ARCHIVES OF HELLENIC MEDICINE: ISSN 11-05-3992

ΕΙΔΙΚΟ ΑΡΘΡΟ
SPECIAL ARTICLE

Μεθοδολογία ασφαλούς αποθήκευσης και διακίνησης ιατρικών δεδομένων με blockchain

ΑΡΧΕΙΑ ΕΛΛΗΝΙΚΗΣ ΙΑΤΡΙΚΗΣ 2020, 37(4):542–554
ARCHIVES OF HELLENIC MEDICINE 2020, 37(4):542–554

Χ. Κοντζίνος,[1]
Μ. Κοντούλης,[1]
Π. Καψάλης,[1]
Ο. Μαρκάκη,[1]
Σ. Μουζακίτης,[1]
Ρ. Μαντά,[2]
Θ. Ανδρούτσου,[2]
Ι. Κουρής,[2]
Χ. Καρανίκας,[3]
Α. Μπιλλήρης,[4]
Α. Χριστοδουλάκης,[4]
Ε. Θηραίος[5]

[1]Εργαστήριο Συστημάτων Αποφάσεων και Διοίκησης, Εθνικό Μετσόβιο Πολυτεχνείο, Αθήνα
[2]Εργαστήριο Βιοϊατρικής Τεχνολογίας, Εθνικό Μετσόβιο Πολυτεχνείο, Αθήνα
[3]Τμήμα Πληροφορικής με Εφαρμογές στη Βιοϊατρική, Πανεπιστήμιο Θεσσαλίας, Λαμία
[4]Datamed SA, Αθήνα
[5]Ιατρική Εταιρεία Αθηνών, Αθήνα

Οι ραγδαίες τεχνολογικές εξελίξεις του 21ου αιώνα και η διείσδυση του Internet 4.0 σε όλες τις εκφάνσεις της καθημερινότητας οδηγούν στην ψηφιοποίηση υπηρεσιών ακόμη και σε τομείς οι οποίοι παραδοσιακά λειτουργούσαν χωρίς τη βοήθεια της τεχνολογίας. Ένας από τους τομείς που έχει οδηγηθεί σε εκσυγχρονισμό λόγω των παραπάνω εξελίξεων είναι και αυτός της υγείας. Η αυτοματοποίηση ιατρικών διαδικασιών, η ρομποτική και οι ιατρικές συσκευές δημιουργούν πληθώρα ψηφιακών δεδομένων υγείας. Τα δεδομένα υγείας κάθε ασθενούς οργανώνονται και δομούνται σε ηλεκτρονικούς φακέλους υγείας (ΗΦΥ), οι οποίοι φυλάσσονται συνήθως σε κεντρικές βάσεις δεδομένων παρόχων υπηρεσιών υγείας. Αν και οι ΗΦΥ προσφέρουν πολλές δυνατότητες, η κεντρική φύλαξη αυτών τους κάνει ευάλωτους σε κακόβουλες επιθέσεις ενώ δεν προσφέρουν ιδιαίτερη διαλειτουργικότητα ανάμεσα σε συστήματα διαφορετικών παρόχων υγείας. Μια τεχνολογία η οποία παρέχει κατάλληλες λύσεις και μπορεί να εξαλείψει τα παραπάνω μειονεκτήματα είναι το blockchain. Η αποκεντρωμένη φύλαξη των δεδομένων και η διαχείρισή τους από τους ίδιους τους ασθενείς μπορεί να προσφέρει μεγαλύτερη ασφάλεια, διαλειτουργικότητα και γενικά περισσότερο αποδοτικές υπηρεσίες υγείας. Σκοπός της συγκεκριμένης έρευνας είναι η παρουσίαση των προβλημάτων που υπάρχουν στον χώρο της ηλεκτρονικής υγείας, η εισαγωγή του blockchain ως λύση για τα περισσότερα από αυτά, καθώς και η παρουσίαση κατάλληλης μεθοδολογίας που θα μπορούσε να χρησιμοποιηθεί για την αποθήκευση ιατρικών δεδομένων στο πλαίσιο μιας εφαρμογής υγείας βασισμένης σε blockchain. Η μεθοδολογία που θα παρουσιαστεί αναπτύσσεται ήδη και θα χρησιμοποιηθεί στο πλαίσιο του ερευνητικού έργου Impilo, το οποίο αποσκοπεί στην ανάπτυξη μιας εφαρμογής κοινωνικής δικτύωσης, η οποία θα στηρίζεται στο blockchain και θα εφαρμοστεί στον χώρο της υγείας.

Methodology for secure storage and information exchange of medical data based on blockchain

Abstract at the end of the article

Λέξεις ευρετηρίου

Ασφάλεια
Blockchain
Διαλειτουργικότητα
GDPR
Ηλεκτρονικός φάκελος υγείας
Ιατρικά δεδομένα

Υποβλήθηκε 23.12.2019
Εγκρίθηκε 27.2.2020

1. ΕΙΣΑΓΩΓΗ

Η ραγδαία ανάπτυξη των καινοτόμων τεχνολογιών Πληροφορικής έχει φέρει επανάσταση σε όλες τις εκφάνσεις της καθημερινότητας. Η αυτοματοποίηση και η εισαγωγή του Διαδικτύου των Πραγμάτων σε διάφορες διαδικασίες και τομείς της καθημερινότητας δημιουργούν πληθώρα ψηφιακών δεδομένων. Τα παραπάνω, σε συνδυασμό με τη ραγδαία αύξηση της χωρητικότητας των βάσεων δεδομένων και τις καινοτόμες τεχνολογίες αποθήκευσης και επεξεργασίας, δημιουργεί ευκαιρίες για ψηφιοποίηση σε διάφορους τομείς μέσα από την ανάπτυξη πληροφοριακών εφαρμογών. Ειδικά στην υγεία, η αυτοματοποίηση ιατρικών εξετάσεων, η ρομποτική και η αυτοδιάγνωση έχουν ήδη

οδηγήσει σε βελτιωμένη φροντίδα του πληθυσμού, στη δημιουργία καλύτερων εμπειριών για τους ασθενείς και για τους εργαζόμενους στον τομέα της υγείας και στην παραγωγή ιατρικών δεδομένων σε ψηφιακή μορφή. Ως ιατρικά δεδομένα ή δεδομένα υγείας χαρακτηρίζονται οποιαδήποτε δεδομένα είναι σχετικά με «τις συνθήκες υγείας, τα αποτελέσματα της αναπαραγωγικής διαδικασίας, τις αιτίες θανάτου και τη γενικότερη ποιότητα ζωής» για ένα άτομο ή μια πληθυσμιακή ομάδα.[1] Τα δεδομένα αυτά συλλέγονται όταν τα άτομα αλληλεπιδρούν με συστήματα υγειονομικής περίθαλψης και συνήθως περιλαμβάνουν ένα αρχείο των υπηρεσιών που προσφέρονται, των συνθηκών υπό τις οποίες αυτές παρέχονται και των κλινικών αποτελεσμάτων ή των πληροφοριών που αφορούν στις εν λόγω υπηρεσίες.[2]

Τα δεδομένα αυτά δομούνται πλέον μέσω των ηλεκτρονικών φακέλων υγείας (ΗΦΥ) (electronic health records, EHR), οι οποίοι προέκυψαν ως άμεσο αποτέλεσμα των παραπάνω εξελίξεων και της αυξανόμενης ψηφιοποίησης στον τομέα της υγείας. Οι ΗΦΥ είναι η συστηματική συλλογή πληροφοριών για την υγεία των ασθενών σε ηλεκτρονική μορφή[3] και περιλαμβάνουν δεδομένα όπως δημογραφικά στοιχεία, ιατρικό ιστορικό, αλλεργίες και φαρμακευτική αγωγή, αποτελέσματα εργαστηριακών εξετάσεων, ζωτικές ενδείξεις και προσωπικά στατιστικά μεταξύ άλλων.[4] Οι ΗΦΥ μπορούν να διαμοιραστούν μεταξύ συνδεδεμένων πληροφοριακών συστημάτων διαφορετικών οργανισμών (νοσοκομεία, ασφαλιστικοί οργανισμοί κ.λπ.) και φυσικών προσώπων (ιατροί, ασθενείς κ.λπ.). Τα συστήματα ΗΦΥ αποτελούν κρίσιμο παράγοντα για τη βελτίωση της νοημοσύνης και της ποιότητας των ιατρικών διαδικασιών,[5] καθώς και τη μείωση των δαπανών στην υγειονομική περίθαλψη.[6] Η ανταλλαγή ιατρικών δεδομένων ανάμεσα σε διαφορετικά συστήματα ΗΦΥ μπορεί να προσφέρει καλύτερη κατανόηση όσον αφορά στα πρότυπα και στις τάσεις της δημόσιας υγείας.[7] Με αυτόν τον τρόπο εξασφαλίζονται καλύτερη ποιότητα φροντίδας,[8] εξατομικευμένες συστάσεις για τους ασθενείς[9] και, συνολικά, περισσότερο αποδοτικές υπηρεσίες υγείας σε εθνικό και παγκόσμιο επίπεδο.[5]

Η δόμηση των ιατρικών δεδομένων για τα συστήματα ΗΦΥ επιτυγχάνεται μέσα από πρότυπα τυποποίησης. Ορισμένα από τα πλέον δημοφιλή πρότυπα και κωδικοποιήσεις τυποποίησης είναι το Health Level 7 ή HL7,[10] το Fast Healthcare Interoperability Resources ή FHIR,[11] το openEHR[12] και, τέλος, ο ΗΦΥ της Ηλεκτρονικής Διακυβέρνησης Κοινωνικής Ασφάλισης (ΗΔΙΚΑ).[13]

Αυτή τη στιγμή, η μεγαλύτερη πρόκληση για την ευρεία υιοθέτηση συστημάτων ΗΦΥ είναι η εύρεση τρόπων συλλογής, αποθήκευσης και ανάλυσης προσωπικών δεδομένων υγείας χωρίς να εγείρονται ανησυχίες παραβίασης της ιδιωτικής ζωής των ασθενών.[14] Σύμφωνα με έκθεση του ONA General Council,[15] η έλλειψη επαρκών μέτρων ασφάλειας έχει οδηγήσει σε πολλές παραβιάσεις σε συστήματα ΗΦΥ, τα οποία αφήνουν τους ασθενείς εκτεθειμένους σε εκμετάλλευση από κακόβουλους χρήστες. Τέτοιου είδους παραβιάσεις, εκτός από τις επιπτώσεις στη φροντίδα του ασθενούς, συνήθως έχουν οικονομικές και νομικές συνέπειες για τους οργανισμούς παροχής υπηρεσιών υγείας.[16] Η διασφάλιση των ΗΦΥ είναι εκ των πραγμάτων δύσκολο έργο ενώ οι συνέπειες που προκύπτουν από τις παραβιάσεις τέτοιων συστημάτων αποτελούν ισχυρό αντικίνητρο για την ανταλλαγή δεδομένων ανάμεσα σε διαφορετικούς παρόχους.[17]

Σημαντικό εμπόδιο για την ανταλλαγή ιατρικών δεδομένων αποτελεί η έλλειψη συμφωνίας όσον αφορά στις τεχνικές υποδομές που θα χρησιμοποιηθούν. Τα περισσότερα συστήματα απαιτούν είτε μια κεντρική πηγή δεδομένων είτε τη μαζική μετάδοση δεδομένων από το ένα σύστημα στο άλλο. Έτσι, η κεντρική φύλαξη των δεδομένων αυξάνει τον κίνδυνο μαζικών υποκλοπών και κακόβουλων επιθέσεων, ενώ η μαζική αποστολή ιατρικών δεδομένων απαιτεί από τους οργανισμούς να παραχωρήσουν την άδεια χρήσης και επεξεργασίας των δεδομένων σε άλλους οργανισμούς. Συμπερασματικά, αν και οι ηλεκτρονικοί φάκελοι υγείας προσφέρουν πολλές δυνατότητες, λόγω των προβλημάτων τους δεν έχουν εφαρμοστεί ευρέως στον τομέα. Μια τεχνολογία, η οποία παρέχει κατάλληλες λύσεις και μπορεί να μειώσει ή ακόμη και να εξαλείψει τελείως τα μειονεκτήματα, είναι το blockchain. Η κατανεμημένη αποθήκευση των δεδομένων μπορεί να μειώσει το κόστος εφαρμογής νέων συστημάτων, ενώ η ασφάλεια την οποία προσφέρει είναι μεγαλύτερη από εκείνη που εξασφαλίζουν οι υπάρχουσες λύσεις.

Υπό το σχετικό πρίσμα, σκοπός της παρούσας μελέτης είναι η διερεύνηση των απαραίτητων τεχνολογιών, η σχεδίαση και η ανάπτυξη μιας πλατφόρμας ηλεκτρονικής υγείας, στο πλαίσιο του ερευνητικού έργου Impilo, η οποία θα αποτελέσει μια καινοτόμο λύση στα χρονίζοντα προβλήματα διαχείρισης ευαίσθητων δεδομένων υγείας. Η πλατφόρμα θα αποτελείται από ένα blockchain, το οποίο θα λειτουργεί ως αποθετήριο δεδομένων υγείας για την κατασκευή και την ανάκτηση ΗΦΥ, καθώς και την εφαρμογή Impilo, που θα λειτουργεί ως εξυπηρετητής του blockchain και θα διαχειρίζεται τις αλληλεπιδράσεις ιατρών και ασθενών.

2. ΕΠΙΣΚΟΠΗΣΗ ΤΕΧΝΟΛΟΓΙΑΣ BLOCKCHAIN ΣΤΟΝ ΧΩΡΟ ΤΗΣ ΥΓΕΙΑΣ

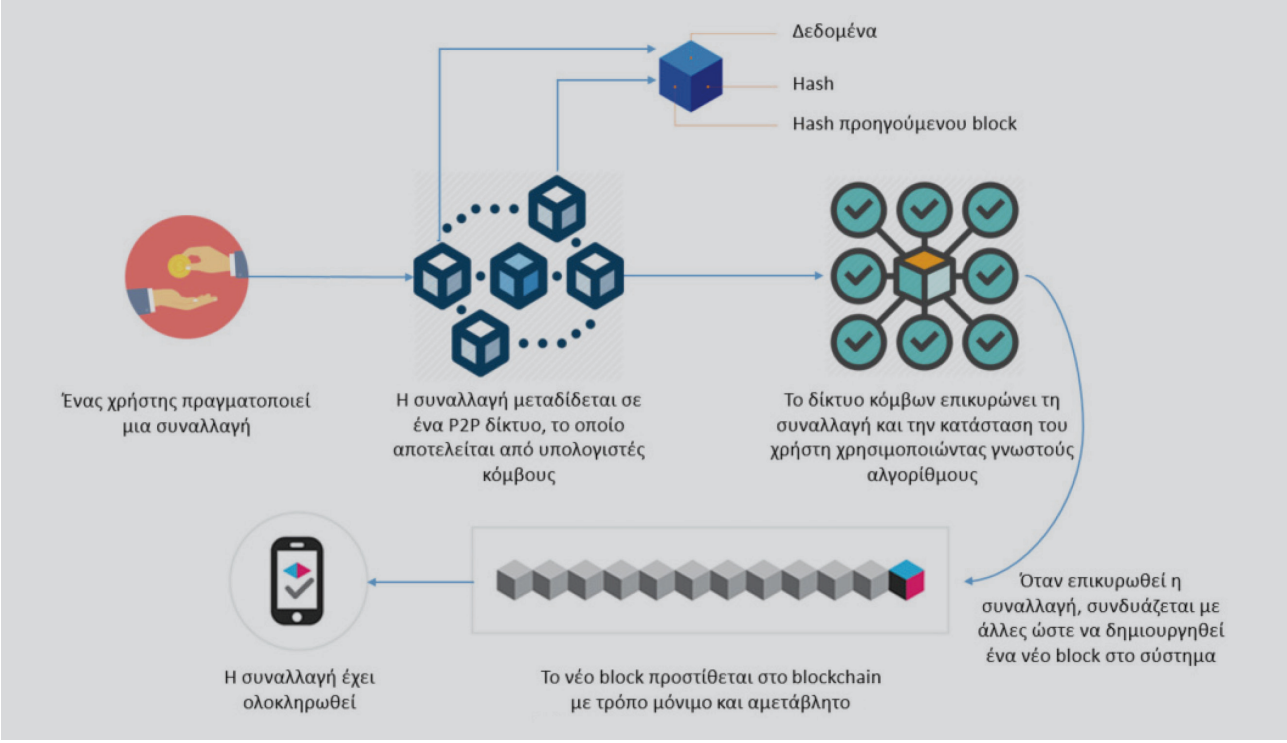
2.1. Εισαγωγή στην τεχνολογία blockchain

Το blockchain είναι μια τεχνολογία η οποία παρέχει

τη δυνατότητα αποκεντρωμένης δόμησης δεδομένων σε έναν κατανεμημένο λογαριασμό συναλλαγών.[18,19] Αποτελείται από έναν αριθμό blocks, τα οποία είναι συνδεδεμένα μεταξύ τους και αντιπροσωπεύουν ένα σύνολο συναλλαγών.[16] Τα blocks διανέμονται σε έναν αριθμό από κατανεμημένους peer-to-peer κόμβους μιας υποδομής και δεν αποθηκεύονται κεντρικά.[20] Κάθε block, εκτός από τα δεδομένα που είναι αποθηκευμένα σε αυτό, περιλαμβάνει ένα hash, το hash του προηγούμενου block, καθώς και τη χρονική στιγμή κατά την οποία δημιουργήθηκε. Ένα hash παράγεται με τη βοήθεια κρυπτογραφικών συναρτήσεων κατακερματισμού (hash functions), αποτελεί την αναπαράσταση των δεδομένων του block και εξαρτάται άμεσα από αυτά. Για τον λόγο αυτόν, μπορεί να χρησιμοποιηθεί για την επαλήθευση της ακεραιότητας των συναλλαγών (δεδομένων) που περιέχονται σε κάθε block. Επί πλέον, το hash κάθε block εξαρτάται από το hash του προηγούμενου σε σειρά block, γεγονός που στην ουσία καθιστά όλο το blockchain αμετάβλητο, καθώς οποιαδήποτε αλλαγή σε ένα block θα μεταβάλλει και το hash, όχι μόνο του εν λόγω block αλλά και όλων των επόμενων σε σειρά από αυτό. Επειδή το blockchain δεν υπόκειται σε διαχείριση από κάποια κεντρική αρχή, η διατήρηση της ακεραιότητας του ιστορικού των συναλλαγών στο σύστημα επιτυγχάνεται μέσα από αλγόριθμους συναίνεσης.

Το blockchain πρωτοεμφανίστηκε το 2008 και έχει γίνει ευρέως γνωστό από τη χρήση του ως δημόσιος λογαριασμός συναλλαγών στον τομέα των κρυπτονομισμάτων όπως το bitcoin και το Ethereum. Παρ' όλα αυτά, μπορεί επίσης να χρησιμοποιηθεί γενικότερα για τη δημιουργία μόνιμων, δημόσιων και διαφανών συστημάτων διαχείρισης δεδομένων.[21] Μάλιστα, τα τελευταία έτη, η προστιθέμενη αξία του blockchain έχει γίνει αντιληπτή από την ερευνητική κοινότητα και από διάφορους οργανισμούς, οι οποίοι προτείνουν και αναπτύσσουν καινοτόμες λύσεις σε τομείς εκτός από τα κρυπτονομίσματα όπως είναι η υγεία, η δημόσια διοίκηση, οι εφοδιαστικές αλυσίδες κ.λπ. Ανεξάρτητα από το πεδίο εφαρμογής, ο γενικός τρόπος λειτουργίας μιας αλυσίδας blockchain φαίνεται στην εικόνα 1.

Είναι ευρέως αποδεκτό ότι το blockchain μπορεί να αποτελέσει αποτελεσματική λύση σε κάθε τομέα ο οποίος περιλαμβάνει συναλλαγές δεδομένων. Μεγάλο ρόλο σε αυτό διαδραματίζουν και τα έξυπνα συμβόλαια, τα οποία είναι συμβάσεις που μπορούν να εκτελεστούν/εφαρμοστούν μερικώς ή πλήρως χωρίς ανθρώπινη αλληλεπίδραση.[22] Επειδή στη γενική περίπτωση ενός ανοικτού, δημόσιου blockchain τα δεδομένα κάθε χρήστη ανήκουν στον ίδιο, τα έξυπνα συμβόλαια χρησιμοποιούνται για τον ορισμό των δικαιωμάτων που έχουν τρίτοι χρήστες στα συγκεκριμένα δεδομένα. Συνολικά, κάθε δίκτυο blockchain προσφέρει



Εικόνα 1. Λειτουργία ενός blockchain.

συνεχή διαθεσιμότητα, αξιοπιστία, ασφάλεια, ανθεκτικότητα και ακεραιότητα.[20]

Ο βασικός λόγος που επιτρέπει στο blockchain να έχει ευρύ πεδίο εφαρμογής είναι ότι σε κάθε στιγμή οι χρήστες του δικτύου είναι σε θέση να γνωρίζουν την κατάσταση του συστήματος. Για την αύξηση της ασφάλειας και της εμπιστοσύνης στο δίκτυο το blockchain διαθέτει διάφορους μηχανισμούς, μέσω των οποίων μπορεί να διασφαλιστεί μια συναλλαγή, οι κυριότεροι από τους οποίους είναι[20] η απόδειξη ύπαρξης και μη ύπαρξης (μπορεί να εξακριβωθεί εύκολα και σίγουρα αν ένα στοιχείο υπάρχει στο σύστημα), η απόδειξη χρόνου (όταν αποθηκεύονται πληροφορίες στο blockchain, αποθηκεύεται και η ώρα κατά την οποία προστέθηκαν), η απόδειξη σειράς (σε περιπτώσεις συμφόρησης του δικτύου, μπορεί να φαίνεται η σειρά με την οποία πραγματοποιήθηκαν κάποιες αιτήσεις/συναλλαγές), η απόδειξη συγγραφής (η εισαγωγή δεδομένων στο blockchain περιλαμβάνει και τα ψηφιακά στοιχεία του χρήστη που τα προσέθεσε) και η απόδειξη ιδιοκτησίας (φαίνεται πάντα με βεβαιότητα σε ποιον ανήκει κάποιο στοιχείο).

2.2. Εφαρμογή του blockchain στον χώρο της υγείας

Στον τομέα της υγείας το blockchain μπορεί να χρησιμοποιηθεί αρχικά ως βάση δεδομένων, καθώς στα παραδοσιακά ιατρικά/νοσοκομειακά συστήματα η ταυτοποίηση των δεδομένων και τα διαφορετικά σημεία επαφής αυξάνουν το κόστος εγκατάστασης και συντήρησης. Επί πλέον, δυσχεραίνουν την επικοινωνία μεταξύ συστημάτων διαφορετικών παρόχων υπηρεσιών υγείας. Το blockchain μειώνει σημαντικά τα εν λόγω προβλήματα καθώς προσφέρει λειτουργίες για την ακεραιότητα, την επικαιροποίηση και τη διατήρηση της ιστορικότητας των δεδομένων, ενώ μειώνει την πιθανότητα μη λειτουργίας του συστήματος. Επίσης, σε ένα blockchain υπεύθυνος για τα δεδομένα του είναι ο ίδιος ο χρήστης, ο οποίος ορίζει και τα δικαιώματα πρόσβασης τρίτων μερών σε αυτά. Δίνοντας τον έλεγχο των δεδομένων στους ίδιους τους ασθενείς και τους χρήστες του δικτύου και όχι μόνο στους οργανισμούς, διασφαλίζεται και η σωστή χρήση τους (ύπαρξη μεγαλύτερης διαφάνειας και αυξημένης ασφάλειας). Τέλος, τα συστήματα blockchain είναι ασφαλέστερα από επιθέσεις και υποκλοπές, οπότε περιπτώσεις κακόβουλης χρήσης αυτών είναι πρακτικά αδύνατες.[23]

Αυτή τη στιγμή, το επικρατές πρότυπο για τη διαχείριση δεδομένων υγείας είναι οι ΗΦΥ. Παρ' όλα αυτά, ο μικρός βαθμός ψηφιοποίησης του τομέα σε συνδυασμό με τα αυξημένα κόστη για την υιοθέτηση τέτοιων συστημάτων εμποδίζει την ευρεία χρήση και εξέλιξή τους. Ο συνδυασμός των ΗΦΥ με υλοποιήσεις blockchain θα μπορούσε να μειώσει τα προαναφερθέντα προβλήματα καθώς απαιτούν λιγότερο εξοπλισμό σε σχέση με παραδοσιακά συστήματα, ενώ, παράλληλα, μειώνουν τα κόστη για τη διαχείριση θεμάτων ασφάλειας και ελέγχου των δεδομένων.[24]

Επί πλέον, η ελεύθερη πρόσβαση στα δεδομένα και ο ανοικτός χαρακτήρας του συστήματος παρέχει τη δυνατότητα δημιουργίας νέων εφαρμογών και υπηρεσιών, δεδομένου ότι το blockchain προσφέρει από μόνο του ένα ασφαλές δίκτυο και μια κατανεμημένη βάση δεδομένων, που μπορούν να χρησιμοποιηθούν χωρίς μεγάλο επιπρόσθετο κόστος. Ακόμη, η διάθεση κρυπτονομισμάτων σε ένα δίκτυο blockchain (peer-to-peer αποκεντρωμένη ηλεκτρονική μορφή χρήματος, η οποία βασίζεται πάνω στις αρχές της κρυπτογραφίας για τη διασφάλιση του δικτύου και την επαλήθευση των συναλλαγών)[25] ενδέχεται να μειώσει τα λειτουργικά κόστη, γεγονός το οποίο ήδη έχουν εφαρμόσει διάφορες εταιρείες, όπως η Bowhead Health, όπου οι χρήστες μπορούν να διαθέτουν τα δεδομένα τους σε ερευνητές έναντι ενός αριθμού κρυπτονομισμάτων.[26] Τέλος, το blockchain μπορεί να χρησιμοποιηθεί για την καταπολέμηση πλαστογραφημένων και ψευδών φαρμάκων και συνταγογραφήσεων. Εφαρμόζοντας συστήματα blockchain στις εφοδιαστικές αλυσίδες φαρμακοβιομηχανιών (συνήθως σε συνδυασμό με το Διαδίκτυο των Πραγμάτων) αυξάνεται η ορατότητα και η αξιοπιστία σε ολόκληρο τον κύκλο ζωής ενός φαρμάκου.

2.3. Νομικό πλαίσιο σχετικά με GDPR, blockchain και δεδομένα υγείας

2.3.1. Αρχές Προστασίας Προσωπικών Δεδομένων και Δικαιώματα Υποκειμένου. Ο Γενικός Κανονισμός για την Προστασία των Δεδομένων (General Data Protection Regulation, GDPR) 2016/679[27] είναι μια ρύθμιση στη νομοθεσία της Ευρωπαϊκής Ένωσης (ΕΕ) περί προστασίας των δεδομένων και της ιδιωτικής ζωής για όλα τα άτομα εντός της ΕΕ και του Ευρωπαϊκού Οικονομικού Χώρου (ΕΟΧ). Αφορά επίσης στην 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.[28] Ο GDPR εκδόθηκε στις 14 Απριλίου 2016 και τέθηκε σε ισχύ στις 25 Μαΐου 2018.[29]

Σύμφωνα με τον GDPR, ως προσωπικά δεδομένα ορίζονται πληροφορίες που περιγράφουν ένα άτομο, όπως στοιχεία αναγνώρισης, φυσικά χαρακτηριστικά, εκπαίδευση, εργασία, οικονομική κατάσταση, ενδιαφέροντα, δραστηριότητες, συνήθειες. Επί πλέον, ευαίσθητα χαρακτηρίζονται τα προσωπικά δεδομένα ενός ατόμου που αναφέρονται

στη φυλετική ή στην εθνική του προέλευση, στα πολιτικά του φρονήματα, στις θρησκευτικές ή στις φιλοσοφικές του πεποιθήσεις, στην υγεία του, στην κοινωνική του πρόνοια, στην ερωτική του ζωή, στις 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 απ' ό,τι τα απλά προσωπικά δεδομένα.[30]

Σύμφωνα με τον GDPR, τα άτομα έχουν έναν αριθμό από δικαιώματα[31] όσον αφορά στα προσωπικά τους δεδομένα, τα κυριότερα από τα οποία είναι το δικαίωμα ενημέρωσης, πρόσβασης, διόρθωσης, διαγραφής, αντίρρησης, κοινοποίησης, λήψης αποφάσεων με αυτόματο τρόπο και φορητότητας των δεδομένων.

Προκειμένου να διασφαλιστεί η συμμόρφωση με τα παραπάνω, σύμφωνα με το GDPR, η διαχείριση των προσωπικών δεδομένων από επιχειρήσεις και λοιπούς οργανισμούς θα πρέπει να καθορίζεται ρητά και να διέπεται από συγκεκριμένες αρχές.[32] Αρχικά, οι οργανισμοί πρέπει να διασφαλίζουν ότι υπάρχουν νόμιμοι λόγοι για τη συλλογή και τη χρήση προσωπικών δεδομένων, λαμβάνοντας τη συγκατάθεση των πελατών τους γι' αυτούς τους σκοπούς. Επί πλέον, οφείλουν να φροντίσουν ότι αποθηκεύουν με απόλυτη ακρίβεια και μόνο τα δεδομένα που είναι απαραίτητα για τον σκοπό της επεξεργασίας για τον οποίο έχει ληφθεί συγκατάθεση. Η ρητή συγκατάθεση των ατόμων απαιτείται και για μεταφορά των δεδομένων σε τρίτους οργανισμούς. Για τον λόγο αυτόν χρησιμοποιούνται φόρμες συγκατάθεσης, οι οποίες αναφέρουν με λεπτομέρεια τους σκοπούς συλλογής των δεδομένων, καθώς και την επεξεργασία που θα υποστούν. Για τη συμμόρφωση με τα παραπάνω, ο GDPR συνιστά στους οργανισμούς τον διορισμό ενός Υπεύθυνου Προστασίας Δεδομένων (data protection officer, DPO), ο οποίος λειτουργεί ως ενιαίο σημείο επαφής ανάμεσα στους πελάτες, στον οργανισμό και στους εποπτικούς φορείς και παρέχει συμβουλές σχετικά με τα μέτρα και τις πολιτικές προστασίας δεδομένων. Τέλος, συνιστάται από τον GDPR η διενέργεια Αξιολόγησης Αντικτύπου Προστασίας Δεδομένων (data protection impact assessment, DPIA) για την αναγνώριση και τη διαχείριση ενδεχόμενων απειλών όσον αφορά στα προσωπικά δεδομένα, ειδικά κατά την υιοθέτηση νέων τεχνολογιών σε παραδοσιακά συστήματα.

Σύμφωνα με τον GDPR, οι ιατρικές πληροφορίες θεωρούνται ευαίσθητα προσωπικά δεδομένα. Ασφαλώς, οι οργανισμοί οι οποίοι δραστηριοποιούνται στον κλάδο της υγείας και είναι υπεύθυνοι για την αποθήκευση και την επεξεργασία ιατρικών δεδομένων πρέπει να ακολουθούν τις βασικές διατάξεις του GDPR. Ωστόσο, υπάρχουν και κάποια θεμελιώδη δικαιώματα όσον αφορά στα δεδομένα των ασθενών, τα οποία ορίζονται από την ελληνική νομοθεσία και πρέπει να τηρούνται από τους οργανισμούς. Συγκεκριμένα, σύμφωνα με το άρθρο 12 του Ν 2472/97,[33] κάθε ασθενής έχει δικαίωμα πρόσβασης στα δεδομένα του και μπορεί να λάβει τον ιατρικό του φάκελο, επισήμως θεωρημένο, από το νοσοκομείο στο οποίο έχει νοσηλευτεί. Επί πλέον, σύμφωνα με τον νόμο 3418/2005,[34] προβλέπεται η χορήγηση δικαιωμάτων πρόσβασης στον ιατρικό φάκελο ενός ασθενούς από κάποιον συγγενή του. Το συγκεκριμένο δικαίωμα πρόσβασης επιτρέπεται μόνο κατ' εξαίρεση σε περίπτωση που το τρίτο πρόσωπο ενεργεί ως νόμιμος αντιπρόσωπος, διαθέτει έγγραφη εξουσιοδότηση, καθώς και σε περίπτωση αδυναμίας του ασθενούς να δώσει τη συγκατάθεσή του ειδικά για τη διαφύλαξη του ζωτικού του συμφέροντος. Από την άλλη, οι επαγγελματίες υγείας, όταν λειτουργούν και ως υπεύθυνοι επεξεργασίας δεδομένων, έχουν την υποχρέωση να γνωστοποιήσουν τυχαίες ή παράνομες καταστροφές, απώλειες, αλλοιώσεις και γνωστοποιήσεις (μη εξουσιοδοτημένες) δεδομένων στις αρμόδιες εποπτικές αρχές. Για την τήρηση των δικαιωμάτων και των υποχρεώσεων που αναφέρθηκαν, οι υπεύθυνοι επεξεργασίας οφείλουν να διαθέσουν στους ασθενείς τα σχετικά έγγραφα τα οποία περιγράφουν τους παραπάνω κανονισμούς και επιτρέπουν σε έναν ασθενή να δώσει τη συγκατάθεσή του (προσωρινή ή μόνιμη) για την επεξεργασία των δεδομένων του.

2.3.2. Συμμόρφωση του Impilo με το νομικό πλαίσιο. Η συμμόρφωση του blockchain με τον κανονισμό GDPR αφορά στον τρόπο με τον οποίο χρησιμοποιείται η εν λόγω τεχνολογία σε διάφορες περιπτώσεις και εφαρμογές και αποτελεί ένα φλέγον ζήτημα, το οποίο απασχολεί την Ευρωπαϊκή Επιτροπή. Ως εκ τούτου, υπάρχουν κάποια σημαντικά ζητήματα τα οποία αξίζουν να αναφερθούν, στο πλαίσιο του GDPR, όσον αφορά στην προστασία των προσωπικών δεδομένων σε ένα blockchain. Συγκεκριμένα, η δομή και η αποθήκευση των δεδομένων σε ένα δίκτυο blockchain γίνεται με τέτοιον τρόπο που δεν επιτρέπει τη διαγραφή ή τη διόρθωση των δεδομένων εφόσον αυτά καταχωρηθούν στην αλυσίδα. Συνεπώς, ακόμη και αν μπορεί να προσδιοριστεί ο υπεύθυνος επεξεργασίας σε ένα δίκτυο, καθίσταται αδύνατο ο εν λόγω υπεύθυνος επεξεργασίας να διαγράψει ή να επικαιροποιήσει το αρχείο μιας συναλλαγής χωρίς να καταστρέψει την αλυσίδα των block. Η τεχνολογία blockchain έχει συνολικά οικοδομηθεί στη βάση της διασφάλισης ότι οι συναλλαγές δεν πρόκειται ποτέ να λησμονηθούν ή να διαγραφούν, με σκοπό τη δημιουργία αποκεντρωμένης εμπιστοσύνης καθώς και την ανάπτυξη και επέκταση του δικτύου των συμμετεχόντων. Παρ' όλα αυτά, η διόρθωση και η διαγραφή των προσωπικών δεδομένων αποτελούν δύο βασικά δικαιώματα που προβλέπει το GDPR.

Για τη συμμόρφωση με τις διατάξεις του GDPR, οργανισμοί οι οποίοι αναπτύσσουν blockchain εφαρμογές χρησιμοποιούν ορισμένες τεχνικές κρυπτογράφησης, που συνδυάζονται με την καταστροφή του κλειδιού το οποίο παρέχει πρόσβαση στα δεδομένα ενός block. Μια άλλη τεχνική η οποία χρησιμοποιείται κατά κόρον είναι η φύλαξη των δεδομένων σε κεντρικές βάσεις και η χρήση του blockchain για την αποθήκευση των συναλλαγών ανάμεσα στους χρήστες του συστήματος. Με αυτόν τον τρόπο αποφεύγονται οι κίνδυνοι που προκύπτουν από την ανάγκη τήρησης των δικαιωμάτων των χρηστών. Ειδικά όσον αφορά στο δικαίωμα της λήθης, η φύλαξη σε κεντρικές βάσεις επιτρέπει τη διαγραφή των δεδομένων των χρηστών. Το γεγονός ότι τα δεδομένα δεν μπορούν να διαγραφούν από το blockchain δεν έχει σε αυτή την περίπτωση μεγάλη σημασία, καθώς το μόνο που διατηρείται είναι τα hashes των συναλλαγών, τα οποία δεν μπορούν να οδηγήσουν σε ταυτοποίηση του χρήστη.

Τελικά, στο πλαίσιο συμμόρφωσης του ερευνητικού έργου Impilo και της εφαρμογής η οποία θα αναπτυχθεί με το νομοθετικό πλαίσιο που προαναφέρθηκε, θα ληφθούν τα ακόλουθα μέτρα. Για τη διασφάλιση της νομιμότητας επεξεργασίας δεδομένων θα λαμβάνεται η συγκατάθεση του χρήστη μέσα από σχετικό έγγραφο, το οποίο περιγράφει επακριβώς τα δεδομένα που θα ληφθούν καθώς και τι περιλαμβάνει η επεξεργασία τους. Επί πλέον, θα οριστεί υπεύθυνος επεξεργασίας δεδομένων (DPO) και θα πραγματοποιηθεί αξιολόγηση του αντικτύπου προστασίας δεδομένων. Τα δεδομένα που θα ληφθούν θα είναι τα απολύτως απαραίτητα και δεν θα υποστούν επεξεργασία η οποία υπερβαίνει τους σκοπούς του έργου, ενώ οι χρήστες της εφαρμογής θα ενημερώνονται για οποιαδήποτε επεξεργασία και μεταποίηση των δεδομένων τους μέσα από ειδοποιήσεις. Τέλος, για τη συμμόρφωση με το δικαίωμα διαγραφής, τα πραγματικά δεδομένα των χρηστών θα διατηρούνται σε κεντρική βάση ενώ το blockchain θα χρησιμοποιείται για την αποθήκευση των συναλλαγών που αφορούν στα εν λόγω δεδομένα.

3. ΜΕΘΟΔΟΛΟΓΙΑ ΑΠΟΘΗΚΕΥΣΗΣ ΔΕΔΟΜΕΝΩΝ ΥΓΕΙΑΣ ΜΕΣΩ BLOCKCHAIN

3.1. Ερευνητικές προσεγγίσεις αποθήκευσης ιατρικών δεδομένων βασισμένες στο blockchain

Ο κύριος στόχος του συγκεκριμένου κεφαλαίου είναι η περιγραφή διαφόρων ερευνητικών προσεγγίσεων βασισμένων στο blockchain, για την αποτελεσματική και ασφαλή ανταλλαγή ιατρικής πληροφορίας ανάμεσα σε ασθενείς, ιατρούς και λοιπούς οργανισμούς.

Μια υβριδική προσέγγιση για την ανάπτυξη ενός blockchain σχετικά με την υγειονομική περίθαλψη κάνει χρήση του ανερχόμενου προτύπου FHIR για τη δόμηση της ιατρικής πληροφορίας. Στο συγκεκριμένο σύστημα, οι κόμβοι του δικτύου αντιπροσωπεύουν συναλλαγές εγγραφών των ασθενών και περιγράφουν την προσθήκη ενός πόρου (δηλαδή μιας συγκεκριμένης ιατρικής πληροφορίας) στο επίσημο αρχείο ασθενών. Οι συναλλαγές, ωστόσο, δεν περιλαμβάνουν το πραγματικό έγγραφο καταγραφής της ιατρικής πληροφορίας. Αντίθετα, δείχνουν προς το μέρος όπου φυλάσσονται οι πόροι του FHIR μέσω διευθύνσεων URL και εκεί έγκειται η υβριδικότητα του συστήματος ανάμεσα στο blockchain και στις κεντρικές βάσεις δεδομένων. Ο τρόπος που είναι δομημένο το σύστημα επιτρέπει στους οργανισμούς παροχής υγειονομικής περίθαλψης να διατηρούν τον λειτουργικό έλεγχο των δεδομένων τους καθώς διατηρεί τα ευαίσθητα δεδομένα των ασθενών εκτός blockchain.[16]

Σε μια άλλη ερευνητική προσέγγιση αναπτύχθηκε αρχιτεκτονική, βασισμένη σε blockchain, η οποία επιτρέπει στον ασθενή να κατέχει, να ελέγχει και να μοιράζεται τα ιατρικά του δεδομένα με ευκολία και ασφάλεια. Το εν λόγω σύστημα συσσωρεύει τα ιατρικά δεδομένα του ασθενούς από πληθώρα συστημάτων (πληροφοριακά συστήματα ιατρικών αρχείων, αλγόριθμοι ανάλυσης δεδομένων, ιατρικά αρχεία κ.λπ.) και του επιτρέπει να τα διαχειρίζεται ενοποιημένα μέσα από την αποκλειστική πύλη δεδομένων του. Τα δεδομένα αποθηκεύονται σε ένα ιδιωτικό blockchain cloud. Το blockchain εγγυάται ότι τα ιατρικά δεδομένα δεν μπορούν να μεταβληθούν από κανέναν, συμπεριλαμβανομένων ιατρών και ασθενών, ενώ διάφορες κρυπτογραφικές τεχνικές χρησιμοποιούνται για την προστασία τους.[5]

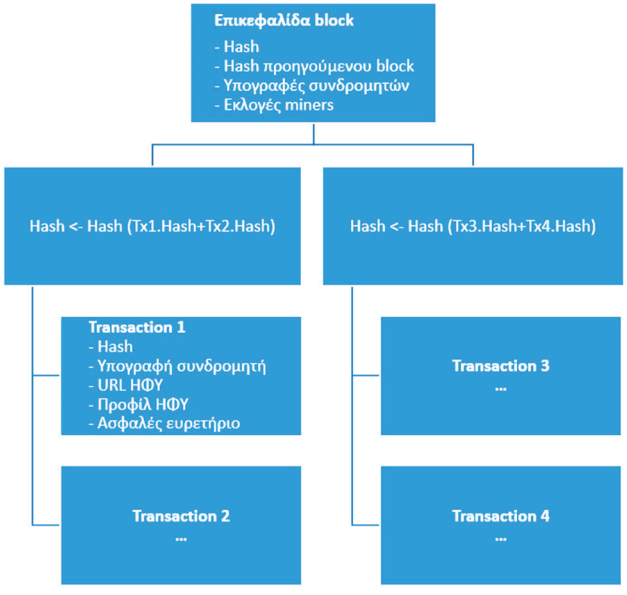
Το MedRec[35] είναι ένα αποκεντρωμένο σύστημα ηλεκτρονικών φακέλων υγείας βασισμένο στο blockchain, το οποίο παρέχει στους ασθενείς ένα πλήρες και αμετάβλητο ημερολόγιο, ώστε να έχουν εύκολη πρόσβαση στις ιατρικές τους πληροφορίες ανεξαρτήτως παρόχου. Μέσα από την αξιοποίηση των εγγενών χαρακτηριστικών του blockchain, το MedRec διαχειρίζεται την προσβασιμότητα, την εμπιστευτικότητα και την ανταλλαγή δεδομένων, τα οποία είναι κρίσιμα ζητήματα κατά τη διαχείριση ευαίσθητης πληροφορίας. Οι χρήστες του συστήματος μπορούν να ελέγξουν την αυθεντικότητα και το ιστορικό των δεδομένων τους και να διαχειριστούν τα δικαιώματα πρόσβασης σε αυτά, ενώ το σύστημα διαθέτει ποικίλα APIs που του επιτρέπουν να ενσωματώνεται με υπάρχουσες βάσεις δεδομένων των διαφόρων παρόχων υγείας.[35]

Σε γενικές γραμμές, είναι εύκολο να παρατηρηθεί μέσα από προσπέλαση της σχετικής βιβλιογραφίας ότι η γενι-

κή περίπτωση χρήσης blockchain στον χώρο της υγείας κινείται στο πλαίσιο των τεχνικών που ήδη παρουσιάστηκαν. Μάλιστα, σε μια σχετική δημοσίευση[36] μελετήθηκαν και παρουσιάστηκαν όλοι οι τρόποι και οι μεθοδολογίες, με βάση τις υπάρχουσες τεχνολογίες, ώστε να βελτιωθεί η διαχείριση της ιατρικής πληροφορίας στον χώρο της υγειονομικής περίθαλψης. Όσον αφορά σε συστήματα βασισμένα στο blockchain, η γενική περίπτωση είναι αυτή η οποία ήδη παρουσιάστηκε. Συμπεραίνεται λοιπόν ότι στον χώρο της υγείας η χρήση του blockchain αποσκοπεί κυρίως στο να προσθέσει ένα στρώμα ασφάλειας στα ευαίσθητα δεδομένα των ασθενών, να τους επιτρέψει τη διαχείριση των δικαιωμάτων πρόσβασης σε αυτά και να διευκολύνει την επικοινωνία ανάμεσα σε διαφορετικούς οργανισμούς οι οποίοι παρέχουν ιατρικές υπηρεσίες στον ίδιο ασθενή. Τα πραγματικά δεδομένα των ασθενών φυλάσσονται στις κεντρικές βάσεις του εκάστοτε οργανισμού, αλλά μέσω της αλυσίδας blockchain ο ασθενής μπορεί να επαληθεύει την ιστορικότητα και την αυθεντικότητα των πληροφοριών και του ιατρικού ιστορικού του.

3.2. Μεθοδολογία αποθήκευσης ιατρικών δεδομένων στο Impilo

3.2.1. Δομή του blockchain block. Στο παρόν κεφάλαιο και λαμβάνοντας υπ' όψη τη σχετική βιβλιογραφία, θα παρουσιαστεί η πληροφορία που θα υπάρχει μέσα σε ένα οποιοδήποτε block του Impilo blockchain. Συγκεκριμένα, η δομή ενός block φαίνεται στην εικόνα 2. Σε γενικές γραμμές, η



Εικόνα 2. Ένα block blockchain της υγειονομικής περίθαλψης που περιέχει καταχωρήσεις στο αρχείο ασθενών.

δομή του Impilo blockchain στηρίζεται στα δένδρα Merkle. Στην κρυπτογραφία και στην επιστήμη των υπολογιστών, ένα δένδρο Merkle ή δένδρο κατακερματισμού (hash) είναι ένα δένδρο στο οποίο κάθε κόμβος φύλλων φέρει την ετικέτα του κατακερματισμού ενός block δεδομένων και κάθε κόμβος που δεν είναι φύλλο επισημαίνεται με τον κρυπτογραφικό κατακερματισμό των ετικετών των κόμβων παιδιών του. Τα δένδρα Merkle επιτρέπουν την αποτελεσματική και ασφαλή επαλήθευση του περιεχομένου των μεγάλων δομών δεδομένων.[37] Στο συγκεκριμένο σύστημα, τα φύλλα κόμβοι αυτού του δένδρου αντιπροσωπεύουν συναλλαγές εγγραφών των ασθενών και περιγράφουν την προσθήκη ενός πόρου –δηλαδή μιας συγκεκριμένης ιατρικής πληροφορίας– στο επίσημο αρχείο ασθενών. Τα hashes όλων των συναλλαγών σε ένα block συμβάλλουν στο hash της ρίζας Merkle, ή αλλιώς της επικεφαλίδας του block.

Η επικεφαλίδα του block περιέχει τα ακόλουθα μεταδεδομένα που χρησιμοποιούνται για την επικύρωση κάθε νέου block: Το hash του block, το hash του προηγούμενου block (για σκοπούς επικύρωσης), τις υπογραφές συνδρομητών κάθε κόμβου που συνέβαλε στο block (για να διασφαλιστεί ότι το block θα παραμείνει έγκυρο αφού συναρμολογηθεί από τον εκάστοτε miner) και τις εκλογές miners (miner elections: κάθε κόμβος που συνέβαλε στο block απαιτείται να παράσχει έναν τυχαίο αριθμό κρυπτογραφημένο με το ιδιωτικό κλειδί του κόμβου για την προετοιμασία της εκλογής του επόμενου miner).

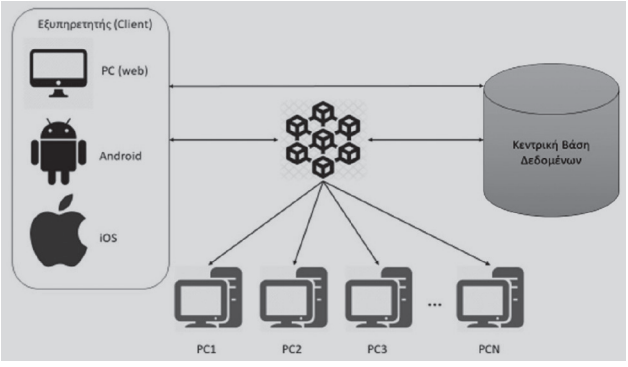
Στη συγκεκριμένη προσέγγιση, μια ιατρική συναλλαγή η οποία αποθηκεύεται σε ένα block της αλυσίδας περιλαμβάνει τις ακόλουθες πληροφορίες: Το hash της συναλλαγής (αν και ο πόρος δεν εισάγεται στο blockchain, το περιεχόμενό του μπορεί να εξακριβωθεί, χρησιμοποιώντας το hash συναλλαγών κατά την ανάκτηση), την υπογραφή προέλευσης (ψηφιακή υπογραφή του κόμβου προέλευσης), το URL του ΗΦΥ (αναφορά στην πραγματική τοποθεσία του πόρου ΗΦΥ, όπου βρίσκονται τα δεδομένα), το προφίλ του ΗΦΥ (URI του προφίλ ΗΦΥ στο οποίο ανταποκρίνεται αυτός ο πόρος) και, τέλος, ένα κρυπτογραφημένο ευρετήριο το οποίο επιτρέπει την ανακάλυψη δεδομένων χωρίς διαρροή πληροφοριών του αρχείου.

Παρ' όλο που το ίδιο το block δεν περιέχει τα πραγματικά δεδομένα, πρέπει να παρέχει δυνατότητες αναζήτησης και ανίχνευσης, καθώς και έναν μηχανισμό πρόσβασης στα δεδομένα μόλις βρεθούν οι κατάλληλες συναλλαγές. Οι εξωτερικές οντότητες, με τα κατάλληλα δικαιώματα, μπορούν να υποβάλλουν ερώτημα στο blockchain, χρησιμοποιώντας λέξεις-κλειδιά στο πεδίο «Ασφαλές ευρετήριο» της συναλλαγής. Οι εν λόγω λέξεις-κλειδιά μπορούν να αναζητηθούν παρά το γεγονός ότι θα κρυπτογραφηθούν για την αποφυγή διαρροής δεδομένων.[38]

3.2.2. Αρχιτεκτονική συστήματος. Στο Impilo τα στοιχεία των ασθενών θα διατηρούνται σε εξωτερική βάση δεδομένων, όπως προαναφέρθηκε, ενώ το blockchain χρησιμοποιείται για την επικύρωση και την αποθήκευση των συναλλαγών. Στο παρόν κεφάλαιο θα παρουσιαστεί η γενική αρχιτεκτονική του συστήματος.

Όπως φαίνεται και στην εικόνα 3, η υψηλού επιπέδου αρχιτεκτονική του Impilo αποτελείται από τρία επί μέρους στοιχεία. Αρχικά, ο εξυπηρετητής (client) είναι η εφαρμογή του Impilo μέσα από την οποία οι χρήστες θα έχουν πρόσβαση στις διάφορες λειτουργίες που θα αναπτυχθούν, στη βάση blockchain και στην κεντρική βάση δεδομένων. Δεύτερον, το αποθετήριο blockchain θα χρησιμοποιείται για την επικύρωση και την αποθήκευση των συναλλαγών που αφορούν στα δεδομένα υγείας ενός ασθενούς. Ένας αριθμός από υπολογιστές θα χρησιμοποιηθεί για την αποκεντρωμένη φύλαξη του blockchain του Impilo ώστε να μην επιβαρύνονται οι προσωπικές (φορητές και μη) συσκευές των χρηστών με την αποθήκευση ολόκληρης της αλυσίδας, αλλά παράλληλα να έχουν πρόσβαση σε αυτή. Με αυτόν τον τρόπο αυξάνεται επίσης η πιθανότητα εντοπισμού κάποιας κακόβουλης ενέργειας. Τέλος, η κεντρική βάση δεδομένων είναι το μέρος όπου θα αποθηκεύεται η πραγματική ιατρική πληροφορία. Για την ασφάλεια του συστήματος τα δεδομένα θα είναι κρυπτογραφημένα, ώστε να διαφυλαχθεί η ακεραιότητά τους και να παρεμποδιστεί η επεξεργασία τους από κακόβουλους χρήστες.

Όσον αφορά στη λειτουργία του συστήματος, θα γίνει κατανοητή μέσα από το ακόλουθο παράδειγμα. Έστω ότι ένας χρήστης του Impilo θέλει να αποθηκεύσει στον ιατρικό του φάκελο τις αιματολογικές του εξετάσεις. Κάνει login στην εφαρμογή του Impilo με τα διαπιστευτήριά του και πραγματοποιεί τις κινήσεις που απαιτούνται για αποθήκευση νέας πληροφορίας στον ιατρικό του φάκελο. Ο εξυπηρετητής (client) του Impilo επικοινωνεί με την κεντρική βάση δεδομένων και αποθηκεύει την πληροφορία στον φάκελο του ασθενούς. Η αλυσίδα blockchain βρίσκεται σε επικοινωνία και με τον εξυπηρετητή και με τη βάση για την παραγωγή του hash που θα χρειαστεί ώστε να αποθηκευτούν οι λεπτομέρειες της συναλλαγής σε ένα block. Μετά την αποθήκευση της νέας πληροφορίας, ο client και η βάση επικοινωνούν με το blockchain, εξετάζουν αν το hash είναι ίδιο και στα δύο μέρη και εφόσον είναι, οι λεπτομέρειες της συναλλαγής αποθηκεύονται σε ένα block του blockchain.



Εικόνα 3. Αρχιτεκτονική συστήματος.

Αξίζει να σημειωθεί ότι για την αύξηση της προστασίας των δεδομένων του ασθενούς στην κεντρική βάση φύλαξης, αυτά αποθηκεύονται hashed με κλειδί τον κωδικό του ασθενούς για πρόσβαση στην εφαρμογή. Αυτό σημαίνει ότι μόνο ο χρήστης μπορεί να αποκρυπτογραφήσει τα δεδομένα του κατά την είσοδό του στην εφαρμογή και σε περίπτωση κακόβουλης επίθεσης στο σύστημα ο εισβολέας θα πρέπει να γνωρίζει και τους κωδικούς πρόσβασης των ασθενών για να λάβει τη σωστή πληροφορία.

3.3. Ασφάλεια συστήματος

Σε γενικές γραμμές, τα συστήματα blockchain χρησιμοποιούν τεχνικές κρυπτογράφησης για την εξασφάλιση της ακεραιότητας των περιεχομένων τους και την ανίχνευση παραβιάσεων. Επί πλέον, για την προστασία των δεδομένων εφαρμόζονται δένδρα κατακερματισμού (Merkle trees) για τη δόμηση των blocks. Σε αυτή την περίπτωση, οποιαδήποτε αλλαγή της κατάστασης του συστήματος οδηγεί σε νέα τιμή κατακερματισμού στον κόμβο ρίζα (root hash). Με αυτόν τον τρόπο, όλοι οι κόμβοι του συστήματος ενημερώνονται για την αλλαγή της κατάστασής του και μπορούν να εγκρίνουν ή να απορρίψουν την αλλαγή. Αν κάποια αλλαγή του συστήματος γίνει αποδεκτή από τους κόμβους του, προσαρτάται στο δίκτυο με τη μορφή ενός νέου αμετάβλητου block.[39]

3.3.1. Συναρτήσεις κατακερματισμού. Μια αλυσίδα κατακερματισμού (hash chain) είναι η διαδοχική εφαρμογή μιας κρυπτογραφικής συνάρτησης κατακερματισμού (hash function) σε ένα κομμάτι δεδομένων. Στην ασφάλεια υπολογιστών, μια αλυσίδα κατακερματισμού είναι μια μέθοδος για την παραγωγή πολλών κλειδιών από ένα μόνο κλειδί ή κωδικό πρόσβασης. Τα κλειδιά αυτά μπορούν να χρησιμοποιηθούν μία φορά το καθένα για απόκτηση πρόσβασης στα δεδομένα που αφορούν. Μια συνάρτηση κατακερματισμού μπορεί να εφαρμοστεί διαδοχικές φορές σε πρόσθετα κομμάτια δεδομένων προκειμένου να καταγραφεί η χρονολογία της ύπαρξης των δεδομένων. Οι κρυπτογραφικές συναρτήσεις κατακερματισμού (cryptographic hash functions) επιτρέπουν τον υπολογισμό ενός hash με εύκολο τρόπο. Ωστόσο, θεωρείται δύσκολο –πρακτικά αδύνατον– να υπολογιστούν τα στοιχεία από τα οποία προέκυψε. Οι

πλέον γνωστές κρυπτογραφικές συναρτήσεις είναι οι MD5, SHA-1, SHA-2 και SHA-3.

Στο πλαίσιο του έργου Impilo θα χρησιμοποιηθεί η συνάρτηση κατακερματισμού BLAKE2. Η BLAKE2 είναι μια κρυπτογραφική συνάρτηση κατακερματισμού ταχύτερη από τις MD5, SHA-1, SHA-2 και SHA-3, αλλά εξ ίσου ασφαλής με το τελευταίο πρότυπο SHA-3. Η BLAKE2 έχει υιοθετηθεί από πολλά έργα λόγω της υψηλής ταχύτητας, της ασφάλειας και της απλότητάς της.

Οι αλυσίδες κατακερματισμού είναι παρόμοιες με τα blockchain, καθώς και στις δύο περιπτώσεις χρησιμοποιούνται κρυπτογραφικές συναρτήσεις κατακερματισμού για τη σύνδεση δύο κόμβων. Ωστόσο, ένα blockchain γενικά έχει ως στόχο την υποστήριξη της κατανεμημένης συναίνεσης σε ένα δίκτυο και ενσωματώνει ένα σύνολο κανόνων για την ενθυλάκωση των δεδομένων και τα συναφή δικαιώματα για την πρόσβαση και τη διαχείρισή τους. Στο blockchain χρησιμοποιούνται αλγόριθμοι κατακερματισμού για τον προσδιορισμό της μοναδικής κατάστασης της αλυσίδας σε κάθε χρονική στιγμή. Τα blocks είναι συνδεδεμένοι κατάλογοι δεδομένων, ενώ, όπως προαναφέρθηκε, στην επικεφαλίδα κάθε block υπάρχει δείκτης κατακερματισμού που δείχνει το προηγούμενο block της αλυσίδας. Τα block συνδέονται μεταξύ τους μέσω δεικτών κατακερματισμού, οι οποίοι αναπαριστούν τον κατακερματισμό των δεδομένων μέσα στα προηγούμενα block μαζί με τη διεύθυνσή τους.

3.3.2. Διαχείριση κλειδιών. Η κρυπτογράφηση δημόσιου κλειδιού (public key cryptography) ή ασύμμετρου κλειδιού (asymmetric cryptography) επινοήθηκε στο τέλος της δεκαετίας του 1970 από τους Whitfield Diffie και Martin Hellman και παρέχει ένα εντελώς διαφορετικό μοντέλο διαχείρισης των κλειδιών κρυπτογράφησης από την προγενέστερη κρυπτογράφηση συμμετρικού κλειδιού. Η βασική ιδέα είναι ότι ο αποστολέας και ο παραλήπτης δεν μοιράζονται ένα κοινό μυστικό κλειδί όπως στην περίπτωση της κρυπτογράφησης συμμετρικού κλειδιού, αλλά διαθέτουν διαφορετικά κλειδιά για διαφορετικές λειτουργίες. Συγκεκριμένα, κάθε χρήστης διαθέτει δύο κλειδιά κρυπτογράφησης: το ένα ονομάζεται ιδιωτικό κλειδί (private key) και το άλλο δημόσιο κλειδί (public key). Τα δύο αυτά κλειδιά (ιδιωτικό και δημόσιο) έχουν μαθηματική σχέση μεταξύ τους. Εάν το ένα χρησιμοποιηθεί για την κρυπτογράφηση κάποιου μηνύματος, τότε το άλλο χρησιμοποιείται για την αποκρυπτογράφηση αυτού. Η επιτυχία του σχετικού είδους κρυπτογραφικών αλγορίθμων βασίζεται στο γεγονός ότι η γνώση του δημόσιου κλειδιού κρυπτογράφησης δεν επιτρέπει με κανέναν τρόπο τον υπολογισμό του ιδιωτικού κλειδιού κρυπτογράφησης. Το δημόσιο κλειδί μπορεί να γνωστοποιηθεί σε τρίτους, και χρησιμοποιείται για την κρυπτογράφηση των δεδομένων, ενώ το ιδιωτικό για την αποκρυπτογράφηση.[40]

Το μοντέλο ασφάλειας του blockchain προϋποθέτει την ύπαρξη κρυπτογραφίας δημόσιου κλειδιού. Οι ταυτότητες, περιλαμβανομένων των ταυτοτήτων χρηστών και συναλλαγών, προέρχονται από πιστοποιητικά δημόσιου κλειδιού. Επομένως, η ασφαλής διαχείριση των κλειδιών είναι απαραίτητη για όλα τα blockchain. Για το έργο Impilo συγκεκριμένα θα χρησιμοποιηθεί το Hyperledger Iroha, το οποίο συνιστά μια πλατφόρμα υλοποίησης blockchain εφαρμογών. Επομένως, η διαχείριση των δημόσιων και ιδιωτικών κλειδιών πρέπει να ακολουθήσει τις οδηγίες της συγκεκριμένης πλατφόρμας.[41]

3.3.3. Επίτευξη συναίνεσης. Ο ρόλος της συναίνεσης στα συστήματα blockchain είναι να διασφαλίσει ότι όλοι οι μη ελαττωματικοί χρήστες του δικτύου εκτελούν τις ίδιες ανανεώσεις κατάστασης του συστήματος με τη σειρά που συνέβησαν τα γεγονότα, τα οποία άλλαξαν την κατάστασή του. Η επίτευξη συναίνεσης σε αποκεντρωμένα συστήματα, όπως το blockchain του Impilo, τα οποία λαμβάνουν ασύγχρονα γεγονότα και υπόκεινται σε «βυζαντινή ανοχή σφάλματος» (Byzantine fault tolerance), είναι ένα συχνό πρόβλημα σε πολλές εφαρμογές.

Για την επίτευξη συναίνεσης στο Impilo θα γίνει χρήση του αλγόριθμου YAC (yet another consensus).[42] Ο YAC είναι ένας πρακτικός αποκεντρωμένος αλγόριθμος συναίνεσης, ο οποίος επιχειρεί να επιλύσει κλασικά προβλήματα που υπάρχουν στη βυζαντινή ανοχή σφάλματος, όπως η μη αποδοτική μετάδοση μηνυμάτων, καθώς και η κατάληψη του συστήματος από «ισχυρούς ηγέτες». Οι ισχυροί ηγέτες σε ένα blockchain σύστημα –χρήστες που καταλαμβάνουν μεγάλο μέρος των κόμβων του– μπορεί να έχουν νόημα σε ένα blockchain κρυπτονομισμάτων. Ωστόσο, σε ένα ιατρικό blockchain πρέπει να υπάρχει μεγαλύτερη ανεξαρτησία των χρηστών από τους «ηγέτες» του συστήματος. Ο συγκεκριμένος αλγόριθμος χρησιμοποιείται για παροχή βυζαντινής συναίνεσης στο Hyperledger Iroha Blockchain project. Μάλιστα, εμπειρικά αποτελέσματα δείχνουν ότι η εν λόγω λύση επιτυγχάνει μικρή αδράνεια του συστήματος, η οποία οδηγεί σε υψηλή απόδοση συναλλαγών.

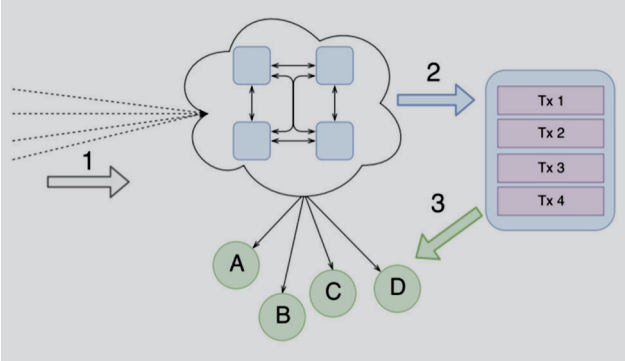
Παρακάτω θα παρουσιαστεί ο τρόπος που λειτουργεί το YAC. Αρχικά, οι τυπικοί συμμετέχοντες του YAC περιλαμβάνουν τον πελάτη, τον peer και την υπηρεσία παραγγελιών. Κάθε πελάτης είναι στην ουσία ένας χρήστης που έχει ένα δημόσιο κλειδί καταχωρημένο στο σύστημα blockchain. Ο ρόλος του πελάτη είναι η δημιουργία συναλλαγών και η αποστολή τους στην υπηρεσία παραγγελιών (ordering service). Ο πελάτης αναπτύσσει επίσης έξυπνες συμβάσεις, για να ορίσει τα δικαιώματα άλλων χρηστών στα δεδομένα του και να διενεργήσει ερωτήματα στους υπόλοιπους peers. Επί πλέον, ένας peer είναι από τους συμμετέχοντες

του δικτύου που είναι υπεύθυνοι για την επικύρωση και την επίτευξη συμφωνίας όσον αφορά στις συναλλαγές και στην αποθήκευση αυτών στα blocks του δικτύου. Οι peers διατηρούν το πλήρες ιστορικό συναλλαγών για την επικύρωση των προτάσεων. Τέλος, η υπηρεσία παραγγελιών είναι μια μονάδα η οποία λαμβάνει ένα σύνολο συναλλαγών και δημιουργεί προτάσεις για νέα blocks. Μια πρόταση block περιέχει μια λίστα συναλλαγών, η οποία πρέπει να συμφωνηθεί ανάμεσα στους peers.

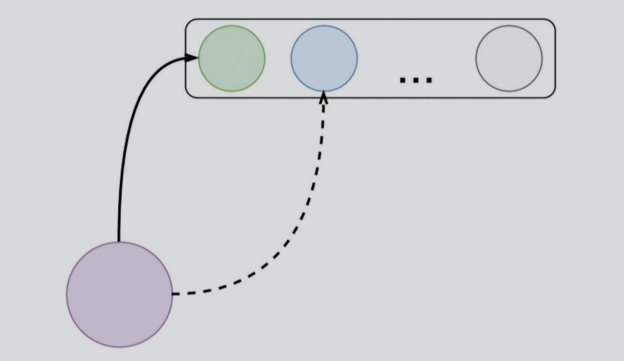
Για την παρουσίαση του τρόπου λειτουργίας του αλγόριθμου θα γίνει ένας αριθμός από υποθέσεις. Αρχικά, θεωρείται ότι ο πελάτης είναι γνωστός στους peers καθώς και ότι κάθε πελάτης διαθέτει μια λίστα από peers με τους οποίους μπορεί να αλληλεπιδράσει. Επί πλέον, γίνεται η υπόθεση ότι ο πελάτης έχει τα δικά του κλειδιά αποθηκευμένα σε κάποια συσκευή (π.χ. στο κινητό του). Τρίτον, ο πελάτης έχει δικαιώματα εκτέλεσης ενός συγκεκριμένου υποσυνόλου εντολών/έξυπνων συμβάσεων (π.χ. δημιουργία συναλλαγής). Η γενική ροή λειτουργίας του συστήματος μπορεί να περιγραφεί με τα ακόλουθα βήματα. Αρχικά, ένας πελάτης δημιουργεί μια συναλλαγή μέσω εντολών που έχει δικαίωμα να εκτελέσει και την υπογράφει με το ιδιωτικό του κλειδί. Στη συνέχεια, ο πελάτης αποστέλλει τη συναλλαγή σε έναν peer, ο οποίος τη λαμβάνει, την επικυρώνει ώστε να βεβαιωθεί ότι έχει τη σωστή μορφή –όπως αυτή ορίζεται από το σύστημα– και τη μεταβιβάζει στην υπηρεσία παραγγελιών. Τέλος, η υπηρεσία παραγγελιών σχηματίζει μια πρόταση, η οποία περιέχει μια λίστα συναλλαγών που δυνητικά θα προστεθεί στο blockchain. Η πρόταση μπορεί να σχηματιστεί εφόσον η υπηρεσία παραγγελιών έχει συλλέξει έναν συγκεκριμένο αριθμό συναλλαγών ή μετά το πέρας συγκεκριμένου χρονικού διαστήματος. Στη συνέχεια, η πρόταση αποστέλλεται στο σύνολο των peers του συστήματος. Αυτή η διαδικασία παρουσιάζεται σχηματικά στην εικόνα 4. Έπειτα, οι peers ανταλλάσσουν ψήφους μέσω του συστήματος και τελικά αποφασίζουν για το νέο block. Στην ουσία, σε αυτό το στάδιο, κάθε peer πρέπει να υπολογίσει αν η πρόταση (σύνολο συναλλαγών) που έστειλε η υπηρεσία παραγγελιών είναι έγκυρη. Το block που δημιουργείται από τον peer περιέχει ένα προτεινόμενο hash, συναλλαγές της επικυρωμένης πρότασης και επί πλέον με τα δεδομένα τα οποία απαιτούνται για την κρυπτογραφική επικύρωση της αλυσίδας. Το προτεινόμενο hash ορίζει μια μοναδική πρόταση για κάθε γύρο συναλλαγών. Το block hash αντιπροσωπεύει την πρόθεση του peer για αποθήκευση ενός υποσυνόλου των συναλλαγών στην αλυσίδα. Αυτά τα hashes είναι απαραίτητα, καθώς κάθε peer μπορεί να υπολογίσει διαφορετικά blocks από μια πρόταση. Στη συνέχεια, οι peers πρέπει να στείλουν μέσω μηνύματος την ψήφο τους. Το εν λόγω μήνυμα περιλαμβάνει τα προαναφερθέντα hashes και μια υπογραφή που πιστοποιεί τον peer. Η σειρά με την οποία οι peers θα ψηφίσουν για ένα block hash καθορίζεται από μια ειδική συνάρτηση (permutation function). Κατά τη διαδικασία ψηφοφορίας, λοιπόν, το μήνυμα αποστέλλεται στον πρώτο peer της λίστας και στη συνέχεια στον επόμενο είτε αφού ο πρώτος στείλει την ψήφο του, είτε μετά το πέρας συγκεκριμένου χρονικού διαστήματος, όπως φαίνεται στην εικόνα 5. Η διαδικασία αυτή συνεχίζεται μέχρι το δίκτυο να λάβει ένα έγκυρο μήνυμα για αποδοχή ή απόρριψη των αλλαγών. Η αποδοχή στο δίκτυο απαιτεί τουλάχιστον τα 2/3 του δικτύου. Όταν ένας peer λάβει την πλειοψηφία του δικτύου μεταδίδει στους υπόλοιπους ένα μήνυμα αποδοχής. Τέλος, ο peer στον οποίο στάλθηκε αρχικά η συναλλαγή αποθηκεύει το block στο τοπικό του αντίγραφο.

4. ΣΥΜΠΕΡΑΣΜΑΤΑ

Σκοπός της παρούσας δημοσίευσης ήταν η ανάλυση του ερευνητικού πεδίου όσον αφορά στο έργο Impilo, καθώς και η παρουσίαση της μεθοδολογίας και της αρχιτεκτονικής που έχουν αναπτυχθεί στο πλαίσιο του έργου. Αρχικά, η σχετική βιβλιογραφία που μελετήθηκε υποστηρίζει την



Εικόνα 4. Αποστολή συναλλαγών.



Εικόνα 5. Διαδικασία ψηφοφορίας.

εφαρμογή της τεχνολογίας blockchain σε συνδυασμό με δημοφιλή ιατρικά πρότυπα για τη δόμηση της ιατρικής πληροφορίας. Επί πλέον, ερευνήθηκε το νομικό πλαίσιο που διέπει την αποθήκευση και την επεξεργασία ευαίσθητων ιατρικών δεδομένων, καθώς και τα μέτρα που θα εφαρμοστούν στο πλαίσιο του Impilo για τη συμμόρφωση των δραστηριοτήτων του με το υπάρχον νομικό καθεστώς.

Στο τεχνικό μέρος της δημοσίευσης, παρουσιάστηκαν ερευνητικές προσεγγίσεις σχετικά με τη δόμηση ιατρικών δεδομένων μέσω blockchain και στη συνέχεια περιγράφηκε η μεθοδολογία και η αρχιτεκτονική που θα ακολουθήσει το Impilo για τη δόμηση της ιατρικής πληροφορίας. Το σύστημα που θα αναπτυχθεί σχεδιάστηκε με μια βασική σύμβαση. Δεδομένων των περιορισμών που προσθέτει το GDPR, το blockchain θα χρησιμοποιείται για την παρακολούθηση και την επικύρωση των συναλλαγών ανάμεσα στους χρήστες του συστήματος, ενώ τα πραγματικά δεδομένα θα διατηρούνται σε κεντρικές βάσεις. Με αυτόν τον τρόπο, το δίκτυο αφ' ενός επωφελείται από τις ιδιότητες του blockchain για ασφάλεια και σταθερότητα και αφ' ετέρου είναι ευέλικτο στις απαιτήσεις των χρηστών. Στο τελευταίο τμήμα της δημοσίευσης περιγράφηκαν οι τεχνικές που θα εφαρμοστούν για τη διασφάλιση των δεδομένων υγείας και, πιο συγκεκριμένα, οι συναρτήσεις κατακερματισμού, η διαχείριση κλειδιών και η επίτευξη συναίνεσης στο δίκτυο.

Συνολικά, μπορεί να αναφερθεί ότι η εφαρμογή της τεχνολογίας blockchain σε τομείς εκτός από κρυπτονομίσματα έχει ιδιαίτερη αξία. Αυτό φαίνεται και από το συνεχώς αυξανόμενο ερευνητικό ενδιαφέρον σχετικά με το blockchain, σε τομείς όπου παραδοσιακά δεν είχε εφαρμογή. Ειδικά στον τομέα της υγείας, στον οποίο δραστηριοποιείται το Impilo, το blockchain ενδέχεται να δημιουργήσει περισσότερο αξιόπιστα και ανθεκτικά δίκτυα, συνδράμοντας παράλληλα στην απρόσκοπτη επικοινωνία ανάμεσα στα διάφορα ενδιαφερόμενα μέρη (ιατροί, ασθενείς, νοσοκομεία κ.λπ.).

Τα επόμενα βήματα του ερευνητικού έργου Impilo περιλαμβάνουν την ανάπτυξη του συστήματος και την πιλοτική εφαρμογή του σε συγκεκριμένους παρόχους υγειονομικής περίθαλψης και δείγμα ασθενών.

ΕΠΙΧΟΡΗΓΗΣΕΙΣ

Το έργο IMPILO χρηματοδοτείται από το επιχειρησιακό πρόγραμμα «Ανταγωνιστικότητα, επιχειρηματικότητα, καινοτομία» – ΕΠΑνΕΚ κίνηση (2014–2020), στη δράση εθνικής εμβέλειας: «ΕΡΕΥΝΩ – ΔΗΜΙΟΥΡΓΩ – ΚΑΙΝΟΤΟΜΩ», με κωδικό έργου Τ1ΕΔΚ-01382.

ABSTRACT

Methodology for secure storage and information exchange of medical data based on blockchain

C. KONTZINOS,[1] M. KONTOULIS,[1] P. KAPSALIS,[1] O. MARKAKI,[1] S. MOUZAKITIS,[1] R. MANTA,[2] T. ANDROUTSOU,[2] I. KOURIS,[2] H. KARANIKAS,[3] A. BILLIRIS,[4] A. CHRISTODOULAKIS,[4] E. THIREOS[5]

[1]Laboratory of Decision Support Systems, National Technical University of Athens, Athens, [2]Laboratory of Biomedical Engineering, National Technical University of Athens, Athens, [3]Department of Computer Science and Biomedical Informatics, University of Thessaly, Lamia, [4]Datamed SA, Athens, [5]Athens Medical Society, Athens, Greece

Archives of Hellenic Medicine 2020, 37(4):542–554

The rapid technological developments of the 21st century and the adoption of Internet 4.0 technologies in all facets of everyday life, has led to the digitization of services even in areas that have traditionally operated without the help of technology. One of the areas that is being modernized due to the abovementioned developments is that of health care. Medical process automation, robotics and medical devices are creating a wealth of digital health data. Each patient's health data is organized and structured in electronic health records (EHR), which are usually stored in the central databases of healthcare providers. Although EHRs offer many possibilities, the centralized data storage makes them vulnerable to malicious attack, and they do not provide interoperability between the systems of different healthcare providers. Blockchain is a technology that provides appropriate solutions and which can eliminate the abovementioned challenges in the healthcare sector. Decentralized data storage and data management by the patients themselves can provide greater security, interoperability and, generally, more efficient health services. The scope of this paper work is to present the challenges in the field of eHealth, to introduce blockchain as a solution for most of these challenges, and to present appropriate methodology that can be used to store medical data in a healthcare application based on blockchain. The methodology presented is already being developed and applied

in the context of the Impilo research project, which aims to develop a blockchain-based social networking application in the healthcare domain.

Key words: Blockchain, Electronic health record, GDPR, Interoperability, Medical data, Security

Βιβλιογραφία

1. SEGEN JC. *Concise dictionary of modern medicine.* McGraw-Hill Education, New York, 2006
2. TZOURAKIS MC. The healthcare industry and data quality. Proceedings of the 1996 International Conference on Information Quality, 1996:87–93
3. GUNTER TD, TERRY NP. The emergence of national electronic health record architectures in the United States and Australia: Models, costs, and questions. *J Med Internet Res* 2005, 7:e3
4. TOP MOBILE TRENDS. Mobile tech contributions to healthcare and patient experiences. Top Mobile Trends, 2014. Available at: http://topmobiletrends.com/ mobile-technology-contributions-patient-experience-parmar/
5. YUE X, WANG H, JIN D, LI M, JIANG W. Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. *J Med Syst* 2016, 40:218
6. KEMKARL OS, DAHIKAR DPB. Can electronic medical record systems transform health care? Potential health benefits, savings, and cost using latest advancements in ict for better interactive healthcare learning. *Int J Comput Sci Commun Netw* 2012, 2:453–455
7. GE Y, AHN DK, UNDE B, GAGE HD, CARR JJ. Patient-controlled sharing of medical imaging data across unaffiliated healthcare organizations. *J Am Med Inform Assoc* 2013, 20:157–163
8. JOTHI N, RASHID NAA, HUSAIN, W. Data mining in healthcare – A review. *Procedia Comput Sci* 2015, 72:306–313
9. ZHANG Y, CHEN M, HUANG D, WU D, LI Y. iDoctor: Personalized and professionalized medical recommendations based on hybrid matrix factorization. *Future Gener Comp Sy* 2017, 66:30–35
10. HL7 INTERNATIONAL. Health level 7. 1st ed. HL7, 1989. Available at: http://www.hl7.org/implement/standards/
11. HL7 INTERNATIONAL. Fast Health Interoperability Resources (FHIR). 4th ed. HL7, 2018. Available at: https://www.hl7.org/fhir/
12. OPENEHR FOUNDATION. OpenEHR. 3rd ed. 2018. Available at: https://www.openehr.org/
13. ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗ ΚΟΙΝΩΝΙΚΗΣ ΑΣΦΑΛΙΣΗΣ. Ηλεκτρονικός φάκελος υγείας (ΗΦΥ). 1η έκδοση. Διαθέσιμο στο: http://www.idika.gr/pfy/ηλεκτρονικος-φακελος-υγειας-ηφυ.html (πρόσβαση 10.12.2019)
14. CLIFTON C, KANTARCIOĞLU M, DOAN A, SCHADOW G, VAIDYA J, ELMAGARMID A ET AL. Privacy-preserving data integration and sharing. Proceedings of the 9th ACM SIGMOD Workshop on Research Issues in Data Mining and Knowledge Discovery, Paris, 2004:19–26
15. ONTARIO NURSES' ASSOCIATION GENERAL COUNCIL. Members and patient privacy: Be aware and beware! ONA, Toronto, 2016. Available at: https://www.ona.org/
16. PETERSON K, DEEDUVANU R, KANJAMALA P, BOLES K. A blockchain-based approach to health information exchange networks. Proceedings of NIST Workshop Blockchain Healthcare, Gaithersburg, 2016:1–10
17. BARROWS RC Jr, CLAYTON PD. Privacy, confidentiality, and electronic medical records. *J Am Med Inform Assoc* 1996, 3:139–148
18. ESPOSITO C, DE SANTIS A, TORTORA G, CHANG H, CHOO KKR. Blockchain: A panacea for healthcare cloud-based data security and privacy? *IEEE Cloud Comput* 2018, 5:31–37
19. NAKAMOTO S. Bitcoin: A peer-to-peer electronic cash system, 2008. Available at: https://bitcoin.org/bitcoin.pdf
20. DRESCHER D. *Blockchain basics: A non-technical introduction in 25 steps.* 1st ed. Apress, Frankfurt, 2017
21. KOTOBI K, BILEN SG. Secure blockchains for dynamic spectrum access: A decentralized database in moving cognitive radio networks enhances security and user access. *IEEE Veh Technol Mag* 2018, 13:32–39
22. FRANCO P. *Understanding bitcoin: Cryptography, engineering, and economics.* 1st ed. Wiley Finance Series, New York, NY, 2014
23. AGBO CC, MAHMOUD QH, EKLUND JM. Blockchain technology in healthcare: A systematic review. *Healthcare (Basel)* 2019, 7:2
24. PETRE A, HAÏ N. Opportunities and challenges of blockchain technology in the healthcare industry. *Med Sci (Paris)* 2018, 34:852–856
25. ΒΙΚΙΠΑΙΔΕΙΑ. Κρυπτονόμισμα. Διαθέσιμο στο: https://el.wikipedia.org/wiki/Κρυπτονόμισμα (πρόσβαση 10.12.2019)
26. BOWHEAD HEALTH. Bowhead. Available at: https://bowheadhealth.com/ (accessed 10.12.2019)
27. ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ. Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων). Eur-Lex, 2016. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32016R0679
28. COUNCIL OF THE EUROPEAN UNION. 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. Brussels, 2015. Available at: https://www.swlaw.com/publications/legal-alerts/2544
29. ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ. Ισχύς του GDPR από 25 Μαΐου 2018. Διαθέσιμο στο: https://eugdpr.org/
30. ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ. Γενι-

κός κανονισμός για την προστασία δεδομένων. Διαθέσιμο στο: https://www.dpa.gr/ portal/page?_pageid=33,213319&_dad=portal&_schema=PORTAL (πρόσβαση 10.12.2019)
31. EUROPEAN COMMISSION. General Data Protection Regulation – chapter 3. GDPR, 2016. Available at: https://gdpr-info.eu/art-3-gdpr/
32. EUROPEAN COMMISSION. General Data Protection Regulation – chapter 5. GDPR, 2016. Available at: https://gdpr-info.eu/art-5-gdpr/
33. ΕΦΗΜΕΡΙΣ ΤΗΣ ΚΥΒΕΡΝΗΣΕΩΣ. Νόμος 2472/1997. Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα – Δικαίωμα πρόσβασης (άρθρο 12). ΦΕΚ 50/Α/10.4.1997. Διαθέσιμο στο: https://www.dpa.gr/portal/ page?_pageid=33,19052&_dad=portal &_schema=PORTAL#12
34. ΕΦΗΜΕΡΙΣ ΤΗΣ ΚΥΒΕΡΝΗΣΕΩΣ. Νόμος 3418/2005. Κώδικας ιατρικής δεοντολογίας. ΦΕΚ 287/Α/28.11.2005. Διαθέσιμο στο: http://www.dpa.gr/APDPXPortlets/htdocs/documentDisplay.jsp?docid=162,112,178,83,91,84,31,147
35. EKBLAW A, AZARIA A, HALAMKA J, LIPPMAN A. A case study for blockchain in healthcare: "MedRec" prototype for electronic health records and medical research data. Proceedings of IEEE Open & Big Data Conference, Washington, DC, 2016:13
36. GORDON WJ, CATALINI C. Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability. *Comput Struct Biotechnol J* 2018, 16:224–230
37. BECKER G. Merkle signature schemes, merkle trees and their cryptanalysis. Ruhr-University Bochum, Tech. Rep 2008
38. IOANNIDIS J. *Applied cryptography and network security.* ACNS, New York, NY, 2005
39. MOHANTA BK, JENA D, PANDA SS, SOBHANAYAK S. Blockchain technology: A survey on applications and security privacy challenges. *Internet Things* 2019, 8:100–107
40. STALLINGS W. *Cryptography and network security: Principles and practice.* 2nd ed. Prentice-Hall Inc, Upper Saddle River, NJ, 1998
41. HYPERLEDGER. Hyperledger Iroha documentation. Available at: https://iroha.readthedocs.io/en/latest/ (accessed 10.12.2019)
42. MURATOV F, LEBEDEV A, IUSHKEVICH N, NASRULIN B, TAKEMIYA M. YAC: BFT consensus algorithm for blockchain. arXiv, 2018

Corresponding author:

C. Kontzinos, Laboratory of Decision Support Systems, National Technical University of Athens, Athens, Greece
e-mail: ckon@epu.ntua.gr