete

1 Ηλεκτρονικός Φάκελος Υγείας

1.1 Εισαγωγή

Στην εποχή μας η εξέλιξη στον τεχνολογικό τομέα έχει οδηγήσει στη συνεχώς αυξανόμενη ανάγκη παροχής καλύτερων υπηρεσιών σε διάφορους τομείς οι οποίοι παραδοσιακά λειτουργούν χωρίς υποστήριξη από ψηφιακά συστήματα. Συγκεκριμένα, στον τομέα της υγείας, η εξέλιξη αυτή συντέλεσε στην έρευνα νέων εργαλειών παροχής ανταγωνιστικότερων υπηρεσιών υγείας με στόχο την καλύτερη παροχή φροντίδας στους ασθενείς, την αποσυμφόρηση των ιατρών, νοσοκομείων και δημόσιων υπηρεσιών αλλά και την παροχή ηλεκτρονικών υπηρεσιών, όπως είναι η συνταγογράφηση και η γνωμάτευση ενός γιατρού όντας σε κάποια απομακρυσμένη περιοχή. Βέβαια όλα αυτά συντελούνται με βασικό γνώμονα την ελαχιστοποίηση του κόστους καθώς και την μεγιστοποίηση του κέρδους.

Σε αυτή την κατεύθυνση οι αρμόδιοι οργανισμοί παροχής υγείας συνειδητοποίησαν ότι η τεχνολογία της Πληροφορικής θα μπορούσε από ένα διαδικαστικού τύπου εργαλείο να καταλάβει πρωταγωνιστικό ρόλο στο τομέα της υγείας. Με αυτό τον τρόπο εισήχθει η έννοια του Ηλεκτρονικού Φακέλου Ασθενή ως μέσο αποθήκευσης ιατρικών δεδομένων με στόχο την άμεση ανάκλησή τους οποιαδήποτε στιγμή.

Στη συνέχεια η τεχνολογική εξέλιξη αλλά και οι αυξανόμενες ανάγκες των οργανισμών υγείας επέβαλλαν την αναβάθμιση του Ηλεκτρονικού Φακέλου Ασθενή από ένα απλό εργαλείο καταγραφής σε ολοκληρωμένο, δομημένο σύστημα διαχείρισης ιατρικών στοιχείων μέσω υπολογιστή. Η τεχνολογία των Πολυμέσων κατέστησε δυνατή την εισαγωγή και τη διαχείριση πραγματικών ιατρικών δεδομένων στον υπολογιστή, όπως αυτά ανακτώνται από ιατρικά μηχανήματα. Τα εξελιγμένα εργαλεία ανάπτυξης λογισμικού κατέστησαν δυνατή την δημιουργία εφαρμογών με εξαιρετικές δυνατότητες ευελιξίας και ευκολίας στην διαχείριση όλων των ιατρικών πληροφοριών μέσω συσχετισμών στοιχείων, διαχρονικών διαγραμμάτων, έκδοση δεικτών αποτελεσματικότητας, ποιότητας και άλλες τεχνικές. Με αυτόν τον τρόπο, ο Ηλεκτρονικός Φάκελος Ασθενή μετονομάστηκε σε Ηλεκτρονικό Φάκελο Υγείας και χρησιμοποιείται πλέον συστηματικά στη συνεχή παρακολούθηση της υγείας ενός ασθενή.

Σήμερα, οι τελευταίες τάσεις στον χώρο, υπαγορεύουν την χρήση του Ηλεκτρονικού Φακέλου Υγείας ως κεντρικού άξονα στην διαχείριση ιατρικής πληροφορίας αλλά και ως κοινού σημείου αναφοράς για ομάδες επαγγελματιών υγείας διαφορετικών ειδικοτήτων ή ακόμα και σε διαφορετικές τοποθεσίες.[1]

1.2 Βασικοί Ορισμοί και Περιγραφή

Ο Ηλεκτρονικός Φάκελος Υγείας (ΗΦΥ) έχει αποτελέσει πεδίο ερευνών τόσο στην ιατρική όσο και στην ιατρική πληροφορική για αρκετά χρόνια. Ο ΗΦΥ αποτελεί έναν ψηφιακά αποθηκευμένο φάκελο, με στόχο να υποστηρίξει την παροχή φροντίδας και υπηρεσιών υγείας ενός ατόμου εφ'όρου ζωής ενώ, προωθεί την έρευνα και την εκπαίδευση των επαγγελματιών υγείας και βοηθά στην πρόσβαση και στο διαμοιρασμό των πληροφοριών στους επαγγελματίες υγείας με ασφαλή τρόπο καθώς ελέγχεται και η ασφάλεια των δεδομένων. Αντικαθιστά το χειρόγραφο φάκελο ως την κύρια πηγή πληροφοριών στον τομέα της υγείας εξασφαλίζοντας κλινικές, διοικητικές και νομικές απαιτήσεις. [1] Ουσιαστικά ο ΗΦΥ αποτελεί ένα μέσο αποθήκευσης ψηφιακών πληροφοριών υγείας των ατόμων κατά τη διάρκεια της ζωής τους έτσι ώστε αυτές να αξιοποιηθούν κατάλληλα από τους νομικά κατοχυρωμένους χρήστες, οι οποίοι μπορούν να έχουν πρόσβαση σε αυτές.

Σύμφωνα με τον Hunter, ο Ηλεκτρονικός Ιατρικός Φάκελος (ΗΙΦ) ή γενικότερα, ο Ηλεκτρονικός Φάκελος Υγείας (ΗΦΥ) ενός ασθενούς είναι:
Όλες οι πληροφορίες οι οποίες σχετίζονται με τη φυσική, ψυχική υγεία ή κατάσταση ενός ασθενούς στο παρελθόν, παρόν και μέλλον, οι οποίες καταγράφονται ψηφιακά σε ηλεκτρονικό σύστημα με τέτοιο τρόπο ώστε να επεξεργάζονται στους Ηλεκτρονικούς Υπολογιστές ή γενικότερα με τη βοήθεια πολυμέσων και να κυκλοφορούν στο Διαδίκτυο, με πρωταρχικό σκοπό πάντοτε την υγειονομική περίθαλψη και φροντίδα του ασθενούς [2] .

Ένας ακόμη ορισμός που δίνεται από το HIMSS (Healthcare Information and Management Systems Society) για τον ΗΦΥ είναι ο ακόλουθος [3]: Ο ΗΦΥ είναι ένας επεκτάσιμος ηλεκτρονικός φάκελος με πληροφορίες υγείας για έναν ασθενή, οι οποίες παράγονται από έναν ή περισσότερους συμμετέχοντες σε συστήματα παροχής υπηρεσιών φροντίδας υγείας. Μεταξύ άλλων συμπεριλαμβάνει τα δημογραφικά στοιχεία του ασθενή, σημειώσεις προόδου, προβλήματα, φάρμακα, ιατρικό ιστορικό, εμβόλια, αποτελέσματα εργαστηριακών εξετάσεων και αναφορές απεικονιστικών εξετάσεων. Ο ΗΦΥ αυτοματοποιεί και βελτιώνει τη ροή της εργασίας των κλινικών ιατρών. Έχει ακόμη τη δυνατότητα να παράγει πλήρη πρακτικά για τον ασθενή, καθώς επίσης και να ενισχύει κι άλλες σχετικές με τη φροντίδα του ασθενή δραστηριότητες άμεσα ή έμμεσα μέσω της ανάλογης διεπαφής (συμπεριλαμβάνονται η υποστήριξη αποφάσεων βάσει γεγονότων, η διαχείριση ποιότητας και η υποβολή εκθέσεων εκβάσεων).
Η καταγραφή πληροφοριών υγείας επιτυγχάνεται με την διασύνδεση διαφορετικών συστημάτων που συλλέγουν πληροφορίες και στοιχεία υγείας. Το περίπλοκο σύστημα συλλογής πληροφοριών αποτελείται από ανθρώπους, δεδομένα, κανόνες και διαδικασίες, συσκευές επεξεργασίας και αποθήκευσης παραμέτρων, επικοινωνία και εγκαταστάσεις υποστήριξης [4].
Οι βασικές προϋποθέσεις που πρέπει να έχει ένα τέτοιο σύστημα είναι [5]:

- Ελεγχόμενη πρόσβαση στις πληροφορίες με βάση ρόλους χρηστών.
- Επικοινωνία των πληροφοριών με ασφαλή τρόπο.
- Πρόσβαση σε αξιόπιστες και ενημερωμένες πληροφορίες.
- Λειτουργικό περιβάλλον αλληλεπίδρασης με τους χρήστες.

- Χρήση τυποποιημένης ορολογίας αναφοράς.
- Εικοσιτετράωρη διαθεσιμότητα και γρήγορη απόκριση.
- Χαμηλό κόστος χρήσης.
- Συντηρησιμότητα

Τέλος, τα συστήματα Ηλεκτρονικού Φακέλου Υγείας υλοποιούνται και διατηρούνται για τη συλλογή, αποθήκευση, ανάκτηση, επεξεργασία και διακίνηση δεδομένων που σχετίζονται με τη παροχή υπηρεσιών υγείας στους ασθενείς συμπεριλαμβανομένων των κλινικών, διοικητικών και οικονομικών δεδομένων.Τα δεδομένα σχετικά με την υγεία του ατόμου αποτελούν προσωπικά δεδομένα του ατόμου και όχι ιδιοκτησία του φορέα που τα συλλέγει και τα επεξεργάζεται. Συμπερασματικά, η επεξεργασία των δεδομένων πρέπει να συνάδει με τις σχετικές διατάξεις για την προστασία των προσωπικών ευαίσθητων δεδομένων και του ιατρονοσηλευτικού απορρήτου.[1]

1.3 Ιστορική Αναδρομή-Χρονολογική Εξέλιξη

Ο Ιπποκράτης ήταν ο πρώτος που πίστευε ότι ο ιατρικός φάκελος ασθενή θα πρέπει να εξυπηρετεί δύο σκοπούς, να αντανακλά επακριβώς την πορεία της ασθένειας και να δίνει πληροφορίες για τα αίτια της ασθένειας. Περιέγραφε την πορεία μιας ασθένειας καταγράφοντας τις παρατηρήσεις του με καθαρά χρονολογική σειρά.[1]
Ο κλασικός ιατρικός φάκελος ασθενή αρχικά μας δίνει μια εικόνα της υγείας του ασθενούς εφόσον ο τελευταίος έχει ζητήσει σχετική θεραπεία σε κάποια βαθμίδα περίθαλψης. Συνήθως, ο ιατρικός φάκελος περιέχει ευρήματα εξετάσεων, πληροφορίες θεραπειών,φαρμάκων καθώς και τα προσωπικά στοιχεία του ασθενούς, τα οποία καταχωρούνται από τον γιατρό ή τους νοσηλευτές. Τα τρία είδη του ιατρικού φακέλου υγείας είναι ο «βασισμένος στο χρόνο» που όρισε ο Ιπποκράτης που καταχωρούσε τα συμπτώματα με χρονολογική σειρά, ο «ασθενοκεντρικός» που ορίστηκε το 1920 στην κλινική του Mayo κατά τον οποίο κάθε γιατρός που εξέταζε έναν ασθενή ήταν υποχρεωμένος να καταγράφει ένα σύνολο δεδομένων σχετικά με τον ασθενή και τέλος ο «προβληματοκεντρικός» τον οποίο ο Weed εισήγαγε μετά το 1960, συμφώνα με το οποίο σε κάθε ασθενή χρεώνονταν κάποια προβλήματα υγείας. Στον τελευταίο για κάθε πρόβλημα κρατούνται σημειώσεις βασισμένες στην δομή SOAP, που σημαίνει Subjective δηλαδή τα παράπονα του ασθενούς, Objective, οι παρατηρήσεις του γιατρού, Assessment, η διάγνωση και τέλος Plan, η θεραπευτική αγωγή. Το 1991 το Institute of Medicine (IOM) δημοσίευσε μια πολύ σημαντική εργασία με τίτλο «The Computer-Based Patient Record: An Essential Technology for Health Care» , όπου αναφερόταν στην σημαντικότητα της έννοιας του ΗΦΥ και εισήγαγε τον όρο CPR (Computer-based Patient Record) ή αλλιώς «φάκελος ασθενούς βασισμένος στον υπολογιστή». Ο συγκεκριμένος όρος ήθελε να αποδώσει ουσιαστικά την έννοια του ηλεκτρονικού φακέλου ασθενούς, ο οποίος βασίζεται σε ένα σύστημα σχεδιασμένο για να υποστηρίζει τους χρήστες μέσω της διάθεσης ολοκληρωμένων και επακριβών πληροφοριών, να δημιουργεί υπενθυμίσεις, να βοηθά στην κλινική εκτίμηση, και να συνδέεται με την ιατρική γνώση μεταξύ άλλων [6].

[1]Βασικά στοιχεία Ηλεκτρονικού Φάκελου Ασθενή: https://el.wikipedia.org/wiki/%CE%97%CE%BB%CE%B5%CE%BA%CF%84%CF%81%CE%BF%CE%BD%CE%B9%CE%BA%CF%8C%CF%82_%CE%B9%CE%B1%CF%84%CF%81%CE%B9%CE%BA%CF%8C%CF%82_%CF%86%CE%AC%CE%BA%CE%B5%CE%BB%CE%BF%CF%82_%CE%B1%CF%83%CE%B8%CE%B5%CE%BD%CE%AE

Ο σύγχρονος φάκελος ασθενή έχει αρκετές διαφορές από το παρελθόν. Πλέον χωρίζεται σε κάποια κύρια μέρη με βάση την πηγή των δεδομένων. Αρχικά, τα δεδομένα που εξάγονται από τις επισκέψεις του ασθενούς διαμορφώνουν το πρώτο μέρος του φακέλου, τα δεδομένα που προκύπτουν από εργαστηριακές μελέτες αποτελούν το δεύτερο, ενώ το τελευταίο μέρος αποτελείται από γνωματεύσεις ακτινογραφιών, από αξονικές τομογραφίες ή υπερήχους.
Σε πολλές περιπτώσεις όμως η σύγχρονη πραγματικότητα αντανακλάται στην έλλειψη συχρονισμού ανάμεσα σε χειρόγραφους φακέλους, παρατηρείται δηλαδή το γεγονός ότι κάποιοι γιατροί μπορεί να δουλεύουν σε διαφορετικές εκδόσεις που αναφέρονται στον ίδιο ασθενή. Επίσης σε ορισμένους φορείς υγείας υπάρχει ένας μοναδικός φάκελος, με αποτέλεσμα να συγχέεται η ιατρική πληροφορία και να οδηγεί σε ανακρίβειες. Τέλος, σε ακραίες περιπτώσεις παρατηρούνται χειρόγραφοι φάκελοι που είτε βρίσκονται εγκαταλελειμμένοι σε ράφια αποθηκών και δεν μπορούν να βρεθούν, είτε είναι προσβάσιμοι, αλλά σε κατάσταση που τους καθιστά ακατάλληλους για οποιαδήποτε χρήση, ακόμα και για την ανάγνωσή τους. Για αυτό και ο χειρόγραφος φάκελος δεν εξυπηρετεί τους σκοπούς του επακριβώς και παράλληλα με την ιατρική γνώση που εμπλουτίζεται συνεχώς, ο ηλεκτρονικός ιατρικός φάκελος γίνεται επιτακτική ανάγκη.
Τα πρώτα χρόνια που έγιναν αξιόλογες προσπάθειες για την χρήση του ηλεκτρονικού ιατρικού φακέλου τα δεδομένα καταγράφονταν σε μορφή κειμένου και οι γιατροί ήταν διστακτικοί όσον αφορά στην υιοθέτησή του. Επιπλέον, η τεχνολογική εκπαίδευση του ιατρικού προσωπικού ήταν ελλιπής και το κόστος τέτοιων πληροφοριακών συστημάτων ήταν υπέρογκο. Παρ' όλα αυτά, ένας μεγάλος αριθμός εύχρηστων και αξιόπιστων ηλεκτρονικών ιατρικών φακέλων όπως τα συστήματα COSTAR, TMR, RMIS, STOP και ELIAS αναπτύχθηκαν και εξελίχθηκαν τα τελευταία χρόνια. Ο ηλεκτρονικός ιατρικός φάκελος χρησιμοποιείται σε δύο επίπεδα παροχής υγείας, στην πρωτοβάθμια φροντίδα και την δευτεροβάθμια ή την πιο ειδικευμένη φροντίδα ασθενών. Αναφορικά με την πρωτοβάθμια φροντίδα, οι γενικοί ιατροί χρησιμοποιούν τον ηλεκτρονικό ιατρικό φάκελο πολύ παραπάνω από τους ειδικούς ιατρούς. Πιο συγκεκριμένα σήμερα στην Ολλανδία το 90% των γενικών ιατρών χρησιμοποιεί ΗΙΦΑ για διάφορους σκοπούς όπως διοικητικούς, ιατρικούς και οικονομικούς. Από ιατρικής πλευράς ο ΗΙΦΑ στην πρωτοβάθμια φροντίδα είναι προβληματοκεντρικός. Χρησιμοποιείται συγκεκριμένη ορολογία, όπως το ICD9-CM για κωδικοποίηση διαγνώσεων. Όσον αφορά τους ειδικούς ιατρούς μέχρι στιγμής χρησιμοποιούν τον ηλεκτρονικό ιατρικό φάκελο λιγότερο από ότι οι γενικοί ιατροί λόγω του ότι οι γενικοί ιατροί δουλεύουν είτε μόνοι τους είτε ανήκουν σε μικρές ομάδες ιατρών με αποτέλεσμα να ελέγχουν σε καλύτερο βαθμό τη διαχείριση της δουλειάς τους. Αντίθετα οι ειδικοί ιατροί δουλεύουν σε περίπλοκα περιβάλλοντα τα οποία θα πρέπει να μετρήσουν την επιρροή του ηλεκτρονικού ιατρικού φακέλου στην όλη δομή της διαχείρισης, την προοπτική μελλοντικής ανάπτυξης και των λογιστικών μεγεθών. Μάλιστα, οι διάφορες ειδικότητες έχουν διαφορετικές απαιτήσεις, οπότε είναι δύσκολο να βρει κανείς έναν που να τις ικανοποιεί όλες. Τα συστήματα ηλεκτρονικών ιατρικών φακέλων αποτελούνται κυρίως από το υλικό, το λογισμικό, τα δεδομένα και το ανθρώπινο δυναμικό. Το υλικό που χρειάζονται είναι κυρίως CD-ROMs ή σκληροί δίσκοι για αποθήκευση των δεδομένων, servers και κατάλληλο δίκτυο για την επικοινωνία των συστημάτων. Το λογισμικό περιλαμβάνει ένα λογισμικό διεπαφής, δηλαδή ένα πρόγραμμα που καθιστά φιλικό το περιβάλλον του ηλεκτρονικού ιατρικού φακέλου για τον χρήστη. Τα δεδομένα είναι τα κλασσικά δεδομένα που εισάγονται σε ένα χειρόγραφο ιατρικό φάκελο. Ως αποτέλεσμα, μέσα στον ιατρικό φάκελο, υπάρχουν δημογραφικά δεδομένα του ασθενούς, τα

αποτελέσματα των εξετάσεων, οι ιατρικές οδηγίες και η φαρμακευτική αγωγή ενώ αποθηκεύονται και ακτινογραφίες, αξονικές και άλλες αντίστοιχες εξετάσεις. Το τελευταίο συστατικό στοιχείο του, το ανθρώπινο δυναμικό είναι το ιατρικό, το παραϊατρικό, το διοικητικό και το γραμματειακό προσωπικό. Ακόμα σε αυτήν την κατηγορία εντάσσονται οι υπεύθυνοι του συστήματος, δηλαδή αυτοί που το υλοποιούν και το συντηρούν όπως αναλυτές, προγραμματιστές και τεχνικοί υλικού.
Στην Ελλάδα έχει αρχίσει να εφαρμόζεται σταδιακά ο Ηλεκτρονικός Φάκελος Υγείας στις τοπικές μονάδες υγείας από τα τέλη του Μαρτίου 2018 με την ονομασία Ατομικός Ηλεκτρονικός Φάκελος Υγείας. [7]

1.4 Περιεχόμενα

Το σύστημα Ηλεκτρονικού Φακέλου Υγείας περιέχει δεδομένα σε ψηφιακή μορφή κατάλληλα για επεξεργασία από ΗΥ και με την δυνατότητα διαθεσής μέσω διαδικτύου. Ο φακελός συνήθως παρέχει και δεδομένα στη μορφή στην οποία εξάγωνται απευθείας από κάποιο εργαστήριο όπως ακτινογραφικό φίλμ με αποτελέσματα βιοχημικών εξετάσεων, χαρτί καρδιογράφου και άλλες πληροφορίες αντίστοιχου περιεχομένου. Γενικά ένας τυπικός Ηλεκτρονικός Φάκελος Υγείας ενός ασθενή επιβάλλεται να παρέχει όλα τα δεδομένα που σχετίζονται με αυτόν οποιαδήποτε χρονική στιγμή κριθεί αναγκαίο. Κάποιες κατηγορίες δεδομένων που εμπεριέχονται στον Ηλεκτρονικό Φάκελο Υγείας αναφέρονται παρακάτω :

1) Συμπτώματα με τα οποία εισήχθη ο ασθενής. Συνήθως τα συμπτώματα του ασθενούς συντάσσονται σε ελεύθερο κείμενο από τους ιατρούς που θα εξετάσουν.
2) Το ιστορικό ιατρικών παθήσεων του ασθενούς, τις κλινικές εξετάσεις του, τις διαγνώσεις, ιατρικές εντολές ή συνταγές οι οποίες έχουν συνταχθεί από τους ιατρούς και σχετίζονται με τη θεραπεία που καλείται να ακολουθήσει ο ασθενής.
3) Σημειώσεις σχετικά με άλλες ασθένειες ή καταστάσεις του ασθενούς οι οποίες ενδέχεται να επηρεάσουν είτε να επηρεαστούν από την παρούσα κατάσταση καθώς και συμπληρωματικές όπως σημειώσεις διατροφής και τρόπου ζωής. [8]
4) Τις απεικονιστικές εξετάσεις όπως ακτινογραφίες και τομογραφίες σε μορφή στατικών εικόνων.
5) Τα ηλεκτροκαρδιογραφήματα τα οποία βρίσκονται σε μορφή βιο-σημάτων όπως ηλεκτρονικά κωδικοποιημένη έξοδος κάποιας συσκευής καταγραφής.
6) Τα αποτελέσματα των ενδοσκοπικών εξετάσεων (γαστροσκόπηση, κολονοσκόπηση κτλ.) που παρουσιάζονται σε μορφή βίντεο.
7) Το ηχοκαρδιογράφημα, το οποίο θα βρίσκεται σε μορφή ήχου.
8) Επιπλέον, πληροφορίες διοικητικής, οικονομικής και στατικής φύσεως, που σχετίζονται με τη μονάδα νοσηλείας του ασθενούς και τα δημογραφικά στοιχεία του ασθενούς. Αυτά περιλαμβάνουν την ηλικία του ασθενούς, το ύψος του, το βάρος του, το φύλο, τον τόπο κατοικίας και γενικά διάφορες πληροφορίες οι οποίες μπορούν να φανούν χρήσιμες με έμμεσο τρόπο. [1]
9) Στοιχεία ταυτοποίησης του ασθενούς. Απαιτείται η ταυτοποίηση του ασθενούς με τη συμπλήρωση διάφορων προσωπικών δεδομένων του ασθενούς, όπως το ονοματεπώνυμό του, ο αριθμός μητρώου κοινωνικής ασφάλισης και πιθανόν άλλες αναγκαίες πληροφορίες. [8]

1.5 Λειτουργίες Διαχείρισης

Οι λειτουργίες του Ηλεκτρονικού Φακέλου Υγείας πρέπει να ανταποκρίνονται στην πολυπλοκότητα του κλινικού περιβάλλοντος και να διαμορφώνονται ανάλογα με τις ανάγκες των χρηστών στα επιμέρους τμήματα του φορέα, καθώς επίσης και να επικοινωνούν μεταξύ τους στο πλαίσιο αυτοματοποίησης των επιχειρησιακών διαδικασιών του φορέα. Η πληροφορία, ο τρόπος παρουσίασης της, και το επίπεδο λεπτομέρειας, αλλάζει ανάλογα με την κλινική, το τμήμα και το ρόλο του χρήστη. Χαρακτηριστικά και διεπαφές του συστήματος πρέπει να ανταποκρίνονται και να διαμορφώνονται ανάλογα ώστε να διευκολύνεται το έργο του κάθε τμήματος με βάση τις ιδιαίτερες ανάγκες του [9]. Σύμφωνα με όσα αναφέρθηκαν οι κύριες λειτουργίες που ο ΗΦΥ θα πρέπει γενικά να παρέχει όσον αφορά τη διαχείριση της ιατρικής πληροφορίας ενός ασθενούς είναι οι παρακάτω:

1) Λειτουργίες Λήψης Δεδομένων

Λειτουργίες που έχουν ως στόχο τη συλλογή και αξιοποίηση ιατρικών πληροφοριών. Τα δεδομένα αυτά πρέπει να περιλαμβάνουν όλα εκείνα τα χαρακτηριστικά που μπορούν να επηρεάσουν την υγεία του ασθενούς. Πρέπει να καταγράφονται τυχόν διαγνώσεις αλλά και φαρμακευτικές αγωγές που λαμβάνει. Τέλος, σημαντικό σημείο στην καταγραφή είναι να τηρείται ιατρικό ιστορικό του ασθενούς, δηλαδή να υπάρχουν όλες οι καταγραφές που έχουν γίνει για οποιοδήποτε λόγο.

Τέτοιου είδους δεδομένα μπορούν να ανακτηθούν από κοντινές ή μακρινές συσκευές παρακολούθησης, από εφαρμογές τηλεϊατρικής, άμεσα από έναν ασθενή ή γενικότερα από το στενό περιβάλλον ενός ασθενή που έχουν πληροφορίες για του ιατρικό του ιστορικό όπως συγγενείς, φίλοι και άλλοι ιατροί που τον έχουν παρακολουθήσει. Τα δεδομένα εισάγονται σε ψηφιακή μορφή στον Ηλεκτρονικό Φάκελο Υγείας μέσω πληκτρολογίου.

2) Λειτουργίες Αποθήκευσης Δεδομένων

Δημιουργία ενός ή και πολλαπλών συστημάτων αποθήκευσης δεδομένων και κατ’έπεκταση των Ηλεκτρονικών Φακέλων Υγείας. Τέτοια συστήματα δεδομένων περιέχουν δεδομένα που έχουν εξαχθεί από άλλες εφαρμογές. Τα δεδομένα έχουν μεταφερθεί και μετατραπεί σε κατάλληλη μορφή και στη συνέχεια εισάγονται στην αποθήκη δεδομένων. Υπάρχουν δύο μείζονα πεδία εφαρμογής για τα συστήματα αποθήκευσης δεδομένων στα νοσοκομεία. Μπορούν είτε να χρησιμοποιηθούν στη διαχείριση του νοσοκομείου είτε στην έρευνα. Σε αντίθεση με άλλους τομείς, τα συστήματα αποθήκευσης δεδομένων στα νοσοκομεία δεν είναι σημαντικά μόνο για τη διοίκηση και για θέματα σχετικού κόστους αλλά και για ιατρικά θέματα σε κλινικές δοκιμές. [8]

3) Λειτουργίες Επεξεργασίας και Ταξινόμησης Δεδομένων βάσει Ιατρικών όρων και διαδικασιών

Το πεδίο αυτό επιδιώκει την ομοιογένεια των ιατρικών όρων αλλά και των ιατρικών διαδικασιών. Σε γενικές γραμμές μπορούν να αναφερθούν πρότυπα ταξινόμησης, ονοματολογίας και κωδικοποίησης, τα οποία είναι ουσιαστικά βάσεις δεδομένων με ιατρικούς όρους ταξινομημένα σε μορφή δέντρου, όπου ο κάθε όρος κωδικοποιείται με ένα συγκεκριμένο κωδικό. Το πρώτο επίπεδο ταξινόμησης γίνεται συνήθως σύμφωνα με την τοπολογία των συμπτωμάτων στο ανθρώπινο σώμα. Πιο εξελιγμένα πρότυπα δημιουργούν συσχετίσεις μεταξύ των όρων αλλά και συσχετίσεις μεταξύ ασθενειών και διαδικασιών επιτρέποντας την υλοποίηση σημασιολογικών σχέσεων μεταξύ των όρων και βοηθώντας τον ιατρό να κάνει πιο αποδοτικά τη δουλειά του. Η επίτευξη της ταξινόμησης και κωδικοποίησης των ιατρικών όρων άρει την όποια αφαιρετικότητα ενδέχεται να εισάγει κάποιος ειδικός και συμβάλει στην ομοιογένεια των ιατρικών δεδομένων. [8]

4) Λειτουργίες Μεταφοράς Δεδομένων

Η μεταφορά των δεδομένων σχετίζεται με μια σειρά από κανόνες και προδιαγραφές που πρέπει να πληρούνται από ιατρικές εφαρμογές και λογισμικά, με σκοπό την έγκυρη και ασφαλή διάδοση της ιατρικής πληροφορίας μεταξύ ιατρικών δομών. Στην περίπτωση αυτή αναφερόμαστε ξεκάθαρα σε προτυποποίηση για την υλοποίηση μέρους πληροφοριακού συστήματος. Συγκεκριμένα προτυποποιείται το υποσύστημα το οποίο είναι υπεύθυνο για την επικοινωνία μεταξύ διαφορετικών συστημάτων με στόχο διάδοση της ιατρικής πληροφορίας. Στο σημείο αυτό είναι αναγκαίο να διευκρινιστεί ότι τα πρότυπα μετάδοσης της ιατρικής πληροφορίας δεν συνιστούν λογισμικό, είναι όμως μια σειρά από κανόνες, οι οποίοι υποδεικνύουν ότι συγκεκριμένες πτυχές της υλοποίησης πρέπει να γίνουν με συγκεκριμένο τρόπο. Για παράδειγμα ένας ιατρός θα μπορούσε να έχει πρόσβαση στο σύνολο των δεδομένων στο νοσοκομείο στο οποίο εργάζεται, ενώ ένας ασθενής θα μπορούσε να έχει πρόσβαση μόνο στα δικά. Τέτοιου τύποι λειτουργίες ορίζονται ρητά από τα πρότυπα.[8]

5) Λειτουργίες Παρουσίασης Πληροφορίας

Σε συνέχεια των προηγούμενων λειτουργιώνοι εξουσιοδοτημένοι πάροχοι φροντίδας και άλλοι με νόμιμες χρήσεις (π.χ. Διοικητικό προσωπικό) έχουν την πληροφορία σε μορφή που τους εξυπηρετεί. Η παρουσίαση μπορεί να γίνει με λεπτομέρεια ή περιληπτικά, ενώ μπορεί να περιλαμβάνει πίνακες, γραφήματα, αναλυτικό κείμενο καθώς και άλλες φόρμες. [1]

6) Λειτουργίες Ασφάλειας Δεδομένων

Αυτές αναφέρονται στην εμπιστευτικότητα της ιδιωτικής ιατρικής πληροφορίας αλλά και στην ακεραιότητα των δεδομένων. Πρέπει να σχεδιάζονται ώστε να είναι σύμφωνες με τους νόμους, τους κανονισμούς, και τα πρότυπα. Τα συστήματα

ασφαλείας πρέπει να εξασφαλίζουν ότι η πρόσβαση παρέχεται μόνο σε εκείνους που είναι εξουσιοδοτημένοι και έχουν το νόμιμο δικαίωμα χρήσης. Θα πρέπει επίσης να εξασφαλίζουν την καταγραφή ιχνών για την καλύτερη αντιμετώπιση τυχόν ακατάλληλης ή παράνομης χρήσης. [1]

1.6 Απαιτήσεις

Για την δημιουργία ενός συστήματος υποστήριξης του Ηλεκτρονικού Φακέλου Υγείας θα πρέπει να πληρούνται ορισμένες απαιτήσεις ώστε να επιτυγχάνεται η αποδοτικότητα και η αποτελεσματικότητα που απαιτείται. Ορισμένες εκ των απαιτήσεων παρουσιάζονται συνοπτικά παρακάτω [1] :

1) Καταγραφή

Είναι απαραίτητη η πλήρη καταγραφή των στοιχείων που προκύπτουν από τις εξετάσεις ενός ασθενούς, τις εργαστηριακές του εξετάσεις καθώς και τη φαρμακευτική αγωγή που του έχει συνταγογραφηθεί. Αυτή η διαδικασία απαιτεί ρητά την καταχωρησή του Ηλεκτρονικού Φακέλου Υγείας με συστηματικό τρόπο και ακολοθώντας συγκεκριμένες διδιακασίες με στόχο την συλλογή των σημαντικών δεδομένων ενός ασθενούς.

2) Συντήρηση

Σε συνέχεια της καταγραφής των δεδομένων θα πρέπει να τηρείται η διαδικασία συλλογής δεδομένων ενός ασθενή καθόλη τη διάρκεια της ζωής του. Αυτό επιτυγχάνεται εισάγοντας κάθε φορά τα νέα κλινικά αποτελέσματα καθώς και κάθε είδους νέα ευρήματα που τυχόν προέκυψαν, ενημερώνοντας έτσι συνεχώς το ιατρικό ιστορικό ενός ασθενούς. Τέλος, πέρα από την ενημέρωση που αναφέρθηκε παραπάνω πρέπει να προσφέρεται επίσης η δυνατότητα δημιουργίας αντιγράφων ασφαλείας του Ηλεκτρονικού Φακέλου Υγείας έτσι ώστε σε περίπτωση λάθους ή και αποτυχίας του συστήματος να έχουμε πρόσβαση στην πρόσθατη ενημέρωση του Φακέλου ενός ασθενούς.

3) Ασφάλεια

Η προστασία ευαίσθητων προσωπικών δεδομένων είναι ίσως πιο σημαντική προδιαγραφή του Ηλεκτρονικού Φακέλου Υγείας. Ο Ηλεκτρονικός Φάκελος Υγείας θα πρέπει να είναι έτσι σχεδιασμένος ώστε να συμφωνεί με τη νομοθεσία μίας χώρας και στη περίπτωση της Ελλάδας, θα πρέπει να συμβαδίζει με τα πρότυπα που έχει καθορίσει η Ευρωπαϊκή Ένωση και αφορούν στην προστασία των προσωπικών δεδομένων (Κανονισμός GDPR). Σε αυτή τη κατεύθυνση τα προσωπικά δεδομένα ενός ασθενούς θα πρέπει να είναι προσβάσιμα μόνο από τον ίδιο καθώς και από φυσικά άτομα ή και οργανισμούς στους οποίους αυτός θα δώσει την άδεια. Η κρυπτογράφηση πληροφορίας καθώς και η δημιουγία κωδικών για την πρόσβαση των προσωπικών δεδομένων συντελεί σε αυτή την κατεύθυνση.

4) Διασυνδεσιμότητα

Ένα πληροφοριακό σύστημα θα πρέπει να προσφέρει τη δυνατότητα σε όλους τους ενδιαφερόμενους χρήστες να προβούν σε ανάγνωση, πρόσθεση , αλλαγή αλλά και φραγή των στοιχείων τους, ενέργειες βέβαια που θα εξαρτώνται άμεσα από τον αντίστοιχο ρόλο του κάθε χρήστη. Για παράδειγμα, δεν πρέπει να δίνεται σε έναν ασθενή η δυνατότητα να διαγράψει κάτι από το ιστορικό του γιατί υπό προϋποθέσεις, μια τέτοια ενέργεια θα μπορούσε να οδηγήσει σε λάθος διάγνωση στο μέλλον. Στην ίδια περίπτωση βέβαια ο ασθενής έχει τη δυνατότητα να κρατήσει μία πληροφορία προσωπική. Τέλος, όλα τα παραπάνω θα πρέπει να ισχύουν σε κάθε περίπτωση ανεξαρτήτως του συστήματος Ηλεκτρονικού Φακέλου Υγείας που χρησιμοποιεί ο ασθενής.

5) Ευρύτητα-περιεκτικότητα

Είναι αναγκαία η υποστήριξη διαφόρων τύπων δεδομένων μέσα στον Ηλεκτρονικό Φάκελο Υγείας του ασθενή. Πρέπει να μπορεί το νοσηλευτικό προσωπικό να εισάγει ελεύθερο κείμενο, ακτινογραφίες σε ηλεκτρονική μορφή, καρδιογραφήματα και οποιαδήποτε άλλη (ηλεκτρονικής μορφής) ιατρική πληροφορία που μπορεί να προκύψει. Επίσης το σύστημα θα πρέπει να προσφέρει τη δυνατότητα καταγραφής ιατρικής πληροφορίας και δεδομένων τόσο με συνοτπτικό όσο και κατανοητό τρόπο.

6) Μεταφερσιμότητα

Ανεξαρτήτως λογισμικού, υλικού καθώς και εθνικής γλώσσας του κάθε χρήστη θα πρέπει το εν λόγω σύστημα να έχει τα χαρακτηριστικά της μεταφερσιμότητας και δυνατότητας επικοινωνίας μεταξύ διαφορετικών κλινικών. Θα πρέπει η ανταλλαγή δεδομένων μεταξύ των παρόχων υγείας να γίνεται με απλό τρόπο και να μην απαιτεί κάποια ειδική γνώση του υπάρχοντος συστήματος.

7) Εξέλιξη

Ένας Ηλεκτρονικός Φάκελος Υγείας πρέπει να τηρεί κανόνες συμβατότητας επεξεργασίας από προηγούμενες και επόμενες εκδόσεις παρόμοιων συστημάτων λογισμικού. Επίσης οι αλλαγές αυτές θα πρέπει να γίνονται με γνώμονα το γεγονός ότι οι ομάδες στις οποίες απευθύνεται το λογισμικό δεν θα πρέπει να διαθέτουν κάποια εξειδικευμένη γνώση, το οποίο προϋποθέτει ένα σύστημα φιλικό προς τον χρήστη. Σημαντικό επίσης είναι σε ενδεχόμενη αναβάθμιση του να μην περιέχει ριζικές αλλαγές ώστε να μην απαιτείται από τον χρήστη μεγάλος χρόνος εξοικείωσης με το ήδη υπάρχων σύστημα.

8) Επεκτασιμότητα

Η επεκτασιμότητα είναι ζωτικής σημασίας, καθώς θα πρέπει να παρέχεται η δυνατότητα προσθήκης νέων δεδομένων, ακόμη και αν πρόκειται για μεγάλο όγκο πληροφοριών. Αυτό σημαίνει, πως δεν θα πρέπει να περιορίζεται η εισαγωγή στοιχείων σε καθορισμένο αριθμό καρτελών, αλλά να χρησιμοποιείται όσος χώρος

είναι απαραίτητος για τη συλλογή των δεδομένων. Για κάθε πληροφορία δεν θα πρέπει να παρέχεται ένας στατικός χώρος για την αποθήκευση τους αλλά ο χώρος αυτός θα πρέπει να παρέχεται με δυναμικό τρόπο και να εξαρτάται από τον όγκος της πληροφορίας που πρέπει κάθε φορά να αποθηκευτεί.

9) Διαθεσιμότητα

Ένας Ηλεκτρονικός Φάκελος Υγείας θα πρέπει να διατίθεται σε κάθε εξουσιοδοτημένο χρήστη άμεσα είτε σε ηλεκτρονική μορφή είτε σε έντυπη για πιθανή αξιοποίηση από τον χρήστη με οποιοδήποτε τρόπο αυτός επιθυμεί.

10) Ευρεία χρήση προτύπων

Τέλος, η στήριξη ενός τέτοιου φακέλου σε υπάρχοντα πρότυπα είναι σημαντική καθώς δεν καθίσταται ως πάρεργο στις γνωστές εργασίες του ιατρικού προσωπικού και διευκολύνει, όσο αυτό είναι δυνατό τη χρήση του.

Κάποιες άλλες ειδικότερες απαιτήσεις που θα πρέπει να πληρεί ένα σύστημα Ηλεκτρονικού Φακέλου Υγείας είναι οι παρακάτω [1]:

- Δημιουργία μίας καρτέλας ανά ασθενή για τον ξεκάθαρο διαχωρισμό της πληροφορίας.
- Δημιουργία μίας δομής δέντρου για την αναπαράσταση της ιατρικής κατάστασης του κάθε ασθενή.
- Πλήρες ιστορικό σε ημερίσια βάση με πληροφορίες για την ιατρική κατάσταση ενός ασθενούς, όπως για παράδειγμα εμφάνιση ημερομηνίας εισαγωγής σε κάποιο νοσοκομείου και του αντίστοιχου εξιτηρίου.
- Ύπαρξη κατάλληλης αναζήτησης για την εύρεση ενός ασθενούς μέσω φίλτρων ή την συμπλήρωση κατάλληλων πεδίων.
- Καταγραφή όλων των εξετάσεων.
- Καταγραφή και επεξεργασία εικόνων.
- Δυνατότητα άντλησης στατιστικών στοιχείων βάση ενός ή και περισσοτέρων χαρακτηριστικών.
- Γραφήματα για την καλύτερη παρουσίαση και εποπτεία δεδομένων.
- Δυνατότητα εκτύπωσης ιατρικών εκθέσεων.
- Ασφάλεια προσωπικών δεδομένων των ασθενών μέσω κατάλληλων δομών του συστήματος.
- Πρόσβαση σε δεδομένα και εκτέλεση ενεργειών ανάλογα με την ομάδα που ανήκει ο χρήστης.
- Αποθήκευση των δεδομένων σε κεντρικό μηχάνημα.

1.7 Πλεονεκτήματα Ηλεκτρονικού Φακέλου Υγείας

Η χρησιμοποίηση του Ηλεκτρονικού Φακέλου Υγείας ως βασικού εργαλείου στην παρακολούθηση και καταγραφή του ιατρικού ιστορικού ενός ασθενούς αποφέρει πολλά πλεονεκτήματα στην καθημερινή πρακτική της Ιατρικής, τα σημαντικότερα από τα οποία παρατίθενται παρακάτω :

• Εύκολη εισαγωγή, αναζήτηση και αλλαγή των στοιχείων, με αποτέλεσμα την ορθότερη εξαγωγή συμπερασμάτων.

• Εύκολη επιθεώρηση και επεξεργασία των ιατρικών εικόνων, το οποίο συντελεί στην ορθότερη διάγνωση.

Ειδικότερα, ο Ηλεκτρονικός Φάκελος Υγείας μπορεί να βοηθήσει τους ιατρούς με τους εξής τρόπους [1] :

1) Εύκολη καταγραφή των παρατηρήσεων, λόγω της ύπαρξης ενιαίων συστημάτων και προτύπων κωδικοποίησης.

2) Εύκολη εισαγωγή δεδομένων από εργαστηριακές εξετάσεις μέσω της αυτόματης ενσωμάτωσης πρωτοκόλλων εργαστηριακών εξετάσεων.

3) Εύκολη αναζήτηση δεδομένων, τόσο στο επίπεδο του τοπικού φακέλου, όσο και στην εύρεση δεδομένων από συστήματα φακέλων ασθενών.

4) Υποβοήθηση στη διάγνωση μέσω της πρόσβασης σε στατιστικά στοιχεία.

5) Βελτιωμένα δεδομένα υγείας του ασθενούς, όπως φωτογραφίες, βιολογικά σήματα, κλινικά σχέδια κτλ.

6) Υποβοήθηση στη δημιουργία του φακέλου, εφόσον τα συστήματα φακέλων κατευθύνουν τον ιατρό με βάση προσυμφωνημένα πρωτόκολλα ενσωματωμένα στα συστήματα αυτά.

7) Δυνατότητα πληρέστερης ανάλυσης των δεδομένων των ασθενών.

8) Δυνατότητα καλύτερης αξιολόγησης του αποτελέσματος της θεραπείας, μέσω της δυνατότητας πρόσβασης στα δεδομένα άλλων ιατρών, με ανάλογα περιστατικά.

9) Υποβοήθηση στην εκτίμηση, διάγνωση, θεραπεία του ασθενούς μέσω της χρήσης του φακέλου στην Τηλεϊατρική. Από τις βασικότερες υπηρεσίες της Τηλεϊατρικής πάνω σε αυτόν τον τομέα είναι η τηλεδιάσκεψη. Η τηλεδιάσκεψη παρέχει τη δυνατότητα για οπτικοακουστική επαφή μεταξύ απομακρυσμένων σημείων χρησιμοποιώντας κάμερες και μικρόφωνα καθώς και δικτυακό εξοπλισμό. Έτσι οι ιατροί μπορούν να πραγματοποιήσουν:

• Ιατρικά συμβούλια μεταξύ των νοσοκομείων της περιοχής.

• Παροχή διάγνωσης σε ασθενείς που βρίσκονται σε διαφορετικό νοσοκομείο ή κλινική.

• Παροχή συμβουλών σε μη ειδικευμένους ιατρούς ή σε ιατρούς άλλης ειδικότητας. Αυτό αποκτά καίρια σημασία στην περίπτωση των κέντρων υγείας, ειδικά απομακρυσμένων περιοχών καθώς και στην αντιμετώπιση επειγόντων περιστατικών.

• Επίσης οι φοιτητές σχολών της Ιατρικής μπορούν να παρακολουθήσουν χειρουργικές επεμβάσεις, καθώς και διαλέξεις που γίνονται σε άλλα σημεία.

Εν ολίγοις, ένας ιατρός μπορεί με τον Ηλεκτρονικό Φάκελο Υγείας:

• Να κάνει διάγνωση ενός ασθενούς που βρίσκεται εκτός της γεωγραφικής του εμβέλειας.

• Να ζητήσει την γνώμη ενός εξειδικευμένου συναδέλφου για τον εξεταζόμενο ασθενή.

• Να έχει άμεση πρόσβαση στο αρχείο των ασθενών.

• Να επωφεληθεί της μείωσης του χρόνου διάγνωσης.

• Να έχει άμεση πληροφόρηση και ενημέρωση.

• Να έχει άμεση επικοινωνία με τους συναδέλφους του μέσω δικτύου. Οφέλη από τα προγράμματα Ηλεκτρονικού Φακέλου Υγείας έχουν επίσης και οι ασθενείς.

Συγκεκριμένα, η προσφορά της Τηλεϊατρικής και για τον απλό πολίτη είναι πολύπλευρη:

• Έρχεται σε άμεση επαφή με τον ιατρό, ακόμη και αν εκείνος βρίσκεται σε κάποια απομακρυσμένη περιοχή.

• Έχει άμεση εξυπηρέτηση και αύξηση της ποιότητας περίθαλψης, αποφεύγοντας τις επαναλήψεις, τις καθυστερήσεις και τα λάθη.

• Ενημερώνεται άμεσα για θέματα δημόσιας υγείας, επιδημίες, αλλά και τρόπους αντιμετώπισης των προαναφερθέντων, συντελώντας ταυτόχρονα και στην πρόληψη.

• Τέλος, τα συστήματα Ηλεκτρονικού Φακέλου Υγείας έχουν ως αποτέλεσμα ταχύτερο χρόνο διάγνωσης και κατ’επέκταση ανάρρωσης, μικρότερη χρήση μη απαραίτητων φαρμάκων και μείωση εξόδων για ασθενείς και νοσοκομεία.

1.8 Μειονεκτήματα Ηλεκτρονικού Φακέλου Υγείας

Προκειμένου να εφαρμοστεί ένα ολοκληρωμένο πληροφοριακό σύστημα, όπως είναι ο Ηλεκτρονικός Φάκελος Υγείας είναι κατανοητό ότι θα πρέπει να λυθούν ένας αριθμός προκλήσεων που θα προκύψουν. Συγκεκριμένα, μερικά από τα εμπόδια που πρέπει να ξεπεραστούν είναι τα εξής [1] :

1. Δεν έχει ορισθεί πρωτόκολλο, το οποίο να διευκρινίζει τα δεδομένα που πρέπει να εισαχθούν μετά το πέρας της εξέτασης του ασθενή. Οι πληροφορίες που καταγράφονται πολλές φορές μπορεί να είναι ακόμα και σε μορφή ελεύθερου κειμένου, γεγονός που κάνει πολύ πιο δύσκολη την τυποποίηση της πληροφορίας. Εύκολα γίνεται αντιληπτό ότι τις περισσότερες φορές οι πληροφορίες που καταγράφονται εξαρτώνται από την εμπειρία του ιατρού, την ασθένεια του εξεταζόμενου καθώς και τον τομέα στον οποίο είναι ειδικευμένος ο ιατρός.

2. Η εισαγωγή του Ηλεκτρονικού Φακέλου Υγείας και η τακτική του χρησιμοποίηση από ιατρό-νοσηλευτικούς οργανισμούς σίγουρα αποφέρει πολλά μακροχρόνια οφέλη, παρ'όλα αυτά τα αποτελέσματα αυτά δεν απορέουν άμεσα από την χρήση του.

3. Με την εγκατάσταση ενός νέου συστήματος μηχανογράφησης, συχνά κρίνεται απαραίτητη η εισαγωγή δεδομένων από το ιατρικό προσωπικό που είναι λογικό να αυξήσει τις ώρες εργασίας που απαιτούνται για την κάλυψη των αναγκών της εργασίας. Ένα καινούριο σύστημα ακόμα και όταν είναι φτιαγμένο με τέτοιο τρόπο έτσι ώστε να είναι φιλικό προς το χρήστη παραμένει μία καινούρια τεχνολογία με την οποία θα πρέπει να έρθει σε επαφή και να αλληλεπιδράσει μαζί της. Σε αυτή την κατεύθυνση ίσως χρειαστούν ακόμα κάποιες επιπρόσθετες ώρες εκπαίδευσης αλλά και επιλέον κόπος για να καταφέρει να ανταπεξέλθει σε αυτή τη νέα τεχνολογία το προσωπικό. Με λίγα λόγια η έλλειψη τεχνογνωσίας και θέλησης για μάθηση από το προσωπικό που έχει συνηθίσει να δουλεύει με συγκεκριμένο τρόπο, δυσκολεύει την αποδοχή ενός νεόυ σύστημα.

4. Σε συνέχεια του παραπάνω επιχειρήματος η εισαγωγή νέας τεχνολογίας προκαλεί προβληματισμό και αμηχανία στο νοσηλευτικό προσωπικό. Ο λόγος είναι ότι πολλοί από τους εν δυνάμει χρήστες δεν έχουν ιδιαίτερα αναπτυγμένη επαφή με την τεχνολογία και συγκεκριμένα με τη χρήση ΗΥ. Επίσης, πολλοί εκ των χρηστών είναι προχωρημένης ηλικίας και θα δυσκολευτούν να μάθουν το σύστημα. Τέλος, η εξάρτηση από μία τεχνολογία για την οποία δεν έχουν το αντίστοιχο γνωσιακό επίπεδο προκαλεί φόβο και απροθυμία όσον αφορά την εφαρμογή της.

5. Σημαντικός παράγοντας που καθιστά δύσκολη την ολοκληρωμένη εφαρμογή του Ηλεκτρονικού Φακέλου Υγείας στα κλινικά ιδρύματα, είναι η δύσχρηστη αλληλεπίδραση με το σύστημα είτε αυτό είναι το user-interface του συτήματος είτε κάποια λίγο πιο τεχνικά θέματα όπως παρουσιάστηκαν και παραπάνω. Αυτό προκάλεσε την έντονη δυσπιστία για μία αποτελεσματική και χρήσιμη εφαρμογή του συστήματος στο μέλλον.

2 Προστασία Προσωπικών Δεδομένων

2.1 Ιστορική Αναδρομή

Στη Ρώμη στις 4/11/1950, η Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου (ΕΣΔΑ), υπογράφηκε μεταξύ των κρατών μελών του Συμβουλίου της Ευρώπης και τέθηκε σε ισχύ τον Σεπτέμβριο του 1953[2]. Απέβλεπε στην ενίσχυση της προστασίας των δικαιωμάτων που αναφέρονταν στην Σχετική Οικουμενική Διακήρυξη, που είχε ψηφίσει το έτος 1948[3] η Γενική Συνέλευση των Ηνωμένων Εθνών. Δημιουργήθηκε, έτσι, το Ευρωπαϊκό Δικαστήριο των Δικαιωμάτων του Ανθρώπου και προβλέπεται η ενώπιον ατομική προσφυγή, αφού προηγουμένως εξαντληθούν τα ένδικα μέσα στα εθνικά δικαστήρια. Η σύμβαση αυτή ακυρώθηκε από το Ελληνικό κράτος με το Ν.2329/1953 και τέθηκε ξανά σε ισχύ με το Ν.Δ.53/1974[4], έκτοτε αποτελεί μέρος της Ελληνικής έννομης τάξης, με υπερέχουσα ισχύ έναντι των κοινών νόμων, ως διεθνής σύμβαση. Το άρθρο 8 της ΕΣΔΑ[5] αναφέρεται στο σεβασμό της ιδιωτικής και οικογενειακής ζωής, χωρίς ειδική αναφορά του δικαιώματος προστασίας των προσωπικών δεδομένων. Σύμφωνα με την νομολογία του Δικαστηρίου Ανθρωπίνων Δικαιωμάτων το άρθρο 8 ΕΣΔΑ ερμηνεύθηκε ώστε τα προσωπικά δεδομένα να θεωρηθούν ειδικότερη έκφανση του γενικού δικαιώματος στην προστασία της ιδιωτικής ζωής. Η τεχνολογική επανάσταση της πληροφορικής και επικοινωνιών και των επιπτώσεων τους στην προστασία της ιδιωτικής ζωής, υποχρέωσε τα κράτη μέλη του Συμβουλίου της Ευρώπης στην υπογραφή της 108/28.1.1981 Σύμβασης του Συμβουλίου της Ευρώπης[6] για τη προστασία των προσώπων έναντι της αυτοματοποιημένης επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και κυρώθηκε από όλα τα κράτη μέλη της ΕΕ. Η Σύμβαση αυτή ισχύει τόσο στον δημόσιο όσο και στον ιδιωτικό τομέα. Το έτος 1977 με Κοινή Δήλωση το Συμβούλιο,

[2] Σύμβαση για την προστασία των δικαιωμάτων του ανθρώπου και των θεμελιωδών ελευθεριών: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005
[3] Η οικουμενική διακήρυξη των ανθρωπίνων: https://www.un.org/en/universal-declaration-human-rights/
[4] Νομοθετικό διάταγμα 53/1974, Σύμβαση της Ρώμης περί ανθρωπίνων δικαιωμάτων: https://www.tideon.org/koinonia-thesmoi-dikaio/2012-05-04-04-20-18/9849-53-1974
[5] Άρθρο 8 – Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου – Δικαίωμα σεβασμού της ιδιωτικής και οικογενειακής ζωής : https://www.lawspot.gr/nomikes-plirofories/nomothesia/esda/arthro-8-eyropaiki-symvasi-dikaiomaton-toy-anthropoy-dikaioma
[6] Σύμβαση για την προστασία των προσώπων έναντι της αυτόματης επεξεργασίας δεδομένων προσωπικού χαρακτήρα: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

το Κοινοβούλιο και η Επιτροπή διακήρυξαν πανηγυρικά ότι οφείλουν κατά την άσκηση των καθηκόντων τους να σέβονται τα ανθρώπινα δικαιώματα, όπως αυτά κατοχυρώνονται στα εθνικά συντάγματα των κρατών μελών και στην ΕΣΔΑ. Η ίδια διατύπωση επαναλαμβάνεται στην Ενιαία Ευρωπαϊκή Πράξη του 1987[7]. Στις 24 Οκτωβρίου 1995 το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο θέσπισαν την Οδηγία 95/46[8] για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών.

Πρόκειται για ένα από τα πληρέστερα παγκοσμίως κείμενα για την προστασία προσωπικών δεδομένων, το οποίο δεσμεύει τα κράτη μέλη της ΕΕ να εισάγουν και να εφαρμόσουν ένα συγκεκριμένο νομικό σύστημα. Υπό την ισχύ του Συντάγματος του 1975 προστατεύονταν η ιδιωτική και οικογενειακή ζωή, δεν υπήρχε όμως πρόβλεψη για την προστασία των προσωπικών δεδομένων. Είχε, όμως, κριθεί αυτό από το ΣτΕ[9] ότι στην ιδιωτική ζωή περιλαμβάνονταν, μεταξύ άλλων και προστατεύονταν κάθε τι που αφορά την υγεία του προσώπου, οι θρησκευτικές του πεποιθήσεις, η οικογενειακή συμπεριφορά του και η ερωτική του ζωή. Άλλωστε, το δικαίωμα στην προστασία από την επεξεργασία δεδομένων προσωπικού χαρακτήρα μπορούσε να θεμελιωθεί και επί των συνταγματικών διατάξεων σεβασμού της αξίας του ανθρώπου και της ελεύθερης ανάπτυξης της προσωπικότητας που προστατεύονται εξ'άλλου και με την σύμβαση για τα ανθρώπινα δικαιώματα (ΕΣΔΑ). Το έτος 1995 εκδόθηκε η γνωστή Οδηγία 95/46 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου προς τα Κράτη – μέλη «για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών», η οποία τα υποχρέωσε να θέσουν σε ισχύ τις αναγκαίες νομοθετικές κανονιστικές και διοικητικές διατάξεις για να συμμορφωθούν προς το περιεχόμενό της. Το Ελληνικό κράτος συμμορφώθηκε με την ως άνω επιταγή και εξέδωσε τον Ν.2472/1997[10] «περί προστασίας του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα» και ίδρυσε τη ανεξάρτητη Αρχή Προστασίας Προσωπικών Δεδομένων με σκοπό την εποπτεία και έλεγχο της τήρησης του νόμου αυτού, καθώς και άλλων ρυθμίσεων. Με το ψήφισμα της Ζ΄ Αναθεωρητικής Βουλής των Ελλήνων της 6ης Απριλίου 2001[11] προστέθηκε στο Σύνταγμα η διάταξη του άρθρου 9Α με την οποία η προστασία των προσωπικών δεδομένων στην Ελλάδα κατοχυρώθηκε και συνταγματικά. Σύμφωνα με το άρθρο 286[12] της Συνθήκης για την ΕΚ, η Κοινότητα

[7] Ενιαία Ευρωπαϊκή Πράξη του 1987: http://www.europarl.europa.eu/about-parliament/en/in-the-past/the-parliament-and-the-treaties/single-european-act
[8] Οδηγία 95/46 : https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046
[9] Συμβούλιο της Επικρατείας και Διοικητικής Δικαιοσύνης: http://www.adjustice.gr/webcenter/portal/ste?_afrLoop=92122612991190678#!%40%40%3F_afrLoop%3D92122612991190678%26_adf.ctrl-state%3Dk7q9xty78_4
[10] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, Νόμος 2472/1997: https://www.dpa.gr/portal/page?_pageid=33,19052&_dad=portal&_schema=PORTAL
[11] Ψήφισμα της Ζ΄ Αναθεωρητικής Βουλής των Ελλήνων της 6ης Απριλίου 2001: https://www.e-nomothesia.gr/syntagma/psephisma-2001.html
[12] Άρθρο 286 – Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης: https://www.lawspot.gr/nomikes-plirofories/nomothesia/slee/arthro-286-synthiki-gia-ti-leitoyrgia-tis-eyropaikis-enosis

αυτοδεσμεύεται να τηρεί και η ίδια την Οδηγία. Σύμφωνα με την Οδηγία αυτή, «προσωπικά δεδομένα» είναι κάθε πληροφορία που αναφέρεται σε έναν άνθρωπο, η ταυτότητα του οποίου μπορεί να προσδιοριστεί. Καμία χρήση («επεξεργασία») αυτών των δεδομένων δεν επιτρέπεται, αν ο σκοπός της δεν είναι νόμιμος, θεμιτός και καθορισμένος.

Για να είναι νόμιμη η χρήση πρέπει τα δεδομένα να είναι κατάλληλα, ακριβή, συναφή προς τον σκοπό συλλογής και χρήσης και όχι περισσότερα από όσα χρειάζονται ενόψει αυτού του σκοπού. Η χρήση των δεδομένων για άλλο σκοπό από αυτόν που αρχικά συγκεντρώθηκαν, απαγορεύεται. Επίσης δεν πρέπει να διατηρούνται για χρονική διάρκεια πέραν από την αναγκαία για την εξυπηρέτηση του σκοπού για τον οποίο έγινε η συλλογή (άρθρο 5). Αξίζει να ξέρουμε ότι η Ευρωπαϊκή Ένωση για λόγους δημόσιας ασφάλειας, έχει εκδώσει την Οδηγία διατήρησης τηλεπικοινωνιακών δεδομένων για αντεγκλητικούς σκοπούς, το Σχέδιο Απόφασης-Πλαισίου του Συμβουλίου ΕΕ για την προστασία προσωπικών δεδομένων στο πεδίο της αστυνομικής και δικαστικής συνεργασίας των κρατών σε ποινικές υποθέσεις. Στη Ευρωπαϊκή Ένωση υπάρχει ένας νέος κοινοτικός θεσμός: του Ευρωπαίου Επόπτη Προστασίας Δεδομένων, ο οποίος αποτελεί την αρμόδια ανεξάρτητη αρχή της ΕΕ. [10]

Ο GDPR (General Data Protection Regulation) 2016/679[13] είναι μια ρύθμιση στην νομοθεσία της ΕΕ περί προστασίας των δεδομένων και της ιδιωτικής ζωής για όλα τα άτομα εντός της Ευρωπαϊκής Ένωσης και του Ευρωπαϊκού Οικονομικού Χώρου (ΕΟΧ). Αφορά επίσης την εξαγωγή δεδομένων προσωπικού χαρακτήρα εκτός των περιοχών της ΕΕ και του ΕΟΧ. Ο GDPR αποσκοπεί πρωτίστως να δώσει στους ιδιώτες τον έλεγχο των προσωπικών τους δεδομένων και να απλοποιήσει τους κανονισμούς για τις διεθνείς επιχειρήσεις, ενοποιώντας τις ρυθμίσεις εντός της ΕΕ. [11] Για τους σκοπούς της παρούσας οδηγίας, οι διατάξεις της οδηγίας 95/46 / ΕΚ σχετικά με την επεξεργασία των προσωπικών δεδομένων των ατόμων, ανεξαρτήτως θέσης και υποκειμένων των δεδομένων, δηλαδή, την επεξεργασία των προσωπικών δεδομένων των υποκειμένων στο πλαίσιο του ΕΟΧ. Ο GDPR εκδόθηκε στις 14 Απριλίου 2016 και τέθηκε σε ισχύ στις 25 Μαΐου 2018[14]. Ο GDPR είναι ένας κανονισμός, όχι μια οδηγία, που είναι άμεσα δεσμευτική και ισχύει, αλλά παρέχει ευελιξία για ορισμένες πτυχές του κανονισμού που πρέπει να ρυθμιστεί από τα μεμονωμένα κράτη μέλη.

2.2 Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR)

Προσωπικά δεδομένα[15] είναι κάθε πληροφορία και περιγράφει ένα άτομο, όπως στοιχεία αναγνώρισης (ονοματεπώνυμο, ηλικία, κατοικία, επάγγελμα, οικογενειακή

[13] Κανοσιμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32016R0679
[14] Ισχύς του GDPR από 25 Μαΐου 2018: https://eugdpr.org/
[15] Προσωπικά δεδομένα, ευαίσθητα προσωπικά δεδομένα, προστασία των προσωπικών δεδομένων: https://en.wikipedia.org/wiki/Personal_data

κατάσταση κλπ), φυσικά χαρακτηριστικά, εκπαίδευση, εργασία (προϋπηρεσία, εργασιακή συμπεριφορά κλπ), οικονομική κατάσταση (έσοδα, περιουσιακά στοιχεία, οικονομική συμπεριφορά), ενδιαφέροντα, δραστηριότητες, συνήθειες. Το άτομο (φυσικό πρόσωπο) στο οποίο αναφέρονται τα δεδομένα ονομάζεται υποκείμενο των δεδομένων.

Ευαίσθητα χαρακτηρίζονται τα προσωπικά δεδομένα ενός ατόμου που αναφέρονται στη φυλετική ή εθνική του προέλευση, στα πολιτικά του φρονήματα, στις θρησκευτικές ή φιλοσοφικές του πεποιθήσεις, στη συμμετοχή του σε συνδικαλιστική οργάνωση, στην υγεία του, στην κοινωνική του πρόνοια, στην ερωτική του ζωή, τις ποινικές διώξεις και καταδίκες του, καθώς και στη συμμετοχή του σε συναφείς με τα ανωτέρω ενώσεις προσώπων. Τα ευαίσθητα δεδομένα προστατεύονται από τον Νόμο με αυστηρότερες ρυθμίσεις από ότι τα απλά προσωπικά δεδομένα.

Η προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής αποτελεί θεμελιώδες ανθρώπινο δικαίωμα. Ο νόμος παρέχει ορισμένα δικαιώματα στα φυσικά πρόσωπα (υποκείμενα των δεδομένων) και θέτει συγκεκριμένες υποχρεώσεις σε όσους τηρούν και επεξεργάζονται προσωπικά δεδομένα (υπευθύνους επεξεργασίας).

Ο κανονισμός GDPR εισάγει αρκετές αλλαγές στο προηγούμενο νομικό καθεστώς για την προστασία των φυσικών προσώπων αναφορικά με την επεξεργασία των προσωπικών δεδομένων τους και θεσπίζει αυξημένες υποχρεώσεις για οποιονδήποτε οργανισμό επεξεργάζεται προσωπικά δεδομένα. Ο GDPR βασίζεται στις ακόλουθες δύο βασικές αξίες[16]:

1) Την αναγνώριση της προστασίας των προσωπικών δεδομένων που ανήκουν σε ένα άτομο και του ελέγχου της επεξεργασίας των δεδομένων ενός ατόμου ως θεμελιώδες δικαίωμα.
2) Όσον αφορά τους επιχειρηματικούς οργανισμούς, εξασφαλίζει τη βεβαιότητα των επιχειρηματικών διαδικασιών που σχετίζονται με την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Οι υπεύθυνοι επεξεργασίας δεδομένων προσωπικού χαρακτήρα[17] πρέπει να εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα για την εφαρμογή των αρχών προστασίας δεδομένων. Επιχειρηματικές διαδικασίες που χειρίζονται τα προσωπικά δεδομένα πρέπει να σχεδιάζονται και να κατασκευάζονται λαμβάνοντας υπόψη τις αρχές και να παρέχουν εγγυήσεις για την προστασία των δεδομένων (για παράδειγμα, με τη χρήση ψευδούς ή πλήρους ανωνυμίας κατά περίπτωση), και χρησιμοποιώντας τις υψηλότερες δυνατές ρυθμίσεις απορρήτου, έτσι ώστε τα δεδομένα να μην διατίθεται δημόσια χωρίς ρητή, ενημερωμένη συγκατάθεση και δεν μπορούν να χρησιμοποιηθούν για την αναγνώριση ενός υποκειμένου χωρίς την αποθήκευση ξεχωριστών πληροφοριών. Δεν επιτρέπεται η επεξεργασία δεδομένων προσωπικού

[16] Βασικές αξίες του GDPR: https://wso2.com/library/solution-briefs/looking-beyond-gdpr-compliance/
[17] GDRP και υπεύθυνοι επεξεργασίας δεδομένων προσωπικού χαρακτήρα: https://www.gdpreu.org/the-regulation/key-concepts/data-controllers-and-processors/

χαρακτήρα χωρίς τον υπεύθυνο επεξεργασίας ή αν ο υπεύθυνος επεξεργασίας έχει λάβει ξεκάθαρη και εξατομικευμένη επιβεβαίωση της συναίνεσης από το υποκείμενο των δεδομένων. Το υποκείμενο των δεδομένων έχει το δικαίωμα να ανακαλέσει αυτή τη συγκατάθεση ανά πάσα στιγμή.

Ο επεξεργαστής δεδομένων προσωπικού χαρακτήρα πρέπει να γνωστοποιεί με σαφήνεια κάθε συλλογή δεδομένων, να δηλώνει τη νομική βάση και το σκοπό της επεξεργασίας των δεδομένων και να δηλώνει πόσο καιρό διατηρούνται τα δεδομένα και αν κοινοποιούνται σε τρίτους ή εκτός ΕΟΧ. Τα υποκείμενα δεδομένων έχουν το δικαίωμα να ζητήσουν ένα φορητό αντίγραφο των δεδομένων που έχουν συλλεχθεί από έναν επεξεργαστή σε κοινή μορφή και το δικαίωμα να διαγραφούν τα δεδομένα τους υπό ορισμένες συνθήκες. Οι δημόσιες αρχές και οι επιχειρήσεις των οποίων οι κύριες δραστηριότητες είναι υπεύθυνες για την τακτική ή συστηματική επεξεργασία δεδομένων προσωπικού χαρακτήρα καλούνται να προσλάβουν έναν υπεύθυνο προστασίας δεδομένων (DPO), ο οποίος είναι υπεύθυνος για τη διαχείριση της συμμόρφωσης με το GDPR. Οι επιχειρήσεις πρέπει να αναφέρουν τυχόν παραβιάσεις δεδομένων εντός 72 ωρών, εάν έχουν αρνητικές επιπτώσεις στο ιδιωτικό απόρρητο των χρηστών. Σε ορισμένες περιπτώσεις, οι παραβάτες του GDPR μπορεί να τους επιβληθεί πρόστιμο μέχρι 20 εκατομμύρια € και μέχρι 4% του ετήσιου παγκόσμιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, στην περίπτωση μιας επιχείρησης, όποιο από τα δύο είναι μεγαλύτερο.

Όσον αφορά τα υπάρχοντα δεδομένα δεν είναι υποχρεωτική η απόρριψη όλων των υπαρχουσών εγκρίσεων και η λήψη νέας συγκατάθεση από τα άτομα για τη συμμόρφωση με το GDPR. Ωστόσο, είναι απολύτως απαραίτητη η ανασκόπηση της συναίνεσης των ατόμων στα οποία ανήκουν τα προσωπικά δεδομένα και εάν αυτή είναι σύμφωνη, η θεώρηση της υπάρχουσας συγκατάθεσης ως έγκυρη και η συνέχεια της επεξεργασίας των δεδομένων.

Ο GDPR (General Data Protection Regulation) - «Γενικός Κανονισμός για την Προστασία Δεδομένων» [12] (εφεξής«Κανονισμός»),όπως αναφέρθηκε και παραπάνω αφορά στη διαμόρφωση ενός ενιαίου νομοθετικού πλαισίου για την επεξεργασία προσωπικών δεδομένων στα κράτη μέλη της Ευρωπαϊκής Ένωσης και αντικαθιστά την προηγούμενη Νομοθεσία «Οδηγία 95/46/ΕΚ». Η προηγούμενη οδηγία είχε ενσωματωθεί στην Ελληνική Νομοθεσία με το Ν.2472/1997. [13]

Με άλλα λόγια, δεν πρόκειται για κάτι εντελώς νέο. Η προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα είναι θεμελιώδες δικαίωμα. Το άρθρο 8 παράγραφος 1 του Χάρτη των Θεμελιωδών Δικαιωμάτων[18] της Ευρωπαϊκής Ένωσης («Χάρτης») και το άρθρο 16 παράγραφος 1 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ)[19] ορίζουν ότι κάθε

[18] Επεξηγήσεις σχετικά με τον χάρτη των Θεμελιωδών Δικαιωμάτων: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32007X1214(01)
[19] Συνθήκη Λειτουργίας της Ευρωπαϊκής Ένωσης: https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=CELEX:12012E/TXT

πρόσωπο έχει δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν. Ο «κανονισμός» είναι δεσμευτικός ως προς όλα τα μέρη του και ισχύει άμεσα σε κάθε κράτος μέλος, δηλαδή δεν απαιτείται ειδική προσαρμογή της Εθνικής Νομοθεσίας, σύμφωνα με το άρθρο 83[20] του «Κανονισμού».

[21]Ως «δεδομένα προσωπικού χαρακτήρα» θεωρείται 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 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.

Ως «επεξεργασία» θεωρείται κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή.

Ως «υπεύθυνος επεξεργασίας» θεωρείται το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που μεμονωμένα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους.

Ως «εκτελών την επεξεργασία» ορίζεται το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας.

Η «παραβίαση δεδομένων προσωπικού χαρακτήρα» ορίζεται ως η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία.

Η αναφερόμενη «εποπτική αρχή» αποτελεί ανεξάρτητη δημόσια αρχή που συγκροτείται από το κράτος μέλος επιφορτισμένη με την παρακολούθηση της εφαρμογής του παρόντος κανονισμού, με σκοπό την προστασία των θεμελιωδών

[20] Άρθρο 83 – Γενικός Κανονισμός για την Προστασία Δεδομένων – Γενικοί όροι επιβολής διοικητικών προστίμων: https://www.lawspot.gr/nomikes-plirofories/nomothesia/kanonismos-gia-tin-prostasia-dedomenon/arthro-83-genikos-kanonismos
[21] Άρθρο 4 – GDPR - Ορισμοί: https://gdpr-info.eu/art-4-gdpr/

δικαιωμάτων και ελευθεριών των φυσικών προσώπων έναντι της επεξεργασίας που τα αφορούν και τη διευκόλυνση της ελεύθερης κυκλοφορίας δεδομένων προσωπικού χαρακτήρα στην Ένωση.

Ο «Υπεύθυνος Προστασίας δεδομένων» - Data Protection Officer (DPO) είναι το φυσικό ή νομικό πρόσωπο που θα ενημερώνει τους χρήστες των οποίων τα δεδομένα επεξεργάζεται η εταιρεία αλλά και θα είναι εκείνος ο οποίος έρχεται σε επικοινωνία με την Εποπτική Αρχή.

Ο «Φορέας Παρακολούθησης» επιφορτίζεται με την επιφύλαξη των καθηκόντων και των αρμοδιοτήτων της αρμόδιας εποπτικής αρχής. Σύμφωνα με τα άρθρα 57[22] και 58[23], η παρακολούθηση της συμμόρφωσης με κώδικα δεοντολογίας δυνάμει του άρθρου 40 μπορεί να διεξάγεται από φορέα που διαθέτει το ενδεδειγμένο επίπεδο εμπειρογνωμοσύνης σε σχέση με το αντικείμενο του κώδικα και είναι διαπιστευμένος για τον σκοπό αυτόν από την αρμόδια εποπτική αρχή.

Σύμφωνα με το άρθρο 42[24] του Κανονισμού, τα κράτη μέλη, οι εποπτικές αρχές, το Συμβούλιο Προστασίας Δεδομένων και η Επιτροπή παροτρύνουν, ιδίως σε ενωσιακό επίπεδο, τη θέσπιση μηχανισμών πιστοποίησης προστασίας δεδομένων και σφραγίδων και σημάτων προστασίας δεδομένων, με σκοπό την απόδειξη της συμμόρφωσης προς τον παρόντα κανονισμό των πράξεων επεξεργασίας από τους υπευθύνους επεξεργασίας και τους εκτελούντες την επεξεργασία. Λαμβάνονται υπόψη οι ειδικές ανάγκες των πολύ μικρών, των μικρών και των μεσαίων επιχειρήσεων.

2.3 Αρχές Προστασίας Προσωπικών Δεδομένων και Δικαιώματα Υποκειμένου

Παρόλο που ο GDPR φαίνεται να αποτελεί άμεση πρόκληση για τις επιχειρήσεις, υπάρχει πιθανή ευκαιρία για ένα νέο επίπεδο ανάπτυξης αυτών. Ειδικά οι επιχειρήσεις που ξεκίνησαν την υιοθέτιση από νωρίς, μπορούν γρήγορα να αξιοποιήσουν τα οφέλη του. Βέβαια η διαχείριση των προσωπικών δεδομένων θα πρέπει να καθορίζεται ρητά καθώς και να διέπεται από ορισμένες αρχές. Οι εν λόγω αρχές παρατίθενται και αναλύονται παρακάτω[25] :

[22] Άρθρο 57 - GDPR: http://www.privacy-regulation.eu/en/article-57-tasks-GDPR.htm
[23] Άρθρο 58 - GDPR: http://www.privacy-regulation.eu/en/article-58-powers-GDPR.htm
[24] Άρθρο 42 - GDPR: https://www.lawspot.gr/nomikes-plirofories/nomothesia/gdpr/arthro-42-genikos-kanonismos-gia-tin-prostasia-dedomenon
[25] Άρθρο 5 – GDPR – Αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα: https://www.lawspot.gr/nomikes-plirofories/nomothesia/kanonismos-gia-tin-prostasia-dedomenon/arthro-5-genikos-kanonismos

1) Νομιμότητα της επεξεργασίας και διαφάνεια

Οι οργανισμοί πρέπει να διασφαλίζουν ότι υπάρχουν νόμιμοι λόγοι για τη συλλογή και τη χρήση προσωπικών δεδομένων. Η ενεργός συγκατάθεση από έναν πελάτη είναι η ευρέως χρησιμοποιούμενη προσέγγιση, αλλά ο GDPR απαιτεί τη συγκατάθεση για να είναι σαφής, συγκεκριμένη, κοκκώδης, μη τιμολογημένη από άλλες πολιτικές και να δίνεται ελεύθερα. Επιπλέον, ο οργανισμός πρέπει να είναι σε θέση να αποδείξει πότε και πώς ο πελάτης παρείχε τη συγκατάθεσή του.

2) Ακρίβεια

Οι οργανισμοί πρέπει να λάβουν μέτρα για να διασφαλίσουν ότι τα προσωπικά δεδομένα είναι ακριβή. Εάν διαπιστωθεί ότι τα δεδομένα είναι ανακριβή, ο οργανισμός θα πρέπει να ενεργήσει αμέσως για τη διόρθωση ή τη διαγραφή αυτών των δεδομένων.

3) Υπεύθυνος προστασίας δεδομένων – Data Protection Officer (DPO)

Οι οργανισμοί επεξεργάζονται μεγάλα ποσά προσωπικών δεδομένων και αναμένεται να διορίσουν έναν υπεύθυνο προστασίας δεδομένων (Data Protection Officer - DPO), ο οποίος όπως αναφέρθηκε και παραπάνω θα ενεργεί ως ενιαίο σημείο επαφής για τα άτομα και τους εποπτικούς φορείς για θέματα που σχετίζονται με την προστασία των δεδομένων. Ο ΥΠΔ μπορεί επίσης να παρέχει συμβουλές στην οργάνωση σχετικά με τα μέτρα και τις πολιτικές προστασίας δεδομένων. Επίσης μπορεί να είναι μέλος του προσωπικού ή να ανατίθεται σε σύμβαση και ένας όμιλος εταιρειών μπορεί να έχει έναν ΥΠΔ που εποπτεύει τις απαιτήσεις σε ολόκληρη την ομάδα.

4) Αξιολόγηση αντικτύπου προστασίας δεδομένων

Ο GDPR συνιστά στους οργανισμούς να διενεργούν αξιολόγηση επιπτώσεων στην προστασία δεδομένων (DPIA), ανάλογα με τη φύση της επεξεργασίας των δεδομένων, ιδίως όταν υιοθετούν νέες τεχνολογίες.

5) Περιορισμοί επεξεργασίας δεδομένων

Ο σκοπός της επεξεργασίας δεδομένων πρέπει να περιορίζεται στον αρχικό σκοπό στον οποίο ο πελάτης έχει δώσει τη συγκατάθεσή του. Δεν επιτρέπεται η χρησιμοποίηση των συλλεχθέντων προσωπικών δεδομένων για οποιονδήποτε άλλο σκοπό, αφού ο σκοπός έχει ολοκληρωθεί. Η λύση θα μπορούσε να είναι η διαγραφή αυτών των δεδομένων ή η μετατροπή τους σε ανώνυμα ή ψευδώνυμα.

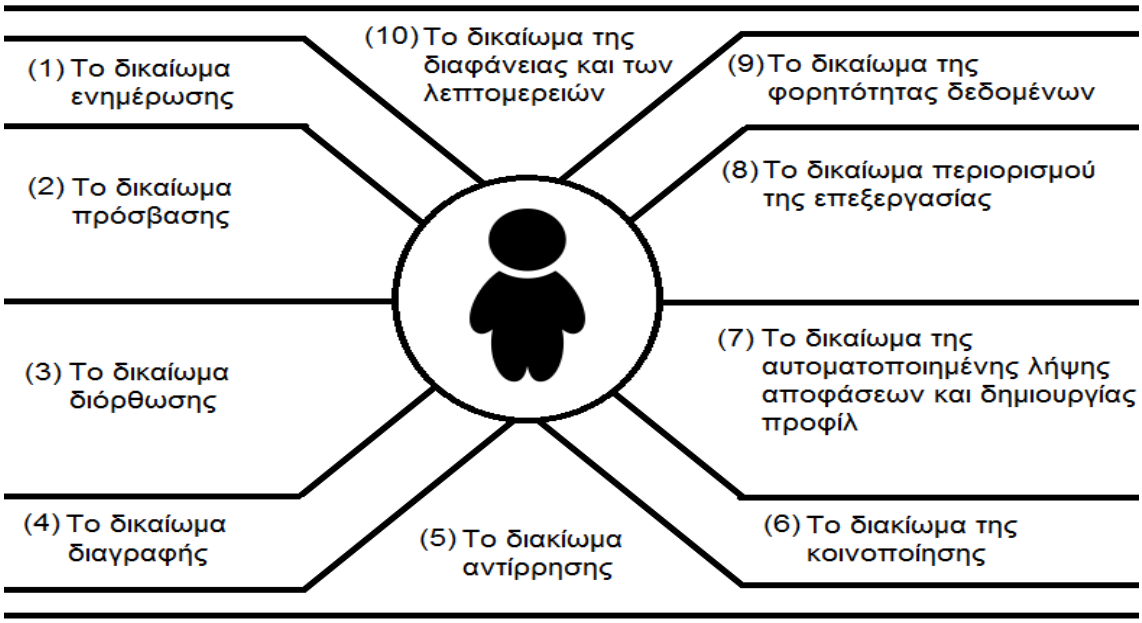
6) Μεταφορά δεδομένων

Κατά τη μεταφορά δεδομένων προσωπικού χαρακτήρα σε χώρα ή οργανισμό που δεν αναφέρεται ως οντότητα με το απαιτούμενο επίπεδο ασφάλειας δεδομένων, ο οργανισμός θα πρέπει να διασφαλίσει ότι ο παραλήπτης τρίτου μέρους έχει εκπληρώσει τα απαιτούμενα μέτρα διασφάλισης ή απαιτεί ρητή συγκατάθεση του ατόμου.

7) Ελαχιστοποίηση δεδομένων

Μόνο προσωπικά δεδομένα που απαιτούνται για τον σκοπό της επεξεργασίας μπορούν να συλλεχθούν και να αποθηκευτούν. Έλεγχος της επιχειρηματικής διαδικασίας και προσδιορισμός του απαιτούμενου συνόλου προσωπικών δεδομένων για επεξεργασία.

Βάσει των παραπάνω και δεδομένου ότι η λειτουργία των οργανισμών θα πρέπει να διέπεται από ορισμένες αρχές γίνεται εύκολα αντιληπτό ότι και τα άτομα ή πελάτες όσον αφορά τα προσωπικά τους δεδομένα έχουν αντίστοιχα ορισμένα δικαιώματα. Τα κυριότερα από τα δικαιώματα[26] αυτά παρουσιάζονται στην επόμενη εικόνα (Εικόνα 1) με την αντίστοιχη συνοπτική περιγραφή του καθενός. [14]



Εικόνα 1: Δικαιώματα Υποκειμένων[27]

(1) Το δικαίωμα ενημέρωσης

Κάθε άτομο πρέπει να ενημερώνεται με τρόπο πρόσφορο και σαφή από τον υπεύθυνο επεξεργασίας όσον αφορά τη μεταποίηση των δεδομένων του. Αυτό περιλαμβάνει το όνομα και τα στοιχεία επικοινωνίας του οργανισμού, το σκοπό της επεξεργασίας των δεδομένων, τη νομική βάση για την επεξεργασία και την προβλεπόμενη χρονική περίοδο που θα διατηρούνται τα δεδομένα του ατόμου, καθώς και τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων. Όλες οι δραστηριότητες επεξεργασίας πρέπει να είναι διαφανείς για το άτομο. Να παρέχονται δηλαδή σαφείς ειδοποιήσεις

[26] Κεφάλαιο 3 – GDPR: https://gdpr-info.eu/chapter-3/
[27] Άρθρο 15 – GDRP: https://gdpr-info.eu/art-15-gdpr/

απορρήτου όπου θα εξηγείται επαρκώς πως ο οργανισμός θα επεξεργαστεί τα προσωπικά δεδομένα.

(2) Το δικαίωμα πρόσβασης

Οι υπεύθυνοι επεξεργασίας έχουν την υποχρέωση να διευκολύνουν τα άτομα να έχουν πρόσβαση στις διαδικασίες προσωπικών δεδομένων τους για να διαπιστώσουν ποια δεδομένα προσωπικού χαρακτήρα έχουν υποστεί επεξεργασία, για ποιο σκοπό κλπ.

(3) Το δικαίωμα διόρθωσης

Εάν τα δεδομένα είναι ανακριβή, τα άτομα μπορούν να ζητήσουν διόρθωση. Εισάγοντας μια φιλική προς το χρήστη, πύλη εξυπηρέτησης πελατών, ώστε οι χρήστες να μπορούν να επαληθεύσουν ποια δεδομένα αποθηκεύονται από τον οργανισμό.

(4) Το δικαίωμα διαγραφής

Επεκτείνοντας την παραπάνω πρόταση, οι οργανισμοί υποχρεούνται επίσης να προσφέρουν στους χρήστες την δυνατότητα διαγραφής των προσωπικών δεδομένων που αυτοί επιθυμούν.

(5) Το δικαίωμα αντίρρησης

Ένα άτομο έχει το δικαίωμα να ζητήσει από έναν οργανισμό να περιορίσει την επεξεργασία των προσωπικών του δεδομένων. Σε τέτοιες περιπτώσεις, ο οργανισμός μπορεί να συνεχίσει να αποθηκεύει τα δεδομένα, αλλά ο σκοπός για τον οποίο μπορούν να υποστούν επεξεργασία τα δεδομένα θα είναι αυστηρά περιορισμένος. Σε αυτή τη κατεύθυνση θα μπορούσε να φανεί πολύ βοηθητική η εισαγωγή ενός εργαλείου διαχείρισης συναίνεσης, ώστε οι πελάτες να μπορούν να παρακολουθούν, να ελέγχουν τη συγκατάθεση και να ανακαλούν τις εγκρίσεις εάν είναι απαραίτητο.

(6) Το δικαίωμα της κοινοποίησης

Ο υπεύθυνος επεξεργασίας έχει την υποχρέωση της ενημέρωσης του υποκειμένου των δεδομένων όσον αφορά την κοινοποίηση αυτών σε τρίτους.

(7) Το δικαίωμα της αυτοματοποιημένης λήψης αποφάσεων και δημιουργίας προφίλ

Ο υπεύθυνος επεξεργασίας έχει την υποχρέωση της ενημέρωσης του υποκειμένου όσον αφορά τη λογική της αυτοματοποιημένης επεξεργασίας.

(8) Το δικαίωμα περιορισμού της επεξεργασίας

Σε περίπτωση που το υποκείμενο αμφισβητήσει την ακρίβεια ή τον τρόπο επεξεργασίας των δεδομένων, έχει το δικαίωμα να «παρέμβει» στον τρόπο

επεξεργασίας των δεδομένων του, όταν για παράδειγμα το υποκείμενο των δεδομένων έχει αντιταχθεί στην αυτοματοποιημένη επεξεργασία.

(9) Το δικαίωμα της φορητότητας δεδομένων

Ένα άτομο έχει το δικαίωμα να διασφαλίσει ότι τα προσωπικά του δεδομένα αποθηκεύονται σε δομημένη, ευρέως χρησιμοποιούμενη και μηχανικά αναγνώσιμη μορφή. Όταν είναι τεχνικά εφικτό, ένα άτομο μπορεί να ζητήσει να μεταφέρει απευθείας τα προσωπικά του δεδομένα από έναν οργανισμό στον άλλο.Η εισαγωγή ενός εργαλείου που επιτρέπει σε ένα άτομο να κατεβάσει τα δικά του δεδομένα σε τυποποιημένες μορφές και μπορεί να διευκολύνει τη μεταφορά δεδομένων πελατών από το ένα σύστημα στο άλλο βάσει ανοικτών προτύπων.

(10) Το δικαίωμα της διαφάνειας και των λεπτομερειών

Καθένας έχει το δικαίωμα να γνωρίζει εάν δεδομένα προσωπικού χαρακτήρα που τον αφορούν αποτελούν ή αποτέλεσαν αντικείμενο επεξεργασίας. Προς τούτο ο υπεύθυνος επεξεργασίας, έχει υποχρέωση να του απαντήσει εγγράφως και λεπτομερώς. [28]

2.4 Νομοθεσία για Προσωπικά Δεδομένα Υγείας

Τα προσωπικά δεδομένα υγείας θεωρούνται ευαίσθητα προσωπικά δεδομένα. Τα δεδομένα προσωπικού χαρακτήρα σχετικά με την υγεία θα πρέπει να περιλαμβάνουν όλα τα δεδομένα που αφορούν την κατάσταση της υγείας του υποκειμένου των δεδομένων. Πιο συγκεκριμένα, τα παραπάνω περιλαμβάνουν όλα τα δεδομένα τα οποία αποκαλύπτουν πληροφορίες για την παρελθούσα, τρέχουσα ή μελλοντική κατάσταση της σωματικής ή ψυχικής υγείας του υποκειμένου των δεδομένων.

Τα προσωπικά δεδομένα υγείας περιλαμβάνουν πληροφορίες σχετικά με το φυσικό πρόσωπο που συλλέγονται κατά την εγγραφή για υπηρεσίες υγείας και κατά την παροχή αυτών όπως αναφέρεται στην οδηγία 2011/24/ΕΕ[29] του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου προς το εν λόγω φυσικό πρόσωπο. Αφορά έναν αριθμό, ένα σύμβολο ή ένα χαρακτηριστικό ταυτότητας που αποδίδεται σε φυσικό πρόσωπο με σκοπό την πλήρη ταυτοποίηση του φυσικού προσώπου για σκοπούς υγείας. Τέτοιου είδους πληροφορίες προκύπτουν από εξετάσεις ή αναλύσεις σε μέρος ή ουσία του σώματος, μεταξύ άλλων από γενετικά δεδομένα και βιολογικά δείγματα και κάθε πληροφορία, παραδείγματος χάριν, σχετικά με ασθένεια, αναπηρία, κίνδυνο ασθένειας, ιατρικό ιστορικό, κλινική θεραπεία ή τη φυσιολογική ή βιοϊατρική κατάσταση του υποκειμένου των δεδομένων, ανεξαρτήτως πηγής, παραδείγματος χάριν, από ιατρό ή άλλο επαγγελματία του τομέα της υγείας, νοσοκομείο, ιατρική συσκευή ή διαγνωστική δοκιμή in vitro. [15]

[28]Κεφάλαιο Γ' – GDPR -Δικαιώματα του Υποκειμένου των Δεδομένων: https://www.dpa.gr/portal/page?_pageid=33,19052&_dad=portal&_schema=PORTAL#11
[29] Οδηγία 2011/24/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32011L0024

Όπως κάθε άλλος οργανισμός έτσι και οι οργανισμοί υγείας υποχρεώνονται από τον GDPR να διαθέτουν υπεύθυνο επεξεργασίας δεδομένων. Προφανώς και ότι αναφέρθηκε παραπάνω όσον αφορά τις αρχές που θα πρέπει να ακολουθεί ένας οργανισμός καθώς και τα δικαιώματα των υποκειμένων δεν παύουν να ισχύουν και σε ότι αφορά και τον κλάδο της υγείας. Πρώτα απ' όλα όμως θα πρέπει να διευκρινιστούν ορισμένες λεπτομέρειες όσον αφορά τα βασικότερα δικαιώματα περί δεδομένων των υποκειμένων στον κλάδο της υγείας που στην συγκεκριμένη περίπτωση είναι οι ασθενείς.

1) Δικαιούται ένας ασθενής πρόσβαση στα δεδομένα υγείας του (στον ιατρικό του φάκελο);

Σύμφωνα με το άρθρο 12 του Ν. 2472/97[30] το υποκείμενο των δεδομένων έχει δικαίωμα να ζητεί και να λαμβάνει από τον υπεύθυνο επεξεργασίας χωρίς καθυστέρηση όλα τα δεδομένα προσωπικού χαρακτήρα που το αφορούν. Επομένως, ένας ασθενής σαφώς και δικαιούται να έχει πρόσβαση στον ιατρικό του φάκελο, ο οποίος μάλιστα περιέχει ευαίσθητα δεδομένα υγείας.

2) Δικαιούται ένας ασθενής να πάρει τον ιατρικό του φάκελο από το νοσοκομείο στο οποίο είχε νοσηλευθεί;

Τα στοιχεία ιατρικού φακέλου ασθενούς που έχει νοσηλευθεί σε νοσοκομείο αποτελούν προσωπικά του δεδομένα και μάλιστα ευαίσθητα επειδή αφορούν την υγεία του. Σύμφωνα με το άρθρο 12 του Ν. 2472/97 το υποκείμενο των δεδομένων έχει δικαίωμα να ζητήσει και να λάβει από τον υπεύθυνο επεξεργασίας χωρίς καθυστέρηση όλα τα δεδομένα προσωπικού χαρακτήρα που το αφορούν. Εν προκειμένω το νοσοκομείο υποχρεούται να χορηγήσει στον νοσηλευθέντα επισήμως θεωρημένα αντίγραφα όλων των ιατρικών εγγράφων (ιατρικές εξετάσεις, γνωματεύσεις και κάθε άλλου είδους ιατρικά έγγραφα) που τον αφορούν και τηρούνται στο αρχείο του Νοσοκομείου.

3) Δικαιούνται συγγενείς ασθενούς πρόσβαση στα δεδομένα υγείας του (στον ιατρικό του φάκελο);

Από το συνδυασμό ιδίως των διατάξεων των Ν. 2472/1997 και 3418/2005 (Κώδικας Ιατρικής Δεοντολογίας)[31] προκύπτει ότι η πρόσβαση τρίτου στα ιατρικά αρχεία ασθενή επιτρέπεται μόνο κατ' εξαίρεση. Αυτό είναι δυνατόν, καταρχήν, σε δύο περιπτώσεις:

- Εφόσον ο τρίτος ταυτίζεται με τον ασθενή, που είναι υποκείμενο των δεδομένων. Αυτό συμβαίνει: (1) εφόσον ο τρίτος έχει την έγγραφη εξουσιοδότηση του ασθενή, ή (2) εφόσον ενεργεί ως νόμιμος εκπρόσωπος του ασθενή (πχ. γονέας ανήλικου τέκνου) ή ως δικαστικός συμπαραστάτης του ασθενή (κατόπιν απόφασης του αρμοδίου δικαστηρίου, που ορίζει συγκεκριμένα πρόσωπα ως δικαστικούς συμπαραστάτες).

[30] Άρθρο 12 – Νόμος 2472/1997 – Δικαίωμα πρόσβασης: https://www.lawspot.gr/nomikes-plirofories/nomothesia/n-2472-1997/arthro-12-nomos-2472-1997-dikaioma-prosvasis
[31] Νόμος 3418/2005 – Κώδικας Ιατρικής Δεοντολογίας: https://www.lawspot.gr/nomikes-plirofories/nomothesia/nomos-3418-2005

- Σύμφωνα με τα οριζόμενα στο άρθρο 7 του Ν. 2472/1997[32], που ορίζει ότι η συλλογή και η επεξεργασία ευαίσθητων δεδομένων, καθώς και η ίδρυση και λειτουργία σχετικού αρχείου, επιτρέπεται μόνο κατ' εξαίρεση, ύστερα από άδεια της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, εφόσον συντρέχει κάποια από τις περιπτώσεις, που προβλέπονται κατά τρόπο περιοριστικό στην παρ. 2 του άρθρου αυτού. Στο πλαίσιο αυτό, επιτρέπεται κατ' εξαίρεση η επεξεργασία ευαίσθητων δεδομένων προσωπικού χαρακτήρα του ασθενή, μετά από σχετική άδεια της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, ιδίως εφόσον η επεξεργασία είναι αναγκαία για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου ή προβλεπόμενου από το νόμο συμφέροντος τρίτου, εάν το υποκείμενο τελεί σε φυσική ή νομική αδυναμία να δώσει τη συγκατάθεσή του ή η επεξεργασία αφορά δεδομένα που δημοσιοποιεί το ίδιο το υποκείμενο ή είναι αναγκαία για την αναγνώριση, άσκηση ή υπεράσπιση δικαιώματος ενώπιον δικαστηρίου ή πειθαρχικού οργάνου (άρθρο 7).

Περνώντας από τα υποκείμενα στην πλευρά των οργανισμών παρακάτω παρουσιάζονται κάποια πιο πρακτικά παραδείγματα εφαρμογής του Κανονισμού στους επαγγελματίες που δραστηριοποιούνται στον κλάδο της υγείας.

Υπάρχουν κατηγορίες επιχειρήσεων και οργανισμών που ενδιαφέρονται ιδιαίτερα για τη γνώση ιατρικών δεδομένων πολιτών. Για παράδειγμα ασφαλιστικές εταιρείες, τράπεζες, αλλά και πολλοί εργοδότες. Χρειάζεται να διασφαλιστεί η προστασία των προσωπικών δεδομένων, η αποκάλυψη να γίνεται μόνο όταν υπάρχει έννομο συμφέρον, ώστε να μην καταλήγουμε σε ιατρικό φακέλωμα του πληθυσμού και παράλληλα, να αποφευχθούν ευγονικού τύπου πρακτικές.

Μεταξύ των αλλαγών που θα επιφέρει η εφαρμογή του νέου κανονισμού, είναι και η διαδικασία λήψης αποτελεσμάτων ιατρικών εξετάσεων. Ήδη, αρκετές μονάδες Υγείας, στον ιδιωτικό και δημόσιο τομέα, σταμάτησαν να αποστέλλουν ηλεκτρονικά τα αποτελέσματα εξετάσεων, ενώ για την παραλαβή τους από τρίτο πρόσωπο, ζητούν εξουσιοδότηση. Τα αποτελέσματα ιατρικών εξετάσεων καταρχήν, πρέπει να παραλαμβάνονται αυτοπροσώπως από τον ασθενή και εάν το ζητήσει ο ίδιος είναι δυνατή και η αποστολή με ηλεκτρονικό ταχυδρομείο. Η ορθή πρακτική για να αποφεύγονται διαρροές είναι να αποστέλλονται κρυπτογραφημένα (κλειδώνεις με τη χρήση λογισμικού, το «κλειδί» να το έχει ο ασθενής). Μέχρι σήμερα η κρυπτογράφηση των προσωπικών δεδομένων για την αποστολή τους μέσω mails δεν ήταν ευρέως διαδεδομένη παρόλο που ήταν απαραίτητη προϋπόθεση για την ασφάλεια των δεδομένων, σύμφωνα και με τις συστάσεις της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

Οι υποχρεώσεις γνωστοποίησης (στις εποπτικές αρχές και στα πρόσωπα στα οποία αναφέρονται τα δεδομένα) ενεργοποιούνται όταν διαπιστώνεται τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, μη εξουσιοδοτημένη γνωστοποίηση προσωπικών δεδομένων ή πρόσβαση σε αυτά. Το πεδίο εφαρμογής του Κανονισμού καταλαμβάνει μόνο τις πραγματικές παραβιάσεις και όχι τις δυνητικές.Ο Κανονισμός απαιτεί από τους υπεύθυνους επεξεργασίας δεδομένων να γνωστοποιούν την παραβίαση στις

[32] Άρθρο 12 – Νόμος 2472/1997 – Επεξεργασία ευαίσθητων δεδομένων: https://www.lawspot.gr/nomikes-plirofories/nomothesia/n-2472-1997/arthro-7-nomos-2472-1997-epexergasia-eyaisthiton

αρμόδιες αρχές προστασίας δεδομένων (εν προκειμένω για την Ελλάδα αρμόδια είναι η "Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα")[33] χωρίς καθυστέρηση και, εν πάση περιπτώσει, εντός 72 ωρών από τη στιγμή που έχουν λάβει γνώση της παραβίασης αυτής. Ειδικότερα, ο Υπεύθυνος Επεξεργασίας οφείλει:

Να γνωστοποιήσει μια παραβίαση στην ΑΠΔΠΧ εάν η παραβίαση ενδέχεται να προκαλέσει κίνδυνο για τα υποκείμενα των δεδομένων καθώς και να ενημερώσει τα ίδια τα υποκείμενα των δεδομένων που θίγονται, εάν η παραβίαση ενδέχεται να τους προκαλέσει υψηλό κίνδυνο.

(α) Συλλογή δεδομένων από τρίτο και όχι από το ίδιο το υποκείμενο των δεδομένων.

Ένας ασθενής (έναντι του οποίου ισχύει η υποχρέωση τήρησης του επαγγελματικού απορρήτου) παρέχει στον ιατρό πληροφορίες σχετικά με την υγεία του που σχετίζονται με μια γενετική πάθηση, την οποία έχουν και πολλοί στενοί συγγενείς του. Ο ιατρός (υπεύθυνος επεξεργασίας δεδομένων), δεσμεύεται από υποχρέωση τήρησης του απορρήτου σε σχέση με τα ιατρικά δεδομένα των ασθενών του. Παράλληλα, ο ασθενής παρέχει στον ιατρό ορισμένα προσωπικά δεδομένα των συγγενών του (υποκείμενα των δεδομένων) που έχουν την ίδια πάθηση. Βάσει του Κανονισμού άρθρο 14)[34], όταν τα δεδομένα προέρχονται από άλλο πρόσωπο εκτός του ίδιου του υποκειμένου, ο υπεύθυνος της επεξεργασίας οφείλει να παρέχει στο υποκείμενο των δεδομένων κάθε απαραίτητη πληροφορία και, μεταξύ άλλων, την πηγή προέλευσης και τους σκοπούς της επεξεργασίας. Ωστόσο, στην προκειμένη περίπτωση, ο ιατρός δεν υποχρεούται να παρέχει στους εν λόγω συγγενείς τις ανωτέρω πληροφορίες, διότι εάν τις παράσχει, παραβιάζεται η υποχρέωση επαγγελματικού απορρήτου, την οποία οφείλει στον ασθενή του. [16]

(β) Παραδείγματα λήψης συγκατάθεσης με ηλεκτρονικά μέσα :

(i) Μια κλινική αισθητικής χειρουργικής ζητά τη ρητή συγκατάθεση ενός ασθενούς για τη μεταφορά του ιατρικού του φακέλου σε έναν εξειδικευμένο ιατρό προκειμένου να εκφράσει τη γνώμη του σχετικά με την κατάσταση του ασθενούς. Το ιατρικό αρχείο τηρείται σε ψηφιακή μορφή. Δεδομένης της ειδικής φύσης των σχετικών πληροφοριών, η κλινική ζητά την ηλεκτρονική υπογραφή του υποκειμένου των δεδομένων προκειμένου αφενός να λάβει έγκυρη ρητή συγκατάθεση και αφετέρου να είναι σε θέση να αποδείξει ότι έχει ληφθεί ρητή συγκατάθεση.

(ii) Η επαλήθευση της συγκατάθεσης σε δύο στάδια μπορεί επίσης να είναι ένας τρόπος έγκυρης ρητής συγκατάθεσης. Για παράδειγμα, ένα υποκείμενο δεδομένων λαμβάνει ένα μήνυμα ηλεκτρονικού ταχυδρομείου που τον ενημερώνει για την πρόθεση του Υπεύθυνου Επεξεργασίας να επεξεργαστεί ένα αρχείο που περιέχει ιατρικά δεδομένα. Ο Υπεύθυνος Επεξεργασίας εξηγεί στο μήνυμα ηλεκτρονικού ταχυδρομείου ότι ζητά τη συγκατάθεσή του για τη χρήση συγκεκριμένων δεδομένων για συγκεκριμένο σκοπό. Εάν το υποκείμενο των δεδομένων συμφωνεί με τη χρήση αυτών των δεδομένων, ο υπεύθυνος επεξεργασίας ζητά από αυτόν να λάβει απάντηση μέσω ηλεκτρονικού ταχυδρομείου που να περιέχει τη δήλωση «Συμφωνώ». Μετά την αποστολή της απάντησης, το υποκείμενο δεδομένων λαμβάνει έναν σύνδεσμο

[33] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα: https://www.dpa.gr/
[34] Άρθρο 14 – GDPR – Πληροφορίες που παρέχονται εάν τα δεδομένα προσωπικού χαρακτήρα δεν έχουν συλλεγεί από το υποκείμενο των δεδομένων: https://www.lawspot.gr/nomikes-plirofories/nomothesia/kanonismos-gia-tin-prostasia-dedomenon/arthro-14-genikos-kanonismos

επαλήθευσης στον οποίο πρέπει να γίνει κλικ ή ένα μήνυμα SMS με κωδικό επαλήθευσης, για να επιβεβαιώσει την παροχή συγκατάθεσης. [16]

2.5 Κατάσταση στην Ευρώπη

Ο Γενικός κανονισμός προστασίας δεδομένων, τέθηκε σε εφαρμογή στις 25 Μαΐου 2018 (άρθρο 99 του «Κανονισμού») στην Ευρωπαϊκή Ένωση και τον Ευρωπαϊκό Οικονομικό χώρο. Το χρονικό διάστημα των δύο ετών, από την ψήφιση δηλαδή του Κανονισμού, μέχρι την έναρξη εφαρμογής του, αποτελούσε περίοδο προσαρμογής για τις επιχειρήσεις.

Η νομοθεσία περί της προστασίας προσωπικών δεδομένων έχει θεωρηθεί ως ένα μέσο ώστε οι κυβερνήσεις των κρατών-μελών της Ευρωπαϊκής Ένωσης να μπορέσουν να εξασφαλίσουν την προστασία προσωπικών δεδομένων. Αξίζει να σημειωθεί ότι πολλές είναι οι περιπτώσεις παραβίασης και διαρροής προσωπικών δεδομένων και πληροφοριών. Αυτά, λοιπόν, τα δυσμενή φαινόμενα καλείται να αντιμετωπίσει η νομοθεσία. Οι κυβερνήσεις ευελπιστούν ότι μέσω της επιβολής αυστηρότερης νομοθεσίας και πολιτικών για την προστασία προσωπικών δεδομένων θα ληφθούν επαρκέστερα μέτρα τα οποία μέχρι τώρα οι επιχειρήσεις δεν είχαν λάβει. Είναι γεγονός ότι επικρατεί προβληματισμός στον κόσμο των επιχειρήσεων σχετικά με το κατά πόσο η σχετική νομοθεσία θα επηρεάσει τη λειτουργία και τις διαδικασίες τους. Μέχρι τώρα, παρότι η νομοθεσία φαινόταν ιδιαίτερα περιοριστική, οι επιχειρήσεις δείχνουν να έχουν μεταβεί ομαλά στην εφαρμογή της. Σίγουρα στο μέλλον θα επηρεαστούν από αυτό το νομικό πλαίσιο οι διαμορφούμενες τεχνολογίες και ο τρόπος εξέλιξής τους.

Ο GDPR θα αποτελέσει αναμφισβήτητα βάση για κάθε είδους νομικό πλαίσιο που θα προκύψει στο μέλλον και αφορά την προστασία της ιδιωτικότητας. Ο διαρκώς μεταβαλλόμενος ψηφιακός κόσμος διαμορφώνει νέες ανάγκες και δεδομένα. Όπως είναι φυσικό, πρέπει να υπάρχει νομική κατοχύρωση των νέων οντοτήτων και καταστάσεων που διαμορφώνονται. Με τον τρόπο αυτό, εξασφαλίζεται η προστασία των δικαιωμάτων νομικών και φυσικών προσώπων στο νέο ψηφιακό κόσμο.

Υπάρχει ιδιαίτερο ενδιαφέρον από τις επιχειρήσεις να ευθυγραμμιστούν με το νέο νομικό πλαίσιο ώστε να αποφύγουν πρώτα από όλα την επιβολή προστίμων, τα οποία σύμφωνα με τον κανονισμό είναι ιδιαίτερα υψηλά. Για το λόγο αυτό, έχει προσληφθεί κατάλληλο προσωπικό, νομικοί ή τεχνικοί σύμβουλοι, καθώς και εξειδικευμένα στελέχη. Με τον τρόπο αυτό, θα προσαρμοστούν στην νέα κατάσταση και θα μπορέσουν να προβλέψουν τα αποτελέσματα αυτής με σκοπό τον καλύτερο δυνατό επιχειρηματικό σχεδιασμό τους.

Το κατά πόσο ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων θα επηρεάσει εξαρτάται από τους αντίστοιχους αρμόδιους εθνικούς φορείς του κάθε κράτους. Συνεπώς, είναι στο χέρι της εκάστοτε επιχείρησης ο βαθμός κατά τον οποίο

θα ευθυγραμμιστεί με τις νέες επιταγές του εκάστοτε εθνικού και ευρωπαϊκού νομικού πλαισίου.

2.6 Πλεονεκτήματα και Μειονεκτήματα νομοθεσίας

- **Πλεονεκτήματα GPDR**

Αναμφισβήτητα το κοινωνικό και οικονομικό περιβάλλον επηρεάζεται από το GDPR και οτιδήποτε αυτό του επιβάλλει. Σε ό,τι αφορά τα πλεονεκτήματα του νέου νομικού πλαισίου, πρέπει να αναφερθεί ότι καλείται να καλύψει κενά του προϋπάρχοντος πλαισίου τα οποία οφείλουν να προσαρμοστούν στις νέες ανάγκες που έχουν προκύψει από τη ραγδαία πλέον εξέλιξη της τεχνολογίας.

1) Βελτίωση ασφάλειας

Πολλά είναι τα φαινόμενα κατά τα οποία παρατηρούνται προσπάθειες εκμετάλλευσης της αδυναμίας προστασίας δικτύων, εφαρμογών, ιστοσελίδων και τέτοιου είδους διαφόρων υποδομών. Η προστασία, λοιπόν, δεδομένων καθίσταται πλέον πιο ευάλωτη εξαιτίας κακόβουλων ενεργειών που προέρχονται είτε από το εξωτερικό είτε από το εσωτερικό περιβάλλον των επιχειρήσεων και οργανισμών.

Μέσω του GDPR, αυξάνεται η προστασία των προσωπικών δεδομένων των επιχειρήσεων που δραστηριοποιούνται εντός της Ευρωπαϊκής Ένωσης ή έχουν πελάτες εκεί. Σε αυτή τη κατεύθυνση ο GDPR μπορεί να βοηθήσει στη δημιουργία μιας ροής εργασίας που θα λαμβάνει υπόψη την ασφάλεια.

Η νομοθεσία απαιτεί από τους οργανισμούς να εντοπίζουν τη στρατηγική ασφαλείας τους και να λαμβάνουν τα κατάλληλα διοικητικά και τεχνικά μέτρα για την προστασία των προσωπικών δεδομένων των πολιτών της ΕΕ. Η καθιέρωση πλήρους ελέγχου σε ολόκληρη την υποδομή πληροφορικής, η δημιουργία υγιέστερης ροής εργασίας προστασίας δεδομένων και βελτίωση της παρακολούθησης της ασφάλειας είναι κάποια από αυτά τα μέτρα. Αυτές οι δραστηριότητες θα βοηθήσουν τους οργανισμούς να μειώσουν τον κίνδυνο «επίθεσης», καθώς και να καταλάβουν καλύτερα τι συμβαίνει στο δίκτυό τους.

Τέλος, η εξασφάλιση της κυβερνο-ασφάλειας εξασφαλίζει την εμπιστοσύνη των πελατών και το γόητρο της εκάστοτε επιχείρησης. Μόνο με τον τρόπο αυτό οι πελάτες θα είναι πρόθυμοι να δώσουν τα προσωπικά τους δεδομένα για επεξεργασία, εξασφαλίζοντάς τους ασφαλές περιβάλλον.[35]

2) Βελτίωση της διαχείρισης δεδομένων

Το πρώτο πράγμα που πρέπει να γίνει για τη συμμόρφωσή με τον GDPR είναι ο έλεγχος όλων των δεδομένων. Αυτό επιτρέπει την ελαχιστοποίηση των δεδομένων

[35] Πλεονεκτήματα και μειονεκτήματα του GDPR: https://www.endpointprotector.com/blog/gdpr-the-pros-and-the-cons/

που συλλέγονται, την καλύτερη οργάνωση και αποθήκευση ώστε να βελτιωθούν οι διαδικασίες διαχείρισης δεδομένων.

Έτσι θα είναι εύκολη η ανίχνευση και απαλλαγή από τα πλεονάζοντα, παρωχημένα και ασήμαντα αρχεία (ROT – Redundant, Outdates, Trivial) που διατηρούν κάποιοι οργανισμοί, αν και δεν έχουν επιχειρηματική αξία. Με τον καθαρισμό των δεδομένων, θα μειωθεί το κόστος αποθήκευσης και επεξεργασίας αυτών των δεδομένων και πιθανώς θα διαγραφούν ευαίσθητα δεδομένα ROT, όπως τα προσωπικά στοιχεία πρώην πελατών, τα οποία και αποτελούν υψηλό και αδικαιολόγητο κίνδυνο για τους οργανισμούς.

Έπειτα αφού αναλυθούν όλα τα δεδομένα, μπορούν να εφαρμοστούν μηχανισμοί για την εκπλήρωση άλλης απαίτησης GDPR - καθιστώντας τα δεδομένα παγκοσμίως αναζητήσιμα μέσω ενός ευρετηρίου. Αυτό βοηθά στον ευκολότερο χειρισμό των αιτημάτων των υποκειμένων που θέλουν να διαγραφούν τα δεδομένα τους. Τέλος η οργάνωση με αυτό τον τρόπο θα βοηθήσει ώστε το προσωπικό να γίνει πιο παραγωγικό και αποδοτικό, ενώ εργάζεται παράλληλα με ακριβή, εύκολα αναζητήσιμα και προσβάσιμα δεδομένα.

3) Αύξηση της απόδοσης της επένδυσης στην αγορά (ROI – Return On Investment)

Μία από τις βασικές αρχές του GDPR είναι ότι οι οργανισμοί πρέπει να εφαρμόσουν μια πολιτική συμμετοχής και να έχουν τη συγκατάθεση του υποκειμένου των δεδομένων για να επεξεργαστούν τα προσωπικά του δεδομένα. Σε συνδυασμό με την απομάκρυνση άσχετων πληροφοριών ROT, σχηματίζεται μία άκαμπτη βάση δεδομένων εξαιρετικά σχετικών πελατών και πελατών που πραγματικά θέλουν να ενημερωθούν.

Με αυτές τις πληροφορίες, οι οργανισμοί είναι σε θέση να πειραματιστούν με το εξειδικευμένο μάρκετινγκ, προσαρμόζοντας τα μηνύματά τους στις συγκεκριμένες ανάγκες και τις συνήθειες ενός σαφώς καθορισμένου κοινού που έχει μεγαλύτερο ενδιαφέρον για τον οργανισμό. Μια τέτοια μέθοδος θα έχει ως αποτέλεσμα υψηλότερα ποσοστά ανταπόκρισης από τους πελάτες και θα αυξήσει την απόδοση της επένδυσης καθώς οι προϋπολογισμοί και οι προσπάθειες θα δαπανηθούν με σύνεση.

4) Ενθάρρυνση της εμπιστοσύνης και της εμπιστοσύνης του κοινού

Η συμμόρφωση με τον GDPR μπορεί να βοηθήσει στην οικοδόμηση σχέσεων εμπιστοσύνης των οργανισμών με τους πελάτες. Κατά τη συγκέντρωση των συγκαταθέσεων για τη χρήση των δεδομένων των υποκειμένων των δεδομένων, θα πρέπει να εξηγείται με σαφήνεια και συνοπτικά ο τρόπος με τον οποίο θα χρησιμοποιούνται τα προσωπικά τους στοιχεία. Δεδομένου ότι οι καταναλωτές γίνονται ολοένα και πιο ύποπτοι για τον τρόπο χειρισμού των δεδομένων τους, η διαφάνεια και η ευθύνη που επιδεικνύεται θα ενθαρρύνουν την εμπιστοσύνη στο

εμπορικό σήμα του εκάστοτε οργανισμού. Έτσι, ένας οργανισμός μπορεί να χρησιμοποιήσει το GDPR για να υπογραμμίσει ότι φροντίζει για το απόρρητο των σημερινών και μελλοντικών πελατών του και στέκεται πάνω από τους ανταγωνιστές του.

5) Δυνατότητα δημιουργίας νέας επιχειρηματικής κουλτούρας

Οι οργανισμοί πρέπει να σκεφτούν το εμπορικό σήμα τους ως ένα αξιοπρεπές ανθρώπινο ον που δεν καταναλώνει μόνο για να διατηρηθεί και να αναπτυχθεί αλλά συμβάλλει και στην κοινότητα.

Ο GDPR αποτελεί ένα πολλά υποσχόμενο πρώτο βήμα προς μια νέα επιχειρηματική κουλτούρα που μπορεί να γίνει ένας κανόνας, μέσω του σεβασμού και της διασφάλισης των δεδομένων όλων των ανθρώπων που εμπιστεύονται τις ευαίσθητες πληροφορίες τους. Λαμβάνοντας υπόψη τον GDPR, καλλιεργούνται οι αξίες της ασφάλειας των δεδομένων στους υπαλλήλους και προωθείται η κοινωνική ευθύνη στις επιχειρήσεις. Με αυτόν τον τρόπο μπορεί ένας οργανισμός να είναι ανάμεσα στους πρώτους που θα εισάγουν μια νέα νοοτροπία που θα σέβεται την ιδιωτικότητα των δεδομένων των πελατών.

Ενώ κανείς δεν αρνείται ότι η συμμόρφωση με τον GDPR είναι δύσκολη, ένας σοφός ηγέτης αντιμετωπίζει αυτή την πρόκληση ως κάτι πιο σημαντικό από το να κάνει ακριβώς το ελάχιστο για να συμμορφωθεί. Τα οφέλη που θα έχει η νομοθεσία μπορούν να δώσουν σε οργανισμούς την ανταγωνιστική διαφοροποίηση που χρειάζονται για να πετύχουν και να είναι από τους πρώτους που εφαρμόζουν μια νέα επιχειρηματική κουλτούρα που ευαισθητοποιείται στην ανθρώπινη ιδιωτικότητα. [17]

- **Μειονεκτήματα GPDR**

Στην αρχική περίοδο επιβολής του οργανισμού, οι οργανισμοί επειδή ήρθαν αντιμέτωποι με μία καινούρια νομοθεσία πανικοβλήθηκαν, δεν ήξεραν τι θα έπρεπε να κάνουν για να συμμορφωθούν καθώς και πόσο θα τους κοστίσει για να το κάνουν. Το γεγονός ότι όλες οι εταιρείες, τόσο μεγάλες όσο και μικρές, πρέπει να συμμορφωθούν με τους κανονισμούς δημιούργησε πανικό ειδικά σε μερικές μικρές επιχειρήσεις.

1) Επιπλέον νομοθεσία

Σε ό,τι αφορά τη νομοθεσία της Ευρωπαϊκής Ένωσης και συγκεκριμένα της Ευρωπαϊκής Επιτροπής, που αποτελεί νομοπαρασκευαστικό όργανο, όταν γίνεται αναφορά στο GDPR, τίθεται ένα ζήτημα «υπερβολικής» νομοθεσίας. Η επιβολή συνεχών περιορισμών στην κάθε είδους μεταφορά ή διαχείρισης δεδομένων ενδεχομένως να αποθαρρύνει το κοινό από την αξιοποίηση των διαδικτυακών υπηρεσιών ή και εφαρμογών. Επίσης η εμφάνιση παραθύρων συγκατάθεσης ή και συναίνεσης στους χρήστες δεν είναι κάτι το ευχάριστο για αυτούς. Σημαντικός παράγοντας για τους χρήστες ή πελάτες είναι οι αντίστοιχες ιστοσελίδες ή εφαρμογές

που χρησιμοποιούν να είναι όσο το δυνατό περισσότερο φιλικές προς τον τελικό χρήστη.

Σε πολλές εταιρείες και οργανισμούς δεν άρεσε το γεγονός ότι θα υπάρξει περισσότερη γραφειοκρατία καθώς και το γεγονός ότι η κυβέρνηση προσπάθησε να τις ρυθμίσει. Αυτή η αίσθηση υπήρχε ιδιαίτερα από εταιρείες που δεν ήταν στην ΕΕ και οι οποίες είχαν μόνο λίγους πελάτες που ήταν από χώρα της ΕΕ.

2) Κόστος προσαρμογής

Ένα από τα σημαντικότερα μειονεκτήματα του Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων είναι προφανώς το κόστος για να συμμορφωθεί η εταιρεία με αυτόν. Για να επιτευχθεί η συμμόρφωση αυτή δεν αρκεί οι εταιρείες απλά να αναπροσαρμόσουν την πολιτική τους. Ανάλογα με το αν διαχειρίζονται προσωπικά δεδομένα πολιτών της Ευρωπαϊκής Ένωσης, πρέπει σε συνεργασία με τον αντίστοιχο Υπεύθυνο Προστασίας Προσωπικών Δεδομένων να εξασφαλίσουν ότι τα προϊόντα και οι υπηρεσίες που παρέχουν τηρούν όλες τις δεσμεύσεις εμπιστευτικότητας και τους αντίστοιχους νομικούς περιορισμούς. [18]

3) Μεγάλα πρόστιμα

Μία άλλη μεγάλη έννοια είναι τα σημαντικά πρόστιμα τα οποία επιβάλλονται στις επιχειρήσεις που δε συμμορφώνονται με τις διατάξεις του κανονισμού GDPR. Τα πρόστιμα για τις επιχειρήσεις ενδεχομένως να φτάνουν έως και τα 20 εκατομμύρια ευρώ ή το 4% των ετήσιων εσόδων για το προηγούμενο οικονομικό έτος, ανάλογα κάθε φορά με το ποιο από τα δύο είναι το μεγαλύτερο σε περίπτωση παράβασης του κανονισμού. Φαίνεται ότι δεν υπάρχει κανένα περιθώριο όταν πρόκειται για την τήρηση των οδηγιών συμμόρφωσης. Όσοι δεν συμμορφώνονται με τους κανόνες θα διαπιστώσουν ότι αντιμετωπίζουν σοβαρότατο πρόβλημα, δεδομένου ότι είναι πιθανόν να ληφθούν έγκαιρα νομικά μέτρα εναντίον εταιρειών.

4) Αύξηση φόρτου εργασίας

Η επεξεργασία δεδομένων με τρόπο που να είναι αποδεκτός από τον GDPR συνεπάγεται επιπλέον χαρακτηριστικά τα οποία πρέπει να ενσωματωθούν στην αρχιτεκτονική του λογισμικού. Αυτό σημαίνει αύξηση του φόρτου εργασίας για τους προγραμματιστές χωρίς απαραίτητα την αντίστοιχη αύξηση μισθού.

Από όλα όσα αναφέρθηκαν παραπάνω γίνεται εύκολα αντιληπτό ότι ο GDPR ήρθε για να μείνει και παρά τα όποια μειονεκτήματά του, θα επανακαθορίσει την ασφάλεια στη νέα ψηφιακή εποχή. Επιπλέον, θα προστατεύσει τα προσωπικά δεδομένα των πολιτών της Ευρωπαϊκής Ένωσης με τις επιχειρήσεις να έχουν νομική ευθύνη.

3 Blockchain Τεχνολογία

3.1 Τι είναι το Blockchain και Ιστορική Αναδρομή

Το Blockchain είναι μία σχετικά πρόσφατη χρονολογικά εφεύρεση, καθώς δημιουργήθηκε μόλις το 2008 και αποτελεί εύρημα ενός ανώνυμου ατόμο ή ακόμα πιθανότερο μίας ομάδας ατόμων, γνωστών με το ψευδώνυμο Satoshi Nakatomo[36]. Η νέα αυτή τεχνολογία προτείνει όσον αφορά τα δεδομένα, αντί να αποθηκεύονται σε ένα μόνο κεντρικό αποθετήριο, να μοιράζεται ένας κατάλογος (Blockchain ledger) με τις πλήρεις συναλλαγές σε ολόκληρο το επιχειρηματικό για παράδειγμα δίκτυο και χωρίς να απαιτείται κεντρικό σημείο ελέγχου. Καθίσταται έτσι αδύνατη η αλλοίωση ή η κλοπή δεδομένων από τρίτους και δημιουργείται εμπιστοσύνη μεταξύ των κόμβων του δικτύου.

Η εμφάνιση αυτής της νέας τεχνολογίας έγινε για πρώτη φορά γνωστή μέσω του Bitcoin, ενός ψηφιακού νομίσματος που βασίστηκε σε ένα πρωτόκολλο που επιτρέπει στους χρήστες του δικτύου να πραγματοποιούν συναλλαγές με εικονικά χρήματα που υπάρχουν μόνο στους υπολογιστές τους με γρήγορο και ασφαλή τρόπο[37]. Ήδη από το 2009 το Blockchain έχει αποκτήσει ευρύτερη χρήση στον κλάδο των χρηματοπιστωτικών υπηρεσιών, με την είσοδο στην αγορά μιας ποικιλίας νέων επιχειρήσεων και υπηρεσιών που επιτρέπουν την ανάληψη επιχειρηματικών δραστηριοτήτων. Η Blockchain τεχνολογία που αρχικά σχεδιάστηκε για τη διατήρηση ενός οικονομικού καταλόγου συναλλαγών, παρατηρήθηκε οτι μπορεί να επεκταθεί και να παρέχει ένα γενικευμένο πλαίσιο για την υλοποίηση εφαρμογών με αποκεντρωμένους υπολογιστικούς πόρους. Καταλαβαίνουμε άρα, ότι η Blockchain τεχνολογία μπορεί να αξιοποιηθεί για κάτι πολύ περισσότερο από ένα μεμονομένο ψηφιακό νόμισμα και αποτελεί μία από τις πρώτες αναγνωρίσιμες μεγάλες υλοποιήσεις αποκεντρωμένου συστήματος που έχουν τη δυνατότητα να αναδιοργανώσουν κάθε είδους ανθρώπινη δραστηριότητα μέσω της ικανότητάς τους να παρέχουν αλληλεπίδραση μεταξύ ανθρώπων χωρίς τριβές με τρίτους μεσολαβητές και με έμπιστο τρόπο.

Το Blockchain βρίσκεται ακόμα στα πρώτα στάδια της ανάπτυξής του (Σχήμα 1). Η πρώτη φάση είναι η φάση εμβρύου. Τα κρυπτονομίσματα είναι αντιπροσωπευτικά αυτού του σταδίου, και το Bitcoin [19] είναι το πιο σημαντικό.

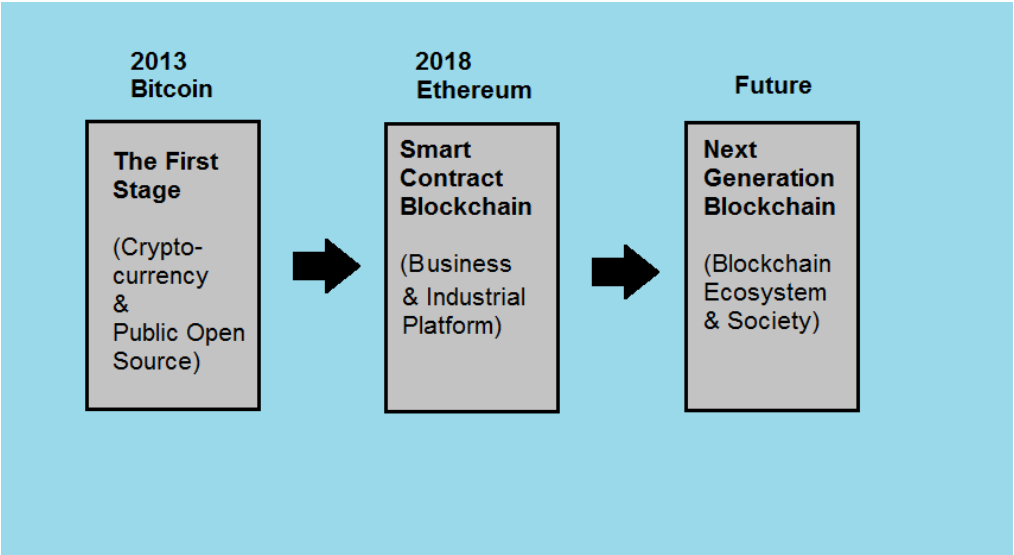
Στη δεύτερη φάση του Blockchain, υποστηρίζεται πια και η δημιουργία προηγμένων έξυπνων συμβολαίων (Smart Contracts) για επιτεύξιμα προγράμματα και εντολές [20], [21], που επεκτείνουν σταδιακά την περιοχή και το πεδίο εφαρμογής του. Αυτή η φάση επεκτείνει την εφαρμογή Blockchain σε διαφορετικές βιομηχανίες και κάνει εφικτή τη συνεργασία μεταξύ τους. Η υιοθέτηση τεχνολογίας Blockchain όχι μόνο

[36] Satoshi Nakatomo, ο δημιουργός του Blockchain: https://en.wikipedia.org/wiki/Satoshi_Nakamoto
[37] Bitcoin και ασφάλεια: https://bitcoin.org/en/faq#security

επιλύει το πρόβλημα της εμπιστοσύνης, αλλά και επιτρέπει την όλο και πιο αυτοματοποιημένη κατανομή πόρων σε παγκόσμια κλίμακα. Σε αυτή τη φάση, το έξυπνο συμβόλαιο έχει χρησιμοποιηθεί και ενσωματωθεί στο σύστημα Blockchain για την αντιμετώπιση των ζητημάτων αμοιβαίας εμπιστοσύνης και ταυτότητας μεταξύ των κόμβων του δικτύου [22]. Συγκεκριμένα, το έργο Hyperledger είναι μία από τις δημοφιλείς υποδομές Blockchain που συνδέονται με την έξυπνη σύμβαση και την εξουσιοδοτημένη αρχή.

Στην επόμενη γενιά οι πτυχές που σχετίζονται με το Blockchain δεν θα επηρεάσουν μόνο την ανθρώπινη ιδεολογία αλλά εν γένει την κοινωνία [23]. Οι κατανεμημένες εφαρμογές συστημάτων τεχνητής νοημοσύνης, όπως η Αποκεντρωμένη Εφαρμογή (Dapp- Decentralized Application) η Αποκεντρωμένη Αυτόνομη Οργάνωση (DAO-Decentralized Autonomous Organization), η Αποκεντρωμένη Αυτόνομη Εταιρεία (DAC-Decentralized Autonomous Corporation), αρχίζουν να εμφανίζονται. Επίσης τα τελευταία χρόνια έχουν διατυπωθεί πολύ ενδιαφέρουσες ιδέες για εφαρμογή της Blockchain τεχνολογίας σε ποικίλλα επιστημονικά πεδία αλλά και στην εξέλιξη "αμφιλεγόμενων" διαδικασιών με τις οποίες ερχόμαστε αντιμέτωποι στην καθημερινότητά μας, όπως για παράδειγμα στη διεξαγωγή μιας ψηφορίας χωρίς νωθεία και με αποδοχή του αποτελέσματος από όλους τους συμμετέχοντες.

Η παρακάτω εικόνα δείχνει τη χρονολογική εξέλιξη της τεχνολογίας Blockchain.



Εικόνα 2: Χρονολογική εξέλιξη της τεχνολογίας Blockchain

3.2 Περιγραφή της Blockchain τεχνολογίας

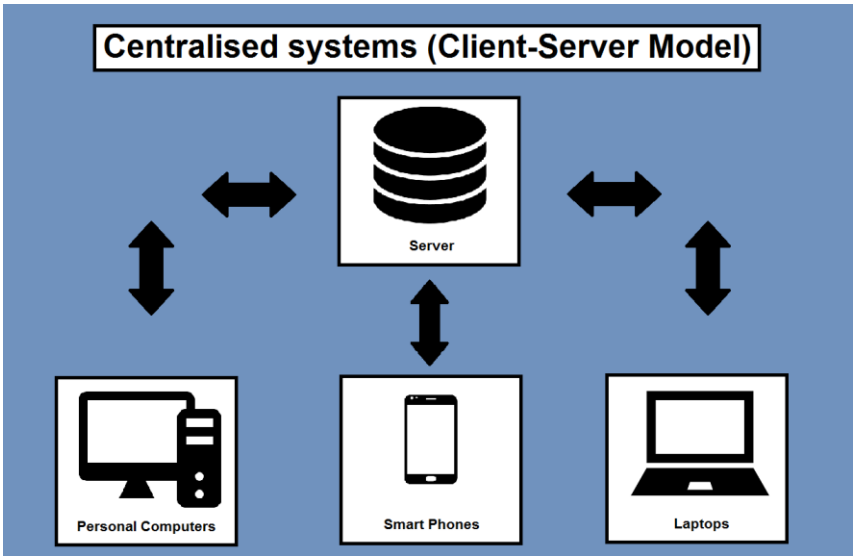
Blockchain είναι ένας αποκεντρωμένος, κατανεμημένος και δημόσιος ψηφιακός κατάλογος (ledger) που χρησιμοποιείται για την καταγραφή συναλλαγών σε πολλούς υπολογιστές έτσι ώστε κάθε εγγραφή που εμπλέκεται να μην μπορεί να τροποποιηθεί αναδρομικά χωρίς την αλλαγή όλων των επόμενων block. Αυτό επιτρέπει στους συμμετέχοντες να επαληθεύουν και να ελέγχουν τις συναλλαγές ανεξάρτητα και σχετικά ανέξοδα. [24] Με λίγα λόγια θα μπορούσαμε να πούμε ότι η τεχνολογία Blockchain βασίζεται σε τρεις θεμελιώδεις πυλώνες που την βοηθούν να κερδίσει

ευρεία αναγνώριση έναντι των υπόλοιπων συστημάτων και αυτοί είναι η αποκέντρωση, η διαφάνεια και η αμεταβλητότητα του συστήματος.

Μία βάση δεδομένων Blockchain διαχειρίζεται αυτόνομα χρησιμοποιώντας ένα δίκτυο peer-to-peer και μία ψηφιακή υπογραφή.[38] Ένα δίκτυο peer-to-peer είναι ένα δίκτυο που επιτρέπει σε δύο ή περισσότερους υπολογιστές να μοιράζονται τους πόρους τους ισοδύναμα. Το δίκτυο αυτό χρησιμοποιεί την επεξεργαστική ισχύ, τον αποθηκευτικό χώρο και το εύρος ζώνης(bandwidth) των κόμβων ενώ όλοι οι κόμβοι του δικτύου έχουν ίσα δικαιώματα. Ένας κόμβος θα μπορούσε να είναι ένας ηλεκτρονικός υπολογιστής. Τέλος, οι πληροφορίες που βρίσκονται στον ένα κόμβο, ανάλογα με τα δικαιώματα που καθορίζονται, μπορούν να διαβαστούν και από τους υπόλοιπους κόμβους και αντίστροφα.[39]

Πριν εμφανιστεί το Blockchain και το Bitcoin η συνήθης πρακτική ήταν τα κεντρικά δίκτυα ή υπηρεσίες. Όσον αφορά τα κεντρικά δίκτυα η λογική είναι πολύ απλή. Υπάρχει μία κεντρική οντότητα, η οποία αποθηκεύει όλα τα δεδομένα και θα πρέπει ένα μέλος του δικτύου να αλληλεπιδρά αποκλειστικά με αυτή για να λάβει τις πληροφορίες που χρειάζεται. Επίσης στα κεντρικά συστήματα όσον αφορά μία συνναλαγή μεταξύ δύο απλών κόμβων του συστήματος είναι απαραίτητη η μεσολάβηση ενός τρίτου φορέα για την επιβεβαίωση της συναλλαγής. Ένα παράδειγμα κεντρικού συστήματος είναι οι τράπεζες, στις οποίες αποθηκεύονται όλα τα χρήματα των καταθετών και ο μόνος τρόπος με τον οποίο μπορεί κάποιος να πληρώσει για κάτι είναι μέσω της τράπεζας, είτε η συναλλαγή είναι ηλεκτρονική είτε είναι φυσική. Ένα άλλο παράδειγμα είναι η αναζήτηση στο Google, όταν θέλουμε να αναζητήσουμε κάτι στο Google ένα query (ερώτημα) στέλνεται στον διακομιστή, ο οποίος στη συνέχεια θα μας απαντήσει για τις σχετικές πληροφορίες.

[38] Blockchain τεχνολογία:https://en.wikipedia.org/wiki/Blockchain
[39] Περιγραφή δικτύου υπολογιστών peer-to-peer (P2P): https://el.wikipedia.org/wiki/Peer-to-peer

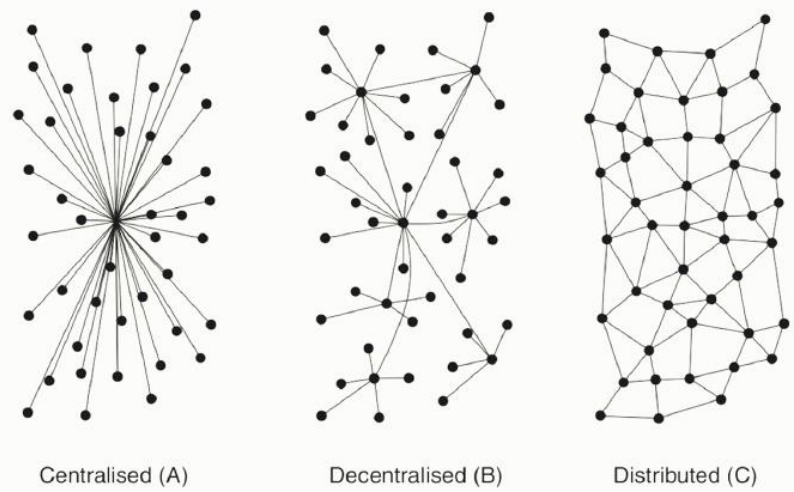


Εικόνα 3: Σύγκριση κεντρικών, αποκεντρωμένων και κατανεμημένων δικτύων όπου οι κόμβοι αναπαριστούν ηλεκτρονικούς υπολογιστές[40]

Τα κεντρικά συστήματα χρησιμοποιούνται εδώ και πολλά χρόνια και ως ένα βαθμό έχουν αντιμετωπίσει αρκετά προβλήματα σε αυτό το διάστημα. Ωστόσο έχουν και σοβαρά μειονεκτήματα, όπως το γεγονός ότι είναι αρκετά ευπαθή σε μία κακόβουλη επίθεση. Αρχικά, επειδή είναι συγκεντρωτικά, όλα τα δεδομένα αποθηκεύονται σε ένα σημείο. Αυτό καθιστά τα κεντρικά συστήματα εύκολους στόχους για πιθανούς χάκερς ή λοιπούς κακόβουλους χρήστες. Έπειτα, σε περίπτωση που το κεντρικό σύστημα πρόκειται να περάσει από αναβάθμιση λογισμικού, θα ήταν αναπόφευκτη η διακοπή της λειτουργίας του, στην καλύτερη το σύστημα υπολειτουργεί μέχρι να ολοκληρωθεί η αναβάθμιση. Σε περίπτωση αναβάθμισης ή για οποιονδήποτε άλλο λόγο τερματιστεί η λειτουργία της κεντρικής οντότητας τότε κανένα μέλος του δικτύου δεν θα μπορεί να έχει πρόσβαση στις πληροφορίες που διαθέτει. Τέλος, στο σενάριο της χειρότερης περίπτωσης, αν αυτή η κεντρική οντότητακαταστραφεί ή γίνει κακόβουλη, όλα τα δεδομένα που βρίσκονται στο δίκτυο θα παραβιαστούν.

Από την άλλη πλευρά σε ένα αποκεντρωμένο σύστημα οι πληροφορίες δεν αποθηκεύονται από μία κεντρική οντότητα. Στην πραγματικότητα όλοι στο δίκτυο κατέχουν τις πληροφορίες. Αυτή είναι και η κύρια διαφορά μεταξύ μιας κεντρικής βάσης δεδομένων και του Blockchain. Τα δεδομένα που βρίσκονται σε ένα δίκτυο προσωπικών υπολογιστών, όπως προαναφέρθηκε ονομάζονται κόμβοι και δεν υπάρχει κεντρική οντότητα ή οργάνωση, (για παράδειγμα μια κυβέρνηση ή μια τράπεζα) η οποία να ελέγχει τα δεδομένα τους. Αντιθέτως όλα τα δεδομένα διαμοιράζονται δημόσια, αν και το περιεχόμενο των εκάστοτε δεδομένων είναι προσβάσιμο μόνο σε όσους έχουν την αντίστοιχη άδεια για το συγκεκριμένο αριθμό δεδομένων. [25]

[40] Παράδειγμα του παραδοσιακού μοντέλου Client-server: https://blockgeeks.com/guides/what-is-blockchain-technology/?fbclid=IwAR19gOJahvGs6g51iY7EdsoZ5Db2TMOpUOkAvb2gkTLl4zsBvMzPw473uXQ



Εικόνα 4: Σύγκριση κεντρικών, αποκεντρωμένων και κατανεμημένων δικτύων όπου οι κόμβοι αναπαριστούν ηλεκτρονικούς υπολογιστές[41]

3.2.1 Επαλήθευση Ταυτότητας

Υπάρχουν δύο βασικές κρυπτογραφικές έννοιες που υποστηρίζουν την τεχνολογία Blockchain. Το πρώτο είναι το hashing, και το δεύτερο είναι οι ψηφιακές υπογραφές (digital signatures).

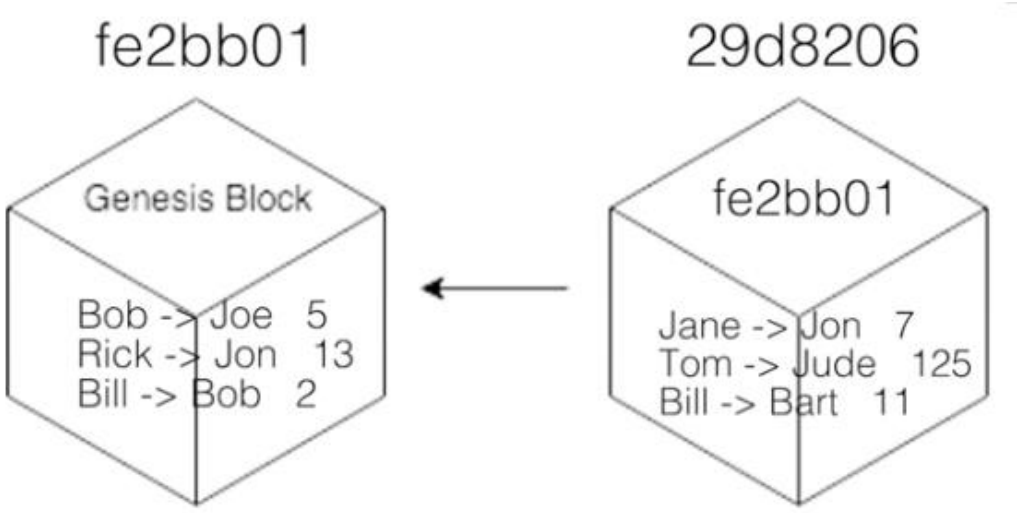
- **Hash**

Οι αλγόριθμοι hash αναφέρονται στην έννοια της λήψης μιας αυθαίρετης ποσότητας δεδομένων εισόδου, την εφαρμογή κάποιου αλγορίθμου σε αυτήν και στη δημιουργία δεδομένων εξόδου σταθερού μεγέθους που ονομάζεται hash. Η είσοδος μπορεί να είναι οποιοσδήποτε αριθμός δυαδικών ψηφίων που θα μπορούσε να αντιπροσωπεύει έναν μόνο χαρακτήρα. Μια είσοδος θα μπορούσε για παράδειγμα να είναι ένα αρχείο MP3, ένα ολόκληρο μυθιστόρημα, ένα υπολογιστικό φύλλο τραπεζικού ιστορικού, ο Ηλεκτρονικός Φάκελος Υγείας ενός ασθενούς ή ακόμα και ολόκληρο το Διαδίκτυο. Το σημαντικό είναι ότι η είσοδος μπορεί να είναι απείρως μεγάλη. Ο κατάλληλος αλγόριθμος hash μπορεί να επιλεγεί ανάλογα με τις ανάγκες του εκάστοτε συστήματος καθώς υπάρχουν πολλοί αλγόριθμοι hash που διατίθενται στο κοινό. Η σημασία αυτών των αλγορίθμων εστιάζεται στο γεγονός οτι παίρνουν μία άπειρη είσοδο δυαδικών ψηφίων και εφαρμόζοντας κάποιους μαθηματικούς υπολογισμούς εξάγουν ένα πεπερασμένο αριθμό δυαδικών ψηφίων.

[41] Η έννοια της αποκέντωσης: https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

Εικόνα 5: Λειτουργία αλγορίθμων Hash

Τα hashes χρησιμοποιούνται σε Blockchains για να αντιπροσωπεύουν την τρέχουσα κατάσταση του δικτύου. Η είσοδος είναι ολόκληρη η κατάσταση του Blockchain, δηλαδή όλες οι συναλλαγές που έχουν πραγματοποιηθεί μέχρι την τρέχουσα στιγμή και η προκύπτουσα hash εξόδος αντιπροσωπεύει την τρέχουσα κατάσταση του Blockchain. Οι αλγόριθμοι hash χρησιμοποιούνται για να συμφωνηθεί μεταξύ όλων των μελών του δικτύου ότι βρίσκονται στην ίδια κατάσταση (κοινή βάση).

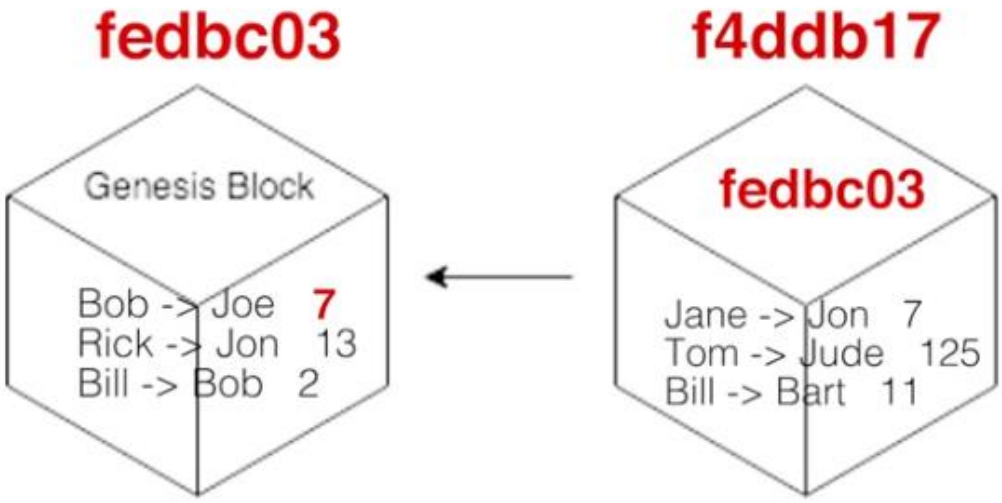


Εικόνα 6: Κάθε block έχει τα δεδομένα του, το hash του και τον δείκτη hash του προηγούμενου block[42]

Για τον υπολογισμό των hashes χρησιμοποιείται η ακόλουθη πρακτική. Το πρώτο hash υπολογίζεται για το πρώτο block χρησιμοποιώντας τις συναλλαγές εντός αυτού του block. Η ακολουθία των αρχικών συναλλαγών χρησιμοποιείται για τον υπολογισμό ενός hash block για το πρώτο block. Για κάθε νέο block που παράγεται από αυτό το σημείο και έπειτα, χρησιμοποιείται επίσης το hash του προηγούμενου block, καθώς και οι δικές του συναλλαγές, ως είσοδος για τον προσδιορισμό του hash του νέου block. Με αυτόν τον τρόπο σχηματίζεται μια αλυσίδα από blocks. Αυτό το σύστημα εξαναγκασμού εγγυάται ότι δεν μπορεί να παραβιαστεί καμία συναλλαγή στην ιστορία, επειδή αν αλλάξει κάποιο τμήμα της συναλλαγής, το ίδιο ισχύει και για το hash του αντίστοιχου block καθώς και των επόμενων. Θα ήταν αρκετά εύκολο να εντοπιστούν τυχόν παραβιάσεις, μόνο μέσα από την σύγκριση των hashes. Το

[42]Hashes και η λειτουργία τους: https://blockgeeks.com/guides/what-is-hashing/

χαρακτηριστικό αυτό είναι αρκετά χρήσιμο επειδή όλοι στο blockchain χρειάζεται μόνο να συμφωνήσουν σε ένα αριθμό από bits για να αντιπροσωπεύσουν την δυνητικά άπειρη κατάσταση του Blockchain. Το Blockchain του Ethereum για παράδειγμα είναι σήμερα δεκάδες gigabytes, αλλά η τρέχουσα κατάσταση του blockchain, από αυτή την εγγραφή, είναι ένα δεκαεξαδικό hash που αντιπροσωπεύει 256 bits.



Εικόνα 7: Οποιαδήποτε τροποποίηση ενός στοιχείου ενός block επιφέρει μεταβολή στο hash του συγκεκριμένου αλλά και των επόμενων block[43]

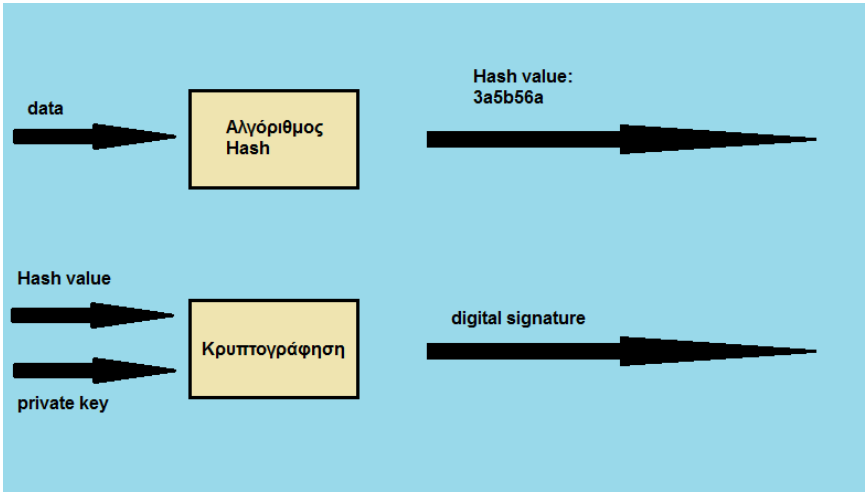
- **Digital signature**

Οι ψηφιακές υπογραφές (digital signatures) όπως οι πραγματικές υπογραφές αποτελούν έναν τρόπο πιστοποίησης ότι κάποιος είναι αυτός που λέει ότι είναι, με την διαφορά ότι χρησιμοποιείται κρυπτογραφία και μαθηματικά, γεγονός που τις κάνει πιο ασφαλείς σε σχέση με τις πραγματικές υπογραφές. Μία ψηφιακή υπογραφή αποτελεί επίσης έναν τρόπο να αποδειχθεί ο πραγματικός αποστολέας ενός μηνύματος.

Σε ασύμμετρα συστήματα κρυπτογράφησης, οι χρήστες δημιουργούν ένα ζεύγος κλειδιών (key pair), το οποίο αποτελείται από ένα δημόσιο κλειδί (public key) και ένα ιδιωτικό κλειδί (private key) χρησιμοποιώντας έναν γνωστό αλγόριθμο. Τα δύο κλειδιά συνδέονται μεταξύ τους μέσω ορισμένων μαθηματικών σχέσεων. Το public key προορίζεται να διανεμηθεί δημόσια ενώ το private key πρέπει να διατηρείται μυστικό και χρησιμοποιείται για την ψηφιακή υπογραφή μηνυμάτων που αποστέλλονται σε άλλους χρήστες. Η υπογραφή περιλαμβάνεται στο μήνυμα, έτσι ώστε ο παραλήπτης να μπορεί να επαληθεύσει τη χρήση του public key του αποστολέα. Με αυτόν τον τρόπο, ο παραλήπτης μπορεί να είναι σίγουρος για την

[43] Μεταβολή των hashes: https://blockgeeks.com/guides/what-is-hashing/

πραγματική ταυτότητα του αποστολέα που έχει στείλει το μήνυμα. Η δημιουργία ενός ζεύγους κλειδιών είναι ανάλογη με τη δημιουργία ενός λογαριασμού στο Blockchain. Επίσης, κάθε συναλλαγή που εκτελείται στο Blockchain υπογράφεται ψηφιακά από τον αποστολέα χρησιμοποιώντας το private key. Αυτή η υπογραφή διασφαλίζει ότι μόνο ο κάτοχος του λογαριασμού μπορεί να μεταφέρει χρήματα από το λογαριασμό.[44] Στην παρακάτω εικόνα φαίνεται γραφικά ο τρόπος με τον οποίο προκύπτει μια ψηφιακή υπογραφή (digital signature). [26]

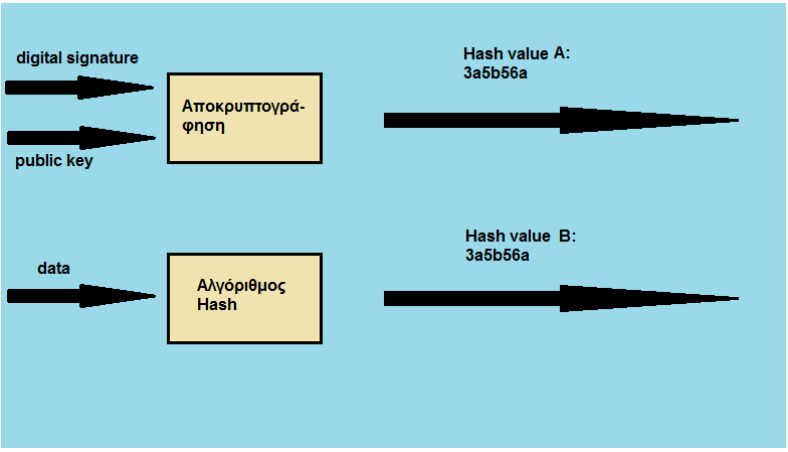


Εικόνα 8: Δημιουργία ψηφιακής υπογραφής (digital signature)[45]

Τα βελάκια αποτελούν τιμές εισόδου και εξόδου αντίστοιχα ενώ τα κουτιά παριστάνουν συναρτήσεις, οπότε εύλογα προκύπτουν οι παρακάτω σχέσεις:

1) Hash value = Hash (data)
2) Digital signature = Κρυπτογράφηση (Hash value , private key)

Στην παρακάτω εικόνα φαίνεται η διαδικασία επαλήθευσης του αποστολέα.



Εικόνα 9: Διαδικασία επαλήθευσης αποστολέα[46]

[44] Σημασία των digital signatures στην Blockchain τεχνολογία: https://blockgeeks.com/what-is-hashing-digital-signature-in-the-blockchain/
[45] Digital signatures και ο τρόπος δημιουργίας τους: https://www.mobilefish.com/services/signature/signature.php?method=realistic

3) Hash value A = Αποκρυπτογράφηση (digital signature , public key)
4) Hash value B = Hash (data)

Συγκρίνοντας οπότε τις τιμές των hash value A και hash value B και εφόσον αυτές είναι ίσες, βγαίνει το ασφαλές συμπέρασμα ότι το μήνυμα που δεχτήκαμε στάλθηκε όντως από τον αναμενόμενο αποστολέα.

Συνοψίζοντας το Blockchain δεν θα μπορούσε να υπάρξει χωρίς hashing και digital signatures. Το hashing παρέχει έναν τρόπο έτσι ώστε τα μέλη του συστήματος να συμφωνήσουν για μία κοινή βάση, ενώ οι ψηφιακές υπογραφές παρέχουν έναν τρόπο ώστε να διασφαλιστεί ότι όλες οι συναλλαγές γίνονται μόνο από τους νόμιμους ιδιοκτήτες. Αυτές οι δύο ιδιότητες διασφαλίζουν ότι το Blockchain δίκτυο παραμένει έμπιστο.

- **Έξυπνα συμβόλαια (smart contracts)**

Ο όρος «έξυπνα συμβόλαια» αναφέρεται σε ψηφιακά συμβόλαια στα οποία έχει ενσωματωθεί κώδικας και τα οποία εκτελούνται αυτόματα αν πληρούνται οι προϋποθέσεις που έχουν τεθεί. Αν και τα συμβόλαια αυτά υπάρχουν εδώ και πολλά χρόνια στην πιο απλή μορφή τους, όπως για παράδειγμα στην περίπτωση ενός αυτόματου πωλητή, η ενσωμάτωσή της λειτουργίας τους μέσα από την τεχνολογία Blockchain τους δίνει νέες δυνατότητες. Χαρακτηριστική περίπτωση αποτελεί ο λεγόμενος διακόπτης εκκίνησης (starter interrupter), δηλαδή, η συσκευή η οποία έχει ενσωματωμένο ένα τέτοιο συμβόλαιο, το οποίο εκτελείται αυτόματα σε περίπτωση που παραβιαστούν οι όροι χρηματοδότησης για την απόκτηση του αυτοκινήτου οπότε και δεν επιτρέπει την εκκίνηση του κινητήρα.

Η τεχνολογία Blockchain όχι μόνο καταργεί την ανάγκη για την ύπαρξη τρίτων μερών, αλλά εξασφαλίζει ότι όλοι οι συμμετέχοντες γνωρίζουν τις λεπτομέρειες του συμβολαίου και ότι οι συμβατικοί όροι θα εκπληρώνονται αυτόματα όταν πληρωθούν ορισμένες προϋποθέσεις. Τα συμβαλλόμενα μέρη σε ένα έξυπνο συμβόλαιο διαπραγματεύονται τους βασικούς όρους, όπως προδιαγραφές των προϊόντων, ποσότητα, τίμημα, χρόνο και τόπο εκπλήρωσης μέσω του Blockchain. Αν εκατομμύρια υπολογιστές βεβαιώσουν ότι έγινε μια δοσοληψία και οι υπολογιστές αυτοί είναι ουδέτεροι και δεν κάνουν υπολογιστικά λάθη, τότε μπορεί κάποιος να υποθέσει με εξαιρετικά μεγάλο βαθμό βεβαιότητας ότι η πληρωμή αυτή, έλαβε χώρα.

Το παράδειγμα του διακόπτη εκκίνησης είναι ακόμη πιο χαρακτηριστικό των δυνατοτήτων του συνδυασμού των έξυπνων συμβολαίων και της τεχνολογίας Blockchain. Αντί ο προγραμματισμός του λογισμικού συμβολαίου (contractware) να καθορίζεται από τον δανειστή, θα καθορίζεται και θα εκτελείται από την πλατφόρμα Blockchain. Κανένα από τα μέρη δεν χρειάζεται να εμπιστεύεται το άλλο για την εκτέλεση του συμβολαίου αλλά την ουδέτερη πλατφόρμα Blockchain, η οποία θα

[46] Αποκρυπτογράφηση και επαλήθευση αποστολέα: https://www.mobilefish.com/services/signature/signature.php?method=realistic

εκτελεί τους σχετικούς συμβατικούς όρους όταν πληρωθούν οι προσυμφωνημένες προϋποθέσεις.[47]

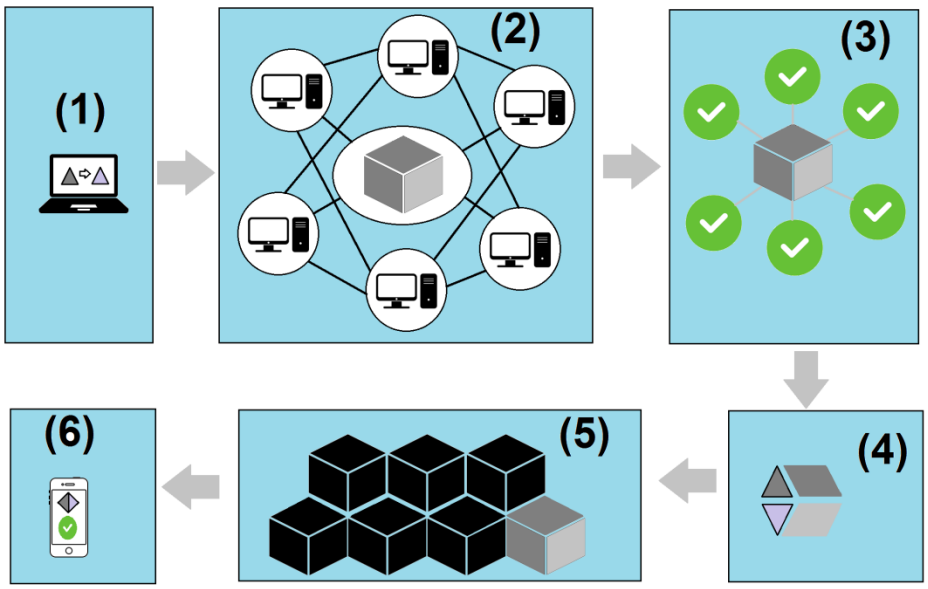
Η εφαρμογή της νέας τεχνολογίας μπορεί να μειώσει τις δαπάνες και τους πιστωτικούς κινδύνους για τους δανειστές, καθώς η εκτέλεση των όρων των συμβολαίων θα γίνεται αυτοματοποιημένα και το ποσοστό ανάκτησης του αντικειμένου εξασφάλισης θα είναι υψηλότερο. Αυτό με τη σειρά του θα μειώσει το κόστος χρηματοδότησης, με χαμηλότερα επιτόκια, τουλάχιστον για όσους οφειλέτες αποδεχτούν την αυστηρότητα και την ακαμψία των όρων ενός έξυπνου συμβολαίου.

3.2.2 Συναλλαγές

Αφού εξηγήθηκαν κάποιοι βασικοί όροι που βοηθούν στην κατανόηση της τεχνολογίας Blockchain θα εστιάσουμε πια στις συναλλαγές και στον τρόπο με τον οποίο αυτές πραγματοποιούνται. Οι συναλλαγές λοιπόν πιστοποιούνται με μαζική συνεργασία που βασίζεται σε κοινά συμφέροντα. Ένας τέτοιος σχεδιασμός διευκολύνει τη στιβαρή ροή εργασιών, όπου η αβεβαιότητα των συμμετεχόντων σχετικά με την ασφάλεια των δεδομένων είναι περιθωριακή. Η χρήση ενός Blockchain αφαιρεί το χαρακτηριστικό της άπειρης αναπαραγωγιμότητας ενός ψηφιακού στοιχείου. Επιβεβαιώνει ότι κάθε μονάδα αξίας μεταφέρθηκε μόνο μία φορά, επιλύοντας το μακροχρόνιο πρόβλημα των διπλών δαπανών. Η ασφάλεια των συναλλαγών διασφαλίζεται επειδή όλα τα μέλη του δικτύου διατηρούν ένα πλήρες αντίγραφο του Blockchain ledger και έτσι δεν είναι δυνατό για ένα μέλος να τροποποιήσει ή να αλλάξει δεδομένα.

Μια αλυσίδα αποτελούμενη από block έχει περιγραφεί ως πρωτόκολλο ανταλλαγής τιμών. Ένα Blockchain μπορεί να διατηρήσει τα δικαιώματα του τίτλου επειδή, όταν έχει ρυθμιστεί σωστά για να διευκρινίσει τη συμφωνία ανταλλαγής, παρέχει ένα αρχείο που υποχρεώνει την προσφορά και την αποδοχή. Επομένως, το Blockchain λειτουργεί ως μία και μοναδική πηγή αλήθειας και τα μέλη σε ένα Blockchain δίκτυο μπορούν να δουν μόνο εκείνες τις συναλλαγές που σχετίζονται με αυτούς.

[47] Περιγραφή των smart contracts: https://m.naftemporiki.gr/story/1363055



Εικόνα 10: Blockchain τεχνολογία[48]

Όπως φαίνεται και στην παραπάνω εικόνα γίνονται με την σειρά οι παρακάτω ενέργειες :

(1) Κάποιος ζητά μία συναλλαγή.
(2) Η ζητούμενη συναλλαγή μεταδίδεται σε ένα δίκτυο P2P που αποτελείται από υπολογιστές, γνωστούς ως κόμβους. Το δίκτυο των κόμβων επικυρώνει τη συναλλαγή και τη κατάσταση του χρήστη χρησιμοποιώντας κάποιο γνωστό αλγόριθμο.
(3) Μία επαληθευμένη συναλλαγή μπορεί να περιλαμβάνει κρυπτογράφηση, συμβόλαια, αρχεία ή άλλες πληροφορίες.
(4) Μόλις επαληθευτεί, η συναλλαγή συνδυάζεται με άλλες συναλλαγές για να δημιουργηθεί ένα νέο block δεδομένων για το Blockchain ledger.
(5) Το νέο block προστίθεται στο υπάρχον Blockchain, με τρόπο που πλέον είναι μόνιμο και αναλλοίωτο.
(6) Η συναλλαγή ολοκληρώνεται.

Κάποια από τα πιο γνωστά παραδείγματα δημόσιων και ευρέως διαδεδομένων συστημάτων Blockchain είναι το Bitcoin και το Ethereum. Με βάση την εφαρμογή του εικονικού νομίσματος που είναι γενικά προσβάσιμο από κάθε άτομο, απαιτείται η ύπαρξη δημόσιου δικτύου, χωρίς εμπόδια για τη συναλλαγή ή καταγραφή του ή και για την πρόσβαση στο πλήρες ιστορικό των συναλλαγών. Αυτό επιτρέπει να διατηρηθεί το άνοιγμα του συστήματος και να αφαιρεθεί οποιαδήποτε λογοκρισία από τους χρήστες. Ωστόσο, η εφαρμογή Blockchain διερευνάται ακόμα στο πλαίσιο της επιχείρησης. Συνήθως, οι λύσεις Blockchain για επιχειρήσεις προορίζονται για ιδιωτική ενδοεταιρική χρήση και όφελος, επομένως οι λειτουργίες εγγραφής και ανάγνωσης επιτρέπονται και απαιτούν από τους συμμετέχοντες να εξουσιοδοτηθούν

[48] Υλοποίηση μίας συναλλαγής μέσω της τεχνολογίας Blockchain:https://blockgeeks.com/guides/what-is-blockchain-technology/

ώστε να τις αξιοποιήσουν. Επίσης το δίκτυο Blockchain εμποδίζει οποιονδήποτε συμμετέχοντα ή ομάδα συμμετεχόντων να ελέγχουν την υποκείμενη υποδομή ή να υπονομεύουν ολόκληρο το σύστημα. Οι συμμετέχοντες στο δίκτυο μπορούν να είναι άτομα, κρατικοί φορείς, οργανισμοί ή ένας συνδυασμός όλων αυτών των τύπων συμμετεχόντων. Στον πυρήνα του, το σύστημα καταγράφει τη χρονολογική σειρά των συναλλαγών με όλους τους κόμβους που συμφωνούν με την εγκυρότητα των συναλλαγών χρησιμοποιώντας το επιλεγμένο μοντέλο συναίνεσης. Το αποτέλεσμα είναι συναλλαγές που δεν μπορούν να τροποποιηθούν ή να αντιστραφούν, εκτός εάν η αλλαγή συμφωνηθεί από όλα τα μέλη του δικτύου σε μια μεταγενέστερη συναλλαγή.

- **Blocks**

Τα blocks κρατούν παρτίδες έγκυρων συναλλαγών που κωδικοποιούνται σε ένα Merkle tree. [27] Στην επιστήμη των υπολογιστών, το Merkle tree είναι ένα δέντρο στο οποίο κάθε κόμβος που είναι φύλλο φέρει την ετικέτα του κατακερματισμού ενός μπλοκ δεδομένων και κάθε κόμβος που δεν είναι φύλλο επισημαίνεται με τον κρυπτογραφικό κατακερματισμό των ετικετών των κόμβων που είναι παιδιά του, εν γένει επιτρέπει την αποτελεσματική και ασφαλή επαλήθευση του περιεχομένου των μεγάλων δομών δεδομένων.[49] Με αυτό το τρόπο κάθε block περιλαμβάνει τον κρυπτογραφικό κατακερματισμό του προηγούμενου block στο Blockchain, που συνδέει τα δύο blocks. Τα συνδεδεμένα blocks αποτελούν μια αλυσίδα. Αυτή η επαναληπτική διαδικασία επιβεβαιώνει την ακεραιότητα του προηγούμενου block και κατ'επέκταση ολόκληρη τη διαδρομή που καταλήγει σε αυτό το block.

Μερικές φορές χωριστά blocks μπορούν να παράγονται ταυτόχρονα, δημιουργώντας ένα fork. Εκτός από ένα ασφαλές ιστορικό, κάθε Blockchain έχει έναν καθορισμένο αλγόριθμο για τη βαθμολόγηση διαφορετικών εκδόσεων του ιστορικού, έτσι ώστε να μπορεί να επιλεγεί κάποιο με υψηλότερη τιμή σε σχέση με τα άλλα. Τα blocks που δεν έχουν επιλεγεί για να συμπεριληφθούν στην αλυσίδα ονομάζονται ορφανά blocks. [28] Οι κόμβοι-χρήστες του P2P δικτύου που υποστηρίζουν τη βάση δεδομένων έχουν διαφορετικές εκδόσεις ιστορικού ανά κάποιες χρονικές στιγμές. Οπότε και διατηρούν μόνο την έκδοση με τη μεγαλύτερη βαθμολογία της βάσης δεδομένων που τους είναι γνωστή. Κάθε φορά που ένας χρήστης λαμβάνει μια έκδοση ιστορικού υψηλότερης βαθμολογίας (συνήθως η παλιά έκδοση που κατέχει με διαφορά κατά ένα καινούριο block) αντικαθιστά τη δική του βάση δεδομένων και επαναμεταδίδει τη βελτίωση στους άλλους κόμβους-χρήστες. Το Blockchain είναι συνήθως σχεδιασμένο έτσι ώστε να προσθέτει νέα blocks σε παλαιότερα και αυτά στη συνέχεια να επεκταθούν αντί να αντικατασταθούν παλαιότερα blocks. Επομένως, η πιθανότητα αντικατάστασης ενός block είναι πολύ μικρή.

- **Block time**

[49] Merkle tree και η συμβολή τους στην κρυπτογραφία και την Επιστήμη των Υπολογιστών: https://en.wikipedia.org/wiki/Merkle_tree

Ο χρόνος αποκλεισμού είναι ο μέσος χρόνος που χρειάζεται για να δημιουργήσει το δίκτυο ένα επιπλέον block στο Blockchain. Ορισμένα Blockchain δημιουργούν ένα νέο block κάθε πέντε δευτερόλεπτα. Τη στιγμή που το block θα έχει ολοκληρωθεί, τα δεδομένα που περιλαμβάνονται θα καταστούν επαληθεύσιμα. Από εκείνη την στιγμή και έπειτα βέβαια δεν μπορεί να τροποποιηθεί με οποιονδήποτε τρόπο μία πληροφορία που περιέχεται στο Blockchain. Στην κρυπτογράφηση, η δημιουργία ενός νέου block συμβαίνει ουσιαστικά όταν πραγματοποιείται η συναλλαγή, οπότε ένας μικρότερος χρόνος αποκλεισμού σημαίνει ταχύτερες συναλλαγές.

3.2.3 Επαλήθευση Δεδομένων και Miners

Η επιτυχία της Blockchain τεχνολογίας σε ένα σημείο στηρίζεται στην αντιμετώπιση του προβλήματος του διπλοξοδέματος χωρίς να απαιτείται από τρίτους να επαληθεύουν τις συναλλαγές. Αυτό επιτυγχάνεται μέσα από την παρακάτω διαδικασία.

Οι miners βοηθούν στην επίλυση του προβλήματος. Με ένα γενικό ορισμό θα μπορούσαμε να πούμε ότι οι miners είναι υπολογιστές αφιερωμένοι στο δίκτυο για να επικυρώνουν συναλλαγές και να απαγορεύουν τις απάτες. Όπως αναφέρθηκε και παραπάνω οι χρήστες δημιουργούν κρυπτογραφικά ασφαλείς συναλλαγές και έπειτα τις μεταδίδουν στο δίκτυο των miners. Οι miners με την σειρά τους προσπαθούν να επικυρώσουν όσες περισσότερες συναλλαγές μπορούν και να τις χωρέσουν σε ένα block και έπειτα περνώντας το από μία μαθηματική επεξεργασία ώστε να το επαληθεύσουν και να το προσθέσουν εν τέλει στο ήδη υπάρχον Blockchain, καταλήγοντας σε ένα αποτέλεσμα παρόμοιο με αυτό που φαίνεται στην Εικόνα 6.

Ουσιαστικά οι miners πρέπει να δημιουργήσουν το hash του νέου block για να το προσθέσουν έπειτα στο Blockchain. Όμως αυτή η διαδικασία δεν είναι τόσο απλή για έναν miner γιατί θα πρέπει να βρουν το σωστό hash το οποίο επιλύει ένα μαθηματικό πρόβλημα, δεδομένου ότι δεν υπάρχει κάποιος τρόπος να ξεκινήσει ο miner με ένα έτοιμο hash και γυρνώντας προς τα πίσω να καταλάβει ποιο κομμάτι των δεδομένων έδωσε αυτό το hash.

Το κίνητρο για την διάθεση υπολογιστικών πόρων στο δίκτυο για την επαλήθευση των συναλλαγών είναι οι ανταμοιβές για block και οι ανταμοιβές για συναλλαγές. Για κάθε block που δημιουργεί ο miner δέχεται μία ανταμοιβή. Αυτή συνήθως με το πέρασμα το χρόνου μειώνεται μέχρι να μην υπάρχουν πια ανταμοιβές. Το δεύτερο κίνητρο που αναφέραμε είναι η ανταμοιβή ανά συναλλαγή. Φυσικά, όταν η ζήτηση για χρήση του δικτύου αυξάνεται ενώ η προσφορά διαθέσιμου χώρου παραμένει σταθερή, χρειάζεται ένας τρόπος να δοθεί προτεραιότητα στις συναλλαγές που εισέρχονται σε κάθε block, οπότε και η ανταμοιβή για μία συναλλαγή σε ένα Blockchain μπορεί να εξαρτάται από το ποσό που είναι διατεθειμένοι να παρέχουν έτσι ώστε να εκπληρωθεί η συναλλαγή αυτή.

Πολλές φορές παρατηρείται συνεργασία μεταξύ miners έτσι ώστε να διαθέτουν στο σύνολο περισσότερη υπολογιστική ισχύ, αυξάνοντας με τον τρόπο αυτό τις πιθανότητες τους να επιλύσουν το πρόβλημα, να προσθέσουν ένα νέο block στο Blockchain και να κερδίσουν την ανταμοιβή και έπειτα την διαιρούν ανάλογα στα μέλη. [29]

Τέλος όσον αφορά την πολιτική που ακολουθεί το data mining, αυτή διαφέρει αναλόγως το Blockchain. Ως επί το πλείστον συνηθίζεται να δημιουργούνται είτε proof-of-working είτε proof-of-stake συστήματα.

3.2.4 Χαρακτηριστικά του Blockchain

- **Αποκέντρωση**

Με την αποθήκευση δεδομένων σε όλο το δίκτυο P2P, το Blockchain εξαλείφει έναν αριθμό κινδύνων που συνοδεύουν τα δεδομένα που κρατούνται κεντρικά. Το αποκεντρωμένο Blockchain μπορεί να χρησιμοποιεί ad-hoc μεταφορά μηνυμάτων(από χρήστη σε χρήστη αποστολή) και κατανεμημένη δικτύωση.

Τα P2P Blockchain δίκτυα από ομότιμους χρήστες δεν διαθέτουν συγκεντρωτικά σημεία τα οποία είναι τρωτά σε μια ηλεκτρονική επίθεση και κατ’επέκταση δεν έχουν κεντρικό σημείο αποτυχίας. Οι μέθοδοι ασφαλείας Blockchain περιλαμβάνουν τη χρήση κρυπτογραφίας δημόσιου κλειδιού[30] . Ένα public key (μια μακρά, τυχαία αναζητούμενη σειρά αριθμών) είναι μια διεύθυνση στο Blockchain. Τιμές tokens που αποστέλλονται μέσω του δικτύου καταγράφουν αν ανήκουν σε αυτή τη διεύθυνση. Ένα private key είναι σαν ένας κωδικός πρόσβασης που δίνει στον ιδιοκτήτη του πρόσβαση στα ψηφιακά του στοιχεία ή τα μέσα για να αλληλεπιδράσει με τις διάφορες δυνατότητες που υποστηρίζει το Blockchains. Τα δεδομένα που είναι αποθηκευμένα στο Blockchain θεωρούνται γενικά απρόσβλητα. [27]

Κάθε κόμβος σε ένα αποκεντρωμένο σύστημα έχει ένα αντίγραφο του ledger του Blockchain. Η ποιότητα των δεδομένων διατηρείται από τη μαζική αναπαραγωγή βάσεων δεδομένων και την εμπιστοσύνη στον υπολογισμό. Δεν υπάρχει κεντρικό αντίγραφο και κανένας χρήστης δεν είναι πιο αξιόπιστος από κάποιον άλλο. Οι κόμβοι miner επικυρώνουν τις συναλλαγές, τις προσθέτουν στο block που δημιουργούν και στη συνέχεια μεταδίδουν το ολοκληρωμένο block σε άλλους κόμβους. Τα Blockchain χρησιμοποιούν διάφορα συστήματα σφράγισης χρόνου, όπως η απόδειξη της εργασίας (proof of working), για τη σειρά των αλλαγών. Οι εναλλακτικές μέθοδοι συναίνεσης περιλαμβάνουν την απόδειξη της συμμετοχής. Η ανάπτυξη ενός αποκεντρωμένου Blockchain συνοδεύεται από τον κίνδυνο συγκέντρωσης λόγω του ότι οι πόροι πληροφορικής που απαιτούνται για την επεξεργασία μεγαλύτερων ποσοτήτων δεδομένων καθίστανται ακριβότεροι.

- **Διαφάνεια**

Μέσω του Blockchain, όλοι οι συμμετέχοντες μοιράζονται αρχεία και queries σε κόμβους σε μια αποκεντρωμένη δομή. Η τεχνολογία Blockchain εξασφαλίζει ότι τα συστήματα καταγράφουν και μεταφέρουν δεδομένα και πληροφορίες. Κάθε συμμετέχων μπορεί να αναζητήσει τα αρχεία στο Blockchain για να κάνει τις πληροφορίες στο κατανεμημένο σύστημα διαφανείς και συνεπείς. Κάθε δεδομένο συναλλαγής ενός κατανεμημένου συστήματος είναι ανοικτό και αξιόπιστο. Κάθε κόμβος της ίδιας πλατφόρμας έχει τα ίδια δικαιώματα και υποχρεώσεις για την πρόσβαση σε εξουσιοδοτημένες πληροφορίες και επιτρέπει σε άλλους κόμβους στο ίδιο δίκτυο να έχουν πρόσβαση σε αυτές τις πληροφορίες. [31], [32]

- **Ανιχνεύσιμο και με Μνήμη**

Το Blockchain χρησιμοποιεί timestamps για τον εντοπισμό και την καταγραφή κάθε συναλλαγής, ενισχύοντας έτσι την χρονική σειρά των δεδομένων. Αυτό επιτρέπει στον κόμβο να διατηρεί τη σειρά των συναλλαγών και να κάνει τα δεδομένα ανιχνεύσιμα. Η χρονική σήμανση όχι μόνο εγγυάται την πρωτοτυπία των δεδομένων, αλλά μειώνει επίσης το κόστος της ανιχνευσιμότητας των συναλλαγών. Παράλληλα, ενισχύει μη αναστρέψιμες τροποποιήσεις δεδομένων ή πληροφοριών. Μόλις μια συναλλαγή επικυρωθεί και προστεθεί στο block, δεν μπορεί να τροποποιηθεί. Οι συναλλαγές πρέπει να επανεξεταστούν από τους περισσότερους κόμβους του συστήματος πριν καταγραφούν. Ακόμα κι αν ένας εισβολέας έχει ισχυρή υπολογιστική ικανότητα, είναι δύσκολο για τον εν λόγω εισβολέα να αποφύγει το σύστημα και να τροποποιήσει το αρχείο. Αυτό μπορεί να συμβεί μόνο όταν ο εισβολέας ελέγχει 51% ή περισσότερους από όλους τους κόμβους. Αυτό το χαρακτηριστικό διασφαλίζει ότι το σύστημα είναι σταθερό και αξιόπιστο και λύνει τα προβλήματα «διπλής δαπάνης» [33], [34].

- **Ανωνυμία**

Το Blockchain κρυπτογραφεί τα δεδομένα χρησιμοποιώντας ασύμμετρες τεχνικές κρυπτογράφησης. Αυτή η ασύμμετρη κρυπτογράφηση έχει δύο χρήσεις σε Blockchains τη κρυπτογράφηση δεδομένων και τις ψηφιακές υπογραφές. Η κρυπτογράφηση δεδομένων στο Blockchain εξασφαλίζει την ασφάλεια των δεδομένων των συναλλαγών και μειώνει τον κίνδυνο απώλειας ή παραποίησης δεδομένων μιας συναλλαγής. Τα δεδομένα συναλλαγών μεταδίδονται μέσω του δικτύου και υπογράφονται ψηφιακά για να δηλώνεται η ταυτότητα του υπογράφοντος και αν έχει προσδιοριστεί η συναλλαγή.

Στο σύστημα Blockchain, είναι περιττό να αποκαλυφθεί η πραγματική ταυτότητα του κόμβου που σχετίζεται με τον συμμετέχοντα. Το χαρακτηριστικό αυτό είναι αμφιλεγόμενο διότι βοηθά έμμεσα ορισμένες παράνομες δραστηριότητες, όπως η νομιμοποίηση εσόδων από παράνομες δραστηριότητες, αλλά τουλάχιστον προστατεύει την ιδιωτική ζωή και την ασφάλεια των συμμετεχόντων [21].

- **Αξιοπιστία**

Η ανταλλαγή δεδομένων στο Blockchain εξαρτάται πλήρως από τον αυτοέλεγχο. Στηρίζεται σε κάθε κόμβο για να σχηματίσει έναν ισχυρό υπολογισμό για να υπερασπιστεί τις εξωτερικές επιθέσεις χωρίς ανθρώπινη παρέμβαση. Οι συμμετέχοντες μπορούν να ολοκληρώσουν τη συναλλαγή υπό συνθήκες πλήρους ανωνυμίας. Προστατεύει την ιδιωτική ζωή όλων των εμπλεκόμενων μελών και αυξάνει την ασφάλεια και την αξιοπιστία της συναλλαγής. Επιπλέον, κάθε κόμβος στο Blockchain αποθηκεύει τα πλήρη δεδομένα. Όταν το 51% όλων των κόμβων του δικτύου δεν καταλαμβάνεται από χάκερς, το σύστημα είναι ακόμα ασφαλές και αξιόπιστο. [35]

- **Μη εξουσιοδοτημένα Blockchain**

Τα ανοιχτά Blockchains είναι πιο φιλικά προς το χρήστη από κάποια παραδοσιακά αρχεία ιδιοκτησίας, τα οποία, ενώ είναι ανοιχτά στο κοινό, απαιτούν ακόμα φυσική πρόσβαση για προβολή. Επειδή τα πρώτα Blockchain ήταν χωρίς εξουσιοδοτήσεις, δημιουργήθηκαν διαμάχες σε σχέση με τον ορισμό του Blockchain.[36] Ένα ζήτημα υπό συζήτηση είναι εάν ένα ιδιωτικό σύστημα με επαληθευτές που έχουν επιφορτιστεί και εγκριθεί από μια κεντρική αρχή θα πρέπει να θεωρηθεί ως Blockchain. Οι υποστηρικτές των εξουσιοδοτημένων ή ιδιωτικών αλυσίδων υποστηρίζουν ότι ο όρος Blockchain μπορεί να εφαρμοστεί σε οποιαδήποτε δομή δεδομένων αναμεταδίδει δεδομένα σε block με χρονική σφραγίδα. Οι αντίπαλοι του Blockchain λένε ότι τα εξουσιοδοτημένα συστήματα μοιάζουν με παραδοσιακές εταιρικές βάσεις δεδομένων, δεν υποστηρίζουν την επαλήθευση των αποκεντρωμένων δεδομένων και ότι τα συστήματα αυτά δεν υποστηρίζουν δομές κατά της παρεμβολής και της αναθεώρησης από κάποιον χειριστή.

- **Εξουσιοδοτημένα Blockchain**

Το μεγάλο πλεονέκτημα για ένα ανοιχτό, εξουσιοδοτημένο ή δημόσιο δίκτυο Blockchain είναι ότι δεν απαιτείται προστασία από «ψεύτικους» χρήστες καθώς και έλεγχος πρόσβασης. Αυτό σημαίνει ότι οι εφαρμογές μπορούν να προστεθούν στο δίκτυο χωρίς την έγκριση ή την εμπιστοσύνη των άλλων, χρησιμοποιώντας το Blockchain ως στρώμα μεταφοράς. Το Bitcoin και άλλες κρυπτοεπιχειρήσεις ασφαλίζουν επί του παρόντος το Blockchain τους απαιτώντας νέες καταχωρήσεις για να συμπεριλάβουν μια απόδειξη της ταυτότητας του χρήστη.

3.3 Εικονικό Νόμισμα / Κρυπτονόμισμα και Blockchain

Πολλές εφαρμογές που έχουν σχεδιαστεί βάσει της τεχνολογίας Blockchain εμπεριέχουν συχνά και ένα σύστημα συναλλαγών για τους χρήστες, δηλαδή ένα τύπο νομίσματος, ο οποίος δεν έχει στην πραγματικότητα κάποια αξία, αλλά στο πλαίσιο της εφαρμογής καθορίζεται ρητά η αξία του, δηλαδή χρησιμοποιώντας ένα εικονικό νόμισμα ο χρήστης γνωρίζει ποια ακριβώς παροχή θα του επιστραφεί. Το bitcoin

πέρα από την πρώτη εφαρμογή που χρησιμοποίησε την Blockchain τεχνολογία ήταν επίσης η πρώτη εφαρμογή που τη συνδύασε με ένα αντίστοιχο εικονικό νόμισμα. Μέσω της μελέτης του τρόπου χρήσης του κρυπτονομίσματος από το bitcoin θα μας βοηθήσει να κατανοήσουμε καλύτερα την γενικότερη αξία ύπαρξης ενός εικονικού νομίσματος ή όπως αλλιώς είναι γνωστό ενός κρυπτονομίσματος σε μία Blockchain εφαρμογή.

Η λογική ενός κρυπτονομίσματος είναι ότι ο χρήστης έχει τη δυνατότητα πραγματοποίησης συναλλαγών μέσω Διαδικτύου χωρίς να βασίζεται σε οικονομικά ιδρύματα, που εξυπηρετούν ως έμπιστοι διαμεσολαβητές επεξεργασίας ηλεκτρονικών πληρωμών. Ένα τέτοιο σύστημα έχει το πλεονέκτημα της εμπιστοσύνης από τους χρήστες του γιατί δεν θα εξαρτώνται πλέον από τρίτους. Σε αντίθεση με το εικονικό νόμισμα, οι συναλλαγές που γίνονται με παραδοσιακούς τρόπους είναι αναστρέψιμες, καθ' όσον τα οικονομικά ιδρύματα δεν μπορούν να αποφύγουν τη διαμεσολάβηση διαφορών. Το κόστος της διαμεσολάβησης αυξάνει τα κόστη των συναλλαγών, περιορίζοντας το ελάχιστο πρακτικό μέγεθος αυτών και αποκόβοντας τη δυνατότητα για μικρές απλές πληρωμές, ενώ υπάρχει και ένα ευρύτερο κόστος στην απώλεια της δυνατότητας για πραγματοποίηση μη αναστρέψιμων πληρωμών για μη αναστρέψιμες υπηρεσίες. Με τη δυνατότητα για αντιστροφή, η ανάγκη για εμπιστοσύνη εξαπλώνεται. Οι έμποροι πρέπει να είναι επιφυλακτικοί όσον αφορά τους πελάτες τους, ενοχλώντας τους για όλο και περισσότερες πληροφορίες που σε αντίθετη περίπτωση δεν θα χρειαζόντουσαν. Ένα δεδομένο ποσοστό εξαπάτησης λαμβάνεται επίσης ως αναπόφευκτο. Αυτά τα κόστη και οι αβεβαιότητες πληρωμών μπορούν να αποφευχθούν χρησιμοποιώντας φυσικά νομίσματα, αλλά δεν υπάρχει κανένας μηχανισμός για την πραγματοποίηση πληρωμών σε κάποιο κανάλι επικοινωνίας χωρίς έναν έμπιστο τρίτο φορέα. Αυτό που χρειάζεται είναι ένα ηλεκτρονικό σύστημα πληρωμών βασισμένο σε απόδειξη κρυπτογραφίας αντί για εμπιστοσύνη, επιτρέποντας σε δύο χρήστες να κάνουν συναλλαγή απευθείας μεταξύ τους χωρίς την ανάγκη για έναν έμπιστο τρίτο. Συναλλαγές που θα είναι υπολογιστικά μη ωφέλιμες από άποψη κέρδους η αντιστροφή τους, θα προστατεύουν τους πωλητές από εξαπάτηση, ενώ απλοί μηχανισμοί μεσεγγύησης θα μπορούν εύκολα να υλοποιούνται για την προστασία των αγοραστών. Ένα εικονικό νόμισμα δίνει μία λύση στο πρόβλημα του διπλόξοδέματος.

Όσον αφορά το τεχνικό κομμάτι της υλοποίησης ενός εικονικού νομίσματος χρησιμοποιείται ένας peer-to-peer κατανεμημένος χρονοσφραγισμένος εξυπηρετητής για τη δημιουργία υπολογιστικής απόδειξης της χρονολογικής σειράς των συναλλαγών. Το σύστημα είναι ασφαλές όσο οι έντιμοι κόμβοι συγκεντρώνουν από κοινού περισσότερη επεξεργαστική ισχύ από οποιαδήποτε συνεργατική ομάδα επιτιθέμενων. Αυτό σημαίνει ότι μία καθαρά peer-to-peer έκδοση ηλεκτρονικών μετρητών θα επιτρέπει σε διαδικτυακές πληρωμές να στέλνονται απευθείας από έναν συμβεβλημένο σε έναν άλλον χωρίς την ανάγκη διαμεσολάβησης ενός οικονομικού ιδρύματος. Το δίκτυο χρονοσφραγίζει (timestamps) συναλλαγές κατακερματίζοντας (transaction hash) τις μέσα σε μία εξελισσόμενη αλυσίδα απόδειξης εργασίας (proof-

of-work) βασισμένη σε αλγορίθμους hash (hash-based), σχηματίζοντας ένα αρχείο καταγραφής το οποίο δεν μπορεί να αλλαχτεί χωρίς να επαναληφθεί ξανά όλη η απόδειξη της εργασίας που έχει προηγηθεί. Η μακρύτερη αλυσίδα δεν εξυπηρετεί μόνο ως απόδειξη της ακολουθίας των συμβάντων που έχουν δημόσια καταγραφεί, αλλά και απόδειξη ότι προήλθε από τη μεγαλύτερη πηγή επεξεργαστικής ισχύος που έχει καταβληθεί για αυτόν το σκοπό. Όσο η πλειοψηφία της επεξεργαστικής ισχύος ελέγχεται από κόμβους που δεν συνεργάζονται για να επιτεθούν στο δίκτυο, αυτοί θα σχηματίζουν ξανά τη μακρύτερη αλυσίδα και θα αφήνουν πίσω τους επιτιθέμενους. Οι απαιτήσεις αυτού του δικτύου είναι ελάχιστες. Τα μηνύματα μεταδίδονται με βάση την καλύτερη δυνατή προσπάθεια του δικτύου (best-effort basis) και οι κόμβοι μπορούν να συνδεθούν στο δίκτυο κατά βούληση, αποδεχόμενοι τη μακρύτερη proof-of-work αλυσίδα ως απόδειξη για ο,τι συνέβη κατά την απουσία τους.

3.4 Προστασία Προσωπικών Δεδομένων

Όπως είναι φυσιολογικό, η νέα τεχνολογία, ως ένας νέος τρόπος καταχώρησης και αποθήκευσης δεδομένων, θα πρέπει καταρχάς να εξεταστεί υπό το πρίσμα του δικαίου της προστασίας προσωπικών δεδομένων. Ερωτήματα όπως ποιος θα θεωρείται ο υπεύθυνος της επεξεργασίας και ποιος ο εκτελών την επεξεργασία θα είναι δύσκολο να απαντηθούν κυρίως σε ανοιχτές (χωρίς άδεια – permissionless) πλατφόρμες Blockchain. Επιπλέον βασικά δικαιώματα των χρηστών όπως το δικαίωμα διαγραφής ή ενημέρωσης των προσωπικών δεδομένων είναι εξαιρετικά αμφίβολο αν και με ποιο τρόπο θα μπορούσαν να ικανοποιηθούν σε μία βάση δεδομένων, η οποία τηρείται ταυτόχρονα σε χιλιάδες αντίτυπα και στην οποία είναι αδύνατον να τροποποιηθεί, πόσο μάλλον να αφαιρεθούν δεδομένα και μάλιστα με τον τρόπο που απαιτεί ο νέος Κανονισμός για την προστασία των προσωπικών δεδομένων (GDPR).

3.4.1 Ιστορική Αναδρομή

Ο νομικός χαρακτηρισμός των κρυπτονομισμάτων είναι προϋπόθεση για τη νομική τους αντιμετώπιση και τη συστηματική τους ένταξη στο αντίστοιχο σύνολο κανόνων δικαίου. Αν και το όνομα παραπέμπει σε νομίσματα, η απάντηση δεν είναι τόσο προφανής καθώς σχεδόν κανένα από τα κρυπτονομίσματα δεν λειτουργεί ως νόμισμα. Κάθε πρωτόκολλο ανοιχτής αλυσίδας blockchain προβλέπει την δημιουργία tokens, τα οποία είναι απαραίτητα για τη συμμετοχή στην πλατφόρμα αυτή. Για να είναι δυνατή η χρήση του πρωτοκόλλου, ή η συνομολόγηση και η εκπλήρωση ενός έξυπνου συμβολαίου, οι συμμετέχοντες σε μία συναλλαγή πρέπει να διαθέτουν tokens του πρωτοκόλλου αυτού στη διάθεσή τους. Επομένως, η φύση και η λειτουργία των κρυπτονομισμάτων προσιδιάζει περισσότερο σε ψηφιακά περιουσιακά στοιχεία, η αξία των οποίων είναι συνδεδεμένη και υπάρχει μόνο μέσα στο οικοσύστημα λειτουργίας ενός συγκεκριμένου πρωτοκόλλου Blockchain. Η αξία αυτή καθορίζεται από τα τεχνικά χαρακτηριστικά του πρωτοκόλλου, τις λειτουργικές

του δυνατότητες και εν τέλει την απήχησή και τη διάδοσή του στην κοινότητα στην οποία απευθύνεται.

Η έννοια των tokens μπορεί να γίνει πιο κατανοητή αν δει κανείς την αρχιτεκτονική και τη δομή των εταιρειών που τα εκδίδουν και τα διαθέτουν, συνήθως μέσω αυτού που ονομάζεται Initial Coin Offering ή ICO . Οι εταιρείες αυτές δημιουργούν υπηρεσίες οι οποίες βασίζονται στην αποκεντρωμένη συν-δημιουργία, εξαρτώνται από την διάδοση των tokens και η βασική, αν όχι η μόνη, πηγή εσόδων είναι η αύξηση της αξίας των tokens ανάλογα με την επιτυχία της «οικονομίας» τους. Πρόσφατα, σε μία περίπτωση διάθεσης tokens μέσω της πλατφόρμας του Ethereum, η Επιτροπή Κεφαλαιαγοράς των ΗΠΑ, έκρινε ότι αυτά πρέπει να αντιμετωπίζονται ως κινητές αξίες και συνεπώς η διάθεσή τους να διέπεται από την ισχύουσα νομοθεσία.[50]

Επιπλέον, τον Οκτώβριο του 2015 το Δικαστήριο της Ευρωπαϊκής Ένωσης στο πλαίσιο της ερμηνείας της Οδηγίας 2006/112/ΕΚ περί Φ.Π.Α. έκρινε ότι το bitcoin, δεν μπορεί να χαρακτηριστεί ως ενσώματο αγαθό κατά την έννοια του άρθρου 14 της οδηγίας περί ΦΠΑ[51], διότι έχει ως αποκλειστικό σκοπό να αποτελέσει μέσο πληρωμής καθώς και ότι η ανταλλαγή παραδοσιακών νομισμάτων έναντι bitcoins απαλλάσσεται από τον Φ.Π.Α.

Επίσης, σύμφωνα με το Δικαστήριο της ΕΕ οι πράξεις που αφορούν μη συμβατικά νομίσματα, δηλαδή νομίσματα που δεν αποτελούν εκ του νόμου μέσα πληρωμής σε μία ή περισσότερες χώρες, είναι χρηματοπιστωτικές πράξεις, υπό την προϋπόθεση ότι τα εν λόγω μη συμβατικά νομίσματα γίνονται δεκτά από τους συναλλασσόμενους ως εναλλακτικό, σε σχέση με τα συμβατικά νομίσματα, μέσο πληρωμής και χρησιμοποιούνται αποκλειστικά ως μέσα πληρωμής. Αξίζει να σημειωθεί ότι σύμφωνα με την απόφαση παραπομπής του αιτούντος δικαστηρίου (Ανώτατο Διοικητικό Δικαστήριο της Σουηδίας) στην ανωτέρω υπόθεση, η διεύθυνση bitcoin (δηλαδή το δημόσιο κλειδί ενός χρήστη) μπορεί να συγκριθεί με τον αριθμό τραπεζικού λογαριασμού.[52]

Περαιτέρω, σύμφωνα με έκθεσή της τον Φεβρουάριο του 2015, η Ευρωπαϊκή Κεντρική Τράπεζα δεν θεωρεί τα εικονικά νομίσματα, όπως το Bitcoin ως μία μορφή χρήματος, όπως ορίζεται στην οικονομική επιστήμη, αλλά ούτε και από νομικής απόψεως.[53] Για τους σκοπούς της εν λόγω έκθεσης, η ΕΚΤ όρισε τα εικονικά νομίσματα ως μία ψηφιακή αποτύπωση αξίας, η οποία δεν εκδίδεται από μία κεντρική τράπεζα, χρηματοπιστωτικό ίδρυμα ή ένα ίδρυμα ηλεκτρονικού χρήματος, η οποία, σε ορισμένες περιπτώσεις, μπορεί να χρησιμοποιηθεί ως εναλλακτική του – παραδοσιακού – χρήματος.

---

[50] Οι νόμοι περί κινητών αξιών των ΗΠΑ μπορούν να υποβάλουν αίτηση για προσφορές, πωλήσεις και εμπορία συμφαρόντων σε εικονικούς οργανισμούς : https://www.sec.gov/news/press-release/2017-131

[51] Το κοινό σύστημα φόρου προστιθέμενης αξίας (ΦΠΑ) της ΕΕ: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=LEGISSUM%3Al31057

[52] ΔικΕΕ, υπόθεση C-264/14, σκέψη 24: http://curia.europa.eu/juris/liste.jsf?num=C-264/14

[53] Συστήματα εικονικού νομίσματος:https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf

Για την ΕΚΤ, η υφιστάμενη ρύθμιση που ισχύει για τον παραδοσιακό οικονομικό τομέα δεν μπορεί να εφαρμοστεί καθώς δεν υπάρχουν τα παραδοσιακά οικονομικά μέρη, και κατηγοριοποιεί το bitcoin ως «μετατρέψιμο αποκεντρωμένο εικονικό νόμισμα».

Η Ευρωπαϊκή Ένωση σχεδιάζει να ρυθμίσει, τουλάχιστον εν μέρει τη διάθεση εικονικών νομισμάτων, στο πλαίσιο της αναθεώρησης της 4ης Οδηγίας (ΕΕ) 2015/849 για τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες. [37]

3.4.2 Blockchain και Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR)

Όπως αναφέρθηκε και παραπάνω από τις 25 Μαΐου 2018 έχει τεθεί σε εφαρμογή ο Γενικός Κανονισμός Προστασίας Δεδομένων ΕΕ 679/2016 (GDPR),[54] ο οποίος και ισχύει άμεσα σε όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης. Η συμμόρφωση της τεχνολογίας Blockchain με τον GDPR αποτελεί ένα φλέγον ζήτημα, που έχει απασχολήσει την Ευρωπαϊκή Επιτροπή. Η συμμόρφωση της τεχνολογίας Blockchain με τον GDPR αφορά τον τρόπο με τον οποίο χρησιμοποιείται η εν λόγω τεχνολογία σε διάφορες περιπτώσεις και εφαρμογές, όπως ακριβώς συμβαίνει και με το Διαδίκτυο και την Τεχνητή Νοημοσύνη. Τα δεδομένα που σχετίζονται με συναλλαγές και είναι καταχωρημένα σε ένα Blockchain ledger ή υπόκεινται σε επεξεργασία σε ένα «έξυπνο συμβόλαιο» (smart contracts), που εκτελεί αυτόματα προκαθορισμένες διαδικασίες για μία συναλλαγή χωρίς να απαιτείται η συμμετοχή ενός τρίτου φορέα (π.χ. τράπεζας), μπορούν να οδηγήσουν σε ταυτοποίηση φυσικών προσώπων και ως εκ τούτου θεωρούνται προσωπικά δεδομένα που προστατεύονται από τον GDPR καθώς και από την ισχύουσα νομοθεσία περί προστασίας προσωπικών δεδομένων. Τρία σημαντικά ζητήματα που ανακύπτουν σχετικά με την προστασία των προσωπικών δεδομένων σε έναν Blockchain ledger, στο πλαίσιο του GDPR, αξίζει να αναφερθούν. [38]

3.4.2.1 Υπεύθυνος Επεξεργασίας Blockchain ledger

Στον GDPR γίνεται σαφής διάκριση ανάμεσα στον υπεύθυνο επεξεργασίας (data controller), που αποτελεί το μέρος που καθορίζει τους σκοπούς και τον τρόπο της επεξεργασίας των προσωπικών δεδομένων και φέρει την πρωταρχική ευθύνη καθώς και στον εκτελούντα την επεξεργασία (data processor), ο οποίος επεξεργάζεται προσωπικά δεδομένα για λογαριασμό του υπευθύνου επεξεργασίας. Σε πολλές περιπτώσεις ο παραπάνω διαχωρισμός σε ένα blockchain ledger καθίσταται δύσκολος, ιδίως σε ένα δημόσιο blockchain ledger, όπως είναι το Bitcoin, όπου δεν υπάρχει έλεγχος επί των δεδομένων που υπόκεινται σε επεξεργασία στο πλαίσιο μιας συναλλαγής. Για παράδειγμα, θα μπορούσε να θεωρηθεί ότι όλα τα μέρη που ανταλλάσσουν προσωπικά δεδομένα στο πλαίσιο μίας τέτοιας συναλλαγής, ενεργούν

[54] Κανοσιμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32016R0679

ως υπεύθυνοι επεξεργασίας. Αντίστοιχα, οι εκτελούντες την επεξεργασία μπορεί να θεωρηθούν και άλλοι συμμετέχοντες σε ένα Blockchain ledger, όπως π.χ. οι προγραμματιστές «έξυπνων συμβολαίων» (smart contracts), οι οποίοι επεξεργάζονται προσωπικά δεδομένα για λογαριασμό αντίστοιχα των συμμετεχόντων που ενεργούν ως υπεύθυνοι επεξεργασίας, καθώς και οι miners (όσοι επιβεβαιώνουν συναλλαγές για την είσπραξη ανταμοιβής), οι οποίοι δεν συμμετέχουν μεν σε μια συναλλαγή αλλά χειρίζονται τους κόμβους (nodes) και επικυρώνουν τις συναλλαγές για λογαριασμό των συμμετεχόντων. [38]

3.4.2.2 Προστασία Προσωπικών Δεδομένων από Σχεδιασμό

Σύμφωνα με τον GDPR, ο υπεύθυνος επεξεργασίας οφείλει να εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα για να διασφαλίζει ότι, εξ ορισμού, υπόκεινται σε επεξεργασία μόνο τα προσωπικά δεδομένα που είναι απαραίτητα για τον εκάστοτε σκοπό της επεξεργασίας και δεν καθίστανται προσβάσιμα χωρίς την παρέμβαση του φυσικού προσώπου σε αόριστο αριθμό φυσικών προσώπων. Σε ένα Blockchain ledger υφίσταται πάντοτε το ζήτημα απουσίας ελέγχου επί των διαδικασιών που πραγματοποιούνται σε αυτόν και ως εκ τούτου καθίσταται κάθε φορά απαραίτητος ο έλεγχος εάν η τεχνολογία Blockchain είναι η κατάλληλη τεχνολογία που πρέπει να χρησιμοποιηθεί για την πραγματοποίηση του επιδιωκόμενου σκοπού. Επίσης, συνιστάται η επιλογή ενός ιδιωτικού Blockchain ledger (αντί ενός δημοσίου), που παρέχει μεγαλύτερο έλεγχο επί των προσωπικών δεδομένων, τα οποία υπόκεινται σε επεξεργασία, ειδικότερα σε ό,τι αφορά την διαβίβαση αυτών εκτός ΕΕ, καθώς πολλοί miners ενδέχεται να μην είναι εγκατεστημένοι εντός ΕΕ. Για τον σκοπό της ασφαλούς διαβίβασης δεδομένων σε χώρες εκτός ΕΕ η εφαρμογή εγγυητικών μηχανισμών (τυποποιημένες συμβατικές ρήτρες, Δεσμευτικοί Εταιρικοί Κανόνες κλπ.) καθίσταται περισσότερο εφικτή σε ένα ιδιωτικό Blockchain ledger παρά σε έναν δημόσιο. Επιπρόσθετα, συνιστάται η επεξεργασία και αποθήκευση μόνο κρυπτογραφημένων, ψευδωνυμοποιημένων ή ανωνυμοποιημένων δεδομένων, καθώς και η διενέργεια εκτίμησης των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία προσωπικών δεδομένων. [38]

3.4.2.3 Άσκηση Δικαιωμάτων των Υποκειμένων των Δεδομένων

Όσον αφορά την άσκηση των δικαιωμάτων, που διατηρούν τα υποκείμενα των δεδομένων σύμφωνα με τον GDPR, πρέπει να σημειωθεί ότι πολλά εκ των βασικών αυτών δικαιωμάτων, όπως το δικαίωμα διόρθωσης και το δικαίωμα διαγραφής (δικαίωμα στη λήθη), ενδέχεται να μην μπορούν να ασκηθούν λόγω του τρόπου δομής και αποθήκευσης των δεδομένων στα Blockchain ledgers. Ειδικότερα, τα Blockchain ledgers έχουν σχεδιαστεί κατά τέτοιο τρόπο, ώστε να μην είναι δυνατή η διαγραφή και διόρθωση των δεδομένων άπαξ αυτά καταχωρηθούν στην αλυσίδα των μπλοκ. Η «μη μεταβλητότητα» (immutability) αποτελεί βασικό χαρακτηριστικό της τεχνολογίας Blockchain. Συνεπώς, ακόμα και αν δύναται να προσδιοριστεί ο

υπεύθυνος επεξεργασίας σε ένα δίκτυο, όπως για παράδειγμα στο Bitcoin, καθίσταται αδύνατο ο εν λόγω υπεύθυνος επεξεργασίας να διαγράψει ή να επικαιροποιήσει το αρχείο μίας συναλλαγής χωρίς να καταστρέψει την αλυσίδα των μπλοκ. Η τεχνολογία Blockchain έχει συνολικά οικοδομηθεί επί τη βάσει της διασφάλισης ότι οι συναλλαγές δεν πρόκειται ποτέ να λησμονηθούν ή να διαγραφούν, με σκοπό την δημιουργία αποκεντρωμένης εμπιστοσύνης καθώς και την ανάπτυξη και επέκταση του δικτύου των συμμετεχόντων. Θα πρέπει να σημειωθεί ότι στον GDPR δεν εξειδικεύεται η έννοια της διαγραφής. Σε αυτό το πλαίσιο, η αρμόδια Γαλλική Εποπτική Αρχή (CNIL) αναγνωρίζει ότι ορισμένες τεχνικές κρυπτογράφησης, που συνδυάζονται με την καταστροφή του κλειδιού, μπορούν ενδεχομένως να θεωρηθούν διαγραφή ακόμα και αν δεν συνιστούν διαγραφή με τη στενή έννοια. Επισημαίνεται επίσης ότι ακόμα και η άσκηση του δικαιώματος πρόσβασης από πλευράς των υποκειμένων των δεδομένων καθίσταται δύσκολη, καθώς είναι δύσκολος ο προσδιορισμός του υπευθύνου επεξεργασίας. Αναφορικά με τους ιδιωτικούς Blockchain ledgers, και πάλι η αρμόδια Γαλλική Εποπτική Αρχή (CNIL) προτείνει τον καθορισμό ενός ελάχιστου αριθμού miners προκειμένου να αποφευχθούν αντιπαραθέσεις μεταξύ των εμπλεκομένων μερών, την εφαρμογή των κατάλληλων τεχνικών και οργανωτικών μέτρων, προκειμένου να ελαχιστοποιηθεί ο αντίκτυπος από την αποτυχία ενός αλγορίθμου στην ασφάλεια των συναλλαγών, καθώς και την κατάρτιση ενός εναλλακτικού σχεδίου τροποποίησης αλγορίθμων σε περίπτωση εντοπισμού μίας ευάλωτης κατάστασης. Επιπλέον, συνιστάται η καταγραφή του τρόπου διακυβέρνησης, η εξέλιξη του λογισμικού που χρησιμοποιείται, καθώς και η διασφάλιση της εμπιστευτικότητας, της ακεραιότητας, της νομιμότητας και της διαφάνειας της τεχνολογίας Blockchain μέσω της εφαρμογής των κατάλληλων μέτρων. [38]

4 Εφαρμογές με Blockchain τεχνολογία

4.1 Τομείς εφαρμογής της Blockchain τεχνολογίας και εφαρμογές

Η τεχνολογία Blockchain έχει τη δυνατότητα να αλλάξει τη λειτουργία των σημερινών επιχειρηματικών μοντέλων. Η κατανεμημένη τεχνολογία Blockchain είναι μια τεχνολογία με τη δυνατότητα δημιουργίας νέων θεμελίων για τα παγκόσμια οικονομικά και κοινωνικά συστήματα. Η χρήση των Blockchains υπόσχεται να επιφέρει σημαντική βελτίωση της αποτελεσματικότητας στις παγκόσμιες αλυσίδες εφοδιασμού, στις χρηματοπιστωτικές συναλλαγές, στα λογιστικά βιβλία εταιρειών και στην αποκεντρωμένη κοινωνική δικτύωση. Η τεχνολογία Blockchain μπορεί να ενσωματωθεί σε πολλούς τομείς. Αυτό σημαίνει ότι οι συγκεκριμένες εφαρμογές Blockchain μπορούν να φέρουν καινοτόμες αλλαγές, επειδή μπορούν να προσφέρουν λύσεις με σημαντικά χαμηλότερο κόστος, γεγονός που μπορεί να διαταράξει τα υπάρχοντα επιχειρηματικά μοντέλα. Τα πρωτόκολλα Blockchain διευκολύνουν τις επιχειρήσεις να χρησιμοποιούν νέες μεθόδους επεξεργασίας ψηφιακών συναλλαγών. Τα παραδείγματα περιλαμβάνουν ένα σύστημα πληρωμών και ένα ψηφιακό νόμισμα, διευκολύνοντας το πλήθος των χρηστών ή εφαρμόζοντας αγορές πρόβλεψης και γενικά εργαλεία διακυβέρνησης. Οι δομές Blockchain μπορούν να θεωρηθούν ως ένα αυτομάτως συμβολαιογραφημένο ημερολόγιο δηλαδή υπάρχει κοινή καταγραφή όλων των σημαντικών γεγονότων από όλες τις εμπλεκόμενες οντότητες. Καταρρίπτουν την ανάγκη για μία έμπιστη οντότητα με περισσότερα δικαιώματα (centralized authority) και αναμένεται ότι θα έχουν ως αποτέλεσμα λιγότερα κεφάλαια να συνδέονται με διαφωνίες. Τα Blockchains έχουν τη δυνατότητα να μειώσουν τον κίνδυνο οικονομικής απάτης. Θεωρητικά, δομές Blockchain στο κοντινό μέλλον θα μπορούν να υποστηρίξουν σημαντικές και χρονοβόρες διαδικασίες όπως: η είσπραξη των φόρων, η διεξαγωγή μεταφορών και η διαχείριση κινδύνων σε διάφορους τομείς. Σημαντικές εφαρμογές του Blockchain περιλαμβάνουν κρυπτονομίσματα, όπως το bitcoin, και πλατφόρμες Blockchain όπως το Factom ως κατανεμημένο μητρώο(distributed registry), το Gems για αποκεντρωμένα μηνύματα, τα Storj και Sia για διανεμημένη αποθήκευση σε cloud και το Tezos για αποκεντρωμένη ψηφοφορία. Νέες μέθοδοι διανομής είναι διαθέσιμες για τον ασφαλιστικό κλάδο, όπως η ασφάλεια σε κοινό δίκτυο (peer-to-peer), η παραμετρική

ασφάλιση και η μικροασφάλιση μετά την υιοθέτηση της Blockchain τεχνολογίας. Οι τράπεζες ενδιαφέρονται για την τεχνολογία αυτή, επειδή έχουν τη δυνατότητα να επιταχύνουν τις υπάρχουσες διαδικασίες. Η διαμοιρασμένη οικονομία και τα δίκτυα από πολλές και διάφορες συσκευές (IoT) είναι επίσης έτοιμα να επωφεληθούν από τα blockchains επειδή εμπλέκουν πολλές συνεργαζόμενες οντότητες. Η ηλεκτρονική ψηφοφορία είναι μια άλλη εφαρμογή του blockchain. Επίσης το τελευταίο χρονικό διάστημα αναπτύσσονται δομές Blockchain για την αποθήκευση δεδομένων, τη δημοσίευση κειμένων και την αναγνώριση της προέλευσης της ψηφιακής τέχνης. Τέλος, χρησιμοποιούνται για την ανάπτυξη συστημάτων πληροφοριών που αφορούν ιατρικά αρχεία (ανταλλαγή, πρόσβαση, διαχείριση) και σε περιπτώσεις συνυφασμένες γενικά στον τομέα της Υγείας όπου θα γίνει λεπτομερής ανάλυση και περιγραφή στη συνέχεια. [39]

1) Χρηματοπιστωτικές / Ασφαλιστικές υπηρεσίες

Εκτός από ένα αποκεντρωμένο μέσο πληρωμών, χωρίς την ανάγκη ύπαρξης ενδιάμεσων προσώπων, η τεχνολογία έχει εφαρμογές σε ένα πλήθος υπηρεσιών του χρηματοπιστωτικού τομέα. Ο παραδοσιακός τρόπος επεξεργασίας και εκκαθάρισης συναλλαγών, εκτός από δαπανηρός, είναι και περίπλοκος και κατ' επέκταση αργός, καθώς αρκετά μέρη ενδέχεται να εμπλέκονται για την ολοκλήρωση μίας συναλλαγής, όπως πράκτορες, θεματοφύλακες, διαχειριστές εκκαθάρισης κτλ. Κάθε ένα από αυτά τα μέρη τηρεί το δικό του αρχείο, γεγονός το οποίο εκτός από ζητήματα πρακτικότητας αυξάνει τις πιθανότητες σφαλμάτων και ανακολουθιών. Η τεχνολογία Blockchain απλοποιεί σημαντικά τη διαδικασία ενώ καθιστά περιττή την ανάγκη ύπαρξης ενδιάμεσων προσώπων. Ο χρόνος επιβεβαίωσης και εκκαθάρισης συναλλαγών μειώνεται δραματικά, ανεξάρτητα μάλιστα από τη γεωγραφική θέση των συναλλασσόμενων. Τα περισσότερα διεθνή χρηματοπιστωτικά ιδρύματα δοκιμάζουν πλέον πιλοτικά τη νέα τεχνολογία προκειμένου να εκμεταλλευτούν τις δυνατότητές της σε όλο το φάσμα των υπηρεσιών που παρέχουν.[55]

Ως μέσο διεκπεραίωσης πληρωμών, η τεχνολογία blockchain θα μπορεί να απλοποιήσει και να επιταχύνει τη διαδικασία επιβεβαίωσης πληρωμών. Σε ένα περιβάλλον το οποίο βασίζεται στην τεχνολογία Blockchain η επιβεβαίωση μίας πληρωμής μεταξύ παραλήπτη εμπορευμάτων και μεταφορέα θα είναι άμεση και μάλιστα μπορεί να γίνει απευθείας από τον παραλήπτη στον αποστολέα, χωρίς τη διαμεσολάβηση τρίτων (τράπεζας).

Ιδιαίτερη αξία έχει η νέα τεχνολογία στην επεξεργασία ασφαλιστικών αξιώσεων όπου με τη χρήση μητρώων θα καταχωρούνται με ασφάλεια και συνέχεια όλες οι σχετικές πληροφορίες. [37]

[55] Τον Σεπτέμβριο του 2016 η Barclays και η εταιρεία Wave έγιναν οι πρώτοι οργανισμοί που εκτελούν μια παγκόσμια εμπορική συναλλαγή βασισμένη στην τεχνολογία Blockchain με πραγματικούς πελάτες: https://www.barclayscorporate.com/insights/innovation/blockchain-revolution-in-trade-finance/

2) Τήρηση μητρώων

Καθώς η τεχνολογία Blockchain αποτελεί ουσιαστικά έναν νέο τρόπο καταχώρησης και αποθήκευσης πληροφοριών έτσι ώστε να δημιουργείται μία αλληλένδετη αλυσίδα δεδομένων, αποτρέποντας διπλές εγγραφές και κακόπιστες καταχωρήσεις, η πιο προφανής εφαρμογή της είναι στην τήρηση μητρώων, όπως το κτηματολόγιο[56], το ληξιαρχείο, το μητρώο εταιρειών, το φορολογικό μητρώο, το μητρώο δικαιωμάτων διανοητικής ιδιοκτησίας κτλ. Επιπλέον, η τεχνολογία θα μπορούσε να εφαρμοστεί σε λογιστικές καταχωρήσεις εταιρειών, καθώς μειώνει σημαντικά την πιθανότητα σφαλμάτων και εξασφαλίζει, τουλάχιστον σε βαθμό μεγαλύτερο από τις σημερινές πρακτικές, την ακεραιότητα των εγγραφών. Η τροποποίηση των εγγραφών από την στιγμή που θα καταχωρηθούν στην βάση δεδομένων Blockchain θα είναι εξαιρετικά δύσκολη, αν όχι αδύνατη, ακόμη και από εκείνον που τηρεί το μητρώο /αρχείο.

Σε όλες τις παραπάνω περιπτώσεις, η καταχώριση δεδομένων μπορεί να συνδυαστεί με επιπρόσθετες λειτουργικές δυνατότητες οι οποίες ενσωματώνονται στην εκάστοτε πλατφόρμα.

Ιδιαίτερη σημασία μπορεί να έχει η νέα τεχνολογία στην καταχώρηση δικαιωμάτων διανοητικής ιδιοκτησίας όπου η απόδειξη της κυριότητας και της χρονικής προτεραιότητας μπορεί να είναι δυσχερής και δαπανηρή, σε αντίθεση με την τεχνολογία Blockchain η οποία μπορεί να προσφέρει βεβαιότητα για τις εν λόγω καταχωρήσεις. Οι πληροφορίες αυτές μπορούν να είναι εξαιρετικά χρήσιμες και στην αντιμετώπιση των απομιμητικών προϊόντων επιτρέποντας τη χρήση ασφαλών και μη τροποποιήσιμων πιστοποιητικών από τις τελωνειακές και αστυνομικές αρχές. [37]

3) Διακυβέρνηση

Η ψηφιακή διακυβέρνηση και η ηλεκτρονική ψηφοφορία καθίσταται πλέον πολύ πιο ασφαλής καθώς εκτός από την κρυπτογράφηση των δεδομένων με μέθοδο που καθιστά εξαιρετικά δύσκολη την παραποίησή τους, διασφαλίζεται και η διαφάνεια αφού οι συμμετέχοντες είναι σε θέση να επιβεβαιώσουν ότι οι ψήφοι τους μετρήθηκαν και ότι το περιεχόμενό τους δεν αλλοιώθηκε.[57]

Η τεχνολογία Blockchain διαθέτει όλα εκείνα τα χαρακτηριστικά που θα αναζητούσε κανείς σε μία πλατφόρμα διαδικτυακής ψηφοφορίας. Δεν επιτρέπει αλλαγές του παρελθόντος, αλλοιώσεις του παρόντος, ούτε και τροποποίηση του τρόπου πρόσβασης στο σύστημα. Κυρίως όμως, κάθε κόμβος με πρόσβαση στο σύστημα μπορεί να «βλέπει» τα ίδια αποτελέσματα και κάθε ψήφος μπορεί να αναχθεί με βεβαιότητα στην πηγή της, χωρίς να διακυβεύεται η ανωνυμία των ψηφοφόρων.

[56] Η UBITQUITY είναι μία εταρεία που δραστηριοποιείται στην αγορά ακινήτων χρησιμοποιώντας μία πλατφόρμα, βασισμένη στην τεχνολογία Blockchain: https://www.ubitquity.io/products.html
[57] Διεξαγωγή ψηφοφορίας χρησιμοποιώντας Blockchain τεχνολογία και ψηφιακά συμβόλαια: https://medium.com/swlh/voting-using-blockchain-and-smart-contractsd-8a277892732f

Ένας άλλος τομέας στον οποίο η νέα τεχνολογία θα έβρισκε σημαντικές εφαρμογές είναι αυτός των μη κερδοσκοπικών οργανισμών, αφού οι δωρητές θα είναι σε θέση να διαπιστώνουν με βεβαιότητα και διαφάνεια πού χρησιμοποιούνται τα χρήματά τους. Πέραν αυτού, το Blockchain διευκολύνει την πιο αποτελεσματική διανομή των κεφαλαίων κι ενισχύει τις δυνατότητες παρακολούθησής τους. [37]

4) Διαχείριση ψηφιακής ταυτότητας

Οι τράπεζες, η υγειονομική περίθαλψη, η εθνική ασφάλεια, η τεκμηρίωση της ιθαγένειας, η λιανική πώληση στο διαδίκτυο ή η πρόσβαση σε ένα μπαρ απαιτούν ταυτότητα και εξουσιοδότηση ταυτότητας. Η επαλήθευση της ταυτότητας είναι μια διαδικασία που υπεισέρχεται στο εμπόριο και τον πολιτισμό παγκοσμίως. Λόγω της έλλειψης κατανόησης και του ανεξέλεγκτου κυβερνοχώρου, η διαδικασία ταυτοποίησης ενός ατόμου στο πλαίσιο της τεχνολογίας αντιμετωπίζει σημαντικά εμπόδια. Γεγονότα όπως ψηφιακές υποκλοπές και παραμορφωμένοι λογαριασμοί καταδεικνύουν τα αυξανόμενα προβλήματα μιας τεχνολογικά προηγμένης κοινωνίας.

Η τεχνολογία Blockchain προσφέρει μια λύση σε πολλά ζητήματα ψηφιακής ταυτοποίησης, όπου η ταυτότητα μπορεί να πιστοποιείται με μοναδικό, αμετάβλητο και ασφαλή τρόπο. Οι τρέχουσες μέθοδοι χρησιμοποιούν παρωχημένα συστήματα βασισμένα σε κωδικό πρόσβασης με διαπιστευτήρια που ανταλλάσσονται και αποθηκεύονται σε ανασφαλή συστήματα. Τα Blockchain συστήματα ελέγχου ταυτότητας βασίζονται στην αδιαμφισβήτητη επαλήθευση ταυτότητας χρησιμοποιώντας ψηφιακές υπογραφές βασιζόμενες στην κρυπτογραφία δημόσιου κλειδιού. Σε αυτά τα συστήματα ο μόνος έλεγχος είναι αν η συναλλαγή που υπογράφηκε είχε το σωστό ιδιωτικό κλειδί. Η κρυπτογραφία μας επιτρέπει να συμπεράνουμε ότι όποιος έχει πρόσβαση στο ιδιωτικό κλειδί είναι ο ιδιοκτήτης και η ακριβής ταυτότητα του ιδιοκτήτη δε λαμβάνεται υπόψη στις παραμέτρους αυτού του πρωτοκόλλου ελέγχου ταυτότητας.[58]

Τα συνήθη σημερινά συγκεντρωτικά συστήματα έχουν ως επί το πλείστον μόνο έναν αριθμό κοινωνικής ασφάλισης, ημερομηνία γέννησης και όνομα, χρησιμοποιώντας αυτό το σύνολο πληροφοριών ως κλειδιά για εκατοντάδες διαφορετικούς λογαριασμούς και πύλες σε απευθείας σύνδεση. Πολλές βασικές καθημερινές λειτουργίες όπως οι τραπεζικές συναλλαγές, οι αγορές και η αποστολή μηνυμάτων μέσω ηλεκτρονικού ταχυδρομείου, προστατεύονται μόνο από έναν ενιαίο κωδικό πρόσβασης και είναι ανασφαλείς όχι μόνο για τα χρήματα αλλά και τις πληροφορίες στους λογαριασμούς αυτούς.

Η τεχνολογία Blockchain παρουσιάζεται ως μια εξαίρετη λύση για τα προβλήματα προσωπικής ασφάλειας και τυχαίες διαδικασίες επαλήθευσης ταυτότητας καθώς κάνει την παρακολούθηση και τη διαχείριση της ψηφιακής ταυτότητας τόσο ασφαλή

[58] Blockchain εφαρμογές στην ταυτοποίηση:
https://www.blockchaintechnologies.com/applications/identity/

όσο και αποτελεσματική, μειώνοντας έτσι τον κίνδυνο της απάτης και ήδη αρκετές εταιρείες έχουν στραφεί προς αυτή τη τεχνολογία.[59]

5) Internet of Things (IoT)

Ως έξυπνες χαρακτηρίζονται οι συσκευές οι οποίες συνδέονται στο διαδίκτυο, αλληλοεπιδρώντας με τον κάτοχό τους και μεταξύ τους, παρέχοντας και λαμβάνοντας συνεχώς δεδομένα. Με τον τρόπο αυτό επιτυγχάνεται αποτελεσματικότερη απόδοση, βέλτιστη κατανάλωση ενέργειας, ενώ οι συσκευές διατηρούνται σε καλύτερη κατάσταση και ελέγχονται από απόσταση. Η τεχνολογία Blockchain είναι ο σύνδεσμος που λείπει για να διευθετήσει τα προβλήματα κλιμάκωσης, ιδιωτικότητας και αξιοπιστίας στο τομέα του Internet-of-Things.

Σύμφωνα με την Cisco, 50 δισεκατομμύρια συσκευές πρόκειται να βρίσκονται σε απευθείας σύνδεση μέχρι το 2020.[60] Το πλήθος των συνδεδεμένων συσκευών, οι οποίες στέλνουν, λαμβάνουν και επεξεργάζονται οδηγίες για να ενεργοποιηθούν, απενεργοποιηθούν ή να μοιράσουν μεγάλη ποσότητα δεδομένων θα μπορούσε να οδηγήσει σε ένα άνευ προηγουμένου κόστος. Άλλα θέματα περιλαμβάνουν το πώς ακριβώς μπορούμε να παρακολουθούμε και να διαχειριζόμαστε δισεκατομμύρια συνδεδεμένες συσκευές, καθώς και να αποθηκεύουμε τα δεδομένα που παράγουν, με ασφαλή και αξιόπιστο τρόπο. Πριν η χρήση του IoT γίνει καθολική τα παραπάνω προβλήματα θα πρέπει να επιλυθούν.

Η τεχνολογία Blockchain θα μπορούσε να είναι η λύση για τη βιομηχανία του IoT. Η τεχνολογία Blockchain μπορεί να χρησιμοποιηθεί για την παρακολούθηση δισεκατομμυρίων συνδεδεμένων συσκευών, τη διεκπεραίωση των συναλλαγών και τον συντονισμό τους, όσον αφορά στην εξοικονόμηση πόρων για τους κατασκευαστές του κλάδου του IoT. Αυτή η αποκεντρωμένη προσέγγιση θα εξαλείψει τα μεμονωμένα σημεία αποτυχίας, δημιουργώντας ένα πιο ανθεκτικό οικοσύστημα για να λειτουργούν οι συσκευές. Οι αλγόριθμοι κρυπτογράφησης που χρησιμοποιεί το Blockchain, θα βοηθούσαν επίσης στην ασφάλεια των δεδομένων των καταναλωτών. Τα οφέλη από την αποκέντρωση του IoT είναι πολυάριθμα έναντι των συγκεντρωτικών συστημάτων.

6) Διαχείριση αλυσίδας εφοδιασμού

Η διαχείριση της σύγχρονης, συχνά παγκόσμιας, αλυσίδας εφοδιασμού είναι μια σειρά εντατικών διαδικασιών που απαιτούν τέλεια ενορχήστρωση μεταξύ πολλών κινούμενων μερών. Η σύνδεση και η δημιουργία συνδέσμων για τη διανομή αγαθών και υπηρεσιών μοιάζει πολύ περισσότερο με έναν ιστό, ο οποίος εκτείνεται σε παγκόσμιο επίπεδο παρά με μια αλυσίδα.

[59] Τρόπος ταυτοποίησης της IBM: https://www.ibm.com/blockchain/solutions/identity
[60] Πρόβλεψη της Cisco: https://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated

Όταν οι διαδικασίες γίνονται σε πολλά στάδια και περιλαμβάνουν πολλούς ενδιάμεσους μεσολαβητές που είναι διάσπαρτοι σε πολλές χώρες, συχνά γίνονται όλο και λιγότερο διαφανείς. Όσο περισσότεροι άνθρωποι εμπλέκονται, τόσο πιο περίπλοκη και δύσκολη μπορεί να γίνει η εξάπλωσης της πληροφορίας. Οι αδιαφανείς λειτουργίες δημιουργούνται ασυνείδητα όταν τα συστήματα που χρησιμοποιούνται για τη διαχείριση της αλυσίδας εφοδιασμού είναι ξεπερασμένα και ογκώδη. Τα γραφειοκρατικά στρώματα αποτελούν συχνά αναπόσπαστο κομμάτι της διαδικασίας διανομής αγαθών και υπηρεσιών. Αυτοί οι περαιτέρω παρεμβαλλόμενοι μεσάζοντες χρησιμεύουν ως μια βραχυπρόθεσμη λύση για να αντισταθμίσουν τους αναποτελεσματικούς παλιούς τρόπους που δεν έχουν καλύψει τις απαιτήσεις μιας ταχείας εξέλιξης της παγκόσμιας αγοράς.[61]

Ο αμετάβλητος χαρακτήρας της τεχνολογίας Blockchain την καθιστά κατάλληλη για σκοπούς όπως η παρακολούθηση των προϊόντων καθώς αυτά αλλάζουν κατόχους στην εφοδιαστική αλυσίδα. Καταχωρήσεις στην βάση του Blockchain μπορούν να χρησιμοποιηθούν για τη δρομολόγηση γεγονότων στην αλυσίδα προμήθειας (όπως π.χ. η κατανομή των προϊόντων όπως φτάνουν σε ένα λιμάνι στα διαφορετικά containers). Η τεχνολογία Blockchain προσφέρει ένα νέο δυναμικό τρόπο για την οργάνωση και παρακολούθηση δεδομένων και προϊόντων.

Επιπλέον, αισθητήρες που τίθενται επί των προϊόντων παρέχουν πλήρη διαφάνεια και ακριβή γνώση της διαδικασίας προμήθειας προϊόντων καθώς παρέχουν δεδομένα σε πραγματικό χρόνο για την τοποθεσία και την κατάστασή τους, καθώς μεταφέρονται στην παγκόσμια αγορά. Σύμφωνα με έρευνα της Deloitte και του σωματείου εταιρειών μηχανογράφησης κι εφοδιαστικής αλυσίδας στις Η.Π.Α. (MHI), το 2016 παρόμοιοι αισθητήρες χρησιμοποιούνταν ήδη σχεδόν από τις μισές εταιρείες του χώρου ενώ η υιοθέτησή τους προβλέπεται να είναι σχεδόν καθολική τα επόμενα χρόνια.[62] Η τεχνολογία blockchain θα αποθηκεύει, διαχειρίζεται, προστατεύει και μεταφέρει τις έξυπνες αυτές πληροφορίες με τον βέλτιστο τρόπο, παρέχοντας διαφάνεια σε πραγματικό χρόνο καθώς όλοι οι συμμετέχοντες (υπολογιστές) θα τηρούν και από ένα πλήρως ενημερωμένο αρχείο αυτών των δεδομένων.

7) Διαχείριση δικαιωμάτων πνευματικής ιδιοκτησίας

Ένα από τα βασικά ζητήματα στον τομέα της διαχείρισης δικαιωμάτων πνευματικής ιδιοκτησίας είναι η περιπλοκότητα των δικαιωμάτων κτήσης, η κατανομή των αμοιβών και η διαφάνεια λειτουργίας των οργανισμών συλλογικής διαχείρισης. Η τεχνολογία blockchain σε συνδυασμό με τα έξυπνα συμβόλαια μπορεί να παρέχει μία πλήρη και ακριβή βάση δεδομένων δικαιωμάτων πνευματικής ιδιοκτησίας, εξασφαλίζοντας διαφανή κατανομή των αμοιβών σε πραγματικό χρόνο σε όλους τους δικαιούχους. Η χρήση ψηφιακών νομισμάτων για την άμεση καταβολή των αμοιβών

[61] Εφαρμογές της τεχνολογίας Blockchain στην αλυσίδα εφοδιασμού: https://www.blockchaintechnologies.com/applications/supply-chain/
[62] Έρευνα της Deloitte: https://www2.deloitte.com/us/en/insights/focus/industry-4-0/artificial-intelligence-supply-chain-planning.html

από τους χρήστες θα διευκολύνει ακόμη περισσότερο την βέλτιστη διαχείριση των εν λόγω δικαιωμάτων. [37]

8) Διαχείριση ευαίσθητων ιατρικών δεδομένων

Η τεχνολογία Blockchain έχει τη δυνατότητα να διαταράξει τις λειτουργίες της βιομηχανίας υγειονομικής περίθαλψης, δημιουργώντας ευκαιρίες όσον αφορά τη βελτίωση στη παροχή υπηρεσιών υγείας. Ο κατανεμημένος κατάλογος (Blockchain ledger) είναι μια καινοτομία με τη δυνατότητα βελτίωσης της διαφάνειας, της ασφάλειας και της αποτελεσματικότητας. Τα έξυπνα συμβόλαια (smart contracts) στο Blockchain λειτουργούν αυτόματα χωρίς να απαιτείται από κάποιον η επαλήθευση εγγράφων ή οποιαδήποτε άλλη γραφειοκρατική διαδικασία. Με την αυτοματοποίηση σημειώνεται μείωση της γραφειοκρατίας χωρίς πια να υπάρχει χρονοτριβή στον τρόπο με τον οποίο οι ασθενείς λαμβάνουν την ιατρική τους πληροφορία και περίθαλψη.
Τα ιδρύματα που έχουν πρόσβαση σε ιατρικά δεδομένα, τα οποία μπορούν να αναλυθούν και να ενημερωθούν σε πραγματικό χρόνο, εργάζονται για την πλήρη αναμόρφωση του τομέα της υγειονομικής περίθαλψης. Τα υφιστάμενα κεντρικά μοντέλα αποδείχθηκαν αναποτελεσματικά όσον αφορά την παροχή προσιτής και ποιοτικής υγειονομικής περίθαλψης. Πολύ πιο αποτελεσματικές εφαρμογές βασισμένες στη τεχνολογία Blockchain είναι έτοιμες να αναπτυχθούν για τον επαναπροσδιορισμό του τρόπου λειτουργίας των ιδρυμάτων υγειονομικής περίθαλψης. Τόσο ο τομέα της υγειονομικής περίθαλψης, όσο και η διαδικασία συνταγογράφησης αλλά και τα μοντέλα ασφάλισης υγείας μπορούν να βελτιωθούν.

Ο κατανεμημένος κατάλογος λειτουργεί για να βελτιώσει δραματικά τη διαφάνεια και την αποδοτικότητα μιας ξεπερασμένης βιομηχανίας, ενώ παράλληλα επωφελούνται οι ασθενείς και οι πάροχοι. Οι κανονισμοί και οι έλεγχοι μπορούν να ρυθμιστούν ευκολότερα με αυτόν τον τρόπο. Η εισαγωγή της τεχνολογίας βελτιώνει επίσης τις επιχειρηματικές λειτουργίες και δίνει στους βασικούς συντελεστές της υγειονομικής περίθαλψης ένα σαφές πλεονέκτημα έναντι των ανταγωνιστών τους.

Όταν το υφιστάμενο πλαίσιο υγειονομικής περίθαλψης είναι αργό, ακριβό και απαιτεί πολλούς διαφορετικούς μεσάζοντες, γίνεται εύκολα αντιληπτό ότι υπάρχει πρόβλημα. Οι κυβερνήσεις και τα νοσοκομεία θέλουν να παρέχουν ολοκληρωμένη περίθαλψη, προσιτή ως προς τη διαχείριση, αλλά και οικονομική προς το κοινό. Μέσω της Blockchain τεχνολογίας οι επιχειρήσεις που δραστηριοποιούνται στην υγειονομική περίθαλψη μπορούν να οργανωθούν καλύτερα, να μειώσουν τα κόστη, να παρέχουν καλύτερη φροντίδα στους ασθενείς και εξορθολογίζουν τις διαδικασίες της ασφαλιστικής τους κάλυψης, με αποτέλεσμα τη συνολική βελτίωση της ποιότητας ζωής των ασθενών.[63]

Παρακάτω θα περιγραφούν δύο γνωστές εφαρμογές που έχουν βασιστεί στη Blockchain τεχνολογία.

[63] Εφαρμογές της τεχνολογίας Blockchain στην Υγειονομική Περίθλαψη: https://www.blockchaintechnologies.com/applications/healthcare/

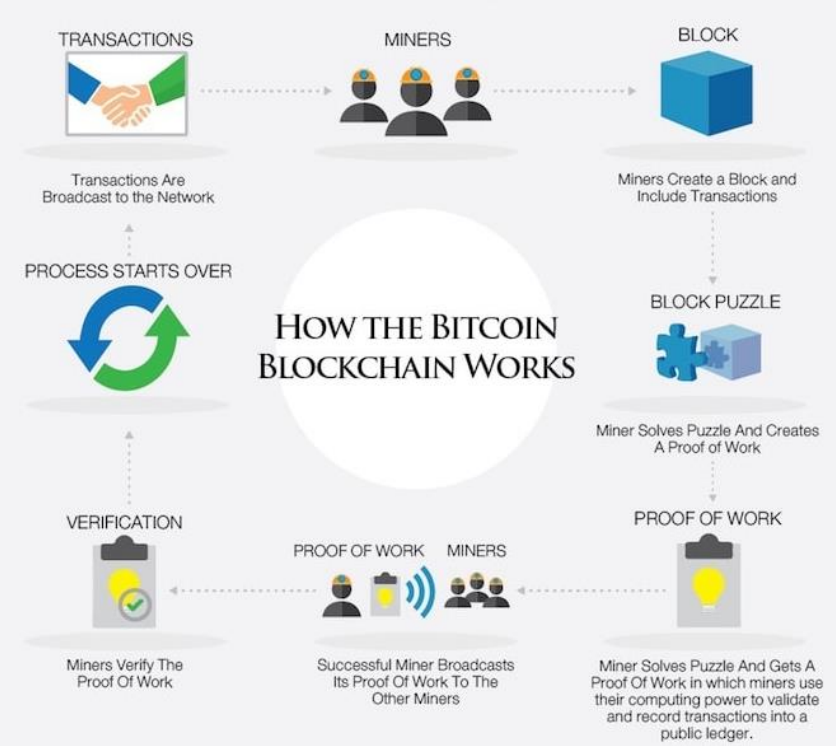
4.1.1 Περιγραφή Bitcoin

Το Bitcoin[64] είναι το πρώτο αποκεντρωμένο ψηφιακό συνάλλαγμα. Τα Bitcoins είναι ψηφιακά νομίσματα που μπορούν να σταλούν μέσο του διαδικτύου. Συγκρινόμενα με άλλες εφαρμογές τα bitcoins μεταφέρονται άμεσα από κόμβο σε κόμβο μέσω του διαδικτύου χωρίς να περνούν από μία τράπεζα ή οποιοδήποτε άλλο κεντρικό αποθετήριο, γεγονός το οποίο συμβάλει στο να είναι οι φόροι πολύ χαμηλότεροι. Μπορεί να χρησιμοποιηθεί σε οποιοδήποτε χώρο, με την μόνη προϋπόθεση να υπάρχει πρόσβαση στο διαδίκτυο. Οι λογαριασμοί δεν μπορούν να δεσμευτούν και δεν υπάρχουν προϋποθέσεις ή όρια αυθαιρεσίας.

Υπάρχουν αρκετά ανταλλακτήρια συναλλαγμάτων όπου μπορούν να αγοραστούν οι να πωληθούν bitcoin με αντάλλαγμα δολάρια, ευρώ ή οποιοδήποτε άλλο νόμισμα. Τα bitcoin κρατώνται σε ένα ψηφιακό πορτοφόλι στον υπολογιστή ή σε κάποια άλλη ηλεκτρονική συσκευή. Η αποστολή bitcoins είναι μία πολύ απλή διαδικασία όπως το να στείλεις ένα ηλεκτρονικό μήνυμα. Τέλος υπάρχει η δυνατότητα απευθείας αγοράς προϊόντων με bitcoin.Το δίκτυο Bitcoin είναι ασφαλισμένο από άτομα που αποκαλούνται miners. Οι miners επιβραβεύονται με bitcoins για να επιβεβαιώνουν τις συναλλαγές και κατόπιν της επιβεβαίωσής τους, οι συναλλαγές καταγράφονται σε ένα διαφανές δημόσιο αρχείο (ledger).

Το Bitcoin επίσης ανοίγει μία ολοκαίνουρια πλατφόρμα για την καινοτομία, καθώς το λογισμικό είναι εξολοκλήρου open source και ο καθένας μπορεί να επιθεωρήσει τον κώδικα, τον οποίο χρησιμοποιεί η εφαρμογή για να λειτουργήσει.Τα Bitcoins είναι ένας καλός τρόπος για τις επιχειρήσεις ούτως ώστε να ελαχιστοποιήσουν τους φόρους των συναλλαγών τους. Δεν κοστίζει τίποτα στην επιχείρηση να τα αποδέχεται και είναι εύκολα στην εγκατάσταση. Τέλος δεν υπάρχουν αντιστροφές χρεώσεων και οι επιχειρήσεις μπορούν επίσης να ευνοηθούν από τους χρήστες που επιλέγουν το Bitcoin ως μέσο πληρωμής.

[64] Σελίδα του Bitcoin: https://bitcoin.org



Εικόνα 11: Τρόπος λειτουργίας του Bitcoin[65]

Υπόλοιπα Λογαριασμού με Blockchain

Το Blockchain ledger είναι ένα κοινόχρηστο δημόσιο λογιστικό βιβλίο πάνω στο οποίο βασίζεται ολόκληρο το δίκτυο Bitcoin. Όλες οι επιβεβαιωμένες συναλλαγές συμπεριλαμβάνονται στο Blockchain. Με αυτό τον τρόπο, τα πορτοφόλια Bitcoin μπορούν να υπολογίζουν το διαθέσιμο υπόλοιπο και οι νέες συναλλαγές μπορούν να επαληθεύουν ότι δαπανώνται bitcoins τα οποία στην πραγματικότητα κατέχονται από αυτόν που τα δαπανά. Η ακεραιότητα και η χρονολογική σειρά της αλυσίδας των μπλοκ εφαρμόζονται με την κρυπτογραφία.

Συναλλαγές - ιδιωτικά κλειδιά

Μια συναλλαγή είναι μια μεταφορά αξίας μεταξύ πορτοφολιών Bitcoin, η οποία συμπεριλαμβάνεται στο Blockchain. Τα πορτοφόλια Bitcoin κρατάνε ένα μυστικό κομμάτι δεδομένων που ονομάζεται ιδιωτικό κλειδί, το οποίο χρησιμοποιείται για να υπογράψει συναλλαγές παρέχοντας μια μαθηματική απόδειξη η οποία έχει προέλθει από το πορτοφόλι του ιδιοκτήτη. Η υπογραφή επίσης εμποδίζει τη συναλλαγή από το να τροποποιηθεί από τον οποιονδήποτε μόλις αυτή έχει εκδοθεί. Όλες οι συναλλαγές μεταδίδονται μεταξύ των χρηστών και συνήθως ξεκινάνε να επιβεβαιώνονται από το δίκτυο στα επόμενα 10 λεπτά μέσω μια διαδικασίας που ονομάζεται mining.

Επεξεργασία - mining

Η εξόρυξη (mining) είναι ένα κατανεμημένο συναινετικό σύστημα που χρησιμοποιείται για την επιβεβαίωση συναλλαγών που βρίσκονται σε αναμονή στο Blockchain. Επιβάλλει μια χρονολογική σειρά στην αλυσίδα των μπλοκ, προστατεύει

[65] Περιραφή της εφαρμογής Bitcoin: https://www.weusecoins.com/

την ουδετερότητα του δικτύου και επιτρέπει σε διαφορετικούς υπολογιστές να συμφωνήσουν σχετικά με την κατάσταση του συστήματος. Για να επιβεβαιωθούν, οι συναλλαγές πρέπει να εντάσσονται σε ένα μπλοκ (block) που υπακούει σε πολύ αυστηρούς κανόνες κρυπτογραφίας που θα επαληθευτούν από το δίκτυο. Οι κανόνες αυτοί εμποδίζουν τα προηγούμενα μπλοκ από το να τροποποιηθούν, διότι κάτι τέτοιο θα ακύρωνε όλα τα ακόλουθα μπλοκ. Η εξόρυξη δημιουργεί επίσης το ισοδύναμο μιας ανταγωνιστικής λοταρίας, η οποία εμποδίζει κάθε άτομο από το να προσθέσει εύκολα νέα διαδοχικά μπλοκ στο Blockchain. Με αυτόν τον τρόπο, κανένα άτομο δεν μπορεί να ελέγξει τι περιλαμβάνεται στην αλυσίδα των μπλοκ ή να αντικαταστήσει τμήματα της αλυσίδας αυτής για να ακυρώσει τις δικές του δαπάνες.

4.1.2 Περιγραφή Ethereum

Σκοπός του Ethereum[66] είναι να δημιουργήσει ένα εναλλακτικό πρωτόκολλο για την οικοδόμηση αποκεντρωμένων εφαρμογών, παρέχοντας ένα διαφορετικό σύνολο συναλλαγών. Η συγκεκριμένη εφαρμογή ταιριάζει περισσότερο σε περιπτώσεις όπου ο χρόνος ανάπτυξης είναι περιορισμένος, παρέχει ασφάλεια για μικρές εφαρμογές που χρησιμοποιούνται σπάνια και επίσης προσφέρει τη δυνατότητα αλληλεπίδρασης διαφορετικών εφαρμογών μεταξύ τους. Το Ethereum το κάνει αυτό κατασκευάζοντας ουσιαστικά το τελικό αφηρημένο θεμελιώδες στρώμα, δηλαδή ένα Blockchain με μια ενσωματωμένη γλώσσα προγραμματισμού Turing-complete, επιτρέποντας σε οποιονδήποτε να γράψει Smart Contracts και αποκεντρωμένες εφαρμογές όπου μπορούν να δημιουργήσουν τους δικούς τους αυθαίρετους κανόνες ιδιοκτησίας, καθώς και παντός είδους μεταβατικές λειτουργίες. Τα έξυπνα συμβόλαια μπορούν να εκτελεστούν χρησιμοποιώντας ένα κοινό δίκτυο δημόσιων κόμβων. Η εφαρμογή υποστηρίζει επίσης τη δημιουργία ενός κρυπτονομίσματος για το οποίο αρκούν δύο σειρές κώδικα και άλλα πρωτόκολλα όπως νομίσματα και συστήματα ανταπόδοσης, τα οποία επίσης απαιτούν πολύ λίγο κώδικα. Τα έξυπνα συμβόλαια (κρυπτογραφικά "κουτιά" που περιέχουν αξία και ξεκλειδώνουν μόνο αν πληρούνται ορισμένες προϋποθέσεις) μπορούν επίσης να χτιστούν μέσω της πλατφόρμας, με πιο αποδοτικό τρόπο από αυτόν που προσφέρει το Bitcoin, λόγω των πρόσθετων δυνατοτήτων της Turing-complete γλώσσας προγραμματισμού και της προσοχής που έχει δοθεί στην αξιοποίηση της Blockchain τεχνολογίας. [39]

Όπως αναφέρθηκε και παραπάνω το Ethereum παρέχει τη δυνατότητα δημιουργίας κρυπτονομίσματος που ονομάζεται "Ether", το οποίο μπορεί να μεταφερθεί μεταξύ λογαριασμών και να χρησιμοποιηθεί για την αντιστάθμιση των συμμετεχόντων κόμβων για υπολογισμούς που εκτελούνται. Χρησιμοποιείται πέρα της ανταλλακτικής του αξίας[67] και σαν «φόρος» για αλληλεπίδραση με τα Smart Contract στο δίκτυο αλλά και ως μέσο κοστολόγησης για την υπολογιστική ισχύ που χρειάζεται το Ethereum Blockchain. Το "Gas", ένας μηχανισμός εσωτερικής τιμολόγησης συναλλαγών, χρησιμοποιείται για την αντιμετώπιση των ανεπιθύμητων μηνυμάτων και την κατανομή πόρων στο δίκτυο. Ουσιαστικά, το Ethereum είναι μια παγκόσμια υπολογιστική μηχανή. Αποτελείται από τους δεκάδες χιλιάδες υπολογιστές που συνδέονται στο δίκτυο για να σφραγίσουν συναλλαγές και οι πόροι τους τρέχουν τις εφαρμογές που δημιουργούμε. Το Ethereum προτάθηκε στα τέλη

[66] Σελίδα της εφαρμογής Ethereum: https://www.ethereum.org/
[67] Ανταλλακτική αξίας γνωστών κρυπτονομισμάτων: https://www.coinbase.com/price

του 2013 από τον Vitalik Buterin, έναν ερευνητή και προγραμματιστή κρυπτογράφησης. Η ανάπτυξη χρηματοδοτήθηκε από μία online κοινότητα από τον Ιούλιο έως τον Αύγουστο του 2014. Το σύστημα τέθηκε σε λειτουργία στις 30 Ιουλίου 2015, με 11,9 εκατομμύρια νομίσματα "premined" για την κοινότητα που το υποστήριξε. Μια από τις ιδέες που βρήκαν εφαρμογή στην πλατφόρμα του Ethereum, ήταν η δημιουργία ενός ανεξάρτητου και αυτόνομου οργανισμού με ψηφιακά κεφάλαια επιχειρηματικών συμμετοχών (venture capital funds).Ο σκοπός αυτών των οργανισμών είναι να υποστηρίζουν νέες startup επιχειρήσεις Τον Απρίλιο του 2016 ο προγραμματιστής Christoph Jentzsch ανακοίνωσε τον οργανισμό DAO. Τα αρχικά σημαίνουν Decentralized Autonomous Organization, ή αλλιώς Αποκεντρωμένη Αυτόνομη Οργάνωση. Με την τεχνολογία των smart contracts του Ethereum, ο Jentzsch δημιούργησε τα νομίσματα DAO tokens. Μέσω της διαδικασίας του Initial Coin Offering (ICO) τα προσφέρει για αγορά σε υποψήφιους επενδυτές. Το όνομα ICO είναι το αντίστοιχο του IPO (Initial Public Offering), που είναι η διαδικασία όταν μια εταιρεία μπαίνει στο χρηματιστήριο και διαθέτει μετοχές για αγορά από το κοινό. Με το ICO, κάθε μέλος αγοράζει ένα ποσοστό των DAO tokens και συμμετέχει στην αύξηση του κεφαλαίου του οργανισμού. Επιπλέον, έχει το δικαίωμα της ψήφου για την τελική επιλογή των startups που έχουν αιτηθεί χρηματοδότησης. Εάν οι νέες επιχειρήσεις πετύχουν, ένα μέρος από τα κέρδη τους επιστρέφεται με την μορφή μερίσματος στους επενδυτές, ανάλογα με το ποσοστό των DAO tokens που κατέχουν. Τον Μάιο του 2016, η αξία των χρημάτων που επενδύθηκαν σε DAO tokens ξεπερνούσε τα $150 εκατομμύρια, προσελκύοντας πάνω από 11.000 επενδυτές. Παράλληλα, η συναλλαγματική αξία της μονάδας των DAO tokens έχει αποδοτική πορεία στην αντίστοιχη αγορά. Τον Ιούνιο του 2016, το DAO δέχτηκε διαδικτυακή επίθεση, λόγω ορισμένων κενών ασφαλείας στα smart contracts του. Ο hacker απέκτησε πρόσβαση και έκλεψε το 1/3 των ψηφιακών περιουσιακών στοιχείων του οργανισμού, που ισοδυναμούσαν εκείνο το διάστημα με $50 εκατομμύρια. Το πλήγμα ήταν τεράστιο τόσο για το DAO όσο και για το Ethereum, από τη στιγμή που χρησιμοποιούσε αυτήν την τεχνολογία για να τρέξει το δίκτυό του. Επιπρόσθετα, χιλιάδες χρήστες έχασαν τα χρήματά τους που τα είχαν μετατρέψει σε DAO tokens. Τις επόμενες ημέρες, η συναλλαγματική αξία της μονάδας του Ethereum κατρακύλησε. Έπρεπε άμεσα να παρθούν αποφάσεις για το μέλλον του Ethereum και για τους καταθέτες του DAO. Η πρώτη ενέργεια των βασικών προγραμματιστών της ομάδας του Ethereum ήταν μια αντισυμβατική κίνηση. Βρήκαν την διεύθυνση στην οποία ήταν αποθηκευμένα τα ηλεκτρονικά χρήματα με την μορφή των smart contracts του DAO, και χάκαραν τον hacker. Με αυτόν τον τρόπο ανέκτησαν ψηφιακά περιουσιακά στοιχεία αξίας $48M, τα οποία θα μοιράζονταν στους ιδιοκτήτες τους. Το επόμενο “αγκάθι” της ομάδας του Ethereum ήταν ότι για να αναδιανεμηθούν τα κλοπιμαία tokens, πρέπει να γίνει μια “επαναφορά” στο σύστημα του Ethereum, το λεγόμενο Fork. Με απλά λόγια, πρέπει να επαναφέρουν τις συναλλαγές (blockchain) στο δίκτυο του Ethereum στο σημείο που ήταν πριν ακριβώς από την επίθεση. Ωστόσο, όπως αναφέραμε και στην αρχή, αν γίνουν αλλαγές στο Blockchain, τίθεται σε περαιτέρω κίνδυνο η αξιοπιστία και συνεπώς η αξία του νομίσματος. Συνεπώς, για να γινόταν αυτή η αλλαγή, έπρεπε να έχουν την σύμφωνη γνώμη όλων όσων εμπλέκονταν άμεσα ή έμμεσα με την πλατφόρμα του Ethereum. Φυσικά, οι developers του Ethereum γνώριζαν ότι καθολική συμφωνία ήταν εξαιρετικά δύσκολο να επιτευχθεί. Οι αντιδράσεις προέρχονταν από την λογική σκέψη ορισμένων χρηστών ότι τα περιουσιακά τους στοιχεία στο δίκτυο του Ethereum θα καταλήξουν να μην αξίζουν τίποτα, ενώ υπήρχαν και οι φωνές από τους διάφορους χρήστες του δικτύου που δεν ήθελαν αυτή την παρέμβαση στο σύστημα

του Ethereum. Η απόφαση πάρθηκε, και μετά από μια μεγάλη αναβάθμιση της ασφάλειας του δικτύου του κυρίως για την αντιμετώπιση DDoS επιθέσεων, το Ethereum χωρίστηκε στα δύο. Οι διαφωνούντες συνεχίζουν στο δίκτυο του Ethereum Classic, ενώ οι περισσότεροι μεταφέρθηκαν στο forked δίκτυο με το σκέτο όνομα Ethereum, που έχει και την υψηλότερη αξία. [40]

4.1.2.1 Ethereum Mining

Στις αρχές του 2018, με την ιλιγγιώδη αύξηση στην αξία του Ethereum, σημαντικός αριθμός χρηστών άρχισε να ενδιαφέρεται για το mining. Ενώ ο τρόπος που γίνεται το mining του Ethereum είναι πιο απλός απλό εκείνον του Bitcoin, και σε αυτή την περίπτωση δεν αρκεί ένας συμβατικός υπολογιστής. Ένα έμπρακτο παράδειγμα είναι ο Anthony Garreffa, ένας από τους συντελεστές της ιστοσελίδας Tweaktown. Στα μέσα Ιουνίου 2017 είχε κέρδος $900 το μήνα σε Ethereum, ωστόσο ο εξοπλισμός που χρησιμοποιούσε για το mining είχε αξία $10.000. Καθώς η συγκεκριμένη ιστοσελίδα ασχολείται με reviews, ο εξοπλισμός ήταν πρακτικά δωρεάν, από κάρτες γραφικών και υποσυστήματα που είχαν στείλει εταιρείες για δοκιμή. Με δεδομένη όμως την αστάθεια των ψηφιακών νομισμάτων, δεν αξίζει με κανένα τρόπο να επενδύσει κανείς μερικές χιλιάδες ευρώ για να ασχοληθεί με το mining, καθώς δεν υπάρχει εγγύηση πως θα κάνει απόσβεση του εξοπλισμού, και του ρεύματος που θα καταναλώσει. Δεν είναι τυχαίο πως μια ψεύτικη είδηση στα τέλη Ιουνίου, για το δήθεν θάνατο του ιδρυτή του Ethereum, είχε σαν αποτέλεσμα το νόμισμα να χάσει 4 δισεκατομμύρια δολάρια από τη συνολική αξία του. [40]

4.1.2.2 Λειτουργία Ethereum και Ethereum Virtual Machine

Το Ethereum είναι ένα προγραμματιζόμενο Blockchain. Αντί να δώσει στους χρήστες ένα σύνολο προκαθορισμένων λειτουργιών (π.χ. Bitcoin συναλλαγές), το Ethereum επιτρέπει στους χρήστες να δημιουργήσουν τις δικές τους λειτουργίες δηλαδή να δημιουργήσουν λογικές συνθήκες οποιασδήποτε πολυπλοκότητας επιθυμούν μέσα στην Blockchain δομή. Με αυτόν τον τρόπο, το Ethereum χρησιμεύει ως πλατφόρμα για πολλούς διαφορετικούς τύπους εφαρμογών αποκεντρωμένων Blockchain, που περιλαμβάνουν αλλά δεν περιορίζονται σε κρυπτονομίσματα. Το Ethereum αναφέρεται σε μια σουίτα πρωτοκόλλων που καθορίζουν μια πλατφόρμα για αποκεντρωμένες εφαρμογές. Στην καρδιά της σουίτας βρίσκεται το Ethereum Virtual Machine (EVM), το οποίο μπορεί να εκτελέσει κώδικα αυθαίρετης αλγοριθμικής πολυπλοκότητας. Σε όρους της επιστήμης των υπολογιστών, το Ethereum είναι "Turing complete". Οι προγραμματιστές μπορούν να δημιουργήσουν εφαρμογές που τρέχουν στο EVM με τη χρήση φιλικών γλωσσών προγραμματισμού οι οποίες βασίζονται σε υφιστάμενες γλώσσες όπως JavaScript και Python. Όπως κάθε blockchain, έτσι και το Ethereum περιλαμβάνει επίσης ένα πρωτόκολλο δικτύου peer-to-peer. Η Ethereum blockchain βάση δεδομένων συντηρείται και ενημερώνεται από πολλούς κόμβους που συνδέονται με το δίκτυο. Κάθε κόμβος του δικτύου διαχειρίζεται το EVM και εκτελεί τις ίδιες οδηγίες. Για το λόγο αυτό, το Ethereum μερικές φορές περιγράφεται ως «ο υπολογιστής του κόσμου». Στην πραγματικότητα, αυτή η μέθοδος καθιστά τους υπολογισμούς στο Ethereum πολύ πιο αργούς και πιο ακριβούς από ότι σε ένα παραδοσιακό "υπολογιστή". Αντίθετα, κάθε Ethereum κόμβος τρέχει το EVM, προκειμένου να διατηρηθεί η συναίνεση σε ολόκληρο το

blockchain. Αυτή η αποκεντρωμένη συναίνεση δίνει στο Ethereum ακραία επίπεδα ανοχής σφαλμάτων, εξασφαλίζει μηδενικό downtime και κάνει τα δεδομένα που είναι αποθηκευμένα στο blockchain για πάντα αναλλοίωτα. Η Ethereum πλατφόρμα προσφέρει μια λογική προγραμματισμού παρόμοια με τις κοινές γλώσσες προγραμματισμού, καθώς εναπόκειται στους προγραμματιστές να αποφασίσουν που θα πρέπει να χρησιμοποιείται. Ωστόσο, είναι σαφές ότι ορισμένοι τύποι εφαρμογών επωφελούνται περισσότερο από άλλους από τις δυνατότητες του Ethereum. Συγκεκριμένα, το Ethereum είναι κατάλληλο για εφαρμογές που αυτοματοποιούν την άμεση αλληλεπίδραση μεταξύ των κόμβων ή διευκολύνουν τη συντονισμένη δράση της ομάδας σε ένα δίκτυο, όπως για παράδειγμα, οι αιτήσεις για το συντονισμό peer-to-peer αγορών, ή η αυτοματοποίηση των σύνθετων χρηματοπιστωτικών συμβάσεων. Το Bitcoin επιτρέπει στα άτομα να ανταλλάσσουν μετρητά χωρίς τη συμμετοχή από τυχόν μεσάζοντες όπως τα χρηματοπιστωτικά ιδρύματα, τράπεζες, ή κυβερνήσεις. Το αντίκτυπο του Ethereum μπορεί να είναι πιο εκτεταμένο. Στη θεωρία, οι οικονομικές αλληλεπιδράσεις ή ανταλλαγές οποιασδήποτε πολυπλοκότητας θα μπορούσαν να πραγματοποιηθούν αυτόματα και αξιόπιστα με τη χρήση κώδικα που εκτελείται σε Ethereum. Η Εικονική Μηχανή Ethereum (Ethereum Virtual Machine) είναι το περιβάλλον εκτέλεσης των Smart Contract στο Ethereum. Ο επίσημος ορισμός του EVM καθορίζεται στην αρχική έκδοση του EthereumYellowPaper[39], διατυπωμένη από τον Gavin Wood. Είναι sandboxed και εντελώς απομονωμένο από το δίκτυο, το σύστημα αρχείων ή άλλες διαδικασίες του κεντρικού υπολογιστή. Κάθε κόμβος Ethereum στο δίκτυο εκτελεί το EVM σύμφωνα με τις ίδιες οδηγίες. Οι εικονικές μηχανές Ethereum έχουν υλοποιηθεί σε C ++, Go, Haskell, Java, JavaScript, Python, Ruby, Rust και Web Assembly. [40]

4.2 Υφιστάμενες εφαρμογές υγείας με Blockchain τεχνολογία και τρόπος λειτουργίας

Το Bitcoin και το Ethereum είναι οι πιο γνωστές εφαρμογές της τεχνολογίας Blockchain μέχρι σήμερα. Ωστόσο υπάρχουν κι άλλες εταιρίες που έχουν εφαρμόσει την τεχνολογία αυτή, ακόμα και για συναλλαγές υγειονομικής περίθαλψης, καθώς και για πληροφορίες ασθενών. Κάποιες από αυτές αναφέρονται παρακάτω[68].

4.2.1 Περιγραφή Patientory

Το Patientory είναι μία κατανεμημένη εφαρμογή σχεδιασμένη με την τεχνολογία Blockchain που παρέχει στους χρήστες πρόσβαση στα δεδομένα υγείας τους και ξεκίνησε στις ΗΠΑ. Λειτουργεί ως μία γέφυρα που ενώνει τα συγκεντρωμένα ιατρικά και υγειονομικά συστήματα αρχειοθέτησης. Δημιουργεί έξυπνα συμβόλαια που μπορούν να εκτελεστούν όσον αφορά ένα πλήρες φαρμακευτικό και ιατρικό ιστορικό ασθενών. Το σύστημα αναδεικνύει την διαλειτουργικότητας και παρέχει ασφάλειας στον κυβερνοχώρο, ενώ παράλληλα έχει τη δυνατότητα να εξαλείψει τις τριβές και το κόστος της ύπαρξης των μεσαζόντων όσον αφορά στην διαχείριση της υγείας. Δίνει έμφαση στην ακεραιότητα των δεδομένων, στη μείωση του κόστους των

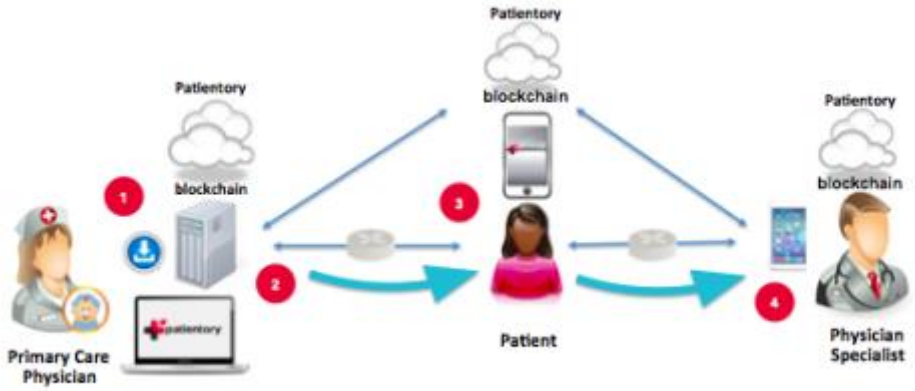
[68] Εταιρείες που έχουν εφαρμόσει την τεχνολογία Blockchain στον τομέα της υγειονομικής περίθαλψης: https://www.beckershospitalreview.com/lists/25-blockchain-companies-in-healthcare-to-know-2017.html

συναλλαγών, στην αποκέντρωση και στη δημιουργία εμπιστοσύνης μεταξύ των οντοτήτων του δικτύου. Ο συντονισμός της περίθαλψη των ασθενών ουσιαστικά ανακουφίζει από τις άσκοπες υπηρεσίες και τις διπλές δοκιμές με τη μείωση του κόστους και τη βελτίωση της αποτελεσματικότητας του κύκλου φροντίδας, τηρώντας παράλληλα όλους τους κανόνες και τα πρότυπα της επικείμενης νομοθεσίας. Τα παραπάνω επιτυγχάνονται μέσω της διαχείρισης ηλεκτρονικών ιατρικών δεδομένων και της αλληλεπίδρασης με κλινικές ομάδες φροντίδας.

4.2.1.1 Σχέση Ασθενούς-Παρόχου στο Patientory

Το νέο πρότυπο της υγειονομικής περίθαλψης απαιτεί την ανάγκη για αποτελεσματική και βέλτιστη φροντίδα στους ασθενείς ώστε να αποφέρει καλύτερα αποτελέσματα περίθαλψης. Αυτό απαιτεί χρόνο και οι πάροχοι υπηρεσιών φροντίδας θα πρέπει να είναι σε θέση να συντονίζονται και να συνεργάζονται ενεργά με άλλους εμπλεκόμενους παρόχους και βοηθητικές οργανώσεις υγείας όπως τα μικροβιολογικά εργαστήρια και τα φαρμακεία. Επιπλέον, για να είναι επιτυχή τα αρχεία ασθενών πρέπει να να ενημερώνονται και να τροποποιούνται έγκαιρα.

Το λογισμικό EMR (Electronic Medical Record) απαγορεύει επί του παρόντος μία αποτελεσματική σχέση ασθενούς παρόχου. Αυτό το λογισμικό παρέχει μόνο μια περιορισμένη δυνατότητα ανταλλαγής πληροφοριών από το ένα σύστημα στο άλλο και συνήθως απαιτεί ένα καθορισμένο άτομο να είναι σε θέση να μεταφέρει τέτοιες πληροφορίες. Αυτό οδηγεί σε αυξημένη καθυστέρηση μεταξύ των οργανισμών στην παροχή φροντίδας για τον ασθενή και έχει επίσης ως αποτέλεσμα τη συνολική μείωση της ποιότητας των υπηρεσιών περίθαλψης. Επίσης, καθώς οι πάροχοι περίθαλψης δαπανούν περισσότερο χρόνο για τον συντονισμό της περίθαλψης, ο φόρτος εργασίας έχει αυξηθεί αισθητά, δημιουργώντας επίσης αρνητικό αντίκτυπο όσον αφορά την περίθαλψη των ασθενών. Επιπλέον, δεδομένου ότι πολλοί γιατροί δεν επιθυμούν την πρόσβαση των ασθενών τους στα EHR(Electronic Health Records), οι ασθενείς υιοθετούν παθητικό ρόλο στην παρακολούθηση της υγείας τους. Αυτό τελικά τους κάνει να αισθάνονται την έλλειψη του ελέγχου της πορείας της υγείας τους που οδηγεί τον ασθενή σε απογοήτευση και στην απεμπλοκή από την φροντίδα του. Παρόλο που υπάρχει πρόσφατη αύξηση των εφαρμογών Mobile Health Care οι οποίες βοηθούν τα άτομα να παρακολουθούν τις ζωτικές παραμέτρους της υγείας τους, η καινοτομία αυτή δεν έχει μεταφραστεί σε βελτιωμένη φροντίδα και αποτελέσματα, ούτε έχουν καταφέρει να ενσωματώσουν τα EHRs.



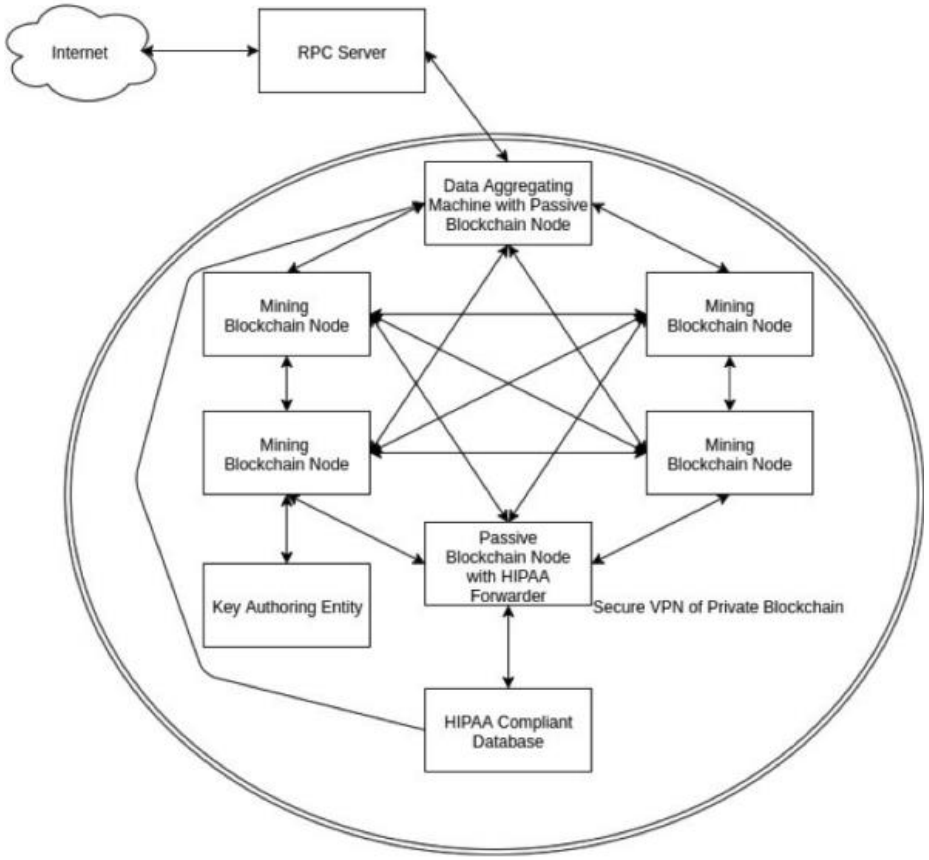
Εικόνα 12: Σχήμα του Patientory[69]

Τα EMR είναι κεντρικές δομές που υπόκεινται σε πειρατεία, αυστηρούς κανονισμούς ασφαλείας και αυξημένες δαπάνες. Το Patientory Blockchain όσον αφορά τις συναλλαγές, ελαχιστοποιεί τις παραβιάσεις εξαιτίας των ιδιοτήτων ελέγχου πρόσβασης του συστήματος και δημιουργεί ένα κανάλι για τη διευκόλυνση του συντονισμού της φροντίδας με αποτελέσματα τη συνολική βελτίωση των αποτελεσμάτων της υγείας. Παραπάνω φαίνεται σχηματικά η υποδομή του Patientory Blockchain και της διαλειτουργικότητάς του μεταξύ των ασθενών και των υπόλοιπων παρόχων. [41]

4.2.1.2 Υλοποίηση του Patientory

Εκτός από τη φυσική απομόνωση των συστημάτων στο υλικό και το δίκτυο εφαρμογής, ο έλεγχος πρόσβασης λογισμικού διευκολύνει την ακεραιότητα των δεδομένων και την επαλήθευση της εξουσιοδότησης για τις οντότητες. Το σύστημα λογισμικού από την οπτική του ελέγχου πρόσβασης και της κρυπτογράφησης δεδομένων περιγράφεται παρακάτω.

[69] Patientory whitepaper: https://www.semanticscholar.org/paper/Patientory-%3A-A-Healthcare-Peer-to-Peer-EMR-Storage-McFarlane-Beer/7c95c0b29abd3701eebc8718528d0cdb72264c47



Εικόνα 13: Τοπογραφία του Patientory Blockchain Δικτύου

Η βάση δεδομένων που είναι συμβατή με το HIPAA (Health Insurance Portability and Accountability Act) θα δέχεται μόνο εισερχόμενες συνδέσεις από τον μεταφορέα HIPAA. Αυτό εξασφαλίζει ότι η ροή της κυκλοφορίας είναι απομονωμένη σε γνωστές ελεγχόμενες διαδρομές. Ο αποστολέας HIPAA θα ενεργήσει μόνο για να διαβιβάσει ένα request στην εγκατάσταση αποθήκευσης HIPAA εν αναμονή μιας έγκυρης συναλλαγής που έχει συμβεί στο Blockchain και την εκπομπή ενός ζητούμενου event. Το event πρέπει να περιέχει το δημόσιο κλειδί του αιτούντος, και τα πεδία δεδομένων που ζητούνται. Τέλος, ο διακομιστής RPC (Remote Procedural Call) χρησιμοποιεί ένα API (Application Programming Interface), έτσι ώστε να μπορούν να το χρησιμοποιήσουν μόνο γνωστοί χρήστες που αλληλεπιδρούν με το διακομιστή.

Κάθε χρήστης στο σύστημα έχει μια ιδιωτική διεύθυνση στο Blockchain. Σε κάθε ιδιωτική διεύθυνση επιτρέπεται μόνο να μιλήσει άμεσα με ένα συμβόλαιο στο Blockchain. Αυτή η σύμβαση είναι η σύμβαση κλάσης του ατόμου. Τα ιδρύματα, οι υπάλληλοι των ιδρυμάτων, και οι πελάτες είναι objects.

Αυτά τα objects είναι διασυνδέσεις που βασίζονται σε δικαιώματα. Η σύμβαση του ιδρύματος έχει μια λίστα με όλους τους πελάτες που έχουν παραχωρήσει δικαιώματα προβολής στο ίδρυμα και κάθε σύμβαση πελάτη έχει κατάλογο όλων των θεσμικών οργάνων όπου τους έχει χορηγηθεί άδεια. Η σύμβαση που κατέχει το ίδρυμα λειτουργεί και διευκολύνει την ανάκληση των αδειών στο θεσμικό όργανο, από τους χρήστες. Η σύμβαση του ιδρύματος δεν μπορεί να τροποποιήσει αυτόν τον κατάλογο, αποτρέποντας μη εξουσιοδοτημένη πρόσβαση σε αρχεία ασθενών.

Στο πλαίσιο αυτού του συστήματος, όλα τα εξωτερικά μέρη αλληλεπιδρούν με την υποβολή υπογεγραμμένων συναλλαγών που κωδικοποιούν την κλήση που ζητείται. Οι συναλλαγές αυτές υποβάλλονται μέσω του διακομιστή RPC κατά την επικύρωση του χρήστη. Οι αναρτήσεις του διακομιστή RPC και τα αιτήματα μεταβαίνουν προς τον διακομιστή συγκεντρωτικών δεδομένων, ο οποίος στη συνέχεια διαβιβάζει αυτά τα αιτήματα στους miners με βάση έναν μηχανισμό επιμερισμού φορτίων. Οι miners στη συνέχεια επεξεργάζονται το αίτημα υποβάλλοντας τη συναλλαγή για λογαριασμό του καλούντος στο συμβαλλόμενο μέρος του αντίστοιχου συμβολαίου ελέγχου. Αυτή η σύμβαση είναι η μόνη οντότητα που θα δεχθεί μια συναλλαγή από εξωτερικό αίτημα. Για κάθε δεδομένη συναλλαγή, υπάρχει ένα αμετάβλητο αρχείο καλούντος. Αυτό εξασφαλίζει ότι όλες οι προσπάθειες πρόσβασης σε πληροφορίες καταγράφονται. Λόγω του περιορισμού ότι ο αιτών μπορεί να ζητήσει μόνο μια έγκυρη συναλλαγή από τη βάση δεδομένων, και οτι ο χρήστης δεν μπορεί να αλλάξει άμεσα τις δικές του πληροφορίες, ο έλεγχος πρόσβασης είναι αποδεδειγμένος. Από την θεσμική άποψη, οι μηχανισμοί είναι παρόμοιοι, εκτός από το γεγονός ότι η σύμβαση ιδρύματος φιλοξενεί έναν κατάλογο χρηστών από τον οποιον μπορεί να ζητήσει δεδομένα και μια λίστα χρηστών που μπορεί να αλληλεπιδράσει με αυτούς ως εργαζομένους. Όταν μια συναλλαγή αίτησης προέρχεται από τον φορέα ενός οργάνου, η σύμβαση ελέγχου καλεί το ίδρυμα, που καλεί τη σύμβαση χρήστη να ζητήσει τους δείκτες δεδομένων που επιλύουν το ePHI.

Για λόγους σαφήνειας, η πλήρης διαδικασία μιας ενιαίας αίτησης έχει ως εξής: Το εξωτερικό μέρος ζητά δεδομένα από την υπηρεσία καλώντας τον RPC Server με την κρυπτογραφικά υπογεγραμμένη συναλλαγή. Ο διακομιστής RPC επαληθεύει την ταυτότητα του εξωτερικού μέρους μέσω της υπογραφής μιας αίτησης σύνδεσης. Εν αναμονή της υπογραφής, ο διακομιστής RPC συνδέεται με μια καταχώρηση στη βάση δεδομένων εξουσιοδοτημένων δημόσιων κλειδιών, δέχεται την αίτηση και υποβάλλει το αίτημα στο μηχάνημα συσσώρευσης δεδομένων. Στη συνέχεια, η μηχανή δεδομένων συσσωρεύει αιτήματα από τους ιδιωτικούς επαληθευτές αλυσίδας. Οι επαληθευτές λαμβάνουν το αίτημα ως μια κλήση από έναν λογαριασμό αλυσίδας σε σχέση με μια σύμβαση-στόχο. Οι επαληθευτές εκτελούν αυτήν την κλήση και, σε περίπτωση που η αίτηση είναι μια επιτρεπόμενη ενέργεια, η συναλλαγή εισάγεται στο επόμενο μπλοκ. Αυτή η συναλλαγή προκαλεί επίσης την εκπομπή ενός μηνύματος συμβάντος στην αλυσίδα. Αυτό το μήνυμα συμβάντος το λαμβάνει το HIPAA Forwarder, το οποίος ενεργεί για να δημιουργήσει μια κρυπτογραφημένη αίτηση έναντι του χώρου αποθήκευσης HIPAA. Αυτό το μήνυμα περιέχει επίσης το κοινό κλειδί του αιτούντος μέρους. Το σύστημα βάσεων δεδομένων που συμμορφώνεται με το HIPAA τηρεί αυτό το αίτημα και μεταδίδει ένα κρυπτογραφημένο αντίγραφο των πληροφοριών στο RPC χρησιμοποιώντας το δημόσιο κλειδί του αιτούντος. Στη συνέχεια, ο διακομιστής RPC επιστρέφει τις πληροφορίες αυτές στο συμβαλλόμενο μέρος, μετατοπίζοντας την αιτούσα διεύθυνση IP στο δημόσιο κλειδί του μηνύματος. Ο διακομιστής RPC μεταδίδει αυτό το μήνυμα χωρίς να δεί τα υποκείμενα δεδομένα. Αυτά τα δεδομένα καταστρέφονται αμέσως από τον διακομιστή RPC, διασφαλίζοντας έτσι ότι ο διακομιστής λειτουργεί ως αγωγός που δεν χρειάζεται να είναι συμβατός με το HIPAA. Ο μηχανισμός δημοσίευσης δεδομένων είναι και πάλι παρόμοιος, αλλά τα δεδομένα που πρόκειται να υποβληθούν κρυπτογραφούνται με το δημόσιο κλειδί της αποθήκευσης HIPAA για ευκολία. Λόγω των χρονικών επισημάνσεων, τα δεδομένα μπορούν να αποθηκευτούν με δεδομένο ότι η σύμβαση μπορεί να υπολογίσει τη διεύθυνση στην οποία υποβλήθηκαν τα στοιχεία η οποία βρίσκεται εντός της εγκατάστασης αποθήκευσης του HIPAA. Τέλος, πρέπει να

αντιμετωπιστεί η κατανομή ιδιωτικών κλειδιών σε οντότητες. Αυτό μπορεί να διευκολυνθεί μέσω οπτικών μέσων σε χρήστες έξυπνων τηλεφώνων, όπως με τη χρήση QR κωδικών ως διευθύνσεις του Ethereum.

4.2.1.3 Επεκτασιμότητα του Patientory

Λόγω της αποκεντρωμένης βάσης δεδομένων, το Blockchain δεν έχει ένα κεντρικό σημείο αποτυχίας και είναι καλύτερο στο να αντέξει κακόβουλες επιθέσεις. Πέρα από αυτό όμως σε ένα δίκτυο φροντίδας είναι απαραίτητο να διασφαλιστεί ότι οι συμμετέχοντες που είναι οι εργαζόμενοι μπορούν να εξαρτώνται ο ένας από τον άλλο για να παρέχουν τις απαραίτητες υπηρεσίες που αναμένονται από αυτούς. Για να επιτευχθεί αυτό, πρέπει να υπάρχει ένα μέσο για να εξασφαλιστεί η λογοδοσία των εργασιών και των υπηρεσιών που αναμένεται να παραδοθούν έγκαιρα, καθώς και η σχετική ευθύνη. Ως εκ τούτου, οποιαδήποτε υποδομή υγείας πρέπει να είναι σε θέση να παρακολουθεί απρόσκοπτα τις απαραίτητες πληροφορίες για να μπορέσει ο πάροχος περίθαλψης να αξιολογήσει το δίκτυο φροντίδας του. Επιπλέον, καθώς μεγαλώνει το δίκτυο φροντίδας και η αλληλεπίδραση μεταξύ των πάροχων, αυξάνεται και η υποδομή υγειονομικής περίθαλψης, η κλιμάκωση της οποίας θα πρέπει να αντιμετωπιστεί με κάποιον τρόπο.

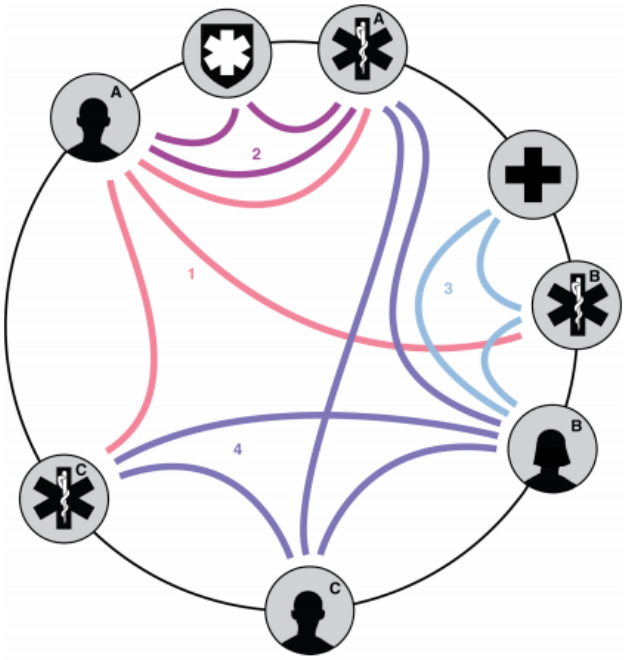
Η βασική πτυχή της οικοδόμησης ενός εξαιρετικά επεκτάσιμου και κατανεμημένου συστήματος διαχείρισης φροντίδας είναι ένα αρχιτεκτονικό πλαίσιο ομότιμης αξιολόγησης. Ένα τέτοιο πλαίσιο έχει ήδη χρησιμοποιηθεί σε διάφορους τομείς της βιομηχανίας, όπως στα μέσα μαζικής ενημέρωσης, στον αθλητισμό και στην αλυσίδα εφοδιασμού. Η εμφάνιση του Blockchain μπορεί εύκολα να είναι ένα πρόσθετο λογισμικό σύνδεσης σε υπάρχοντα κεντρικά πλαίσια.[42] Αυτό οδήγησε στη διερεύνηση του τρόπου χρήσης του Blockchain με στόχο τη δημιουργία ενός πλαισίου ομότιμης συνεργασίας για την υγειονομική περίθαλψη.

Το Blockchain προσφέρει τη διαδικασία επικύρωσης δύο ή περισσοτέρων οντοτήτων που έχουν εμπλακεί σε μια "συναλλαγή" υγειονομικής περίθαλψης. Αυτό παρέχει δύο βασικά χαρακτηριστικά σε σύγκριση με ένα κεντρικό μοντέλο πιστοποίησης. Το πρώτο είναι ότι τα ενδιαφερόμενα μέρη μπορούν να αλληλεπιδρούν μεταξύ τους σε ένα επίπεδο "συναλλαγής" με "σχέση εμπιστοσύνης". Το δεύτερο είναι ότι η ευθύνη σε μια τέτοια σχέση περιορίζεται μόνο στη δέσμευση σε επίπεδο "συναλλαγής". Αυτό είναι πολύ χρήσιμο καθώς περιορίζει την πρόσβαση των πληροφοριών και των υποχρεώσεων μεταξύ των εμπλεκόμενων μερών και ταυτόχρονα επιτρέπει σε ένα συμβαλλόμενο μέρος να έρθει σε μια συναλλακτική σχέση με ένα αριθμό άλλων παρόχων βάσει των ειδικών ικανοτήτων τους και του είδους φροντίδας που πρέπει να παραδοθεί στον ασθενή. Αυτό είναι σημαντικά καλύτερο από ένα συμβατικό συγκεντρωτικό σύστημα που πρέπει να περιορίσει τον αριθμό των παρόχων για ένα ευρύ φάσμα αναγκών των ασθενών λόγω της προσπάθειας που απαιτείται για τη διαχείριση της πρόσβασης και των υποχρεώσεων.

4.2.2 Περιγραφή MedRec

Το MedRec είναι ένα σύστημα που δίνει προτεραιότητα στην εξυπηρέτηση ασθενών, δίνοντας μια διαφανή και προσιτή εικόνα για το ιατρικό ιστορικό. Σε αντίθεση με τα χρηματοπιστωτικά συστήματα που ενδεχομένως να περιέχουν πολλά διαφορετικά αποθετήρια νομίσματος, τα αρχεία υγείας δεν μπορούν να υποκατασταθούν γιατί το καθένα αποτελεί το μοναδικό αποτύπωμα ενός ατόμου. Δεν υπάρχει ομοιότητα με τις συναλλαγές που μπορούμε να κάνουμε με χρήματα. Ενώ ο ανταγωνισμός οδηγεί συχνά σε χαμηλότερο καταναλωτικό κόστος, εδώ ελλοχεύουν εμπόδια στην ανταλλαγή και τον έλεγχο των ιατρικών αρχείων. Για αυτό τον λόγο το MedRec, ως ένα σύστημα κατανεμημένης πρόσβασης και επικύρωσης ιατρικής πληροφορίας χρησιμοποιεί την Blockchain τεχνολογία ούτως ώστε να αντικαταστήσει τους «κεντρικούς» ενδιάμεσους. [43]

Η πρώτη εφαρμογή του MedRec, που σχεδιάστηκε από τον ArielEkblaw και τον AsaphAzaria, δοκιμάστηκε τον Αύγουστο του 2016 στο ιατρικό κέντρο Beth Israel Deaconess. Η εφαρμογή αυτή αποτελεί μια αρχιτεκτονική βάση για το MedRec 2.0, αλλά με σημαντικές αλλαγές. Συγκεκριμένα, το MedRec 2.0 αναπτύσσεται χρησιμοποιώντας Go-ethereum (Geth) και Solidity - σε αντίθεση με τις βιβλιοθήκες Pyethereum και Serpent στις οποίες αναπτύχθηκε το πρωτότυπο. Επιπλέον πραγματοποιήθηκαν αλλαγές στην ποσότητα των πληροφοριών που αποθηκεύονται στο Blockchain, με σκοπό τη βελτίωση τόσο στις ιδιότητες κλιμάκωσης όσο και την ιδιωτικότητα της συναλλαγής.



Εικόνα 14: Αναπαράσταση σχέσεων μεταξύ στοιχείων στο MedRec[70]

Το MedRec 1.0 δεν χτίστηκε στο ζωντανό δίκτυο Ethereum, αντιθέτως δημιουργήθηκε σε ένα ιδιωτικό Blockchain μικρής κλίμακας με συγκεκριμένα APIs. Προκειμένου να διατηρηθεί η ευελιξία αυτής της πλατφόρμας, έγιναν τροποποιήσεις

[70] Σελίδα της εφαρμογής MedRec: https://medrec.media.mit.edu/

στο χρόνο αναμονής πριν από την αποδοχή νέων μπλοκ και το μηχανισμό συναίνεσης για την απόδειξη μίας εργασίας. Δεδομένου ότι η αρχική αλυσίδα είχε ήδη αρκετές διαφορές από την δημόσια αλυσίδα του Ethereum, ο επίσημος client άλλαξε σε σημείο όπου η εφαρμογή MedRec δεν μπορούσε να επιστραφεί στο δημόσιο Blockchain (όπως είχε αρχικά προβλεφθεί) και ο κώδικας έχει ξεπερασθεί. [40]

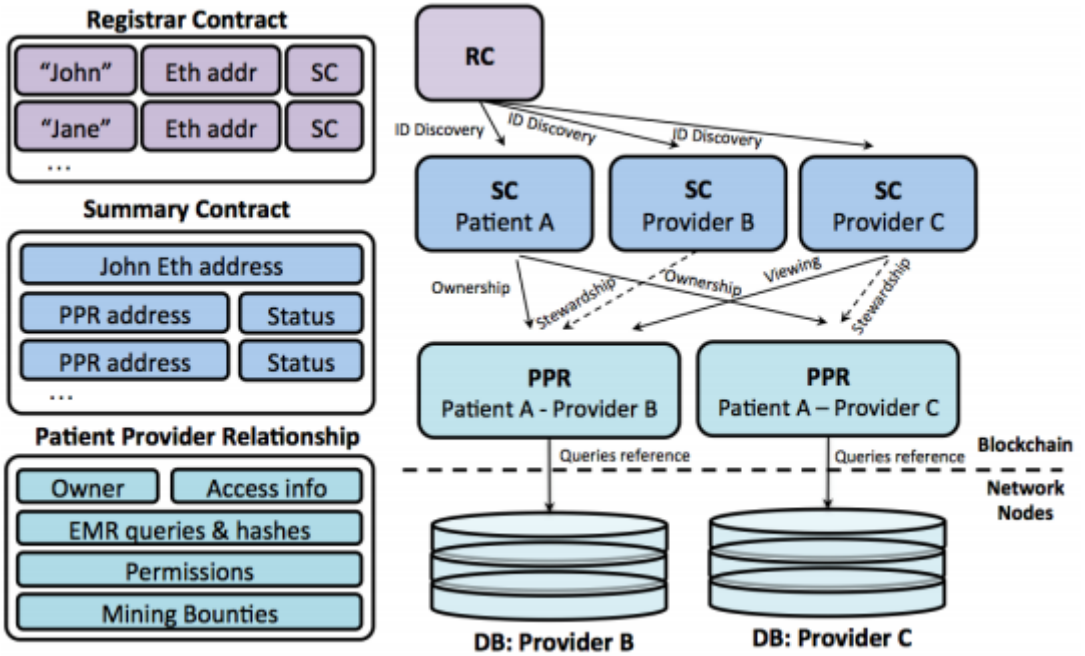
4.2.2.1 Η τεχνολογία που χρησιμοποιεί

Το MedRec αναπτύχθηκε ως μέσο καταγραφής οικονομικών συναλλαγών για ψηφιακά νομίσματα, όπου το Blockchain μπορεί να επεκταθεί γενικότερα ως πλατφόρμα για κατανεμημένους υπολογισμούς. Το Blockchain χρησιμοποιεί κρυπτογράφηση δημόσιου κλειδιού για να δημιουργήσει μια ανθεκτική αλυσίδα, η οποία δεν υποστηρίζεται από κεντρικό εξυπηρετητή, αλλά από ένα αποκεντρωμένο δίκτυο συμμετεχόντων κόμβων. Συμβατικά, κάθε μεμονωμένος κόμβος εργάζεται για την επίλυση μιας σειράς «εργασιών» κατακερματισμού, οι οποίες συμβάλλουν στη διαμόρφωση της αλυσίδας, μια διαδικασία γνωστή ως mining.

Οι έξυπνες συμβάσεις λειτουργούν ως σχέσεις που συνδέουν τους ασθενείς και τους παρόχους με τις διευθύνσεις των υπαρχόντων ιατρικών αρχείων. Το MedRec δεν αποθηκεύει απευθείας την εγγραφή. Συγκεκριμένα κωδικοποιεί τα μεταδεδομένα που επιτρέπουν την ασφαλή πρόσβαση των αρχείων από τους ασθενείς, παρέχοντας την πρόσβαση σε δεδομένα σε διαφορετικούς παρόχους. Τα μεταδομένα περιέχουν πληροφορίες σχετικά με την ιδιοκτησία, την άδεια και την ακεραιότητα των δεδομένων που ζητούνται.

4.2.2.2 Δομή των Smart Contracts

Το Medrec δεν αποθηκεύει ιατρικούς φακέλους απευθείας στο μπλοκ Ethereum, αλλά χρησιμοποιεί ένα σχεσιακό σύνολο έξυπνων συμβολαίων για να κωδικοποιεί δείκτες, οι οποίοι μπορούν να χρησιμοποιηθούν για τον εντοπισμό και τον έλεγχο ταυτότητας των ιατρικών φακέλων.



Εικόνα 15: Τα έξυπνα συμβόλαια MedRec στα αριστερά δείχνουν δεδομένα που περιέχονται σε κάθε συμβόλαιο. Παράδειγμα σχέσεων μεταξύ συμβολαίων και κόμβων δικτύου στα δεξιά [43]

Ένα διάγραμμα που δείχνει τις πιθανές σχέσεις μεταξύ διαφορετικών συμβάσεων ασθενούς και παρόχων παρουσιάζεται παρακάτω. Σημειώνεται ότι η κατάσταση ενός συγκεκριμένου συμβολαίου μπορεί να έχει διαφορετικές τιμές ανάλογα με τα δικαιώματα που παρέχει (π.χ. η σχέση για τον Patient A - Provider B κωδικοποιεί τα δικαιώματα ώστε να μπορεί ο Πάροχος Β να τα δει, αλλά η σχέση Patient A - Provider C δεν κωδικοποιεί τα ίδια δικαιώματα για τον πάροχο Β). Τέλος, οι συμβάσεις χρησιμοποιούνται μόνο για την παροχή δικαιωμάτων πρόσβασης, καθώς τα queries που επιστρέφουν τα ίδια τα αρχεία διαχειρίζονται εκτός αλυσίδας. [43]

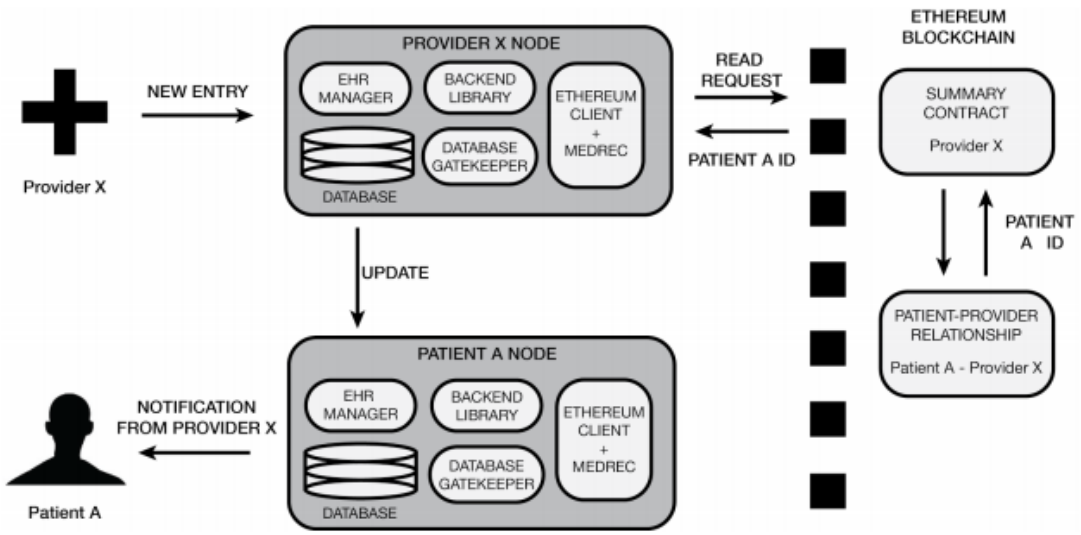
4.2.2.3 Διαχείριση Δεδομένων

Όταν ένας ασθενής ζητήσει πρόσβαση σε ένα συγκεκριμένο ιατρικό αρχείο, στέλνει αίτημα στην βάση του παρόχου, η οποία αποτελεί μέρος της εκτός δικτύου υποδομής του MedRec. Ο πάροχος υλοποιεί μια διεπαφή πρόσβασης στην τοπική βάση δεδομένων του κόμβου του ασθενούς, που διέπεται από δικαιώματα αποθηκευμένα στο Blockchain. Ο πάροχος λειτουργεί μέσω ενός διακομιστή που ακούει query requests από clients στο δίκτυο, τα οποία υπογράφονται κρυπτογραφικά από τον χρήστη. Η κρυπτογραφική υπογραφή επιτρέπει την επιβεβαίωση ταυτότητας και στη συνέχεια τον έλεγχο των συμβάσεων Blockchain για να επαληθεύει εάν η διεύθυνση που εκδίδει το αίτημα έχει πρόσβαση στο query. Εάν η διεύθυνση είναι έγκυρη, εκτελεί το query στην τοπική βάση δεδομένων του κόμβου και επιστρέφει το αποτέλεσμα στον πελάτη. Το MedRec ορίζει επίσης ένα πρωτόκολλο διαλειτουργικότητας, το οποίο μπορεί να διασυνδέεται με οποιαδήποτε εφαρμογή backend ή UI υλοποίησης. Οι κόμβοι των ασθενών περιέχουν επίσης μια πιο ελαφριά τοπική βάση δεδομένων η οποία λειτουργεί ως κρυφή μνήμη των δεδομένων του

ασθενούς. Η εφαρμογή κόμβου δηλαδή του ασθενούς είναι ένας «ελαφρύς» κόμβος, ο οποίος θα μπορούσε να εκτελεστεί σε υπολογιστή ή κινητό τηλέφωνο.[71]

4.2.2.4 Επεκτασιμότητα του MedRec

Η επεκτασιμότητα είναι μια συνεχιζόμενη ανησυχία στην κοινότητα του Ethereum και δεν έχει ακόμη επιλυθεί πλήρως. Ένα από τα βασικά ζητήματα είναι ότι κάθε event που θα αποθηκευτεί ανά πάσα στιγμή στο Blockchain θα εμφανιστεί και στα επόμενα μπλοκ. Το Ethereum παρέχει τη δυνατότητα τόσο για αποθήκευση δεδομένων όσο και για πιο περίπλοκες λειτουργίες. Ένα πλεονέκτημα ενός ιδιωτικού Blockchain είναι ότι η εφαρμογή χρειάζεται μόνο να εντοπίσει τη γένεση της ιδιωτικής αλυσίδας, όχι το Ethereum στο σύνολό της. Μια βασική αρχιτεκτονική τροποποίηση μεταξύ του MedRec 1.0 και του 2.0 είναι η παράκαμψη του Blockchain για τις ειδοποιήσεις ασθενών. Αυτό εμποδίζει ένα event που πρέπει να καταγράφεται στο Blockchain κάθε φορά που μια ιατρική εγγραφή υποβάλλεται σε αλλαγή της κατάστασης (γεγονός το οποίο μπορεί να συμβεί αρκετές φορές την ημέρα για έναν ασθενή υπό συνεχή ιατρική φροντίδα) και περιορίζει την αποθήκευση στο Blockchain στη δημιουργία και τροποποίηση ταυτότητας και σχέσεων, αντί των μεταδεδομένων που τις περιβάλλουν. Εξετάζοντας το Blockchain, ένας εξωτερικός παρατηρητής μπορεί να δει μια σχέση μεταξύ του ασθενή και του παρόχου, αλλά δεν θα είναι σε θέση να προσδιορίσει τη συχνότητα με την οποία επικοινωνούν, όπως και το περιεχόμενο της συναλλαγής. Η εναλλακτική προσέγγιση (που αλλάζει μεταξύ MedRec 1.0 και 2.0) περιγράφεται λεπτομερώς στο παρακάτω διάγραμμα:



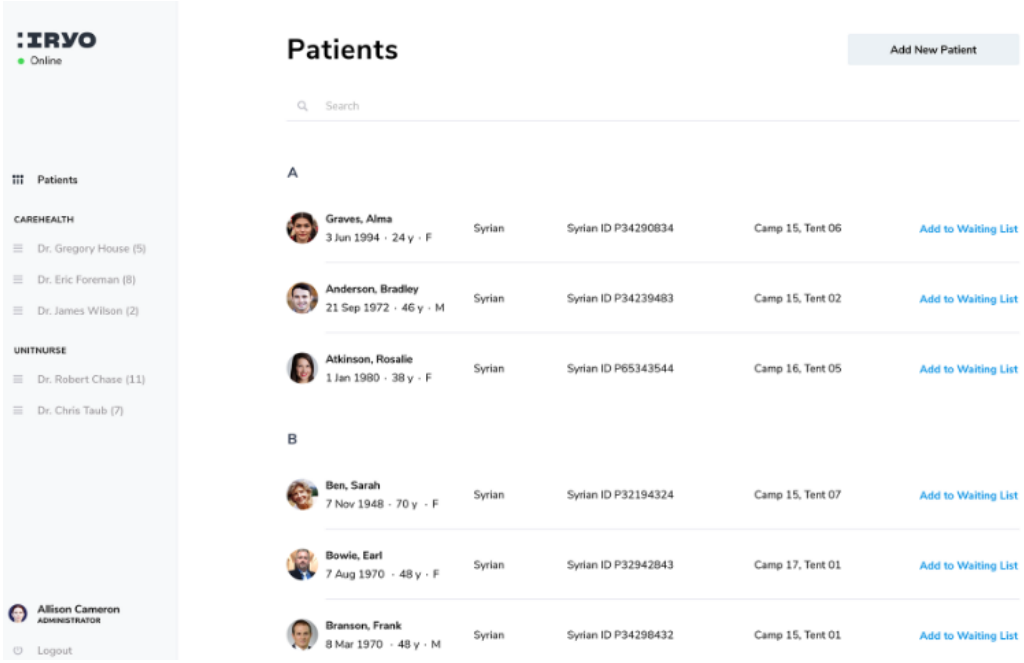
Εικόνα 16: Εισαγωγή στοιχείων μιας νέας εγγραφής ενός καινούριου ασθενή

[71] MedRec' s technical Documentation: https://medrec.media.mit.edu/technical/

4.2.3 Περιγραφή Iryo

Το Iryo[72] είναι μια πλατφόρμα αποθήκευσης ιατρικών πληροφοριών, και διαθέτει μια ανώνυμη διεπαφή για queries. Χρησιμοποιεί την τεχνολογία Blockchain, για τη διαχείριση των αδειών πρόσβασης στα αρχεία των ασθενών και tokens για να πάρει τη συγκατάθεση των τελικών χρηστών.

Η πιλοτικό εφαρμογή αποτελείται από ένα σύγχρονο ηλεκτρονικό σύστημα, το οποίο διαχειρίζεται την κατάσταση υγείας ενός ασθενή και πρόκειται να αναπτυχθεί περαιτέρω στο μέλλον. Μάλιστα το Iryo θα εφαρμοστεί σε σημεία φιλοξενίας προσφύγων για την αποτελεσματική και ασφαλή αποθήκευση και ανταλλαγή ιατρικών δεδομένων μεταξύ ασθενών και παρόχων υγειονομικής περίθαλψης.

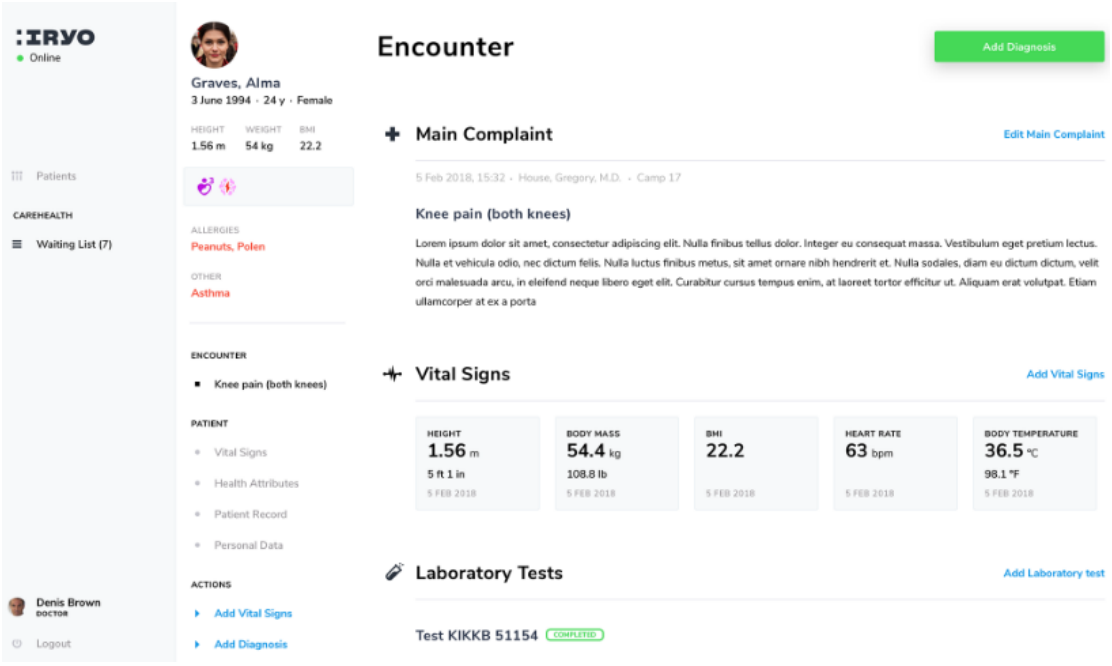


Εικόνα 17: Διεπαφή με καταχωρήσεις κλινικής που παρουσιάζουν τους εγγεγραμμένους ασθενείς[73]

Οι ιατρικές κλινικές στα σημεία φιλοξενίας θα έχουν τη δυνατότητα δημιουργίας τυποποιημένων ιατρικών αρχείων για τους ασθενείς με τη χρήση του openEHR[74], το οποίο επιτρέπει την ομαλή ανταλλαγή δεδομένων με την αύξηση της ιατρικής διαλειτουργικότητας στα νοσοκομεία. Επιπλέον, όταν ένα άτομο ή μια οικογένεια μετακομίζει σε ένα σημείο, θα έχουν τη δυνατότητα να πάρουν μαζί τους τα ιατρικά τους ιστορικά, τα οποία θα βελτιώσουν αυτόματα το επίπεδο φροντίδας που μπορούν να λάβουν στο μέλλον.

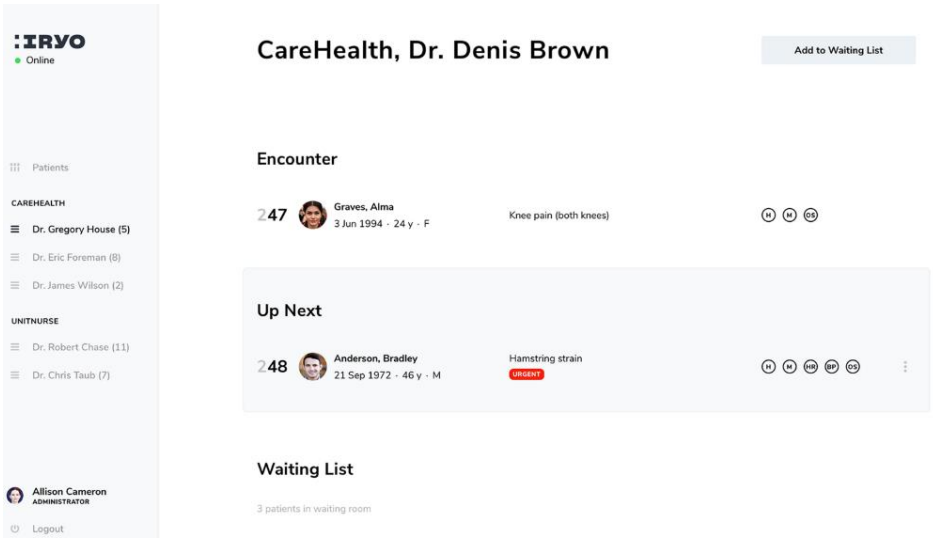
[72] Σελίδα της εφαρμογής Iryo: https://iryo.io/#intro
[73] Πως θα φαίνεται η πλατφόρμα Iryo:https://medium.com/iryo-network/iryo-network-product-update-ea43c289f9c8
[74] Τι είναι το openEHR: https://www.openehr.org/about/what_is_openehr

Η διαλειτουργικότητα βελτιώνει το συνολικό επίπεδο και την αποτελεσματικότητα της παρεχόμενης θεραπείας. Ένα πρόσθετο πλεονέκτημα του openEHR είναι ότι παρέχει στους ασθενείς τη δυνατότητα να μεταπηδούν από έναν πάροχο υγειονομικής περίθαλψης σε άλλο χωρίς να χρειάζεται να ξεκινήσει το ιατρικό ιστορικό τους από το μηδέν. [44]



Εικόνα 18: Διεπαφή γιατρού-ασθενή στην πλατφόρμα Iryo [44]

Μια από τις πιο κρίσιμες πτυχές της δημιουργίας μιας πλατφόρμας που χειρίζεται ιατρικά δεδομένα είναι η ασφάλεια και η ιδιωτικότητα. Τα προσωπικά και ευαίσθητα ιατρικά δεδομένα που αποθηκεύονται στο δίκτυο του Iryo και στην προσωπική εφαρμογή για κινητά Iryo είναι κρυπτογραφημένα μέσω ιδιωτικού κλειδιού που βρίσκεται στη διάθεση του ασθενή.



Εικόνα 19: Διεπαφή γατρού στην πλατφόρμα Iryo [44]

4.2.3.1 OpenEHR και Zero-knowledge storage

Δεδομένου ότι η επαναχρησιμοποίηση των δεδομένων και η διαλειτουργικότητα μεταξύ διαφόρων παρόχων είναι συχνά υπερβολικά δαπανηρές ή και αδύνατες, το Iryo προσπάθησε να καταστήσει τα δεδομένα ανοικτά και όσο το δυνατόν πιο ουσιαστικά. Για αυτόν τον λόγο χρησιμοποιήθηκε το openEHR για τη μοντελοποίηση και ανταλλαγή δεδομένων. Στον πυρήνα του openEHR υπάρχουν μοντέλα, τα οποία συνδέουν τιμές με την πραγματική σημασία τους (π.χ. πίεση του αίματος).

Τα μοντέλα αυτά μπορούν στη συνέχεια να συνδεθούν με πιο σύνθετες δομές για να υποστηρίξουν διάφορους τύπους διαδικασιών που απαιτούνται από τις κλινικές και χρησιμοποιούνται στην AQL (Archetype Querying Language) του openEHR, απ' όπου μπορούν να επαναχρησιμοποιηθούν για την κατασκευή και την εκτέλεση εκτεταμένων queries σε όλα τα δεδομένα. Το openEHR έχει ήδη επιλεγεί ως πρότυπο σε εθνικά προγράμματα ανταλλαγής δεδομένων σε ορισμένες χώρες της Ευρωπαϊκής Ένωσης. [45] Αυτό σημαίνει ότι πρόκειται για μία ενδεδειγμένη λύση προς υιοθέτηση για την αύξηση της διαλειτουργικότητας στον τομέα της υγείας.

Όπως αναφέρθηκε και παραπάνω το Iryo είναι ένας παγκόσμιος χώρος αποθήκευσης δεδομένων openEHR. Επειδή λίγοι άνθρωποι είναι διατεθειμένοι να παράσχουν τα ιατρικά τους δεδομένα στο "GoogleEHR" λόγω της αξιοποίησης των ιατρικών τους δεδομένων για εμπορικούς σκοπούς, το Iryo αποφάσισε να εγκαταλείψει την πρόσβαση σε απλά δεδομένα. Αντιλαμβάνεται τα ιατρικά δεδομένα που κατέχει ως «τοξικά στοιχεία», διότι θεωρεί οτι η κατοχή πάρα πολλών δεδομένων σε ένα μέρος παρουσιάζει υπερβολικά μεγάλο κίνδυνο.

Η λύση για τη διαχείριση αυτού του κινδύνου είναι το λεγόμενο zero-knowledge storage**,** το οποίο είναι ανθεκτικό σε όλες τις επιθέσεις, καθώς λειτουργεί μέσω των χρηστών που κρυπτογραφούν τα δεδομένα τους στις κινητές συσκευές τους με δημόσιο κλειδί. Ένα ιδιωτικό κλειδί αποκρυπτογράφησης παραμένει στη συσκευή του ασθενούς. Κάθε φορά που κάποιος επιθυμεί να έχει πρόσβαση στα δεδομένα ασθενών (για παράδειγμα ένας γιατρός ή ένας ερευνητής), ο ασθενής πρέπει να εγκρίνει την πρόσβασή του. Αυτό θα γίνει από τον ασθενή κάνοντας κλικ στο "yes" στην εφαρμογή IryoEHR, δίνοντας έτσι ένα κλειδί επανα-κρυπτογράφησης στο δημόσιο κλειδί του γιατρού.

Επίσης μέσως της αποθήκευσης του συνόλου των ιατρικών δεδομένων στις συσκευές των ασθενών υποστηρίζεται η αμετάβλητη λειτουργία της πλατφόρμας, με αποτέλεσμα εάν αλλάξει κάτι, να το γνωρίζει ο αντίστοιχος χρήστης. Όλοι οι κόμβοι αποθήκευσης παρέχουν κρυπτογραφικές αποδείξεις στους ασθενείς, γράφοντας hashes στο EOS Blockchain[75]. Με αυτόν τον τρόπο, αν αποτύχει η επαλήθευση του ελέγχου, ο συμβιβασμένος κόμβος αποθήκευσης μπορεί εύκολα να αναγνωριστεί και να αντικατασταθεί. Για να μειωθεί ο αριθμός των hashes, χρησιμοποιείται

[75] Περιγραφή του EOS Blockchain: https://blockgeeks.com/guides/eos-blockchain/

συνάθροιση σε ένα δέντρο Merkle. Οι ασθενείς λαμβάνουν μια απόδειξη από το Blockchain, την οποία μπορούν να χρησιμοποιήσουν για επαλήθευση.

4.2.3.2 Έλεγχοι άδειας του Blockchain

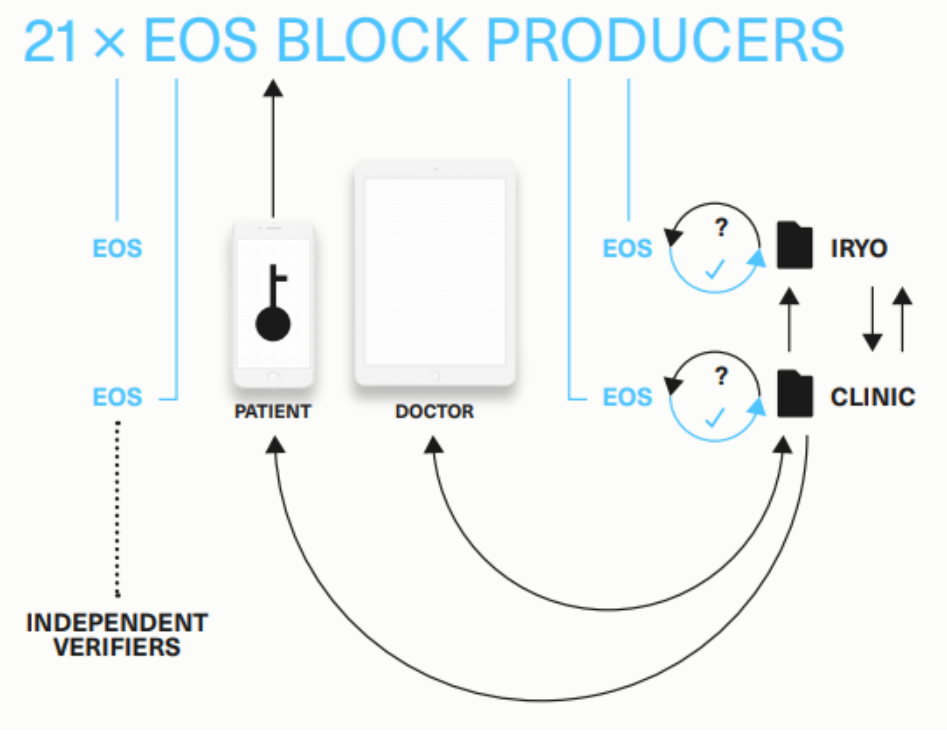
Οι τελικοί χρήστες (ασθενείς) μπορούν να μοιράζονται όλα τα ηλεκτρονικά αρχεία υγείας με τον προσωπικό γιατρό τους (με ή χωρίς χρονικά όρια), την ανάκληση της πρόσβασης στον EHR τους και την ανταλλαγή συγκεκριμένων πληροφοριών των ιατρικών αρχείων τους με ειδικούς (με χρονικό περιορισμό). Επιπλέον, οι ασθενείς θα μπορούν να εκδίδουν δικαιώματα εγγραφής αλλά όχι ανάγνωσης σε συσκευές IoT.

Η χρήση των έξυπνων συμβολαίων επιτρέπει στο Iryo να μπορεί να υπολογίσει την κατάσταση του κόμβου Blockchain τη στιγμή που έλαβε κάποια πληροφορία.

Τα πλεονεκτήματα διαχείρισης των αδειών στο Iryo μέσω Blockchain παρουσιάζονται παρακάτω.

• Σταθερή χρονική σήμανση. Όλοι οι πλήρεις κόμβοι του Iryo, συμπεριλαμβανομένων των συναινετικών κόμβων που παράγουν μπλοκ, θα επικυρώνουν όλα τα μηνύματα.

• Μετατρέψιμο αρχείο καταγραφής όλων των μηνυμάτων. Δεν υπάρχει η «δυνατότητα» άρνησης σε έγκυρη αίτηση πρόσβασης. Αυτό θα μειώσει την πιθανότητα δικαστικών αντιδικιών όταν κάποιοι ασθενείς ισχυρίζονται ότι δεν έχουν εκδοθεί δικαιώματα πρόσβασης.



Εικόνα 20: Απλή επισκόπηση του Iryo

4.2.4 Περιγραφή Bowhead

Το Bowhead είναι μία εφαρμογή, η οποία επί της ουσίας στηρίζεται σε μία ιατρική συσκευή μετρήσεων που συνδέεται με το διαδίκτυο και μπορεί να παρακολουθεί την υγεία των ατόμων στο σπίτι ενώ μπορεί επίσης να χρησιμοποιηθεί ως απομακρισμένος πόρος για τους επαγγελματίες του τομέα της υγείας για την έγκαιρη παροχή συμβουλών σε άτομα που χρειάζονται ιατρική φροντίδα και καθοδήγηση. Η συσκευή Bowhead μπορεί να διανείμει εξατομικευμένες επιλογές και δοσολογίες συμπληρωμάτων διατροφής και φαρμάκων με βάση τις μοναδικές ανάγκες του ατόμου.

Στο μέλλον, η εφαρμογή θα μπορεί να λαμβάνει δεδομένα από άλλους βιομετρικούς αισθητήρες που χρησιμοποιούνται από τους χρήστες, όπως φορητές συσκευές, εφαρμογές υγείας σε κινητά τηλέφωνα, συσκευές παρακολούθησης του καρδιακού ρυθμού, μέτρησης της πίεσης, βηματομετρητές και άλλες έξυπνες συσκευές που θα μπορούσαν να βοηθήσουν τους επαγγελματίες υγείας του Bowhead να παρακολουθούν τα στάδια του ιστορικού υγείας του ασθενούς και να παρέχουν συστάσεις.

Μέσω της τεχνολογίας Blockchain, οι χρήστες θα έχουν ασφαλή πρόσβαση στις δικές τους προσωπικές πληροφορίες υγείας ενώ θα επωφελούνται από μια συνεχώς αυξανόμενη βάση δεδομένων με ανώνυμα συλλογικά δεδομένα υγείας ασθενών επιμελημένα για την παροχή λύσεων ευεξίας και μακροζωίας. [46]

4.2.4.1 Τρόπος λειτουργίας

1. Ο χρήστης παρέχει δείγμα αίματος (παρόμοιο με τη δοκιμή γλυκόζης) ή δείγμα σάλιου που τοποθετείται στο δοχείο δοκιμής.

2. Ο χρήστης ακολουθεί τις οδηγίες και εισάγει το δοχείο δοκιμής στο πλάι της συσκευής για ανάγνωση.

3. Η συσκευή Bowhead χρησιμοποιεί την μηχανική όραση και έναν αλγόριθμο για τον προσδιορισμό της έντασης του σήματος και των αποτελεσμάτων των δοκιμών, και κατόπιν ερμηνεύει τα αποτελέσματα για αυτόν τον χρήστη.

4. Με βάση το αποτέλεσμα της δοκιμής και τα ποιοτικά δεδομένα που παρέχει ο χρήστης, ένας εξουσιοδοτημένος επαγγελματίας υγείας προσφέρει συμβουλές ώστε να ξεκινήσει η διανομή των σχετικών προϊόντων.

5. Όλα τα σήματα παρακολουθούνται με ασφάλεια και αποθηκεύονται χρησιμοποιώντας την τεχνολογία Blockchain.

4.2.4.2 Blockchain βάση δεδομένων

Η διαλειτουργικότητα των ιατρικών δεδομένων μεταξύ διαφορετικών ιδρυμάτων έχει ακολουθήσει τρία μοντέλα: Push, Pull και View. Η τεχνολογία Blockchain προσφέρει ένα τέταρτο μοντέλο, το οποίο έχει τη δυνατότητα να καταστήσει δυνατή την ασφαλή ανταλλαγή ιατρικών αρχείων καθ 'όλη τη διάρκεια ζωής των παρόχων.

Το Push είναι η διαδικασία κατά την οποία ένα ωφέλιμο φορτίο ιατρικών πληροφοριών αποστέλλεται από έναν πάροχο σε έναν άλλο. Παρόλο που στο παρελθόν αυτο εφαρμόστηκε στους παρόχους υγειονομικής περίθαλψης, προϋποθέτει ότι υπάρχει η κατάλληλη υποδομή για την λειτουργία του, όπως η ύπαρξη ενός ηλεκτρονικού καταλόγου παρόχων και ενός συνόλου νομικών συμφωνιών που επιτρέπουν την ευρεία ανταλλαγή δεδομένων. Το Push είναι μια μετάδοση μεταξύ δύο μερών και κανένα άλλο μέρος δεν έχει πρόσβαση στη συναλλαγή. Αν ένας ασθενής μεταφερθεί σε άλλο νοσοκομείο, το νέο νοσοκομείο ενδέχεται να μην έχει πρόσβαση στα δεδομένα σχετικά με τη φροντίδα του στο πρώτο. Επίσης, δεν υπάρχει εγγύηση για την ακεραιότητα των δεδομένων από το σημείο δημιουργίας μέχρι το σημείο χρήσης τους.

Το Pull είναι η διαδικασία όπου ένας πάροχος μπορεί να ζητήσει πληροφορίες από έναν άλλο. Για παράδειγμα, ένας καρδιολόγος θα μπορούσε να ζητήσει πληροφορίες από τον γιατρό πρωτοβάθμιας φροντίδας. Όπως και με το Push, κάθε συγκατάθεση και άδεια είναι άτυπη και γίνεται χωρίς κάποιο τυποποιημένο είδος ελέγχου.

Το View είναι η διαδικασία κατά την οποία ένας πάροχος μπορεί να δει τα δεδομένα μέσα στο αρχείο κάποιου άλλου παρόχου. Για παράδειγμα, ένας χειρουργός ενός νοσοκομείου θα μπορούσε να δει μια ακτινογραφία που είχε πραγματοποιηθεί στον ασθενή σε ένα επείγον κέντρο φροντίδας. Η συγκατάθεση και πάλι είναι άτυπη και δεν υπάρχει κάποιος τυποποιημένος έλεγχος.

Όλες αυτές οι προσεγγίσεις λειτουργούν τεχνολογικά, αλλά οι πολιτικές που τις περιβάλλουν υπόκεινται σε θεσμική διαφοροποίηση και στους εκάστοτε κρατικούς νόμους. Το Blockchain είναι ένα διαφορετικό κατασκεύασμα, παρέχοντας ένα καθολικό σύνολο εργαλείων για κρυπτογραφική διασφάλιση της ακεραιότητας των δεδομένων, τυποποιημένο έλεγχο και επίσημες "συμβάσεις" για πρόσβαση σε δεδομένα. Το Bowhead θα χρησιμοποιήσει ένα παρόμοιο μοντέλο με την καινοτομία που ονομάζεται Anonymized Healthcare Token, η οποία χρησιμοποιεί smart contracts για την παραγωγή της παρακάτω εκτελέσιμης ροής:

1. Τα ερευνητικά ιδρύματα ή οι φαρμακευτικές εταιρείες θα συνάψουν υπηρεσίες Bowhead και θα μπορούν να δημιουργήσουν προφίλ κλινικών χαρακτηριστικών που αναζητούν στην έρευνά τους, προσφέροντας μια συγκεκριμένη μίσθωση.

2. Το αποκεντρωμένο σύστημα θα έχει διαλείπουσα λειτουργία όπου τα ανώνυμα αρχεία ασθενών θα καταγράφονται ή θα παρακολουθούνται και θα συγκρίνονται με τα ερευνητικά χαρακτηριστικά του ιδρύματος.

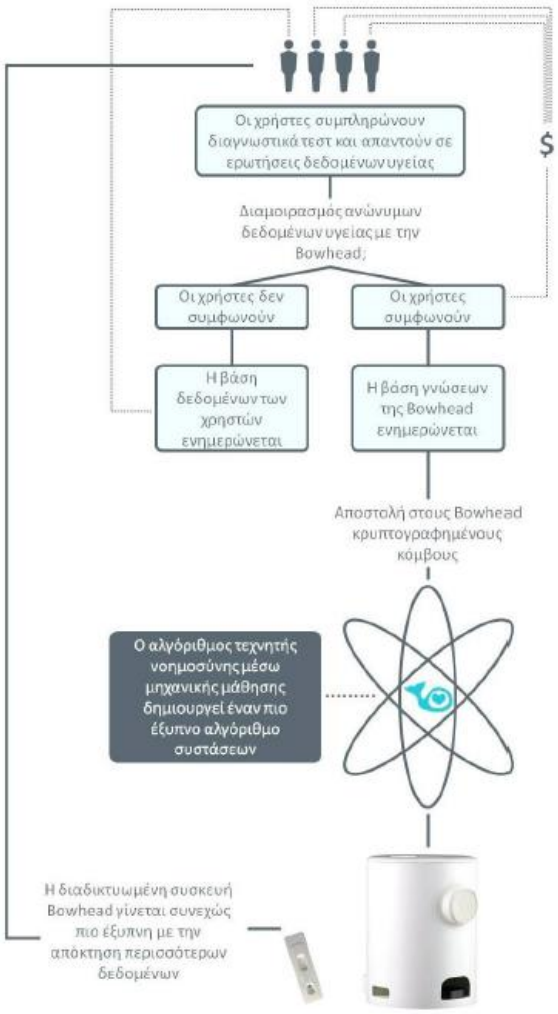
3. Οι ασθενείς θα έχουν την επιλογή να συμμετάσχουν στην κλινική μελέτη κατόπιν συγκατάθεσης.

4. Οι ασθενείς και μια ανεξάρτητη επιτροπή δεοντολογίας θα έχουν τη δυνατότητα επανεξέτασης της προσφοράς μίσθωσης για δεδομένα ανώνυμων ασθενών και τυχόν πρόσθετα χαρακτηριστικά.

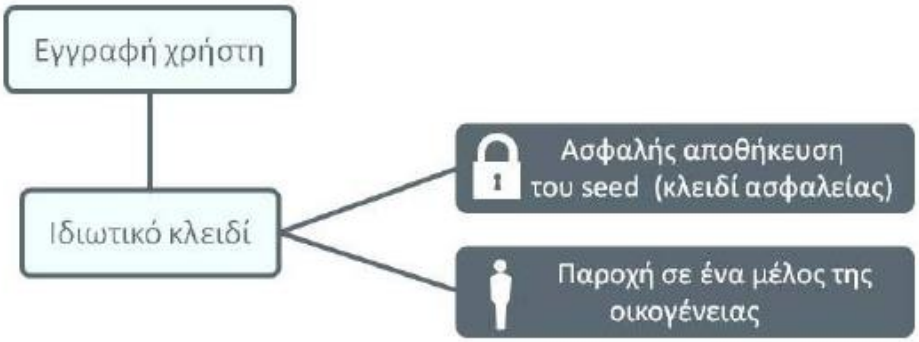
5. Εάν ο ασθενής δώσει τη συγκατάθεσή του να συμμετάσχει σε μια μελέτη, θα έχει τον πλήρη έλεγχο του τι μισθώνεται χρησιμοποιώντας μια έξυπνη σύμβαση. Οι ασθενείς έχουν τη δυνατότητα να διατηρούν προσωπικά δεδομένα, όπως το πλήρες όνομα, τη διεύθυνση ή τα προσωπικά στοιχεία αναγνώρισης τους, ασφαλή και ιδιωτικά.

6. Οι ασθενείς θα έχουν πρόσβαση στο δίκτυο Bowhead των επαγγελματιών υγείας για διαβουλεύσεις και θα μπορούν να ελέγχουν ποιος έχει πρόσβαση και σε ποιες προσωπικές / ιατρικές πληροφορίες.

Από τα παραπάνω γίνεται εύκολα αντιλυπτό οτι οι χρήστες έχουν τον πλήρη έλεγχο των δεδομένων της υγείας τους. Οι ίδιοι καθορίζουν το εάν, πότε, πού και πώς θα μοιράζονται τα δεδομένα τους. Οποιαδήποτε δικαιώματα πρόσβασης ή μελέτης που έχει διαμορφώσει ο χρήστης θα μπορούν επίσης να ανακληθούν από αυτόν ανά πάσα στιγμή. [46]



Εικόνα 21: Τρόπος λειτουργίας του Bowhead[76]

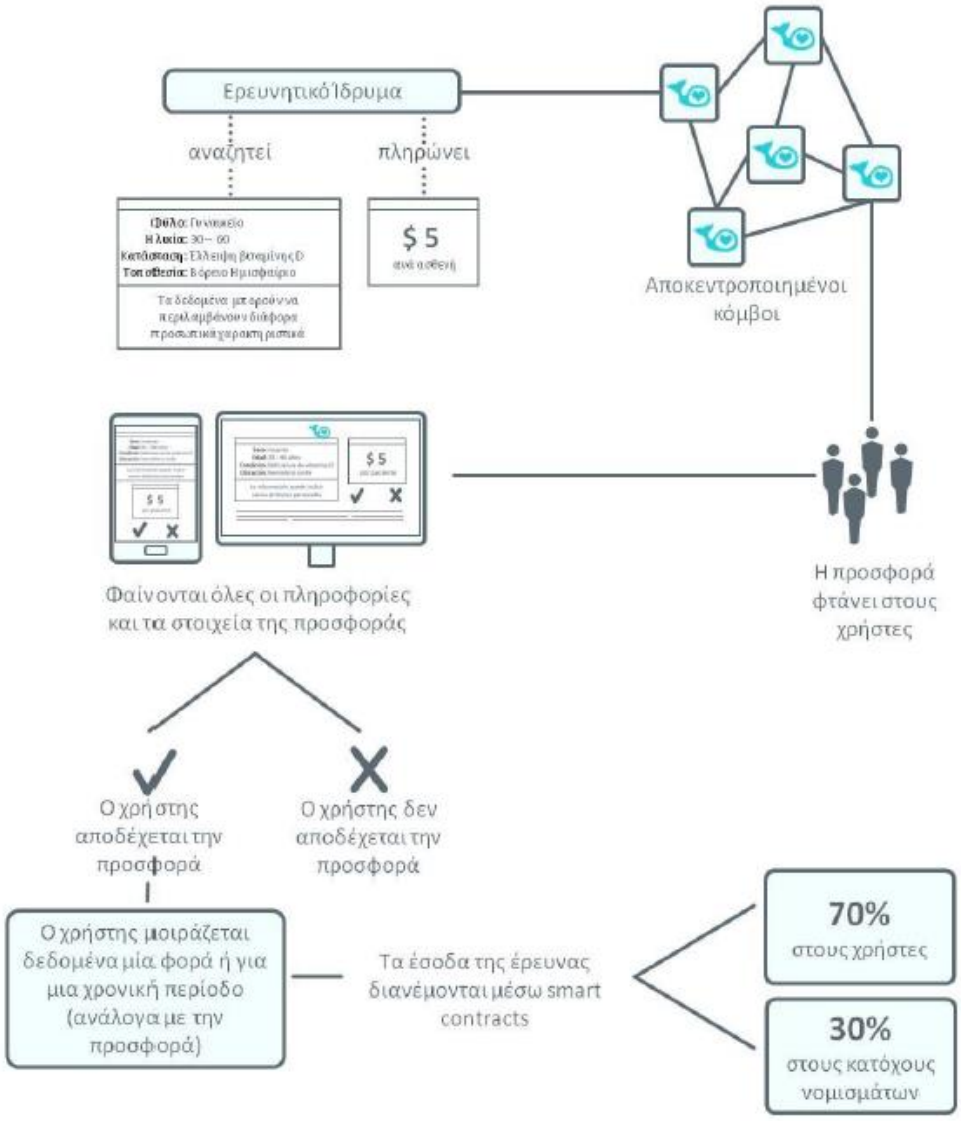


Εικόνα 22: Τρόπος παραχώρησης δικαιώματος πρόσβασης

[76] Bowhead Whitepapaer: https://icofever.net/files/455.pdf

4.2.4.3 Σύστημα ανταμοιβής

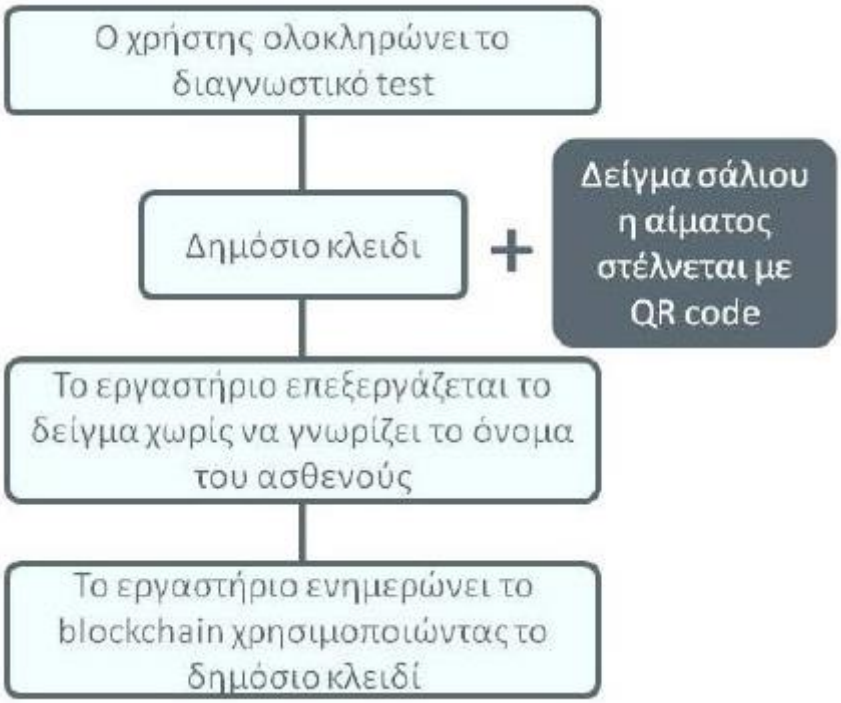
Ένα σύστημα ανταμοιβής εξαλείφει την ανάγκη για ενδιάμεσες εταιρείες ενώ παράλληλα με αυτόν τον τρόπο επιβραβεύονται οι χρήστες με ανώνυμο τρόπο. Ακολουθεί ένα παράδειγμα του τρόπου με τον οποίο οι ασθενείς μπορούν να ανταμείβονται, μοιράζοντας τα δεδομένα υγείας τους και κρατώντας την ανωνυμία τους. [46]



Εικόνα 23: Τρόπος ανταμοιβής

Για παράδειγμα, ένας νέος ασθενής που ολοκληρώνει μια έρευνα με επίκεντρο την υγεία ή ολοκληρώνει μια διαγνωστική εξέταση μπορεί να έχει τη δυνατότητα να λάβει νομίσματα Bowhead. Επίσης, εάν ένα ερευνητικό ίδρυμα ή φαρμακευτική εταιρεία επιθυμεί να αγοράσει δεδομένα, οι συμμετέχοντες και οι δικαιούχοι των νομισμάτων θα μπορέσουν να ωφεληθούν σε μεγάλο βαθμό. Για παράδειγμα, το 70% των κεφαλαίων που καταβάλλει το ερευνητικό ίδρυμα για ένα συγκεκριμένο σύνολο

δεδομένων θα μπορούσε να μεταφερθεί στους ασθενείς που παρείχαν τα δεδομένα τους και το υπόλοιπο 30% των κεφαλαίων θα μπορούσε να μεταβεί στο ερευνητικό προσωπικό που διέθεσε Bowhead νομίσματα στους κατόχους των δεδομένων. [46]



Εικόνα 24: Τρόπος επίτευξη ανωνυμίας

4.2.5 Περιγραφή doc.ai

Το doc.ai είναι μία πλατφόρμα που βασίζεται στην ανάλυση της ιατρικής πληροφορίας μέσω της τεχνητής νοημοσύνης και σχεδιάστηκε για να καλύψει τις ανάγκες διαφόρων ιατρικών πεδίων. Στοχεύει στη δημιουργία ενός αποκεντρωμένου δικτύου τεχνητής νοημοσύνης που ονομάζεται Neuron για να βοηθήσει στην ανάπτυξη ενός καλύτερου μοντέλου υπηρεσιών υγειονομικής περίθαλψης βασισμένο σε προγνώσεις που προκύπτουν από αναλύσεις τεχνητής νοημοσύνης και ενθάρυνση της ένταξης μεγαλύτερου αριθμού ασθενών. Το doc.ai επικεντρώνεται στο Bio-Omics, επιτρέποντας στα άτομα να φορτώσουν τα δικά τους ιατρικά δεδομένα που επιτρέπουν στους αλγόριθμους μηχανικής μάθησης να επιτύχουν ακριβέστερη μοντελοποίηση σύνθετων ασθενειών. Το οικοσύστημα doc.ai συνδέει τέσσερις τύπους συμμετεχόντων, ιδιοκτήτες δεδομένων, χορηγούς έρευνας, ερευνητές και προγραμματιστές με σημαντικές ερευνητικές μελέτες. [47]

4.2.5.1 Neuron

Το Neuron είναι ένα Blockchain, υλοποιημένο μέσω της εφαρμογής Ethereum, που εφαρμόζει το παράδειγμα της αποκεντρωμένης τεχνητής νοημοσύνης. Η

αποκεντρωμένη τεχνητή νοημοσύνη έχει τα οφέλη της προστασίας του απόρρητου των δεδομένων και τη δημιουργία κλίματος συνεργασίας. Το απόρρητο δεδομένων διασφαλίζεται μέσω της επικοινωνίας των μοντέλων μηχανικής μάθησης και της διατήρησης δεδομένων στη συσκευή του τελικού χρήστη. Επιπλέον, μόλις τα μοντέλα ωριμάσουν, είναι προσβάσιμα σε όλους τους κόμβους του δικτύου. Οι ομάδες που συμμετέχουν στη φάση μάθησης NeuRoN είναι οι παρακάτω:

1. Ερευνητικοί οργανισμοί - Μέρη που ενδιαφέρονται να χρησιμοποιήσουν το NeuRoN για να εκπαιδεύσουν τα μοντέλα τους.

2. Χρήστες - Συμμετέχοντες που ενδιαφέρονται να συνδέσουν τις συσκευές και τα δεδομένα τους στο δίκτυο.

3. Μοντέλα νευρωνικών δικτύων - μοντέλα που εκπαιδεύονται με τα δεδομένα του χρήστη.

Οι τρεις αυτές ομάδες αλληλεπιδρούν για να εκπαιδεύσουν τα μοντέλα νευρωνικών δικτύων που αποτελούν τη βάση της τεχνητής νοημοσύνης. Οι φάσεις στις οποίες συλλογικώς υποβάλλονται συνιστούν τη μάθηση. Οι φάσεις που εμπλέκονται στη μάθηση είναι η πρόταση, η εκπαίδευση, ο συγχρονισμός και η πληρωμή.

4.2.5.2 Μάθηση

Η μάθηση αποτελείται από ένα μοντέλο που μεταδίδεται ώστε να μάθει από τα δεδομένα. Ένας κύκλος εκμάθησης έχει τις παρακάτω φάσεις:

1. Πρόταση

2. Εκπαίδευση

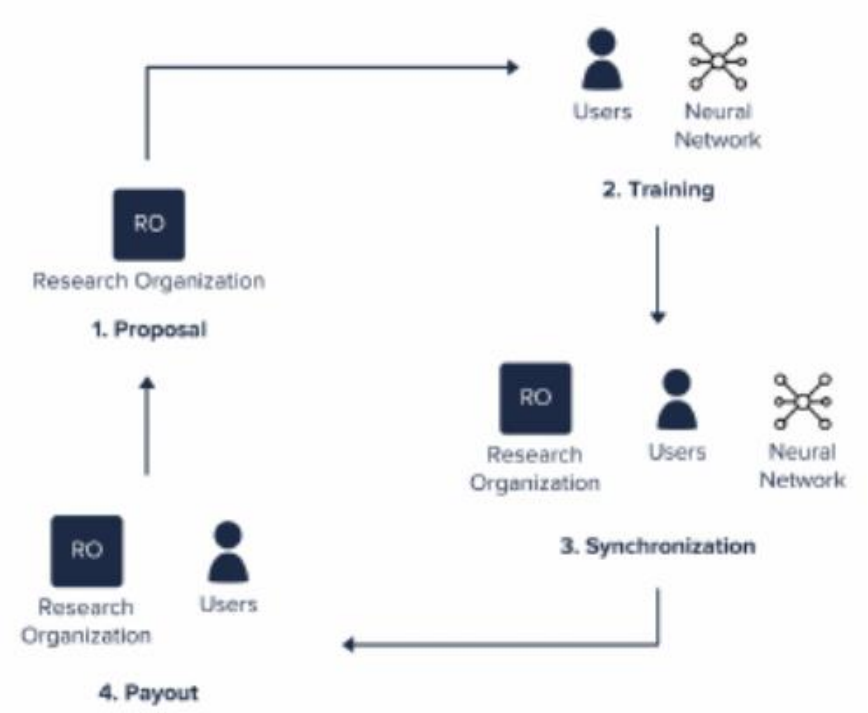
3. Συγχρονισμός

4. Πληρωμή

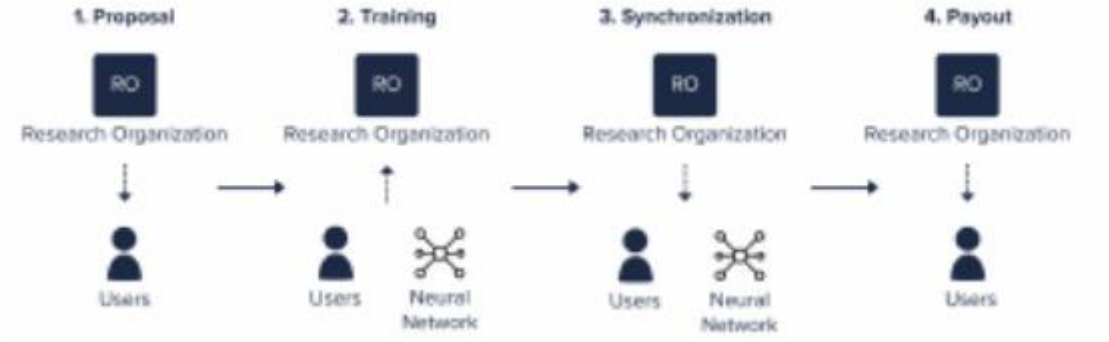
Η φάση της πρότασης αποτελείται από διακομιστές ακρόασης και παρακολούθησης για να προσδιοριστεί εάν υπάρχει το dataset (σύνολο δεδομένων) για την κατάρτιση της μηχανικής μάθησης ενός μοντέλου νευρωνικού δικτύου. Ένα dataset σε αυτό το δίκτυο αποτελείται από τα δεδομένα που έχει να συνεισφέρει ο κάθε χρήστης. Αφού το dataset των χρηστών έχει καθοριστεί, αρχίζει η φάση της εκπαίδευσης.

Η φάση της εκπαίδευσης αποτελείται από ένα αρχικό βάρος w0 που μεταδίδεται στους χρήστες. Ο κάθε χρήστης χρησιμοποιεί αυτό το αρχικό βάρος για να υπολογίσει το σχετικό βάρος κλίσης wi. Αυτό αποδίδει ένα σύνολο W n βαθμίδων, με το οποίο θα ενημερωθεί το αρχικό βάρος w0. Όταν ολοκληρωθεί η επανάληψη, οι κλίσεις στέλνονται πίσω στο διακομιστή για τη φάση του συγχρονισμού.

Ο διακομιστής λαμβάνει και συντάσει κάθε κλίση wi από όλους τους συνδεδεμένους χρήστες σε ένα σύνολο W n βαθμίδων με το οποίο θα εκτελεστούν οι στοχαστικές ενημερώσεις στο w0 (Stochastic Gradient Descent). Με τον όρο Stochastic Gradient Descent εννοούμε έναν αλγόριθμο μηχανικής εκμάθησης, ο οποίος επαναλαμβάνεται μέσω μιας σειράς δεδομένων πολλές φορές για να βρει τα καλύτερα βάρη σε ένα μοντέλο. Αυτό το ενημερωμένο βάρος μεταδίδεται στο ίδιο δίκτυο χρηστών για συγχρονισμό του νέου μοντέλου. Μετά τον συγχρονισμό και τον ανασχηματισμό του dataset, οι χρήστες πληρώνονται. Οι αλληλεπιδράσεις NeuRoN απεικονίζονται ως βρόγχος στην Εικόνα 24 και στην Εικόνα 25. [48]



Εικόνα 25: Φάσεις μάθησης (βρόγχος)

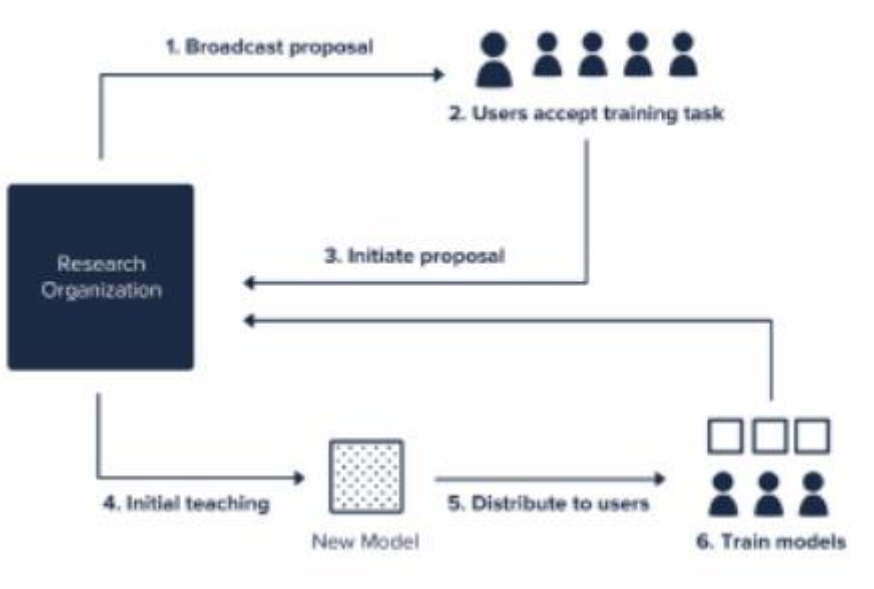


Εικόνα 26: Φάσεις μάθησης (διαδοχικά)

Πρόταση

Η φάση της πρότασης, που παρουσιάζεται στην Εικόνα 26, αποτελείται από την εκπομπή του dataset που διατίθεται για την εκπαίδευση. Όταν ο διακομιστής

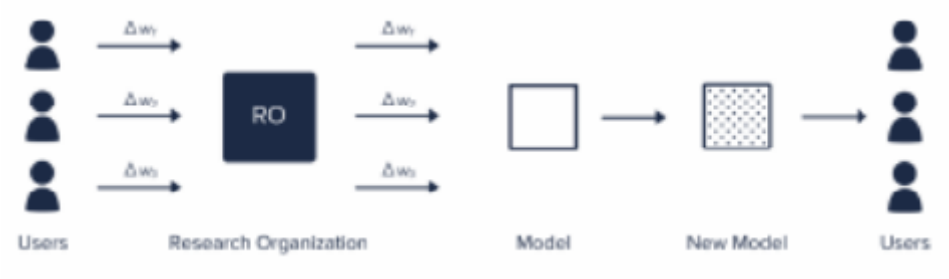
προσδιορίσει ότι υπάρχουν αρκετοί κόμβοι με datasets όμοιων χαρακτηριστικών, ο διακομιστής θα ξεκινήσει μια πρόταση. Αυτό απαιτεί από τον διακομιστή να επιλέξει τους χρήστες οι οποίοι επιθυμούν να ξεκινήσουν μια διαδικασία μάθησης και να υποβληθούν σε μια αρχική διδασκαλία. Προκειμένου να υπολογιστούν σωστά οι στοχαστικές κλίσεις, το dataset που θα υποβληθεί στη διαδικασία μάθησης θα πρέπει να έχει ένα σταθερό μέγεθος. Ως αποτέλεσμα, οι χρήστες πρέπει να είναι παρόντες καθ 'όλη τη διάρκεια της μάθησης. Η αρχική φάση διδασκαλίας αποτελείται από τον καθορισμό ενός αρχικού βάρους. Αυτό το αρχικό βάρος, μαζί με το μοντέλο, διαβιβάζεται στους χρήστες για τη φάση της μάθησης. Κατά τη διάρκεια της πρότασης, ο διακομιστής πρέπει να καθορίσει πώς θα ήθελε να αποζημιώσει τους χρήστες του. Οι χρήστες μπορούν να πληρώνονται σε κάθε περίοδο συλλογής ενός dataset ή κατά την ολοκλήρωσή της. [48]



Εικόνα 27: Πρόταση

Εκπαίδευση

Η αρχικοποίηση της εκπαίδευσης συνεπάγεται τη μεταφορά των παραμέτρων που απαιτούνται για την διεξαγωγή της στον πρώτο χρήστη. Η αρχικοποίηση της εκπαίδευσης αποτελεί την πρώτη εκπαίδευση σε μια ακολουθία διαδικασιών όπου το μοντέλο προωθείται από τους χρήστες ασύγχρονα. Η πρώτη εκπαίδευση συνίσταται στη μετάδοση του αρχικού στοχαστικού βάρους και του μοντέλου που θα μεταφερθεί στη συσκευή των χρηστών. Ο χρήστης θα διδάξει το νευρονικό δίκτυο με βάση το τοπικά αποθηκευμένο dataset. Το νευρονικό δίκτυο θα επιστρέψει μόνο τα νέα υπολογισμένα βάρη σε σχέση με τη γνώση που είχε αρχικά για να είναι έτοιμο το dataset για την επόμενη επανάληψη, όπως φαίνεται στην Εικόνα 27. Το νευρωνικό δίκτυο θα επισκεφτεί τη συσκευή κάθε χρήστη μέχρι να έχει υπολογίσει ένα βάρος στοχαστικής κλίσης από τον καθένα. Η ολοκλήρωση αυτής της διαδικασίας θα σηματοδοτήσει μια πλήρη περίοδο για το συγκεκριμένο dataset. [48]



Εικόνα 28: Εκπαίδευση

Συγχρονισμός

Ο συγχρονισμός λαμβάνει χώρα αφού το νευρικό δίκτυο έχει ολοκληρώσει μια περίοδο λειτουργίας. Αυτό αποτελείται από τον server που συσσωρεύει όλα τα βάρη και υπολογίζει ένα νέο μοντέλο ή ένα νέο αρχικό βάρος που πρέπει να παρέχει στο δίκτυο. Αυτό το αρχικό βάρος μεταδίδεται και πάλι στους χρήστες, εάν οι χρήστες είναι ακόμα διαθέσιμοι για μια δεύτερη περίοδο συλλογής δεδομένων και εκμάθησης του νευρωνικού δικτύου.

Πληρωμή

Κατά την περίοδο της αρχικής πρότασης, οι χρήστες λαμβάνουν το ποσό tokens που ο διακομιστής είναι πρόθυμος να πληρώσει. Όταν ο αριθμός των απαιτούμενων περιόδων από τον διακομιστή ολοκληρωθεί, οι χρήστες αποζημιώνονται για τη διδασκαλία των νευρωνικών δικτύων. Όταν λαμβάνεται μια πρόταση, οι χρήστες έχουν την ευκαιρία να απορρίψουν την προσφορά. Η πρόθεση είναι να ενθαρρυνθούν οι ερευνητικοί οργανισμοί να πληρώσουν ένα δίκαιο και ελκυστικό ποσό στους χρήστες, προκειμένου να ενθαρρύνουν τη συμμετοχή τους στο δίκτυο.

4.3 Πλεονεκτήματα εφαρμογής Blockchain τεχνολογίας στο χώρο της Υγείας

Όπως περιγράφηκε και παραπάνω η τεχνολογία του blockchain προσφέρει πολλές λύσεις και έχει πολλά πλεονεκτήματα τα οποία θα αναφερθούν. Τα κυριότερα από αυτά παρουσιάζονται παρακάτω :

- **Διαλειτουργικότητα**

Η διαλειτουργικότητα της υγειονομικής περίθαλψης περιγράφει την ικανότητα του δικτύου να επικοινωνεί με άλλα συστήματα χωρίς φραγμούς ή περιορισμούς και πιο συγκεκριμένα την ικανότητα για ετερογενείς πληροφορίες, τεχνολογικά συστήματα και εφαρμογές λογισμικού, να επικοινωνούν, να ανταλλάσσουν δεδομένα και να χρησιμοποιούν τα ανταλλασσόμενα δεδομένα σύμφωνα με τις εκάστοτε ανάγκες τους [46]. Με την ύπαρξη διαλειτουργικότητας στον ιατρικό τομέα θα μπορούσαν να αποφευχθούν περιστατικά όπου τα EHR δεν είναι σε θέση να επικοινωνούν σωστά μεταξύ τους, με αποτέλεσμα πολλές φορές να χορηγούνται φάρμακα που θα

μπορούσαν να επηρεάσουν αρνητικά τη φροντίδα των ασθενών. Ένα σύστημα υγείας που χρησιμοποιεί Blockchain μπορεί να αποτελέσει σημείο σύγκλισης για τις πληροφορίες υγείας ενός ασθενούς . Σε ένα πραγματικά διαλειτουργικό δίκτυο λοιπόν, τα δεδομένα που συλλέγονται κατά τη διάρκεια όλης της ζωής ενός ασθενούς, όπως οι συναντήσεις με γιατρούς, οι διαδικασίες εξέτασης, οι εργαστηριακές εξετάσεις, οι έξυπνες συσκευές και ακόμη και οι υπηρεσίες γενετικού ελέγχου, θα μπορούσαν να ενσωματωθούν με ασφάλεια στο μοναδικό ηλεκτρονικό φάκελο του ασθενούς,ο οποίος θα χρησιμοποιείται από κάθε ιατρικό σύστημα υγείας. [28]

- **Ευελιξία-Ταχύτητα**

Ένα ακόμα πλεονέκτημα της τεχνολογίας Blockchain, είναι η ευελιξία. Ένα πρακτικό σύστημα υγείας βασισμένο σε Blockchain μπορεί να διαχειρίζεται και να παρακολουθεί την κατάσταση υγείας μεγάλου αριθμού ασθενών από οποιαδήποτε τοποθεσία [46]. Η διαθεσιμότητα των πληροφοριών οδηγεί στη βελτίωση του συντονισμού φροντίδας από γιατρούς, φαρμακοποιούς και ασφαλιστικούς παρόχους, οι οποίοι παραδοσιακά επικοινωνούν μέσω καναλιών που είναι χειροκίνητα και χρονοβόρα, δυσχεραίνοντας έτσι τη διαδικασία παροχής ιατρικής φροντίδας.

Όπως αναφέρθηκε και παραπάνω τα δεδομένα συλλέγονται, επικυρώνονται και διανέμονται σε όλα τα εμπλεκόμενα μέρη, ενώ ο πάροχος υπηρεσιών φροντίδας μπορεί να έχει εύκολη και γρήγορη πρόσβαση μέσω του Blockchain για να παρακολουθεί και να βελτιώνει την υγεία του ασθενούς. Ο ασθενής μπορεί να ωφεληθεί από δραστηριότητες και αλλαγές στην αγωγή του και ο ασφαλιστής του ασθενούς μπορεί να ελέγξει με ακρίβεια και να αποφασίσει τις πληρωμές που πρέπει να γίνουν χωρίς περιθώρια για απάτη. Έτσι ανεξάρτητα από την κατάσταση του ασθενούς και τις συνθήκες που επικρατούν, επαληθεύονται εύκολα τα στοιχεία και το ιστορικό του, μέσω του Blockchain και μπορεί άμεσα να ληφθεί απόφαση για την κατάλληλή αγωγή. Μία τέτοια αλλαγή στον ιατρικό τομέα μπορεί να αποφέρει αποτελεσματικότερη και γρηγορότερη ιατρική περίθαλψη, καθώς και μείωση του χρόνου εξυπηρέτησης των επειγόντων περιστατικών στα κέντρα περίθαλψης. Η γενική διαθεσιμότητα των δεδομένων είναι ζωτικής σημασίας σε καταστάσεις έκτακτης ανάγκης. [28]

- **Έρευνα**

Οι κλινικές δοκιμές χρησιμοποιούνται για τον προσδιορισμό της αποτελεσματικότητας συγκεκριμένων φαρμάκων ή για την εφεύρεση καινούριων. Κατά τη διάρκεια κλινικών δοκιμών, οι ερευνητές αποκτούν και επεξεργάζονται πολλές πληροφορίες σχετικά με στατιστικές, αποτελέσματα δοκιμών, εκθέσεις ποιότητας κλπ. Πολλές φορές, αυτά τα δεδομένα, τροποποιούνται προκειμένου να αλλάξουν το σύνολο των αποτελεσμάτων της έρευνας. [28]

Η τεχνολογία Blockchain θα μπορούσε να βελτιώσει το σύνολο της ερευνητικής διαδικασίας όχι μόνο στο στάδιο της αναθεώρησης, αλλά και κατά την εκτέλεση της

ίδιας της πειραματικής εργασίας. Το Blockchain θα μπορούσε να διευκολύνει τέτοιες μελέτες σε διάφορα επίπεδα [50] , συμπεριλαμβανομένων των εξής:

• Σχεδιασμός Μελέτης

Το πρωτόκολλο μελέτης σε ένα δίκτυο Blockchain μπορεί να καταγράφει στοιχεία με όλη την πολυπλοκότητα που απαιτείται, συμπεριλαμβανομένης της στατιστικής ανάλυσης. Μπορεί να καθορίσει τον τύπο και το είδος της μελέτης, τα πρωτογενή και δευτερογενή προσδοκόμενα αποτελέσματα και να καθορίσει τα κριτήρια για την καταχώριση, την ομαδοποίηση και το μέγεθος του δείγματος. Αυτές οι πληροφορίες μπορούν να καταγραφούν ώστε να αποφευχθεί οποιαδήποτε αλλοίωση στο δείγμα. Αυτό, βέβαια, εμποδίζει τη δυνατότητα τροποποίησης του αρχικού σχεδιασμού και της αλλαγής της μελέτης [51]. Αν ένας ερευνητής θελήσει να αλλάξει τις παραμέτρους της μελέτης του θα πρέπει να ζητήσει εκ νέου δικαιώματα πρόσβασης στα δεδομένα επεξηγώντας και πάλι πως αυτά θα χρησιμοποιηθούν.

• Κλινικές Δοκιμές

Ένας άλλος τομέας που μπορεί να βελτιωθεί με τη χρήση αυτής της τεχνολογίας είναι η αύξηση του αριθμού συμμετοχής και συγκατάθεσης στη μελέτη. Με την εφαρμογή αυτής της τεχνολογίας, η συναίνεση του ασθενούς καταγράφεται και το πρωτόκολλο μελέτης μπορεί να αποθηκευτεί μαζί με την ενημερωμένη συγκατάθεση, οι οποία φέρει την ψηφιακή υπογραφή του συμμετέχοντα. Στην περίπτωση τροποποιήσεων της μελέτης, μπορεί να γίνει επανεξέταση της άδειας ασθενούς και να αναδημοσιευτεί μαζί με την τροποποίηση. Αυτή η διαδικασία είναι ένας τρόπος παροχής μεγαλύτερης εμπιστοσύνης στην ασφάλεια και την αξιοπιστία της συγκατάθεσης. [28]

Είναι επίσης αυτονόητο ότι οι κλινικές δοκιμές είναι αποτελεσματικές εάν δημοσιευθούν, καθώς μόνο τότε έχουν πρόσβαση σε αυτές κι άλλα ινστιτούτα έρευνας. Τα δεδομένα από κλινικές δοκιμές αποκρύπτονται συνήθως από ερευνητές, γιατρούς και ασθενείς, οδηγώντας σε έλλειψη εμπιστοσύνης στην όλη διαδικασία και υπογραμμίζοντας την ανάγκη μεγαλύτερης διαφάνειας [52]. Η χρήση Blockchain για τη διαχείριση όλων των καταγραφών, μπορεί να αποτελέσει μία εναλλακτική στρατηγική για την αντιμετώπιση αυτών των προκλήσεων [28]. Για παράδειγμα μέσω της τεχνολογίας Blockchain δίνεται η δυνατότητα στον ασθενή να είναι ο μόνος κάτοχος των δεδομένων του, οπότε αυτός αποφασίζει τι δικαιώματα πρόσβασης θα δώσει σε ερευνητές και σε ποιες πληροφορίες. Τέλος, κάθε φορά που τα δεδομένα του ασθενή θα ζητούνται για κάποια ιατρική έρευνα θα μπορεί να ενημερώνεται μέσω ενός ηλεκτρονικού μηνύματος ή μιας ειδοποίησης και να αρνηθεί την πρόσβαση σε αυτά.

• Ανάλυση δεδομένων

Η ανάλυση δεδομένων μέσω μιας εφαρμογής Blockchain μπορεί να γίνει αυτόματα και σύμφωνα με τον τρόπο που περιγράφηκε στο έξυπνο συμβόλαιο με το οποίο συμφώνησε ο ασθενής να παραχωρήσει τα δεδομένα του. Οποιαδήποτε προσπάθεια

αλλαγής των μεταβλητών του τρόπου επεξεργασίας θα σταματούσε αμέσως τον κώδικα της ίδιας της μελέτης, εμποδίζοντας τη χρήση της. Αυτή η διαδικασία όχι μόνο θα βελτίωνε σημαντικά την ασφάλεια των πληροφοριών, αλλά θα μπορούσε να χρησιμοποιηθεί και να αξιοποιηθεί από έναν άλλο ερευνητή. Επειδή πρόκειται για ένα αποκεντρωμένο σύστημα που συντηρείται από τους ίδιους τους χρήστες, μπορεί να επικυρωθεί η πορεία της μελέτης από τους διάφορους ασθενείς που εμπλέκονται σε αυτήν. Επιπλέον, χάρη στην ικανότητά της τεχνολογίας αυτής να χρησιμοποιεί κρυπτογραφία, οι ασθενείς μπορούν να μοιράζονται κλινικά δεδομένα χωρίς να χρειάζεται να μοιράζονται ευαίσθητα προσωπικά δεδομένα. Επιπροσθέτως, διαφορετικοί ερευνητές από εκείνους που συμμετέχουν στη μελέτη θα μπορούσαν να έχουν πρόσβαση σε κλινικά δεδομένα ασθενών πριν από την αναλυτική επεξεργασία (ακατέργαστα και μη επεξεργασμένα δεδομένα) για δευτερογενείς αναλύσεις, αναθεωρήσεις ή και μεταγενέστερες αναλύσεις. [28]

- **Διαφάνεια και Ασφάλεια**

Εκτός από τη διαμεσολάβηση, την ακεραιότητα και την προέλευση των δεδομένων, οι πάροχοι υγειονομικής περίθαλψης θεωρούν τη διαφάνεια ως ένα από τα πλέον σημαντικά πλεονεκτήματα της χρήσης του Blockchain στη βιομηχανία τους. Η υγειονομική περίθαλψη είναι μια κρίσιμη και υπό συνεχή έλεγχο βιομηχανία και είναι πολύ σημαντικό να διασφαλιστούν οι διαφανείς διαδικασίες. Ταυτοχρόνως, τα μέτρα ασφαλείας υψηλού επιπέδου και η απόλυτη ακρίβεια των δεδομένων είναι σημαντικά ζητήματα και προκλήσεις. Η τεχνολογία Blockchain δεν οδηγεί μόνο σε ολοκληρωμένες πληροφορίες για την υγειονομική περίθαλψη, αλλά διατηρεί επίσης ανιχνεύσιμα αρχεία κατανεμημένων δεδομένων και εργασίας. Εξάλλου, η πρόσβαση του δημόσιου ή ιδιωτικού κλειδιού διασφαλίζει τη συνολική ασφάλεια εξαλείφοντας τις πιθανότητες διαρροής δεδομένων. Επιπλέον, μπορεί να διευκολύνει την παρακολούθηση της διαδρομής ενός φαρμάκου από τον παραγωγό έως τον ασθενή. Εκτός από τη διασφάλιση της έγκαιρης προμήθειας, εξαλείφει επίσης τις πιθανότητες παραχάραξης από τρίτους. Τέλος, βελτιώνει την ασφάλεια της παροχής υγειονομικής περίθαλψης.

Η καθιέρωση ενός αμετάβλητου Blockchain ledger, στο οποίο οι ασθενείς ενημερώνονται για όλες τις αλλαγές στα αρχεία και τους λογαριασμούς τους για την υγειονομική περίθαλψη, θα εξαλείψει την πιθανότητα καταχρήσεων και παραπληροφόρησης. Η θέσπιση ενός τέτοιου συστήματος θα ενίσχυε επίσης την ασφάλεια των αλυσίδων εφοδιασμού φαρμάκων. Συστήματα που βασίζονται σε Blockchain και στοχεύουν στην παρακολούθηση κάθε σταδίου της προμήθειας φαρμάκων βρίσκονται ήδη υπό ανάπτυξη.

Υπάρχουν επίσης ζητήματα ασφάλειας που σχετίζονται με την κεντρική φύση αυτών των αρχείων με την τρέχουσα μορφή τους, καθιστώντας τους συχνούς στόχους επιθέσεων στον κυβερνοχώρο. Η μετάβαση από το σημερινό παράδειγμα της ανταλλαγής πληροφοριών σε ένα EHR έχει τη δυνατότητα να επιστρέψει την κυριότητα των δεδομένων περί υγειονομικής περίθαλψης στους ίδιους τους ασθενείς.

Οι πάροχοι υγειονομικής περίθαλψης θα χρειάζονται κρυπτογραφημένα κλειδιά για να ζητήσουν πληροφορίες από ασθενείς και οι ασθενείς θα μπορούν με τη σειρά τους να επιλέξουν ποιος έχει πρόσβαση στα ιατρικά τους αρχεία και πότε. Οι ασθενείς θα μπορούν επιπλέον να παραμετροποιήσουν την εξουσιοδότηση ανταλλαγής πληροφοριών με νόμιμους παρόχους σε απρόβλεπτες καταστάσεις έκτακτης ανάγκης, χωρίς στην πραγματικότητα να μοιράζονται εκ των προτέρων τα δεδομένα αυτά. [28]

4.4 Μειονεκτήματα εφαρμογής Blockchain τεχνολογίας στο χώρο της Υγείας

Παρακάτω παρατίθενται όλα τα βασικά μειονεκτήματα που προκύπτουν από την εφαρμογή της Blockchain τεχνολογίας στο χώρο της υγείας και της υγειονομικής περίθαλψης, τα οποία προέκυψαν από μελέτες και αναφορές.

- **Ηθικό Πλαίσιο, Αδυναμία Διαγραφής και Ανθρώπινο Λάθος**

Το θεμελιώδες δικαίωμα των ασθενών στην προστασία των δεδομένων τους σχετικά με την υγεία αποτελεί μείζων ζήτημα σε διάφορα πλαίσια, όπως η υγειονομική περίθαλψη, η φροντίδα που παρέχεται μέσω της ηλεκτρονικής υγείας ή σε διασυνοριακό πλαίσιο, καθώς και στην έρευνα. Η υγεία και τα γενετικά δεδομένα των ασθενών είναι ευαίσθητες πληροφορίες που απαιτούν υψηλό επίπεδο προστασίας για να διασφαλιστεί ότι δεν αποκαλύπτονται άσκοπα και χωρίς λόγο. Ταυτόχρονα, η ομαλή ανταλλαγή αυτών των δεδομένων είναι απολύτως απαραίτητη για την καλή λειτουργία των υπηρεσιών υγειονομικής περίθαλψης, την ασφάλεια των ασθενών και την προώθηση της έρευνας.

Ο σεβασμός της ιδιωτικής ζωής των δεδομένων και των συναλλαγών είναι ένας βασικός συντελεστής για αυτά τα έργα, όπως το Blokchain, Bitcoin κ.λπ. . Ταυτόχρονα όμως αποτελεί και εμπόδιο στην ανάπτυξη τους λόγω της απουσίας ενός νομοθετικού και ηθικού πλαισίου γύρω από την αποθήκευση δεδομένων σε Blockchain.

Θεωρητικά τα Blockchain δίκτυα είναι αμετάβλητα και δεν μπορούν να αλλάξουν το περιεχόμενο τους μόλις δημιουργηθούν. Σε μια παραδοσιακή βάση δεδομένων, ένας πελάτης μπορεί να εκτελέσει τέσσερις λειτουργίες δεδομένων, δηλαδή δημιουργία, ανάγνωση, ενημέρωση και διαγραφή (συλλογικά γνωστές ως εντολές CRUD – Create, Read, Update, Delete). Σε αντίθεση, ένα Blockchain έχει σχεδιαστεί για να έχει μόνο μία από τις παραπάνω λειτουργίες. Ένας χρήστης μπορεί μόνο να προσθέσει περισσότερα δεδομένα, με τη μορφή επιπλέον μπλοκ. Όλα τα προηγούμενα δεδομένα αποθηκεύονται μόνιμα και δεν μπορούν να τροποποιηθούν ή ακόμα και να διαγραφούν. Επομένως, οι μόνες εργασίες που σχετίζονται με μπλοκ αλυσίδες είναι η ανάγνωση λειτουργιών, δηλαδή ανάκτηση δεδομένων από το δίκτυο Blockchain και λειτουργίες εγγραφής, δηλαδή πρόσθεση δεδομένων στο δίκτυο Blockchain.

Βάσει των παραπάνω εργασιών ενός τέτοιου δικτύου για τις συναλλαγές δεν υπάρχει κάποιο μειονέκτημα ή αντίθετο επιχείρημα, σχετικά με το αν η μονιμότητα των πληροφοριών δημιουργεί πρόβλημα στην ορθή λειτουργία. Υπάρχουν όμως δύο βασικά προβλήματα όσον αφορά τη διαγραφή ή τροποποίηση αρχείων και ταυτότητας. Κατ 'αρχάς, υπάρχει η ανησυχία ότι οι χρήστες θα έχουν ψευδείς πληροφορίες σχετικά με αυτές που αναφέρονται στην πλατφόρμα δικτύου, καθώς αυτό αποτελεί από μόνο του πρόβλημα εφόσον δεν μπορούν να διορθωθούν σωστά. Δεύτερον, και πιο σημαντικό, υπάρχουν σαφείς κανονισμοί σε διάφορες χώρες που απαιτούν την κατάργηση ορισμένων πληροφοριών περί ταυτότητας υπό ορισμένες συνθήκες.

Όλα τα παραπάνω καθιστούν αναγκαία την τροποποίηση των νομοθεσιών σε αρκετές χώρες προκειμένου προσωπικά στοιχεία στο θέμα της υγείας να μπορούν να καταγραφούν σε μία κοινή πλατφόρμα δικτύου, δεδομένου ότι σε ένα δίκτυο Blockchain δεν δύναται η διαγραφή ή τροποποίηση στοιχείων.

Απόρροια αυτής της αδυναμίας διαγραφής αποτελεί επίσης το γεγονός ότι είναι πολύ πιθανόν να υπάρχουν ανθρώπινα λάθη, καθώς οι εγγραφές των δεδομένων στο δίκτυο γίνονται από τον ίδιο τον άνθρωπο. Εάν τα δεδομένα που αποθηκεύτηκαν στο δίκτυο είναι ανακριβή ή περιέχουν σφάλματα που οφείλονται σε ανθρώπινο παράγοντα, τότε υπάρχουν ελάχιστες επιλογές διόρθωσης, έως και μηδαμινές, καθώς το δίκτυο κρατάει σχεδόν τα πάντα αμετάβλητα. Ένα ολοκληρωμένο ιατρικό ιστορικό αρχείο, το οποίο μπορεί να αξιοποιηθεί και στον ερευνητικό τομέα αλλά και στην ιατρική περίθαλψη, πρέπει να περιέχει δεδομένα που συνδέονται άρρηκτα ή αιτιωδώς με τις ασθένειες (χρόνιες και μη) και με τη συνολική υγεία των ασθενών του. Τα ιατρικά αρχεία πρέπει δηλαδή να περιέχουν το ονοματεπώνυμο, το πατρώνυμο, το φύλο, την ηλικία, το επάγγελμα, τη διεύθυνση του ασθενή, τις ημερομηνίες της επίσκεψης, καθώς και κάθε άλλο ουσιώδες στοιχείο που συνδέεται με την παροχή φροντίδας στον ασθενή, όπως, ενδεικτικά και ανάλογα με την ειδικότητα, την κατάσταση της υγείας του και το λόγο της επίσκεψης, την πρωτογενή και δευτερογενή διάγνωση ή την αγωγή που ακολουθήθηκε. Πολλά από αυτά τα στοιχεία βραχυπρόθεσμα μπορεί να είναι σταθερά, όμως μακροπρόθεσμα υπάρχει περίπτωση να αλλάξουν και να τροποποιηθούν. Ένα σύστημα Blockchain εμφανίζεται ελλιπές σε τέτοιες αλλαγές και είναι ανάγκη να προβλεφθούν τρόποι παράκαμψης αυτών των δυσκολιών, αλλιώς το σύστημα θα αποτελεί ανακριβή βιβλιοθήκη πληροφοριών. [28]

- **Πολυπλοκότητα και Περιορισμοί Αποθήκευσης**

Ένα άλλο μειονέκτημα, το οποίο συνδέεται και με το κόστος της επένδυσης είναι ο αναγκαίος χώρος αποθήκευσης όλων των δεδομένων του δικτύου. Όπως αναφέρθηκε το δίκτυο παρουσιάζει αδυναμία διαγραφής ή τροποποίησης στοιχείων και δεδομένων. Αυτό έχει ως συνέπεια οι ανάγκες για αποθηκευτικό χώρο συνεχώς να αυξάνονται. Η αποθήκευση πληροφοριών σε μια βάση δεδομένων Blockchain σημαίνει ότι τα δεδομένα :

1. Αποθηκεύονται σε κάθε πλήρες κόμβο στο δίκτυο.

2. Αποθηκεύονται απεριόριστα εφόσον η βάση δεδομένων Blockchain είναι μονομερώς προσαρτημένη και αμετάβλητη.

Επομένως, η αποθήκευση δεδομένων επιβάλλει ένα τεράστιο κόστος σε ένα αποκεντρωμένο δίκτυο, όπου κάθε πλήρης κόμβος πρέπει να αποθηκεύει όλο και περισσότερα δεδομένα στο άπειρο. Ως αποτέλεσμα, η αποθήκευση παραμένει ως ένα εμπόδιο και περιορισμό για κάθε ρεαλιστική εφαρμογή που χτίζεται στο Blockchain.[28]

- **Εκπαίδευση Ιατρικού Προσωπικού**

Τέλος, όπως ισχύει σε κάθε νέα τεχνολογία έτσι και σε αυτή ένα βασικό μειονέκτημα είναι η ανάγκη εκπαίδευσης του προσωπικού. Είναι λογικό ότι το ιατρικό προσωπικό ως επί το πλείστον δεν θα γνωρίζει το πως μπορεί να χρησιμοποιήσει ένα τέτοιο σύστημα, το οποίο διαφέρει σημαντικά από τα υπάρχοντα. Σε αυτή τη κατεύθυνση θα πρέπει να υπάρξει μία περίοδος εξοικείωσης με αυτή τη νέα τεχνολογία.

5 Σενάρια Χρήσης μίας Blockchain Εφαρμογής στην Υγεία

5.1 Εισαγωγή

Η ερευνητική κοινότητα έχει αρχίσει να αξιοποιεί τις δυνατότητες της τεχνολογίας Blockchain πέρα από τις οικονομικές εφαρμογές. Όπως αναφέρθηκε και στο προηγούμενο κεφάλαιο το Blockchain ως αποκεντρωμένη τεχνολογία μπορεί να έχει πολύ χρήσιμες εφαρμογές και σε άλλους τομείς όπως η υγειονομική περίθαλψη, η λογιστική , η διαχείριση της αλυσίδας εφοδιασμού και το Διαδίκτυο των πραγμάτων (IoT). [53],[54],[55] Το Blockchain παρέχει ασφαλή κατανεμημένη βάση δεδομένων που μπορεί να εκτελέσει τις λειτουργίες της χωρίς καμία παρέμβαση από εφαρμογές τρίτου μέρους ή κεντρικής διοίκησης, κάτι το οποίο είναι ιδιαίτερα χρήσιμο στην περίπτωση που διάφορα ενδιαφερόμενα μέρη επιθυμούν να αποκτήσουν πρόσβαση σε αυτές τις πληροφορίες. Έτσι, τα συστήματα που βασίζονται σε Blockchain έχουν τεράστιες δυνατότητες να ελαχιστοποιήσουν το κόστος και τους απαιτούμενους πόρους των σημερινών ενδιάμεσων. [56]

Το Διαδίκτυο των πραγμάτων [57] και άλλες τεχνολογίες επικοινωνίας (όπως το 5G) [58], [59] έχουν τεράστιο αντίκτυπο στις υπηρεσίες υγειονομικής περίθαλψης και παρέχουν στους καταναλωτές καλύτερες και βελτιωμένες ιατρικές υπηρεσίες, αλλά δίνουν και τη δυνατότητα της δημιουργίας εσόδων στους εμπλεκόμενους φορείς. Η αποθήκευση και η ανταλλαγή ιατρικών δεδομένων αποτελεί αναπόσπαστο μέρος των συστημάτων υγειονομικής περίθαλψης, προκειμένου να βελτιωθεί η ποιότητα και οι υπηρεσίες υγείας. Ωστόσο, η ανταλλαγή αρχείων μεταξύ διαφόρων οντοτήτων μέσω μη ασφαλών μέσων μπορεί να οδηγήσει σε διαρροή προσωπικών και κρίσιμων πληροφοριών του ασθενούς. [56] Οι χρήστες θα πρέπει να έχουν τη δυνατότητα ελέγχου των προσωπικών τους πληροφοριών για να μπορούν να αποτρέψουν επιβλαβείς για τους ίδιους συνέπειες, όπως η πρόσβαση μη εξουσιοδοτημένων οντοτήτων στις προσωπικές ιατρικές πληροφορίες τους. Επίσης, κατά την ανταλλαγή ιατρικών πληροφοριών σε διάφορα συστήματα υγειονομικής περίθαλψης θα μπορούσε να προκληθεί κατακερματισμός τους, γεγονός το οποίο θα μπορούσε να οδηγήσει σε διάφορους κινδύνους. [55]

Ένα από τα βασικά ζητήματα στα σημερινά ηλεκτρονικά ιατρικά αρχεία (HER/EMR) είναι η διατήρηση της διαλειτουργικότητας μεταξύ διαφόρων ενδιαφερομένων μερών.[60] Αυτό το ζήτημα μπορεί να προκαλέσει εμπόδια στη συναλλαγή δεδομένων μεταξύ τους. Η έλλειψη συντονισμένου μηχανισμού διαχείρισης και

ανταλλαγής δεδομένων μεταξύ διαφόρων φορέων μπορεί να προκαλέσει τον κατακερματισμό των πληροφοριών της υγειονομικής περίθαλψης. Εκτός από τη διαλειτουργικότητα, η ασφάλεια των δεδομένων και η προστασία της ιδιωτικής ζωής αποτελούν βασικές προκλήσεις στους τρέχοντες τρόπους αποθήκευσης και ανταλλαγής δεδομένων μέσω συστημάτων HER/EMR. [60], [61]. Οι περισσότεροι από τους ασθενείς διστάζουν να μοιραστούν και να αποθηκεύσουν τις προσωπικές τους ιατρικές πληροφορίες λόγω της διαρροής δεδομένων και πιθανών ελλείψεων στον μηχανισμό ασφαλείας. [62],[63] Συνεπώς, υπάρχει σαφής ανάγκη για κατανεμημένο τρόπο ανταλλαγής δεδομένων και αποθήκευση όπου οι ασθενείς είναι πιο σίγουροι για την ασφάλεια των δεδομένων και την ιδιωτική τους ζωή και επιπλέον όλοι οι εμπλεκόμενοι φορείς μπορούν να έχουν μία καθολική άποψη της συνολικής συναλλαγής και των αλληλεπιδράσεων.[60]

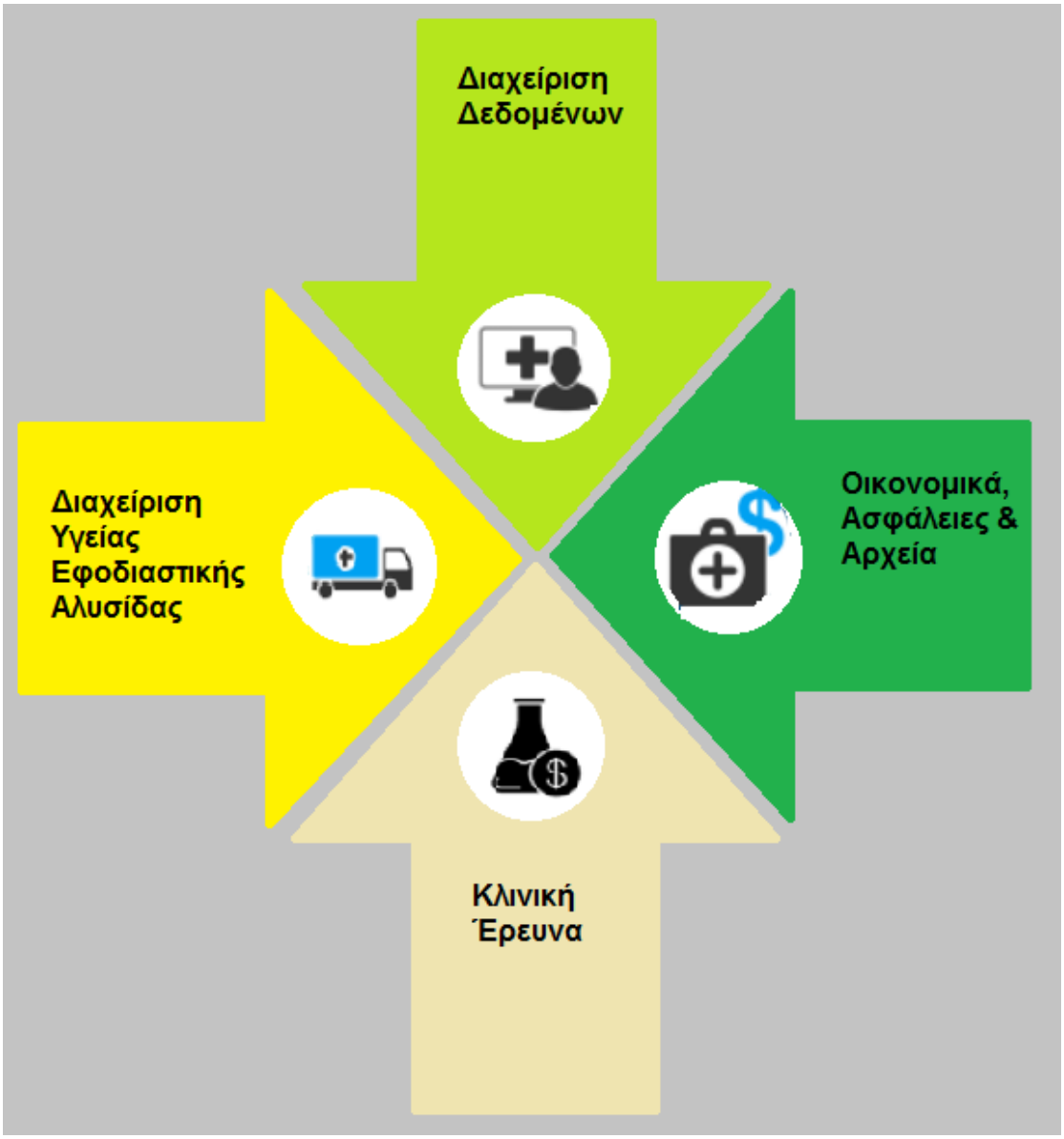
Επομένως, λαμβάνοντας υπόψη αυτές τις προκλήσεις στα τρέχοντα συστήματα υγειονομικής περίθαλψης, είναι ζωτικής σημασίας να αξιοποιηθεί η δυναμική της τεχνολογίας Blockchain στον τομέα αυτό. [55] Η τεχνολογία Blockchain μπορεί να διασφαλίσει την ασφάλεια των κρίσιμων πληροφοριών των ασθενών και να διασφαλίσει ότι θα έχουν πρόσβαση μόνο έγκυρες και εξουσιοδοτημένες οντότητες στα δεδομένα [64], [65],[66], [67]. Επιπλέον, το Blockchain χρησιμοποιεί τα έξυπνα συμβόλαια, επιτρέποντας έτσι τη δημιουργία αξιόπιστων χαρακτηριστικών μεταξύ των διαφόρων οντοτήτων του συστήματος. Τα συστήματα υγειονομικής περίθαλψης που βασίζονται σε Blockchain τεχνολογία κατασκευάζονται επίσης με τρόπο που να υποστηρίζει τη διαλειτουργικότητα των συστημάτων αυτών. [56]

Το Blockchain στον τομέα της υγειονομικής περίθαλψης μπορεί να λύσει πολλά προβλήματα που προγενέστερες εφαρμογές δεν αντιμετώπισαν με αποτελεσματικό τρόπο. Πολλές εταιρείες που δραστηριοποιούνται στην υγειονομική περίθαλψη και στο Blockchain εργάζονται επί του παρόντος ή έχουν ήδη εκδώσει συστήματα βασισμένα σε Blockchain για τη βελτίωση της υγειονομικής περίθαλψης τόσο για τους επαγγελματίες όσο και για τους ασθενείς. Με την αποκέντρωση του ιστορικού υγείας των ασθενών, την παρακολούθηση των φαρμάκων και τη βελτίωση των επιλογών πληρωμής, το Blockchain γίνεται ένα πολύτιμο εργαλείο για την υγειονομική περίθαλψη.

5.2 Περιγραφή Σεναρίων Χρήσης

Σε αυτή την ενότητα θα εστιάσουμε στη περιγραφή βασικών σεναρίων χρήσης μίας εφαρμογής που έχει αναπτυχθεί με Blockchain τεχνολογία στον τομέα της υγειονομικής περίθαλψης. Παρακάτω παρουσιάζεται μία κατηγοριοποίηση βάσει κοινών χαρακτηριστικών που εμφανίζονται σε κάποια σενάρια χρήσης από δείγμα συγκεκριμένων περιπτώσεων. Με αυτή τη λογική έχουν δημιουργηθεί τέσσερις βασικοί πυλώνες σεναρίων χρήσης. Τέλος, για κάθε μία από αυτές τις τέσσερις κατηγορίες θα γίνει εκτενής περιγραφή των σεναρίων από τα οποία αποτελούνται και

θα αναφερθούν οι τρόποι με τους οποίους κάθε συμμετέχουσα στην εφαρμογή ομάδα θα μπορούσε να επωφεληθεί.



Εικόνα 29: Βασικοί πυλώνες σεναρίων χρήσης

5.2.1 Διαχείριση Δεδομένων

- **Ψηφιακή Διαχείριση Ταυτότητας**

Ένα θεμελιώδες στοιχείο στην ανταλλαγή πληροφοριών για την υγεία είναι η ταυτοποίηση των ασθενών [68], η οποία εντοπίζει έναν ασθενή σε μια βάση χρησιμοποιώντας ένα μοναδικό σύνολο δεδομένων. Παρά την αυξημένη προσπάθεια δημιουργίας κατάλληλων συστημάτων για τη διαχείριση των ταυτοτήτων, η ακριβής και σταθερή αντιστοίχιση των δεδομένων των ασθενών παραμένει δύσκολη. Η

αναντιστοιχία της ταυτότητας των ασθενών έχει συμβάλει σε διπλότυπα αρχεία και ελλιπή ή λανθασμένα ιατρικά δεδομένα. Υπάρχει επίσης σημαντικό κόστος για τους οργανισμούς υγειονομικής περίθαλψης που διατηρούν αυτά τα διπλά αρχεία και διορθώνουν λανθασμένα συγχωνευμένα σφάλματα καθώς και ασθενείς που επαναλαμβάνουν εξετάσεις ή καθυστερείται η θεραπεία τους. Επιπλέον, αυτά τα σφάλματα επηρεάζουν την επιστροφή χρημάτων από τις ασφάλειες, καθώς οι απαιτήσεις ενδέχεται να απορριφθούν λόγω "εσφαλμένων πληροφοριών", ενώ οι ασθενείς αντιμετωπίζουν και κινδύνους ασφαλείας όταν αποκαλύπτουν τα προσωπικά τους στοιχεία. Χωρίς κοινά πρότυπα για τη συλλογή πληροφοριών ταυτοποίησης ασθενών, η ταυτότητα του ιδίου ασθενούς μπορεί να διαφέρει από τη μία μονάδα φροντίδας στην άλλη. Τέλος, χωρίς λειτουργικό, ενοποιημένο σύστημα διαχείρισης ταυτότητας, τα συστήματα ταυτοποίησης ασθενών που χρησιμοποιούνται από διάφορους παρόχους φροντίδας μπορεί να αντιμετωπίζουν συνεχώς προβλήματα ασυμβατότητας και αδυναμίας ταυτοποίησης ασθενών, εκτός και εάν ο ασθενής λαμβάνει αποκλειστικά φροντίδα σε έναν οργανισμό.

Η διαδικασία ταυτοποίησης των διαφόρων οντοτήτων είναι θεμελιώδης σημασίας για μία εφαρμογή που χρησιμοποιεί τεχνολογία Blockchain στην υγειονομική περίθαλψη (π.χ. ασθενών, ιατρών). Κάθε φορά που πρέπει να επαληθευτεί κάποιο στοιχείο (π.χ. το όνομα, η διεύθυνση ή ο αριθμός ασφάλισης ενός ασθενή) ακολουθείται μια διαδικασία επαλήθευσης ταυτότητας. Μια ελεγκτική διαδικασία επιβεβαιώνει ότι τα δεδομένα που ζητούμε για τον εαυτό μας είναι αληθή ή ψευδή. Το Blockchain μέσω ενός κατανεμημένου ledger επιτρέπει σε όλους τους χρήστες του δικτύου να έχουν την ίδια πηγή αλήθειας σχετικά με τα πιστοποιητικά που είναι έγκυρα και τα οποία βεβαιώνουν την εγκυρότητα των δεδομένων κατά την πιστοποίηση, χωρίς να αποκαλύπτουν τα πραγματικά δεδομένα.

- **Κοινή χρήση ιατρικών δεδομένων**

Μία χρήσιμη και βασική δυνατότητα της τεχνολογίας Blockchain όσον αφορά την υγειονομική περίθαλψη είναι η ανταλλαγή ιατρικών δεδομένων μεταξύ των διαφόρων οντοτήτων του συστήματος (π.χ. ασθενείς, ιατροί, ερευνητές κτλ). Οι ΗΦΥ περιέχουν εξαιρετικά κρίσιμες και ευαίσθητες ιατρικές πληροφορίες, οι οποίες σχετίζονται με τους ασθενείς και θα πρέπει να αποθηκεύονται, να επεξεργάζονται, να μοιράζονται αλλά και να εποπτεύονται μόνο από όσους έχουν πρόσβαση σε αυτές. Για παράδειγμα ένας ασθενής θα πρέπει να έχει την δυνατότητα αν επιθυμεί να μπορεί να μοιραστεί τις ιατρικές του πληροφορίες με συγγενικά και φιλικά του πρόσωπα. Πέρα από αυτή την ανάγκη θα πρέπει να μπορεί να δείξει τα ιατρικά του δεδομένα και σε άλλους γιατρούς που τυχόν επιθυμεί ούτως ώστε να μπορεί να πάρει και μία δεύτερη γνωμάτευση καθώς και να είναι δυνατή η διόρθωση κάποιου λάθους από τυχόν απροσεξία ή κάποιο άλλο ανθρώπινο και όχι μόνο σφάλμα (για παράδειγμα λάθος ένδειξη μηχανήματος).

Επίσης συχνά παρατηρείται ότι προκειμένου να βελτιωθεί η ποιότητα των υπηρεσιών υγειονομικής περίθαλψης, αυτές οι ιατρικές πληροφορίες θα πρέπει να

αποθηκεύονται και να διαμοιράζονται μεταξύ πολλών συμμετεχόντων, όπως ασθενείς, γιατροί, πάροχοι υπηρεσιών υγείας, κλινικές, φαρμακεία, ασφαλιστικές εταιρείες, ερευνητές κτλ. Αυτού του είδους η ανταλλαγή θα πρέπει να διέπεται από αυστηρούς κανόνες έτσι ώστε οι συναλλαγές να γίνονται με τρόπο διαφανή και ξεκάθαρο και πάντοτε με στόχο την κατοχύρωση των δικαιωμάτων των κατόχων των ιατρικών πληροφοριών. Σε αυτή τη κατεύθυνση μία εφαρμογή, η οποία θα αξιοποιούσε την Blockchain τεχνολογία θα προσέφερε περισσότερη διαφάνεια σε τέτοιες περιπτώσεις, καθώς διατηρεί ένα ledger, το οποίο παραμένει ενημερωμένο μεταξύ όλων των εμπλεκομένων φορέων ολόκληρου του δικτύου. Με λίγα λόγια το Blockchain παρέχει έναν ασφαλή τρόπο ανταλλαγής δεδομένων μεταξύ των κόμβων του δικτύου, όπου όλα τα μέρη γνωρίζουν τις συναλλαγές.

- **Παγκόσμια Καταγραφή Δεδομένων**

Σε περίπτωση που ένας ασθενής ταξιδεύει στο εξωτερικό, οι αντίστοιχοι γιατροί / νοσοκομεία της άλλης χώρας πρέπει να έχουν γνώση των πληροφοριών του ασθενή. Μέσω προσεγγίσεων που βασίζονται σε Blockchain, οι ιατρικές πληροφορίες μπορούν εύκολα να μοιραστούν με ιατρικούς οργανισμούς άλλων χωρών και ο ασθενής θα έχει τη δυνατότητα να δώσει τη συγκατάθεση για τον έλεγχο των δεδομένων του. Για να γίνει καλύτερη ιατρική περίθαλψη εκτός της χώρας το ιατρικό ιστορικό θα πρέπει να είναι προσβάσιμο από υπηρεσίες υγειονομικής περίθαλψης που βρίσκονται εκτός της χώρας του ασθενή. [55], [56] Αν και το Blockchain μπορεί να επιτρέψει αυτή τη λειτουργία, απαιτείται συγχρονισμός των μοντέλων και των συστημάτων ιατρικής περίθαλψης σε παγκόσμιο επίπεδο.

- **Διατήρηση του Ιατρικού Ιστορικού**

Μία άλλη δυνατότητα που προσθέτει η τεχνολογία Blockchain είναι η αποθήκευση αλλά και η διατήρηση του ιατρικού ιστορικού των ασθενών. Για παράδειγμα, οι ασθενείς μπορεί να επισκέπτονται νοσοκομεία, κλινικές ή γιατρούς, οι οποίοι δεν έχουν δυνατότητα πρόσβασης στο ιατρικό τους ιστορικό. Αυτό έχει ως αποτέλεσμα όχι μόνο την άγνοια πολλών σημαντικών πληροφοριών που πιθανό να οδηγούσαν σε καλύτερη διάγνωση και κατ' επέκταση αντιμετώπιση κάποιας πάθησης αλλά και παράλληλα το σπάσιμο της αλυσίδας του ιατρικού ιστορικού του ασθενή. Προκειμένου να ξεπεραστούν τέτοια προβλήματα, το Blockchain οδηγεί στη διατήρηση του ιστορικού των αρχείων ενός ασθενή για κάθε επίσκεψη του σε οποιονδήποτε γιατρό, νοσοκομείο ή κλινική. Επιπλέον, λόγω της αδυναμίας στη πρόσβαση ορισμένων δεδομένων που σχετίζονται με ιατρικές ή εργαστηριακές αναφορές, συνηθίζεται οι ασθενείς να υποβάλλονται ξανά στις ίδιες ιατρικές εξετάσεις. Το γεγονός αυτό δεν αυξάνει μόνο το κόστος λόγω της επανάληψης της ίδιας εργαστηριακής δοκιμής, αλλά μπορεί να αποβεί και επικίνδυνο όσον αφορά την υγεία του ασθενή, ειδικά σε περιπτώσεις που επαναλαμβάνονται δοκιμές που τον εκθέτουν σε υψηλές ακτινοβολίες. [64], [69]

5.2.2 Κλινική Έρευνα

- **Έρευνα και Κλινικές Δοκιμές**

Οι κλινικές δοκιμές διεξάγονται προκειμένου να διασφαλιστεί και να αναλυθεί η αποτελεσματικότητα οποιουδήποτε συγκεκριμένου φαρμάκου που αναπτύσσεται και προτείνεται για τη θεραπεία μιας συγκεκριμένης ασθένειας. Τα προτεινόμενα φάρμακα αρχικά δοκιμάζονται και με βάση την επιτυχία της δοκιμής, μπορούν να εφαρμοστούν σε μεγαλύτερη κλίμακα. Επομένως, προκειμένου να διεξαχθεί μια κλινική δοκιμή, απαιτούνται τεράστιες ποσότητες δεδομένων. Οι ερευνητές επικεντρώνονται σε αυτά τα σύνολα δεδομένων και διεξάγουν τακτικές δοκιμές υπό διαφορετικές συνθήκες για τη δημιουργία αναφορών, στατιστικών στοιχείων κτλ. Με βάση αυτές τις αναφορές, τα δεδομένα αναλύονται και λαμβάνονται περαιτέρω αποφάσεις.

Σε πολλές περιπτώσεις, ωστόσο, οι φαρμακευτικές εταιρείες δείχνουν ενδιαφέρον για την καταγραφή των αποτελεσμάτων που μπορούν να εξασφαλίσουν ορισμένα οφέλη για τις επιχειρήσεις τους. Σε τέτοιες περιπτώσεις, οι ερευνητές συχνά κρύβουν ή τροποποιούν τα δεδομένα και τις πληροφορίες που συλλέγουν προκειμένου να αλλάξουν το αποτέλεσμα.

Ως αποτέλεσμα, για διεξαγωγή έμπιστων κλινικών δοκιμών, τα δεδομένα και οι συναλλαγές επί αυτών πρέπει να είναι ασφαλή και διαφανή. Για να επιτευχθεί αυτό, τα έγγραφα που δημιουργήθηκαν και χρησιμοποιήθηκαν στη διαδικασία, όπως η ενημερωμένη συγκατάθεση, τα ερευνητικά σχέδια, οι κανονισμοί και το πρωτόκολλο μελέτης, πρέπει να φέρουν χρονική σφραγίδα. Αυτό σημαίνει ότι τα έγγραφα θα πρέπει να έχουν απόδειξη και λεπτομέρειες του χρόνου δημιουργίας τους. Είναι ιδιαίτερα σημαντικό να κρατηθούν αυτές οι πληροφορίες με χρονική σήμανση για να δημιουργηθεί ένα αποδεικτικό που να δείχνει ότι υπήρξε συμφωνία πριν από την έναρξη της δοκιμής.

Η τεχνολογία Blockchain θα βοηθήσει στην αξιοπιστία των κλινικών δοκιμών και των αποτελεσμάτων. Αυτά τα έγγραφα μπορούν να αποθηκευτούν ως έξυπνες συμβάσεις στο Blockchain και λειτουργούν ως ψηφιακά αποτυπώματα. Αυτός ο κατάλογος εγγράφων θα μειώσει το κόστος ελέγχου, την αναθεώρηση των φακέλων, τα χαμένα έγγραφα και τις απάτες. Το Blockchain θα διατηρήσει επίσης τη διαχείριση της αλυσίδας εφοδιασμού και παρακολούθησης των φαρμάκων. Ως εκ τούτου, το Blockchain μπορεί να είναι ένα ζωτικής σημασίας εργαλείο στη προσπάθεια για την αντιμετώπιση της αξιοπιστίας τέτοιων ερευνητικών δοκιμών όπου κάθε φάση μπορεί να ανιχνευθεί σωστά και τα δεδομένα μπορούν να διαχειρίζονται και να αναλύονται χωρίς μεγάλη απώλεια πόρων και όντας παράλληλα ασφαλή όσον αφορά τη πρόσβαση σε αυτά από τρίτους φορείς. [70]

5.2.3 Οικονομικά, Ασφάλειες και Αρχεία

- **Συναλλαγές μεταξύ των οντοτήτων**

Μία εφαρμογή βασισμένη σε Blockchain θα πρέπει να υποστηρίζει κάποιον τρόπο μέσω του οποίου θα μπορούν να πραγματοποιηθούν συναλλαγές μεταξύ των διαφόρων οντοτήτων. Για παράδειγμα, αν ένας ασθενής θέλει να ζητήσει ηλεκτρονικά μία συμβουλή από τον γιατρό για κάποια συνταγή ή ακόμα και για μια απλή διάγνωση βάσει περιγραφής ορισμένων συμπτωμάτων, θα πρέπει να μπορεί με κάποιον τρόπο να πληρώσει το γιατρό για τις υπηρεσίες του. Σε αυτή την κατεύθυνση η εφαρμογή θα πρέπει να υποστηρίζεται από κάποιο κρυπτονόμισμα που θα υποβοηθά αυτή τη διαδικασία. Παράλληλα, οι ερευνητές μπορούν να προσφέρουν συγκεκριμένο αριθμό κρυπτονομισμάτων στους ασθενείς για την αξιοποίηση της ιατρικής τους πληροφορίας. Οι ασθενείς με την σειρά τους θα μπορούσαν να αξιοποιήσουν αυτά τα κρυπτονομίσματα για την διεξαγωγή κάποιας εξέτασης ή την παρακολούθησή τους από κάποιον γιατρό ή κλινική.

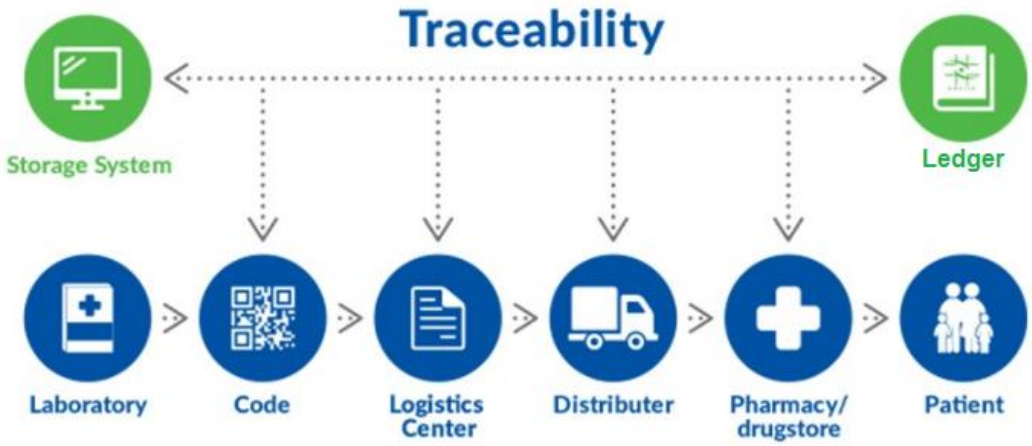
- **Χρέωση και πληρωτές**

Οι παραδοσιακοί τρόποι συστημάτων τιμολόγησης ασθενών θεωρούνται αρκετά χρονοβόρες σε πολλές περιπτώσεις, ειδικά όταν σε αυτές συμμετέχουν δημόσιοι οργανισμοί ή ασφαλιστικές εταιρείες. Αναμένεται ότι οι λύσεις όσον αφορά τις πληρωμές που βασίζονται σε Blockchain θα κάνουν τη διαδικασία χρέωσης πολύ πιο εύκολη σε σύγκριση με τις παραδοσιακές προσεγγίσεις τιμολόγησης, όπου χρειάζονται αρκετές ημέρες για τη διεκπεραίωση μίας συναλλαγής. Επιπλέον, αυτό επιτρέπει σε ασφαλιστικές εταιρείες να έχουν γρηγορότερες και πιο αποδοτικές συναλλαγές, μειώνοντας έτσι τους πρόσθετους πόρους, το χρόνο και το κόστος. [73], [74].

5.2.4 Διαχείριση Υγείας Εφοδιαστικής Αλυσίδας

- **Διαχείριση Αλυσίδας Εφοδιασμού**

Η διαχείριση της προμήθειας ιατρικών φαρμάκων είναι ζωτικής σημασίας για τη σύγχρονη ιατρική βιομηχανία, αλλά εξακολουθεί να πάσχει από διάφορες δυσκολίες εξαιτίας των παραχαρακτών και των κλοπών που γίνονται όσον αφορά τα φάρμακα. Το Blockchain μπορεί να διατηρήσει την ανιχνευσιμότητα τέτοιων πράξεων εφοδιαστικής αλυσίδας και να ενισχύσει την ακεραιότητα της συνολικής διαδικασίας.[71],[72],[73] Το Blockchain είναι επίσης χρήσιμο για την επαλήθευση της αυθεντικότητας των φαρμάκων και της αλυσίδας εφοδιασμού τους στα εξουσιοδοτημένα μέρη.



Εικόνα 30: Παράδειγμα που εξηγεί την ανιχνευσιμότητα των φαρμάκων[77]

5.3 Οφέλη για κάθε συμμετέχουσα ομάδα

Όπως φανερώνεται και από τα παραπάνω σενάρια χρήσης όλες οι συμμετέχουσες οντότητες ή ομάδες σε μία Blockchain εφαρμογή στην υγειονομική περίθαλψη μόνο κερδισμένες θα μπορούσαν να βγουν από αυτή τους την συμμετοχή. Κάθε μία από αυτές τις οντότητες (ασθενείς, γιατρούς, ερευνητές, κλινικές ή άλλους οργανισμούς που επιχειρούν στον τομέα της υγείας) έχουν προφανώς διαφορετικά κίνητρα και στόχους ούτως ώστε να χρησιμοποιήσουν μία τέτοιου είδους εφαρμογή, η αλληλεπίδραση όμως όλων αυτών των οντοτήτων μόνο θετικά αποτελέσματα θα μπορούσε να επιφέρει στον γενικότερο τομέα της υγειονομικής περίθαλψης. Παρακάτω θα παρουσιαστούν αναλυτικά τα οφέλη που θα μπορούσε να έχει μεμονωμένα κάθε μία εκ των ομάδων με την συμμετοχή τους σε μία τέτοιου είδους εφαρμογή.

- **Οφέλη για ασθενείς**

Οι ασθενείς θα έχουν πια άμεση πρόσβαση στο ιατρικό τους ιστορικό οποιαδήποτε στιγμή το επιθυμήσουν και αξιοποιώντας το με αυτόν τον τρόπο για οποιονδήποτε σκοπό κρίνουν. Θα μπορούν έτσι να έχουν μία καλύτερη εποπτεία των εξετάσεων που έχουν κάνει, των συνταγών που τους έχουν χορηγηθεί και όλα αυτά τα έχουν σε ηλεκτρονική μορφή χωρίς να υπάρχει ο κίνδυνος απώλειας. Επίσης, οι ασθενείς έχουν το δικαίωμα αν επιθυμούν να δώσουν πρόσβαση σε κάποιο συγγενικό-φιλικό τους πρόσωπο, γιατρό ή και ερευνητή στο ιατρικό τους ιστορικό. Έπειτα, μέσω της κρυπτοοικονομίας που μπορεί να υποστηρίξει μία εφαρμογή βασισμένη στην τεχνολογία Blockchain μπορούν για πρώτη φορά να αξιοποιήσουν τα ιατρικά τους δεδομένα, κερδίζοντας ηλεκτρονικά νομίσματα, τα οποία και μπορούν να

[77] Blockchain in Heathcare: Opportunities, Challenges and Applications: https://hackernoon.com/blockchain-in-healthcare-opportunities-challenges-and-applications-d6b286da6e1f

αξιοποιήσουν μελλοντικά στον τομέα της υγειονομικής τους περίθαλψης. Παράλληλα, γλυτώνουν πολύ χρόνο στην αναζήτηση ενός γιατρού που θα καλύπτει τις ανάγκες τους, καθώς μέσω τις εφαρμογής η αναζήτηση αυτή θα είναι πολύ πιο απλή αλλά και πιο αποτελεσματική αφού θα έχουν μία μεγαλύτερη γκάμα επιλογών. Τέλος, επειδή η εφαρμογή μπορεί να υποστηρίξει άμεση ηλεκτρονική επικοινωνία μεταξύ γιατρού και ασθενή, θα μπορούν οι ασθενείς να γλυτώσουν χρόνο για να κάνουν ορισμένες διαδικαστικού περιεχομένου ερωτήσεις ή ακόμα και να έχουν μία γρήγορη πρώτη διάγνωση για το πρόβλημα υγείας που αντιμετωπίζουν.

- **Οφέλη για γιατρούς, κλινικές**

Οι γιατροί με την σειρά τους μπορούν να έρθουν πολύ πιο εύκολα σε επαφή με έναν ασθενή. Μέσω της ηλεκτρονικής επικοινωνίας με τους ασθενείς, θα μπορούσαν μέσα σε πολύ λιγότερο χρόνο να εξυπηρετήσουν περισσότερους ασθενείς δίνοντάς τους κάποιες γρήγορες οδηγίες, δημιουργώντας έτσι τις κατάλληλες συνθήκες και για την αύξηση των κερδών τους. Οι γιατροί επίσης μέσω της πρόσβασης που θα μπορούσαν να πάρουν από τον εκάστοτε ασθενή στα προσωπικά του ιατρικά δεδομένα, επωφελούνται από άποψη χρόνου αφού πλέον θα έχουν πρόσβαση σε παλιότερες εξετάσεις που δεν θα χρειαστεί να επαναλάβουν και θα σχηματίζουν μία ιατρική διάγνωση μέσα σε αισθητά μικρότερο χρονικό διάστημα. Επίσης, οι κλινικές οι οποίες δραστηριοποιούνται στον τομέα της υγειονομικής περίθαλψης θα μπορούν μέσω της εφαρμογής να έρθουν εύκολα σε επαφή με ερευνητές και έχοντας τη σύμφωνη γνώμη του ασθενή να προωθήσουν κάποια ιατρικά αποτελέσματα.

- **Οφέλη για ερευνητές**

Οι ερευνητές μέσω της εφαρμογής μπορούν εύκολα να έρθουν σε επαφή με πληθώρα ασθενών αλλά και πολλές φορές ακόμα και οι ίδιοι οι ασθενείς να αναζητήσουν ερευνητές για κάποια πιθανή συνεργασία μεταξύ των δύο πλευρών. Η αξιοποίηση των ιατρικών δεδομένων και του ιατρικού ιστορικού των ασθενών από τους ερευνητές θα γίνεται με αντάλλαγμα έναν αριθμό ηλεκτρονικών νομισμάτων. Μία τέτοια συνεργασία θα έκανε ακόμα πιο εύκολη την δουλειά των ερευνητών καθώς η κύρια ασχολία τους θα είναι η αξιοποίηση των ιατρικών δεδομένων, χωρίς να χρονοτριβούν κατά τη διαδικασία λήψης των δεδομένων που χρειάζονται. Σύμμαχός τους σε αυτή την προσπάθεια είναι η τεχνολογία Blockchain, η οποία προσφέρει δικλείδα ασφαλείας στους ασθενείς ότι τα προσωπικά τους δεδομένα δεν θα μπορούν να αξιοποιηθούν από τρίτους παρά μόνο για τον σκοπό για τον οποίο συμφώνησαν με τους ερευνητές, ενώ με αυτό τον τρόπο θα μπορούν πολύ πιο εύκολα οι ερευνητές να προσελκύσουν ασθενείς ώστε να λάβουν μέρος σε ερευνητικά προγράμματα. Τέλος, οι ερευνητές θα μπορούν να έρθουν εύκολα σε επαφή με κλινικές και φαρμακευτικές εταιρίες με τις οποίες θα μπορούσαν να συνεργαστούν αξιοποιώντας έτσι την έρευνα την οποία έχουν εκπονήσει.

6 Λειτουργικές Απαιτήσεις μίας Blockchain Εφαρμογής στην Υγεία

6.1 Εισαγωγή

Η υγειονομική περίθαλψη είναι ένας τομέας που καλείται να διαχειριστεί μεγάλη ποσότητα δεδομένων. Η αποθήκευση και η διάδοση αυτού του μεγάλου αριθμού δεδομένων είναι ζωτικής σημασίας λόγω της ευαίσθητης φύσης τους και παραγόντων, όπως είναι η ασφάλεια και η προστασία της ιδιωτικής ζωής των ασθενών. [75]

Στον τομέα της υγειονομικής περίθαλψης και των κλινικών ρυθμίσεων, η ασφαλής και κλιμακούμενη ανταλλαγή δεδομένων είναι επιτακτική για τη διάγνωση, καθώς και για τη συνδυασμένη λήψη κλινικών αποφάσεων. Η πρακτική κοινής χρήσης δεδομένων είναι πολύ σημαντική για να μπορέσουν οι γιατροί να μεταφέρουν τα κλινικά δεδομένα των ασθενών τους στην αρμόδια αρχή για γρήγορη παρακολούθηση. Οι γιατροί θα πρέπει να μπορούν να μεταφέρουν τα κλινικά δεδομένα των ασθενών τους με ασφαλή και έγκαιρο τρόπο, ώστε να διασφαλίζεται ότι και τα δύο μέρη θα έχουν πλήρεις και ενημερωμένες πληροφορίες σχετικά με το ιατρικό ιστορικό των ασθενών.

Από την άλλη πλευρά, η τηλεϊατρική και η ηλεκτρονική υγεία είναι δύο εξελίξιμοι τομείς, όπου τα κλινικά δεδομένα μεταφέρονται εξ' αποστάσεως σε έναν ειδικό (σε μια απομακρυσμένη τοποθεσία) για μια γνώμη εμπειρογνώμονα. Σε αυτές τις δύο online κλινικές ρυθμίσεις, τα δεδομένα του ασθενούς μεταφέρονται είτε μέσω μιας «τεχνολογίας αποθήκευσης και προώθησης» είτε με τη βοήθεια διαδικτυακής κλινικής παρακολούθησης σε πραγματικό χρόνο (π.χ. τηλε-παρακολούθηση, τηλεμετρία κτλ) [76], [77]. Χρησιμοποιώντας αυτές τις διαδικτυακές εφαρμογές, οι ασθενείς μπορούν να διαγνωσθούν από απόσταση μέσω ανταλλαγής κλινικών δεδομένων. Σε όλες αυτές τις εφαρμογές, η ασφάλεια, η ευαισθησία και η ιδιωτικότητα των κλινικών δεδομένων αποτελούν μερικές από τις μείζονες προκλήσεις. Έτσι, η δυνατότητα ανταλλαγής δεδομένων με ασφάλεια και κλιμάκωση είναι πολύ σημαντική για την υποστήριξη της επικοινωνίας, όσον αφορά την απομακρυσμένη παρακολούθηση ασθενών. [78]

6.2 Λειτουργικές Απαιτήσεις

Στόχος αυτού του κεφαλαίου είναι να περιγραφούν οι λειτουργικές απαιτήσεις που απαιτείται να διαθέτει μία εφαρμογή υγειονομικής περίθαλψης βασισμένη στη Blockchain τεχνολογία, ούτως ώστε να έχει την δυνατότητα καταγραφής ιατρικών δεδομένων ασθενών και παρακολούθησής τους από εξουσιοδοτημένους γιατρούς. Ο καθορισμός των λειτουργικών απαιτήσεων στηρίχθηκε στην περιγραφή των σεναρίων χρήσεως μιας εφαρμογής στην υγειονομική περίθαλψη που περιγράφηκαν στο προηγούμενο κεφάλαιο.

Διαλειτουργικότητα

Αυτή είναι μία από τις βασικές απαιτήσεις για τα συστήματα που βασίζονται στην τεχνολογία Blockchain. Το συγκεκριμένο σύστημα υγειονομικής περίθαλψης θα πρέπει να υποστηρίζει τη διαλειτουργικότητα τουλάχιστον σε πανελλαδικό επίπεδο. Ένας από τους κύριους λόγους έλλειψης διαλειτουργικότητας στα τρέχοντα συστήματα είναι η έλλειψη καθολικών προτύπων. Το Blockchain θα μπορούσε να ενδυναμώσει τη διαλειτουργικότητα του ΗΦΥ για τα τρέχοντα συστήματα υγειονομικής περίθαλψης. Η τεχνολογία Blockchain παρέχει μηχανισμό για ανώνυμα δεδομένα και διασφαλίζει ότι αυτά δεν μπορούν να αλλοιωθούν. Το Blockchain χρησιμοποιεί κρυπτογράφηση δημόσιου κλειδιού για να δημιουργήσει αρχεία που είναι χρονοσφραγισμένα και αμετάβλητα. Αντίγραφα αυτών των αρχείων δεδομένων αποθηκεύονται σε χιλιάδες κόμβους σε ψηφιακό δίκτυο μέσω ενός Blockchain ledger στον οποίο έχουν πρόσβαση όλα τα μέλη-κομβοι του συστήματος. Η αλλαγή αυτών των εγγραφών σε κάθε κόμβο καθίσταται ένα αδύνατο έργο και απαγορευτικά δαπανηρό, καθιστώντας με αυτό τον τρόπο τα αρχεία αξιόπιστα. Το δίκτυο εμπιστοσύνης που δημιουργείται με αυτόν τον τρόπο είναι ένα από τα πιο ελκυστικά χαρακτηριστικά αυτής της τεχνολογίας. Πρέπει να σημειωθεί ότι το Blockchain δεν αντιμετωπίζει τις βασικές απαιτήσεις διαλειτουργικότητας, αλλά παρέχει τη βάση για ένα ασφαλές και έγκυρο πλαίσιο ανταλλαγής δεδομένων όπου ενοποιημένα πρότυπα μπορούν να συνδεθούν.

Ασφάλεια Δεδομένων

Μια άλλη σημαντική προϋπόθεση κατά το σχεδιασμό τέτοιων συστημάτων υγειονομικής περίθαλψης βασισμένα στη τεχνολογία Blockchain είναι η ασφάλεια των ευαίσθητων δεδομένων των ασθενών. Οι πολλαπλές οντότητες που εμπλέκονται στους μηχανισμούς υγειονομικής περίθαλψης που βασίζονται σε Blockchain έχουν ως προτεραιότητα τη διασφάλιση της ασφάλειας των ευαίσθητων ιατρικών δεδομένων. Το Blockchain αναμένεται να εξασφαλίσει μεγαλύτερη ασφάλεια, ιδιωτικότητα και εμπιστοσύνη σε σύγκριση με τα παραδοσιακά συστήματα υγειονομικής περίθαλψης. [79], [80], [81].

Οι ασθενείς, χρήστες μίας Blockchain εφαρμογής θα είναι σε θέση, μέσω της σύνδεσης στον λογαριασμό τους όχι μόνο να έχουν την εποπτεία του ιατρικού τους

ιστορικού αλλά και να εγκρίνουν ή να αρνούνται οποιαδήποτε διανομή ή αλλαγή στα δεδομένα τους, συμβάλλοντας στην εξασφάλιση υψηλότερου επιπέδου προστασίας της ιδιωτικής ζωής τους.

Η σημαντική διαφορά σε σχέση με υπάρχοντα συστήματα είναι η δυνατότητα επικύρωσης. Οι ασθενείς και οι πάροχοι υγείας θα μπορούν να εμπιστεύονται ότι ο ΗΦΥ είναι ακριβής για τα αρχεία που μετακινούνται μεταξύ νοσοκομείων, κλινικών ή άλλων οργανισμών και θα γνωρίζουν επίσης ότι οι πληροφορίες έχουν υποβληθεί σε επικύρωση, γεγονός που αυξάνει την ασφάλεια και την εμπιστοσύνη. Επιπλέον, οι ασθενείς θα έχουν τη δυνατότητα να στείλουν την ενοποιημένη ιατρική τους πληροφορία σε έναν νέο ειδικό ή ακόμα και σε κάποιο συγγενικό-φιλικό τους πρόσωπο, προσθέτοντας τους απλώς στην αλυσίδα.

Μια άλλη σημαντική συνιστώσα για τους επαγγελματίες στον τομέα της ασφάλειας των δεδομένων υγείας είναι ο τρόπος με τον οποίο οι κανονισμοί που αφορούν τα ιατρικά δεδομένα θα μπορούσαν να εφαρμοστούν στην τεχνολογία Blockchain. Οι πληροφορίες για τους ασθενείς θα πρέπει να παραμείνουν ασφαλείς μέσω οποιασδήποτε διαδικασίας μεταφοράς δεδομένων, οπότε οι διάφοροι οργανισμοί θα πρέπει να εξετάσουν τις απαραίτητες φυσικές, τεχνικές ή διοικητικές διασφαλίσεις που ίσως χρειαστεί να εφαρμοστούν. Για παράδειγμα, η κρυπτογράφηση δεδομένων μπορεί να είναι απαραίτητη για αυτή τη διαδικασία. Επομένως, οι ασθενείς θα πρέπει να γνωρίζουν ότι χρησιμοποιούνται τα κατάλληλα κρυπτογραφικά πρότυπα και οι σωστές κατευθυντήριες γραμμές.

Συνέπεια δεδομένων / ακεραιότητα / μεταλλαξιμότητα

Μία από τις προκλήσεις που αντιμετωπίζουν τα τρέχοντα συστήματα διαχείρισης της υγειονομικής περίθαλψης είναι ο κατακερματισμός και η ασυνέπεια των ιατρικών δεδομένων. Η ασυνέπεια των δεδομένων μπορεί να προκαλέσει καθυστέρηση και υψηλότερο κόστος για την ολοκλήρωση της συνολικής διαδικασίας υγειονομικής περίθαλψης για κάθε χρήστη. Επομένως, ένα σύστημα υγειονομικής περίθαλψης που βασίζεται σε Blockchain τεχνολογία πρέπει να εξασφαλίζει ότι τα δεδομένα της υγειονομικής περίθαλψης είναι συνεπή και να καταστήσει ανέφικτη την οποιαδήποτε τροποποίηση τους από μη εξουσιοδοτημένες οντότητες. [80], [81]

Πολυπλοκότητα και Κρυπτονόμισμα

Τα τρέχοντα συστήματα υγειονομικής περίθαλψης είναι σχετικά πιο σύνθετα από την άποψη της αποθήκευσης, της ανταλλαγής και της επεξεργασίας των ιατρικών δεδομένων και άλλων πληροφοριών. Ως εκ τούτου, μία από τις απαιτήσεις για ένα Blockchain σύστημα υγειονομικής περίθαλψης είναι να έχουν λιγότερο σύνθετες λειτουργίες για την αποφυγή περίπλοκων και περιττών καθυστερήσεων σε διάφορες φάσεις [82]. Αξίζει να σημειωθεί ότι οι διαδικασίες που πραγματοποιούνται από προγραμματιστικής απόψεως είναι σαφώς πιο πολύπλοκες σε σχέση με τα παραδοσιακά συστήματα. Ωστόσο, αυτό μεταφράζεται σε ευκολότερες διαδικασίες στις οθόνες που θα διαχειρίζεται ο ασθενής σε μία τέτοια εφαρμογή.

Επίσης η παρουσία ενός κρυπτονομίσματος σε μία Blockchain εφαρμογή στον τομέα της υγειονομικής περίθαλψης θα βοηθούσε πολύ στην πραγματοποίηση των συναλλαγών που θέλουν να πραγματοποιήσουν οι διάφορες οντότητες. Στο προηγούμενο κεφάλαιο περιγράφηκαν αναλυτικά με ποιο τρόπο θα μπορούσαν να γίνουν συναλλαγές έναντι αμοιβής με κρυπτονομίσματα.

Αποτελεσματικότητα κόστους / πόρων

Τα τρέχοντα συστήματα υγειονομικής περίθαλψης καταναλώνουν περισσότερους πόρους όσον αφορά το κόστος, τους υπολογισμούς, το χρόνο κτλ. Για παράδειγμα, στις περισσότερες συναλλαγές, πρέπει να υπάρχουν διαμεσολαβητές που προσθέτουν μεγαλύτερη καθυστέρηση για την εκτέλεση των συγκεκριμένων λειτουργιών [82]. Μία από τις βασικές απαιτήσεις μίας Blockchain εφαρμογής είναι η μείωση του κόστους συναλλαγών / καθυστέρησης. Κάθε συναλλαγή που θα γίνεται στην Blockchain εφαρμογή χρειάζεται να "πιστοποιηθεί" από κάποιο κόμβο του συστήματος, διαδικασία γνωστή και ως data mining, με σκοπό την επίτευξη consensus στην αλυσίδα. Στη συγκεκριμένη περίπτωση αυτή η διαδικασία πραγματοποιείται από τους ίδιους τους κόμβους του συστήματος. Οποιοσδήποτε χρήστης θα έχει την δυνατότητα να είναι και miner του συστήματος και να ανταμείβεται αντίστοιχα για αυτό είτε με κάποιο αριθμό κρυπτονομισμάτων είτε ακόμα και με ανταλλαγή ιατρικών δεδομένων (σε περίπτωση που είναι ερευνητής ή πάροχος υγείας).

Επεκτασιμότητα

Ένα κατανεμημένο Blockchain που περιέχει αρχεία υγείας, έγγραφα και άλλες σχετικές πληροφορίες θα έχει περιορισμό στην αποθήκευση δεδομένων και στην απόδοση. Κάθε μέλος του κατανεμημένου δικτύου του Blockchain για την υγεία θα έχει αντίγραφο κάθε καταγραφής υγείας για κάθε άτομο που περιλαμβάνεται επίσης στο δίκτυο, όμως κάτι τέτοιο δεν θα ήταν πρακτικό από την άποψη της αποθήκευσης δεδομένων. Επειδή τα δεδομένα υγείας είναι δυναμικά, η αναπαραγωγή όλων των εγγραφών υγείας σε κάθε μέλος του δικτύου θα είναι συχνή, σπαταλώντας έτσι τους πόρους του δικτύου και προκαλώντας ανησυχίες σχετικά με τη διακίνηση δεδομένων. Σε αυτή την κατεύθυνση το Blockchain λειτουργεί ως διαχειριστής ελέγχου πρόσβασης για τα αρχεία υγείας και τα δεδομένα. Στην αποσυμφόρηση αυτού του μεγάλου όγκου δεδομένων θα βοηθούσε η δημιουργία μίας εφαρμογής με Ethereum Blockchain και η ύπαρξη μίας ανεξάρτητης κεντρικής βάσης δεδομένων.

1) Ethereum Blockchain

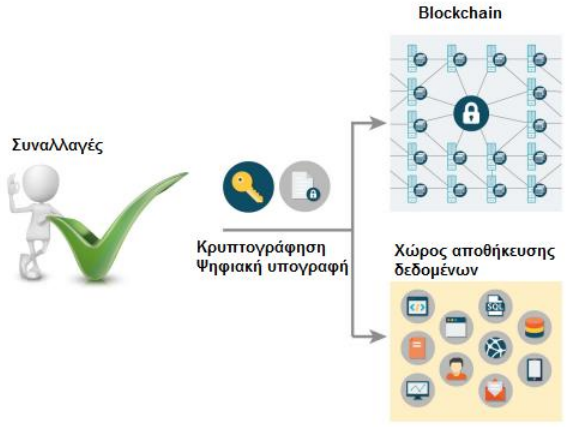
Αν η εφαρμογή χτιστεί μέσω Ethereum θα μπορεί να είναι επεκτάσιμη καθώς θα μπορεί κάθε χρήστης ή οργανισμός να αναπτύσσει τα δικά του Microservices πάνω στο Blockchain και να υπάρχουν τα κατάλληλα APIs για επικοινωνία του Blockchain με αυτές τις εφαρμογές και τα δημόσια αποθετήρια ιατρικών πληροφοριών.

2) Κεντρική Βάση εκτός Blockchain

Οι πληροφορίες που περιέχονται στη προτεινόμενη Blockchain εφαρμογή για την υγεία θα είναι ένας δείκτης-διεύθυνση σε μία λίστα που περιέχει όλους τους ΗΦΥ και τα δεδομένων υγείας των χρηστών. Οι συναλλαγές στα μπλοκ θα περιέχουν ένα μοναδικό αναγνωριστικό πεδίο χρήστη (π.χ. το id), ένα κρυπτογραφημένο σύνδεσμο με το αρχείο υγείας και ένα χρονικό σήμα για τη στιγμή της δημιουργίας της συναλλαγής. Για να βελτιωθεί η αποτελεσματικότητα της πρόσβασης στα δεδομένα, η συναλλαγή μπορεί να περιέχει επίσης τον τύπο των δεδομένων που περιέχονται στο αρχείο υγείας καθώς και άλλα μεταδεδομένα που θα διευκόλυναν τα συχνά χρησιμοποιούμενα queries.

Όλα τα ιατρικά δεδομένα θα αποθηκεύονται εκτός Blockchain σε ένα χώρο αποθήκευσης δεδομένων. Αυτοί οι χώροι αποθήκευσης δεδομένων είναι κλιμακούμενοι και μπορούν να αποθηκεύσουν μια μεγάλη ποικιλία δεδομένων. Οι πληροφορίες που αποθηκεύονται στους χώρους δεδομένων θα κρυπτογραφηθούν και θα υπογραφούν ψηφιακά για να διασφαλιστεί η ιδιωτικότητα και η αυθεντικότητα των πληροφοριών. Επιπλέον, η τεχνολογία Blockchain θα χρησιμοποιείται για την πραγματοποίηση των συναλλαγών στο δίκτυο και την επικύρωση των αδειών πρόσβασης, αναγκαίων για την ανάλυση δεδομένων και την μηχανική μάθηση.

Συγκεκριμένα, όταν ένας πάροχος υγειονομικής περίθαλψης δημιουργεί ένα ιατρικό αρχείο (συνταγή, εργαστηριακό τεστ, αποτέλεσμα έρευνας), θα δημιουργηθεί και μία ψηφιακή υπογραφή για την επαλήθευση της αυθεντικότητας του εγγράφου. Τα δεδομένα υγείας θα κρυπτογραφηθούν και θα αποσταλούν στο χώρο δεδομένων για αποθήκευση. Κάθε φορά που αποθηκεύονται πληροφορίες στο χώρο αποθήκευσης δεδομένων, ένας δείκτης στο αρχείο καταγραφής υγείας καταχωρείται στο Blockchain μαζί με το μοναδικό αναγνωριστικό του χρήστη. Ο ασθενής ενημερώνεται ότι τα δεδομένα υγείας έχουν προστεθεί στο Blockchain του. Με τον ίδιο τρόπο ένας ασθενής θα μπορεί να προσθέσει δεδομένα υγείας με ψηφιακές υπογραφές και κρυπτογράφηση από κινητές εφαρμογές και φορητούς αισθητήρες. [83]



Εικόνα 31: Δομή της Blockchain εφαρμογής

Smart Contracts

Για να θεωρείται μια συναλλαγή έγκυρη στο Blockchain θα πρέπει να υπογραφεί ένα Smart Contract. Στη πραγματικότητα με τον όρο “υπογραφεί” εννοούμε την διαδικασία που ενώνει μια συναλλαγή με το ιδιωτικό κλειδί του χρήστη και μπορεί να διαβαστεί μόνο από το δημόσιο κλειδί. Οι ψηφιακές υπογραφές χρησιμοποιούν συνδυασμό μιας κρυπτογραφικής συνάρτησης κατατεμαχισμού (hash function) για δημιουργία της σύνοψης (hash) σε συνδυασμό με ασυμμετρική κρυπτογραφία για κρυπτογράφηση/αποκρυπτογράφηση σύνοψης (ο συνδυασμός σύνοψης και κρυπτογράφησης με ασυμμετρική κρυπτογραφία αποδεικνύει την ακεραιότητας της συναλλαγής αλλά και την απόδειξη ταυτότητας του αποστολέα).

Παρακάτω περιγράφονται τα τρία διαφορετικά Smart Contracts που προτείνεται να υποστηρίζει μία εφαρμογή blockchain στον τομέα της υγείας.

Register Contract (RC) Σύμβαση Μητρώου

Αυτό το Smart Contract ενεργεί ως μητρώο όλων των χρηστών του συστήματος. Οι χρήστες θα χωρίζονται σε πέντε διαφορετικές κατηγορίες-οντότητες, δηλαδή (i) Ασθενείς, (ii) Γιατροί, (iii) Ερευνητές, (iv) Φαρμακεία ή (v) Άλλοι Πάροχοι Υγείας. Το RC περιέχει μια αντιστοίχιση ενός χρήστη του συστήματος μέσω του μοναδικού αναγνωριστικού πεδίου του (π.χ. id) με μια μοναδική διεύθυνση smart contract που ονομάζεται Data Contract (DC) και αντιστοιχεί σε δεδομένα. Αυτό το μοναδικό αναγνωριστικό πεδίο θα πρέπει να είναι μοναδικό ανά χρήστη και να μην μπορεί να αποκαλύψει την ταυτότητά του.

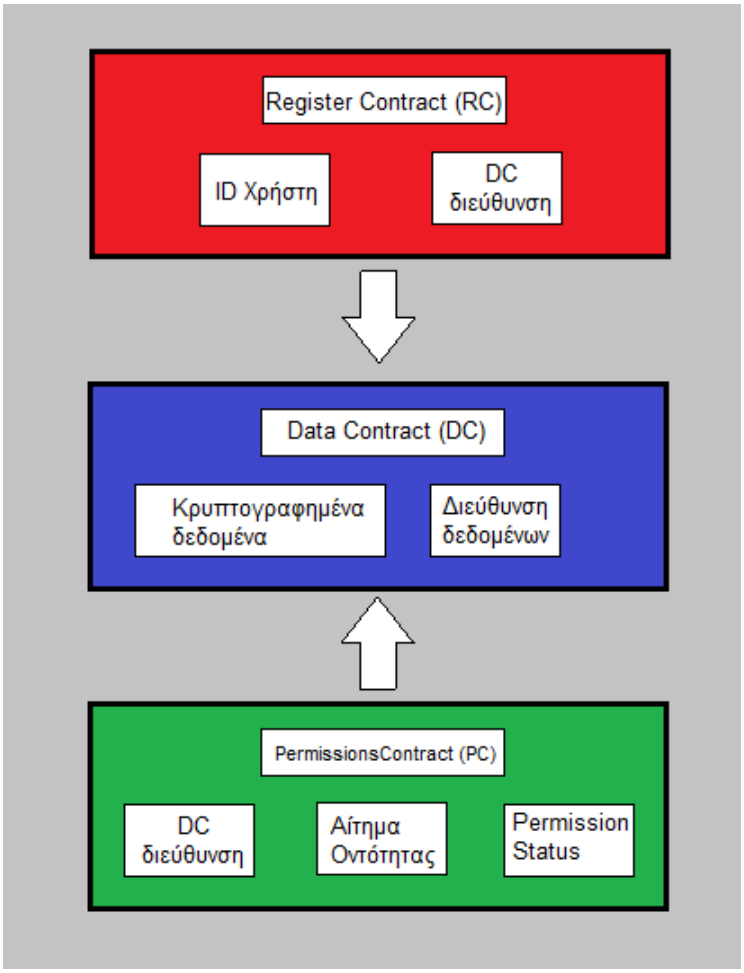
Data Contract (DC) Σύμβαση Δεδομένων

Αυτό το smart Contract είναι μοναδικό για κάθε χρήστη και περιέχει τα κρυπτογραφημένα ιατρικά δεδομένα του μαζί με μια διεύθυνση για το που βρίσκονται. Χρησιμοποιείται ένα κρυπτογραφημένο αντίγραφο των δεδομένων προκειμένου οι οντότητες που επιθυμούν πρόσβαση στα δεδομένα να είναι σε θέση να επαληθεύσουν την ακεραιότητα τους, αντιμετωπίζοντας έτσι παράλληλα το μοντέλο απειλών διαχειριστή κακόβουλων δεδομένων.

Permissions Contract (PC) Σύμβαση Αδειών

Αυτό το Smart Contract αφορά τη διαχείριση δικαιωμάτων των δεδομένων των χρηστών. Συγκεκριμένα, περιέχει μια αντιστοίχιση της διεύθυνσης της σύμβασης δεδομένων (DC) ενός χρήστη με κάποιον άλλο χρήστη. Αυτά τα smart contracts προσδιορίζονται με μοναδικό τρόπο μέσω ενός πεδίο που ονομάζεται "Status" το οποίο περιέχει το είδος της έγκριση-πρόσβασης που δίνει ο ιδιοκτήτης των εκάστοτε δεδομένων σε κάποιον άλλο χρήστη.

Οι έξυπνες συμβάσεις του συστήματος μαζί με τα δεδομένα που περιέχουν και τις σχέσεις υψηλού επιπέδου μεταξύ τους απεικονίζονται στη παρακάτω εικόνα.



Εικόνα 32: Smart Contracts με τα δεδομένα τους και τις μεταξύ τους συσχετίσεις

Βασικές Λειτουργίες Συστήματος

• Οι χρήστες μπορούν να εγγράφονται στην εφαρμογή.

• Οι χρήστες μπορούν να συνδέονται στην εφαρμογή.

• Οι χρήστες μπορούν να αποσυνδέονται από την εφαρμογή.

• Οι γιατροί, οι άλλοι πάροχοι και οι ερευνητές μπορούν να ζητήσουν δικαιώματα από τους ασθενείς για συγκεκριμένες ενέργειες που αφορούν το προσωπικό του ιατρικό φάκελο.

• Οι ασθενείς μπορούν να εξουσιοδοτήσουν γιατρούς με διάφορα δικαιώματα για να αλληλεπιδράσουν με τα ιατρικά τους αρχεία.

• Οι ασθενείς μπορούν να εξουσιοδοτήσουν ερευνητές και άλλους ασθενείς για εποπτεία των ιατρικών τους αρχείων για ερευνητικούς σκοπούς.

• Τα φαρμακεία και οι άλλοι πάροχοι μπορούν να ζητήσουν δικαιώματα από τους ερευνητές για αξιοποίηση της ερευνάς τους.

• Οι ερευνητές μπορούν να εξουσιοδοτήσουν φαρμακεία και άλλους παρόχους υγείας για εποπτεία της έρευνάς τους.

• Δίνεται η δυνατότητα στον χρήστη να αλλάξει τα δικαιώματα που έχει δώσει σε κάποιον άλλο χρήστη.

• Μπορούν να πραγματοποιηθούν συναλλαγές έναντι κάποιου αριθμού κρυπτονισμάτων.

• Μπορούν να πραγματοποιηθούν συναλλαγές έναντι ιατρικών δεδομένων.

• Δυνατότητα προβολής Ιστορικού των διαφόρων συναλλαγών.

6.3 Μελλοντικές Προοπτικές και Συμπεράσματα

Κάποια πεδία μελλοντικής έρευνας είναι η δημιουργία ενός νομικού πλαισίου γύρω από την λειτουργία της τεχνολογίας Blockchain και την αξιοποίησή της. Η δημιουργία σωστών πρακτικών υλοποίησης Blockchain δικτύων και κατ' επέκταση εφαρμογών που να αποθηκεύουν την ιατρική πληροφορία μέσα στο Blockchain με τρόπο γρήγορο και αποδοτικό αλλά και που θα επιτρέπει παράλληλα στον χρήστη να διατηρεί τα θεμελιώδη δικαιώματά του, όπως αυτό της διαγραφής των ευαίσθητων προσωπικών του δεδομένων.

Συνολικά, η εφαρμογή της τεχνολογίας Blockchain στον ιατρικό κλάδο μπορεί να προσφέρει πολλά πλεονεκτήματα. Ο τρόπος με τον οποίο το διαδίκτυο επέφερε επανάσταση στην υγειονομική περίθαλψη και εισήγαγε την τηλεϊατρική, πρέπει να εκμεταλλευτεί την τεχνολογία blockchain, ώστε να οδηγήσει την ιατρική επιστήμη στο επόμενο επίπεδο στο μέλλον μειώνοντας το κόστος παρακολούθησης, διαμόρφωσης και διαχείρισης των ιατρικών δεδομένων. Η χρήση Blockchain σε κλινικά πλαίσια θα μειώσει δραστικά τον χρόνο επεξεργασίας, επειδή μόλις ένας ασθενής εγγράφεται σε μια μελέτη, η πλήρης συλλογή δεδομένων θα είναι διαθέσιμη ταυτόχρονα, λόγω της διαθεσιμότητας του κατανεμημένου βιβλίου.

Οι γιατροί δεν θα πρέπει να ανησυχούν για τον ασθενή, δίνοντάς του ένα ειλικρινές ιατρικό ιστορικό, λόγω της ικανότητάς τους να βλέπουν τα πρωτότυπα και αυθεντικά δεδομένα σε πραγματικό χρόνο μειώνοντας πιθανά λάθη ιατρικού ιστορικού. Ομοίως, οι ασθενείς δεν θα πρέπει να ανησυχούν για τη λήψη μιας δεύτερης γνώμης από άλλο γιατρό, λόγω της διαφάνειας των δεδομένων. Οι ασθενείς θα έχουν πλήρη αυτονομία στα δεδομένα τους και θα αποφασίζουν με ποιον θα διαχειριστούν.

7 Βιβλιογραφία

[1] Βαλσαμά Μαρία (April 2005), "Ηλεκτρονικός Φάκελος Υγείας"

[2] Hunter, K. M. (2002), " Electronic Health Records. In S. P. Englebardt and R. Nelson (Eds), Health Care Informatics, An Interdisciplinary Approach" (Copyright ed. , pp. 209-230), St Louis (Missouri, USA): Mosby

[3] Healthcare Information and Management Systems Society (5 April 2015), "Electronic Health Records"

[4] IOM, Key Capabilities of an Electronic Health Record System, 2003

[5] Katehakis, D.G. and M. Tsiknakis, Electronic Health Record, in Wiley Encyclopedia of Biomedical Engineering (6-Volume Set), Metin Akay (Editor), John Wiley & Sons, Inc., ISBN: 0- 471-24967-X, May 2006.

[6] Richard S. Dick, Elaine B. Steen, (25 October 1991), "An Essential Technology for Health Care"

[7] Wikipedia (2013), "Ηλεκτρονικός ιατρικός φάκελος ασθενή"

[8] Μ.Τσίπουρας, Α. Τζάλλας, Ε. Καρβούνης, Ν. Γιαννακέας, "Ιατρική Πληροφορική"

[9] Α. Κουρούμπαλη, Δ. Γ. Κατεχάκης, Α. Μπέρλερ, Μ. Τσικνάκης, (20 July 2012), " ΗΛΕΚΤΡΟΝΙΚΟΣ ΦΑΚΕΛΟΣ ΥΓΕΙΑΣ: ΠΡΟΤΑΣΗ ΕΦΑΡΜΟΓΗΣ ΣΤΟΥΣ ΦΟΡΕΙΣ ΤΟΥ ΕΘΝΙΚΟΥ ΣΥΣΤΗΜΑΤΟΣ ΥΓΕΙΑΣ "

[10] Δ. Δελλής, (November 2007), "ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ"

[11] Council of the European Union, (11 June 2015), "Presidency of the Council: Compromise text. Several partial general approaches have been instrumental in converging views in Council on the proposal for a General Data Protection Regulation in its entirety. The text on the Regulation which the Presidency submits for approval as a General Approach appears in annex."

[12] ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2016/679 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ (27 April 2016)

[13] ΝΟΜΟΣ 2472/1997 ΠΡΟΣΤΑΣΙΑ ΤΟΥ ΑΤΟΜΟΥ ΑΠΟ ΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ ΜΕ ΕΝΣΩΜΑΤΩΜΕΝΕΣ ΤΙΣ ΤΡΟΠΟΠΟΙΗΣΕΙΣ

[14] Patrick McCallum (21 November 2017), "Individuals' Rights"

[15] ΟΔΗΓΙΑ 2011/24/ΕΕ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ (9 March 2011)

[16] Nextdeal, (9 May 2018), "Νομοθεσία ποσωπικών δεδομένων και γιατροί. Όσα πρέπει να γνωρίζουν"

[17] Michael Filmin (29 March 2018), "Five Benefits GDPR Compliance Will Bring To Your Business"]

[18] Andrada Coos (1 February 2018), "GDPR: The Pros and The Cons"

[19] Satoshi Nakamoto ," Bitcoin: A Peer-to-Peer Electronic Cash System"

[20] L. Luu, D.-H. Chu, H. Olickel, P. Saxena (2016), " A. Hobor, Making Smart Contracts Smarter"

[21] K. Christidis, M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things, IEEE Access"

[22] H. Yin, D. Guo, K. Wang, Z. Jiang, Y. Lyu, J. Xing (2018), "Hyperconnected network: A decentralized trusted computing and networking paradigm"

[23] Y. Lu (2018), "Blockchain and the related issues: a review of current research topics, J. of Manag. Analytics"

[24] Catalini, Christian, Gans, Joshua S. (21 September 2017), "Some Simple Economics of the Blockchain"

[25] Κουτάκης Κωνσταντίνος (October 2018), "Επισκόπηση και Συγκριτική Μελέτη Πλεονεκτημάτων και Μειονεκτημάτων της εφαρμογής της τεχνολογίας Blockchain στο χώρο της Υγείας"

[26] Tai Mino (23 December 2018), "Digital Signatures in a Blockchain: Digital Signtures-Part 3"

[27] The Economist (31 October 2015), "Blockchains: The great chain of being sure about things"

[28] Bhaskar, Nirupama Devi, David LEE Kuo (2015), "Bitcoin Mining Technology"

[29] Blair Marshall (2 February 2018), "How are transactions validated?"

[30] Jerry Brito, Andrea Castillo (2013), "Bitcoin: A Primer for Policymakers"

[31] I. C. Lin, T. C. Liao (2017), “A survey of blockchain security issues and challenges”

[32] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, E. W. Felten, Sok (2015): “Research Perspectives and Challenges for Bitcoin and Cryptocurrencies”

[33] G. O. Karame, E. Androulaki and S. Capkun (2012), “Double-spending fast payments in bitcoin”

[34] J. Yli-Huumo, D. Ko, S. Choi, S. Park, K. Smolander (2016), “Where is current research on blockchain technology?”

[35] G. O. Karame, E. Androulaki, S. Capkun (2012), “Double-spending fast payments in bitcoin”

[36] Στυλιανός Αρακλιώτης, “Ανάπτυξη Πλατφόρμας βασισμένη σε τεχνολογία Blockchain, για ασφαλή διαχείριση ιατρικών δεδομένων”

[37] Κωνσταντίνος Λογαράς (21 June 2018), “Η τεχνολογία Blockchain, οι εφαρμογές της και οι νομικές πτυχές της”

[38] KG Law Firm (December 2018), “Blockchain & Γενικός Κανονισμός Προστασίας Δεδομένων(GDPR)”

[39] Buterin Vitalik (2013), “A Next-Generation Smart Contract and Decentralized Application Platform’”

[40] Στυλιανός Αρακλιώτης, “Ανάπτυξη Πλατφόρμας βασισμένη σε τεχνολογία Blockchain, για ασφαλή διαχείριση ιατρικών δεδομένων”

[41] Chrissa McFarlane, Michael Beer, Jesse Brown, Nelson Prendergast (May 2017), “Patientory: A Healthcare Peer-to-Peer EMR Storage Network v1.1”

[42] Mayo Clinic, “Changes in Burnout and Satisfaction With Work-Life Balance in Physicians and the General US Working Population Between 2011 and 2014”

[43] Ariel Ekblaw, Asaph Azaria, John D. Halamka, Lippman, MIT Media Lab, Beth Israel Deaconess Medical Center (August 2016), “A Case Study for Blockchain in Healthcare: “MedRec” prototype for electronic health records and medical research data”

[44] Alberto Malave (14 March 2018), “What will the Iryo platform look like”

[45] Iryo Network technical whitepaper, “:IRYO Global participatory healthcare ecosystem.”

[46] Bowhead Health (13 July 2017), “The Future of Digital Health”

[47] NKB Group (4 June 2018), “Docai Token Review”

[48] Walter De Brouwer and Mason Borda (7 September 2017), “NeuRoN: Decentralized Artificial Intelligence, Distributing Deep Learning to the Edge of the Network”

[49] P. Zhang, D. C. Schmidt, J. White, G. Lenz (2018), “Blockchain Technology Use Cases in Healthcare”

[50] M. Benchoufi, P. Ravaud (December 2017), “Blockchain technology for improving clinical research quality,”

[51] M. Roman-Belmonte, H. De la Corte-Rodriguez, E. C. RodriguezMerchan (May 2018), “How blockchain technology can change medicine”

[52] H. Rang (May 2013), “Bad Pharma: how drug companies mislead doctors and harm patients by Ben Goldacre”

[53] T. Aste, P. Tasca, T. D. Matteo (2017), “Blockchain technologies: The foreseeable impact on society and industry”

[54] R. Beck (2018), “Beyond bitcoin: The rise of blockchain world”

[55] M. Mettler (2016) “Blockchain technology in healthcare: The revolution starts here”

[56] Tanesh Kumar, Vidhya Ramani, Ijaz Ahmad, An Braeken, Erkki Harjula, Mika Ylianttila (2018), “Blockchain Utilization in Healthcare: Key Requirements and Challenges”

[57] S. B. Baker, W. Xiang, I. Atkinson (2017) “Internet of things for smart healthcare: Technologies, challenges, and opportunities”

[58] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, A. Gurtov (March 2018), ”Overview of 5G Security Challenges and Solutions,”

[59] T. Kumar, M. Liyanage, I. Ahmad (2018), “User privacy, identity and trust in 5G. In: A Comprehensive Guide to 5G Security”

[60] K.Peterson, Kevin (2016), ”A blockchain-based approach to health information exchange networks”

[61] Azaria A, Ekblaw A, Vieira T, Lippman A. (2016), “MedRec: using blockchain for medical data access and permission management”

[62] T. Kumar, A. Braeken, M. Liyanage and M. Ylianttila (2017), ”Identity privacy preserving biometric based authentication scheme for Naked healthcare environment”

[63] T. Kumar, M. Liyanage, A. Braeken, I. Ahmad and M. Ylianttila (2017), ”From gadget to gadget-free hyperconnected world: Conceptual analysis of user privacy challenges”

[64] C. Esposito, A. De Santis, G. Tortora, H. Chang, K. K. R. Choo (2018), ”Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?”

[65] Peng Zhang, Michael A. Walker, Jules White, Douglas C. Schmidt (2017), “Metrics for Assessing Blockchain-based Healthcare Decentralized Apps”

[66] Yue, X., Wang, H., Jin, D., Li, M.,Jiang (2016), “Healthcare data gateways: found healthcare intelligence on Blockchain with novel privacy risk control”

[67] Yli-Huumo, J., Ko, D., Choi, S., Park, S., Smolander, K. (2016), “Where is current research on blockchain technology?”

[68] B.H. Just, D. Marc, M. Munns, R. Sandefer (2016), “Why patient matching is a challenge: research on master patient index (MPI) data discrepancies in key identifying fields”

[69] RJ Krawiec, Dan Housman, Mark White, Mariya Filipova, Florian Quarre, Dan Barr, Allen Nesbitt, Kate Fedosova, Jason Killmeyer, Adam Israel, Lindsay Tsai (2016), “Blockchain : Opportunities for health care Deloitte”

[70] Maank Pratap (6 August 2016), “Blockchain in Healthcare: Opportunities, Challenges, and Applications”

[71] Kuo, Tsung-Ting, Hyeon-Eui Kim, and Lucila Ohno-Machado (2017), ”Blockchain distributed ledger technologies for biomedical and health care applications.”

[72] Clauson, Kevin A. (2018), ”Leveraging Blockchain Technology to Enhance Supply Chain Management in Healthcare.”

[73] Clauson, Engelhardt, Mark A. (2017),”Hitching healthcare to the chain: An introduction to blockchain technology in the healthcare sector.”

[74] Boulos, M. N. K., Wilson, J. T., Clauson, K. A. (2018), “Geospatial blockchain: promises, challenges, and scenarios in health and healthcare, International Journal of Health Geographics”

[75] Griebel L., Prokosch H.U., Köpcke F., Toddenroth D., Christoph J., Leb I., Engel I., Sedlmayr M. (2015), “A scoping review of cloud computing in healthcare”

[76] Houston M.S., Myers J.D., Levens S.P., McEvoy M.T., Smith S.A., Khandheria B.K., Shen W.K., Torchia M.E., Berry D.J. (1999), “Clinical consultations using store-and-forward telemedicine technology”

[77] Bhatti A., Siyal A.A., Mehdi A., Shah H., Kumar H., Bohyo M.A. (23 February 2018), "Development of cost-effective tele-monitoring system for remote area patients”

[78] Asad Ali Siyal, Aisha Zahid Junejo, Muhammad Zawish, Kainat Ahmed, Aiman Khalil, Georgia Soursou (2 January 2019), “Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives”

[79] M. Puppala, T. He, X. Yu, S. Chen, R. Ogunti, and S. T. C. (2016), “Wong,Data security and privacy management in healthcare applications andclinical data warehouse environment”

[80] Al Omar, A., Rahman, M. S., Basu, A., Kiyomoto, S. (2017), “Med-ibchain: A blockchain based privacy preserving platform for healthcaredata”

[81] G. Zyskind, O. Nathan and A. ’. Pentland (2015), ”Decentralizing Privacy:Using Blockchain to Protect Personal Data,”

[82] RJ Krawiec, Dan Housman, Mark White, Mariya Filipova, FlorianQuarre, Dan Barr, Allen Nesbitt, Kate Fedosova, Jason Killmeyer, AdamIsrael, Lindsay Tsai (2016), “Blockchain : Opportunities for health care Deloitte”

[83] Laure A. Linn, Martha B. Koo, M.D., “Blockchain For Health Data and Its Potential Use in Health IT and Health Care Related Research”