



ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
[ΠΛΗΡΟΦΟΡΙΑΚΑ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΑ ΣΥΣΤΗΜΑΤΑ]

“Η τεχνολογία Blockchain στον τομέα της Υγείας”

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της

ΑΝΑΣΤΑΣΙΑΣ Γ. ΙΝΤΖΕ

Επιβλέπων : ΓΕΩΡΓΙΟΣ ΚΟΡΜΕΤΖΑΣ

Μέλη εξεταστικής επιτροπής: ΣΚΟΥΤΑΣ ΔΗΜΗΤΡΙΟΣ, ΚΑΠΟΡΗΣ ΑΛΕΞΗΣ

Σάμος, Οκτώβριος 2020

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πρόλογος και ευχαριστίες

Θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή μου Κ. Κορμέντζα Γεώργιο για την ανάθεση της πολύ ενδιαφέρουσας διπλωματικής εργασίας στο χώρο του blockchain, καθώς και για την εμπιστοσύνη που μου έδειξε κατά τη διάρκεια της εκπόνησής της. Ευχαριστώ επίσης τον καθηγητή μου για τις πολύτιμες γνώσεις που αποκόμισα από τον ίδιο καθ'όλη τη διάρκεια του μεταπτυχιακού προγράμματος.

Εν συνεχεία, για την έως τώρα σταδιοδρομία μου θα ήθελα να ευχαριστήσω θερμά τους γονείς μου Γεώργιο και Άννα για την αμέριστη και συνεχή συμπαράστασή τους και για όλα όσα μου έχουν προσφέρει όλα αυτά τα χρόνια της ζωής μου και σπουδών μου.

Ευχαριστώ επίσης τα αδέρφια μου Στέργιο, Αθηνόδωρο και Σωτηρία που είναι πάντα δίπλα μου και με στηρίζουν σε όλες μου τις επιλογές. Ευχαριστώ τον παππούλη μου Γέροντα Μάξιμο που προσεύχεται για εμένα και με ενισχύει πνευματικά.

Ιδιαίτερα θερμές ευχαριστίες θέλω να δώσω στο σύζυγό μου Θεόδωρο που με υπομονή και αγάπη μου προσέφερε την απαραίτητη ηθική συμπαράσταση για την ολοκλήρωση της διπλωματικής μου εργασίας.

Χωρίς τους ανθρώπους που ανέφερα δεν θα μπορούσα να έχω φτάσει στο σημείο που είμαι σήμερα.

Τέλος, ευχαριστώ όλους τους καθηγητές, το υποστηρικτικό προσωπικό και όλους τους ανθρώπους που συντελούν στην άψογη λειτουργία του Πανεπιστημίου Αιγαίου.

Η παρούσα διπλωματική εργασία αφιερώνεται στη μνήμη του Κωνσταντίνου Κατσίφα που την 28^η Οκτωβρίου συμπληρώνονται 2 χρόνια από τη δολοφονία του.

© 2020

της

ΑΝΑΣΤΑΣΙΑΣ Γ. INTZE

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πίνακας περιεχομένων

1	Εισαγωγή	Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.
2	Θεωρητικό υπόβαθρο -Συσχετιζόμενες εταιρίες και εργασίες	7
2.1	Bitcoin	7
2.2	Κρυπτονομίσματα: Προκλήσεις και Λύσεις	8
2.2.1	Peer-to-peer double spending problem	8
2.2.2	Single-point-of-failure	8
2.2.3	The Bitcoin blockchain solution	8
2.3	Μηχανισμός blockchain	9
2.3.1	PoW Πρωτόκολλο	10
2.3.2	Κακόβουλες αλυσίδες	11
2.4	Απλοποιημένο blockchain	12
2.5	Ανατομία του Block	14
2.6	Εναλλακτικά blockchains	15
2.7	Τύποι blockchain	16
2.8	Συσχετιζόμενες εταιρίες και εργασίες	17
2.8.1	Εργασίες σχετικά με την ανταλλαγή, διαχείριση, αποθήκευση δεδομένων και EHRs	24
2.8.2	Εργασίες σχετικά με τις κλινικές δοκιμές	27
2.8.3	Εργασίες σχετικά με τη φαρμακευτική	28
2.8.4	Εργασίες σχετικά με το IoT και τις ιατρικές συσκευές	28
2.8.5	Εργασίες σχετικά με την Τεχνητή Νοημοσύνη	32
3	Εφαρμογές	33
3.1	Data Management apps	36
3.1.1	Παγκόσμια ανταλλαγή επιστημονικών δεδομένων για έρευνα και ανάπτυξη (data sharing)	37
3.1.2	Διαχείριση δεδομένων (data management)	38
3.1.3	Αποθήκευση δεδομένων (data storage)	38
3.1.4	Ηλεκτρονικά αρχεία υγείας : EHRs (electronic health records)	38
3.2	Supply Chain Management (SCM) apps	40
3.2.1	Κλινικές δοκιμές (clinical trials)	43
3.2.2	Φαρμακευτική (pharmaceutical)	43
3.3	Internet of Medical Things (IoMT) apps	44
3.3.1	IoT στην Υγειονομική περίθαλψη και Ιατρικές συσκευές (Healthcare IoT and Medical devices)	45

3.3.2 Υποδομή των IoT στην Υγειονομική περίθαλψη και Ασφάλεια των δεδομένων (Healthcare IoT Infrastructure and Data Security)	45
3.3.3 Τεχνητή Νοημοσύνη (Artificial Intelligence)	46
3.4 Απομακρυσμένη παρακολούθηση ασθενών (remote patient monitoring)	46
3.4.1 Περιγραφή του συστήματος.....	48
3.4.2 Ροή εκτέλεσης του συστήματος	50
3.4.3 Ανάλυση του συστήματος και σύγκριση με το παραδοσιακό σύστημα	51
3.5 Ιατρική Εκπαίδευση (medical education)	52
3.5.1 Περιγραφή του συστήματος <i>VECefblock</i>	57
3.5.2 Ροή εκτέλεσης του συστήματος <i>VECefblock</i>	59
3.6 Γονιδιωματικά δεδομένα (genomic data generation)	60
3.6.1 Περιγραφή του συστήματος <i>NEBULA BLOCKCHAIN</i>	66
3.6.2 Ροή εκτέλεσης του συστήματος <i>NEBULA BLOCKCHAIN</i>	68
3.7 Βελτίωση ποιότητας Κλινικών Δοκιμών (Clinical research quality)_	75
3.7.1 Ροή εκτέλεσης του συστήματος	76
3.8 Γεωχωρικές εφαρμογές για έξυπνες υγιείς πόλεις (Geospatial application for smart healthy cities) .	78
3.8.1 Έξυπνο Ασθενοφόρο	79
3.8.2 Απινιδωτής σε drone	80
3.9 Νευροεπιστήμες (Neuroscience)	82
3.10 Διαχείριση δεδομένων εγγραφής (Enrollment Data Management)	84
3.11 Διαχείριση απαιτήσεων τιμολογίων (Claims and Billing Management)	88
3.12 Εντοπισμός απάτης (fraud detection) και Διαχείριση Ποιότητας (Quality management)	89
3.13 Μοντέλα πρόβλεψης για την προστασία της ιδιωτικής ζωής (privacy-preserving predictive models)	92
4 Προκλήσεις	94
4.1 Διαφάνεια (transparency) - Εμπιστευτικότητα (confidentiality)	94
4.2 Ταχύτητα (speed)	94
4.3 Επεκτασιμότητα (scalability)	95
4.4 Απειλή επίθεσης 51% (threat of 51% attack).....	95
4.5 Ασφάλεια (Security)	96
4.6 Αποθήκευση (Storage).....	97
4.7 Τροποποίηση (modification).....	97
4.8 Προστασία της ιδιωτικότητας και κανονισμοί (Privacy and Regulations).....	98
4.8.1 Blockchain και GDPR.....	99
5 Επίλογος.....	102
5.1 Μελλοντικές προοπτικές.....	102

5.2	Επιπτώσεις και συμπεράσματα	102
Βιβλιογραφία	104

Λίστα Σχημάτων

Εικόνα 1.1 : Ροή εργασίας της διαδικασίας blockchain	5
Εικόνα 2.1 : Το πρόβλημα της διπλής δαπάνης χωρίς κεντρικό διαμεσολαβητή	8
Εικόνα 2.2: Σύγκριση των τοπολογιών κατανεμημένων δικτύων	9
Εικόνα 2.3: Παράδειγμα απλοποιημένου blockchain (hash-chain)	9
Εικόνα 2.4: Παράδειγμα του μηχανισμού nonce για το PoW πρωτόκολλο	10
Εικόνα 2.5: Παράδειγμα του πώς το blockchain διαχειρίζεται τις αλυσίδες διακλάδωσης	12
Εικόνα 2.6 : Απλοποιημένο blockchain τριών blocks	13
Εικόνα 2.7 : Απλοποιημένο blockchain με πειραγμένο block	13
Εικόνα 2.8: Ανατομία του block	14
Εικόνα 2.9 : Διάφοροι τύποι της τεχνολογίας blockchain	17
Εικόνα 3.1 : Αναπαράσταση της ροής εργασίας των εφαρμογών υγειονομικής περίθαλψης που βασίζονται στο blockchain	33
Εικόνα 3.2: Οι ενδιαφερόμενοι για τα δεδομένα υγειονομικής περίθαλψης	35
Εικόνα 3.3: Διαχείριση δεδομένων υγειονομικής περίθαλψης στο blockchain	36
Εικόνα 3.4: EMR	39
Εικόνα 3.5: Δεδομένα αισθητήρων	39
Εικόνα 3.6: Διαχείριση της εφοδιαστικής αλυσίδας στο blockchain.....	41
Εικόνα 3.7: Internet of medical things (IoMT) στο blockchain	44
Εικόνα 3.8: Τα ακατέργαστα δεδομένα των αισθητήρων συγκεντρώνονται από τη κύρια συσκευή και έπειτα αποστέλλονται στους κόμβους του blockchain για επεξεργασία από το έξυπνο συμβόλαιο	49

Εικόνα 3.9: Τα προσαρμοσμένα δεδομένα των έξυπνων συσκευών αποστέλλονται στα έξυπνα συμβόλαια, τα οποία επεξεργάζονται και εκτελούν τις απαραίτητες ενέργειες, με βάση τα αποτελέσματα και τις προκαθορισμένες παραμέτρους	49
Εικόνα 3.10: Η λογική ροή εκτέλεσης του συστήματος	50
Εικόνα 3.11: Οι εννέα κατηγορίες της Ιατρικής Εκπαίδευσης	53
Εικόνα 3.12: Ιδανικός σχεδιασμός	54
Εικόνα 3.13: Σχεδιασμός των τεσσάρων φάσεων του VECefblock	57
Εικόνα 3.14: Αρχιτεκτονική του συστήματος	58
Εικόνα 3.15: VECefblock επιχειρηματική διαδικασία	59
Εικόνα 3.16: Κόστος αλληλουχίας ανθρώπινου γονιδιώματος, 2001-2018	60
Εικόνα 3.17: Το παραδοσιακό μοντέλο για τη δημιουργία και κοινή χρήση των γονιδιωματικών μοντέλων	61
Εικόνα 3.18: Εναλλακτικό μοντέλο που μπορεί να αντιμετωπίσει τις προκλήσεις	63
Εικόνα 3.19: Πλατφόρμα NEBULA	66
Εικόνα 3.20: Επιδότηση πληρωμής για την αλληλουχία του γονιδιώματος στο blockchain ...	68
Εικόνα 3.21: Τα blocks δεδομένων αποθηκεύονται στο KEEP. Οι κατακερματισμοί αποθηκεύονται στο blockchain	70
Εικόνα 3.22: Απλοποιημένη παρουσίαση μιας “tile library” και ενός CGF αρχείου. Τα ορθογώνια αντιπροσωπεύουν παραλλαγές των tile διαφορετικών θέσεων. Η διακεκομμένη γραμμή απεικονίζει τη σύνθεση των tiles συγκεκριμένου γονιδιώματος	71
Εικόνα 3.23: Ασφαλής ανακάλυψη δεδομένων μέσω ερωτημάτων στα ομομορφικά κρυπτογραφημένα δεδομένα	72
Εικόνα 3.24: Έλεγχος πρόσβασης στα δεδομένα και αγορά δεδομένων	74
Εικόνα 3.25: Ροή εργασίας σύνθετων κλινικών δοκιμών κωδικοποιημένη σε blockchain	76
Εικόνα 3.26: Προτεινόμενο μοντέλο	79
Εικόνα 3.27: Ανάγκη για ασθενοφόρο ή όχι	80

Εικόνα 3.28: Το drone ενσωματώνεται με μια συσκευή IoT, επιτρέποντάς της να έχει πλήρεις δυνατότητες blockchain	82
Εικόνα 3.29: Εγγραφή ταυτότητας χρήστη στο blockchain	85
Εικόνα 3.30α: Δημιουργία και κοινή χρήση ενός EMR σε ένα blockchain (α μέρος)	86
Εικόνα 3.30β: Δημιουργία και κοινή χρήση ενός EMR σε ένα blockchain (β μέρος)	87
Εικόνα 3.31: Ερώτηση στο EMR σε ένα blockchain	88
Εικόνα 3.32: Απλοποιημένη εφοδιαστική αλυσίδα φαρμάκων βασισμένη στην τεχνολογία blockchain	91
Εικόνα 4.1: Απειλή επίθεσης 51%	96
Εικόνα 4.2: Κύκλος κινδύνου για την ασφάλεια των μεγάλων δεδομένων υγειονομικής περίθαλψης	97
Εικόνα 4.3: off-chain blockchain αρχιτεκτονική	100
Εικόνα 4.4: Συνεργασία του blockchain συμβατή με το GDPR για τα μεγάλα δεδομένα υγειονομικής περίθαλψης	101

Λίστα Πινάκων

Πίνακας 3.1 : Ανάλυση του συστήματος blockchain και σύγκριση με το παραδοσιακό σύστημα	51
Πίνακας 3.2 : Σύγκριση των πλατφορμών βιοπληροφορικής	64
Πίνακας 3.3 : Σύγκριση των πλαισίων Blockchain	65
Πίνακας 3.4 : Σύγκριση των privacy-preserving τεχνολογιών	65
Πίνακας 4.1 : Κανονισμοί προστασίας της Ιδιωτικότητας για τις διάφορες χώρες και οργανισμούς..	98

Ακρωνύμια

DLT	Distributed ledger technology
P2P	Peer to peer
EHR	Electronic health records
EMR	Electronic medical records
SCM	Supply chain management
DDBMS	Distributed database management system
SHA-256	Secure hash algorithm
ECDSA-256	Elliptic curve digital signature algorithm
POW	Proof of work
BTC	Bitcoin
CPU	Central processing unit
KSI	Keyless Signature Infrastructure
UAE	United Arab Emirates
HIPPA	Health Insurance portability and accountability act
GDPR	General data protection regulation
UHC	Universal Health Coin
PHI	Personal health information
PHR	Personal health records
PCOR	Patient centered outcomes research
NIST	National Institute of standards and technology
PoET	Proof of elapsed time
PoS	Proof of stake
PBFT	Practical byzantine fault tolerance
RFID	Radio frequency identification
PSN	Pervasive Social Network
APIs	Application program interface
IDSs	Intrusion Detection Systems
ADS	Anomaly detection System
MDS	Misuse detection
ITI	Information Technology Infrastructure
PD	Parkinson Disease
WBAN	Wireless body- area network

ICT	Information and Communication Technology
DApps	Decentralized Applications
CPD	Continuing Professional Development
HPO	Human Phenotype Ontology
FHIR	Fast Healthcare Interoperability Resources
AES	Advanced encryption standard
AWS	Amazon Web Services
GCP	Google Cloud Platform
CGF	Compact Genome Format
CWL	Common Workflow Language
OSMaps	Ordnance Survey map data
S.A.	Smart ambulance
ToF	Time of Flight
CA	Client app
ECert	Enrollment Certificate
TCert	Transaction Certificate
IoMT	Internet of medical things
CRAB	Create Retrieve Append Burn

Περίληψη

Στις μέρες μας η τεχνολογία blockchain έχει συγκεντρώσει την προσοχή όλων, με αυξανόμενο ενδιαφέρον για πληθώρα εφαρμογών, από τη δημιουργία του κρυπτονομίσματος Bitcoin έως τις μη- χρηματοοικονομικές υπηρεσίες. Τα τελευταία χρόνια λόγω της ραγδαίας ανάπτυξης της τεχνολογίας αυτής, οι επιστήμονες εξέτασαν νέους τρόπους εφαρμογής της τεχνολογίας σε ένα ευρύ φάσμα τομέων, συμπεριλαμβανομένου του τομέα Υγείας.

Το blockchain είναι μια τεχνολογία κοινού, κατακεταμμένου, ψηφιακού ημερολογίου, η οποία διευκολύνει τη διαχείριση, την προέλευση και την ασφάλεια των δεδομένων. Πρόκειται για μια αλυσίδα που καλύπτει πληροφορίες και διατηρεί την εμπιστοσύνη μεταξύ των ατόμων, ανεξαρτήτου τοποθεσίας, βελτιώνοντας τον έλεγχο της αυθεντικότητας και της διαφάνειας των δεδομένων υγειονομικής περίθαλψης.

Η βασική αρχή του blockchain είναι ότι κάθε υπηρεσία που βασίζεται σε αξιόπιστους τρίτους μπορεί να κατασκευαστεί με έναν διαφανή, αποκεντρωμένο και ασφαλή τρόπο στον οποίο δεν απαιτείται εμπιστοσύνη. Στην πραγματικότητα υπάρχει εμπιστοσύνη αλλά είναι σκληρά κωδικοποιημένη μέσω ενός σύνθετου κρυπτογραφικού αλγορίθμου. Οι χρήστες κατέχουν υψηλό βαθμό ελέγχου, αυτονομίας, εμπιστοσύνης και ακεραιότητας των δεδομένων. Επίσης, το blockchain επιτρέπει την επίτευξη σημαντικού επιπέδου ιστορικότητας των δεδομένων, χωρίς να επιτρέπεται η οποιαδήποτε παραβίαση, για ολόκληρη τη ροή των δεδομένων. Τέλος, η τεχνολογία εξασφαλίζει τον λεπτομερή έλεγχο των δεδομένων και την ασφάλειά τους για κάθε ενδιαφερόμενο που συμμετέχει στο δίκτυο των ομότιμων κόμβων P2P.

Οι blockchain λύσεις διερευνώνται για: τη διατήρηση αδειών στα ηλεκτρονικά αρχεία υγείας (EHRs), τη διαχείριση της φαρμακευτικής εφοδιαστικής αλυσίδας και της αλυσίδας των ιατρικών συσκευών, την κλινική έρευνα και τη νομιμοποίηση των δεδομένων, την ανίχνευση ιατρικής απάτης και την ενίσχυση της συμμόρφωσης, την επιτήρηση της δημόσιας υγείας, την τροφοδοσία πολλών αυτόνομων συσκευών που συνδέονται στο IoT, τις φορητές συσκευές, το drone απινιδωτή, το έξυπνο ασθενοφόρο, την έρευνα του εγκεφάλου, την ιατρική εκπαίδευση, την ανάλυση του γονιδιώματος, τη διαχείριση δεδομένων.

Η παρούσα διπλωματική περιγράφει τα βασικά στοιχεία του blockchain, αναφέρει συσχετιζόμενες εταιρείες και παρέχει μια ολοκληρωμένη ανασκόπηση των αναδυόμενων εφαρμογών υγειονομικής περίθαλψης που βασίζονται σε blockchain. Τέλος, συζητούνται οι προκλήσεις και οι μελλοντικές προοπτικές της τεχνολογίας.

Λέξεις Κλειδιά: *Blockchain, υγειονομική περίθαλψη, διαχείριση δεδομένων, εφοδιαστική αλυσίδα, Διαδίκτυο των πραγμάτων, κλινικές δοκιμές, τηλεϊατρική, γονιδίωμα, ηλεκτρονικά αρχεία υγείας, ιατρική εκπαίδευση, προκλήσεις, προοπτικές.*

Abstract

Now a days , blockchain technology has considerable attention, with an escalating interest in a plethora of numerous applications, ranging Bitcoin creation to financial services. In the last years, due to the rapid growth of this technology, scientists scrutinize new ways to apply blockchain technology with a wide range of domains, included the Health domain.

Blockchain is a shared, distributed, digital ledger technology, which facilitate data management, provenance and security. It is a chain of blocks that covers information and maintains trust between individuals, regardless of location, improving the control of the authenticity and transparency of healthcare data.

The core principle of blockchain is that any service relying on trusted third parties can be built in a transparent, decentralized, secure “trustless” manner. In fact there is trust, but it is hardcoded via a complex cryptographic algorithm. Users have a high degree of control, autonomy, trust and integrity of the data. Also, blockchain allows for reaching a substantial level of historicity of data, without allowing any violation for the whole data flow. Finally, the technology ensures fine-grained control of the data and its security for every stakeholder that participates in the P2P network.

Blockchain solutions are being explored for: maintaining permissions in EHRs, managing pharmaceutical and medical device supply chains, clinical research and data monetization, medical fraud detection and enhance compliance, public health surveillance, powering many IoT-connected autonomous devices, drone defibrillator, smart ambulance, brain research, medical education, genomic analysis, data management.

This diploma thesis describes the basics of blockchain, reports related companies and provides a comprehensive overview of emerging blockchain-based healthcare applications. Finally, the challenges faced and future perspectives are discussed.

Keywords: *Blockchain, healthcare, data management, supply chain, IoT, clinical trials, tele-medicine, genomic, EHRs, medical education, challenges, perspectives.*

ΚΕΦΑΛΑΙΟ 1 : ΕΙΣΑΓΩΓΗ

Η υγειονομική περίθαλψη είναι ένας σύγχρονος κλινικός τομέας, όπου με γοργό ρυθμό παράγεται τεράστιος όγκος δεδομένων, υψίστης σημασίας. Η αποθήκευση και η διάδοση αυτού του μεγάλου όγκου δεδομένων είναι καίριας σημασίας λόγω της ευαίσθητης φύσης των ιατρικών δεδομένων και των περιοριστικών παραγόντων, όπως η ασφάλεια και το απόρρητο. Σύμφωνα με μελέτη που δημοσίευσε το περιοδικό Forbes, το 2015, περισσότερα από 112 εκατομμύρια αρχεία είτε εκλάπησαν, είτε χάθηκαν, είτε χαρακτηρίστηκαν ως ακατάλληλα [1].

Οι αναλυτές των μεγάλων δεδομένων υγειονομικής περίθαλψης, όπως και οι ερευνητές, δουλεύουν σκληρά για την απόκτηση και την ερμηνεία των πολυδιάστατων αυτών δεδομένων, ενώ οι πάροχοι διστάζουν να μοιραστούν τα ευαίσθητα ιατρικά δεδομένα των ασθενών. Συνεπώς, η φροντίδα και η περίθαλψη που σχετίζεται με τον ασθενή, όπως και η σχετική εξόρυξη δεδομένων μεγάλης κλίμακας συνεχίζουν να αποτελούν δύσκολη πρόκληση στον τομέα της Υγείας.

Στον τομέα της υγειονομικής περίθαλψης και των κλινικών ερευνών, η κοινή χρήση των δεδομένων είναι επιτακτική για οποιαδήποτε διάγνωση καθώς και συνδεδεμένη με τη λήψη κλινικών αποφάσεων. Η κοινή χρήση των δεδομένων είναι απολύτως απαραίτητη για να επιτρέπεται στους γιατρούς να μεταφέρουν τα κλινικά δεδομένα των ασθενών τους σε κάθε ενδιαφερόμενη αρχή / οντότητα για γρήγορη παρακολούθηση. Οι φροντιστές και οι γιατροί θα πρέπει να είναι ικανοί να διαχειρίζονται τα κλινικά δεδομένα των ασθενών τους με μεγάλη ευαισθησία, για την προστασία του απορρήτου των ιατρικών δεδομένων και εγκαίρως, προκειμένου να διασφαλιστεί ότι όλες οι ενδιαφερόμενες οντότητες έχουν πλήρη και ενημερωμένα στοιχεία σχετικά με τη κατάσταση υγείας των ασθενών.

Από την άλλη πλευρά, η τηλεϊατρική και η ηλεκτρονική υγεία (EHR), είναι δύο τομείς που χρησιμοποιούνται πολύ, καθώς τα κλινικά δεδομένα μεταφέρονται εξ'αποστάσεως σε κάθε ειδικό εμπειρογνώμονα με σκοπό την ανάλυση και τη γνωμοδότηση. Σε αυτές τις δύο διαδικτυακές κλινικές ρυθμίσεις, τα δεδομένα του ασθενούς μεταφέρονται είτε μέσω τεχνολογίας που αποθηκεύει και προωθεί τα δεδομένα, είτε μέσω των μέσων διαδικτυακής κλινικής παρακολούθησης σε πραγματικό χρόνο. Χρησιμοποιώντας αυτές τις διαδικτυακές κλινικές ρυθμίσεις, οι ασθενείς διαγιγνώσκονται από απόσταση από τους κλινικούς εμπειρογνώμονες από διάφορα μέσα ανταλλαγής κλινικών δεδομένων με σκοπό τη θεραπεία τους. Σε όλες αυτές τις κλινικές ρυθμίσεις, η ασφάλεια, το απόρρητο, η ακεραιότητα των κλινικών δεδομένων είναι μερικές από τις σημαντικές προκλήσεις που πρέπει να απαντηθούν λόγω της περίπτωσης της ευαίσθητης φύσης των δεδομένων των ασθενών. Έτσι, η δυνατότητα ανταλλαγής δεδομένων με ασφάλεια είναι εξαιρετικά σημαντική για την υποστήριξη υγιούς και ουσιαστικής κλινικής επικοινωνίας, σχετικά με περιπτώσεις απομακρυσμένων ασθενών. Η ασφαλής και επιτυχημένη ανταλλαγή δεδομένων βοηθά στην κλινική επικοινωνία, συλλέγοντας επιβεβαιώσεις από μια ομάδα ειδικών, οι οποίες έχουν ως αποτέλεσμα την βελτιωμένη διαγνωστική ακρίβεια και αποτελεσματική θεραπεία.

Επίσης, μια από τις πιο αναπτυσσόμενες βιομηχανίες που αποτελεί έναν κορυφαίο τομέα στην παροχή υγειονομικής περίθαλψης, είναι η φαρμακευτική βιομηχανία. Ο φαρμακευτικός τομέας όχι μόνο βοηθά στην εισαγωγή νέων φαρμάκων στην αγορά, αλλά επίσης βοηθά στη διασφάλιση της ακεραιότητας και της εγκυρότητας των ιατρικών προϊόντων και φαρμάκων που πωλούνται στον τελικό καταναλωτή. Επιπλέον, βοηθά στην αξιολόγηση και επεξεργασία των φαρμάκων, τα οποία βοηθούν στην ταχύτερη ανάρρωση των ασθενών. Οι εταιρείες φαρμάκων αντιμετωπίζουν τις προκλήσεις της έγκαιρης παρακολούθησης των προϊόντων τους, κάτι που μερικές φορές οδηγεί σε σοβαρούς κινδύνους, επιτρέποντας στους παραποιητές φαρμάκων να θέσουν σε κίνδυνο την παραγωγή ή να εισχωρήσουν ψεύτικα φάρμακα στο σύστημα. Κατά συνέπεια, η παραγωγή και διανομή παραποιημένων φαρμάκων έχει καταστεί ένας από τους πιο σημαντικούς κινδύνους της εφοδιαστικής αλυσίδας φαρμάκων για την υγεία σε παγκόσμιο επίπεδο.

Επιπλέον, υπάρχουν διάφορες προκλήσεις διαλειτουργικότητας που αντιμετωπίζονται συνεχώς στον τομέα της Υγείας. Η μη ασφαλής και μη επιτυχημένη ανταλλαγή κλινικών δεδομένων μεταξύ των οργανισμών υγειονομικής περίθαλψης ή ερευνητικών ιδρυμάτων, μπορούν να θέσουν σοβαρές προκλήσεις στην ομαλή λειτουργία. Τέτοιες ανταλλαγές κλινικών δεδομένων απαιτούν ουσιαστική, αξιόπιστη και υγιή συνεργασία μεταξύ των οντοτήτων που εμπλέκονται. Μεταξύ των πιθανών περιορισμών που αντιμετωπίζει αυτή η διαδικασία, είναι η φύση των κλινικών δεδομένων, η ευαισθησία αυτών, οι συμφωνίες ανταλλαγής δεδομένων, οι διαδικασίες, οι σύνθετοι αλγόριθμοι αντιστοίχισης ασθενών καθώς και οι κανόνες και πολιτικές που ακολουθούνται με βάση το ηθικό πλαίσιο. Αυτές είναι μερικές από τις σημαντικές ανησυχίες που πρέπει να συμφωνηθούν αμοιβαία, πριν πραγματοποιηθεί πρακτικά οποιαδήποτε ανταλλαγή κλινικών δεδομένων.

Η τεχνολογία blockchain αποτελεί έναν ισχυρό υποψήφιο για τη διαμόρφωση του τομέα Υγείας παγκοσμίως. Το blockchain χρησιμοποιείται ευρέως για να εξαλείψει την ανάγκη για εμπιστοσύνη μεταξύ των ενδιαφερομένων κατά τη μεταφορά/ ανταλλαγή κλινικών δεδομένων .

Το blockchain έγινε γνωστό, ως η τεχνολογία που τροφοδοτεί το κρυπτονόμισμα Bitcoin , ως ένα τεράστιο, δημόσιο, ανοιχτό, ασφαλές, αποκεντρωμένο, καταναμημένο δημόσιο ημερολόγιο DLT (distributed ledger technology) κατά μήκος ενός δικτύου ομότιμων χρηστών (P2P: peer to peer), που καταγράφει όλες τις συναλλαγές , οικονομικές και μη , με ασφάλη και επαληθεύσιμο τρόπο χωρίς την ανάγκη αξιόπιστης τρίτης οντότητας που θα επεξεργάζεται τις συναλλαγές.

Προσφάτως, υπήρξε αξιοσημείωτο ενδιαφέρον για τη χρήση εφαρμογών blockchain στους παρακάτω κλάδους του τομέα Υγείας : διαχείριση δεδομένων υγείας (data management) , διαχείριση της εφοδιαστικής αλυσίδας φαρμάκων (SCM), ηλεκτρονικά αρχεία υγείας (EHR), απομακρυσμένη παρακολούθηση ασθενών-τηλεϊατρική (remote patient monitoring), φορητές ιατρικές συσκευές (wearable medical devices) , ιατρική εκπαίδευση (medical education), γονιδιωματικά δεδομένα (genomic data generation) , βελτίωση της ποιότητας κλινικών δοκιμών (Clinical research quality), γεωχωρικές εφαρμογές για έξυπνες υγιείς πόλεις (έξυπνο ασθενοφόρο και drone απινιδωτής), Νευροεπιστήμες (Neuroscience), διαχείριση δεδομένων εγγραφής (Enrollment Data Management) , διαχείριση απαιτήσεων τιμολογίων (Claims and Billing Management), διαχείριση ποιότητας (Quality Management) και εντοπισμό απάτης (fraud

detection) και μοντέλων πρόβλεψης για την προστασία της ιδιωτικής ζωής (privacy-preserving predictive models).

Ο λόγος που καθιστά το Blockchain «distributed ledger technology»(DLT) δημοφιλές στις εφαρμογές της Ιατρικής βρίσκεται στις τεράστιες δυνατότητες που πηγάζουν από τα βασικά στοιχεία του , τα οποία θα αντιπαραβάλλουμε στη συνέχεια με τα αντίστοιχα μιας παραδοσιακής βάσης δεδομένων «distributed database management system» (DDBMS).

(DDBMS είναι τα συστήματα SQL-based (π.χ Oracle,) και τα NoSQL-based (π.χ Apache Cassandra).

1) Αποκεντρωμένη Διαχείριση (decentralized management) :

Η αποκέντρωση επιτρέπει την αντίσταση στην αποτυχία του συστήματος, των επιθέσεων, τη χειραγώγηση καθώς και τη συμπαιγνία μεταξύ των συμμετεχόντων. Πώς επιτυγχάνεται αυτό: Η αύξηση του αριθμού των συμμετεχόντων (κόμβοι, υπολογιστές) και ο αριθμός των μοναδικών κατόχων σε ολόκληρο το σύστημα, μειώνει την πιθανότητα συνολικής αποτυχίας ή εξαγοράς του συστήματος. Εάν ένας Η/Υ που αποθηκεύει όλα τα δεδομένα αποτύχει ή καταστραφεί, τότε το σύστημα δεν θα μπορέσει να ανακτήσει τις πληροφορίες αυτές. Η αποκέντρωση εμποδίζει σε μεγάλο βαθμό να συμβεί κάτι τέτοιο [2].

Το DDBMS είναι κεντρικά διαχειριζόμενο (centralized-management).

Η Blockchain DLT είναι ένα σύστημα διαχείρισης αποκεντρωμένης βάσης δεδομένων από ομότιμους χρήστες (peer-to-peer , decentralized database management system). Κάθε κόμβος εργάζεται ανεξάρτητα ακολουθώντας τα συμφωνηθέντα πρωτόκολλα [3]. Το blockchain αποθηκεύει τις πληροφορίες οι οποίες είναι διαφανείς και παραδίδονται στο τρίτο μέρος βάση συγκατάθεσης του δημιουργού. Είναι ένας αποκεντρωμένος τρόπος αποθήκευσης πληροφοριών, διατηρώντας πολλαπλά αντίγραφα αυτών των πληροφοριών σε πολλά σημεία.

Συμπέρασμα: Το Blockchain είναι κατάλληλο για εφαρμογές βιοϊατρικής/υγειονομικής περίθαλψης όπου οι ανεξάρτητοι ενδιαφερόμενοι (stakeholders) επιθυμούν να συνεργάζονται μεταξύ τους χωρίς να μεταβιβάζουν τον έλεγχο σε έναν κεντρικό διαμεσολαβητή διαχείρισης (νοσοκομείο, ασθενείς, γιατροί, ασφαλιστικές) [4].

2) Αμετάβλητη διαδρομή ελέγχου (immutable audit trail):

Η μη μεταβλητότητα δηλώνει ότι ορισμένα αρχεία (συναλλαγές) δεν μπορούν να αλλοιωθούν ή να τροποποιηθούν παρά μόνο να προσαρτηθούν σε άλλα αρχεία. Βέβαια, τα blockchains δεν πετυχαίνουν πάντοτε τέλεια μη μεταβλητότητα. Μόνο με τη σωστή υλοποίηση και αποκέντρωση εξασφαλίζεται ότι καμιά οντότητα δεν κατέχει ή δεν ελέγχει την πλειονότητα των κόμβων στο δίκτυο blockchain.

Το DDBMS υποστηρίζει λειτουργίες όπως δημιουργία(create), ανάγνωση(read), ενημέρωση(update), διαγραφή(delete) όπως συμβαίνει σε όλα τα συστήματα Β.Δ.

Η Blockchain DLT υποστηρίζει μόνο τις λειτουργίες δημιουργία(create), ανάγνωση(read).Είναι σχεδόν ακατόρθωτο να αλλάξεις ή να τροποποιήσεις τα δεδομένα ή τα αρχεία [5].

Συμπέρασμα: Το Blockchain είναι κατάλληλο για την καταγραφή κρίσιμων πληροφοριών υγείας (π.χ. αρχεία ασφαλιστικών εταιρειών) καθώς είναι ένα ημερολόγιο που δεν αλλάζει(unchangeable ledger) .

3) Προέλευση δεδομένων (data provenance):

Στο DDBMS ο διαχειριστής της Β.Δ. μπορεί να τροποποιήσει την ιδιοκτησία των ψηφιακών αγαθών(digital assets).

Στη Blockchain DLT η ιδιοκτησία των ψηφιακών αγαθών(digital assets) μπορεί μόνο να αλλάξει από τον ίδιο τον ιδιοκτήτη(owner) ακολουθώντας τα κρυπτογραφικά πρωτόκολλα [5]. Επίσης, η προέλευση των αγαθών είναι ανιχνεύσιμη , αυξάνοντας την επαναχρησιμοποίηση των επιβεβαιωμένων δεδομένων(για ασφαλιστικές συναλλαγές) [6].

Συμπέρασμα: Το Blockchain είναι κατάλληλο για τη διαχείριση κρίσιμων ψηφιακών στοιχείων (π.χ. αρχεία συγκατάθεσης ασθενούς).

4) Ευρωστία και Διαθεσιμότητα (robustness and availability):

Το DDBMS βασίζεται στην κατακευματισμένη τεχνολογία (distributed) και δεν υποφέρει από το πρόβλημα του *Single-point-of-failure* αλλά είναι δαπανηρό να επιτευχθεί το υψηλό επίπεδο πλεονασμού δεδομένων (data redundancy).

Η Blockchain DLT βασίζεται και αυτή στην κατακευματισμένη τεχνολογία (distributed) και δεν υποφέρει από το πρόβλημα του *Single-point-of-failure* αλλά δεν είναι δαπανηρό να επιτευχθεί το υψηλό επίπεδο πλεονασμού δεδομένων (data redundancy), καθώς κάθε κόμβος έχει ένα ολόκληρο αντίγραφο από ολόκληρο το ιστορικό αρχείο δεδομένων [7].

Συμπέρασμα: Το Blockchain είναι κατάλληλο όταν η διατήρηση και η διαρκής διαθεσιμότητα των αρχείων είναι σημαντική (π.χ. τα EHRs των ασθενών).

5) Κρυπτογραφία (cryptography):

Η Κρυπτογραφία σχετίζεται με όλες τις μαθηματικές τεχνικές που στοχεύουν στην ικανοποίηση των βασικών απαιτήσεων ασφαλείας : Εμπιστευτικότητα (μη αποκάλυψη πληροφορίας σε μη εξουσιοδοτημένες οντότητες), Ακεραιότητα (μη εξουσιοδοτημένη τροποποίηση πληροφορίας), Διαθεσιμότητα (διαθέσιμη πληροφορία ανά πάσα στιγμή μόνο σε εξουσιοδοτημένες οντότητες), Αυθεντικοποίηση (ο τρόπος με τον οποίο θα πιστοποιηθεί η ταυτότητα του αποστολέα).

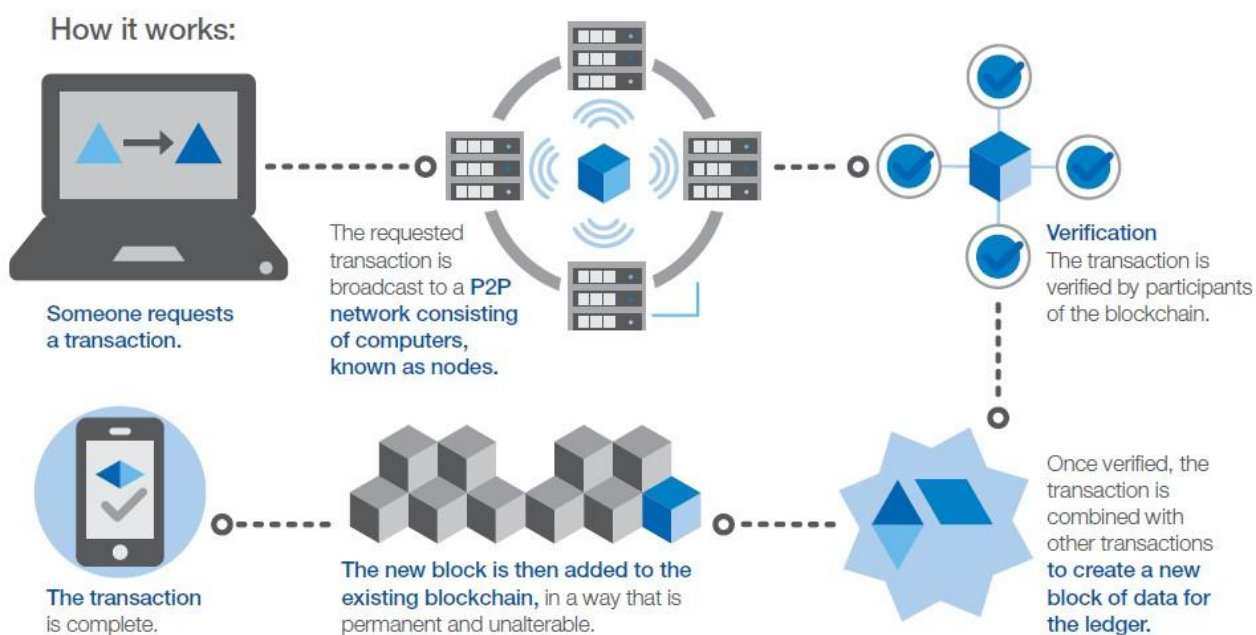
Το DDBMS δεν χρησιμοποιεί κρυπτογραφικούς αλγορίθμους.

Το blockchain χρησιμοποιεί κρυπτογραφικούς αλγορίθμους για να εξασφαλίσει την ιδιοκτησία των ψηφιακών αγαθών, τους *SHA-256* και *ECDSA-256*.

Η *SHA-256* χρησιμοποιείται για τη δημιουργία διεύθυνσης χρήστη (user address) για βελτίωση της ιδιωτικότητας (privacy) και της ανωνυμίας (anonymity). Κάθε χρήστης αντιπροσωπεύεται από μια τιμή κατακερματισμού (hash value) αντί μιας πραγματικής ταυτότητας (real identity), όπως είναι η IP διεύθυνση [8].

ECDSA-256: Η *ECDSA-256* χρησιμοποιείται για τη δημιουργία και την επιβεβαίωση των δημόσιων/ιδιωτικών κλειδιών μιας ψηφιακής υπογραφής [9].

Κάθε συμμετέχων που είναι μέρος αυτού του δικτύου, πρέπει να επαληθεύει καθεμία νέα συναλλαγή που πραγματοποιείται. Καθώς καθεμία συναλλαγή σε ένα block ενός blockchain επαληθεύεται από όλους τους κόμβους του δικτύου, γίνεται όλο και περισσότερο αμετάβλητο. Το παρακάτω διάγραμμα δείχνει τη ροή εργασίας της διαδικασίας blockchain.



Εικόνα 1.1 : Ροή εργασίας της διαδικασίας blockchain [10]

Κάποια οντότητα ζητάει να κάνει μια συναλλαγή. Η ζητούμενη συναλλαγή μεταδίδεται σε ένα P2P δίκτυο, το οποίο αποτελείται από υπολογιστές, γνωστοί ως κόμβοι. Η συναλλαγή επαληθεύεται από τους συμμετέχοντες στο blockchain. Αφού επαληθευτεί η συναλλαγή, συνδυάζεται με άλλες συναλλαγές, με σκοπό να δημιουργηθεί ένα νέο block δεδομένων για το ledger. Το νέο block προστίθεται στο υπάρχων blockchain, με τρόπο που είναι μόνιμος και αναλλοίωτος. Η συναλλαγή έχει ολοκληρωθεί.

Στο μέλλον, το blockchain θα μπορούσε να είναι μια τεχνολογία που θα βοηθήσει στην αξιόπιστη, εξατομικευμένη και ασφαλή υγειονομική περίθαλψη. Συγχωνεύοντας ολόκληρα τα κλινικά δεδομένα σε πραγματικό χρόνο για κάθε ασθενή, ενημερώνει με ασφάλεια καθεμία εγκατάσταση υγειονομικής περίθαλψης.

Στην παρούσα διπλωματική παρουσιάζεται η υπάρχουσα πρόοδος του μοντέλου blockchain καθώς και οι τελευταίες εξελίξεις στον τομέα της Υγείας , μέσω των διαφόρων εργασιών που έχουν επιτελεστεί.

Οργάνωση κειμένου:

Το κείμενο της διπλωματικής αποτελείται από 5 Κεφάλαια.

Το Κεφάλαιο 1 αποτελεί την εισαγωγή.

Στο Κεφάλαιο 2 παρουσιάζεται το θεωρητικό υπόβαθρο της τεχνολογίας καθώς επίσης και οι συσχετιζόμενες εργασίες και εταιρείες που αφορούν στην τεχνολογία blockchain στον τομέα της υγειονομικής περίθαλψης.

Στο Κεφάλαιο 3 παρουσιάζονται και αναλύονται λεπτομερώς οι εφαρμογές της τεχνολογίας στον τομέα της υγειονομικής περίθαλψης.

Στο Κεφάλαιο 4 γίνεται αναφορά στις προκλήσεις που αντιμετωπίζονται.

Το Κεφάλαιο 5 αποτελεί τον επίλογο του κειμένου. Σε αυτό συνοψίζονται οι μελλοντικές προοπτικές καθώς επίσης οι επιπτώσεις και τα συμπεράσματα.

ΚΕΦΑΛΑΙΟ 2

ΘΕΩΡΗΤΙΚΟ ΥΠΟΒΑΘΡΟ- ΣΥΣΧΕΤΙΖΟΜΕΝΕΣ ΕΤΑΙΡΙΕΣ ΚΑΙ ΕΡΓΑΣΙΕΣ

Στο κεφάλαιο αυτό διατυπώνεται το θεωρητικό υπόβαθρο σχετικά με την τεχνολογία του blockchain. Αρχικά παρουσιάζεται το Bitcoin , ως η πρώτη εφαρμογή του blockchain. Στη συνέχεια παρουσιάζονται οι προκλήσεις που αντιμετώπισαν τα κρυπτονομίσματα, καθώς και η λύση που προτάθηκε. Έπειτα γίνεται μια περιγραφή του μηχανισμού της τεχνολογίας blockchain, του PoW πρωτοκόλλου και των κακόβουλων αλυσίδων. Στη συνέχεια γίνεται μια σύντομη ανάλυση ενός απλοποιημένου blockchain και της ανατομίας του block, το οποίο αποτελεί το θεμέλιο λίθο της λειτουργίας του blockchain. Έπειτα γίνεται μια σύντομη παρουσίαση της εξέλιξης της τεχνολογίας blockchain, ανάλογα με τις ανάγκες που παρουσιάστηκαν καθώς και η τάση που αυτή τη στιγμή υπάρχει. Στη συνέχεια, παραθέτονται οι τρεις τύποι blockchain, οι οποίοι χρησιμοποιούνται με βάση την άδεια χρήσης και το πεδίο εφαρμογής , στον τομέα της Υγείας. Τέλος γίνεται αναφορά στις συσχετιζόμενες εταιρίες και σχετικές εργασίες που έχουν προταθεί.

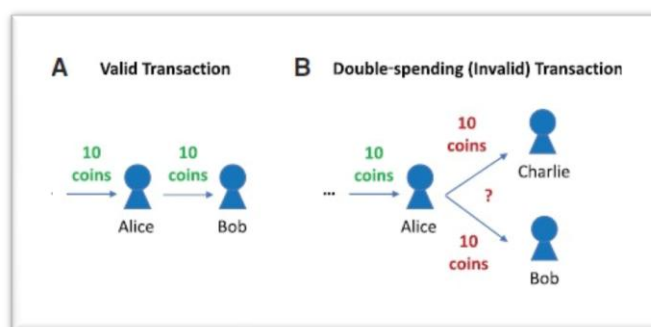
2.1) Bitcoin :

Μια από τις πιο γνωστές εφαρμογές του blockchain είναι το Bitcoin κρυπτονόμισμα. Το Bitcoin εφευρέθηκε από τον Satoshi Nakamoto τον Οκτώβριο του 2008. Ένα χρόνο αργότερα κυκλοφόρησε η εφαρμογή Bitcoin ανοιχτού κώδικα. Πρόκειται για ένα αποκεντρωμένο ψηφιακό νόμισμα από ομότιμους χρήστες χωρίς κεντρικό διαχειριστή, έτσι κατηγοριοποιείται από το Αμερικάνικο Ταμείο. Το Bitcoin έχει το ανεπίσημο ISO-4217 currency code XBT, το οποίο χρησιμοποιείται από οργανισμούς και εταιρείες όπως η Bloomberg . Η μονάδα Bitcoin είναι BTC και 1BTC ήταν ισοδύναμο περίπου με 1200 δολάρια Αμερικής τον Απρίλιο του 2017. Μέχρι σήμερα , το Bitcoin έχει την υψηλότερη συνολική αγοραία αξία μεταξύ περισσότερων από 100 διαφορετικών κρυπτονομισμάτων που χρησιμοποιούνται σήμερα. Επίσης, τα bitcoins μπορούν να χρησιμοποιηθούν σε ιστότοπους ηλεκτρονικού εμπορίου για να αγοράσουν ένα ευρύ φάσμα προϊόντων και υπηρεσιών [11].

2.2) Κρυπτονομίσματα: Προκλήσεις και Λύσεις

2.2.1) Peer-to-peer double spending problem:

Το αρχικό κίνητρο της Bitcoin-blockchain τεχνολογίας ήταν η επίλυση του «προβλήματος διπλής δαπάνης από ομότιμους χρήστες». Η ερώτηση είναι: πώς μπορούμε να εμποδίσουμε τα ηλεκτρονικά νομίσματα, όπως τα Bitcoins, να ξοδεύονται δύο φορές χωρίς κεντρικό ενδιαμέσο;



Εικόνα 2.1 : Το πρόβλημα της διπλής δαπάνης χωρίς κεντρικό διαμεσολαβητή [12]

Ας υποθέσουμε ότι η Alice έχει 10 νομίσματα και τα στέλνει όλα στον Bob. Πώς μπορεί ο Bob (και οι άλλοι χρήστες που χρησιμοποιούν νομίσματα) να γνωρίζει εάν η Alice δεν έχει στείλει από πριν αυτά τα ίδια 10 νομίσματα στον Charlie, χωρίς να υπάρχει μια τράπεζα για να επαληθεύσει τις συναλλαγές;

2.2.2) Single-point-of-failure:

Centralized Network (Εικόνα 2.2A)

Ο κεντρικός διαμεσολαβητής (πχ Τράπεζα) δεν είναι επιθυμητός, διότι δημιουργεί «μοναδικό σημείο αποτυχίας». Αυτό συμβαίνει διότι αν ο κεντρικός διαμεσολαβητής είναι εκτός λειτουργίας για κάποιο λόγο (πχ προσχεδιασμένη συντήρηση), ολόκληρο το σύστημα δικτύου σταματά. Επίσης, αν παραβιαστεί ο λογαριασμός του κεντρικού διαμεσολαβητή τότε ολόκληρο το δίκτυο αντιμετωπίζει τον κίνδυνο εισβολής [13].

Decentralized Network (Εικόνα 2.2B)

Σε αυτή την περίπτωση δεν υπάρχει «μοναδικό σημείο αποτυχίας». Εάν κάποιος από τους κόμβους δεχθεί επίθεση, το υπόλοιπο δίκτυο θα μπορεί να λειτουργεί κανονικά.

2.2.3) The Bitcoin blockchain solution:

Για την επίλυση των προβλημάτων που αναφέρθηκαν πιο πάνω θα χρειαστούν δύο εργαλεία επίλυσης: hash-chain time stamping και PoW algorithm.

Κάθε κόμβος υπολογισμού στο blockchain δίκτυο, χρειάζεται να αποθηκεύσει κάθε συναλλαγή για να επιτραπεί η κατανεμημένη επαλήθευση των συναλλαγών και να ακολουθήσει

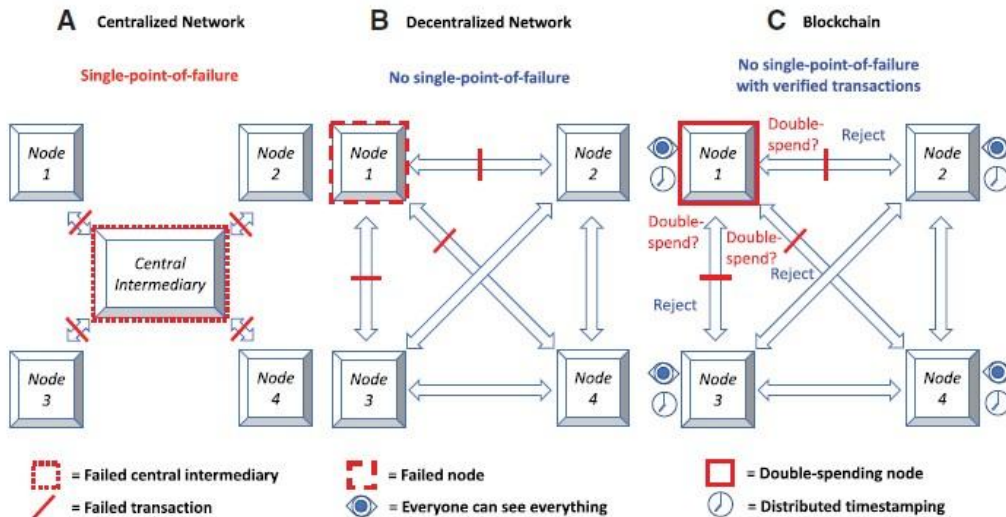
επίσης ένα κατακεντρωμένο μηχανισμό χρονικής σήμανσης για να καθοριστεί ποια συναλλαγή πρέπει να γίνει αποδεκτή και ποια πρέπει να απορριφθεί.

Blockchain (Εικόνα 2.2C)

«Εάν οι πάντες μπορούν να δουν τα πάντα» και υπάρχει ένας κατακεντρωμένος μηχανισμός με χρονική σήμανση, τότε το «πρόβλημα διπλής δαπάνης από τους ομότιμους χρήστες», μπορεί να λυθεί σε ένα αποκεντρωμένο (decentralized) δίκτυο.

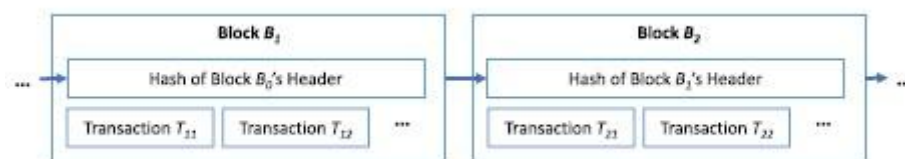
Στην Εικόνα 2.1, εάν ο καθένας (Alice, Bob, Charlie και όλοι οι άλλοι συμμετέχοντες του δικτύου αυτού) γνωρίζει πως η Alice (node1) έστειλε χθες 10 νομίσματα στον Charlie, τότε η συναλλαγή αποστολής των ίδιων 10 νομισμάτων στον Bob σήμερα, μπορεί να απορριφθεί μέσω μιας διαδικασίας επαλήθευσης (verification process) χωρίς την ανάμειξη μιας τράπεζας.

Το blockchain εκμεταλλεύεται την αλυσίδα κατακερματισμού (hash chain) ως μηχανισμό κατακεντρωμένου χρονικού σήματος (distributed timestamp mechanism) και κάθε κόμβος διατηρεί αντίγραφο της αλυσίδας για την αποθήκευση κάθε συναλλαγής [14].



Εικόνα 2.2: Σύγκριση των τοπολογιών κατακεντρωμένων δικτύων [12]

2.3) Μηχανισμός blockchain :



Εικόνα 2.3: Παράδειγμα απλοποιημένου blockchain (hash-chain) [15].

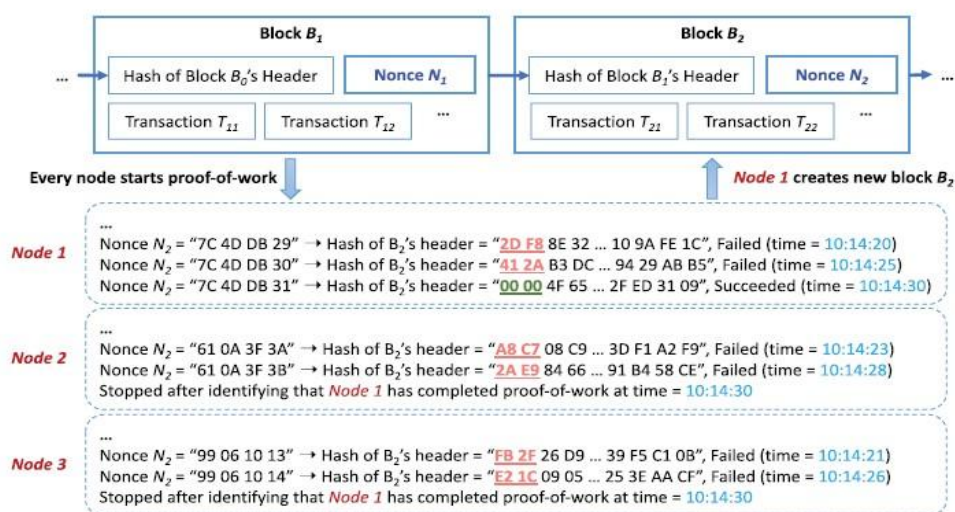
Κάθε συναλλαγή περικλείεται σε ένα block. Το block είναι μια βασική μονάδα η οποία περιέχει πολλαπλές συναλλαγές και πρέπει να επαληθεύεται. Κάθε block περιέχει επίσης μια τιμή κατακερματισμού της κεφαλίδας του προηγούμενου block (hash value of the previous block’s header) και έτσι σχηματίζεται μια αλυσίδα κατακερματισμού (hash-chain) ή blockchain. Καθώς όλα τα block είναι αλυσοδεμένα, η σειρά των blocks είναι καθοριστική, επομένως, κάθε block μπορεί να χρησιμεύσει ως χρονική σφραγίδα (timestamp) των κλειστών συναλλαγών για την επίλυση του double-spending προβλήματος. Κάθε κόμβος διατηρεί ένα αντίγραφο ολόκληρου του blockchain, έτσι κάθε κόμβος μπορεί να επιβεβαιώσει κάθε συναλλαγή.

Ας υποθέσουμε ότι η συναλλαγή από την Alice στον Charlie περικλείεται στο block B1 και η συναλλαγή από την Alice στον Bob περικλείεται στο block B2. Όπως φαίνεται και στην εικόνα, όλοι στο δίκτυο μπορούν να επιβεβαιώσουν ότι το B1 συνέβη πριν το B2 ελέγχοντας το hashed blockchain και έτσι η συναλλαγή διπλής δαπάνης από την Alice πρέπει να απορριφθεί.

Επιπροσθέτως, η διαδικασία εξόρυξης (mining process) είναι αρκετά δύσκολο να πραγματοποιηθεί, αλλά σχετικά εύκολο να ελεγχθεί [16]. Η διαδικασία θα πρέπει να είναι δύσκολη, δαπανηρή και χρονοβόρα προκειμένου να αποτρέπεται οποιαδήποτε προσπάθεια δημιουργίας μη έγκυρων blocks από επιτήδειους. Το blockchain για να μπορέσει να κάνει πράξη αυτό το σχέδιο, υιοθετεί ένα PoW πρωτόκολλο, το οποίο θα πρέπει να ακολουθήσει κάθε δημιουργός block.

2.3.1) PoW Πρωτόκολλο

Ένα από τα πλεονεκτήματα του PoW πρωτοκόλλου που χρησιμοποιείται ομόφωνα στο blockchain, είναι η ικανότητα επίλυσης της διαφωνίας των αλυσίδων αφήνοντας τα blockchains να είναι αμετάβλητα μονοπάτια ελέγχου (immutable audit trails) [16]. Τι σημαίνει αυτό: όταν ένας επιτιθέμενος τροποποιήσει ένα block, όλα τα blocks μετά από αυτό το block αναπροσαρμόζονται, διότι κάθε block περιέχει την τιμή κατακερματισμού της κεφαλίδας του προηγούμενου block (hash-value of the previous block’s header) και το υπολογιστικό κόστος μιας τέτοιας τροποποίησης θα πρέπει να είναι αρκετά υψηλό ώστε να απαγορεύει τις επιθέσεις. Στην Εικόνα 2.4, θα εξετάσουμε πώς δημιουργείται μια αλυσίδα blocks με το PoW πρωτόκολλο [17].



Εικόνα 2.4: Παράδειγμα του μηχανισμού nonce για το PoW πρωτόκολλο [17].

Κάθε block περιέχει ένα πρόσθετο “nonce” (32 bits ή 8 δεκαεξαδικά ψηφία) , το οποίο είναι ένας μετρητής που χρησιμεύει ως μια από τις εισόδους (inputs) της συνάρτησης κατακερματισμού (hash-function). Για να “αποδείξει” το έργο κατακερματισμού (“proof”), το nonce αυξάνεται κατά 1bit κάθε φορά για τον υπολογισμό κατακερματισμού (“the work”) , έως ότου η τιμή του hash (256 bits ή 64 δεκαεξαδικά ψηφία) να περιέχει έναν προκαθορισμένο αριθμό μηδενικών bits (zero bits). Σε αυτό το παράδειγμα, 16 bits ή 4 δεκαεξαδικά ψηφία για “proof-of-work”. Οι μη επιβεβαιωμένες συναλλαγές που δημιουργήθηκαν πρόσφατα, συλλέγονται σε μια μνήμη (memory pool) σε κάθε κόμβο (node).

Ο πρώτος κόμβος που επιτυχώς ολοκλήρωσε το “proof-of-work” (Node 1 στις 10:14:30) , έχει τα παρακάτω προνόμια: 1) να δημιουργήσει ένα νέο block (Block B2), 2) να επαληθεύσει τις συναλλαγές, 3) να μετακινήσει τις επιβεβαιωμένες συναλλαγές από τη μνήμη σε ένα νεο-δημιουργημένο block, 4) να προσθέσει το block στο τέλος της μεγαλύτερης αλυσίδας (εάν υπάρχουν ανταγωνιστικές αλυσίδες), 5) να πληρωθεί για αυτή τη δουλειά(π.χ. 12,5 bitcoins).

Οι υπόλοιποι κόμβοι (Node 2, Node 3) σταματούν την P-o-W εξόρυξη για το B2 όταν το Node1 ολοκληρώνει το P-o-W.

Με αυτό τον τρόπο η διαδικασία εξόρυξης (mining process) γίνεται δύσκολη (πρέπει κανείς να υπολογίσει το δύσκολο πρόβλημα κατακερματισμού δοκιμάζοντας διαφορετικές “nonce” τιμές). Από την άλλη, η διαδικασία ελέγχου (checking process) παραμένει εύκολη (αρκεί μόνο ένα hash για να δούμε εάν τα προκαθορισμένα leading bits είναι όλα zeros).

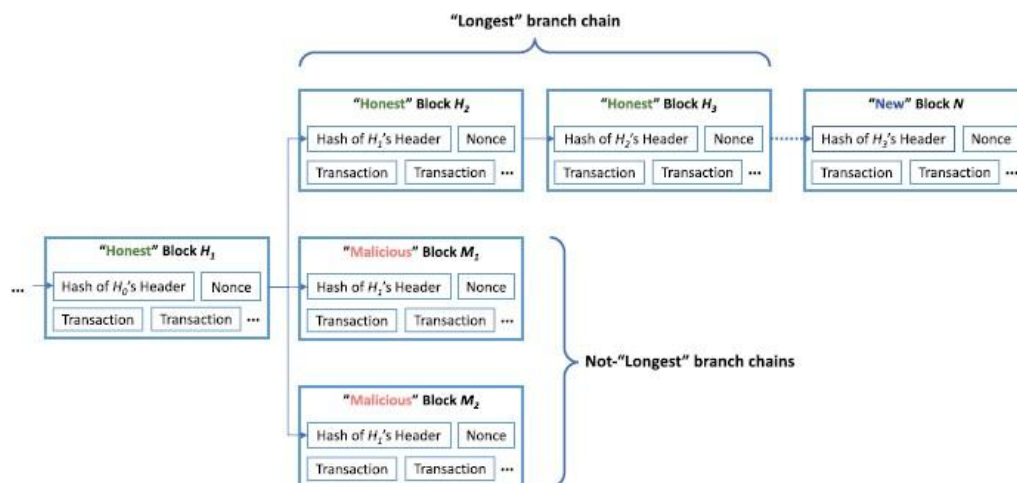
Στο παράδειγμά μας, η Alice δεν μπορεί εύκολα να δημιουργήσει ένα μη έγκυρο block για τη συναλλαγή διπλής δαπάνης (double spending transaction) , ενώ ο Bob και ο Charlie μπορούν εύκολα να ελέγξουν εάν το block της Alice είναι μη έγκυρο.

2.3.2) Κακόβουλες αλυσίδες :

Αξίζει να επισημάνουμε την περίπτωση ενός επιτιθέμενου στο blockchain. Εάν ένας επιτιθέμενος τροποποιήσει οποιαδήποτε από τις συναλλαγές στο block B1, την τιμή της “hash of block B1’s header” , επόμενο είναι να πρέπει να υπολογιστεί εκ νέου το block B2 και κατά συνέπεια όλα τα blocks μετά (B2, B3, B4, B5,...) θα πρέπει να αναπροσαρμοστούν. Επομένως το κόστος υπολογισμού της επίθεσης γίνεται απαγορευτικά υψηλό, όπως αναφέρθηκε και πιο πάνω.

Τι θα συμβεί όμως εάν ένας επίμονος επιτιθέμενος δημιουργήσει μια κακόβουλη αλυσίδα (malicious chain) για να ανταγωνιστεί μια έντιμη αλυσίδα (honest chain) αντικαθιστώντας την με αυτή; Ο πλειοψηφικός μηχανισμός ψηφοφορίας PoW μπορεί να μειώσει σημαντικά την πιθανότητα της επιτυχίας μιας τέτοιας επίθεσης. Το πρωτόκολλο συναίνεσης PoW του blockchain έχει ικανότητες για να αντισταθεί στις επιθέσεις, εικόνα 2.5 [18].

Ο μηχανισμός παρέχει ανταμοιβή στους κόμβους , ως κίνητρο για την αντιστάθμιση του υψηλού κόστους που συνδέεται με την εξόρυξη ενός νέου block και την επιβεβαίωση συναλλαγών. Στην Εικόνα 2.5 θα εξετάσουμε πώς αντιστέκεται το blockchain στη δημιουργία κακόβουλων αλυσίδων .



Εικόνα 2.5: Παράδειγμα του πώς το blockchain διαχειρίζεται τις αλυσίδες διακλάδωσης [12]

Σε αυτό το σενάριο οι επιτιθέμενοι δημιουργούν κακόβουλα blocks M₁, M₂ για να ανταγωνιστούν με ένα έντιμο block H₂, σε μια προσπάθεια ανάληψης της έντιμης αλυσίδας (H₁ και όλα τα προηγούμενα blocks). Υποθέτοντας ότι η υπολογιστική ισχύς των έντιμων κόμβων είναι μεγαλύτερη από αυτή των κακόβουλων κόμβων, ένα έντιμο block H₃ δημιουργείται αμέσως μετά το H₂, πριν οι επιτιθέμενοι δημιουργήσουν νέα κακόβουλα blocks μετά τα M₁ και M₂.

Με βάση τον μηχανισμό blockchain, κάθε κόμβος προσδιορίζει πρώτα ένα έγκυρο block με βάση το μήκος της αλυσίδας και δημιουργεί ένα νέο block N, μόνο στο τέλος της μακρύτερης αλυσίδας (longest chain H₁→H₂→H₃) ενώ αγνοεί τις κοντύτερες αλυσίδες (shorter chains H₁→M₁ και H₁→M₂). Με λόγια απλά, το blockchain που έχει εργαστεί περισσότερο, κερδίζει το διαγωνισμό (η πλειοψηφία των ψήφων, μια CPU μια ψήφος, η longest chain αντιπροσωπεύει την απόφαση της πλειοψηφίας των δημιουργών block).

Δεδομένου ότι η διαδικασία εξόρυξης είναι ακριβή και οι έντιμοι κόμβοι έχουν υψηλότερη υπολογιστική δύναμη (έχουν περισσότερους CPU voters) από τους κακόβουλους κόμβους, η πιθανότητα να τροποποιηθεί επιτυχώς ένα block από τους επιτιθέμενους και όλα τα blocks μετά από αυτό, είναι πολύ μικρή.

2.4) Απλοποιημένο blockchain:

Το blockchain είναι ένα τεράστιο αποθετήριο δεδομένων από αρχεία και γεγονότα/συναλλαγές όπου η κάθε αποθήκη του ονομάζεται **block**.

Κάθε block περιέχει μια χρονική σφραγίδα (timestamp) και συνδέεται με ένα προηγούμενο block.

Τα γεγονότα μπορούν να ενημερωθούν μόνο από την πλειοψηφία των χρηστών.

Οι πληροφορίες δεν μπορούν να διαγραφούν.

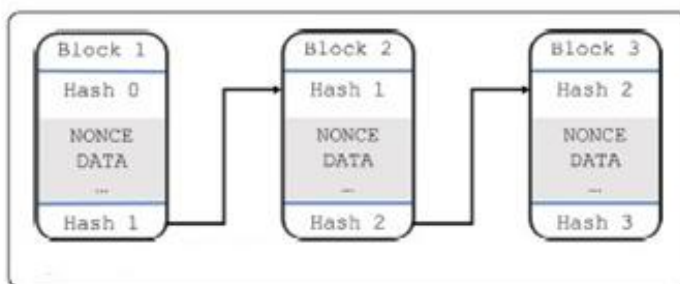
Το αποθετήριο δεν ανήκει σε κανέναν, ελέγχεται από τους χρήστες και δεν διοικείται από κανένα κεντρικό ρυθμιστικό όργανο ή αξιόπιστη τρίτη οντότητα [19].

Στην πραγματικότητα, η εμπιστοσύνη κωδικοποιείται στο εκάστοτε πρωτόκολλο και διατηρείται από την κοινότητα των χρηστών.

Το block λοιπόν μπορούμε να το φανταστούμε ως ένα δοχείο-αποθήκη μέσα στο οποίο αποθηκεύονται όλα τα είδη δεδομένων που διαδίδονται στους διάφορους κόμβους.

Στο PoW πρωτόκολλο, τα τέλη συναλλαγών (transaction fees) καταβάλλονται στους miners, για να διατηρήσουν αυτούς τους κόμβους ανοιχτούς, οι οποίοι με τη σειρά τους διατηρούν το blockchain ασφαλές.

Κάθε block είναι αριθμημένο και διαθέτει τις τιμές “hash value” και “nonce value” [20].



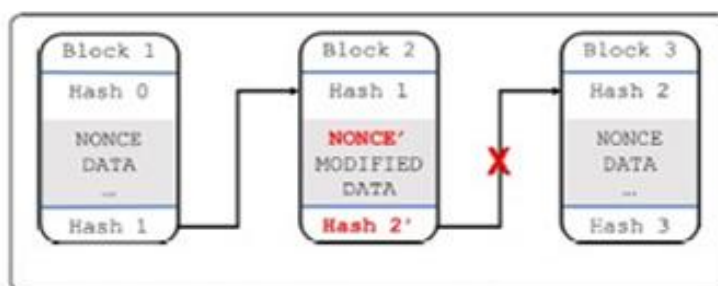
Εικόνα 2.6 : Απλοποιημένο blockchain τριών blocks, [20].

Hash value: Η τιμή αυτή συνδέει κάθε block με το επόμενο και θεωρείται ως ένα στρώμα προστασίας που οδηγεί στην μη μεταβλητότητα.

Nonce value: Είναι μια τυχαία μεταβλητή τιμή, που εξασφαλίζει ότι επιτυγχάνεται η σωστή κατακερμάτιση σε ένα POW σύστημα. Αυτή είναι η τιμή που προσπαθούν να βρουν οι miners [20] και χρησιμοποιείται μια φορά για να εξασφαλιστεί ότι η σωστή hash value έχει οριστεί κατά την εξόρυξη (mining) στο blockchain.

Η τιμή αυτή εξορύσσεται για να ικανοποιήσει την PoW συναίνεση .

Δεδομένου ότι κάθε block είναι συνδεδεμένο με το επόμενο βάσει της hash value που διαθέτει, γνωρίζουμε ότι οποιαδήποτε αλλαγή συμβεί στα δεδομένα θα προκαλέσει δραματική αλλαγή στην hash value . Στο blockchain κάθε block που θα ακολουθεί μετά το πειραγμένο block, δεν θα είναι έγκυρο [21].



Εικόνα 2.7 : Απλοποιημένο blockchain με πειραγμένο block [20]

Για να αλλάξουμε λοιπόν ένα block και να βάλουμε τη σωστή value για να το επικυρώσουμε , θα πρέπει όλα τα blocks που θα ακολουθήσουν να επαναπροσδιοριστούν και αυτά. Πρόκειται για ένα πολύ δύσκολο εγχείρημα που θα κοστίζει ακριβιά για να πετύχει ακόμα και σε πολύ ισχυρά δίκτυα [22].

Η hash value ήταν το πρώτο επίπεδο προστασίας που οδηγεί στην μη μεταβλητότητα.

Ας υποθέσουμε ότι μέχρι στιγμής το πρώτο επίπεδο προστασίας ξεπεράστηκε και ο επιτιθέμενος κατάφερε μια επιτυχή επίθεση.

Το επόμενο επίπεδο προστασίας που οδηγεί στην μη μεταβλητότητα είναι η κατανομή (distribution) και η αποκέντρωση (decentralization).

Όχι μόνο πρέπει να αναφερθεί ολόκληρο το blockchain μετά το πειραγμένο block, αλλά τουλάχιστον το 51% όλων των κατανεμημένων αντιγράφων (distributed) θα πρέπει επίσης να τροποποιηθεί και στη συνέχεια να επανέλθει για να εφαρμοστεί η αλλαγή [20].

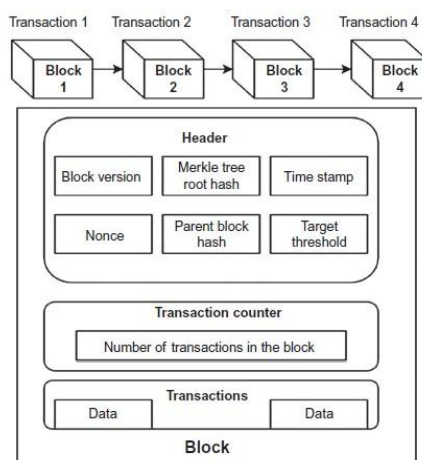
Αυτή η ενέργεια αυξάνει το κόστος της επίθεσης ακόμη περισσότερο και μας δείχνει γιατί εάν εφαρμοστεί και διατηρηθεί σωστά , τότε η μη μεταβλητότητα είναι πολύ αξιόπιστη.

2.5) Ανατομία του Block :

Πρακτικά , η αρχιτεκτονική του blockchain επιτρέπει την αποθήκευση της ύπαρξης των δεδομένων. « The only proof of data, is the data of proof »

Block:

Είναι ένα μόνιμο και αμετάβλητο αρχείο που παρομοιάζει με αποθήκη για πληροφορίες συναλλαγής. Παρομοιάζοντας με ένα ledger, ένα block δείχνει την τρέχουσα συναλλαγή ή την απόφαση που θα δηλώνει τελικά ένα νέο block, μόλις γίνει μια νέα συναλλαγή. Τα κύρια μέρη ενός block είναι: 1) Header (κεφαλίδα), 2) Transaction counter (μετρητής συναλλαγών) , 3) Transaction data (δεδομένα συναλλαγής).



Εικόνα 2.8: Ανατομία του block [23].

- 1) **Header (κεφαλίδα):** Οι κεφαλίδες του περιεχομένου του blockchain ακολουθούν μια λίστα πληροφοριών σε ξεχωριστά υποτιμήματα:
 - Block version: αντιπροσωπεύει τον τρέχοντα block version number, ο οποίος αποφασίζει τους κανονισμούς που θα ακολουθήσει αυτό το block.
 - Parent block hash: αποθηκεύει το προηγούμενο block hash, το οποίο δείχνει το προηγούμενο block.
 - Merkle tree root hash: είναι μια διαδικασία διατήρησης των πληροφοριών blockchain, μετά από ένα double SHA-256 hashing.
 - Time stamp: καταγράφει την ώρα έγκρισης αυτού του συγκεκριμένου block.
 - Target threshold: εκφράζει το στόχο για το επιθυμητό όριο εξόρυξης (mining) ή τη δυσκολία για τη δημιουργία block.
 - Nonce: Είναι η τιμή που χρησιμοποιείται μόνο μια φορά. Η είσοδος του nonce αλλάζει το hash output των περιεχομένων του block.

- 2) **Transactions counter (μετρητής συναλλαγών):** Μετράει τον αριθμό των επιτυχώς ολοκληρωμένων συναλλαγών. Επίσης εκφράζει τον αύξοντα αριθμό του block που χρησιμοποιείται, (serial number of block).

- 3) **Transaction data (δεδομένα συναλλαγής):** Ανάλογα με τη χρησιμότητα, ο σκοπός αυτού του πεδίου ποικίλλει. Μπορεί να χρησιμοποιηθεί για συναλλαγές Bitcoin, πληροφορίες υγειονομικής περίθαλψης, δεδομένα επιχειρήσεων, αρχεία συμβολαίων κτλ. Στην περίπτωση της υγειονομικής περίθαλψης, αποθηκεύει κλινικές/ιατρικές πληροφορίες που σχετίζονται με τους ασθενείς.

2.6) Εναλλακτικά blockchains:

Blockchain 1.0:

Θεωρούνται τα διάφορα εναλλακτικά blockchains που έχουν προταθεί ανά καιρούς . Κάποια από αυτά είναι : Altchains, Colored Coins, Sidechains.

Blockchain 2.0:

Αρχικά το blockchain σχεδιάστηκε ως κρυπτονομίσμα αλλά στη συνέχεια θεωρήθηκε ως μια νέα μορφή κατανεμημένης βάσης δεδομένων (distributed database) ή ως ένα καθολικό ημερολόγιο (ledger), καθώς αυθαίρετα δεδομένα μπορούν να αποθηκευτούν στα μεταδεδομένα των συναλλαγών. Το Bitcoin blockchain υποστηρίζει τα μεταδεδομένα από το 2014. Το αρχικό Bitcoin blockchain υποστηρίζει μόνο 80 bytes από μεταδεδομένα, αλλά άλλα blockchains

υποστηρίζουν μεγαλύτερα μεγέθη. Π.χ. το MultiChain υποστηρίζει μεταδεδομένα με ρυθμιζόμενο μέγεθος και το BigChainDB δεν έχει όριο στο μέγεθος των μεταδομένων [24].

Το Blockchain 2.0 είναι λοιπόν ένα καταναμημένο ημερολόγιο βασισμένο σε blockchain, το οποίο περιλαμβάνει τις νέες τεχνολογίες των α) *έξυπνων δεξιοτήτων* (smart properties) και β) *έξυπνων συμβολαίων* (smart contracts).

Οι *έξυπνες δεξιότητες* αναφέρονται στις ψηφιακές δεξιότητες με ιδιοκτησία ελεγχόμενη από το blockchain.

Τα *έξυπνα συμβόλαια* αναφέρονται στα προγράμματα των υπολογιστών που έχουν σχεδιαστεί για τη διαχείριση των έξυπνων δεξιοτήτων.

Ένα από τα πιο γνωστά συστήματα έξυπνης ιδιοκτησίας-έξυπνου συμβολαίου είναι το Ethereum, το οποίο είναι μια αποκεντρωμένη πλατφόρμα για έξυπνα συμβόλαια. Το Ethereum έχει ως κρυπτονόμισμα το δεύτερο μεγαλύτερο ανώτατο όριο αγοράς μετά το Bitcoin από τον Απρίλιο του 2017. Αξιοσημείωτο είναι πως το Ethereum υιοθετήθηκε από τη Microsoft ως ο πυρήνας του νέου “Blockchain-as-a-service” στο “Azure Cloud Computing” περιβάλλον, [25].

Blockchain 3.0:

Μέχρι στιγμής παρατηρούμε ότι το Blockchain αναφέρεται στον τομέα των οικονομικών. Το Blockchain 3.0 έχει προταθεί για μη οικονομικές εφαρμογές, όπως οι εφαρμογές του τομέα Υγείας.

Το blockchain μπορεί να εφαρμοστεί στον κύκλο της επιστημονικής έρευνας καθώς έχει ιδιαίτερα χαρακτηριστικά όπως: α) αποκεντρωμένο (decentralized), β) καταναμημένο (distributed), γ) αμετάβλητο (immutable), δ) με διαφάνεια (transparent), τα οποία και θα αναλύσουμε λεπτομερώς παρακάτω.

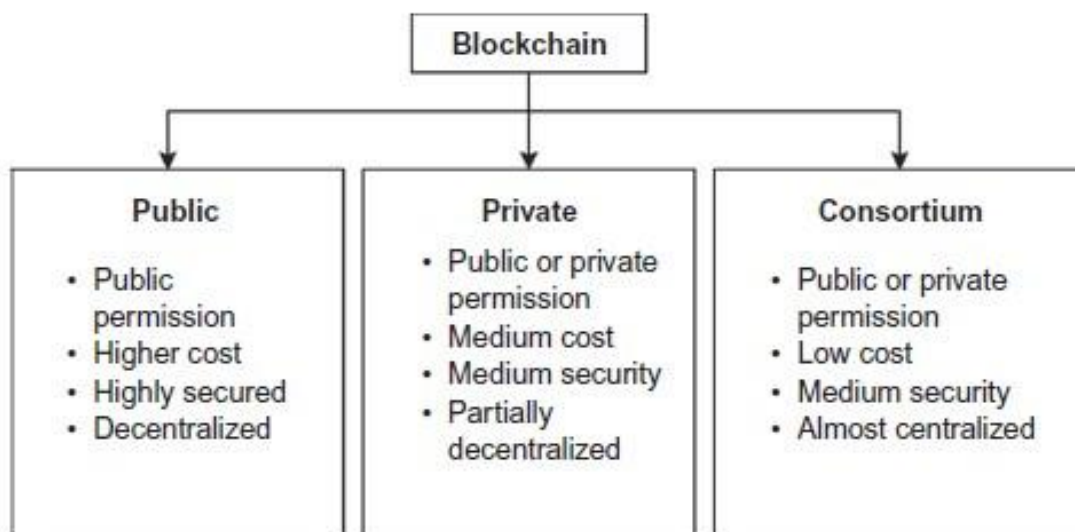
Στις οικονομικές εφαρμογές δικαίωμα συμμετοχής είχαν όλοι όσοι επιθυμούσαν. Σε αυτή την διπλωματική θα ασχοληθούμε με τον τομέα της Υγείας, όπου οι εφαρμογές υλοποιούνται ως blockchain δίκτυα είτε *permission less* (κάθε χρήστης μπορεί να συμμετέχει) , είτε *permissioned* (μπορούν να συμμετέχουν μόνο εξουσιοδοτημένοι ερευνητές ή ιδρύματα).

2.7) Τύποι blockchain

Η τεχνολογία blockchain χωρίζεται σε τρεις τύπους με βάση την άδεια χρήσης (user level permission) και το πεδίο εφαρμογής, στον τομέα υγειονομικής περίθαλψης. Πρόκειται για το δημόσιο (public) , το ιδιωτικό (private) , το κοινοπραξιακό ή ημι-ιδιωτικό (consortium) .

Ένα δημόσιο blockchain χρησιμοποιείται κυρίως για την αποκέντρωση δικτύων και την παροχή ασφαλούς διαφάνειας.

Το ιδιωτικό και το κοινοπραξιακό blockchain προτιμάται όταν απαιτείται περισσότερος έλεγχος και προστασία της ιδιωτικής ζωής .



Εικόνα 2.9 : Διάφοροι τύποι της τεχνολογίας blockchain [26].

2.8) Συσχετιζόμενες εταιρίες και εργασίες:

Guard time [27]

Το 2011, η κυβέρνηση της Εσθονίας και πιο συγκεκριμένα η ‘Εσθονική Αρχή Ηλεκτρονικής Υγείας’ συνεργάστηκε με την εταιρεία Guardtime, μια εταιρεία ασφάλειας δεδομένων. Σκοπός αυτής της συνεργασίας ήταν η δημιουργία ενός πλαισίου βασισμένου σε blockchain για την επικύρωση των ταυτοτήτων των ασθενών. Όλοι οι πολίτες είχαν εκδώσει μια έξυπνη κάρτα, η οποία συνδέει τα EHR με την blockchain-based ταυτότητα. Οποιαδήποτε ενημέρωση στο EHR κατακερματίζεται (hashed) και καταχωρείται στο blockchain. Αυτή η προσέγγιση εξασφαλίζει ότι τα δεδομένα ενός EHR περιέχουν μια αμετάβλητη διαδρομή και ότι τα αρχεία δεν μπορούν να τροποποιηθούν με κακό τρόπο. Οποιαδήποτε τροποποίηση στο EHR είναι ασφαλής και ελεγχόμενη. Τα αμετάβλητα αρχεία καταγραφής δεδομένων με σφραγίδα χρόνου μπορούν επίσης να αρχειοθετήσουν την κατάσταση των πληροφοριών από τις υπάρχουσες Β.Δ. υγειονομικής περίθαλψης. Σε οποιαδήποτε ενημέρωση στη Β.Δ. υγειονομικής περίθαλψης, όπως ο προγραμματισμός ραντεβού, έχει εκχωρηθεί χρονική σφραγίδα και έχει υπογραφεί κρυπτογραφικά σε ένα block. Η εφαρμογή αυτής της blockchain λύσης οδήγησε μέχρι το 2016 στην αποθήκευση 1 εκατομμυρίου ιατρικών αρχείων Εσθονών πολιτών, επιτρέποντας στους ασθενείς να ελέγχουν την πρόσβαση σε δεδομένα μέσω του ‘Keyless Signature Infrastructure’ (KSI). Αυτή η καινοτομία ήταν ένας τρόπος να βοηθήσει στην επίλυση της πρόκλησης για αύξηση της ανταλλαγής κλινικών δεδομένων και της διαλειτουργικότητας για την υγεία και συνεπώς, βελτίωση της διαφάνειας των δεδομένων. Η χρήση της τεχνολογίας Blockchain από την

Εσθονία την έχει καταστήσει μια χώρα όπου το 100% των ιατρικών αρχείων είναι online με ασφαλή και ιδιωτική μέθοδο. Η επιτυχία της Εσθονίας έδωσε εμπιστοσύνη και σε άλλες περιοχές, όπως στο UAE και σε έναν σημαντικό πάροχο υγειονομικής περίθαλψης εκεί. Τέλος αυτή η πλατφόρμα χρησιμοποίησε εκτός από τη Β.Δ. Blockchain και την Oracle για τη διαχείριση των EHR και θεωρείται ως η μεγαλύτερη blockchain πλατφόρμα στον κόσμο.

Health bank: [28]

Η Healthbank, εταιρεία με έδρα την Ελβετία χρησιμοποιεί την χαρακτηριστική φράση : “my data, my choice, my healthbank”. Ο έλεγχος των δεδομένων αφήνεται στο χρήστη ο οποίος μπορεί να επιλέξει να παρέχει τα δεδομένα του για ιατρική έρευνα και ίσως λάβει οικονομική αποζημίωση για αυτή του την επιλογή. Ο χρήστης μπορεί να ανταμειφθεί με υψηλότερο ποσοστό από το κανονικό, εάν τα δεδομένα του έχουν σημαντική αξία. Με αυτό τον τρόπο , η Healthbank γίνεται ένα σύστημα που βασίζεται στον ασθενή (patient-driven system) και το blockchain ερευνάται περισσότερο για να εξασφαλίσει τη γρήγορη, ασφαλή και πιστοποιημένη αυθεντικότητα στην πρόσβαση στα δεδομένα των ασθενών. Αυτό θεωρείται ως ένα καλό παράδειγμα για τη βελτίωση της διαφάνειας και της ασφάλειας στην παγκόσμια κοινότητα των κλινικών ερευνών.

Patientory: [29]

Είναι μια νέα εταιρεία με έδρα της την Ατλάντα των ΗΠΑ. Η φράση κλειδί της εταιρείας είναι: “Your health, at your fingertips”. Η εταιρεία ενισχύει τους τελικούς χρήστες παγκοσμίως με τη χρήση ασφαλούς πλατφόρμας για τη διαχείριση και μεταφορά των δεδομένων υγείας τους και την επίτευξη ενεργών πληροφοριών για βελτιωμένα αποτελέσματα υγείας. Το Patientory δίνει τη δυνατότητα στους ασθενείς, τους κλινικούς ιατρούς, και τους οργανισμούς υγειονομικής περίθαλψης να έχουν ασφαλή πρόσβαση και μεταφορά προστατευμένων πληροφοριών για την υγεία, παρέχοντας παράλληλα χρήσιμες πληροφορίες για τη βελτίωση των αποτελεσμάτων της υγείας. Το Patientory χρησιμοποιεί τεχνολογία blockchain μέσω του PTOYNetwork για να εξασφαλίσει κρυπτογράφηση από άκρη σε άκρη, ενώ τηρεί τις κανονιστικές οδηγίες και τις απαιτήσεις συμμόρφωσης και είναι συμβατό με το HIPPA. Οι ασθενείς συνεργάζονται πιο στενά με τους παρόχους υγειονομικής περίθαλψης για τη μετάδοση των δεδομένων. Η εφαρμογή για κινητές υπηρεσίες υγείας, βοήθησε τους ασθενείς να παρακολουθούν το ιατρικό ιστορικό τους, τους λογαριασμούς τους, τα φάρμακά τους, την ασφάλισή τους και ούτω καθεξής. Επίσης οι ασθενείς μπορούν να συνδεθούν με άλλους ασθενείς με παρόμοια προβλήματα υγείας.

iSolve : [30]

Η Advanced Digital Ledger Technology είναι μια λύση του iSolve που διαχειρίζεται τον κύκλο ζωής ανάπτυξης φαρμάκων και την φαρμακευτική εφοδιαστική αλυσίδα (drug supply chain) στη βιοφάρμα και στη βιομηχανία της υγειονομικής περίθαλψης χρησιμοποιώντας το blockchain ως μηχανισμό παρακολούθησης, ελέγχου και καταγραφής καθ'όλη τη διάρκεια της εφοδιαστικής

κυκλοφορίας των φαρμάκων. Η κοινή χρήση των δεδομένων (data sharing) και η διαφάνεια αποτελούν βασικά στοιχεία του συστήματος. Υπάρχει ανάγκη για σχολαστική παρακολούθηση των φαρμάκων λόγω παραποιημένων και δόλιων φαρμάκων. Αυτό το ζήτημα επισημαίνεται περισσότερο σε περιοχές όπου να κανονιστικά και νομικά πλαίσια δεν είναι ώριμα ή δεν γίνονται οι κατάλληλοι έλεγχοι και παρακολούθηση. Το Blockchain μπορεί να χειριστεί τον κύκλο ζωής των φαρμάκων από την ανάπτυξη έως τη διανομή. Παραδείγματος χάριν οι ημερομηνίες λήξης μπορούν να οδηγήσουν με ακρίβεια και να αναιρέσουν πιθανούς δόλιους επαναπροσδιορισμούς της αλλαγής ημερομηνιών. Το iSolve διαχειρίζεται επίσης την απόκτηση των IP αγαθών, μπορεί να αυξήσει τη χρηματοδότηση και να προωθήσει την ανάπτυξη των φαρμάκων μέσω της Smart Market , όπου οι πληροφορίες διατηρούνται με ασφαλή μέθοδο και είναι ανιχνεύσιμες, αμετάβλητες και ορατές για οποιοδήποτε επενδυτή ή πάροχο επιθυμεί να τις αγοράσει.

Genomes: [31]

Πρόκειται για μια πλατφόρμα αποθήκευσης γονιδιωματικών πληροφοριών εκτός αλυσίδας και εντός αλυσίδας (off-chain, on-chain) η οποία προτάθηκε από τον Hannel. Το Genomes παρέχει επίσης μια πλατφόρμα για την ασφαλή ανταλλαγή βιολογικών πληροφοριών μεταξύ τρίτων. Ως μέσο συναλλαγής εισήχθησαν τα GENE-tokens.

Universal Health Coin : [32]

Πρόκειται για ένα κρυπτονόμισμα που βασίζεται σε blockchain και A.I. για την ανταλλαγή δεδομένων μεταξύ των ενδιαφερομένων και το οποίο πρότεινε ο Gordon. Ο χρήστης αυτού του συστήματος μπορεί να επικοινωνήσει απευθείας με τον καθένα ιδιοκτήτη ή επεξεργαστή δεδομένων για να αγοράσει και να πουλήσει δεδομένα με αυτό το νόμισμα, UHC. Όλες αυτές οι συναλλαγές και τα δεδομένα είναι κρυπτογραφημένα και ασφαλή με ένα ζεύγος κλειδιών ιδιωτικού-δημόσιου.

Modum : [33]

Η εταιρεία Modum ιδρύθηκε το 2016 με σκοπό να βελτιώσει την παρακολούθηση της αλυσίδας εφοδιασμού φαρμάκων (Pharmaceutical Supply Chain). Η ανιχνευσιμότητα και η συμμόρφωση είναι δύσκολο να επιτευχθεί στα τρέχοντα σενάρια και το blockchain μπορεί να παρέχει ένα πιο ανθεκτικό σύστημα παρακολούθησης που ελέγχεται καθ'όλη τη διάρκεια. Ιδιαίτερως στην φαρμακοβιομηχανία, όπου σε ορισμένους κανονισμούς, είναι απαραίτητο να αναφέρονται αποκλίσεις στη θερμοκρασία, τις συνθήκες φωτός, την υγρασία, καθώς οι IoT αισθητήρες παρακολουθούν την θερμοκρασία των προϊόντων και τα δεδομένα των αισθητήρων και μεταφέρονται στο blockchain. Ένα έξυπνο συμβόλαιο (smart contract) πραγματοποιείται στη συνέχεια και οι εγγραφές δεδομένων συγκρίνονται με τις μετρήσεις έναντι απαίτησης συμμόρφωσης. Αυτή είναι η ακεραιότητα και το αμετάβλητο που προσφέρει το σύστημα. Εάν προκύψει κάποια απόκλιση, τότε με μια ειδοποίηση ενημερώνονται τα εμπλεκόμενα μέρη που πρέπει να γνωρίζουν .

Gem Health : [34]

Είναι μια εταιρεία από την Καλιφόρνια, η οποία σε συνεργασία με την εταιρεία-κολοσσό Philips, δημιούργησαν ένα blockchain οικοσύστημα για την υγειονομική περίθαλψη, ονομαζόμενο Gem Health Network. Πρόκειται για μια πλατφόρμα που βρίσκεται στην κορυφή της blockchain-αρχιτεκτονικής και μπορεί εύκολα να αναπτύξει καταναμημένες εφαρμογές. Ο στόχος είναι να συνδέσει όλους τους διαφορετικούς βραχίονες της υγειονομικής περίθαλψης (ασθενείς, πάροχοι, βιομηχανία) έχοντας ως επίκεντρο τον ασθενή για την ανταλλαγή δεδομένων υγείας. Δεδομένου ότι είναι ένα permissioned blockchain μπορεί να ελέγξει ποιος έχει πρόσβαση σε ευαίσθητες πληροφορίες και να διασφαλίσει επίσης την ανωνυμία.

Το GemHealth παρέχει ένα σύστημα διαφανές και σε πραγματικό χρόνο για κάθε ισχυρισμό υγείας. Οι επιστήμονες αναφέρουν ότι σε συνεργασία με την εταιρεία-κολοσσό Philips, αυτή η πλατφόρμα θα μπορεί επίσης να μεταφέρει δεδομένα υγειονομικής περίθαλψης σε πραγματικό χρόνο.

Model-chain: [35]

Οι Kuo και Ohno-Machado πρότειναν την αρχιτεκτονική μοντέλου αλυσίδας, όπου ένας διεπιστημονικός ερευνητής μπορεί να συνεργαστεί για δεδομένα σχετικά με την υγεία. Αυτή η μελέτη εισήγαγε ένα ιδιωτικό blockchain για τη διαχείριση των μεταδεδωμένων των πληροφοριών που σχετίζονται με την υγεία. Το Model-chain υιοθετεί επίσης το blockchain για την ασφαλή και ισχυρή διάδοση μοντέλων πρόβλεψης (privacy-preserving predictive models) για την προστασία της ιδιωτικής ζωής μεταξύ των ιδρυμάτων υγειονομικής περίθαλψης, διότι διαδίδει μόνο προγνωστικά μοντέλα αλλά όχι PHI.

Αυτή η μελέτη χρησιμοποίησε μαζί blockchain και machine learning για τη διευκόλυνση της PCOR έρευνας και τη συνεργασία μεταξύ των θεσμικών οργάνων. (Patient centered outcomes research). Επίσης, η διαδικασία του machine learning χρειάζεται αρκετή ώρα για να «τρέξει», έτσι η ταχύτητα συναλλαγής στο blockchain γίνεται σχετικά αμελητέα.

Επίσης, το Model-chain υιοθετεί permissioned blockchain networks και έτσι οι κακόβουλοι κόμβοι δεν θα μπορέσουν να συμμετάσχουν αυθαίρετα στο δίκτυο και ως εκ τούτου ο κίνδυνος μιας επίθεσης 51% είναι ελάχιστος.

Pokitdoc: [36]

Η αμερικανική πλατφόρμα API as-a-service του Pokitdoc, το καθιστά γρήγορο και εύκολο για τους οργανισμούς υγειονομικής περίθαλψης να φέρουν στην αγορά νέες εφαρμογές και υπηρεσίες. Οι χρήστες μπορούν να αλληλεπιδρούν και να συνδέονται απευθείας με περισσότερους από 700 εμπορικούς συνεργάτες για την ενσωμάτωση των δεδομένων σε πραγματικό χρόνο και να διαχειρίζονται τις ταυτότητές τους για την επικύρωση των συναλλαγών. Οι χρήστες μπορούν να αποκτήσουν πρόσβαση στο 93% των καλυμμένων ζώων των ΗΠΑ από μία πηγή. Είναι συμβατό ως προς τη συμμόρφωση και ασφάλεια με τους HIPPA, HITRUST, PCI, EHNAC, SOC 2, CORE, (Pokitdoc.com)

Burst IQ : [37]

Πρόκειται για μια αμερικάνικη τεχνολογία για την ανάπτυξη ερευνητικών οργανισμών η οποία βασίζεται στο blockchain. Το Burst IQ προσφέρει ένα οικοσύστημα διαχείρισης δεδομένων του χρήστη μέσω διαφόρων υπηρεσιών, κυρίως πλατφορμών. Συγκεκριμένα παρέχει μια διαδραστική πλατφόρμα για την κατανομή των big data μεταξύ ατόμων, χρηστών, οργανισμών. Μέσω της πλατφόρμας αναπτύσσονται γραφήματα προσωπικής ζωής (life graphs) με τα δεδομένα του χρήστη, τα οποία αποθηκεύονται σε ένα πορτοφόλι υγείας (health wallet). Ο χρήστης μπορεί να μοιραστεί, να διαχειριστεί, να πουλήσει και να δωρίσει ατομικές πληροφορίες από αυτό το πορτοφόλι. Για τη σωστή διαχείριση των big data το Burst IQ χρησιμοποιεί επίσης τη Μηχανική Μάθηση. Το Burst IQ είναι συμβατό με το HIPPA, GDPR, NIST.

Medical Chain : [38]

Πρόκειται για ένα κατανεμημένο καθολικό που επιτρέπει στο permissioned based blockchain να αποθηκεύσει με ασφάλεια τα αρχεία υγείας ασθενών και ο χρήστης μπορεί να παραχωρήσει άδεια στους επαγγελματίες της υγείας (γιατροί, φαρμακοποιοί, νοσοκομεία, εργαστήρια) για πρόσβαση στα προσωπικά του ιατρικά δεδομένα. Οι συναλλαγές καταγράφονται και ελέγχονται με ένα διαφανή τρόπο, αλλά το απόρρητο του ασθενούς έχει καίρια σημασία. Αυτό φροντίζει τα ζητήματα της διαλειτουργικότητας και το σενάριο για τον κατακερματισμό των υπηρεσιών υγείας, χρησιμοποιώντας απλά χαρακτηριστικά για να διευκολύνει την αλληλεπίδραση με τους ασθενείς. Σε μια έρευνα που πραγματοποίησε το Νοσοκομείο John Hopkins των ΗΠΑ, συμπεραίνεται ότι τα ιατρικά λάθη είναι ο τρίτος κύριος λόγος θανάτων.

Στη συνέχεια θα μελετήσουμε τι είπε ο καθηγητής Andrew Lippman (αναπληρωτής καθηγητής του MIT Media Lab) για το MedRec στο συνέδριο της MIT Technology Review. Όπως εξήγησε, οι πλήρεις κόμβοι, λειτουργούν ως διακομιστής δεδομένων (data server) και θανάτων στις ΗΠΑ. Με βάση αυτή την έρευνα, εάν οι πληροφορίες θα μπορούσαν να είναι πιο ολοκληρωμένες και η προσέγγιση των δεδομένων υγειονομικής περίθαλψης πιο συντονισμένη, θα είχαμε μείωση των ιατρικών σφαλμάτων.

Youbase: [39]

Πρόκειται για ένα ιεραρχικό ποιοτικό πορτοφόλι HD (hierarchical deterministic wallet) το οποίο προτάθηκε από τον Josh. Αυτό το HD wallet ελέγχει την πρόσβαση στις προσωπικές πληροφορίες και περιέχει δομή τύπου δέντρου με κλειδιά. Το βασικό πλεονέκτημα είναι, λόγω της ύπαρξης διαφόρων κλαδιών (γονική και παιδική αλυσίδα), αυτή η Youbase μπορεί να αποθηκεύσει δεδομένα ξεχωριστά και ανάλογα με το συγκεκριμένο τύπο πληροφοριών. Η τεχνική ανωνυμοποίησης δεδομένων εφαρμόζεται εδώ για συμμόρφωση με τους κανονισμούς προστασίας προσωπικών δεδομένων.

Health-Combix : [40]

Το Health-Combix είναι μια πλατφόρμα διαχείρισης δεδομένων ασθενών η οποία διατηρεί το ιδιωτικό απόρρητο (token-based privacy). Επιπλέον, αυτή η πλατφόρμα εξυπηρετεί και την

πρόβλεψη της ασθένειας, βασισμένη στην ανάλυση των big data και τη νομιματοποίηση διαφανών data αγαθών με διαχείριση κινδύνου (transparent data asset monetization). Ο κύριος σκοπός αυτής της πλατφόρμας είναι η δημιουργία ενός αποκεντρωμένου οικοσυστήματος υγειονομικής περίθαλψης με τη χρήση της peer-to-peer επικοινωνίας σε πραγματικό χρόνο. Για να ξεκινήσει ένα συνεργατικό-ερευνητικό περιβάλλον χρησιμοποιείται ένα ιδιωτικό blockchain.

Blockchain Health : [41]

Πρόκειται για μια αμερικάνικη εταιρεία λογισμικού η οποία διαχειρίζεται δεδομένα που σχετίζονται με την υγειονομική περίθαλψη. Ο Smith ανέπτυξε μια υπηρεσία ,το Pokitdoc, μέσω της οποίας πάνω από 700 ασθενείς και ερευνητές μπορούν να μοιραστούν πληροφορίες. Οι συμμετέχοντες χρησιμοποιούν την Dokchain, η οποία βασίζεται σε μια υποδομή αποθήκευσης δεδομένων εντός και εκτός αλυσίδας. (on-chain and off-chain data storing). Για την επαλήθευση της ταυτότητας ,σε κάθε κόμβο, υπάρχει ένα ζεύγος κλειδιών. Αυτό το σύστημα χρησιμοποιεί ως αλγόριθμο συναίνεσης (consensus algorithm) το PoET. Η συνεχής παρακολούθηση και ασφάλεια των αποθηκευμένων πληροφοριών εξασφαλίζονται μέσω μιας ισχυρής ταυτότητας. Αυτή η πλατφόρμα είναι συμβατή με το HIPPA.

MedRec: [42]

Το *MIT Media Lab* και το ιατρικό κέντρο *Beth Israel Deaconess Health Center* (νοσοκομείο της Ιατρικής Σχολής του Harvard), ανέπτυξαν από κοινού ένα blockchain-based μοντέλο με Ethereum Smart contracts που ονομάζεται MedRec. Σκοπός του να διαχειριστεί τα EHRs ενσωματώνοντας ένα αποκεντρωμένο μοντέλο το οποίο θα παρέχει στους ασθενείς ένα ολοκληρωμένο, αμετάβλητο αρχείο καταγραφής και εύκολη πρόσβαση στις ιατρικές τους πληροφορίες, με όλη την ασφάλεια και με εγγυημένη την ακεραιότητα των δεδομένων μεταξύ των παρόχων και ιστοτόπων θεραπείας. Το MedRec δημιουργήθηκε για να διαχειριστεί πτυχές όπως υπευθυνότητα (accountability), αυθεντικότητα (authentication), εμπιστευτικότητα (confidentiality) οι οποίες είναι απαραίτητες απαιτήσεις για την τρέχουσα κατάσταση παραβίασης δεδομένων (data breach), παραβίαση του κώδικα δεοντολογίας και άλλα συναφή εγκλήματα που σχετίζονται με τα δεδομένα υγειονομικής περίθαλψης.

Το MedRec αποτελεί μια ολοκληρωμένη πλατφόρμα για τον έλεγχο ταυτότητας των ασθενών (data authentication) και την ανταλλαγή (sharing) μεταξύ των ενδιαφερομένων (stakeholders).Πιο συγκεκριμένα προσφέρει μια αποκεντρωμένη προσέγγιση στη διαχείριση των αδειών (permissions), την εξουσιοδότηση (authorization) και την ανταλλαγή των δεδομένων (data sharing) μεταξύ των συστημάτων υγειονομικής περίθαλψης.

Η χρήση blockchain σε αυτή την εφαρμογή έχει ως στόχο να δώσει στους ασθενείς την ικανότητα να έχουν την υπηρεσία και τη γνώση του ποιος μπορεί να έχει πρόσβαση στα δεδομένα υγειονομικής περίθαλψης. Αυτά τα δικαιώματα μπορούν να μοιραστούν σε ένα blockchain για να δημιουργήσουν μια πιο αυτοματοποιημένη προσέγγιση με σκοπό την κοινή χρήση των δεδομένων

για κλινική και ερευνητική χρήση, παρ’όλο που τα πραγματικά δεδομένα της υγειονομικής περίθαλψης δεν αποθηκεύονται στο blockchain.

Ενώ οι άδειες (permissions) , η θέση αποθήκευσης δεδομένων και τα ημερολόγια ελέγχου διατηρούνται στο blockchain, όλα τα στοιχεία της υγειονομικής περίθαλψης παραμένουν στα EHRs συστήματα και απαιτούν πρόσθετα στοιχεία λογισμικού για την επίτευξη πραγματικής διαλειτουργικότητας (interoperability).

Το MedRec δουλεύει με διαφορετικό τρόπο για την αποθήκευση των δεδομένων σε σύγκριση με τον παραδοσιακό τρόπο αποθήκευσης δεδομένων στο EHR: Σε ένα blockchain αποθηκεύει την υπογραφή του αρχείου αντί για τα πραγματικά αρχεία υγείας (έτσι διασφαλίζεται το αμετάβλητο) και έπειτα ειδοποιεί τον ασθενή , ο οποίος είναι υπεύθυνος για το αρχείο και καθορίζει την κίνηση του αρχείου με βάση την απαίτηση. Η αποθήκευση του αμετάβλητου αντιγράφου του αρχείου εξασφαλίζεται με την υπογραφή στο αρχείο. Σε αυτό το μοντέλο ο ασθενής είναι υπεύθυνος για τα δεδομένα και αν τυχόν ο ασθενής δεν ενδιαφέρεται για τη φροντίδα των δεδομένων , τότε κάποιος οργανισμός εξυπηρέτησης θα παίξει αυτό το ρόλο. Τα δεδομένα εισάγονται από τον ιατρό μέσω του MedRec Provider App, όπου η πρόσβαση στα αποθηκευμένα δεδομένα γίνεται μέσω του κατακερματισμένου συνδέσμου (hashed link). Το Ethereum blockchain ελέγχει τις άδειες και ο ασθενής έχει δικαίωμα λήψης (download) ανά πάσα στιγμή καθώς το blockchain επικυρώνει έγκυρα δικαιώματα. Αντί να δημιουργούνται διαφορετικές διεπαφές χρήστη (user interfaces) για διαφορετικά ιδρύματα, το σύστημα MedRec απλοποιεί τη λειτουργία του , διατηρούν το blockchain. Οι κόμβοι αυτοί συντηρούνται από τις οντότητες που παράγουν δεδομένα (ιατροί και ιδρύματα). Τα έξυπνα συμβόλαια ορίζουν την πρόσβαση και τα δικαιώματα στα δεδομένα και είναι η «γλώσσα» στην οποία ορίζεται το blockchain. Τα πορτοφόλια των ασθενών είναι ο τρόπος με τον οποίο τα άτομα αλληλεπιδρούν με το blockchain. Τα πορτοφόλια περιέχουν κλειδιά που παρέχουν πρόσβαση στα κατάλληλα δεδομένα. Όπως αναφέραμε και πιο πάνω τα δεδομένα παραμένουν στον οργανισμό που τα δημιούργησε και όχι στο MedRec. Αυτός ο οργανισμός λειτουργεί τώρα ως κάτοχος ή αποθετήριο δεδομένων όταν εκτελεί τον πλήρη κόμβο. Κατά την εκτέλεση του κόμβου ο οργανισμός συμφωνεί να: 1) είναι το αποθετήριο των Έξυπνων συμβολαίων που αποθηκεύονται στο blockchain και των δεδομένων που δημιουργούνται, 2) τηρεί τις οδηγίες στα Έξυπνα συμβόλαια για να είναι διαθέσιμα τα δεδομένα όπου χρειάζεται και με άδεια.

Το MedRec blockchain βρίσκεται κάπου μεταξύ των Bitcoin blockchain και μιας παραδοσιακής βάσης δεδομένων. Στο Bitcoin blockchain οποιοσδήποτε μπορεί να πάρει μέρος και να συμμετάσχει, γεγονός που αυξάνει σημαντικά την πολυπλοκότητα και τα έξοδα, για να κρατηθεί η αλυσίδα σε λειτουργία. Το MedRec περιορίζει ποιος μπορεί να ενταχθεί στο blockchain σε ιατρικές παροχές και οργανώσεις. Το MedRec blockchain συντηρείται από ιατρικούς ερευνητές. Ως πληρωμή για τη συντήρηση του blockchain , θα αποκτούσαν πρόσβαση σε τυχαία, ανώνυμα δεδομένα υγείας για λόγους έρευνας.

Επίσης, αναφέρεται ότι το MedRec μετατράπηκε περαιτέρω σε ένα PoS μοντέλο: 1) δεν υπάρχουν τέλη συναλλαγής για τη μετακίνηση των δεδομένων ή τη χρήση συμβολαίων , 2) δεν υπάρχει νόμισμα που πρέπει να εξορύσσεται για τις συναλλαγές , 3) διατηρείται από την ομάδα των ενδιαφερομένων (stakeholders) που συνθέτουν οι οργανώσεις υγειονομικής περίθαλψης που συμμετέχουν στο MedRec blockchain.

Το πρόγραμμα MedRec έχει δοκιμαστεί ως απόδειξη της ιδέας (Proof-of-Concept), με τα δεδομένα φαρμάκων και τους προγραμματιστές να προσπαθούν συνεχώς να ενισχύσουν το εύρος του έργου, προσθέτοντας περισσότερους τύπους δεδομένων, συνδρομητές δεδομένων και χρήστες. Όπως αποδεικνύεται από το Proof-of-Concept, η βιοϊατρική και τα αποτελέσματα έρευνας μπορούν να επωφεληθούν σημαντικά από την εφαρμογή του blockchain για την παροχή ταχείας και ασφαλούς πρόσβασης σε διαχρονικά ερευνητικά δεδομένα.

Το blockchain έχει τη δυνατότητα να διευκολύνει την καλύτερη ανταλλαγή δεδομένων για την υγειονομική περίθαλψη και βοηθά και σε διάφορες άλλες εφαρμογές διάγνωσης. Επίσης, είναι πολύ χρήσιμο για τη διαχείριση των δεδομένων, την αποθήκευση, τα EHRs, τις κλινικές δοκιμές, το φαρμακευτικό τομέα, το IoT και τις ιατρικές συσκευές και την τεχνητή νοημοσύνη.

Παρακάτω θα δούμε κάποιες από τις συνεισφορές που προτάθηκαν σχετικά, κάποιες από τις τεχνολογίες και τα συστήματα που αναπτύχθηκαν για αυτό το σκοπό, καθώς επίσης και κάποιες προτάσεις που διατυπώθηκαν.

2.8.1) Εργασίες σχετικά με την ανταλλαγή, διαχείριση, αποθήκευση δεδομένων και EHRs:

Logging system: [43]

Οι επιστήμονες Castaldo και Cinque πρότειναν ένα σύστημα καταγραφής (Logging system) για τη διευκόλυνση και βελτίωση της ανταλλαγής των ηλεκτρονικών δεδομένων υγείας σε πολλές χώρες της Ευρώπης με τον ασφαλέστερο τρόπο.

Healthcare Data Gateway (HDG): [44]

Ο επιστήμονας Yue ανέπτυξε μια εφαρμογή ανταλλαγής δεδομένων υγειονομικής περίθαλψης, την HDG, η οποία βασίζεται στην αρχιτεκτονική του blockchain. Η παρεχόμενη λύση βοηθά στον έλεγχο και την εύκολη κοινή χρήση των δεδομένων του πελάτη χωρίς να θέτουν σε κίνδυνο την ιδιωτικότητα. Η εφαρμογή παρέχει έναν εξαιρετικό τρόπο αύξησης της νοημοσύνης των συστημάτων υγειονομικής περίθαλψης και παράλληλα διατηρεί τα δεδομένα των ασθενών ιδιωτικά.

Cross-domain image sharing: [45]

Ο επιστήμονας Vishal Patel παρουσίασε ένα πλαίσιο για κοινή χρήση εικόνων μεταξύ τομέων, χρησιμοποιώντας την τεχνολογία blockchain ως μια κατακερματισμένη αποθήκευση δεδομένων, για τη δημιουργία ενός ledger ακτινολογικών μελετών και του ελέγχου της κοινής χρήσης των εικόνων από προσαρμοσμένη άδεια του χρήστη.

Med Block: [46]

Ο επιστήμονας Fan και η ομάδα του ανέπτυξαν το Med Block, ένα πλαίσιο, το οποίο βασίζεται στην τεχνολογία blockchain. Τα προβλήματα που επιθυμεί να επιλύσει αφορούν α) στη διαχείριση και κοινή χρήση των δεδομένων σε ένα EMRs σύστημα και β) στη βελτίωση της ανταλλαγής ιατρικών πληροφοριών. Οι ασθενείς μπορούν να έχουν πρόσβαση στο EMR των διαφόρων νοσοκομείων μέσω του πλαισίου Med Block, αποφεύγοντας έτσι τα προηγούμενα ιατρικά δεδομένα να είναι κατακερματισμένα σε διάφορες βάσεις δεδομένων. Επιπλέον, η κοινή χρήση και συνεργασία μέσω blockchain, θα μπορούσαν να βοηθήσουν τα νοσοκομεία να έχουν μια προηγούμενη γνώση του ιατρικού ιστορικού των ασθενών πριν από τη διαβούλευση.

Multi-level location sharing scheme: [47]

Οι επιστήμονες Ji και Zhang, πρότειναν ένα σχήμα κοινής χρήσης τοποθεσίας πολλαπλών επιπέδων που βασίζεται στο blockchain. Ο στόχος ήταν να επιτευχθεί η διαφύλαξη της ιδιωτικής ζωής μέσω blockchain για συστήματα τηλεμεταφοράς ιατρικών πληροφοριών. Οι βασικές απαιτήσεις καθορίζονται για α) αποκέντρωση της κοινής χρήσης τοποθεσίας, β) εμπιστευτικότητα, γ) μεταβλητότητα, δ) προστασία πολλαπλών επιπέδων της ιδιωτικής ζωής, ε) επανόρθωση, στ) αδυναμία, με τη χρήση του Merkle tree και της κρυπτογραφίας. Τα πειραματικά αποτελέσματα έδειξαν ότι το σχέδιο είναι πρακτικό και εφικτό για τους ασθενείς, το ιατρικό προσωπικό, και μπορεί να εφαρμοστεί στην προστασία των πληροφοριών θέσης στα πληροφοριακά συστήματα τηλεργασίας.

Med Chain: [48]

Οι επιστήμονες Shen και Yang πρότειναν μια αποτελεσματική κοινή χρήση δεδομένων, βασισμένη σε συνεδρίες, το Med Chain. Το Med Chain χρησιμοποιεί μια προσέγγιση δομής της αλυσίδας αφοπλισμού για να ελέγξει την ακεραιότητα μιας κοινής ροής ιατρικών δεδομένων IoT. Αυτό γίνεται για να ξεπεραστούν τα θέματα αποτελεσματικότητας των συστημάτων MedRec και Med Block. Τα αποτελέσματα της αξιολόγησης δείχνουν ότι το Med Chain μπορεί να επιτύχει μεγαλύτερη αποτελεσματικότητα και να ικανοποιήσει τις απαιτήσεις ασφαλείας των δεδομένων στην κοινή χρήση των δεδομένων υγειονομικής περίθαλψης.

Controllable blockchain data management in Cloud: [49]

Οι επιστήμονες Zhu, Wu και Gai πρότειναν μια προσέγγιση για την επίτευξη μιας ελεγχόμενης blockchain διαχείρισης δεδομένων σε περιβάλλον Cloud, για την αντιμετώπιση των ανησυχιών των χρηστών σχετικά με την έλλειψη ελέγχου των καταγεγραμμένων ledgers. Στο μοντέλο τους,

σχεδίασαν έναν ειδικό κόμβο εμπιστοσύνης , ο οποίος θα επιτρέπει στους χρήστες να τερματίσουν και να αποτρέψουν τυχόν δυνητικές κακόβουλες ενέργειες ακόμη και σε επιθέσεις που οι κακόβουλοι χρήστες έχουν την πλειοψηφία.

Reshape the consent management: [50]

Σε μια άλλη μελέτη, οι επιστήμονες Genestier και Zouarhi είχαν την ιδέα αναμόρφωσης της διαχείρισης της συγκατάθεσης στο σύστημα υγειονομικής περίθαλψης , η οποία παρέχει κυρίως στο χρήστη τη δυνατότητα του ελέγχου όλης της καταγραφής των δεδομένων υγείας με τη χρήση του blockchain. Ωστόσο, δεν υπάρχει σχεδιασμός εξουσιοδότησης και δεν υπάρχει επίσης έλεγχος πρόσβασης σε αυτή την εκτέλεση.

Patient-centric healthcare data management system: [51]

Οι επιστήμονες Omar και Basu πρότειναν ένα σύστημα διαχείρισης δεδομένων υγειονομικής περίθαλψης με επίκεντρο τον ασθενή, χρησιμοποιώντας την τεχνολογία blockchain για αποθήκευση, που συμβάλλει στην επίτευξη της προστασίας της ιδιωτικής ζωής. Η βασική ιδέα ήταν να κρατηθούν τα ευαίσθητα δεδομένα υγειονομικής περίθαλψης στο blockchain, καθορίζοντας ένα σύνολο από απαιτήσεις ασφαλείας και προστασίας της ιδιωτικής ζωής, για την επίτευξη των α) λογοδοσίας (accountability) , β) ακεραιότητας (integrity), γ) ασφαλείας (security).

Block Cloud: [52]

Οι επιστήμονες Kaur και Alam εισήγαγαν το νέο όρο Block Cloud, που είναι στην πραγματικότητα η μείξη του blockchain που εφαρμόζεται σε περιβάλλον Cloud. Η ιδέα πίσω από την εφαρμογή, είναι να διατηρηθούν τα δεδομένα καταναμημένα και ασφαλή κάτω από την ίδια στέγη χωρίς να εμπλέκονται τρίτοι. Η μελέτη ασχολήθηκε με τις προκλήσεις για το πώς οι πάροχοι και οι οργανισμοί υγειονομικής περίθαλψης , οι δημόσιοι οργανισμοί υγείας και οι κυβερνήσεις , πρέπει να συνεργαστούν και να δημιουργήσουν μια πολιτική επιβολής.

Secure blockchain framework: [53]

Οι επιστήμονες Chen και Zheng ανέπτυξαν ένα ασφαλές πλαίσιο blockchain για την κοινή χρήση των ιατρικών δεδομένων, σχεδιάζοντας ένα ασφαλές cloud αποθετήριο για τα ευαίσθητα ιατρικά αρχεία των ασθενών. Σε αυτό το πλαίσιο η διαχείριση των ιατρικών δεδομένων επιτυγχάνεται με τη χρήση ψηφιακού αρχείου που έχει δικαίωμα ελέγχου πρόσβασης σε πληροφορίες των ιδιοκτητών. Αυτό αποθηκεύεται αναπτύσσοντας κρυπτογράφηση στο cloud.

Attributed-based signature scheme: [54]

Ο επιστήμονας Guo εισήγαγε ένα σχήμα υπογραφής βάσει χαρακτηριστικών, που χρησιμοποιεί τεχνολογία blockchain με πολλαπλές αρχές για την εγγύηση και επικύρωση των EHRs. Αυτό το σχήμα διευκολύνει τις εκπομπές ομαδικών μηνυμάτων και θα μπορούσε να αντισταθεί σε επιθέσεις αθέμιτης σύμπραξης.

Cloud-based EHR system + attribute-based cryptosystem: [55]

Οι επιστήμονες Wang και Song πρότειναν το συνδυασμό ενός ασφαλούς EHR συστήματος που βασίζεται στο Cloud και ενός κρυπτοσυστήματος που βασίζεται στα χαρακτηριστικά. Για να κρυπτογραφήσουν τα ιατρικά δεδομένα χρησιμοποίησαν ένα μείγμα από identity-based encryption + identity-based signatures (κρυπτογράφηση και υπογραφές βασισμένες στην ταυτότητα), ταυτόχρονα για την υλοποίηση ψηφιακών σημάτων.

Omni-PHR: [56]

Οι επιστήμονες αντιμετώπισαν διάφορες προκλήσεις που σχετίζονται με την ενοποίηση του διάσπαρτου αρχείου υγείας και με τη διαχείριση πρόσβασης των ενδιαφερομένων φορέων παροχής υγειονομικής περίθαλψης. Αυτά τα δύο θέματα επιλύθηκαν προτάσσοντας το Omni-PHR. Πρόκειται για ένα καταναμημένο μοντέλο για την ενσωμάτωση των PHR, που χρησιμοποιεί μια παράλληλη βάση δεδομένων για την αποθήκευση των PHR σε blocks.

Genetic algorithms + wavelet transforms: [57]

Οι επιστήμονες ανέπτυξαν ένα πλαίσιο για την εξασφάλιση των ιατρικών αρχείων χρησιμοποιώντας την τεχνολογία blockchain, που βασίζεται σε γενετικούς αλγόριθμους και σε διακεκριμένους μετασχηματισμούς wavelet. Η μέθοδος αυτή χρησιμοποιεί μια τροποποιημένη κρυπτογραφική γεννήτρια κατακερματισμού για τη δημιουργία του απαραίτητου κλειδιού ασφαλείας του χρήστη. Χρησιμοποιήθηκε ο αλγόριθμος MD5 για να παραχθεί μια νέα μορφή κλειδιού, υιοθετώντας ένα διακεκριμένο μετασχηματισμό wavelet. Αυτή η προσέγγιση ενισχύει τη γενική ασφάλεια του συστήματος και την ασυλία σε διάφορες επιθέσεις.

MD5: a message-digest algorithms using a hash function που παράγει μια 128-bit hash value.

2.8.2) Εργασίες σχετικά με τις κλινικές δοκιμές: [58]

Οι επιστήμονες πρότειναν έξυπνα συμβόλαια σε ένα ιδιωτικό Ethereum δίκτυο για την αντιμετώπιση της υποβάθμισης της εμπιστοσύνης και την ενίσχυση της διαφάνειας των δεδομένων σχετικά με τις κλινικές δοκιμές. Ο σκοπός αυτής της μελέτης είναι να βελτιωθεί η επιστημονική αξιοπιστία των ευρημάτων από τις κλινικές δοκιμές, τα οποία θα μπορούσαν να υπονομεύονται από προβλήματα, όπως δεδομένα που λείπουν και επιλεκτική δημοσίευση.

Για να αυξηθεί η ικανότητα των κλινικών δοκιμών και της Ιατρικής Ακριβείας (Precision Medicine), έχουν αναπτυχθεί τέσσερα νέα στοιχεία του συστήματος στην κορυφή του παραδοσιακού blockchain. Αυτά αποτελούνται από: α) πρωτότυπο καταναμημένο και παράλληλο υπολογιστικό σύστημα βασισμένο σε blockchain για αναλύσεις big data, β) στοιχείο διαχείρισης δεδομένων για την ενσωμάτωση των δεδομένων, γ) στοιχείο διαχείρισης ταυτότητας για την προστασία της ιδιωτικότητας στις IoT συσκευές, δ) στοιχείο διαχείρισης της κοινής χρήσης δεδομένων για το συνεργατικό ερευνητικό οικοσύστημα.

Οι επιστήμονες ανέπτυξαν μια ροή εργασίας συναίνεσης στην κορυφή της μεθοδολογίας των κλινικών δοκιμών. Το Proof-of-concept protocol του blockchain, το οποίο βασίζεται σε συλλογή από χρονική σφραγίδα συγκατάθεσης, περιλαμβάνει εγγραφή έξυπνων συμβολαίων. Η ιστορική

ιχνηλασιμότητα παρέχει την ευκαιρία να διασφαλιστεί η επαλήθευση και η διαφάνεια τέτοιων εξαιρετικά ευαίσθητων δεδομένων , ακόμη και όταν αποθηκεύεται ένα έγγραφο σε δημόσιο αποθηκευτικό χώρο , όπως είναι ένας δημόσιος ιστότοπος (website).

2.8.3) Εργασίες σχετικά με τη φαρμακευτική: [59]

Οι επιστήμονες ανέπτυξαν ένα blockchain σύστημα φάρμακο-επαγρύπνησης σε ένα δίκτυο προσομοίωσης για να ελέγξουν τη σκοπιμότητα της εφαρμογής της τεχνολογίας και των αρχών της σε ένα φαρμακευτικό σύστημα επιτήρησης. Ο στόχος ήταν να βελτιωθεί η ανιχνευσιμότητα των ψευδεπίγραφων φαρμάκων. Το σύστημα αντιστέκεται στην παραχάραξη της συμβατικής εφοδιαστικής αλυσίδας φαρμάκων, γεγονός που αποτελεί σημαντικό ζήτημα σε αρκετές Ασιατικές χώρες.

Με πολλούς τρόπους, το Gcoin, Global Governance Coin, παρέχει ένα δυναμικό ρόλο σε όλους τους κόμβους, συμπεριλαμβανομένων των : εκδότης κερμάτων (coin issuer), πλήρης κόμβος (full node), miners, ή απλών κόμβων , σε μια σχέση ιεραρχίας για τη χρήση του στην διαχείριση της εφοδιαστικής αλυσίδας φαρμάκων, SCM.

Οι επιστήμονες πρότειναν ένα Gcoin blockchain , ως βάση της ροής των φαρμακευτικών δεδομένων , για τη δημιουργία διαφανών δεδομένων σχετικά με τις συναλλαγές φαρμάκων. Αυτό μοιράζεται μεταξύ των κατασκευαστών, των χονδρέμπορων, των λιανοπωλητών, των φαρμακείων, των νοσοκομείων και των καταναλωτών. Η καταγραφή των φαρμακευτικών συναλλαγών μπορεί να μετατρέψει τη φαρμακευτική εφοδιαστική αλυσίδα από τη ρύθμιση (κρατικοί έλεγχοι) έως την επιτήρηση (από κάθε συμμετέχοντα). Επιπλέον, θα μπορούσε να αλλάξει το μοντέλο ρύθμισης της εφοδιαστικής αλυσίδας φαρμάκων από την εξέταση και την επιθεώρηση έως το μοντέλο του δικτύου επιτήρησης .

Πάνω από μια δεκαετία, η RFID , (radio frequency identification) , δηλαδή η τεχνολογία αναγνώρισης ραδιοσυχνοτήτων , θεωρείται ως ένας ισχυρός συντηρητής της ιδιοκτησίας. Ωστόσο, έξω από τον τομέα εμπιστοσύνης RFID, το δίκτυο μετά την εφοδιαστική αλυσίδα είναι ευάλωτο να πλαστογραφηθεί με την κλωνοποίηση αυτής της ταυτοποίησης. Αξιοποιώντας την Ethereum Platform και το wallet , τέτοιες ευπάθειες θα μπορούσαν να εξαλειφθούν σε ολόκληρη την εφοδιαστική αλυσίδα, ξεκινώντας από τον κατασκευαστή μέχρι τους τελικούς πελάτες.

2.8.4) Εργασίες σχετικά με το IoT και τις ιατρικές συσκευές:

Οι επιστήμονες εισήγαγαν την ενσωμάτωση των WBANs με blockchain έξυπνα συμβόλαια, για την ασφαλή παρακολούθηση των ασθενών σε πραγματικό χρόνο (secured real-time patient monitoring) και για τα συστήματα ιατρικών παρεμβάσεων (medical interventions systems). Η μελέτη προτείνει την ενσωμάτωση του blockchain για την εκτέλεση των έξυπνων συμβολαίων, που θα αξιολογούσαν τις πληροφορίες που συλλέχθηκαν από τις IoT συσκευές υγειονομικής περίθαλψης του ασθενούς, με βάση τις οριακές τιμές (threshold values). Αυτό γίνεται για να ξεπεραστεί το πρόβλημα της καταγραφής των συναλλαγών των δεδομένων σε ένα IoT σύστημα υγειονομικής περίθαλψης.

Intelligent dyslexia analytics solution: [60]

Οι επιστήμονες εισήγαγαν μια ευφυή λύση για την ανάλυση της δυσλεξίας, όπου ένα αποκεντρωμένο αποθετήριο μεγάλων δεδομένων (a decentralized big data repository) χρησιμοποιείται για αποθήκευση και έπειτα για κοινή χρήση μεταξύ των κοινοτήτων της υγειονομικής περίθαλψης, των ομάδων, καθώς και των μεμονωμένων ατόμων της υγειονομικής περίθαλψης που χρησιμοποιούν το blockchain. Τα “Mobile Multimedia Health” δεδομένα, «συλλαμβάνονται» κατά τη διάρκεια των δοκιμών δυσλεξίας και αποθηκεύονται σε ένα αποκεντρωμένο αποθετήριο μεγάλων δεδομένων (a decentralized big data repository) το οποίο μπορεί να μοιραστεί για περαιτέρω κλινική έρευνα και στατιστική ανάλυση.

Structural Health Monitoring: [61]

Οι επιστήμονες εισήγαγαν την διαρθρωτική παρακολούθηση της υγείας, χρησιμοποιώντας IoT και blockchain. Σε αυτό το νέο σύστημα, η τοπική κεντρική κατανομή και η παγκόσμια αποκεντρωμένη κατανομή ενεργοποιούνται με τη διαίρεσή τους σε δίκτυο άκρων και πυρήνα. Με αυτό τον τρόπο ενισχύεται η αποδοτικότητα και η επεκτασιμότητα του blockchain συστήματος.

PSN based healthcare model: [62]

Οι επιστήμονες εισήγαγαν ένα μοντέλο για τη χρήση ασφαλούς υγειονομικής περίθαλψης βασισμένη σε PSN (Pervasive Social Network). Η βασική πρόκληση αυτού του μοντέλου είναι η διασφάλιση της ασφάλειας των δεδομένων (security) καθώς και η κοινή χρήση τους μεταξύ των PSN κόμβων. Για την αντιμετώπιση αυτού του προβλήματος, οι συγγραφείς ανέπτυξαν δύο πρωτόκολλα.

Το πρώτο πρωτόκολλο που σχεδιάστηκε είναι μια βελτιωμένη έκδοση του IEEE802.15.6, η οποία καθιερώνει ασφαλείς συνδέσμους με μη-ισορροπημένες υπολογιστικές απαιτήσεις για κινητές συσκευές και κόμβους αισθητήρων με περιορισμένους πόρους.

Το δεύτερο πρωτόκολλο χρησιμοποίησε την τεχνολογία blockchain κοινή χρήση δεδομένων υγείας μεταξύ των PSN κόμβων.

A framework tamper-resistant mobile health system for insomnia: [63]

Οι επιστήμονες ανέπτυξαν ένα πλαίσιο ανθεκτικό στις παραβιάσεις για το κινητό σύστημα υγείας (mobile health system) χρησιμοποιώντας την τεχνολογία blockchain, προκειμένου να διασφαλιστεί η αυθεντικότητα των δεδομένων. Ο σκοπός αυτής της μελέτης ήταν να αναπτυχθεί ένα κινητό σύστημα υγείας για τη θεραπεία της αϋπνίας, μέσω εφαρμογής σε Smartphone.

Software defined network: [64]

Ο Nikoloudakis και άλλοι επιστήμονες πρότειναν ένα καθορισμένο δίκτυο από λογισμικά, το οποίο εικονικοποιεί (virtualizes) την παραδοσιακή υποδομή δικτύου σε πολλά αφαιρετικά επίπεδα, για την οικοδόμηση ενός μηχανισμού αντίστασης κατά των κακόβουλων επιθέσεων.

A fog computing architecture: [64]

Οι συγγραφείς πρότειναν επίσης μια αρχιτεκτονική ομίχλης , που εκτιμά τα τρωτά σημεία των νέων και των υφισταμένων hardware του IoT στην υγειονομική περίθαλψη, χρησιμοποιώντας το πλαίσιο Open VAS framework. Το κύριο μειονέκτημα του προτεινόμενου μοντέλου είναι ότι η μέση περίοδος αξιολόγησης μιας μόνο συσκευής είναι περίπου 7 min και 21 sec , η οποία είναι υπερβολικά μεγάλη και δημιουργεί σοβαρές ανησυχίες σχετικά με την επεκτασιμότητα του συστήματος. Αυτό το θέμα θα μπορούσε να αντιμετωπιστεί χρησιμοποιώντας την Blockchain-based Ethereum Platform , καθώς εδώ ο χρόνος εξόρυξης ενός block (block-mining) είναι 10-15 sec.

Application hardening: [65]

Μια άλλη μελέτη από τους Nausheen και Begum προτείνει μια διαφορετική λύση βασισμένη σε application hardening, όπως παραμόρφωση κώδικα (code obfuscation) και εφαρμογή προγράμματος διεπαφής (APIs = application program interface) , για την προστασία του key logic και mobile apps, αντίστοιχα. Η μελέτη προτείνει την προσθήκη ενός αμυντικού στρώματος (defense layer) εναντίον της αντίστροφης μηχανικής (reverse engineering) , με return oriented προγραμματισμό και τεχνικές αθροίσματος ελέγχου (check summing techniques). Παρ’όλο που η προστασία της ασφάλειας των εμφυτευμένων ιατρικών συσκευών (implanted medical devices gadgets) υποστηρίζεται καλά σε αυτή τη μελέτη, απαιτούνται να ενσωματωθούν ετερογενείς τεχνολογίες για μεγαλύτερη απόδοση, αλλά σε βάρος της αυξημένης πολυπλοκότητας σε όλο το σύστημα.

Adaptively supervised and Clustered Hybrid IDS (ASCH-IDS): [66]

Προκειμένου να ενισχυθούν τα συστήματα ανίχνευσης εισβολών IDSs (Intrusion Detection Systems) στο IoT , οι ερευνητές εισήγαγαν την τεχνική ASCH-IDS, η οποία ταξινομεί τους πιθανούς εισβολείς από τα συγκεντρωτικά δεδομένα των αισθητήρων. Μια ανάμοια αναλογία αθροιστικής κυκλοφορίας στους αισθητήρες τροφοδοτείται σε δύο υποσυστήματα ανίχνευσης για καλύτερη απόδοση: 1) Anomaly detection = ADSs (ανίχνευση ανωμαλιών) και 2) Misuse detection= MDSs (κοινή χρήση ανίχνευσης) .

Έχει ενδιαφέρον, όταν η αναλογική προσαρμογή αυξάνει την καλή λειτουργία του συστήματος και δείχνει την υψηλότερη ακρίβεια όσον αφορά την Ευαισθησία και την Ειδικότητα , στην περίπτωση που η αναλογία των αισθητηριακών δεδομένων για την ανίχνευση αποτυχίας (misuse detection) είναι 0:25 % . Αυτή η διαδικασία υποδεικνύει ένα αυξημένο ποσοστό ανίχνευσης.

Restricted Boltzmann Machine-based Clustered IDS (RBC-IDS): [67]

Οι ίδιοι ερευνητές εισήγαγαν την RBC-IDS, μια μεθοδολογία βασισμένη σε deep-learning για την παρακολούθηση της υποδομής για πιθανούς εισβολείς. Χρησιμοποιήθηκαν τρία κρυμμένα επίπεδα (hidden layers) , τα οποία δείχνουν αυξημένη ακρίβεια 99.91% σε σύγκριση με το 99.80% της προηγούμενης μελέτης. Ωστόσο, το κόστος αυτού του πειράματος είναι διπλάσιο από το προηγούμενο.

Smart hospital system: [68]

Οι Catarinucciet και De Donno σε μια προσπάθεια να μειωθεί η ευπάθεια της ασφάλειας της RFID στην υποδομή της IoT υγειονομικής περίθαλψης, πρότειναν ένα έξυπνο νοσοκομειακό σύστημα που αποτελείται από hybrid-sensing network, εκμεταλλευόμενοι α) την περιορισμένη εφαρμογή πρωτοκόλλου, β) την IoT smart gateway , γ) user interface , παρέχοντας σε τρίτους τη δυνατότητα ενίσχυσης των ασθενών με το σύστημα παρακολούθησης της υγείας (health monitoring system). Ωστόσο, τα δεδομένα που συλλέγονται από τις IoT συσκευές, αποθηκεύονται σε μια κεντρική βάση δεδομένων, η οποία είναι επιρρεπής. Αυτό θα μπορούσε να αντιμετωπιστεί χρησιμοποιώντας ένα αποκεντρωμένο ημερολόγιο (decentralized ledger), όπως το blockchain, επειδή τα data blocks αντιγράφονται σε κατανεμημένους κόμβους δικτύου (decentralized network nodes), για βελτιωμένη διαφάνεια.

Internet of entities: [69]

Ο Robereto Saia πρότεινε παράλληλα με το παραπάνω έργο, μια νέα προσέγγιση για το δίκτυο των οντοτήτων, που ενσωματώνει Mobile και IoT δίκτυα σε δύο βασικά στοιχεία: οντότητες όπως οι συσκευές χρηστών και έναν ιχνηλάτη που διευκολύνει την μετάδοση των πληροφοριών στο blockchain. Η προτεινόμενη αρχιτεκτονική είναι μια μείξη των ασύρματων (wireless) δικτύων και των blockchain δικτύων, που μπορούν να χρησιμοποιηθούν για υπηρεσίες υγειονομικής περίθαλψης. Η σωστή εφαρμογή ενός τόσο μεγάλου και περίπλοκου δικτύου μπορεί να εμφανίσει κάποιους περιορισμούς. Ένας από αυτούς είναι η υπολογιστική βελτιστοποίηση του blockchain.

A novel lightweight architecture for networks: [70], [71]

Οι επιστήμονες έχουν διερευνήσει την ασφάλεια (security) και ιδιωτικότητα (privacy) των δεδομένων στον τομέα της υγειονομικής περίθαλψης , εισάγοντας διαφορετικές μορφές δομής δεδομένων στο blockchain. Ωστόσο, λόγω της πολυπλοκότητας που υπάρχει στην αποθήκευση του μεγάλου όγκου δεδομένων υγείας στο blockchain, η μελέτη χρησιμοποιεί μόνο το “hash” των δεδομένων ως συναλλαγή. Αυτό μόνο δεν φτάνει για να διασφαλιστεί η ασφάλεια των δεδομένων. Μειώνοντας τα γενικά έξοδα της εφαρμογής blockchain στα δίκτυα μικρών περιοχών (small area networks) είναι μια δύσκολη πρόκληση, δεδομένου ότι η προσθήκη blocks στην αλυσίδα, ακολουθώντας κρυπτογραφικούς αλγορίθμους εξόρυξης (mining algorithms), όπως είναι το PoW, απαιτεί τεράστια υπολογιστική ισχύ. Για την αντιμετώπιση αυτής της πρόκλησης, οι Doris και Kanhere πρότειναν μια νέα ελαφριά αρχιτεκτονική για δίκτυα, που περιλαμβάνει πολλές IoT συσκευές.

Ένας υπολογιστής χρησιμοποιείται ως miner και ένας αριθμός IoT συσκευών συλλέγονται μεταξύ τους, έτσι ώστε να επιλέγεται ένα ως Cluster head (κεφαλίδα συμπλέγματος) , με σκοπό να μειώσει την επαλήθευση πρόσβασης (access verification), χρησιμοποιώντας Policy header. Αυτό το σχήμα επιτρέπει στον Policy header να διαθέτει ενημερωμένη λίστα ελέγχου πρόσβασης , την οποία διαχειρίζεται ο διαχειριστής του δικτύου (network operator). Επιπλέον, αυτή η μελέτη χρησιμοποίησε ένα κοινό δίκτυο επικάλυψης (shared overlay network), όπου πολλοί data owners επιτρέπεται να εισάγουν δεδομένα στα blocks, τα οποία ελέγχονται από έναν μόνο διαχειριστή. Ωστόσο, αυτό μπορεί να οδηγήσει σε έλλειψη αξιοπιστίας μεταξύ των χρηστών.

Οι Khan και Salah, κάνοντας μια ανασκόπηση, εντόπισαν πολλές αδυναμίες ασφάλειας και προστασίας της ιδιωτικότητας στο παρόν IoT οικοσύστημα. Μία περίπτωση αφορά την προστασία κατά τη διάρκεια της ενημέρωσης του λογισμικού δισεκατομμυρίων IoT συσκευών υγειονομικής περίθαλψης. Το blockchain θα μπορούσε να χρησιμοποιηθεί για την ενίσχυση της ασφάλειας. Στα μέσα του 2016, 3,62 εκατομμύρια δεδομένα ασθενών, συμπεριλαμβανομένων των προσωπικών πληροφοριών, του αριθμού κοινωνικής ασφάλισης και του αριθμού της πιστωτικής κάρτας, διακυβευόνταν στο Banner Health της Αριζόνας.

Το Banner Health είναι ένα μη κερδοσκοπικό σύστημα υγείας που ιδρύθηκε το 1999 στις ΗΠΑ. Στο σύνολό του λειτουργεί 28 νοσοκομεία σε 6 πολιτείες με περισσότερους από 50.000 υπαλλήλους και θεωρείται ένας από τους μεγαλύτερους εργοδότες στις ΗΠΑ, (https://en.wikipedia.org/wiki/Banner_Health).

2.8.5) Εργασίες σχετικά με την Τεχνητή Νοημοσύνη:

Model Chain framework: [72]

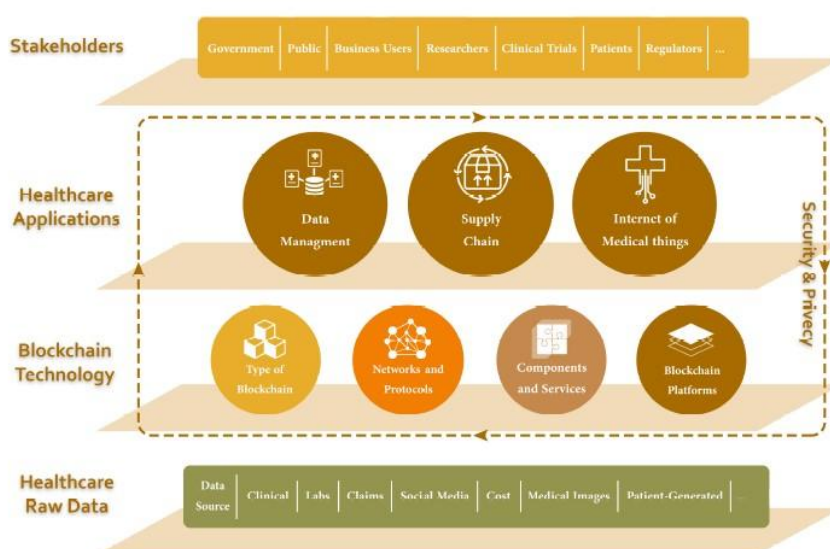
Οι Kuo και Ohmo-Machado εισήγαγαν το πλαίσιο Model Chain, που βασίζεται στην τεχνολογία blockchain. Αυτό το πλαίσιο χρησιμοποιεί ένα ιδιωτικό blockchain, προκειμένου να δοθεί η δυνατότητα σε πολλά ιδρύματα να προσφέρουν τα δεδομένα υγείας και τις απαραίτητες πληροφορίες, με σκοπό την κατάρτιση ενός μοντέλου μηχανικής μάθησης, χωρίς να αποκαλύπτονται όμως τα αρχεία υγείας τους. Ένα τέτοιο πλαίσιο αυξάνει την ασφάλεια και την ευρωστία του κατανεμημένου μοντέλου πρόβλεψης για την προστασία της ιδιωτικής ζωής, σε πολλά ιδρύματα.

Parallel Health System (PHS): [73]

Οι Wang και Yuan πρότειναν ένα παράλληλο σύστημα υγειονομικής περίθαλψης βασισμένο στο blockchain. Σε αυτό το σύστημα συμπεριλαμβάνονται: α) artificial systems (τεχνητά συστήματα), β) computational experiments (υπολογιστικά πειράματα), γ) parallel execution (παράλληλη εκτέλεση), δηλαδή ACP. Το ACP επικεντρώνεται κατά κύριο λόγο σε: α) διάγνωση του ασθενούς, β) κατάσταση, γ) διαδικασία θεραπείας. Στο PHS προστίθεται ένα consortium blockchain, για να συνδέσει νοσοκομεία, ασθενείς, υγειονομικό προσωπικό και τις συναφείς κοινότητες.

ΚΕΦΑΛΑΙΟ 3 : ΕΦΑΡΜΟΓΕΣ

Η τεχνολογία blockchain επαναπροσδιορίζει τη μοντελοποίηση των δεδομένων και τη διακυβέρνηση που αναπτύσσονται σε πολλές εφαρμογές της υγειονομικής περίθαλψης. Αυτό οφείλεται κυρίως στην προσαρμοστικότητα και τις ικανότητές του να διαχωρίζει, να διασφαλίζει και να μοιράζεται τα ιατρικά δεδομένα και υπηρεσίες υγείας με πρωτοφανή τρόπο. Η τεχνολογία blockchain βρίσκεται στο επίκεντρο πολλών πρόσφατων εξελίξεων στον τομέα της Υγείας. Οι αναδόμενες τεχνολογίες στον τομέα της Υγείας που βασίζονται στο blockchain είναι οργανωμένες σε τέσσερα επίπεδα : Data sources(πηγές δεδομένων) , Blockchain technology, Healthcare apps, Stakeholders(ενδιαφερόμενοι) , όπως φαίνεται και στην παρακάτω εικόνα.



Εικόνα 3.1 : Αναπαράσταση της ροής εργασίας των εφαρμογών υγειονομικής περίθαλψης που βασίζονται στο blockchain [74]

Πρώτο στρώμα:

Όλα τα δεδομένα από τις ιατρικές συσκευές, τα εργαστήρια, τα κοινωνικά μέσα και πολλές άλλες πηγές, ενοποιούνται και δημιουργούν τα Πρωτογενή δεδομένα (Raw data), τα οποία στη συνέχεια αυξάνονται σε κλίμακα και δημιουργούνται τα big data. Αυτά τα δεδομένα είναι το βασικό και κύριο συστατικό της συνολικής υγειονομικής περίθαλψης βασισμένη σε blockchain [74].

Δεύτερο στρώμα:

Πάνω από το στρώμα των Raw Data βρίσκεται η Τεχνολογία Blockchain, η οποία θεωρείται ότι αποτελεί το κύριο πλαίσιο που επιδιώκει μια ασφαλή αρχιτεκτονική και χωρίζεται σε τέσσερις συνιστώσες.

- Type of blockchain:

Οι υπεύθυνοι χάραξης πολιτικής θα μπορούσαν να επιλέξουν είτε Public, είτε Private, είτε Consortium blockchain, βάσει των απαιτήσεων που πρέπει να εκπληρωθούν.

- Networks and Protocols:

Για την επικοινωνία με άλλα προγράμματα και πλαίσια ή ακόμη και μέσω διαφορετικών δικτύων, θα μπορούσε να χρησιμοποιηθεί ένα ευρύ φάσμα δικτύων και πρωτοκόλλων. Αυτό μπορεί να περιλαμβάνει: P2P, centralized, decentralized, distributed.

- Components and services:

Οι βασικές συνιστώσες του blockchain είναι: smart contracts, signatures, digital wallet, digital assets, events, membership.

- Blockchain platforms:

Κάθε blockchain platform έχει διαφορετικά χαρακτηριστικά, όπως αλγορίθμους συναίνεσης και πρωτόκολλα. Οι blockchain platforms διευκολύνουν τους χρήστες στο να δημιουργούν και να διαχειρίζονται τις συναλλαγές τους. Αρκετές από αυτές έχουν δημιουργηθεί και χρησιμοποιούνται επί του παρόντος, όπως Ethereum, Ripple, Hyperledger fabric [75].

Τρίτο στρώμα:

Μόλις δημιουργηθεί η Blockchain platform, η επόμενη φάση είναι να διασφαλιστεί ότι οι εφαρμογές είναι ενσωματωμένες σε ολόκληρο το σύστημα, αυτές είναι οι Healthcare applications.

Οι Healthcare applications μπορούν να ταξινομηθούν σε τρεις μεγάλες κατηγορίες: Data Management, Supply Chain, Internet of Medical Things [74].

- 1) Data Management apps:

- 1.1) Παγκόσμια ανταλλαγή επιστημονικών δεδομένων για έρευνα και ανάπτυξη (global scientific data sharing)
- 1.2) Διαχείριση δεδομένων (data management)
- 1.3) Αποθήκευση δεδομένων (data storage)
- 1.4) Ηλεκτρονικά αρχεία υγείας: EHRs (electronic health records).

- 2) Supply Chain Management (SCM) apps:

- 2.1) Κλινικές δοκιμές (clinical trials)
- 2.2) Φαρμακευτική

- 3) Internet of Medical Things (IoMT) apps:

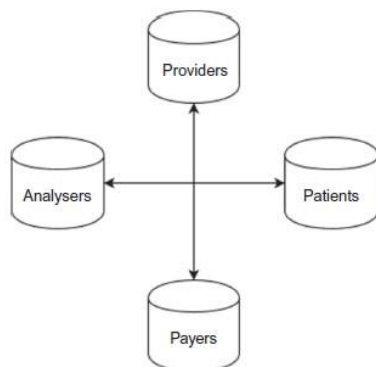
- 3.1) Υγειονομική περίθαλψη με IoT και ιατρικές συσκευές
- 3.2) Υποδομή του IoT στον τομέα της υγείας και της ασφάλειας των δεδομένων
- 3.3) Τεχνητή Νοημοσύνη (Artificial Intelligence)

Τέταρτο στρώμα:

Στην κορυφή της ιεραρχίας είναι οι Stakeholders (ενδιαφερόμενοι). Αυτό το επίπεδο αποτελείται από τα μέρη που επωφελούνται από τις εφαρμογές του blockchain στον τομέα της υγειονομικής περίθαλψης. Οι βασικές ανησυχίες των χρηστών σε αυτό το επίπεδο είναι να μοιράζονται, να

επεξεργάζονται και να διαχειρίζονται τα δεδομένα χωρίς όμως να θέτουν σε κίνδυνο την ασφάλεια και την ιδιωτικότητά τους (security-privacy) [74]. Οι κύριοι Stakeholders στον τομέα της Υγείας είναι : οι ασθενείς, οι πάροχοι, οι αναλυτές και αυτοί που πληρώνουν (ασφαλιστικές) οι οποίοι συνεργάζονται μεταξύ τους.

Για να εκτελεστεί μια λεπτομερής ανάλυση των ιατρικών αρχείων, θα πρέπει να υπάρχει επαρκής συνεργασία και επικοινωνία μεταξύ των τεσσάρων αυτών ενδιαφερομένων. Επίσης, τα περιστατικά ασφαλείας και παραβίασης της ιδιωτικής ζωής συνδέονται με αυτές τις τέσσερις οντότητες [23].



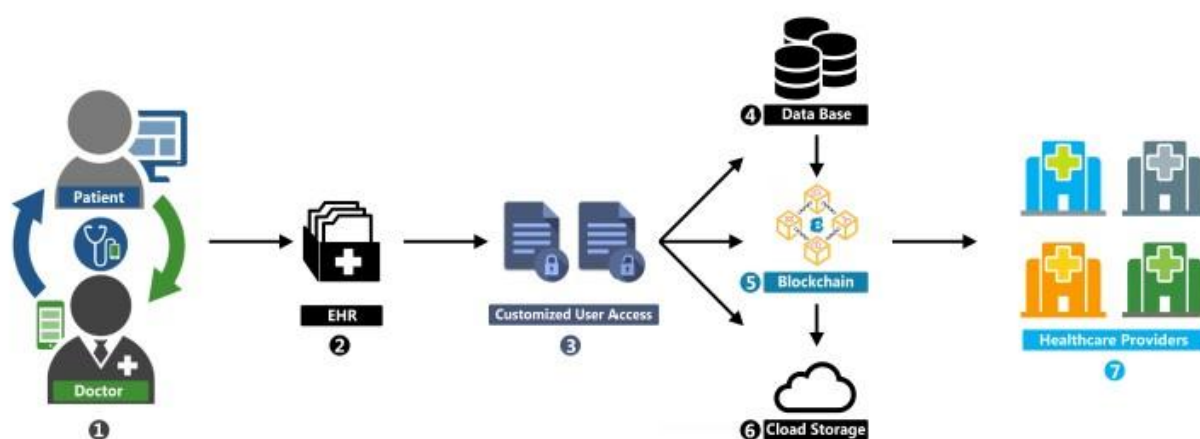
Εικόνα 3.2: Οι ενδιαφερόμενοι για τα δεδομένα υγειονομικής περίθαλψης [23]

- Οι ασθενείς (patients) αποτελούν την πηγή όλων των τύπων δεδομένων. Οι ασθενείς παράγουν αυτές τις πληροφορίες χρησιμοποιώντας Φορητές συσκευές (wearable devices) και αρχεία υγείας.
- Οι οντότητες που πληρώνουν (payers) είναι αυτοί που υποστηρίζουν άμεσα ή έμμεσα τους ασθενείς καταβάλλοντας το ποσό για την υγειονομική περίθαλψη (ασφαλιστικές εταιρείες, στεγαστικά δάνεια, ιδιωτικές πηγές) .
- Οι πάροχοι (providers) είναι αυτοί που συλλέγουν και αποθηκεύουν τα ιατρικά αρχεία (νοσοκομεία, κλινικές, ιατρικά κέντρα, τράπεζες αίματος).
- Οι αναλυτές και οι ερευνητές (analyzers) είναι αυτοί που χρησιμοποιούν τις πληροφορίες που παρέχονται από τις προαναφερθείσες πηγές με σκοπό τη βελτίωση της απόδοσης του τομέα Υγείας.

3.1) Data Management apps:

Με την πρόοδο στα ηλεκτρονικά δεδομένα που σχετίζονται με την υγεία (electronic health related data) , στην αποθήκευση δεδομένων υγείας σε cloud (cloud healthcare data storage) και στους κανονισμούς προστασίας ιδιωτικότητας των δεδομένων των ασθενών (patient data privacy protection regulations) , δημιουργούνται νέες ευκαιρίες για τη διαχείριση δεδομένων υγείας (Health data management) καθώς και για την ευκολία των ασθενών να έχουν πρόσβαση και να μοιράζονται τα δεδομένα τους [76]. Η διασφάλιση, η αποθήκευση, η συναλλαγή, η διαχείριση της ομαλής ενσωμάτωσής τους είναι εξαιρετικά πολύτιμη σε οποιαδήποτε οργάνωση που βασίζεται σε δεδομένα, ειδικά στην υγειονομική περίθαλψη όπου η τεχνολογία blockchain έχει να επιλύσει αυτά τα κρίσιμα ζητήματα με έναν ισχυρό και αποτελεσματικό τρόπο [74].

Στην παρακάτω εικόνα θα δούμε τα 7 στάδια της ροής εργασιών στη διαχείριση δεδομένων υγειονομικής περίθαλψης στο blockchain. Οι εφαρμογές αυτής της κατηγορίας περιλαμβάνουν : data sharing, data management, data storage, EHRs .



Εικόνα 3.3: Διαχείριση δεδομένων υγειονομικής περίθαλψης στο blockchain [74]

Βήμα 1:

Τα πρωτογενή δεδομένα δημιουργούνται μεταξύ των ασθενών και των γιατρών τους. Αυτά τα δεδομένα αποτελούνται από το ιατρικό ιστορικό, το τρέχον πρόβλημα και άλλες πληροφορίες σχετικές.

Βήμα 2:

Δημιουργείται ένα EHR αρχείο για κάθε ασθενή χρησιμοποιώντας τα πρωτογενή δεδομένα που συλλέχθηκαν στο Βήμα 1. Στο EHR περιλαμβάνονται και άλλες ιατρικές πληροφορίες ,όπως αυτές που προκύπτουν από νοσηλευτική φροντίδα, ιατρική απεικόνιση και ιστορικό φαρμάκων.

Βήμα 3:

Κάθε μεμονωμένος ασθενής έχει στην ιδιοκτησία του ένα ευαίσθητο EHR και ο προσαρμοσμένος έλεγχος πρόσβασης (customized user access) δίνεται μόνο στον ιδιοκτήτη αυτής της ιδιοκτησίας. Τα μέρη που επιθυμούν να έχουν πρόσβαση σε αυτές τις πολύτιμες πληροφορίες , πρέπει να

ζητήσουν άδεια από τον ιδιοκτήτη του EHR και ο ιδιοκτήτης θα αποφασίσει σε ποιον θα παρασχεθεί πρόσβαση.

Βήματα 4,5,6 :

Αυτά τα τρία βήματα είναι μέρος του πυρήνα της όλης διαδικασίας, συμπεριλαμβανομένων των : Database, Blockchain, Cloud Storage. Το Database και το Cloud Storage αποθηκεύουν τα αρχεία με έναν κατακεντρωμένο τρόπο και το Blockchain παρέχει υψηλή προστασία της ιδιωτικότητας (privacy) για να διασφαλιστεί η προσαρμοσμένη, αυθεντική πρόσβαση χρηστών (user access).

Βήμα 7:

Οι Healthcare Providers (πάροχοι υγειονομικής περίθαλψης) , όπως κλινικές, κοινοτικά κέντρα φροντίδας, νοσοκομεία είναι οι τελικοί χρήστες που θέλουν να έχουν πρόσβαση για μια ασφαλή και υγιή παράδοση φροντίδας, η οποία θα εγκριθεί από τον ιδιοκτήτη. Ανεξαρτήτως από το πού δέχεται ιατρική φροντίδα ένας ασθενής σε όλο τον κόσμο, το δικό του EHR θα είναι διαθέσιμο και επίσης προσβάσιμο στο τηλέφωνό του και επικυρωμένο μέσω ενός DLT , όπως το blockchain, στο οποίο οι πάροχοι θα συνεχίζουν να προσθέτουν πληροφορίες με την πάροδο του χρόνου [77].

3.1.1) Παγκόσμια ανταλλαγή επιστημονικών δεδομένων για έρευνα και ανάπτυξη (data sharing)

Η ανταλλαγή των ιατρικών δεδομένων και των δεδομένων υγειονομικής περίθαλψης είναι ένα βασικό και ουσιαστικό βήμα για τη βελτίωση της ποιότητας των παρόχων υγειονομικής περίθαλψης και καθιστά το σύστημα της υγειονομικής περίθαλψης πιο έξυπνο [44].

Η ανταλλαγή των αρχείων υγείας θα μπορούσε να γίνει μεταξύ ατόμων.

Ένα σενάριο θα μπορούσε να είναι ένας ασθενής που θέλει να μοιραστεί το ιατρικό του ιστορικό με έναν γιατρό στην πρώτη τους συνάντηση [78]. Επιπλέον , η ανταλλαγή μπορεί να συμβεί μεταξύ ενός ατόμου με έναν stakeholder. Ο ασθενής που θέλει να μοιραστεί το ιατρικό του ιστορικό με μια ασφαλιστική εταιρεία ή ένα ερευνητικό κέντρο. Επιπλέον, τα δεδομένα μπορούν να μοιραστούν και πέρα από τα σύνορα [43].

Ωστόσο, ο μηχανισμός λειτουργίας των σημερινών συστημάτων που σχετίζονται με την υγεία έχει κάποιους περιορισμούς.

Ένας περιορισμός είναι ότι οι ασθενείς μόλις που έχουν πρόσβαση στα ιατρικά τους αρχεία. Ως εκ τούτου, δεν έχουν ιδέα για την ανταλλαγή και κοινή χρήση των δικών τους ιατρικών δεδομένων μεταξύ αγνώστων [79].

Για να βελτιωθεί η αλληλεπίδραση και η συνεργασία με τη βιομηχανία της υγειονομικής περίθαλψης, η τεχνολογία blockchain θα μπορούσε να διαδραματίσει καίριο ρόλο, επιτρέποντας και εξασφαλίζοντας ένα βολικό μηχανισμό ανταλλαγής και κοινής χρήσης των ηλεκτρονικών

δεδομένων υγείας. Αυτό θεωρείται ως μια από τις σημαντικότερες συνεισφορές της τεχνολογίας [80].

3.1.2) Διαχείριση δεδομένων (data management)

Τα ιδρύματα υγειονομικής περίθαλψης και οι εταιρείες που καθοδηγούνται από δεδομένα καθώς και ο όγκος των δεδομένων που δημιουργούνται σε αυτή την περιοχή ή σε άλλη περιοχή (IoT) , αυξάνεται σημαντικά. Παρά όλα αυτά, η ασφάλεια των δεδομένων και της ιδιωτικής ζωής παραβιάζονται συνεχώς , τόσο ακούσια, όσο και από παράνομους χρήστες [81]. Ως αποτέλεσμα, πολλά ιδρύματα έχουν βιώσει τεράστια απώλεια φήμης και κεφαλαίου. Οι διαφορετικοί χρήστες των ιατρικών δεδομένων έχουν διαφορετικούς ρόλους και η πρόσβαση στα δεδομένα θα πρέπει να διέπεται από τα δικαιώματα που χορηγούνται σε αυτούς τους ρόλους. Αυτή η πρόσβαση μπορεί να εξασφαλιστεί με ομαλό τρόπο, με τη χρήση της τεχνολογίας blockchain.

3.1.3) Αποθήκευση δεδομένων (data storage)

Σε ένα σύστημα υγειονομικής περίθαλψης που βασίζεται στο blockchain , κάθε συναλλαγή αποθηκεύεται σε blocks σε σύστημα αποκεντρωμένης αποθήκευσης. Σε ένα σύστημα υγειονομικής περίθαλψης τα δεδομένα των ασθενών οργανώνονται σε EMRs, τα οποία θεωρούνται τα δομικά στοιχεία μιας μεγάλης κατανεμημένης ιατρικής αποθήκης [82]. Αυτά θα μπορούσαν να αποθηκευτούν επί τόπου ή στο Cloud, όπου η ασφάλεια είναι το κύριο μέλημα.

Η Cloud Storage, είναι κυρίως η σύνθεση πολυάριθμων συσκευών αποθήκευσης , που συνδέονται όλες μαζί για να σχηματίσουν έναν μεγάλο όγκο αποθήκευσης , με σκοπό να φιλοξενήσουν πολλές υποδομές τεχνολογίας πληροφοριών, (ITI=Information Technology Infrastructure) . Ένα σύστημα υγειονομικής περίθαλψης που βασίζεται στο blockchain είναι ένα παράδειγμα ITI.

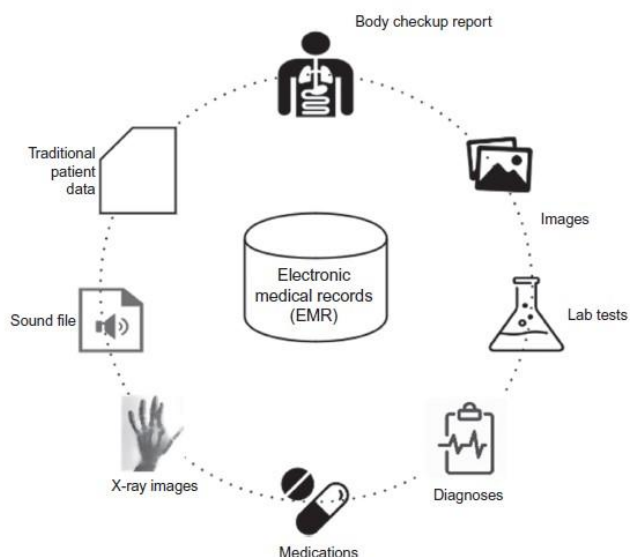
Η Cloud Storage έχει τα πλεονεκτήματά της , όπως: α)γρήγορη μετάδοση, β)σωστή κοινή χρήση, γ)χωρητικότητα αποθήκευσης, δ)χαμηλό κόστος, ε)εύκολη πρόσβαση, στ) δυναμική σύνδεση [83].

3.1.4) Ηλεκτρονικά αρχεία υγείας : EHRs (electronic health records).

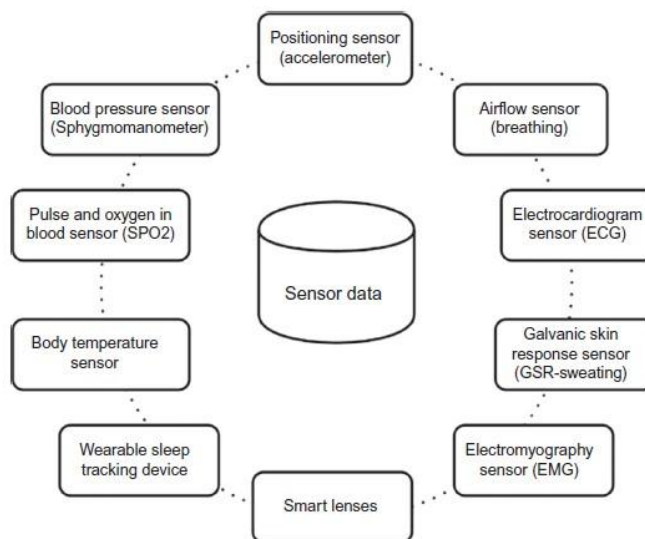
Εξαιτίας της εμφάνισης του σύγχρονου τομέα υγειονομικής περίθαλψης, τα περισσότερα από τα συστατικά που συνδέονται με τις βιομηχανίες υγειονομικής περίθαλψης παράγουν τεράστια ποσά δεδομένων. Διάφορα ιατρικά αρχεία είναι διαθέσιμα από διάφορες πηγές, όπως δεδομένα ασθενών, ακτινογραφίες, υπέρηχοι, μαγνητικές, αρχεία συζήτησης γιατρού με τον ασθενή και IoT συσκευές [23]. Επίσης τα παραδοσιακά ιατρικά αρχεία είναι στο χαρτί και είναι κουραστική η

παρακολούθηση της χρονικής εξέλιξης της κατάστασης της υγείας του ασθενούς [84]. Επιπλέον, είναι επιρρεπή σε λανθασμένα δεδομένα, γεγονός που οδηγεί μερικές φορές στην κακομεταχείριση των ασθενών. Η τεχνολογία πληροφοριών δίνει την ευκαιρία να μειωθεί η προσπάθεια αυτή με την καθιέρωση των EHRs.

Ο Lee [85] ανέφερε δύο κατευθύνσεις των EHRs (δηλαδή των μεγάλων δεδομένων υγειονομικής περίθαλψης, big data) που είναι α) EMR (electronic medical records) και β) δεδομένα αισθητήρων (sensor data) από διάφορες συσκευές.



Εικόνα 3.4: EMR [23]



Εικόνα 3.5: δεδομένα αισθητήρων [23]

Δεδομένου ότι υπάρχουν εκατομμύρια τύποι ιατρικών δεδομένων υπάρχει η ανάγκη για ταξινόμησή τους.

Τα EMRs είναι ένας κατάλογος πληροφοριών που συλλέγονται από τα ιατρικά ιδρύματα, από την έναρξη της θεραπείας έως τη θεραπεία της νόσου. Πρόκειται για μια σειρά από χρονικές πληροφορίες (time-specific information) που έχουν καταγραφεί από τα νοσοκομεία (Εικόνα 3.4).

Ο ευρέως χρησιμοποιούμενος εξοπλισμός IoT είναι τα : κινητά, φορητές συσκευές, μικρόφωνα, CCTV, αισθητήρες περιβάλλοντος, ενσωματωμένοι αισθητήρες δέρματος, έξυπνα ρολόγια. Οι προαναφερθείσες συσκευές συλλέγουν πληροφορίες με σκοπό την παρακολούθηση διαφόρων τμημάτων του σώματος ή διαφόρων λειτουργιών των ασθενών. Οι διάφοροι αισθητήρες συλλέγουν τα sensor data (Εικόνα 3.5).

Τελικά, οι προαναφερθείσες πηγές παράγουν συνολικά το τεράστιο ποσό των healthcare big data, τα οποία αυξάνονται με αστρονομικό ρυθμό. Η έρευνα του Stanford Medicine [86] αναφέρει : «153 exabytes data δημιουργήθηκαν το 2013, όπου το αναμενόμενο ποσό για το 2020 είναι 2314 exabytes» . Ωστόσο, με τον ετήσιο ρυθμό αύξησης 48% , αναμένεται να δημιουργηθεί το yottabyte εύρος [23].

Μια ακόμη έρευνα αναφέρει ότι οι βιομηχανίες ανάλυσης της υγειονομικής περίθαλψης αναπτύσσονται με εκθετικό ρυθμό, με ετήσια ανάπτυξη CAGR 27,3% (compound annual growth rate) και αυτό αναμένεται να φτάσει τα 29,84 δισεκατομμύρια δολάρια μέχρι το 2022 από τα 8,92 δισεκατομμύρια δολάρια το 2017 [87].

(1 exabyte = 1 δισεκατομμύριο gigabytes και 1 yottabyte=1000⁸ bytes)

Η εξόρυξη των δεδομένων υγειονομικής περίθαλψης (healthcare data mining) και τα μεγάλα δεδομένα (big data) είναι στενά συνδεδεμένα, καθώς η εξαγωγή ενός σχεδίου από τα EHRs μπορεί να βοηθήσει τους γιατρούς στη μελλοντική πρόβλεψη ασθενειών [23]. Επίσης, η ηλεκτρονική πρόσβαση στα αρχεία υγείας, επιτρέπει στο γιατρό να εφαρμόσει πρακτικές για τη σημαντική βελτίωση της ποιότητας της θεραπείας [88]. Επιπλέον, το EHR α) επιτρέπει καλύτερη διαχείριση της ασθένειας, β) αύξησε τα επίπεδα προληπτικής φροντίδας, γ) παρέχει καλύτερες λειτουργίες υποστήριξης αποφάσεων, δ) αύξησε τη συνεργασία μεταξύ των φροντιστών. Επομένως, υπάρχει αυξημένη αναγνώριση του ρόλου του στην κοινότητα της υγειονομικής περίθαλψης [89].

Αξίζει να αναφερθούμε σε ένα παράδειγμα. Η σχέση μεταξύ της Νόσου Πάρκινσον με το βάδισμα αναλύθηκε σαφώς χρησιμοποιώντας την προσέγγιση text mining [90]. Η σύνδεση μεταξύ της νόσου και των υγιών ηλικιωμένων/ενηλίκων αναλύθηκε χρησιμοποιώντας τεχνικές machine learning βασισμένες στο πρότυπο που δημιουργήθηκε, χρησιμοποιώντας τα χαρακτηριστικά βάδισης [91]. Τα δεδομένα βάδισης για τη Νόσο Πάρκινσον μετρήθηκαν χρησιμοποιώντας φορητούς αισθητήρες και χρησιμοποιούνται για την ανάπτυξη ενός διαγνωστικού εργαλείου για την αξιολόγηση των ασθενών με PD (Parkinson Disease) [92].

Πολλές ερευνητικές εργασίες αναπτύχθηκαν για να σχεδιάσουν την τεχνολογία blockchain προκειμένου να διασφαλιστούν, να μοιραστούν και να αποθηκευτούν τα δεδομένα των EHRs, τόσο εντός όσο και μεταξύ των ιδρυμάτων.

3.2) Supply Chain Management (SCM) apps :

Το SCM έχει σχεδιαστεί ώστε να περιλαμβάνει τις βέλτιστες πρακτικές για το σύνολο των διαδικασιών παράδοσης από την παραγγελία έως την προμήθεια [93]. Το SCM αποτελεί προκλητική προοπτική για την Υγεία. Με τα διάσπαρτα σύνολα παραγγελιών για ιατρικά εφόδια, φάρμακα και κρίσιμους πόρους, υπάρχει κίνδυνος να υπονομευθεί η διαδικασία της εφοδιαστικής αλυσίδας, με αποτέλεσμα να επηρεάσει άμεσα την ασφάλεια των ασθενών [94]. Σύμφωνα με μια μελέτη του Π.Ο.Υ. περισσότεροι από 100.000 άνθρωποι πεθαίνουν στην Αφρική εξαιτίας ακατάλληλης δοσολογίας από παραποιημένα φάρμακα που παραγγέλθηκαν από μη αξιόπιστους ή αγνώστους προμηθευτές. Εκτός από την παραποίηση προϊόντων και φαρμάκων, η έλλειψη μητρώου προϊόντων και τα σφάλματα στη συσκευασία σε μια μονάδα υγειονομικής περίθαλψης, μπορεί να διαταράξουν ολόκληρο το SCM [95].

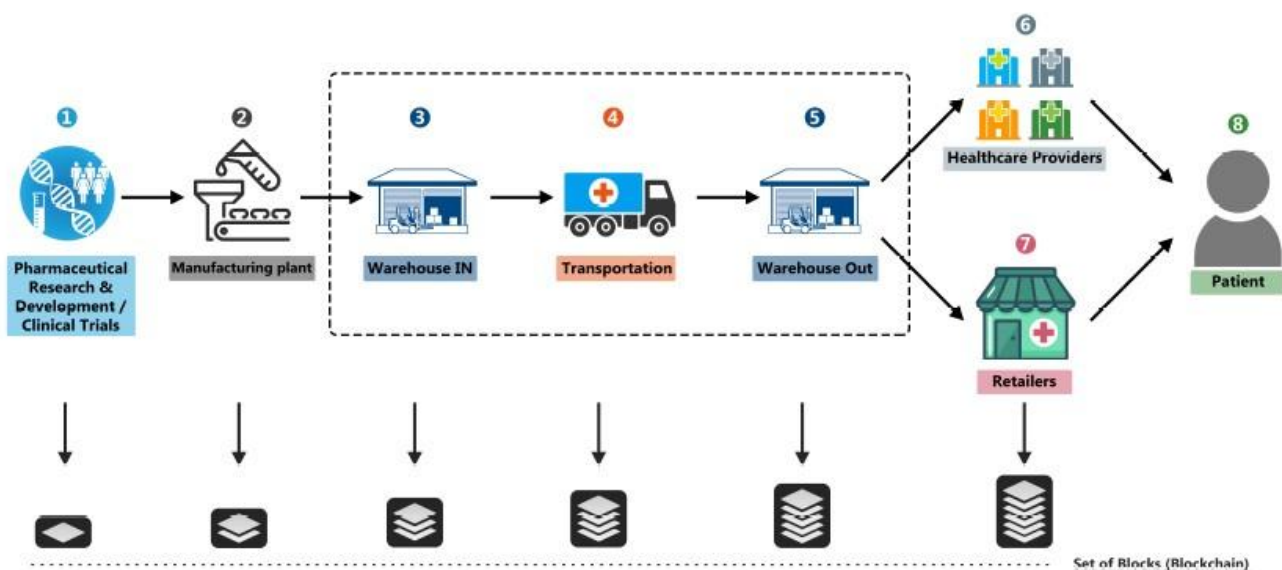
Το blockchain μπορεί να χαρακτηριστεί ως η βασική τεχνολογία παρακολούθησης για την αξιοποίηση ολόκληρης της πορείας των μετακινήσεων των φαρμάκων και των ιατρικών προϊόντων [96]. Δεδομένου ότι όλες οι συναλλαγές καταγράφονται στο ledger και κάθε κόμβος

διατηρεί ένα αρχείο της συναλλαγής, είναι εύκολο να επιβεβαιωθεί η προέλευση του φαρμάκου, ο πωλητής και ο διανομέας, αμέσως. Επιπλέον, το κατακευματισμένο ledger, επιτρέπει στους υπαλλήλους της υγειονομικής περίθαλψης και στο γιατρό να ελέγξουν και να πιστοποιήσουν τα διαπιστευτήρια των προμηθευτών [97].

Με καλύτερη κατανόηση της Supply Chain μέσω κατάλληλης και έγκαιρης διαδικασίας ταυτοποίησης, τα φαρμακεία και οι πάροχοι υγειονομικής περίθαλψης θα είναι σε θέση να διασφαλίσουν ότι η ροή των αυθεντικών φαρμάκων συνεχίζει να φτάνει στους ασθενείς που το χρειάζονται περισσότερο. Από αυτή την άποψη, η τεχνολογία blockchain κρατά μια μεγάλη υπόσχεση για τη δημιουργία ενός αξιόπιστου δικτύου προμηθευτών που θα επιτρέπουν στους διαχειριστές της υγειονομικής περίθαλψης να προστατεύουν τους ασθενείς από τους αναξιόπιστους προμηθευτές.

Η τεχνολογία blockchain υπόσχεται σημαντική βελτίωση στους τομείς: προέλευση δεδομένων, πρόληψη απάτης, συναλλαγές, πρόβλεψη της ζήτησης.

Στην παρακάτω εικόνα θα δούμε τα 8 στάδια της ροής εργασιών στη διαχείριση της εφοδιαστικής αλυσίδας της υγειονομικής περίθαλψης στο blockchain.



Εικόνα 3.6: Διαχείριση της εφοδιαστικής αλυσίδας στο blockchain [74]

Βήμα 1:

Ένα νέο block δημιουργείται κατά την εφεύρεση ενός νέου φαρμάκου ή μιας νέας φαρμακευτικής θεραπείας. Το νέο block περιλαμβάνει την προστασία των ευρεσιτεχνιών (patent protection) και μια μακρά διαδικασία κλινικών δοκιμών (clinical trials). Αυτές οι πληροφορίες καταγράφονται στο ψηφιακό ledger ως μια μορφή συναλλαγής.

Βήμα 2:

Όταν ολοκληρωθεί με επιτυχία μια κλινική δοκιμή, η ευρεσιτεχνία αποστέλλεται στη μονάδα παραγωγής για πρωτότυπη δοκιμή (test prototype) και μαζική παραγωγή. Κάθε προϊόν έχει τη δική του μοναδική ταυτότητα, που είναι ενσωματωμένη με μια άλλη συναλλαγή ή block στο blockchain, συμπεριλαμβανομένων άλλων σχετικών πληροφοριών.

Βήμα 3:

Μόλις ολοκληρωθεί η μαζική παραγωγή μαζί με την ευρεσιτεχνία, το φάρμακο συγκεντρώνεται σε μια αποθήκη (warehouse) για μελλοντική διανομή. Πληροφορίες όπως, ώρα, παρτίδα, κωδικός, ημ/νία λήξης, συμπεριλαμβάνονται στο blockchain.

Βήμα 4:

Οι πληροφορίες μεταφοράς περιλαμβάνονται επίσης στο blockchain, το οποίο μπορεί να περιλαμβάνει το χρόνο από μια αποθήκη σε άλλη (warehouse IN), τον τρόπο μεταφοράς, τον εξουσιοδοτημένο αντιπρόσωπο και άλλες πληροφορίες.

Βήμα 5:

Ένα τρίτο δίκτυο διανομής είναι συνήθως υπεύθυνο για τη διανομή φαρμάκων και ιατρικών προμηθειών στους παρόχους υγειονομικής περίθαλψης. Μια αποθήκη (warehouse OUT) χρησιμοποιείται για κάθε τρίτο μέρος για το σκοπό αυτό, με το οποίο συνδέονται όλα τα τελικά σημεία διανομής. Μια ακόμη συναλλαγή προστίθεται στο blockchain.

Βήμα 6:

Οι πάροχοι υπηρεσιών φροντίδας, όπως νοσοκομεία και κλινικές, πρέπει να παρέχουν πληροφορίες, όπως το σύνολο παραγωγής, τον αριθμό παρτίδας, τον ιδιοκτήτη του προϊόντος, την ημ/νία λήξης για τον έλεγχο αυθεντικοποίησης και την αποτροπή της παραποίησης. Αυτά περιλαμβάνονται επίσης στο blockchain.

Βήμα 7:

Οι ενέργειες του εμπορίου λιανικής (retailers) είναι παρόμοιες με αυτές των παρόχων υγειονομικής περίθαλψης, όπως περιγράφηκαν στο Βήμα 6.

Βήμα 8:

Οι ασθενείς ενθαρρύνονται στο να μπορούν να προσδιορίσουν τη γνησιότητα καθ'όλη τη διαδικασία, καθώς το SCM blockchain προσφέρει διαφανείς πληροφορίες για επαλήθευση στους πιθανούς αγοραστές.

3.2.1) Κλινικές δοκιμές (clinical trials)

Οι κλινικές δοκιμές στην υγειονομική περίθαλψη αντιμετωπίζουν πολλές προκλήσεις , συμπεριλαμβανομένων της ανταλλαγής δεδομένων (data sharing), της προστασίας δεδομένων (data privacy) και της εγγραφής ασθενών (patient enrolment) [98].

Η τεχνολογία blockchain έχει τη δυνατότητα να αντιμετωπίσει αυτές τις προκλήσεις. Παρέχει μοντέλα δεδομένων από κλινικές δοκιμές που επιτρέπουν τη διαφάνεια και την αναπαραγωγικότητα [99].

3.2.2) Φαρμακευτική (pharmaceutical)

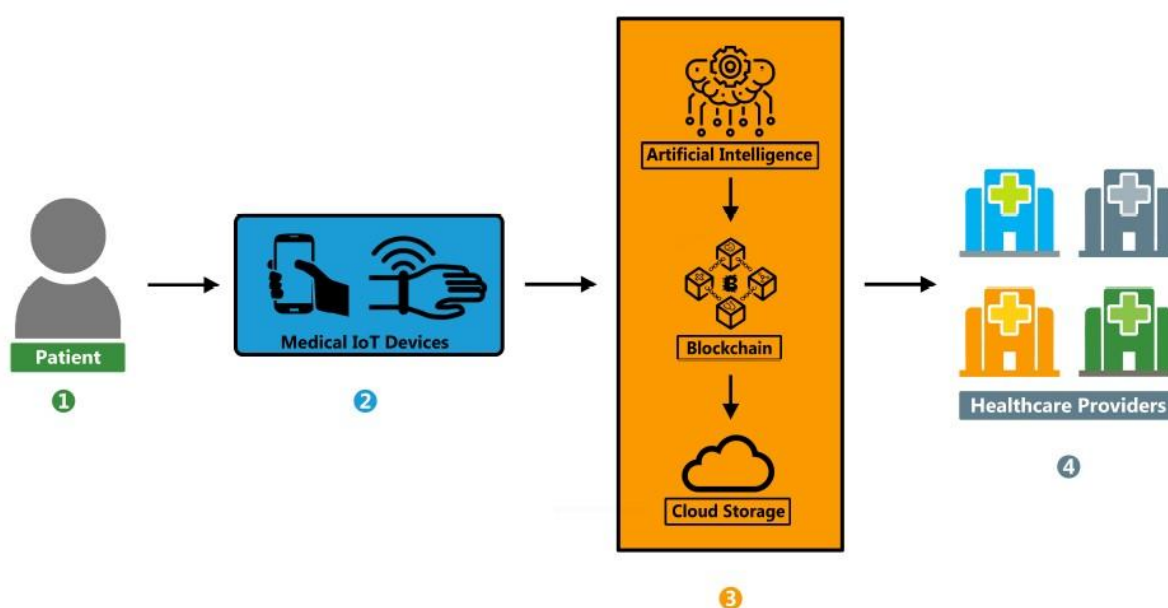
Οι φαρμακευτικές εταιρείες προσπαθούν αδιάκοπα να βελτιώσουν την ποιότητα των φαρμάκων καθώς και να εφεύρουν νέα φάρμακα για τις διάφορες ασθένειες. Για το κάθε φάρμακο απαιτείται μια μακρά διαδικασία για να διασφαλιστούν : α) προστασία της ευρεσιτεχνίας (patent protection) , β) ασφάλεια, γ) αποτελεσματικότητα, δ) στατιστική εγκυρότητα , ε) έγκριση από ρυθμιστικές αρχές. Κανονικά, αυτή η διαδικασία διαρκεί πολλά χρόνια, ξεκινώντας από την ανακάλυψη έως την εμπορευματοποίηση, όπου οι κλινικές δοκιμές καταλαμβάνουν σημαντικό μέρος της διάρκειας [100]. Κατά συνέπεια, αυτή η μακρά διαδικασία είναι ευάλωτη στην ανάκληση και την απομίμηση των φαρμάκων λόγω έλλειψης ασφάλειας (security) και προστασίας της ιδιωτικής ζωής (privacy) [101]. Αυτό το εμπόδιο θα μπορούσε να εξαλειφθεί με τη χρήση της τεχνολογίας blockchain καθ'όλη τη διάρκεια της φαρμακευτικής διαδικασίας.

Θα μπορούσαμε να διασφαλίσουμε το security και να διατηρήσουμε το privacy , χρησιμοποιώντας blockchain distributed ledger (κατανεμημένο ημερολόγιο blockchain) , εξασφαλίζοντας ότι κάθε δοκιμή καταγράφεται στους κόμβους , το οποίο δηλώνει ανθεκτικότητα στις παραβιάσεις (tamper- proof). Ένα ιδιωτικό blockchain θα μπορούσε να χρησιμοποιηθεί για να εξασφαλίσει ότι όλα τα φαρμακευτικά προϊόντα τηρούν την προστασία της ευρεσιτεχνίας. Αυτό μπορεί να γίνει χρησιμοποιώντας ένα έξυπνο συμβόλαιο , το οποίο παρέχει ακεραιότητα, ανιχνευσιμότητα και διαφάνεια [102].

Σύμφωνα με μια πρόσφατη μελέτη [103], περίπου το 60% των φαρμακευτικών εταιρειών είτε εργάζονται, είτε πειραματίζονται με το blockchain, το οποίο αντανάκλα τις δυνατότητές του σε μια τόσο μεγάλη βιομηχανία. Τα παραπονημένα φάρμακα αποτελούν πρόκληση, καθώς πρόκειται για ένα παγκόσμιο πρόβλημα με εξαιρετικούς κινδύνους για το ευρύ κοινό και τους καταναλωτές [59].

3.3) Internet of Medical Things (IoMT) apps:

Τα IoMT συστήματα διαδραματίζουν ζωτικό ρόλο στην ανάπτυξη των πληροφοριακών συστημάτων υγείας και ιατρικής [104]. Με την τεχνολογία IoMT και τον εξοπλισμό της υγειονομικής περίθαλψης (heart monitor, body scanners, wearable devices) μπορούν να συλλέγονται, να επεξεργάζονται και να μοιράζονται δεδομένα μέσω του Διαδικτύου σε πραγματικό χρόνο. Με την πρόοδο της AI, οι πάροχοι υγειονομικής περίθαλψης με τη χρήση του IoMT προτύπου, μπορούν να: α) καταγράψουν μια εικόνα, β) να προσδιορίσουν κακοήθη ύποπτα μέρη, γ) μοιράζονται αυτές τις γνώσεις με εκείνους που έχουν δικαίωμα πρόσβασης στις πληροφορίες.



Εικόνα 3.7: Internet of medical things (IoMT) στο blockchain [74].

Βήμα 1:

Στον τομέα του IoMT ο ασθενής είναι η πηγή των δεδομένων.

Βήμα 2:

Οι “medical IoT devices”, συνήθως συνδέονται απομακρυσμένα (κινητό) ή στενά (βραχιόλι) για την παρακολούθηση του σώματος των ασθενών και δημιουργούν κατά συνέπεια μεγάλο όγκο δεδομένων.

Βήμα 3:

Τα δεδομένα που δημιουργούνται στο Βήμα 2, αποθηκεύονται στα blocks ή σε Cloud αποθετήριο. Η AI θα βοηθήσει το blockchain να δημιουργήσει “ευφυείς εικονικούς πράκτορες”, οι οποίοι με τη σειρά τους θα δημιουργήσουν αυτόματα νέα ledgers. Στην περίπτωση των ευαίσθητων ιατρικών δεδομένων (Sensitive Medical Data), όπου η ασφάλεια είναι πρώτη προτεραιότητα, θα

μπορούσε το αποκεντρωμένο AI σύστημα να βοηθήσει το blockchain να φτάσει την υψηλότερη ασφάλεια [105].

Βήμα 4:

Οι πάροχοι υγειονομικής περίθαλψης είναι οι τελικοί χρήστες , οι οποίοι αναζητούν πρόσβαση σε μια ασφαλή και υγιή παράδοση φροντίδας , η οποία επιτρέπεται από τον ιδιοκτήτη.

3.3.1) IoT στην Υγειονομική περίθαλψη και Ιατρικές συσκευές (Healthcare IoT and Medical devices)

Το IoT είναι μια ένωση υπολογιστικών συσκευών με μοναδικά αναγνωριστικά, ικανά να μεταφέρουν δεδομένα μέσω δικτύου, χρησιμοποιώντας το Internet Protocol, χωρίς να υπάρχει αλληλεπίδραση μεταξύ ανθρώπου και μηχανής. Αυτού του είδους αλληλεπίδραση , ισχυρή και αδιάλειπτη, καθιστά το Internet κρίσιμο παράγοντα στο σύστημα της υγειονομικής περίθαλψης [106].

Οι φορητές και οι ιατρικές συσκευές (wearable and medical devices) βρίσκονται στην καρδιά του IoMT [107]. Ένα σημαντικό συστατικό του IoMT στη βιομηχανία της υγειονομικής περίθαλψης , είναι τα συστήματα WBAN (wireless body-area network). Τα WBAN είναι μια σημαντική τεχνολογία που επιτρέπει ευρεία ποικιλία εφαρμογών, ειδικά σε ιατρικά και υγειονομικά περιβάλλοντα για “απομακρυσμένη παρακολούθηση” (*remote monitoring*) των φυσιολογικών παραμέτρων [108]. Οι χρήστες μπορούν να χρησιμοποιούν τις IoT συσκευές τους για υπενθύμιση των ραντεβού, κάψιμο θερμίδων, μεταβολές στην αρτηριακή πίεση και πολλά ακόμη [109]. Παρακάτω θα κάνουμε μια ανασκόπηση κάποιων μελετών για την ενσωμάτωση του blockchain με το IoMT :

3.3.2) Υποδομή των IoT στην Υγειονομική περίθαλψη και Ασφάλεια των δεδομένων (Healthcare IoT Infrastructure and Data Security)

Η υποδομή των τεχνολογιών πληροφορικής και επικοινωνιών στον τομέα της υγειονομικής περίθαλψης (ICT = Information and Communication Technology) , αποτελείται από πολλά δίκτυα και IoT συσκευές, συμπεριλαμβανομένων των : αισθητήρων , τερματικών , διαγνωστικών εργαλείων και σημείων ασύρματης πρόσβασης. Αυτή η υποδομή επιτρέπει σε πολλά συστήματα υγειονομικής περίθαλψης , όπως φορητές συσκευές (wearable devices) και υπηρεσίες απομακρυσμένης παρακολούθησης (*remote monitoring services*) , τη μετάδοση και ανταλλαγή των δεδομένων μεταξύ των ασθενών και των φροντιστών τους.

Κατά τη διάρκεια της διαδικασίας μετάδοσης , τα δεδομένα διαβιβάζονται μέσω αγνώστων δικτύων επικοινωνίας (wide area networks) , τα οποία ενδέχεται να είναι ευάλωτα σε παραβιάσεις ασφαλείας και ιδιωτικότητας (security and privacy).

Πράγματι, υπάρχουν πολλές περιπτώσεις όπου κακόβουλοι χρήστες προσπαθούν αδιάκοπα να ανακαλύψουν οποιαδήποτε αδυναμία για να διεισδύσουν στο δίκτυο υγειονομικής περίθαλψης και να θέσουν σε κίνδυνο πολύτιμες πληροφορίες των υπηρεσιών των παρόχων. Ένα παράδειγμα είναι αυτό που συμβαίνει στη Βόρεια Καρολίνα. Στο Catwaba Valley Medical Center , 3 Phishing επιθέσεις επιβαρύνουν την παραβίαση των προσωπικών δεδομένων 20.000 ασθενών [110].

Προκειμένου να αντιμετωπιστούν οι προαναφερθείσες προκλήσεις ασφαλείας στην ΙοΤ υγειονομική περίθαλψη , οι ερευνητές διευρύνουν διάφορες τεχνικές για την προστασία των δεδομένων των χρηστών από την παράνομη εισχώρηση στο δίκτυο.

3.3.3) Τεχνητή Νοημοσύνη (Artificial Intelligence)

Οι τεχνολογίες blockchain γίνονται ολοένα πιο δυνατές και ισχυρές , καθώς συνδυάζονται με ΑΙ σε διάφορες λύσεις στον τομέα της υγειονομικής περίθαλψης . Ο τομέας της ΑΙ βελτιώνεται ολοένα και περισσότερο με την πρόοδο της αυτοματοποίησης, καθώς δύο βασικά συστατικά του είναι τα α) Machine Learning και β) Deep Learning.

Όσο περισσότερα δεδομένα δίνουμε στη μηχανή, τόσο περισσότερη θα είναι η ικανότητα που θα αποκτήσει η μηχανή στην ταξινόμηση (classify) ή στην πρόβλεψη (predict) των σχεδίων με ακρίβεια [111].

3.4) Απομακρυσμένη παρακολούθηση ασθενών (remote patient monitoring)

Η γρήγορη ανάπτυξη των συσκευών ΙοΤ και της φορητής τεχνολογίας, άνοιξε νέες δυνατότητες στον τομέα των ιατρικών αισθητήρων, ιδιαίτερα για την απομακρυσμένη παρακολούθηση των ασθενών. Το υποσύνολο αυτής της τάσης για την ΙοΤ υγειονομική παρακολούθηση είναι το WBAN (Wireless Body Area Networks) . Σε ένα WBAN, ο ασθενής είναι εξοπλισμένος με διάφορες φορητές ή εμφυτευμένες ιατρικές συσκευές, που λαμβάνουν μετρήσεις σε πραγματικό χρόνο, για ζωτικούς δείκτες, όπως είναι οι καρδιακοί παλμοί ή τα επίπεδα γλυκόζης. Άλλες συσκευές μπορεί να λειτουργήσουν ως ενεργοποιητές, οι οποίοι μπορούν να παρέχουν αυτόματη επεξεργασία, βασισμένη στις μετρήσεις που λαμβάνουν οι αισθητήρες. Όλες οι WBAN συσκευές του ασθενούς αναφέρουν σε μια κύρια συσκευή (κινητό τηλέφωνο), η οποία μεταδίδει τα δεδομένα που συλλέγονται στους παρόχους υγειονομικής περίθαλψης. Η μέθοδος της απομακρυσμένης παρακολούθησης μειώνει την ανάγκη για χρονοβόρα ραντεβού με το γιατρό και αφήνει περισσότερο ελεύθερο χρόνο στους ασθενείς.

Η δημοτικότητα της εξ’αποστάσεως παρακολούθησης αυξάνεται ραγδαία, καθώς το 2016, 7.1 εκατομμύρια ασθενείς σε όλο τον κόσμο χρησιμοποίησαν την απομακρυσμένη παρακολούθηση και ο αριθμός προβλέπεται να φτάσει τα 50.2 εκατομμύρια μέχρι το 2021 [112]. Στις ΗΠΑ, από την 1/1/2018, τα κέντρα υγειονομικής περίθαλψης, “US Centers for Medicare and Medicaid Services”, χρηματοδοτούν την προώθηση των συσκευών, για την παρακολούθηση σε πραγματικό χρόνο [113].

Παρά την όλη αύξηση της δημοτικότητας της απομακρυσμένης παρακολούθησης, υπάρχουν ανησυχίες που αφορούν στην *αποτελεσματική* και *ασφαλή* μετάδοση των ιατρικών δεδομένων. Οι μετρήσεις που συλλέγονται από τους αισθητήρες, πρέπει να συγκεντρωθούν, να διαμορφωθούν και να υποβληθούν σε επεξεργασία. Τα δεδομένα της υγειονομικής περίθαλψης είναι ένας επικερδής στόχος για τους κακόβουλους χρήστες (χάκερς) και για αυτό υπάρχει ισχυρό κίνητρο για τη διασφάλιση της μετάδοσης των πληροφοριών με σκοπό την προστασία της υγείας. Συνεπώς, οι προκλήσεις έχουν ως εξής :

- διατήρηση της προστασίας της ιδιωτικής ζωής των ασθενών
- εύκολα διαχειρίσιμα EHRs
- προστασία της ακεραιότητας της φροντίδας του ασθενούς
- διατήρηση χρονοδιαγράμματος ακριβείας για όλα τα γεγονότα.

Για την αντιμετώπιση αυτών των προκλήσεων προτείνεται η ενσωμάτωση των συστημάτων *WBAN με Smart Contracts*, σε ένα *private/consortium-led blockchain*, προκειμένου να παρέχεται μια υπηρεσία κατανεμημένης επεξεργασίας δεδομένων, που δημιουργεί ένα αμετάβλητο αρχείο συναλλαγών μεταξύ των συσκευών WBAN και των παρόχων υγειονομικής περίθαλψης [114].

Τα Smart Contracts χρησιμοποιούνται για τη διευκόλυνση της αυτόματης ανάλυσης των δεδομένων υγείας που συλλέγονται από τις συσκευές WBAN, με βάση τις οριακές τιμές κάθε ασθενούς και είναι δομημένα και προσαρμοσμένα για κάθε ασθενή και τις συσκευές του. Ο γιατρός μπορεί να λάβει ειδοποιήσεις για οποιαδήποτε ασυνήθιστη δραστηριότητα. Η δομή των έξυπνων συμβολαίων θα κλιμακωθεί, με όλες τις κύριες συσκευές που καλούν το ίδιο αρχικό smart contract, το οποίο με τη σειρά του θα καλέσει τη σχετική υπο-σύμβαση (sub-contract) για τη συσκευή του συγκεκριμένου ασθενούς και θα της διαβιβάσει τα δεδομένα εισόδου (input data) και τις προσαρμοσμένες τιμές. Αυτή η ατομική σύμβαση θα αναλύσει τα δεδομένα, σύμφωνα με τις οριακές τιμές και στη συνέχεια θα εκδώσει όλες τις απαραίτητες ειδοποιήσεις για τη θεραπευτική αγωγή με βάση τα πορίσματά της. Μια σύμβαση δεν μπορεί να επεξεργαστεί μετά την ανάπτυξή της, αλλά μπορεί να «θανατωθεί» και να εκδοθεί μια νέα σύμβαση έτσι ώστε να διευκολυνθεί η αντικατάσταση της επαφής μιας συσκευής χωρίς να επηρεαστεί η λειτουργία των υπολοίπων [114].

Το μόνιμο αρχείο καταγραφής των μεταδόσεων (ledger) από και προς έναν κόμβο WBAN χρησιμοποιείται για την παρακολούθηση των metadata σχετικά με τις μετρήσεις και τις εντολές θεραπείας που εκδίδονται [114].

Το private/consortium-led blockchain χρησιμοποιείται λόγω του κόστους και της αυξημένης ιδιωτικότητας για τα PHI. Μόνο οι εξουσιοδοτημένοι φορείς μπορούν να έχουν πρόσβαση στο blockchain για ανάγνωση, επιθεώρηση και επαλήθευση του κάθε block, σε αντίθεση με το

δημόσιο blockchain , όπως είναι το Bitcoin. Κάθε εξουσιοδοτημένος χρήστης θα έχει δικό του ανώνυμο λογαριασμό και θα μπορεί να εντοπιστεί μόνο με τη δική του διακριτική ευχέρεια. Επίσης, μόνο ορισμένοι κόμβοι μπορούν να εκτελέσουν smart contracts και να επαληθεύσουν νέα blocks . Σε αυτού του τύπου blockchain, ένα σύνολο προ-εγκεκριμένων μελών λειτουργεί τους κόμβους και ένα έγκυρο block πρέπει να περιέχει υπογραφές από τουλάχιστον 10-15 κόμβους. Χρησιμοποιώντας προ-εγκεκριμένους κόμβους επαλήθευσης, εξασφαλίζεται ότι κανένας αδίστακτος κόμβος δεν μπορεί να συνεννοηθεί για να εισαγάγει ψευδείς συναλλαγές στην αλυσίδα, καθώς και να εξαλείψει την ανάγκη πληρωμής του νομίσματος για τη διαδικασία εξόρυξης (mining) για το πρωτόκολλο Proof-of-work. Αντιθέτως πρωτόκολλο όπως το PBFT, μπορούν να χρησιμοποιηθούν για την επίτευξη συναίνεσης, καθώς οι κόμβοι που συμμετέχουν είναι γνωστοί και υπόκεινται σε έλεγχο [114].

Η ασφαλής απομακρυσμένη παρακολούθηση παρέχει στους επαγγελματίες του ιατρικού κλάδου να λαμβάνουν ειδοποιήσεις σχετικά με τους ασθενείς τους σε πραγματικό χρόνο, διευκολύνοντας έτσι την Precision Medicine.

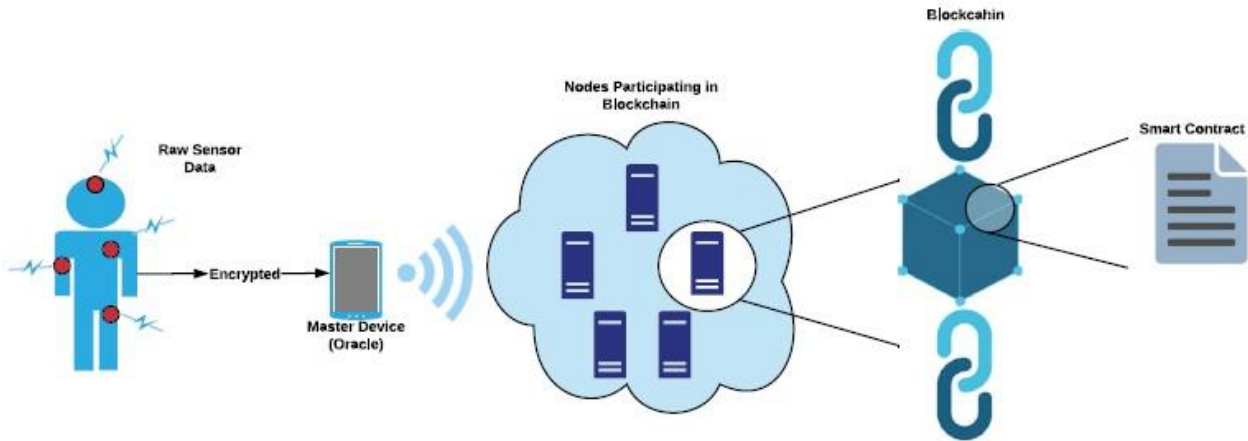
Παρακάτω θα δούμε το βασικό σχεδιασμό του συστήματος αυτού σε εικόνες και με περισσότερη ανάλυση. Για έξυπνη συσκευή Smartphone/tablet (Εικόνα 3.8) και για έξυπνη συσκευή Oracle (Εικόνα 3.9).

3.4.1) Περιγραφή του συστήματος :

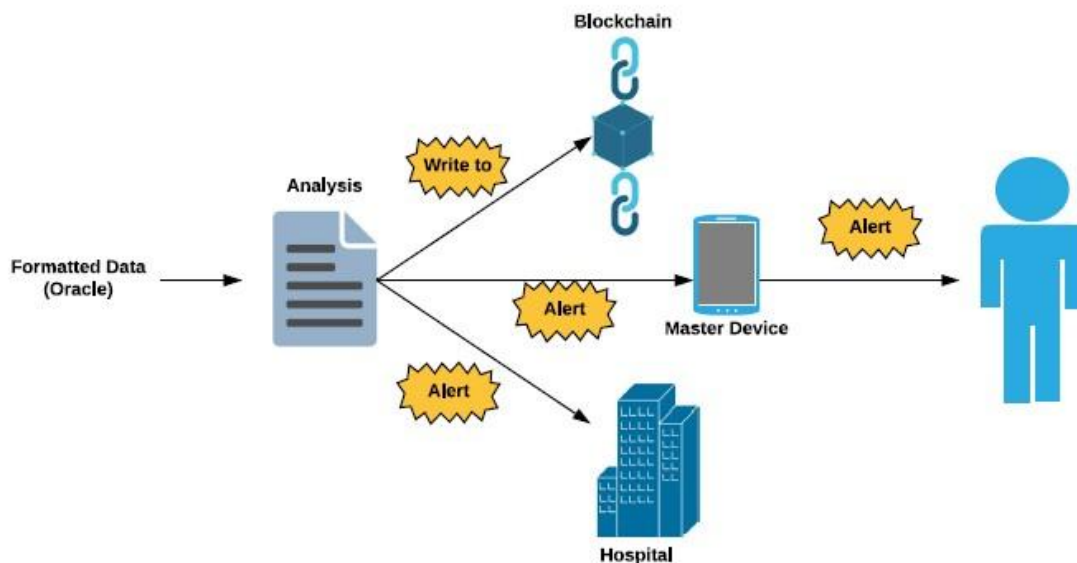
- Ο ασθενής παρακολουθείται εξ'αποστάσεως από το γιατρό και είναι εφοδιασμένος με διάφορα ιατρικά βοηθήματα, όπως μια συσκευή παρακολούθησης της πίεσης ή των επιπέδων ινσουλίνης.
- Τα ακατέργαστα δεδομένα (raw data), αποστέλλονται σε μια «έξυπνη συσκευή», (Smartphone ή tablet) , για συσσωμάτωση και μορφοποίηση από την εφαρμογή.
- Αυτές οι μορφοποιημένες πληροφορίες αποστέλλονται στο «έξυπνο συμβόλαιο» , για πλήρη ανάλυση μαζί με τα προσαρμοσμένα όρια τιμών.
- Το «έξυπνο συμβόλαιο» αξιολογεί τα δεδομένα που έλαβε και εκδίδει ειδοποιήσεις τόσο στον ασθενή (μέσω της έξυπνης συσκευής) όσο και στον πάροχο υγειονομικής περίθαλψης, καθώς και αυτοματοποιημένες οδηγίες θεραπείας για τους ενεργούς κόμβους του blockchain, εάν είναι επιθυμητό.
- Στο πρωτόκολλο Ethereum , η Oracle είναι η «έξυπνη συσκευή» , η οποία επικοινωνεί απευθείας με τα έξυπνα συμβόλαια για την τροφοδότηση των πληροφοριών σε αυτά [115].

Καμία εμπιστευτική ιατρική πληροφορία δεν θα αποθηκευτεί στο blockchain ή στα έξυπνα συμβόλαια , λόγω της συμμόρφωσης με το HIPPA [114]. Στο blockchain ledger καταγράφεται μόνο το γεγονός ότι συνέβησαν αυτές οι ενέργειες. Οι ίδιες οι μετρήσεις προωθούνται σε μια αποθηκευτική βάση δεδομένων για EHR, ενώ στο blockchain θα αποθηκευτεί μόνο η συναλλαγή, δηλώνοντας ότι τα δεδομένα υποβλήθηκαν σε επιτυχή επεξεργασία. Το σύστημα θα ενσωματωθεί

με EHR APIs και θα στείλει τα δεδομένα καθώς και τη θεραπευτική αγωγή απευθείας στο EHR για αποθήκευση. Αυτές οι συναλλαγές στο blockchain μπορούν στη συνέχεια να συνδεθούν με το EHR, προκειμένου να εξακριβωθεί η αυθεντικότητα των δεδομένων στο ιατρικό ιστορικό του ασθενούς. Αυτός ο έλεγχος αυθεντικοποίησης συμβάλλει στην πρόληψη και την ανίχνευση των συναλλαγών [114].



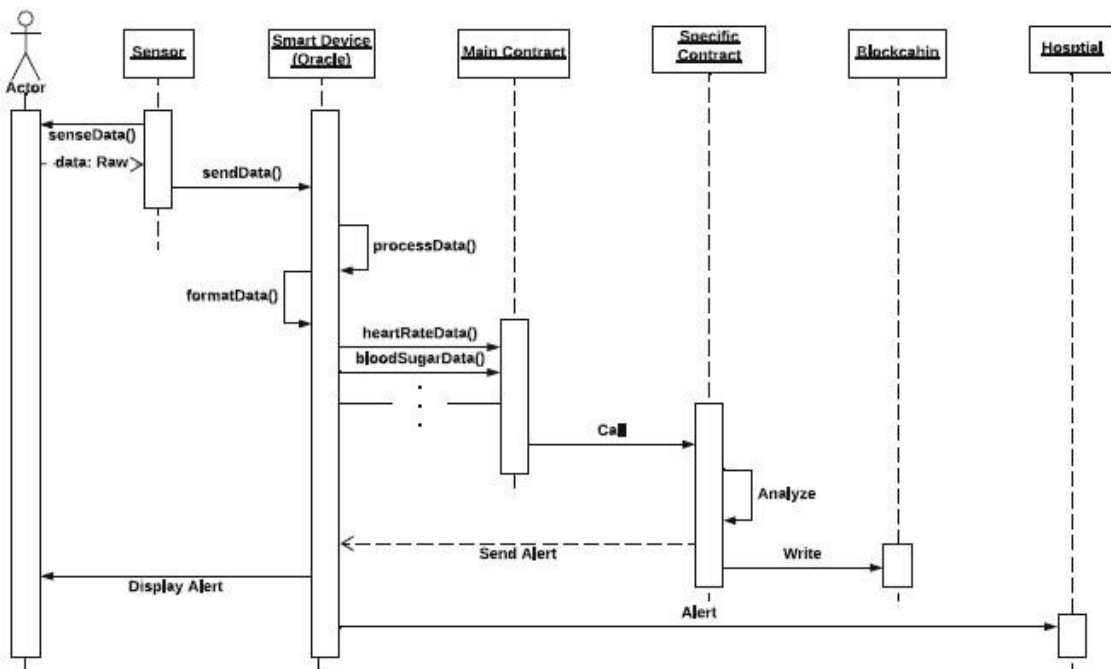
Εικόνα 3.8: Τα ακατέργαστα δεδομένα των αισθητήρων συγκεντρώνονται από τη κύρια συσκευή και έπειτα αποστέλλονται στους κόμβους του blockchain για επεξεργασία από το έξυπνο συμβόλαιο [114].



Εικόνα 3.9: Τα προσαρμοσμένα δεδομένα των έξυπνων συσκευών αποστέλλονται στα έξυπνα συμβόλαια, τα οποία επεξεργάζονται και εκτελούν τις απαραίτητες ενέργειες, με βάση τα αποτελέσματα και τις προκαθορισμένες παραμέτρους [114].

3.4.2) Ροή εκτέλεσης του συστήματος :

Πριν περάσουμε στην ανάλυση της ροής εκτέλεσης του συστήματος , θα αναφέρουμε κάποια στοιχεία για τα έξυπνα συμβόλαια. Τα έξυπνα συμβόλαια υλοποιήθηκαν χρησιμοποιώντας τη γλώσσα Ethereum Solidity. Δεν εκτελούμε τις λειτουργίες μας και τις έξυπνες συμβάσεις στο δημόσιο Ethereum blockchain, αλλά σε ένα ιδιωτικό blockchain, χρησιμοποιώντας το πρωτόκολλο Ethereum. Στη συνέχεια θα μελετήσουμε τη λογική ροή για τη χρήση των έξυπνων συμβολαίων.



Εικόνα 3.10: Η λογική ροή εκτέλεσης του συστήματος [114]

- Τα sensor data αποστέλλονται στην έξυπνη συσκευή (oracle).
- Η έξυπνη συσκευή εκτελεί τις λειτουργίες : ProcessData() και FormatData() , δηλαδή επεξεργασία και μορφοποίηση.
- Τα αποτελέσματα αποστέλλονται στην κύρια σύμβαση (main contract), η οποία στη συνέχεια διαβιβάζεται στην ειδική σύμβαση (specific contract) του ασθενούς για ανάλυση.
- Εάν τα measured data είναι εκτός των προκαθορισμένων οριακών τιμών, θα γίνει ενημέρωση των απαραίτητων ειδοποιήσεων και μια συναλλαγή θα εγγραφεί στο blockchain.

Ας εξετάσουμε ένα παράδειγμα με δεδομένα καρδιακού παλμού.

- Τα sensor data αποστέλλονται στην έξυπνη συσκευή (oracle).
- Η έξυπνη συσκευή θα καλέσει το κύριο έξυπνο συμβόλαιο (main smart contract) , το οποίο είναι το “HealthContractCaller” και θα ονομάσει τη συνάρτηση

“heartRateMonitor()”. Η έξυπνη συσκευή θα μεταβιβάσει τα δεδομένα και τις μέγιστες/ελάχιστες οριακές τιμές ως παραμέτρους.

- Η συνάρτηση heartRateMonitor() θα δημιουργήσει στη συνέχεια ένα νέο αντικείμενο heartRateMonitor() και θα περάσει τις ίδιες παραμέτρους στην συνάρτηση analyze().
- Οι δύο συγκεκριμένες υπο-συμβάσεις (specific sub-contract) θα αναλύσουν (analyze) τα εισερχόμενα δεδομένα και θα εκτελέσουν οι ίδιες τις απαραίτητες δράσεις απόκρισης, αντί να επιστρέψουν τον έλεγχο στην κύρια σύμβαση, η οποία λειτουργεί περισσότερο σαν ευρετήριο που συνδέει όλες τις συσκευές με τις αντίστοιχες υπο-συμβάσεις, για δομημένη και εύκολη συντήρηση.
- Αν η συνάρτηση analyze επιστρέψει κάποιον άλλο κωδικό, εκτός από το “OK”, η υπο-σύμβαση θα γράψει (write) αυτή τη συναλλαγή στο blockchain. Ο ίδιος κωδικός θα αποσταλεί (send alert) στην έξυπνη συσκευή, είτε για να ειδοποιήσει το χρήστη (alert), είτε για να ειδοποιήσει (alert) το νοσοκομείο ή να προβεί σε κάποια ενέργεια (carry out), π.χ. «δώστε φάρμακο για υψηλή αρτηριακή πίεση» ή «αντλήστε ινσουλίνη».

3.4.3) Ανάλυση του συστήματος και σύγκριση με το παραδοσιακό σύστημα:

	Παραδοσιακό σύστημα	Blockchain σύστημα
Εμπιστευτικότητα (confidentiality)	Κρυπτογραφημένη μετάδοση δεδομένων από άκρη σε άκρη σε μια καθορισμένη Β.Δ.	Ισοδύναμο επίπεδο ασφαλείας
Μη-μεταβλητότητα (immutability)	Οι Β.Δ. είναι ευπαθείς τόσο στις τυχαίες όσο και στις κακόβουλες παρεμβάσεις	Τα επιβεβαιωμένα blocks είναι αμετάβλητα και ανθεκτικά σε όλους τους τύπους χειραγώγησης.
Διαθεσιμότητα (availability)	Το αντίγραφο ασφαλείας των Β.Δ. πρέπει να γίνεται με χειροκίνητη διαχείριση και ο πλεονασμός πρέπει να θεσπιστεί για να εξασφαλιστεί η εξυπηρέτηση σε περίπτωση αποτυχίας	Παρέχεται υψηλότερη ανοχή σφάλματος και διαθεσιμότητα υπηρεσιών, καθώς όλοι οι κόμβοι έχουν ένα αντίγραφο του blockchain με κάθε καταγεγραμμένη συναλλαγή. Οι αποτυχίες ενός ή περισσότερων κόμβων μπορούν να αντιμετωπιστούν με αλγορίθμους PBFT.
Ιχνηλασιμότητα (traceability)	Τα αρχεία υγείας και καταγραφής μπορεί να αλλάξουν και η ανίχνευση μπορεί να μην είναι εγγυημένη.	Οι συναλλαγές μπορούν να εντοπιστούν από την προέλευση της δημιουργίας με εγγυημένη μη μεταβλητότητα και υπογράφονται από τους επαληθευτές.

Ταχύτητα (speed)	Οι συναλλαγές περιορίζονται μόνο από τις ταχύτητες μετάδοσης του δικτύου.	Μπορεί να υπάρξει αμελητέα καθυστέρηση ανάλογα με το χρονικό διάστημα που απαιτείται για την επαλήθευση ενός block.
Ιδιωτικότητα (privacy)	Οι μεταδόσεις προστατεύονται με κρυπτογράφηση για να αποκρύψουν τυχόν πληροφορίες ταυτοποίησης, οι οποίες μπορεί να εντοπιστούν ακόμα και στους τελικούς χρήστες.	Οι ανώνυμες διευθύνσεις προστατεύουν την ταυτότητα των ασθενών, επομένως δεν μπορούν να γίνουν συνδέσεις μεταξύ των ασθενών και των δεδομένων τους.
Διαφάνεια (transparency)	Οι ασθενείς δεν έχουν άμεσο έλεγχο στα δικά τους δεδομένα και δεν μπορούν να συσχετίσουν απομακρυσμένες συναλλαγές με τα αρχεία τους.	Οι ασθενείς είναι σε θέση να συνδέουν τις απομακρυσμένες ενέργειες παρακολούθησης απευθείας με τα ιατρικά τους αρχεία, διατηρώντας την ιδιωτικότητα και τον έλεγχο.

Πίνακας 3.1 : Ανάλυση του συστήματος blockchain και σύγκριση με το παραδοσιακό σύστημα [114]

3.5) Ιατρική Εκπαίδευση (medical education)

Τα παραδοσιακά συστήματα Ιατρικής Εκπαίδευσης είναι σε μεγάλο βαθμό centralized και περιορίζονται στα όρια των ακαδημαϊκών ιδρυμάτων. Η αποτελεσματικότητα και η παγκόσμια σκέψη δεν προωθούνται καθώς τα περισσότερα από τα ιδρύματα έχουν επικεντρωθεί στην εσωτερική οργάνωσή τους και είναι περιορισμένα στους δικούς τους θεσμικούς κανόνες και πλαίσια [117].

Η κύρια χρήση του blockchain μπορεί να θεωρηθεί ότι είναι ο μηχανισμός για την καταγραφή των συναλλαγών του ψηφιακού νομίσματος Bitcoin. Βέβαια, ο μηχανισμός αυτός θα μπορούσε να χρησιμοποιηθεί και στον εκπαιδευτικό τομέα, διότι η βάση της εκπαίδευσης είναι η συναλλαγή γνώσεων και δεξιοτήτων από πολλές πηγές και προϋποθέτει την αξιοπιστία όλων των εμπλεκομένων. Με την άνοδο των αποκεντρωμένων εφαρμογών DApps (Decentralized Applications), διερευνώνται τα πιθανά οφέλη αυτής της τεχνολογίας στην τριτοβάθμια εκπαίδευση. Με την αύξηση της εξ'αποστάσεως εκπαίδευσης, θεωρείται πρόκληση για τους ρυθμιστικούς οργανισμούς ο έλεγχος της μεταβολής της γνώσης στην Ιατρική Εκπαίδευση.

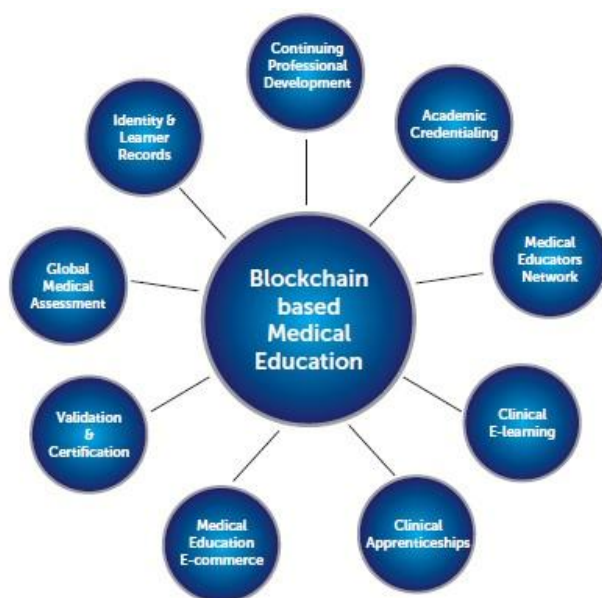
Η τεχνολογική εκπαίδευση των επαγγελματιών του τομέα υγείας θα μπορούσε να βελτιώσει την ποιότητα της εκπαίδευσης σε πολλές γενιές εκπαιδευομένων. Μπορεί επίσης να συμβάλει στην οικοδόμηση αξίας των εκπαιδευτικών παρεμβάσεων. Επιπλέον κάθε ίδρυμα που υιοθετεί την

τεχνολογία blockchain θα είναι σε θέση να παρέχει πιστοποίηση (certification) από μόνο του, στους σωστούς ανθρώπους, χωρίς την παρέμβαση τρίτων. Το blockchain θα μπορούσε επίσης να επηρεάσει τη διαχείριση των βιβλιοθηκών ιατρικής με πολλούς τρόπους, όπως συγκέντρωση, διατήρηση, ανταλλαγή έγκυρων πληροφοριών, με τη δημιουργία επαληθεύσιμων (verifiable) και χρονικά επισημασμένων (time-stamped) άρθρων, περιοδικών και εκδόσεων. Επίσης θα επιτρέπεται η εύκολη παρακολούθηση των πλέον χρησιμοποιούμενων και αποτελεσματικών ενοτήτων μάθησης [119]. Χρησιμοποιώντας το blockchain στην υγειονομική περίθαλψη, μπορούμε να εξασφαλίσουμε ότι η γνώση είναι ασφαλής και όχι αλλοιωμένη. Το blockchain μπορεί να εξαλείψει το αυξανόμενο πρόβλημα των πλαστών ακαδημαϊκών πιστοποιήσεων.

Για την Ιατρική Εκπαίδευση υπάρχουν εννέα κατηγορίες οι οποίες εφαρμόζονται σε φοιτητές ιατρικής, μεταπτυχιακούς γιατρούς και νοσοκόμες και στους παρεμφερείς κλάδους.

Οι εννέα αυτές κατηγορίες είναι :

- 1) Identity and learner records management
- 2) Funding, payment, educational e-commerce
- 3) Medical Meta-University – Medical Education without borders
- 4) Global medical assessment
- 5) Validation, Authentication, Certification
- 6) Learner credentialing
- 7) Clinical e-learning
- 8) Medical CPD (Continuing Professional Development)
- 9) Learning in clinical setting & clinical apprenticeships



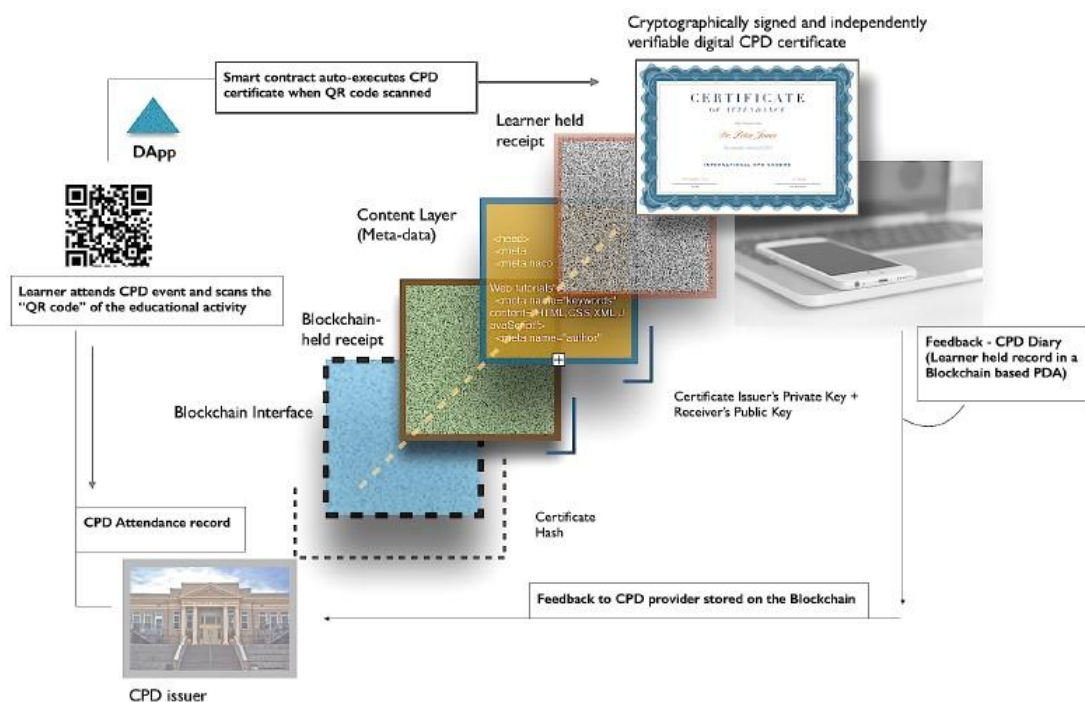
Εικόνα 3.11: Οι εννέα κατηγορίες της Ιατρικής Εκπαίδευσης [116]

- Identity & Learner records και Academic Credentialing :

Οι οργανισμοί δαπανούν σημαντικό χρόνο και πόρους για την επαλήθευση των ακαδημαϊκών διαπιστευτηρίων. Με την ανάθεση αυτών των διαπιστευτηρίων στο blockchain , εξασφαλίζουμε ότι το αμετάβλητο, ανεξάρτητο, επαληθεύσιμο και χρονικά σεσημασμένο αρχείο μπορεί να αποθηκευτεί μόνιμα. Σε περίπτωση χαμένων αρχείων ή μετεγγραφής φοιτητών/γιατρών από ένα πανεπιστημιακό ίδρυμα σε ένα άλλο, μπορεί να εξασφαλιστεί μέσω του blockchain η άμεση διάθεση και πρόσβαση χωρίς να ζητηθεί διπλό αντίγραφο από το ίδρυμα [118]. Εφόσον τα δεδομένα κρυπτογραφούνται, πρόσβαση στα διαπιστευτήρια μπορεί να έχουν μόνο οι κάτοχοι των ψηφιακών κλειδιών.

- Μάθηση βασισμένη στο blockchain και CPD (Continuing Professional Development)

Η Ιατρική Εκπαίδευση εξελίσσεται γρήγορα και γίνεται όλο και πιο διεπιστημονική. Οι φοιτητές ιατρικής καλούνται όλο και περισσότερο να συλλέγουν ένα ευρύ φάσμα από CPD , το οποίο ενσωματώνει τόσο κλινικές όσο και μη κλινικές δραστηριότητες [119]. Το blockchain μπορεί να συλλέξει στοιχεία μάθησης σε πραγματικό χρόνο, τα οποία μπορούν να αποθηκευτούν και να μοιραστούν άμεσα στους φορείς . Μπορεί επίσης να γίνει αποτελεσματικό σε χρόνο και πόρους για την παρακολούθηση αρχείων, εκδίδοντας πιστοποιητικά CPD στο blockchain, καταγράφοντας τα σχόλια των μαθητών, Επίσης είναι τεράστιας αξίας καθώς μπορεί να επιβεβαιώσει την ιδιοκτησία των ακαδημαϊκών αρχείων και CPD για τον κάθε μαθητή [120].



(Source: Copyrights Naqvi, N 2018, The British Blockchain Association)

IDEALISTIC SOLUTION DESIGN – A 360 degree complete CPD Loop

Technology stack: Blockchain based CPD, Certification and Feedback

Εικόνα 3.12: Ιδανικός σχεδιασμός [116]

- Ιατρική εκπαίδευση χωρίς όρια και Medical Education Network :

Η μάθηση σε ένα κλινικό περιβάλλον γίνεται όλο και πιο πολύπλοκη και μπορεί να είναι δύσκολο να καταγραφεί. Οι φοιτητές Ιατρικής και οι γιατροί μαθαίνουν τεράστιο όγκο γνώσεων και δεξιοτήτων, που είναι δύσκολο να αντικατοπτριστεί, να επαληθευτεί, να αναγνωριστεί και να επικυρωθεί. Συχνά είναι δύσκολο να παρακολουθηθεί η μάθηση πίσω από κάθε πηγή. Δεδομένου ότι η επικύρωση στο blockchain λαμβάνει χώρα τη στιγμή της δημιουργίας ενός αρχείου και όχι αργότερα, ένα πρόγραμμα βασισμένο στο blockchain θα μπορούσε να προσφέρει μια λύση. Τώρα είναι πρακτικά δυνατό για το εκπαιδευτικό περιεχόμενο να κρυπτογραφηθεί, να επικυρωθεί, να είναι χρονικά σημασμένο και να είναι διαθέσιμο στο blockchain [121]. Το εκπαιδευτικό περιεχόμενο είναι αμετάβλητα αποθηκευμένο σε ένα αποκεντρωμένο ημερολόγιο (decentralized ledger). Ο μαθητής είναι σε θέση να αποκτήσει πρόσβαση στα δεδομένα από οπουδήποτε στον κόσμο και να σχολιάσει άμεσα κάποιο κομμάτι πληροφοριών, ενός δημιουργού κάνοντας «hash tagging». Αυτό θα πιστωθεί στο χαρτοφυλάκιο του δημιουργού ως μια πλήρως αποκεντρωμένη, μόνιμη μορφή απόδειξης. Η κρυπτογραφία θα εξασφαλίσει διαφάνεια, ορατότητα και πλήρη έλεγχο στο χρήστη με τρόπο peer-to-peer, χωρίς την ανάγκη ενός αξιόπιστου διαμεσολαβητή.

- Smart Contracts και Medical Education Hub:

Τα Medical Education “tokens” μπορούν να δημιουργηθούν σε ένα αποκεντρωμένο blockchain. Μπορούν να χρησιμοποιηθούν για την πληρωμή των εκπαιδευτικών υπηρεσιών απευθείας από το mobile wallet. Αυτό θα επιτρέψει την απευθείας σύνδεση των χρηστών με τους παρόχους υπηρεσιών εκπαίδευσης για την πληρωμή των εκπαιδευτικών υπηρεσιών σε ψηφιακό νόμισμα. Επίσης τα ψηφιακά tokens θα μπορούσαν να απονεμηθούν για ακαδημαϊκά επιτεύγματα και μπορεί να γίνουν αποδεκτά ως αναγνώριση της απονομής από πολλά ιδρύματα βάσει προσυμφωνημένων κριτηρίων. Μια πλατφόρμα βασισμένη σε blockchain θα επιτρέψει στους χρήστες να αναζητούν, να συνδέονται και να πληρώνουν για τις εκπαιδευτικές υπηρεσίες σε ένα αυτόνομο οικοσύστημα ηλεκτρονικού εμπορίου (e-commerce), που θα είναι παγκοσμίως προσβάσιμο από όλες τις χώρες και θα επιτρέπεται τη λειτουργία του στο πλαίσιο των κανονιστικών ρυθμίσεων [122]. Μια ψηφιακή πύλη θα επιτρέψει την διαχείριση των πληροφοριών των μαθητών, των ανταμοιβών και τη συμμετοχή στις εκπαιδευτικές δραστηριότητες με έναν απλοποιημένο τρόπο.

- Validation και Certification

Η έξαρση των πλαστών πτυχίων και των οργανισμών που τα παράγουν (diploma mills), δημιούργησε τεράστια αβεβαιότητα όχι μόνο στον ακαδημαϊκό χώρο αλλά και στην εμπιστοσύνη του κοινού προς τους επαγγελματίες της υγειονομικής περίθαλψης. Αυτό το αυξανόμενο πρόβλημα με τα πλαστά διαπιστευτήρια υπονομεύει τον ίδιο τον ιστό της τριτοβάθμιας εκπαίδευσης καθώς υποτιμά το χρόνο και τη σκληρή δουλειά καθώς και την υποκειμενική αξία της τριτοβάθμιας εκπαίδευσης. Όταν οι άνθρωποι αμφισβητούν τις δυνατότητες και τις γνώσεις των γιατρών τους δημιουργούνται δυσάρεστες καταστάσεις, όπως ασθενείς που δεν ακολουθούν τις οδηγίες σχετικά με την πρόληψη φαρμάκων, την αποκατάσταση και στη συνέχεια να καταφεύγουν στην κατηγορία για έλλειψη εμπιστοσύνης στο φροντιστή τους ως τον κύριο λόγο για τα συνεχιζόμενα προβλήματά τους και τις ασθένειές τους.

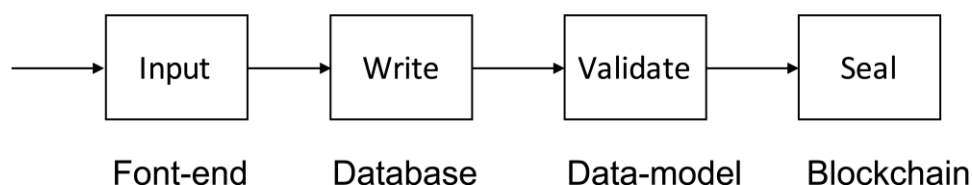
Άτομα με πλαστά πτυχία θέτουν σε κίνδυνο το κοινό, καθώς το δηλωμένο σύνολο δεξιοτήτων τους δεν υπάρχει, είτε λόγω ελαχίστων γνώσεων είτε πλήρους απουσίας εκπαίδευσης. Κάποιοι χρησιμοποιούν τα ψεύτικα πιστοποιητικά τους για να κερδίσουν την εμπιστοσύνη των ανθρώπων και έπειτα τους εξαπατούν με κίνδυνο την απώλεια της ίδιας τους της ζωής. Αξίζει να αναφερθούμε σε κάποια περιστατικά. Δύο άντρες αγόρασαν τα doctors' ID για \$100 και διέκοψαν τη θεραπεία από ένα νεαρό κορίτσι στο οποίο χορηγούνταν ινσουλίνη για να της δώσουν για την πάθησή της λάδι φιδιού που οι ίδιοι παρασκεύασαν. Το νεαρό κορίτσι έχασε τη ζωή του και οι δύο άντρες κατηγορήθηκαν για ανθρωποκτονία στη Βόρεια Καρολίνα [123].

Αυτό το πρόβλημα υπάρχει εδώ και αιώνες, αλλά τις τελευταίες δεκαετίες, λόγω της μεγάλης προόδου της τεχνολογίας έχει αυξηθεί ραγδαία. Το πιο διάσημο πρόσφατο παράδειγμα ευρείας κατάχρησης αφορά στην εταιρεία AXACT, στο Πακιστάν, η οποία επινόησε πάνω από 300 ψεύτικα Πανεπιστήμια, χρησιμοποιώντας τεχνητές ειδήσεις για να ξεγελάσει τους εργοδότες που ενδεχομένως ελέγχουν τις αναφορές. Το 2018, ο διευθύνων σύμβουλος και 22 υπάλληλοι καταδικάστηκαν σε 22 χρόνια φυλάκισης για το ψεύτικο degree mill [124]. Στην Κίνα το πρόβλημα είναι τόσο διαδεδομένο που υπάρχουν ιστοσελίδες δημιουργημένες από απάτες μαζί με «true or false» πύλες, όπου οι χρήστες μπορούν να επιβεβαιώσουν/επαληθεύσουν μη καταχωρημένα σχολεία. Το Υπουργείο Παιδείας της Κίνας στοχεύει ενεργά στην καταστολή αυτής της απάτης. Επίσης, έχουν παρατηρηθεί άτομα που ως γιατροί με διδακτορικό διδάσκουν. Αυτό όχι μόνο υπονομεύει το εμπλεκόμενο εκπαιδευτικό ίδρυμα, αλλά θέτει σε κίνδυνο τη νομιμότητα των βαθμών των μαθητών που διδάσκονται. Ο εκπρόσωπος της Vancouver Island Health Authority, Shannon Marshall, δήλωσε: « Δεν θα ελέγχαμε τακτικά τα διαπιστευτήρια οποιουδήποτε διευθυντή, εκτός εάν υπήρχε κάποια ένδειξη ότι έπρεπε να επαληθευτούν». Μόλις γίνει αντιληπτή η απάτη, δεν είναι πάντα εύκολη διαδικασία να αποκρυπτογραφηθούν πόσα από τα προσόντα είναι αληθινά και πόσα αγοράστηκαν από το Διαδίκτυο. Ο πρώην πράκτορας του FBI, Allen Ezell, ισχυρίζεται ότι πάνω από το ήμισυ των PhDs που εκδίδονται στις ΗΠΑ κάθε χρόνο είναι πλαστά [125]. Η αγορά των ψεύτικων διαπιστευτηρίων χρονολογείται από πολύ παλιά και από τα περίπου 200.000 πλαστά πιστοποιητικά που εκδίδονται ετησίως στις ΗΠΑ ένα μεγάλο μέρος αφορά στον Ιατρικό τομέα. Η ενέργεια και τα χρήματα που δαπανούνται για την καταπολέμηση αυτού του αυξανόμενου προβλήματος, θα μπορούσαν να σωθούν, με τη χρήση του blockchain. Ανοιχτά και διαφανή ακαδημαϊκά πιστοποιητικά Blockchain, που αντικατοπτρίζουν την αληθινή δουλειά και εργασία που δαπανάται από τον κάθε εκπαιδευόμενο. Μπορεί να δημιουργηθεί ένα έξυπνο «bionetwork», βασισμένο στο blockchain και να προκαλέσει αλλαγή στον ακαδημαϊκό χώρο.

Στη συνέχεια θα μελετήσουμε το σχεδιασμό μιας blockchain λύσης για certificate authentication, έτσι όπως προτείνεται στο Βιετνάμ, από μια εργασία που εκδόθηκε φέτος, το 2020, (<https://peerj.com/articles/cs-266/>). Θα μελετήσουμε το σχεδιασμό για τη δημιουργία του συστήματος VECefblock.

3.5.1) Περιγραφή του συστήματος *VECefblock*

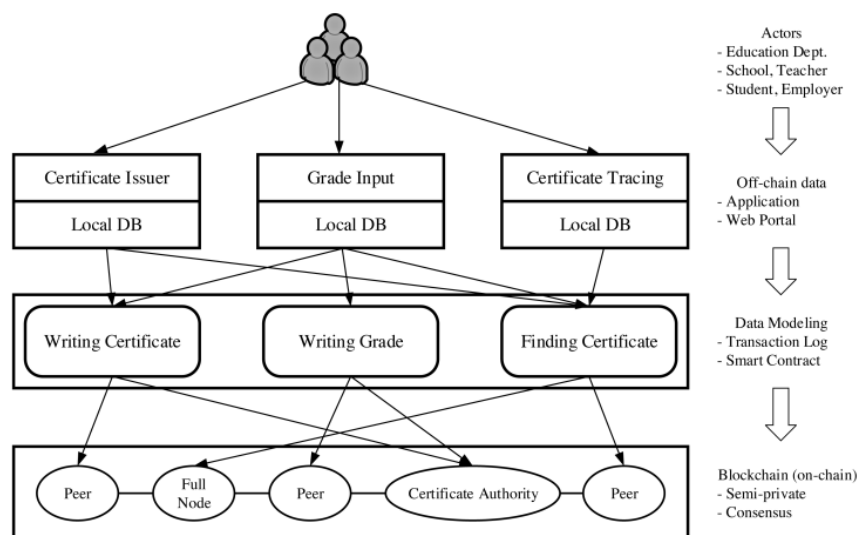
Για το VECefblock, προτείνεται η αρχιτεκτονική input-write-validate-seal, που βελτιώνει και ενισχύει την εμπιστοσύνη για τη διαχείριση των παραδοσιακών εκπαιδευτικών συστημάτων. Η προτεινόμενη αρχιτεκτονική αποτελείται από 4 φάσεις σε σχέση με τη παραδοσιακή που έχει 2 φάσεις, input-write.



Εικόνα 3.13: Σχεδιασμός των τεσσάρων φάσεων του VECefblock (<https://doi.org/10.7717/peerjcs.266/fig-2>)

- **Input:** Είναι το ίδιο και στις δύο αρχιτεκτονικές, όπου τα εκπαιδευτικά δεδομένα, όπως, αξιολογήσεις, αναγνώριση μαθητή και πληροφορίες πιστοποιητικού, εισάγονται από μια διαδικτυακή πύλη. Τα εκπαιδευτικά ιδρύματα ελέγχουν αυτές τις εφαρμογές εισαγωγής. Οι πιθανοί παράγοντες αυτών των εφαρμογών είναι οι πρυτάνεις, οι διευθυντές, οι εκπαιδευτικοί.
- **Write:** Στην προσέγγισή μας τα δεδομένα γράφονται τόσο στην τοπική Β.Δ. (παραδοσιακό σύστημα), όσο και στο blockchain. Τα δεδομένα εισαγωγής μετατρέπονται μέσω της δομής χαρτογράφησης δεδομένων.
- **Validate:** Εφόσον τα δεδομένα εισαγωγής ταιριάζουν με τη δομή δεδομένων του VECefblock, ελέγχεται η μορφή και η υπογραφή. Αυτά τα δεδομένα εισόδου γίνονται μια συναλλαγή στο VECefblock. Οι ηλεκτρονικές υπογραφές παρέχονται και διασφαλίζονται από εθνικούς κεντρικούς παρόχους. Αναγνωρίζοντας τους παράγοντες του συστήματος, τα δεδομένα που είναι αποθηκευμένα στο blockchain είναι αξιόπιστα.
- **Seal:** Οι επικυρωμένες συναλλαγές αποθηκεύονται σε ένα block, και ένα νέο block δημιουργείται για να «σφραγίσει» αυτές τις συναλλαγές. Μετά τη σφραγίδα, είναι σχεδόν αδύνατο να αλλάξουν τα δεδομένα και οποιαδήποτε τροποποίηση θα καταγραφεί στο blockchain.

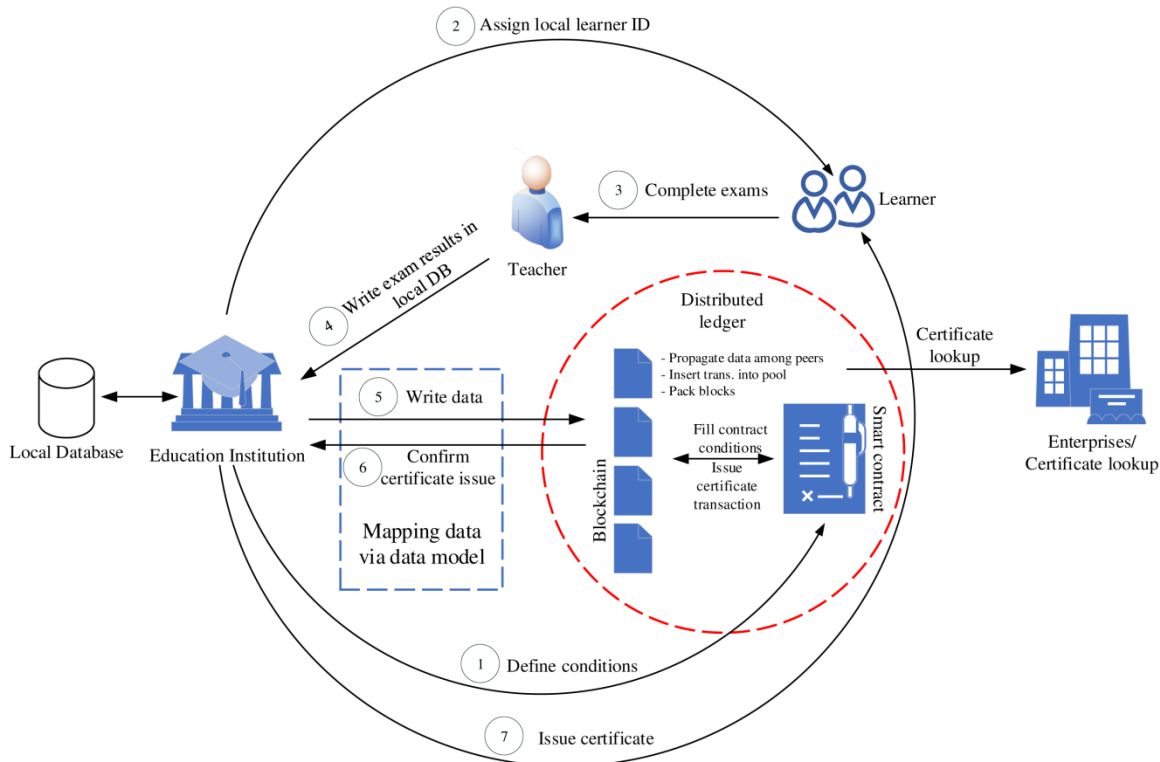
Το VECefblock αποτελείται από τρία κύρια επίπεδα που περιλαμβάνουν αυτή την αρχιτεκτονική των τεσσάρων φάσεων. Στην κορυφή βρίσκονται οι παράγοντες και έπειτα τα τρία επίπεδα : off-chain writing (local database), data modeling , on-chain writing (blockchain). Φαίνονται στην παρακάτω εικόνα.



Εικόνα 3.14: Αρχιτεκτονική του συστήματος (<https://doi.org/10.7717/peerjcs.266/fig-3>)

- Application layer:** Οι φάσεις input και local write ανήκουν σε αυτό το επίπεδο που καλύπτει όλες τις διαδραστικές εφαρμογές που εκτελούνται στα εκπαιδευτικά ιδρύματα. Ονομάζουμε off-chain data δεδομένα που εισόδου (input) δεν ανταποκρίνονται στο VECefblock.
- Data modeling layer:** Πριν γραφτούν στο VECefblock blockchain, τα δεδομένα από το Application layer πρέπει να μετατραπούν στην δομή των δεδομένων μας. Αυτό το επίπεδο περιέχει μια δομή χαρτογράφησης δεδομένων, όπως σύνταξη πιστοποιητικών, βαθμός, εύρεση πιστοποιητικού.
- Blockchain layer:** Η επικύρωση και η σφράγιση πραγματοποιείται στο blockchain. Τα τυπικά στοιχεία περιλαμβάνουν ομότιμους, πλήρεις κόμβους και την αρχή έκδοσης των πιστοποιητικών. Το VECefblock θα μπορούσε να αναπτυχθεί σε διάφορες πλατφόρμες blockchain, (Hyperledger Fabric, Korum, EOSIO). Ωστόσο, επειδή ο έλεγχος αυθεντικότητας του πιστοποιητικού είναι μια διαδικασία που τη διαχειρίζεται το κράτος, απαιτείται ασφάλεια υψηλού επιπέδου. Εξάλλου το κράτος διατηρεί το δικαίωμα έκδοσης εκπαιδευτικών πιστοποιητικών. Για κάθε αναπτυσσόμενο δίκτυο blockchain (Πανεπιστήμιο) , τρεις κόμβοι και ένας κόμβος ελέγχου αυθεντικότητας πιστοποιητικού συστήματος είναι τα ελάχιστα μοτίβα ανάπτυξης.

3.5.2) Ροή εκτέλεσης του συστήματος VECefblock



Εικόνα 3.15: VECefblock επιχειρηματική διαδικασία (<https://doi.org/10.7717/peerjcs.266/fig-4>)

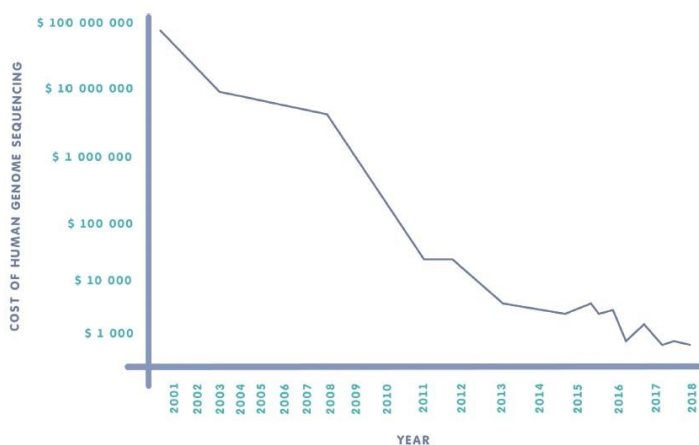
- Τα εκπαιδευτικά ιδρύματα διαδραματίζουν το ρόλο του καθορισμού των όρων της έξυπνης σύμβασης κατάρτισης, οι οποίες επισημαίνουν τον αριθμό των μαθημάτων πίστωσης που πρέπει να συλλέξει ένας φοιτητής προτού λάβει το πιστοποιητικό. Ο εκπαιδευόμενος πρέπει να συμπληρώσει τους όρους της σύμβασης μέσω της συλλογής πιστώσεων μαθημάτων. Όταν ένας εκπαιδευόμενος εγγράφεται σε ένα εκπαιδευτικό ίδρυμα, εκδίδεται για τον ίδιο ένα αναγνωριστικό από το ίδρυμα. Ως σχεδιασμός, κάθε ίδρυμα διαθέτει μία τοπική Β.Δ. που παρέχει ένα αποθετήριο δεδομένων για τη διαχείριση του εκπαιδευτικού συστήματος. Το αναγνωριστικό μαθητή είναι μια μοναδική ταυτότητα στο σύστημα του ιδρύματος. Ωστόσο, για να διασφαλίσουμε ότι το αναγνωριστικό του εκπαιδευόμενου είναι μοναδικό στο VECefblock, επιλέγουμε εθνικά αναγνωριστικά. Σε περίπτωση που ένα εκπαιδευτικό ίδρυμα δεν αποθηκεύει εθνικά αναγνωριστικά, χρησιμοποιείται το αναγνωριστικό μαθητή, το όνομα του ιδρύματος, η χρονική σήμανση κατά τη στιγμή καταχώρισης των δεδομένων ταυτότητας. Αυτές οι τιμές θα κατακερματιστούν για να δημιουργήσουν το κλειδί αναγνώρισης του εκπαιδευόμενου στο δίκτυο blockchain.
- Στη διαδικασία λειτουργίας, ο μαθητής θα δώσει τις εξετάσεις που έχουν ανατεθεί από τον καθηγητή. Μόλις ο εκπαιδευόμενος περάσει τις εξετάσεις, ο καθηγητής θα γράψει τα αποτελέσματα σε μια τοπική Β.Δ. του εκπαιδευτικού ιδρύματος. Τα δεδομένα θα

μεταφερθούν αυτόματα στο VECefblock μέσω του μοντέλου δεδομένων που θα δούμε στη συνέχεια.

- Όταν πληρούνται όλοι οι όροι της έξυπνης σύμβασης που σχετίζονται με τα credit records, δημιουργείται και αποθηκεύεται αυτόματα μια συναλλαγή για την έκδοση του πιστοποιητικού στο δίκτυο blockchain. Με τη δομή χαρτογράφησης δεδομένων, οι πληροφορίες έκδοσης πιστοποιητικών θα σταλούν στο εκπαιδευτικό ίδρυμα με το κλειδί. Με βάση τα πλεονεκτήματα της τεχνολογίας blockchain, οι πληροφορίες πιστοποιητικού διαδίδονται και επαληθεύονται από block που είναι αποθηκευμένα σε πολλούς και διαφορετικούς κόμβους. Επομένως, οι πληροφορίες μπορούν να είναι αξιόπιστες και δεν μπορούν να αλλάξουν από τρίτους. Με βάση τις πληροφορίες πιστοποιητικού στο δίκτυο blockchain, το ίδρυμα θα εκδώσει τόσα πιστοποιητικά με τη μορφή εγγράφου, όσο και ηλεκτρονικά για τους μαθητές (κωδικός πιστοποιητικού).
- Για τις επιχειρήσεις που θα ήθελαν να αναζητήσουν ένα πιστοποιητικό, μπορούν να υποβάλλουν ερώτημα για δεδομένα που είναι αποθηκευμένα στις συναλλαγές blockchain μέσω των κωδικών πιστοποιητικών που εκδίδονται για τους φοιτητές. Από την άλλη πλευρά, για να διασφαλίσουμε τις διαδικασίες αποτελεσμάτων γραφής του μαθήματος, χρησιμοποιούμε κρυπτογραφημένα ιδιωτικά κλειδιά. Κατά τη σύνταξη των δεδομένων των αποτελεσμάτων των εξετάσεων, οι εκπαιδευτικοί πρέπει να ενσωματώσουν τα ιδιωτικά τους κλειδιά. Το εκπαιδευτικό ίδρυμα χρησιμοποιεί επίσης το κλειδί του σε συνδυασμό με τα κλειδιά του εκπαιδευτικού για τη σύνταξη των δεδομένων στο σύστημα blockchain. Αυτός ο μηχανισμός βοηθά στην αποτροπή πλαστών συναλλαγών .

3.6) Γονιδιωματικά δεδομένα (genomic data generation)

Οι πρώτες απόπειρες ανάλυσης της αλληλουχίας του ανθρώπινου γονιδιώματος είχαν κόστος πάνω από \$3 δισεκατομμύρια , ενώ σήμερα, με τη χρήση νέων τεχνολογιών η τιμή οδηγήθηκε κάτω από \$1.000 , καθιστώντας την αλληλουχία του προσωπικού γονιδιώματος προσιτή σε όλους. Αυτή η τιμή πρόκειται να μειωθεί στα \$100 τα επόμενα χρόνια [127]. Στην παρακάτω εικόνα μπορούμε να δούμε το κόστος τα τελευταία χρόνια.



Εικόνα 3.16: Κόστος αλληλουχίας ανθρώπινου γονιδιώματος, 2001-2018 [126]

Το 2005, ξεκίνησε το «Πρόγραμμα Προσωπικού Γονιδιώματος (Human Genome Project), το οποίο είναι μια βάση δεδομένων και μέχρι στιγμής έχει εγγεγραμμένους χιλιάδες εθελοντές που συμφώνησαν να αλληλουχηθεί το γονιδιώμα τους και να γίνει κοινή χρήση των γονιδιωματικών δεδομένων τους [129].

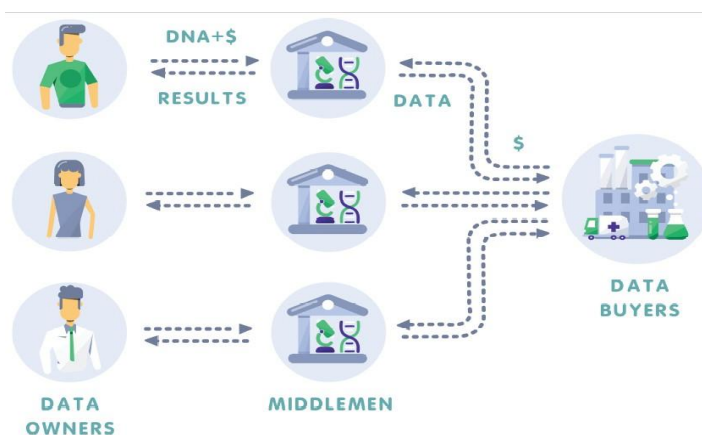
Η αλληλουχία του προσωπικού γονιδιώματος έχει δυνατότητες, όπως, καλύτερη πρόληψη ασθενειών, διαγνώσεις με μεγαλύτερη ακρίβεια, εξατομικευμένες θεραπείες, αναγνώριση πολλών ασθενειών και ανάπτυξη νέων θεραπειών μέσω της ανταλλαγής των γονιδιωματικών δεδομένων μεταξύ των ερευνητών [126].

Ωστόσο, ενώ το Πρόγραμμα Προσωπικού Γονιδιώματος έχει αξιοθαύμαστη πρόοδο, δεν έχει επεκτατική ανάπτυξη [128]. Υπάρχουν εμπόδια στην ανάπτυξη και κοινή χρήση των γονιδιωματικών δεδομένων, όπως, το κόστος της αλληλουχίας, οι ανησυχίες σχετικά με το απόρρητο, οι κανονιστικοί περιορισμοί και τεχνικές προκλήσεις [126]. Λίγοι άνθρωποι αισθάνονται άνετα να δημοσιοποιήσουν τις προσωπικές γενετικές πληροφορίες τους και πολλοί ανησυχούν για τις πολιτικές απορρήτου. Επίσης οι περισσότεροι δεν εκτιμούν την αλληλουχία του προσωπικού γονιδιώματος καθώς η πιθανότητα να επωφεληθούν άμεσα και σημαντικά είναι σχετικά χαμηλή [128]. Έτσι η μείωση του κόστους δεν είναι αρκετή για να ενθαρρύνει τη μαζική υιοθεσία.

Personal Genomics 2.0

Το παραδοσιακό μοντέλο για τη δημιουργία και κοινή χρήση των γονιδιωματικών δεδομένων που έχει υιοθετηθεί από διάφορες εταιρείες συμβάλλει στις προκλήσεις που περιγράψαμε. Αυτό το μοντέλο απαιτεί από τους καταναλωτές να πληρώσουν για τις γενετικές δοκιμές και για την ερμηνεία των αποτελεσμάτων, ενώ οι εταιρείες συχνά παίρνουν την ιδιοκτησία των δημιουργημένων γονιδιωματικών δεδομένων και τα πουλούν σε εταιρείες biopharma [126].

Αυτό το μοντέλο απαιτεί από τους καταναλωτές να πληρώσουν και να παραιτηθούν από την κυριότητα και τον έλεγχο των γονιδιωματικών δεδομένων τους, το οποίο είναι αποθαρρυντικό για τον γενετικό έλεγχο [126].



Εικόνα 3.17: Το παραδοσιακό μοντέλο για τη δημιουργία και κοινή χρήση των γονιδιωματικών μοντέλων, [126]

Θα αναφερθούμε σε τρεις τύπους εταιρειών που η καθεμία επιλύει και μία πρόκληση. Παρ’όλα αυτά, καμία δεν μπορεί να ξεπεράσει το σύνολο των προκλήσεων που αναφέραμε πιο πάνω.

1) Το GA4GH Beacon Project [130] και το i2b2 SHRINE [131] είναι δύο από τα πιο προηγμένα συστήματα κοινής χρήσης βιοϊατρικών δεδομένων. Και τα δύο είναι δίκτυα που επιτρέπουν στα συμμετέχοντα ιδρύματα να συνδέσουν τις βάσεις δεδομένων τους και να επεξεργαστούν ερωτήματα σχετικά με την παρουσία γενετικών παραλλαγών και χαρακτηριστικών. Αυτό το μοντέλο ελαχιστοποιεί τις ακριβές μεταφορές δεδομένων και επιτρέπει σε ιδρύματα να διατηρήσουν τον έλεγχο των δεδομένων τους. Αυτό αφορά το απόρρητο και τις κανονιστικές και τεχνικές προκλήσεις που σχετίζονται με την κεντρική αποθήκευση και τις μεταφορές των γονιδιωματικών δεδομένων.

Ωστόσο υπάρχουν περιορισμοί. Αρχικά, περιορίζεται η λειτουργικότητα, καθώς δεν υποστηρίζονται προς το παρόν υπολογισμοί που απαιτούνται για την επεξεργασία και ανάλυση των δεδομένων. Επίσης, η συμμετοχή περιορίζεται στα ακαδημαϊκά ερευνητικά ιδρύματα και νοσοκομεία. Δεν υπάρχουν εστιασμένες πύλες για τον ασθενή-καταναλωτή που θα επιτρέψουν σε άτομα να συνεισφέρουν εύκολα τα προσωπικά τους γονιδιωματικά δεδομένα. Επιπλέον, δε έχουν εφαρμοστεί μηχανισμοί αποζημίωσης και αποκεντρωμένη διακυβέρνηση.

2) Η κατανεμημένη αποθήκευση μπορεί να βοηθήσει στην προστασία του απορρήτου. Ωστόσο, οι ιδιοκτήτες των δεδομένων δεν μπορούν πάντα να διατηρούν τους in-house servers τους και συχνά αναθέτουν σε τρίτους την αποθήκευση των δεδομένων, όπως οι πάροχοι των υπηρεσιών cloud. Για την προστασία του απορρήτου των γονιδιωματικών δεδομένων που έχουν κοινοποιηθεί σε μη αξιόπιστα τρίτα μέρη, έχουν υιοθετηθεί encryption-based privacy preserving τεχνικές. Αυτές οι τεχνικές επιτρέπουν σε τρίτα συμβαλλόμενα μέρη να εκτελέσουν υπολογισμούς και να επιστρέψουν αποτελέσματα χωρίς να υπάρχει πρόσβαση στο plaintext των γονιδιωματικών δεδομένων. Αυτές οι encryption-based privacy preserving τεχνικές, έχουν εφαρμοστεί προηγουμένως σε κατανεμημένες βάσεις δεδομένων.

Το MedCo ενσωματώνεται με το i2b2 SHRINE και χρησιμοποιεί ένα ομομορφικό σχήμα κρυπτογράφησης δεδομένων για να ενεργοποιήσει την εξωτερική ανάθεση για την αποθήκευση των γονιδιωματικών δεδομένων και την εκτέλεση ερωτήματος σε μη αξιόπιστα τρίτα μέρη [132].

Το Secure Multi Party Query Language εφαρμόζει παρόμοια λειτουργικότητα και εγγυήσεις απορρήτου. Τα δεδομένα μπορούν να προστατευτούν χρησιμοποιώντας κατάλληλο αξιόπιστο hardware.

Το Princess εκτελεί υπολογισμούς σε γονιδιωματικά δεδομένα μέσα σε προστατευμένες περιοχές μνήμης μικροεπεξεργαστών Intel [133].

3) Οι εταιρείες γονιδιωματικής έχουν εξερευνήσει διάφορα μοντέλα για να αποζημιώσουν άτομα που συνεισφέρουν τα προσωπικά γονιδιωματικά δεδομένα στους ερευνητές.

Η Ginos, το 2016, προσφέρθηκε να βοηθήσει τους πελάτες της να πουλήσουν τα δεδομένα τους σε ερευνητές [134].

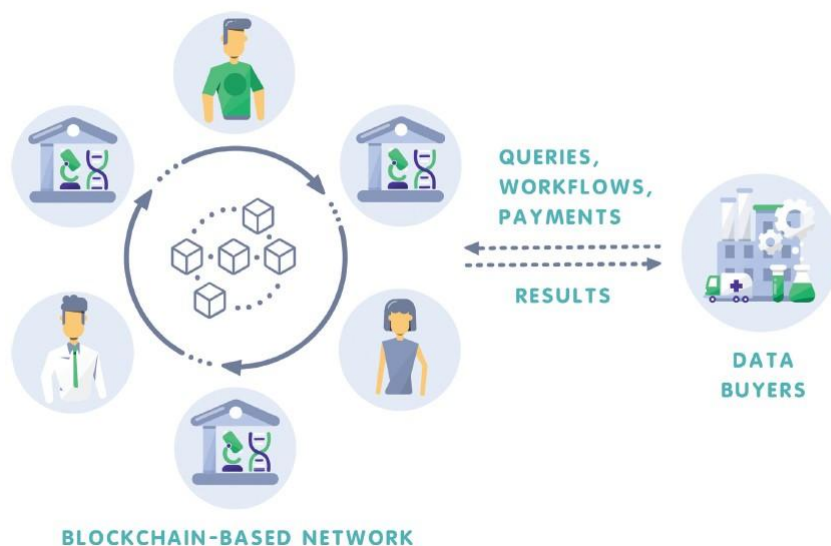
Η EncrypGen, το 2017, χρησιμοποίησε κρυπτονόμισμα αντί για πραγματικό νόμισμα για τον ίδιο λόγο.

Η LunaDNA, ανακοίνωσε ότι θα αποζημιώσει τους συνεισφέροντες γονιδιωματικών δεδομένων με απόθεμα της εταιρείας [135].

Blockchain και γονιδιωματικά δεδομένα

Αυτές οι προκλήσεις μπορούν να αντιμετωπιστούν με το συνδυασμό 1)δικτύων κοινής χρήσης γονιδιωματικών δεδομένων, 2)τεχνολογίας προστασίας απορρήτου (privacy-preserving) και 3)δίκαιου μοντέλου αποζημίωσης, σε μια πλατφόρμα που θα δίνει τον έλεγχο των δεδομένων σε μεμονωμένους χρήστες και θα εξασφαλίζει διαφάνεια και μυστικότητα, (Εικόνα 3.8).

Έχουν διερευνηθεί διάφορες προσεγγίσεις για τη διάδοση της αλληλουχίας του προσωπικού γονιδιώματος και τη βελτίωση της πρόσβασης στα γονιδιωματικά δεδομένα [128]. Η τεχνολογία blockchain μπορεί να βοηθήσει στην καταλυτική επανάσταση των γονιδιωματικών δεδομένων.



Εικόνα 3.18: Εναλλακτικό μοντέλο που μπορεί να αντιμετωπίσει τις προκλήσεις, [126].

- 1) Η λειτουργικότητα της ανταλλαγής των γονιδιωματικών δεδομένων στα δίκτυα πρέπει να επεκταθεί. Αυτό απαιτεί ένα δίκτυο που μπορεί να είναι ενσωματωμένο με μια πλήρη πλατφόρμα βιοπληροφορικής που υποστηρίζει την επεξεργασία και ανάλυση των γονιδιωματικών δεδομένων. Εφαρμόζοντας αυτή τη λειτουργικότητα θα ομαδοποιηθούν κατακερματισμένα δεδομένα και θα είναι διαθέσιμα για ανάλυση σε ένα μόνο δίκτυο, διευκολύνοντας έτσι την πρόσβαση των ερευνητών σε δεδομένα, [126].
- 2) Το δίκτυο κοινής χρήσης δεδομένων πρέπει να επεκταθεί πέρα από τα ερευνητικά ιδρύματα και πρέπει να είναι προσβάσιμο σε άτομα που θέλουν να μοιραστούν τα δικά τους προσωπικά γονιδιωματικά δεδομένα. Ωστόσο, η αποκέντρωση του δικτύου θα απαιτήσει ένα περισσότερο δημοκρατικό μοντέλο διακυβέρνησης. Αυτό μπορεί να

επιτευχθεί με την ενσωμάτωση του blockchain, το οποίο υπόσχεται αποκεντρωμένα και αυτοδιοικούμενα δίκτυα [126].

- 3) Ο έλεγχος στην πρόσβαση των δεδομένων στο blockchain μπορεί να εξασφαλίσει διαφανή διαχείριση συναίνεσης, ενώ οι privacy-preserving τεχνολογίες μπορούν να βοηθήσουν στην προστασία της κοινής χρήσης των γονιδιωματικών δεδομένων, επιτρέποντας στους συμμετέχοντες στο δίκτυο να διατηρήσουν την κυριότητα και τον έλεγχο των δεδομένων [126].
- 4) Η αλληλουχία του γονιδιώματος και η κοινή χρήση πρέπει να ενθαρρυνθούν και να δοθούν κίνητρα με την εφαρμογή μηχανισμών επιδότησης και αποζημίωσης. Το blockchain μπορεί να διευκολύνει αυτή την κατάσταση, καθώς επιτρέπει στους ερευνητές να συνδεθούν απευθείας με άτομα, επιδοτώντας το κόστος της γονιδιωματικής αλληλουχίας και αντισταθμίζοντας την κοινή χρήση. Η εξάλειψη των μεσαζόντων μπορεί να οδηγήσει στη μείωση των τιμών [126].

Συγχεδιασμός

Για την επίτευξη ενός τέτοιου συστήματος που θα υποστηρίζει την αποκεντρωμένη αποθήκευση δεδομένων και υπολογισμού τους με την διασφάλιση απορρήτου και θα πληροί τα παραπάνω χαρακτηριστικά, απαιτούνται :

- Πλατφόρμα βιοπληροφορικής
- Πλαίσιο Blockchain
- Privacy-preserving τεχνολογίες

Criteria	Arvados ^{42,43}	DNASTack ⁴⁴	Seven Bridges ⁴⁵	DNAnexus ⁴⁶	Galaxy ⁴⁷
Hardware	Federated clouds and servers	Google Cloud with Beacon Network integration	Clouds	Clouds	Local servers
Pipeline design	API-based; web GUI	API-based; web GUI	Web GUI	Web GUI	Web GUI
Containers	Yes	Yes	Yes	Yes	Yes
Workflow language	CWL	WDL	CWL	Custom	Custom
Open source	Yes	No	No	No	Yes
Platform launch year	2013	2014	2012	2010	2005

API: application programming interface; CWL: Common Workflow Language; GUI: graphical (rather than textual) user interface; WDL: Workflow Description Language.

Πίνακας 3.2 : Σύγκριση των πλατφορμών βιοπληροφορικής [126]

Criteria	Exonum ⁵⁰	Hyperledger Fabric ⁵¹	Ethereum ⁵²
Read access	Public	Private	Public
Write access	Private	Private	Public
Consensus	Byzantine fault-tolerant (BFT)	Fault-tolerant (FT)	Proof of work (PoW)
Transactions per second (TPS)	~3,000	~3,000	~15
Smart contracts	Yes (Rust, Java)	Yes (Go, Java)	Yes (Solidity)
Light clients	Yes	No	Yes
Public blockchain anchoring	Yes	No	NA
Open source	Yes	Yes	Yes

NA: not applicable.

Πίνακας 3.3 : Σύγκριση των πλαισίων Blockchain [126]

Criteria	Fully Homomorphic Encryption	Secure Multiparty Computations	Intel Software Guard Extensions	Differential Privacy
Principle	Computations (additions AND multiplications) on ciphertexts	Distributed computations on ciphertexts	Computations inside private memory regions	Introduction of randomness to data/results of computations
Computation time	Very slow	Slow	Fast	Fast
Memory usage	Very high	High	Low	Very low
Communication cost	High	Very high	Low	Low
Specific limitations	None	None	Vulnerabilities have been discovered; requires Intel CPUs	Noise makes interpretation of results more difficult

CPU: central processing unit.

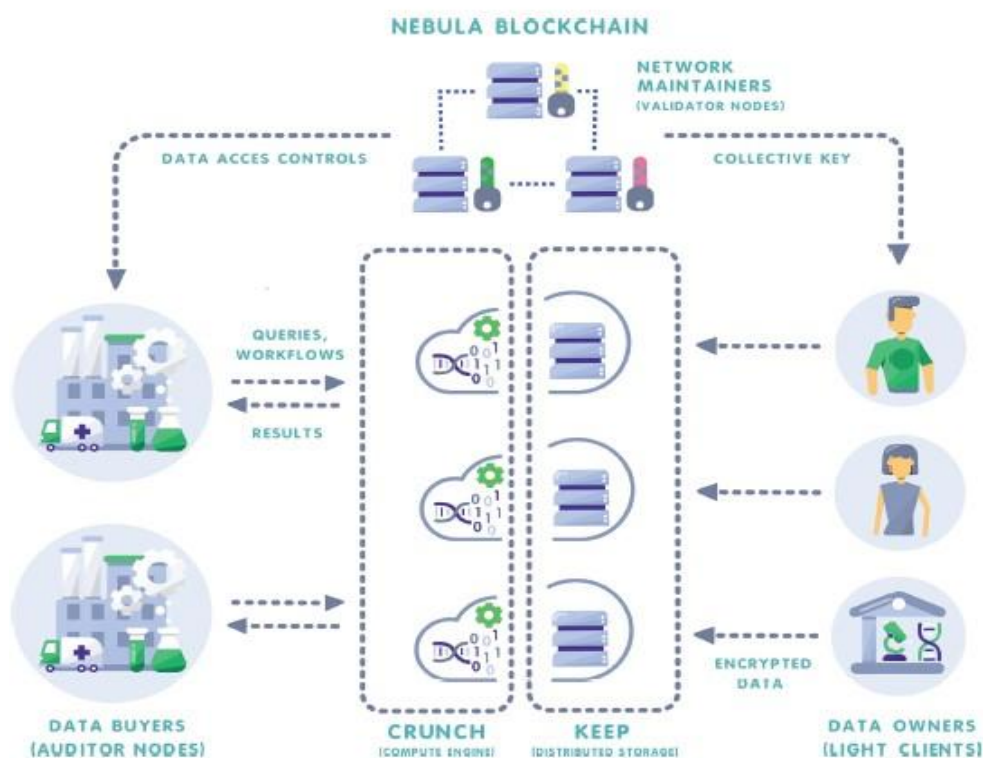
Πίνακας 3.4 : Σύγκριση των privacy-preserving τεχνολογιών [126]

Στη συνέχεια θα μελετήσουμε το σχεδιασμό μιας blockchain λύσης για την αντιμετώπιση των προκλήσεων που αντιμετωπίζονται στον τομέα της γονιδιωματικής αλληλουχίας, έτσι όπως προτείνεται από τη NEBULA του Σαν Φραντσίσκο στις Η.Π.Α. Θα μελετήσουμε το σχεδιασμό για τη δημιουργία του συστήματος NEBULA.

3.6.1) Περιγραφή του συστήματος *NEBULA BLOCKCHAIN*

Η Nebula είναι μια αποκεντρωμένη πλατφόρμα παραγωγής, κοινής χρήσης και ανάλυσης δεδομένων.

Η Nebula ενσωματώνει την πλατφόρμα βιοπληροφορικής Arvados [136] , (github.com/curoverse/arvados), με το blockchain πλαίσιο Exonum [137] , (github.com/exonum), και ένα πλήρως ομομορφικό σχήμα κρυπτογράφησης δεδομένων.



Εικόνα 3.19: Πλατφόρμα NEBULA [126]

1) Η πλατφόρμα βιοπληροφορικής Arvados έχει δύο βασικές λειτουργίες: KEEP και CRUNCH

- **KEEP:** Είναι ένα κατανεμημένο σύστημα αποθήκευσης με δυνατότητα διανομής περιεχομένου, που επιτρέπει την κλιμακούμενη αποθήκευση των γονιδιωματικών μεγάλων δεδομένων (big data), πρόσβαση σε δεδομένα υψηλής απόδοσης και αποτελεσματική διαχείριση δεδομένων [126].
- **CRUNCH:** Είναι μια μηχανή διαχείρισης της ροής εργασίας που επιτρέπει την ευέλικτη δημιουργία και παράλληλη εκτέλεση των data analysis pipelines (αγωγών ανάλυσης δεδομένων) και τη δημιουργία αναπαραγόμενων αποτελεσμάτων [126].

Η πλατφόρμα βιοπληροφορικής Arvados εφαρμόζει κατανεμημένη αποθήκευση δεδομένων και υπολογιστικού μοντέλου που ελαχιστοποιεί τα απαιτούμενα δεδομένα μεταφορών. Αυτό βοηθά στην αντιμετώπιση των προκλήσεων για τα μεγάλα δεδομένα (big data), των κανονιστικών περιορισμών και τους κινδύνους για το απόρρητο των δεδομένων [126].

2) Το Nebula blockchain, είναι ένα Exonum-based blockchain, μέσω του οποίου θα διέπεται το δίκτυο Nebula, η συναίνεση θα τεκμηριώνεται και τα δεδομένα θα είναι ασφαλή.

Το Exonum-based blockchain έχει τρεις τύπους κόμβων : auditors(ελεγκτές), light clients, validators (επικυρωτές) [126].

- Οι auditors είναι πλήρεις κόμβοι (full nodes) που διατηρούν αντίγραφο του συνόλου του περιεχομένου του blockchain και μπορούν να δημιουργήσουν συναλλαγές.
- Οι light clients μπορούν επίσης να δημιουργήσουν συναλλαγές, αλλά αναπαράγουν μόνο πληροφορίες που είναι σχετικές σε αυτούς, αντί για ολόκληρο το περιεχόμενο blockchain.
- Οι validators είναι κόμβοι με άδεια (permissioned) που επαληθεύουν τις συναλλαγές που λαμβάνονται από τους auditors και τους light clients και γράφουν νέα blocks στο blockchain.

Η τρέχουσα εφαρμογή Nebula χρησιμοποιεί το Exonum , όμως μπορεί να χρησιμοποιηθεί και το Hyperledger Fabric ως άλλη επιλογή .

3) Η χρήση της ομομορφικής κρυπτογράφησης δεδομένων επιτρέπει την εφαρμογή των privacy-preserving ερωτημάτων στα γονιδιωματικά δεδομένα. Η πρόθεση είναι να διατηρηθεί το απόρρητο ενεργοποιώντας ερευνητές για να ρωτήσουν ολόκληρη τη βάση δεδομένων και να ανακαλύψουν τα δεδομένα ενδιαφέροντος τους, χωρίς να διακυβεύεται το απόρρητο των ερωτηθέντων δεδομένων [126].

4) Το δίκτυο Nebula έχει τέσσερις τύπους συμμετεχόντων: data owners, network maintainers, data buyers, storage/compute providers [126].

- **Data owners:** Μπορεί να είναι ιδιώτες ή ιδρύματα. Αποθηκεύουν τα κρυπτογραφημένα γονιδιωματικά δεδομένα σε δημόσιο ή ιδιωτικό cloud το οποίο είναι μέρος συστήματος αποθήκευσης. Αυτοί είναι σε θέση να ελέγχουν την πρόσβαση στα δεδομένα τους και να λαμβάνουν πληρωμές στα πορτοφόλια τους από τους light clients στο Nebula blockchain.
- **Network maintainers:** Είναι διάφοροι οργανισμοί που λειτουργούν κόμβους επικύρωσης στο Nebula blockchain. Οι κόμβοι επικύρωσης, συλλογικά θα ελέγχουν την πρόσβαση στα δεδομένα, με τη διαχείριση των κλειδιών κρυπτογράφησης, επαλήθευση συναλλαγών και παρακολούθηση των δεδομένων που είναι αποθηκευμένα στο “KEEP” και υπολογισμών που εκτελέστηκαν από το “CRUNCH”.
- **Data buyers:** Είναι ερευνητές που επιθυμούν να αποκτήσουν πρόσβαση στα γονιδιωματικά δεδομένα. Λειτουργούν τους auditor nodes για να διατηρήσουν ένα τοπικό αντίγραφο των metadata, το οποίο θα χρησιμοποιήσουν για τον εντοπισμό δεδομένων που είναι αποθηκευμένα στο “KEEP” , για την επαλήθευση ακεραιότητας των δεδομένων και την παρακολούθηση των δικαιωμάτων πρόσβασης. Οι ίδιοι θα είναι σε θέση να υποβάλλουν ερωτήματα για ομομορφικά κρυπτογραφημένα δεδομένα, να χρησιμοποιούν έξυπνες συμβάσεις για την απόκτηση των δικαιωμάτων πρόσβασης στα δεδομένα, από τους data owners, και να χρησιμοποιούν το “ CRUNCH” για την εκτέλεση αγωγών ανάλυσης (pipelines).

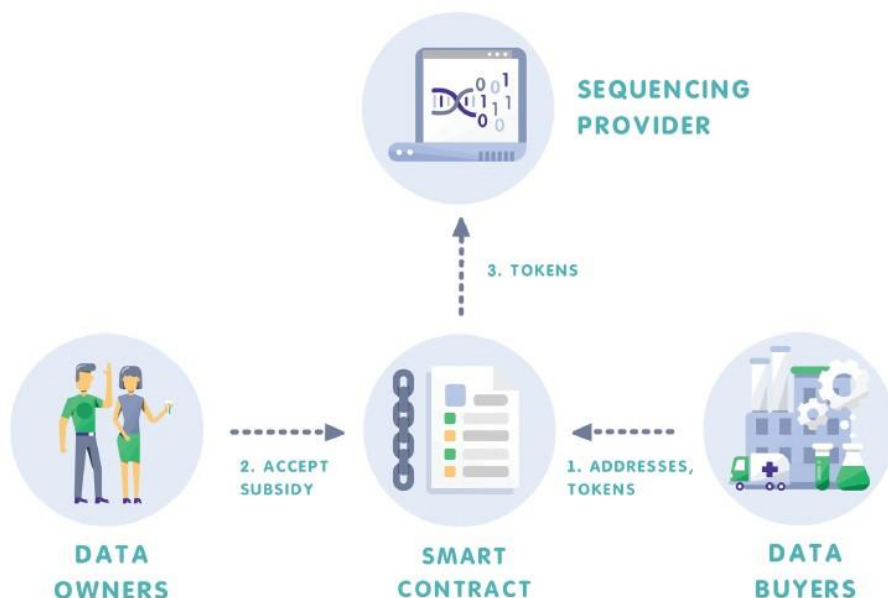
- **Storage and compute providers:** Είναι data owners που λειτουργούν ιδιωτικά clouds ή τρίτα μέρη που προσφέρουν υπηρεσίες αποθήκευσης και υπολογισμού (Google, Amazon, Microsoft). Οι ίδιοι θα σχηματίσουν ομοσπονδιακό περιβάλλον cloud , το οποίο φιλοξενεί το “KEEP storage system” και “CRUNCH-managed containers” , εντός των οποίων εκτελούνται οι υπολογισμοί.

3.6.2) Ροή εκτέλεσης του συστήματος NEBULA BLOCKCHAIN:

Παραγωγή δεδομένων

1) Γονιδιωματικά δεδομένα:

Όπως αναφέρθηκε και πιο πάνω, το κόστος αλληλουχίας του προσωπικού γονιδιώματος είναι ένας σημαντικός παράγοντας στην αποτροπή της ευρύτερης υιοθέτησης από τους καταναλωτές. Ως εκ τούτου, ένα βασικό ζήτημα στο σχεδιασμό της πλατφόρμας Nebula ήταν να παρέχει ένα μηχανισμό μετατόπισης της αλληλουχίας από τους data owners (καταναλωτές, βιοτράπεζες) στους data buyers (φαρμακευτικές εταιρείες). Αυτό έχει τεθεί σε εφαρμογή, επιτρέποντας στους data buyers να εξετάσουν τη Nebula βάση δεδομένων, να προσδιορίσουν τα σύνολα δεδομένων ενδιαφέροντος και να πληρώσουν το κόστος αλληλουχίας για τη δημιουργία και πρόσβαση των γονιδιωματικών δεδομένων [126].



Εικόνα 3.20: Επιδότηση πληρωμής για την αλληλουχία του γονιδιώματος στο blockchain [126]

Η πλατφόρμα Nebula επιτρέπει σε έναν data buyer να δημιουργήσει ένα έξυπνο συμβόλαιο που καθορίζει τις blockchain διευθύνσεις των data owners που είχαν προσδιοριστεί σε κάποιο ερώτημα και στέλνει κρυπτονομίσματα tokens σε αυτό το έξυπνο συμβόλαιο.

Οι data owners ειδοποιούνται πως ένας data buyer προσφέρθηκε να πληρώσει το κόστος αλληλουχίας τους.

Εάν ο data owner δεχτεί την προσφορά εκτελώντας το έξυπνο συμβόλαιο, τα κατατεθέντα tokens αποστέλλονται σε έναν πάροχο αλληλουχίας.

Στη συνέχεια, ο data owner παραλαμβάνει ένα κιτ συλλογής σάλιου και υποβάλλει δείγμα σάλιου. Το δείγμα είναι η αλληλουχία και τα γονιδιωματικά δεδομένα κατατίθενται σε έναν “KEEP server” που καθορίζεται από τον data owner.

Τα κατακερματισμένα δεδομένα, μαζί με τις διευθύνσεις blockchain όλων των data owners και data buyers, γράφονται στο blockchain.

Ο data buyer που πλήρωσε το κόστος της αλληλουχίας, έχει πλέον πρόσβαση στα δεδομένα και την ανάλυσή τους.

Ο data owner λαμβάνει τις ερμηνείες των γονιδιωματικών δεδομένων του και είναι σε θέση να μοιραστεί την πρόσβαση στα δεδομένα με επιπλέον data buyers.

2) Φαινοτυπικά δεδομένα:

Οι πληροφορίες που έχουν σχέση με τις ιατρικές παθήσεις και άλλα γνωρίσματα, αναφέρονται ως φαινοτυπικά δεδομένα. Αυτά τα δεδομένα δημιουργούνται κυρίως μέσω έρευνας που γίνεται με ερωτήσεις. Η πλατφόρμα Nebula ένα κιτ εργαλείων φαινοτύπου, που χαρτογραφεί τις απλές απαντήσεις της έρευνας σε κλινικές περιγραφές στην μορφή «Human Phenotype Ontology HPO», [138]. Τα δεδομένα της έρευνας μπορούν να επαληθευτούν με δύο προσεγγίσεις: με αναφορά στα EHRs που εισάγονται μέσω FHIR (Fast Healthcare Interoperability Resources) και με τη σύγκριση της συχνότητας εμφάνισης παθήσεων στο γενικό πληθυσμό με την επίπτωση που παρατηρείται στο σύνολο δεδομένων της πλατφόρμας.

Κρυπτογράφηση δεδομένων

Το απόρρητο των γονιδιωματικών και φαινοτυπικών δεδομένων προστατεύεται μέσω κρυπτογράφησης από τους data owners και μέσω διαχείρισης του κλειδιού κρυπτογράφησης από τους κόμβους επικύρωσης. Για να μπορέσουν οι data buyers να ανακαλύψουν δεδομένα πριν από την αγορά πρόσβασης στα δεδομένα, η πλατφόρμα δημιουργεί ένα πλέγμα βασισμένο σε ομομορφικό σχήμα κρυπτογράφησης. Για το σκοπό αυτό, οι κόμβοι επικύρωσης δημιουργούν ζεύγη κλειδιών και κατασκευάζουν από κοινού ένα μοναδικό κλειδί.

Οι data owners κρυπτογραφούν τις απαντήσεις έρευνας που έδωσαν και τις λίστες γενετικών παραλλαγών, με το μοναδικό κλειδί και τα ανεβάζουν στο διακομιστή “KEEP”.

Το ομομορφικό σχήμα κρυπτογράφησης προστατεύει το απόρρητο, επιτρέποντας στους data buyers να εκτελούν ερωτήματα τύπου SQL στα ομομορφικά κρυπτογραφημένα δεδομένα.

Αρχεία που περιέχουν ακατέργαστα δεδομένα αλληλουχίας και δεν χρησιμοποιούνται για ερωτήματα είναι κρυπτογραφημένα με AES (advanced encryption standard).

Αποθήκευση δεδομένων

Τα γονιδιωματικά δεδομένα αποθηκεύονται στο “KEEP”, ένα καταναμημένο, υβριδικό σύστημα αποθήκευσης με δυνατότητα διανομής περιεχομένου που ανακτά αρχεία με βάση το περιεχόμενό τους. Οι διευθύνσεις των αρχείων δημιουργούνται μέσω κρυπτογραφικής συγχώνευσης του περιεχομένου τους.

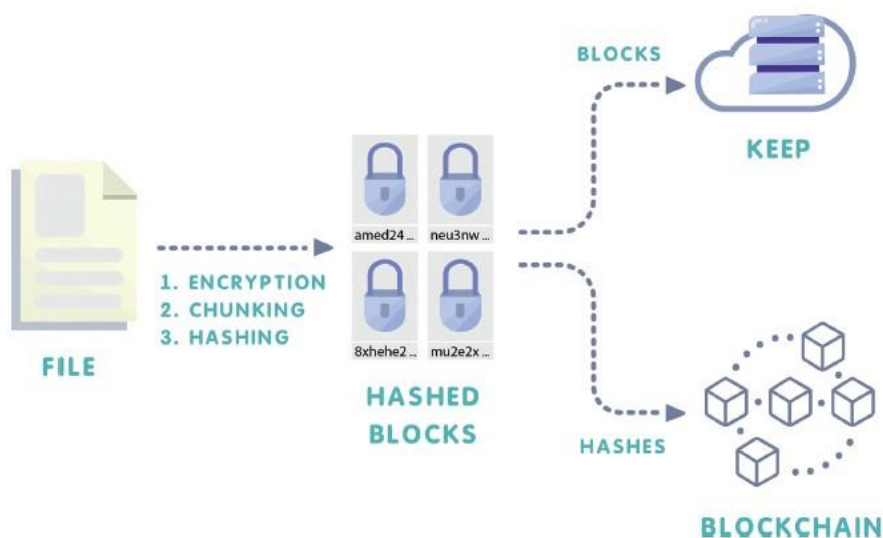
Το “KEEP” συνδυάζει την αντιμετώπιση του περιεχομένου με την αρχιτεκτονική καταναμημένης αποθήκευσης του Google File System [139].

Το “KEEP” διαχωρίζει τα κρυπτογραφημένα αρχεία σε 64-megabyte blocks και τα αποθηκεύει σε μια αποθήκη ή σε ένα σύστημα αρχείων, (Εικόνα 3.21).

Οι διευθύνσεις περιεχομένου των blocks αποθηκεύονται στο blockchain και χρησιμοποιούνται για την εύρεση τοποθεσιών των δεδομένων και ελέγχουν την ακεραιότητα των δεδομένων.

Το “KEEP” έχει σχεδιαστεί για την αποθήκευση των data blocks που περιέχουν γονιδιωματικά και άλλα βιοϊατρικά δεδομένα.

Οι data owners μπορούν να επιλέξουν να αποθηκεύσουν τα δεδομένα τους σε clouds, όπως το Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure ή σε ιδιωτικούς bare-metal διακομιστές, ή σε κοινόχρηστα clouds.



Εικόνα 3.21: Τα blocks δεδομένων αποθηκεύονται στο KEEP. Οι κατακερματισμοί αποθηκεύονται στο blockchain [126]

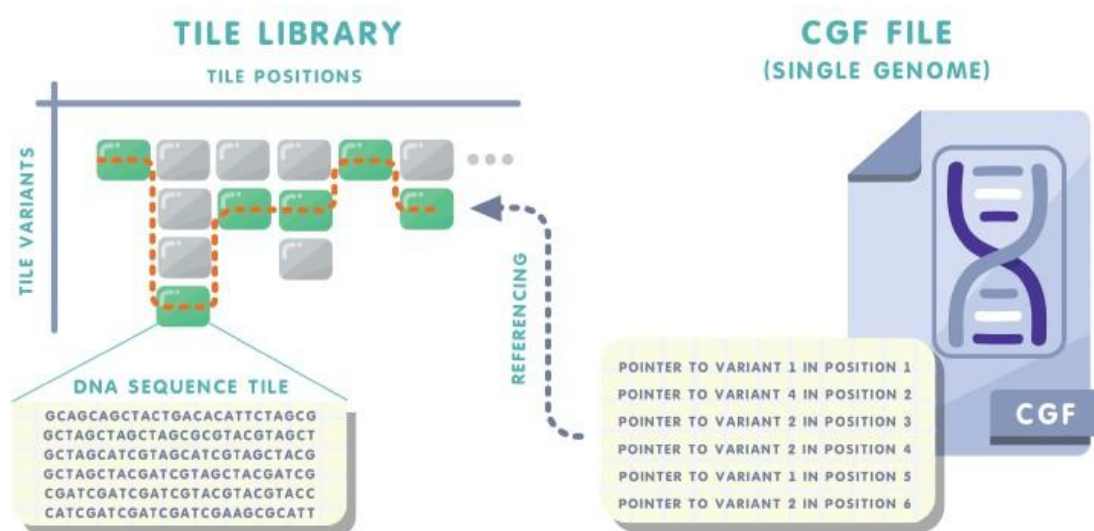
Καθώς τα δεδομένα αλληλουχίας υποβάλλονται σε επεξεργασία, δημιουργούνται διαφορετικές μορφές αρχείων οι οποίες αποθηκεύονται στο KEEP.

Τυπικά, το KEEP αποθηκεύει FASTQ αρχεία που περιέχουν ακατέργαστα δεδομένα αλληλουχίας (~ 200gigabytes/ γονιδίωμα), Binary Alignment Map αρχεία που αποθηκεύουν ευθυγραμμισμένες αναλύσεις αλληλουχίας (~ 100 gigabytes/ γονιδίωμα) και Variant Call Format αρχεία που αποθηκεύουν γενετικές παραλλαγές (~ 200gigabytes/ γονιδίωμα).

Επίσης, το NEBULA χρησιμοποιεί το Compact Genome Format (CGF), για τη δημιουργία συνοπτικών περιλήψεων γονιδιωματικών δεδομένων. Τα γονιδιωματικά δεδομένα σε μορφή CGF αντιπροσωπεύονται από δείκτες που αναφέρονται σε αλληλουχίες σε μια “tile library”, όπως φαίνεται στην εικόνα.

Το CGF προσφέρει μια σταθερή, τυποποιημένη αναπαράσταση γονιδιωματικών δεδομένων που δημιουργεί διαφορετικούς τύπους προσδιορισμού αλληλουχίας και γονότυπου για διαλειτουργικά δεδομένα.

Η CGF αναπαράσταση είναι πολύ αποδοτική στο χώρο, (~ 30gigabytes/ γονιδίωμα), το οποίο διευκολύνει τη μεταφορά αρχείων και επιτρέπει γρήγορες ερωτήσεις και αποτελεσματική ανάλυση [139].



Εικόνα 3.22: Απλοποιημένη παρουσίαση μιας “tile library” και ενός CGF αρχείου. Τα ορθογώνια αντιπροσωπεύουν παραλλαγές των tile διαφορετικών θέσεων. Η διακεκομμένη γραμμή απεικονίζει τη σύνθεση των tiles συγκεκριμένου γονιδιώματος [126]

Για την οργάνωση των δεδομένων που είναι αποθηκευμένα στο KEEP, ο NEBULA αποθηκεύει metadata στο blockchain, σε ένα αποθετήριο. Όταν τα νέα δεδομένα προστίθενται στο KEEP, ή τροποποιούνται τα υπάρχοντα δεδομένα, τότε δημιουργούνται συναλλαγές blockchain.

Οι κόμβοι επικύρωσης επιβεβαιώνουν αυτές τις συναλλαγές, προσθέτουν νέα blocks στο blockchain και ενημερώνουν το αποθετήριο. Η αποθήκευση των metadata στο αμετάβλητο ledger εξασφαλίζει την ακεραιότητα της αποκεντρωμένης βάσης δεδομένων Nebula.

Ανακάλυψη δεδομένων

Η χρήση της ομομορφικής κρυπτογράφησης προορίζεται για την αντιμετώπιση κινδύνων που αφορούν το απόρρητο κατά την κοινή χρήση των δεδομένων. Επιτρέπει στους data owners να διαθέσουν τα δεδομένα τους χωρίς κινδύνους, ενώ ταυτόχρονα επιτρέπει στους data buyers να

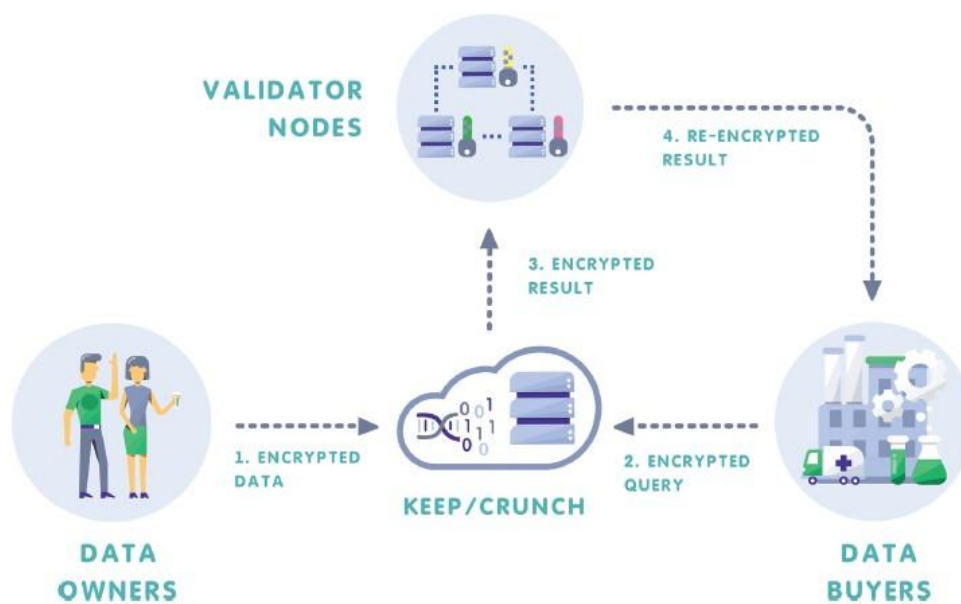
εξερευνήσουν τη βάση δεδομένων πριν από την αγορά πρόσβασης στα δεδομένα για την εκτέλεση αναλύσεων.

Για το σκοπό αυτό, οι data buyers θα κατασκευάσουν ένα SQL-like ερώτημα και θα το κρυπτογραφήσουν με το μυστικό κλειδί, το οποίο έχει κατασκευαστεί από τους κόμβους επικύρωσης και χρησιμοποιείται για την κρυπτογράφηση πληροφοριών φαινοτύπου και για τις γενετικές παραλλαγές.

Το κρυπτογραφημένο ερώτημα εκτελείται σε ομομορφικά κρυπτογραφημένα δεδομένα και δημιουργείται ένα κρυπτογραφημένο αποτέλεσμα.

Το αποτέλεσμα της ερώτησης επανακρυπτογραφείται από τους κόμβους επικύρωσης με το δημόσιο κλειδί του data buyer, ο οποίος μπορεί να το αποκρυπτογραφήσει με το ιδιωτικό του κλειδί.

Ένα ερώτημα μπορεί να επιστρέψει ως απάντηση τον αριθμό των data owners που ταιριάζουν με τα καθορισμένα κριτήρια, καθώς και τις blockchain διευθύνσεις τους. Αυτό επιτρέπει στους data buyers να συνδεθούν με τους data owners για να πληρώσουν το κόστος της αλληλουχίας, ή να αγοράσουν την πρόσβαση σε υπάρχοντα γονιδιωματικά δεδομένα [126].



Εικόνα 3.23: Ασφαλής ανακάλυψη δεδομένων μέσω ερωτημάτων στα ομομορφικά κρυπτογραφημένα δεδομένα [126]

Ανάλυση δεδομένων

Το Arvados container και η μηχανή διαχείρισης αγωγών, CRUNCH, εκτελεί υπολογισμούς σε δεδομένα που είναι αποθηκευμένα στο KEEP και τους διανέμει μεταξύ πολλών μονάδων επεξεργασίας.

Το CRUNCH εφαρμόζει ένα καταναμημένο υπολογιστικό μοντέλο με το οποίο οι ροές εργασίας και όχι τα δεδομένα, μετακινούνται όπου είναι δυνατό, μεταξύ διαφόρων cloud.

Το CRUNCH διασφαλίζει την αναπαραγωγικότητα των αποτελεσμάτων μέσω της τυποποίησης υπολογιστικών ροών εργασίας ,χρησιμοποιώντας την Common Workflow Language (CWL) [140].

Το CRUNCH μπορεί να έχει πρόσβαση σε CWL pipelines (αγωγούς) που είναι αποθηκευμένοι σε δημόσια ή ιδιωτικά αποθετήρια, όπως το Github.

Η CWL μπορεί να χρησιμοποιηθεί για την υλοποίηση από την αρχή μέχρι το τέλος της ανάλυσης και ερμηνείας των αγωγών βιοπληροφορικής, δηλαδή των γονιδιωματικών και φαινοτυπικών δεδομένων.

Οι χρήστες μπορούν να δημιουργήσουν τους δικούς τους αγωγούς για την ανάλυση των δεδομένων τους και να μοιραστούν μεταξύ τους αυτούς τους αγωγούς χρησιμοποιώντας δημόσια Git αποθετήρια.

Οι προγραμματιστές μπορούν να δημιουργήσουν γονιδιωματικές εφαρμογές. Για το σκοπό αυτό, οι CWL αγωγοί μπορούν να αποθηκευτούν σε ιδιωτικά αποθετήρια και η πρόσβαση από το CRUNCH μπορεί να απαιτήσει μια έξυπνη πληρωμή token με συμβόλαιο στον προγραμματιστή αγωγού (pipeline) [126].

Ασφάλεια δεδομένων

Οι περισσότεροι υπολογισμοί που είναι απαραίτητοι για τις τυπικές ροές εργασίας ανάλυσης των γονιδιωματικών δεδομένων δεν πετυχαίνουν πρακτικούς χρόνους εκτέλεσης όταν εκτελούνται σε ομοιομορφικά κρυπτογραφημένα δεδομένα. Για αυτό το λόγο θα πρέπει να χρησιμοποιηθούν άλλοι μηχανισμοί ασφαλείας.

- Έλεγχος πρόσβασης στην πλατφόρμα:

Για την προστασία των data owners και των δεδομένων τους, οι data buyers θα πρέπει να περάσουν από μια αποκεντρωμένη διαδικασία αδειών.

Ο κόμβος επικύρωσης blockchain θα επαληθεύσει την ταυτότητα του data buyer (authentication). Οι επαληθευμένες διευθύνσεις blockchain των data buyers θα προστεθούν στο αποθετήριο των metadata στο blockchain. Οι data buyers θα μπορούν τότε να συνδεθούν στους διακομιστές Nebula REST API και να χρησιμοποιήσουν το CRUNCH για την εκτέλεση των αγωγών στα δεδομένα , που είναι αποθηκευμένα στο KEEP.

Ο έλεγχος ταυτότητας του data buyer θα επιτρέψει στους data owners να επαληθεύσουν την ταυτότητα του data buyer, πριν συμφωνηθεί η κοινοποίηση της πρόσβασης στα δεδομένα. Επιπλέον, η αμετάβλητη αποθήκευση των ταυτοτήτων των data buyers στο blockchain, επιτρέπει την ταυτοποίηση των data buyers που έχουν παραβιάσει συμφωνίες ή έχουν παρακάμψει τον έλεγχο εκτέλεσης του αγωγού (pipeline).

- Έλεγχος εκτέλεσης αγωγού:

Για την προστασία του απορρήτου των δεδομένων, ο σχεδιασμός της πλατφόρμας ενσωματώνει την ικανότητα καθορισμού εγκεκριμένων εργαλείων βιοπληροφορικής και ροών εργασίας CWL. Ο σκοπός είναι να αποτραπούν οι data buyers από τη λήψη γονιδιωματικών δεδομένων ή την εκτέλεση οποιονδήποτε υπολογισμών που επιχειρούν να εξάγουν μεγάλο όγκο πληροφοριών σχετικά με τα δεδομένα μεμονωμένων ιδιοκτητών. Αυτή η προσέγγιση επιλέχθηκε διότι έχει την ικανότητα να παρέχει επαρκές επίπεδο προστασίας του απορρήτου των δεδομένων, χωρίς να περιορίζονται σημαντικά οι data buyers.

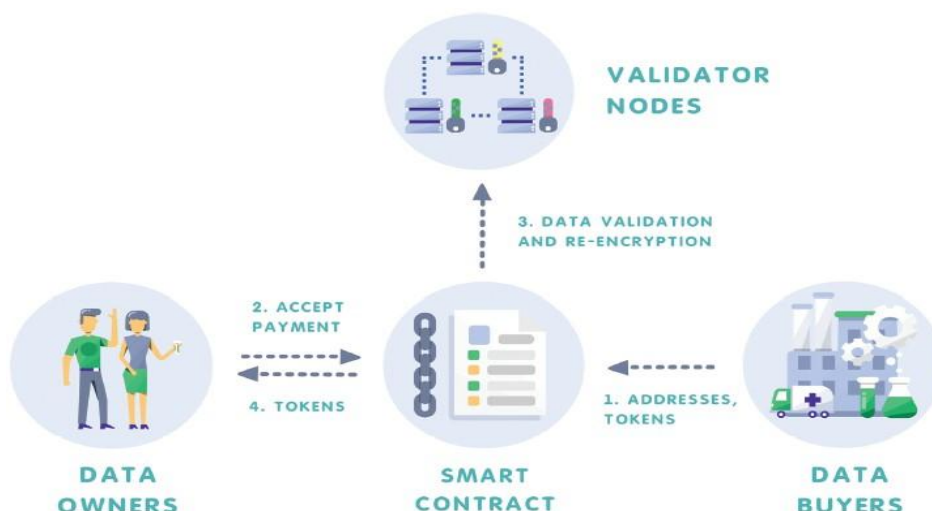
- Έλεγχος πρόσβασης στα δεδομένα:

Η πρώτη εργασία σε κάθε CWL αγωγό, είναι η πρόσβαση στα δεδομένα εισόδου (input data). Ο data buyer εκτελεί ένα έξυπνο συμβόλαιο στο blockchain. Τα δεδομένα εισόδου (inputs) είναι η blockchain διεύθυνση του data buyer και η διεύθυνση περιεχομένου όλων των δεδομένων των blocks των αρχείων εισόδου.

Ο data buyer καταθέτει tokens μέσα στο έξυπνο συμβόλαιο και καθορίζει μια token πληρωμή για πρόσβαση στα δεδομένα. Όταν ο πελάτης συγχρονίζεται με το blockchain, ο data owner ειδοποιείται για το αίτημα πρόσβασης στα δεδομένα. Ο data owner μπορεί να αποφασίσει σχετικά με την κοινή χρήση των δεδομένων, με βάση την προσφερόμενη πληρωμή και την ταυτότητα του αγοραστή.

Ο data owner παραχωρεί την πρόσβαση, εκτελώντας το έξυπνο συμβόλαιο. Οι κόμβοι επικύρωσης στη συνέχεια επαληθεύουν την ακεραιότητα των ζητούμενων δεδομένων, που είναι αποθηκευμένα στο KEEP, συγκρίνοντας τα κατακερματισμένα δεδομένα με τις διευθύνσεις περιεχομένου που είναι αποθηκευμένες στο blockchain και κρυπτογραφούν εκ νέου τα δεδομένα με το δημόσιο κλειδί του data buyer. Η άδεια πρόσβασης του data buyer είναι καταχωρημένη στο blockchain και τα tokens αποστέλλονται από το έξυπνο συμβόλαιο στο πορτοφόλι του data owner.

Το CRUNCH μπορεί τώρα να φορτώσει αποκρυπτογραφημένα δεδομένα σε ένα Docker container και να ξεκινήσει την εκτέλεση αγωγού [126].



Εικόνα 3.24: Έλεγχος πρόσβασης στα δεδομένα και αγορά δεδομένων [126]

3.7) Βελτίωση ποιότητας Κλινικών Δοκιμών (Clinical research quality)

Η ανταλλαγή δεδομένων, οι ανησυχίες περί προστασίας της ιδιωτικής ζωής και η εγγραφή ασθενών σε κλινικές δοκιμές, είναι τεράστιες ιατρικές προκλήσεις για τη σύγχρονη κλινική έρευνα. Μέσω της τεχνολογίας Blockchain μπορούν να αντιμετωπιστούν αυτές οι προκλήσεις, καθώς επιτρέπει την επίτευξη σημαντικού επιπέδου ιστορικότητας, ανιχνευσιμότητας, αναπαραγωγικότητας και απαραβίαστου των δεδομένων για ολόκληρη τη ροή εγγραφών σε μια κλινική δοκιμή και επιτρέπει την ασφαλή αυτοματοποίησή της μέσω των Έξυπνων Συμβολαίων (smart contracts).

Η έλλειψη αναπαραγωγικότητας, η οποία συνδέεται με ένα ευρύ φάσμα επιστημονικών, παραπλανητικών πτυχών, από σφάλματα μέχρι και απάτες, διακυβεύουν τα αποτελέσματα μιας κλινικής μελέτης και υπονομεύουν την ποιότητα της έρευνας. Πολλές από τις ιατρικές επιστημονικές δημοσιεύσεις έχουν βρεθεί στο σύνολό τους ότι δεν αναπαράγονται, διότι είναι γεμάτες σφάλματα. Ο Έλληνας επιστήμονας κ. Ιωαννίδης υπολόγισε ότι περίπου το 80% των μελετών δεν μπορούν να αναπαραχθούν (μη αναπαραγωγικές μελέτες) [141]. Αυτό το ποσοστό μπορεί να σχετίζεται με διάφορους τύπους σφαλμάτων, παραπτωμάτων ή και απάτης.

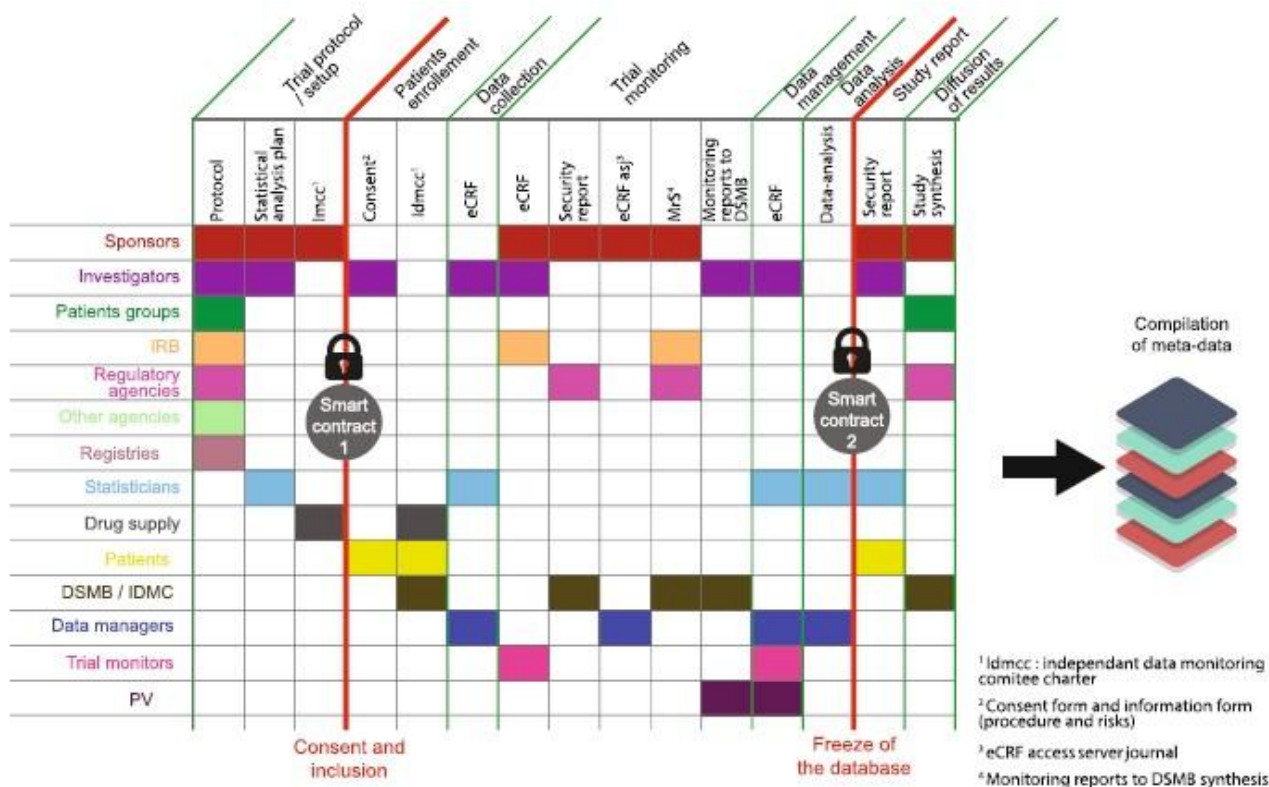
Το blockchain έχει παγκόσμιο αντίκτυπο στην κλινική έρευνα, διότι επιτρέπει την παρακολούθηση, την κοινή χρήση, τη διαφάνεια και την φροντίδα των δεδομένων και μπορεί να θεωρηθεί ως βάση για τη βελτίωση της μεθοδολογίας της κλινικής έρευνας και της εμπιστοσύνης μεταξύ των κοινοτήτων των ερευνητών και των ασθενών.

Για την επίτευξη αξιόπιστων κλινικών μελετών, σε κάθε βήμα είναι απαραίτητη η παρακολούθηση και χρονική σήμανση των δεδομένων και όλων των συναλλαγών που πραγματοποιούνται στο blockchain. Η ύπαρξη των δεδομένων γίνεται ευαπόδεικτη ενώ τα δεδομένα παραμένουν εμπιστευτικά.

Επίσης, σε μια πειραματική μελέτη, πρόκληση αποτελεί και η συλλογή συγκατάθεσης (consent collection) του συμμετέχοντος για μια κλινική δοκιμή [142]. Η Αμερικανική Υπηρεσία Τροφίμων και Φαρμάκων, αναφέρει ότι το 10% των δοκιμών που παρακολουθούν τα χαρακτηριστικά γνωρίσματα που σχετίζονται με τη συλλογή συγκατάθεσης έχουν: α) αδυναμία λήψης γραπτής ενημερωμένης συγκατάθεσης, β) μη εγκριθέντα έντυπα, γ) μη έγκυρο έγγραφο συγκατάθεσης, δ) αδυναμία εκ νέου συγκατάθεσης σε αναθεωρημένο πρωτόκολλο και ε) έλλειψη έγκρισης από το διοικητικό συμβούλιο για την αναθεώρηση των πρωτοκόλλων.

Σε μια ψεύτικη πειραματική μελέτη, οι επιστήμονες έδωσαν χρονική σήμανση για κάθε συγκατάθεση του ασθενούς στο blockchain και έπειτα ζήτησαν ξανά την ανανέωση της συναίνεσης με κάθε αναθεώρηση του πρωτοκόλλου. Οι επιστήμονες έλαβαν ένα βασικό μοναδικό έγγραφο, που περιέχει σε μια ενιαία δομή δεδομένων ή κομμάτι κώδικα που ονομάζεται “Chain script”, ολόκληρη τη συλλογή δεδομένων συγκατάθεσης, έκαστο δε δεσμεύεται σε μια έκδοση αναθεωρημένων πρωτοκόλλων. Στην πραγματικότητα αυτά τα δεδομένα είναι κατακερματισμένα. Αυτό το βασικό μοναδικό έγγραφο αποτελεί μια ασφαλή και ισχυρή απόδειξη ολόκληρης της διαδικασίας συλλογής συναίνεσης, λόγω της αυστηρής «αλληλογραφίας» μεταξύ των κατακερματισμένων δεδομένων που έχουν χρωθεί και των δεδομένων αποτελεσματικής συναίνεσης [143].

Στην παρακάτω εικόνα θα δούμε τις σύνθετες ροές ετερογενών δεδομένων και μεταδεδομένων, που συναντώνται σε μια κλινική δοκιμή, όπως επίσης και τους ενδιαφερόμενους της υγειονομικής περίθαλψης και όλα τα έγγραφα των οποίων η απόδειξη ύπαρξης μπορεί να αποθηκευτεί στο Blockchain [143].



Εικόνα 3.25: Ροή εργασίας σύνθετων κλινικών δοκιμών κωδικοποιημένη σε blockchain [143].

3.7.1) Ροή εκτέλεσης του συστήματος

Πριν ξεκινήσει η κλινική δοκιμή, γνωστοποιείται το « *data sharing plan* », το οποίο περιλαμβάνει α) το πρόγραμμα (schedule), β) την τεκμηρίωση του συνόλου δεδομένων, (dataset documentation) και γ) τη συμφωνία για την κοινή χρήση δεδομένων (data sharing agreement) εάν υπάρχει. Αυτά τα μεταδεδομένα (*metadata*) μπορούν να έχουν χρονική σήμανση (time stamped) με χρονολογική σειρά.

Επίσης, πριν ξεκινήσει η κλινική δοκιμή, οι «*consents*» (συναινέσεις) και το «*clinical trial protocol*» (πρωτόκολλο κλινικής δοκιμής), συμπεριλαμβανομένων α) είδος μελέτης, β) πρωτογενή/ δευτερογενή αποτελέσματα, γ) κριτήρια συμπερίληψης και αποκλεισμού, μπορούν να συνδυαστούν σε δομές δεδομένων (data structures) που είναι αποθηκευμένες στο blockchain [144].

Οι «*data structures*» έπειτα είναι σε μία προς μία αλληλογραφία με τις συναινέσεις και το πρωτόκολλο, γεγονός που συνιστά έντονη απόδειξη της ύπαρξής του.

Στο σύνολο των μεταδεδομένων μπορούν να αποθηκευτούν πληροφορίες, όπως : α) ο τρόπος συλλογής των δεδομένων, β) η μέθοδος κατανομής, γ) οι ημερομηνίες των επαναλαμβανόμενων γεγονότων, δ) οι ημερομηνίες των αποσύρσεων.

Το «*statistical analysis plan*» είναι μια κρίσιμη ανάγκη και είναι με χρονική σήμανση, δηλαδή χρονολογείται πριν από την ολοκλήρωση της ανάλυσης και προτού αποκαλυφθούν τα δεδομένα. Το «*statistical analysis plan*» περιλαμβάνει α) τις στατιστικές μεθόδους (*statistical methods*), β) τον ορισμό των συμβάντων βλάβης (*definition of harm events*) και γ) πολλαπλές μεταβλητές προσαρμογής (*multiple variable adjustments*), εάν υπάρχουν.

Οι ερευνητικές ομάδες συχνά δεν έχουν ιδέα για τα αποτελέσματα, οπότε είναι δύσκολη η εκ των προτέρων εκτίμηση της απαιτούμενης ισχύος, γεγονός που οδηγεί σε εκ των υστέρων μεροληψία του λογισμικού. Η απεικόνιση ενός συνόλου μεταδεδομένων με χρονική σήμανση στο blockchain, θα περιλάμβανε : *sample size* (μέγεθος του δείγματος), *type1/ type2 errors*, εκτιμώμενο ποσοστό συμβάντων, επίδραση θεραπείας. Η χρονική σήμανση (*time stamping*) θα αποτελέσει ορόσημο στο blockchain που θα πιστοποιεί το μέγεθος του δείγματος εκ των προτέρων [143].

Ο αναλυτικός κώδικας θα πρέπει να μοιράζεται και να είναι ανοιχτός για την αποφυγή σφαλμάτων [145]. Λαμβάνοντας υπόψη ότι τα σενάρια συνεχίζουν να εξελίσσονται και ότι για τη διεκπεραίωση των δεδομένων χρησιμοποιείται ένας κώδικας που δεν αλλάζει, αυτή η κατάσταση του κώδικα πρέπει να φέρει χρονική σήμανση και να εξασφαλίσει ότι οι συνθήκες υπό τις οποίες τα δεδομένα ελέγχθηκαν και αναλύθηκαν είναι αναπαραγωγίσιμα. Ο κώδικας που φέρει χρονική σήμανση είναι για τη σημερινή κατάσταση η μόνη ισχυρή μη αναστρέψιμη μέθοδος χρονοσήμανσης [143].

Το «*smart contract*» (έξυπνο συμβόλαιο), αντιπροσωπεύει ένα κομμάτι κώδικα, το οποίο διατηρεί γραπτά συμβόλαια μεταξύ πολλών μερών, όπως απαιτείται , χωρίς αξιόπιστο τρίτο μέρος και εκτελείται αλγοριθμικά με τους όρους που συμφώνησαν τα συμβαλλόμενα μέρη. Τα έξυπνα συμβόλαια επιτρέπουν την ένταξη ασθενών στο blockchain, με τη μόνη προϋπόθεση ότι έχουν συναινέσει. Επίσης τα έξυπνα συμβόλαια χρησιμοποιούνται για την ενεργοποίηση της ανάλυσης δεδομένων με τη μόνη προϋπόθεση ότι η βάση δεδομένων δεν θα αλλαχθεί [143].

Καθένα από τα βήματα της κλινικής δοκιμής που περιγράφονται στην παραπάνω εικόνα, μπορεί να αλυσοδεθεί μαζί με μια σειρά που προηγείται, εδραιώνοντας μια διαφανή δοκιμή και αποτρέποντας την εκ των υστέρων αναπροσαρμογή των δεδομένων.

3.8) Γεωχωρικές εφαρμογές για έξυπνες υγιείς πόλεις (Geospatial application for smart healthy cities)

Το IoT είναι το θεμέλιο των έξυπνων υγείων πόλεων και περιοχών του σήμερα και του αύριο. Για να επιτευχθεί η βελτίωση της ευημερίας και της ποιότητας ζωής των πολιτών, το IoT δημιουργεί και καταναλώνει μεγάλα ευπροσάρμοστα ποσά δεδομένων. Αυτά τα δεδομένα και η επεξεργασία τους μπορούν να επωφεληθούν σε μεγάλο βαθμό από το blockchain και τις σχετικές τεχνολογίες.

Πολλές τρέχουσες προσφορές ανοιχτών δεδομένων είναι centralized , όπως το “UK Ordnance Survey map data” (OSMaps), τα οποία είναι τα δεδομένα χαρτών του OSMaps στο Ηνωμένο Βασίλειο, που αν και είναι δωρεάν στους τελικούς χρήστες, χρηματοδοτούνται από τους φορολογούμενους. Οι IoT εφαρμογές συχνά βασίζονται σε τρίτους για τα γεωχωρικά στοιχεία τους, όπως είναι το OSMaps ή Google Maps. Με την πρόσβαση σε καταμεμημένα δεδομένα τύπου blockchain, αυτές οι εφαρμογές μπορούν να γίνουν πιο αξιόπιστες και φθηνότερες για να λειτουργήσουν και να διατηρηθούν [2]. Με τα ανοιχτά δεδομένα τύπου blockchain κανείς δεν μπορεί να περιορίσει την πρόσβαση σε αυτά , σε αντίθεση με ένα κεντρικό σύστημα. Επίσης, το κόστος μπορεί να περιοριστεί στο ελάχιστο, χάρη στον ανοιχτό χαρακτήρα των ανταγωνιστικών κόμβων και των οντοτήτων που συνεισφέρουν. Οι συνεισφέροντες γεωχωρικά δεδομένα μπορούν να επιβραβευθούν με κάποια μορφή tokens και να τηρηθεί δημόσιο αρχείο για όλες τις συναλλαγές και τις συνεισφορές που έγιναν [2].

Η αγορά IoT συσκευών και εφαρμογών, που διαπραγματεύονται και πληρώνουν αμοιβαία για ασφάλεια λειτουργιών και υπηρεσιών αναμένεται να χρησιμοποιηθούν από το κοινό στο εγγύς μέλλον. Κάποια από αυτά είναι αυτόνομες συνδεδεμένες συσκευές και έξυπνα οχήματα για αντιμετώπιση σε επείγουσα κατάσταση, όπως είναι : αυτοκινούμενο ασθενοφόρο ή ελικόπτερο, απινιδωτής σε drone και drone για τη μεταφορά ιατρικών αγαθών και φαρμάκων [146].

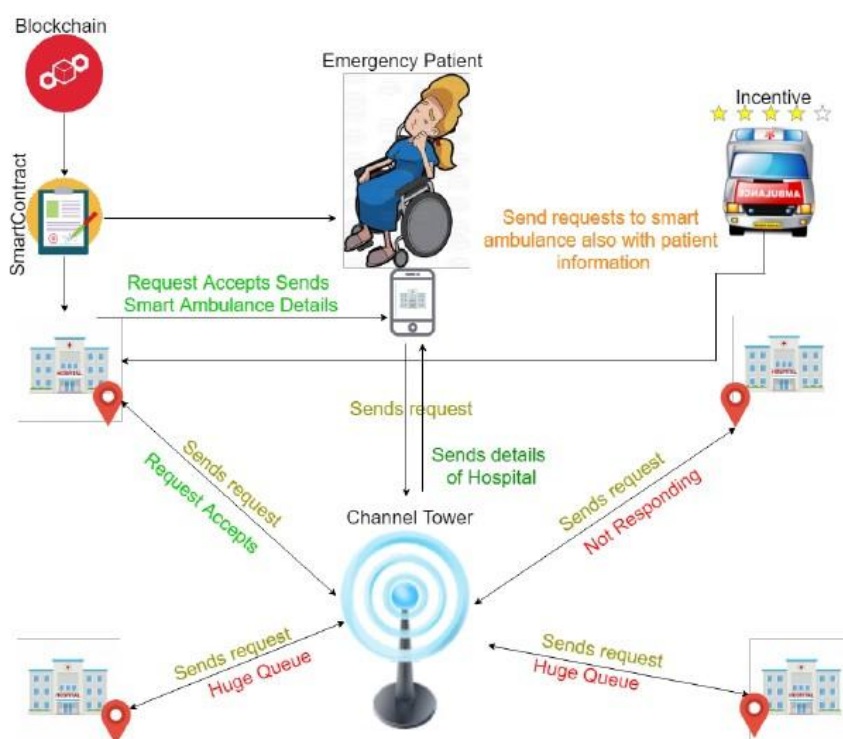
Οι καταμεμημένες εφαρμογές peer-to-peer που τροφοδοτούν αυτά τα έξυπνα οχήματα ή έξυπνα drones, θα αποκόψουν τον μεσάζοντα και την εξάρτηση από τρίτους παρόχους πλοήγησης και άλλα γεωχωρικά δεδομένα [146]. Ένα καλά σχεδιασμένο blockchain μπορεί να μετριάσει την πιθανότητα ενός αυτόνομου οχήματος που τροφοδοτείται από IoT , να πειραματιστεί και να βρεθεί σε λάθος θέση. Αν εξετάσουμε τα δεδομένα που μεταφέρουν τις οδηγίες στο όχημα ως συναλλαγές και το δίκτυο βρίσκεται σε ένα blockchain, τότε η διαδικασία συναίνεσης θα βοηθήσει στην επικύρωση αυτών των συναλλαγών, στην παγίδευση οποιωνδήποτε παράνομων και στην απομάκρυνση των λανθασμένων οδηγιών που φέρουν [2].

Η εμπλοκή των πολιτών στη συλλογή των γεωχωρικών δεδομένων μπορεί να συνδυαστεί με A.R. (επαυξημένη πραγματικότητα) και την τεχνολογία blockchain, σε ισχυρά νέα σενάρια χαρτογράφησης και ανάκαμψης μιας κρίσης που μπορεί να συμβαίνει. Θα μπορούσαμε να αναφερθούμε στο παράδειγμα όπου παράγεται και ενημερώνεται σε πραγματικό χρόνο ένας επαυξημένος χάρτης κρίσης για την πλοήγηση σε μια περιοχή που έχει πληγεί από καταστροφές. Τα αντικείμενα A.R. με γεωγραφική σήμανση παρέχουν χρήσιμες πληροφορίες και συμβουλές και τοποθετούνται επάνω στην πραγματική «σκηνή» στο Smartphone του χρήστη. Ο χρήστης θα ενημερωθεί από μηνύματα όπως : «Μην οδηγείτε! Πεσμένα καλώδια στο δρόμο!» όταν πλησιάζει σε μια πλημμυρισμένη περιοχή [2].

Η υλοποίηση «FOAM» είναι ένα καλό παράδειγμα ενός blockchain που ενεργοποιείται με βάση το γεωγραφικό περιβάλλον, χρησιμοποιώντας κρυπτο-χωρικό σύστημα συντεταγμένων «CSC system» (crypto-spatial coordinate system). Ένα FOAM blockchain δεν καταγράφει μόνο τη συγκεκριμένη χρονική στιγμή μιας εισόδου, αλλά απαιτεί και επικυρώνει την απόδειξη της θέσης του, δίνοντας ένα αμετάβλητο χωρικό πλαίσιο που δεν διαθέτουν τα κανονικά blockchains και επιτρέποντας την ακριβή χαρτογράφηση των φυσικών γεγονότων σε μια χρονική ακολουθία, [147].

Στη συνέχεια θα μελετήσουμε το έξυπνο ασθενοφόρο και τον απινιδωτή σε drone.

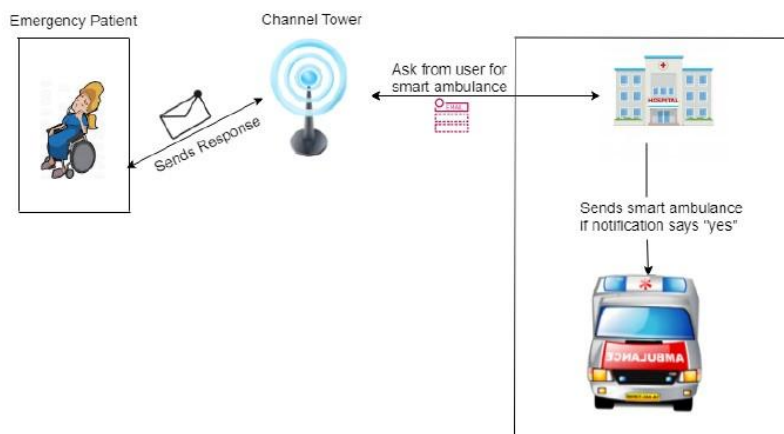
3.8.1) Έξυπνο Ασθενοφόρο



Εικόνα 3.26: Προτεινόμενο μοντέλο [148].

Όταν ένας ασθενής υποβάλλει αίτημα μέσω της έξυπνης συσκευής του για επείγουσα θεραπεία, το αίτημα αποστέλλεται μέσω καναλιού/ διακομιστή στα πλησιέστερα νοσοκομεία. Στην απάντηση του αιτήματος, ο ασθενής θα λάβει πληροφορίες για το πιο κοντινό νοσοκομείο με ελάχιστη ή καθόλου ουρά αναμονής από άλλους ασθενείς έκτακτης ανάγκης που έχουν ήδη φτάσει.

Όταν κάποιο νοσοκομείο ανταποκριθεί στο αίτημα του ασθενή, τότε ο ασθενής και το νοσοκομείο υπογράφουν το έξυπνο συμβόλαιο και το νοσοκομείο δεν θα φανερώσει ποτέ το δημόσιο κλειδί του ασθενούς και το ιατρικό του ιστορικό. Έτσι διασφαλίζεται η ασφάλεια των αρχείων του ασθενούς.



Εικόνα 3.27: Ανάγκη για ασθενοφόρο ή όχι [148]

Στη συνέχεια το νοσοκομείο θα ρωτήσει τον ασθενή για την υπηρεσία του έξυπνου ασθενοφόρου. Εάν κάποιος ασθενής δεχτεί την S.A. (smart ambulance) υπηρεσία τότε το αίτημα θα σταλεί στο ασθενοφόρο και το νοσοκομείο θα στείλει το κοντινότερο ασθενοφόρο στη διεύθυνση του ασθενούς, όπως φαίνεται στην πάνω εικόνα.

Έπειτα το νοσοκομείο θα στείλει τις λεπτομέρειες του έξυπνου ασθενοφόρου και ο ασθενής θα συνδεθεί απευθείας με αυτό. Το νοσοκομείο θα καθοδηγήσει το έξυπνο ασθενοφόρο για την πρώτη επαφή με τον ασθενή. Το έξυπνο ασθενοφόρο περιορίζεται στο να διατηρήσει το ιατρικό ιστορικό και όλες τις πληροφορίες του ασθενή μόνο στο ασθενοφόρο και σε κανέναν άλλο. Το ιατρικό ιστορικό αποθηκεύεται χρησιμοποιώντας την αρχιτεκτονική blockchain, διότι εξασφαλίζεται η διαφάνεια, η ασφάλεια και η προστασία. Ο ασθενής στη συνέχεια θα δώσει βαθμολογία (ratings) στο ασθενοφόρο σύμφωνα με τις υπηρεσίες που του προσφέρθηκαν. Η βαθμολογία βελτιώνει το προτεινόμενο σύστημα του έξυπνου ασθενοφόρου [148].

Τα πειραματικά αποτελέσματα δείχνουν ότι το προτεινόμενο blockchain σύστημα είναι πιο αποτελεσματικό για υπηρεσίες θεραπείας έκτακτης ανάγκης.

3.8.2) Απινιδωτής σε drone

Όταν η ζωή ενός ανθρώπου βρίσκεται σε κατάσταση έκτακτης ανάγκης, τα πρώτα λεπτά είναι ζωτικής σημασίας για την παροχή της σωστής φροντίδας και την πρόληψη της κλιμάκωσης. Στην Ευρωπαϊκή Ένωση, ετησίως, περίπου 800.000 άνθρωποι πάσχουν από καρδιακή ανακοπή, με ποσοστό επιβίωσης μόνο 8%, κυρίως λόγω του αργού χρόνου απόκρισης των υπηρεσιών υγείας (10 λεπτά). Ο εγκεφαλικός θάνατος αρχίζει να εμφανίζεται σε μόλις 4 έως 6 λεπτά οδηγώντας σε θάνατο, [149]. Με την επιτάχυνση της αντιμετώπισης έκτακτης ανάγκης, οι πάροχοι υγειονομικής περίθαλψης μπορούν να αποτρέψουν πιθανούς θανάτους και να επιταχύνουν τη θεραπεία των ασθενών. Ένα βοηθητικό αεροσκάφος εφοδιασμένο με τεχνολογία διάσωσης, όπως αυτοματοποιημένο εξωτερικό απινιδωτή (AED), φάρμακα και βοηθήματα καρδιοπνευμονικής ανάνηψης (CPR), θα μπορούσε ενδεχομένως να φέρει την επανάσταση στην αντίδραση έκτακτης

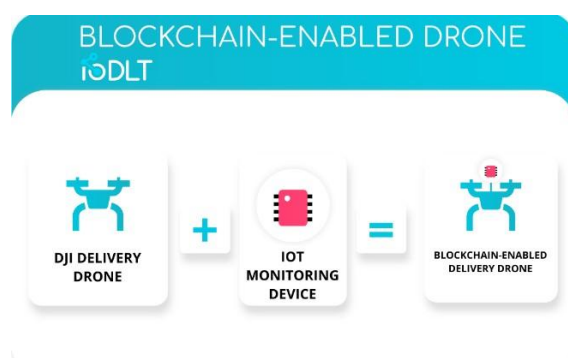
ανάγκης. Ένα ασθενοφόρο χρειάζεται κατά μέσο όρο 10 λεπτά για να φτάσει σε έναν ασθενή με καρδιακή ανακοπή και η πιθανότητα επιβίωσης είναι μόνο 8%. Το drone απινιδωτής μπορεί να προσεγγίσει οποιοδήποτε ασθενή σε ακτίνα 5 μιλίων, σε λιγότερο από 1 λεπτό και μπορεί να πετάξει με ταχύτητα έως και 100 km ανά ώρα παρακολουθώντας τις κλήσεις έκτακτης ανάγκης μέσω GPS για την πλοήγησή [149].



Η FAA προβλέπει ότι η εμπορική αγορά drone θα τριπλασιαστεί τα επόμενα χρόνια, φτάνοντας τα 835.000 μίνι αεροσκάφη έως το 2023. Με χιλιάδες μίνι αεροσκάφη στον ουρανό, θα υπάρξουν ευκαιρίες και προκλήσεις που θα πρέπει να ληφθούν υπόψη. Χωρίς τον κατάλληλο έλεγχο, με παρακολούθηση και ασφάλεια, η τεχνολογία drone θα μπορούσε να δημιουργήσει περισσότερο κακό παρά καλό. Κάθε κατασκευαστής drone ελέγχει καθένα από αυτά μέσω των δικών του πρωτοκόλλων και δεν είναι σε θέση αποτελεσματικά και με ασφάλεια να επικοινωνήσει με άλλα drones. Για τους κανονισμούς του εναέριου χώρου, αυτό θα μπορούσε να δημιουργήσει πρόβλημα για τα αεροσκάφη που θα πετούσαν ταυτόχρονα. Υπάρχει επίσης η πιθανότητα να παραβιαστεί η αρχιτεκτονική backend. Τα drones πρέπει να είναι σε θέση να επικοινωνούν με ασφάλεια μεταξύ τους, ανεξάρτητα από το εμπορικό τους σήμα. Η διαλειτουργικότητα μεταξύ των συσκευών είναι απαραίτητα για το μέλλον των IoT. Επίσης, κακόβουλοι χρήστες μπορεί να εκμεταλλευτούν τα drones μέσω της εισβολής και του κακόβουλου λογισμικού [150]. Χρησιμοποιώντας την τεχνολογία blockchain μπορούμε να επιλύσουμε τα προαναφερθέντα προβλήματα και επίσης να αναδείξουμε την πραγματική έννοια του IoT, μέσω μιας πλήρους κατανομημένης, ανθεκτικής και ανεκτικής σε σφάλματα και λύσης. Μια συσκευή IoT πολλαπλών χρήσεων μαζί με το blockchain, θα είναι υπεύθυνη για τη διευκόλυνση όλων των αλληλεπιδράσεων των drones. Αυτή η συσκευή IoT επικοινωνεί απευθείας στο blockchain χωρίς ενδιάμεσους διακομιστές για να εξασφαλιστεί η πλήρης ασφάλεια. Το blockchain συνδυάζει πολλές πτυχές μιας καλής λύσης: αποκέντρωση, ασφάλεια, επεκτασιμότητα. Εκτός από το ότι είναι αρχιτεκτονικά υγιές, το blockchain λειτουργεί ως επαληθευτής όλων των πληροφοριών που του αποστέλλονται. Μέσω μοναδικών κρυπτογραφικών κλειδιών, αυτό επιτρέπει την εύκολη επαλήθευση και εγγραφή ψηφιακών ταυτοτήτων, υπογραφών και ιδιοκτησίας σε μορφή τύπου καθολικού (ledger). Οι λήψεις των αισθητήρων, οι αναλύσεις, τα δεδομένα διαδρομής των drones Μπορούν επίσης να υπογραφούν αμετάβλητα στο blockchain, αφήνοντας πίσω ένα μόνιμο ίχνος [150].

Η τεχνολογία βασίζεται σε ένα έξυπνο συμβόλαιο blockchain, ως μηχανισμός που παρέχει μοναδικότητα και αμετάβλητο, ως μια ασφαλή και αξιόπιστη πηγή επικύρωσης. Τα έξυπνα συμβόλαια είναι κωδικοί γραμμένοι σε ένα δίκτυο blockchain, το οποίο ορίζει όρους συμφωνίας και όταν επιτευχθεί συναίνεση επιτρέπει την ενεργοποίηση των όρων. Καθώς η συσκευή IoT έχει

ήδη διαμορφωθεί για να λειτουργήσει απευθείας με το blockchain, χρειάζεται απλώς η είσοδος αισθητήρα από εξωτερική πηγή. Σε αυτή την περίπτωση, το drone απινιδωτής θα παρέχει όλες τις πληροφορίες στη συσκευή IoT, συμπεριλαμβανομένων των γεωχωρικών και άλλων δεδομένων ToF (Time of Flight), της τηλεμετρίας πτήσης και του ταξιδιού. Το DJI έχει δημιουργήσει μια σειρά από drones που είναι ήδη σε θέση να επικοινωνούν απευθείας με τη συσκευή IoT, μέσω σειριακής επικοινωνίας. Το DJI διαθέτει επίσης ένα ισχυρό OnBoard SDK, το οποίο δίνει πλήρη πρόσβαση σε όλες τις δυνατότητες του drone, τους αισθητήρες και τον εσωτερικό ελεγκτή πτήσης. Σε συνδυασμό με μια συμβατή συσκευή IoT, τα drones είναι έτοιμα να διαμορφωθούν σε απινιδωτές drone με ενσωματωμένη τεχνολογία blockchain [150].



Εικόνα 3.28: Το drone ενσωματώνεται με μια συσκευή IoT, επιτρέποντάς της να έχει πλήρεις δυνατότητες blockchain [150].

3.9) Νευροεπιστήμες (Neuroscience)

Οι σύγχρονες νευρωνικές τεχνολογίες επιδιώκουν να διαμορφώσουν ένα νέο παράδειγμα που αποκλείει τη μηχανική αλληλεπίδραση με τη γύρω υποδομή και επιτρέπει σε κάποιον να ελέγχει συσκευές και δεδομένα μέσω διανοητικών εντολών. Αυτές οι νευρωνικές συσκευές μπορούν να ερμηνεύσουν τα μοτίβα της εγκεφαλικής δραστηριότητας και να τα μεταφράσουν σε εντολές για τον έλεγχο εξωτερικών συσκευών, καθώς και για την ανίχνευση της τρέχουσας ψυχικής κατάστασης ενός ατόμου, με βάση τα δεδομένα της εγκεφαλικής του δραστηριότητας.

Το ειδικό καθήκον της ανάγνωσης και της ερμηνείας εγκεφαλικών σημάτων επιλύεται από συσκευές νευρωνικής διεπαφής (neural interface devices), εξοπλισμένες με αρκετούς αισθητήρες, υπολογιστικά τσιπ και ασύρματη επικοινωνία. Αυτές οι συσκευές διαβάζουν την ηλεκτρική δραστηριότητα του εγκεφάλου, η οποία αποκρυπτογραφείται περαιτέρω και μεταδίδεται στον υπό έλεγχο εξοπλισμό.

Οι αλγόριθμοι και τα μεγάλα δεδομένα θα χρησιμοποιηθούν από το blockchain για την αποθήκευση αυτών των εγκεφαλικών σημάτων στην νευρωνική διεπαφή.

Μια από τις εταιρείες που επιβεβαιωμένα χρησιμοποιούν τεχνολογία blockchain είναι η *Neurogress* [151]. Με έδρα στη Γενεύη, ιδρύθηκε το 2017 και η εταιρεία επικεντρώνεται στη

δημιουργία συστημάτων νευρωνικού ελέγχου, επιτρέποντας στους χρήστες να ελέγχουν ρομποτικούς βραχίονες, drones, έξυπνες συσκευές, συσκευές AR και VR, με τις δικές τους σκέψεις.

Το σύστημα ελέγχου Neurogress βασίζεται στη χρήση της μηχανικής μάθησης (machine learning) για τη βελτίωση ανάγνωσης του εγκεφάλου με ακρίβεια, κάτι που απαιτεί τη διατήρηση του 90% των δεδομένων του εγκεφάλου, προκειμένου να εκπαιδεύσει την τεχνητή νοημοσύνη (AI) που χρησιμοποιείται από το σύστημα. Με άλλα λόγια, απαιτούνται τα μεγάλα δεδομένα της νευρικής δραστηριότητας των χρηστών, για την ανάγκη του προγράμματος “Human Brain” για exabytes μνήμης, ως παράδειγμα της χωρητικότητας μνήμης που απαιτείται.

Επομένως, δεν προκαλεί έκπληξη ότι το Neurogress σχεδιάζει να χρησιμοποιήσει το blockchain, το οποίο πιστεύει ότι μπορεί να αντιμετωπίσει αποτελεσματικά το πρόβλημα της ασφαλούς αποθήκευσης των δεδομένων και του απορρήτου. Καταγράφοντας τα δεδομένα των χρηστών σε ένα αποκεντρωμένο blockchain, αυτά τα δεδομένα γίνονται ανθεκτικά στις επιθέσεις των hackers, και ως εκ τούτου πιο ασφαλή. Ταυτοχρόνως, η χρήση της τεχνολογίας blockchain καθιστά το σύστημα Neurogress ανοιχτό και με διαφάνεια στους πιθανούς χρήστες των υπηρεσιών της πλατφόρμας Neurogress. Επειδή οποιαδήποτε μη φυσιολογική δραστηριότητα είναι εύκολα ανιχνεύσιμη, το σύστημα διασφαλίζει την ασφάλεια και την εμπιστευτικότητα των προσωπικών δεδομένων. Είναι επομένως προφανές, ότι το blockchain είναι μια μορφή τεχνολογίας πληροφοριών, με πολλές σημαντικές εφαρμογές, ικανές να υποστηρίξουν την ανίχνευση του εγκεφάλου, την προσομοίωση του εγκεφάλου και την σκέψη.

Η ψηφιοποίηση ολόκληρου του ανθρώπινου εγκεφάλου απαιτεί προφανώς και κάποιον ενδιάμεσο για την αποθήκευση και όπως αναφέραμε και πιο πάνω η τεχνολογία blockchain μας είναι απαραίτητη. Μια πρόταση είναι η αποθήκευση των “mindfiles”, τα οποία θα λειτουργούσαν ως δομικά στοιχεία δεδομένων στις αλυσίδες της προσωπικής σκέψης, με δυνατότητα κοινής χρήσης, σε ένα σύστημα αρχείων ενός P2P δικτύου, το οποίο επιτρέπει την έκδοση του ιστορικού. Αυτός ο blockchain τρόπος σκέψης προτείνεται ως ένα <<input-processing-output computational system>>, δηλαδή υπολογιστικό σύστημα εισόδου-επεξεργασίας-εξόδου, με πολλά χαρακτηριστικά, που προσφέρουν την ευκαιρία για Α.Ι. και ανθρώπινη βελτίωση. Το blockchain επιτρέπει σε ένα διασυνδεδεμένο δίκτυο υπολογιστών να συνεργαστεί σε διαστήματα μιας χρονικής σήμανσης, για την επικύρωση της πηγής ενός ledger.

Εάν επρόκειτο να φτιάξουμε έναν εγκέφαλο από την αρχή, αυτός ο τύπος μηχανισμού εμπιστοσύνης, θα μπορούσε να επιτρέψει στα δίκτυα των νευρώνων να αποθηκεύουν και να ανακαλούν πληροφορίες, με ακρίβεια και εμπιστοσύνη για το τι είναι υποκειμενικό έναντι του στόχου μιας δεδομένης εμπειρίας. Η σύνδεση ελέγχου ταυτότητας πολλαπλών παραγόντων σε μια αλυσίδα προσωπικής σκέψης, ως μια εφαρμογή του blockchain, μπορεί να δώσει την ευκαιρία της ασφαλούς οικοδόμησης ποσοτικοποίησης των κοινών προσωπικών δεδομένων για τα ανθρώπινα όντα. Αυτά τα κοινά προσωπικά δεδομένα μειώνουν τα siloes των ανθρώπινων δεδομένων, ενώ επιτρέπουν σε κάθε άνθρωπο να διατηρεί την κυριότητα του απορρήτου ή της κοινής χρήσης αυτής της εμπειρίας, πιθανώς για τη συγκέντρωση χρηματικού οφέλους χωρίς τη χρήση τρίτης οντότητας.

Στο μέλλον, όταν δύο ή περισσότεροι άνθρωποι βιώνουν την ίδια στιγμή την ίδια εμπειρία, αν και υπό υποκειμενικές προοπτικές, η χρήση της επαυξημένης έκδοσης αυτής της τεχνολογίας, θα

μπορούσε να ξανά-συναρμολογήσει εμπειρίες, οι οποίες θα είναι πιο αντικειμενικές για τα συμβάντα εκείνης της στιγμής. Στην ιδανική περίπτωση, αυτό θα επέτρεπε τη δημιουργία εικονικών προσομοιώσεων, για αναμνήσεις του παρελθόντος.

Μόλις υπάρξει καλύτερη κατανόηση των μεμονωμένων αντιστοιχιών στα συναισθήματα και οι αισθητηριακές εμπειρίες συμβάλλουν σε μια μεμονωμένη μνήμη, θα λαμβάνονται τα δεδομένα από τις αισθήσεις (όραση, όσφρηση, ακοή) σε αυτό το μελλοντικό blockchain.

Το γεγονός είναι ότι οι τεχνολογίες που χρειάζονται για να πραγματοποιηθούν τα παραπάνω, ήδη αναπτύσσονται. Στο όχι τόσο μακρινό μέλλον, μπορούμε να αρχίσουμε να καταγράφουμε τις εμπειρίες, με τη χρήση φορητής τεχνολογίας, την τρέχουσα κατάσταση εμφυτευμάτων εγκεφάλου και νευρώνων, την απεικόνιση της βιο-ανάδρασης, και οποιουσδήποτε άλλους αισθητήρες που χρειάζονται ένα δακτυλικό αποτύπωμα, ειδικά για ένα συγκεκριμένο αρχείο κάποιου ανθρώπου για κάποια εμπειρία του, κάποιο χρονικό διάστημα. Χρησιμοποιώντας αυτές τις τεχνολογίες ως σημείο εκκίνησης, μπορεί να πραγματοποιηθεί έρευνα για τη βελτίωση των πρωτοκόλλων που αφορούν στη λήψη αποφάσεων, στη μάθηση, και στην αποκατάσταση [151].

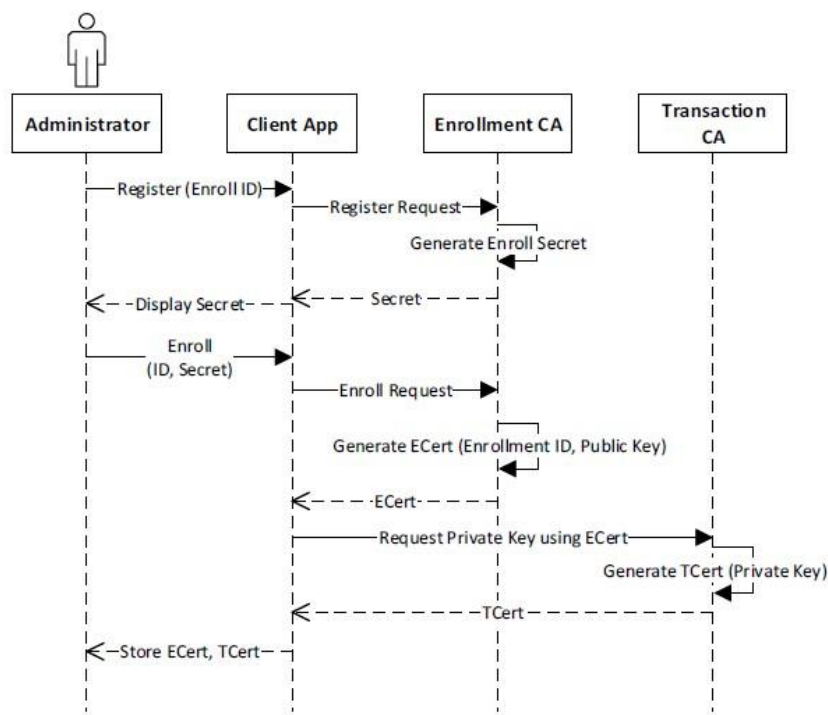
3.10) Διαχείριση δεδομένων εγγραφής (Enrollment Data Management)

Η εγγραφή των μελών στα σχέδια της υγειονομικής περίθαλψης, η παράδοση, τα κριτήρια, τα πιστοποιητικά εγγραφής, έχουν ως αποτέλεσμα την εγγραφή διοικητικών δεδομένων. Αν και ο πρωτογενής παραγωγός των δεδομένων αυτών είναι μια υπηρεσία της κυβέρνησης, μπορούν να χρησιμοποιήσουν τα δεδομένα που παράγονται από μικρούς, μεσαίους, ή μεγάλους παρόχους [152]. Η διαχείριση αυτών των δεδομένων που ποικίλουν, είναι χειροκίνητη, γεγονός που απαιτεί μια εκτενή διαδικασία ελέγχου αναφοράς, διαπιστευτηρίων, και αρμοδιοτήτων. Κατά συνέπεια, σε κάποιο βαθμό, η όλη διαδικασία παρατείνεται και έτσι επιβραδύνεται ολόκληρη η διαδικασία εγγραφής (enrollment process) καθώς αποτελεί εμπόδιο για την αποτελεσματικότητα του συστήματος υγειονομικής περίθαλψης. Ωστόσο, αυτές οι πληροφορίες θα μπορούσαν να αποθηκευτούν σε ένα blockchain για να ελεγχθούν οι αξιόπιστες αναφορές και οι σχετικές εγγραφές στο συντομότερο δυνατό χρόνο. Για την αύξηση της αποτελεσματικότητας στη διαδικασία εγγραφής, αυτό θα μπορούσε να βοηθήσει έναν διοικητικό υπάλληλο, μέσω διαδικαστικής απλούστευσης, αιτήσεων αρμοδιοτήτων, διαχείρισης δικτύου και συντονισμού [74].

Στη συνέχεια, θα μελετήσουμε τη διαδικασία εκτέλεσης εγγραφής στην προτεινόμενη blockchain πλατφόρμα ιατρικής.

Η παρακάτω εικόνα αντιπροσωπεύει την εγγραφή της ταυτότητας του χρήστη, στάδιο απαραίτητο για την πρόσβαση του ασθενή στο σύστημα. Ο διαχειριστής του δικτύου θέλοντας να αποκτήσει την ταυτότητα του χρήστη (user identity), υποβάλλει το αίτημα εγγραφής στο “Enrollment CA”, το οποίο εκδίδει ένα μυστικό για τη διαδικασία εγγραφής. Έπειτα, το αίτημα εγγραφής αποστέλλεται από τον πελάτη στην CA, περνώντας το αναγνωριστικό εγγραφής και το μυστικό που αποκτήθηκε κατά τη διαδικασία εγγραφής. Σε απάντηση, η CA περνά το

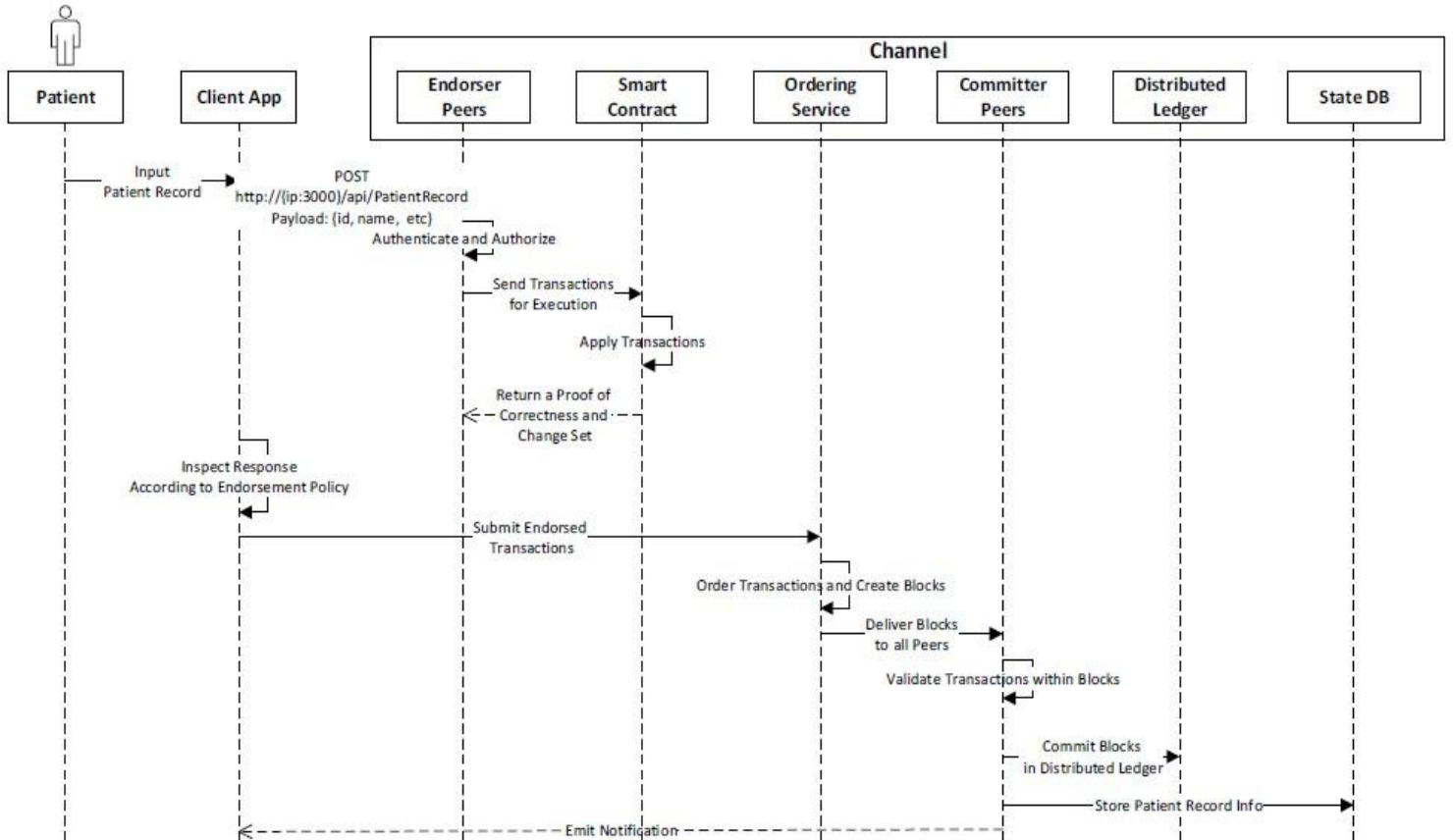
Πιστοποιητικό Εγγραφής, “Enrollment Certificate” (ECert) μαζί με το δημόσιο κλειδί. Το ECert χρησιμοποιείται για να ζητήσει το Πιστοποιητικό Συναλλαγής “Transaction Certificate” (TCert), και η συναλλαγή CA περνά το TCert μαζί με το ιδιωτικό κλειδί για την υπογραφή των συναλλαγών. Μετά από την εγγραφή, στον ασθενή επιτρέπεται η πρόσβαση στην πλατφόρμα με το πιστοποιητικό που έχει εκδοθεί.



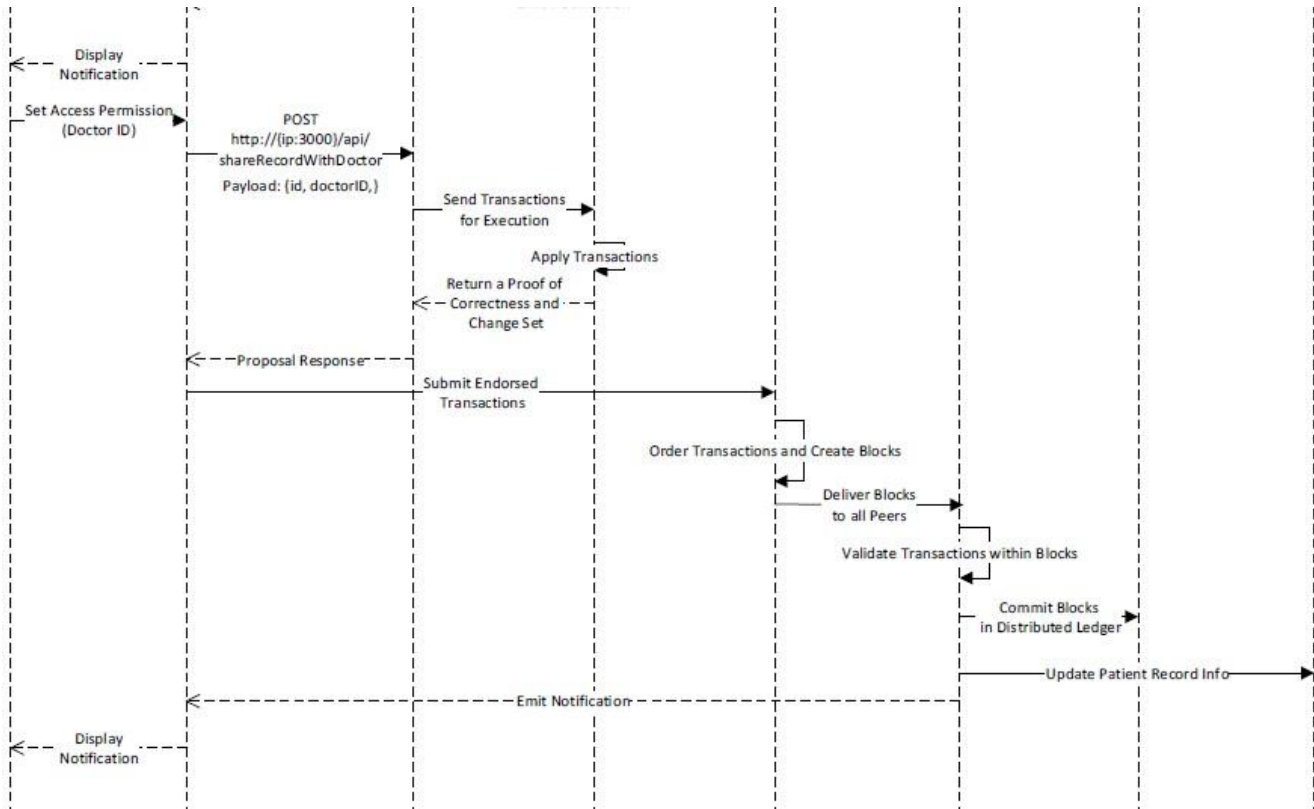
Εικόνα 3.29: Εγγραφή ταυτότητας χρήστη στο blockchain [153]

Στην επόμενη εικόνα, απεικονίζονται διάφορες επιχειρησιακές διαδικασίες για την υποβολή της συναλλαγής με σκοπό τη δημιουργία ενός EMR και την κοινή χρήση ενός EMR σε ένα blockchain. Ο ασθενής μπορεί να εισάγει πληροφορίες στο EMR μέσω της CA, και ο πελάτης δημιουργεί το προτεινόμενο αίτημα συναλλαγής, χρησιμοποιώντας τη μέθοδο POST, για να επικαλεστεί τη λειτουργία της έξυπνης σύμβασης στους ομότιμους κόμβους. Στη συνέχεια, το έξυπνο συμβόλαιο εκτελείται για την παραγωγή των αποτελεσμάτων συναλλαγής και το σύνολο αυτών των τιμών επιστρέφεται στον πελάτη. Η CA επαληθεύει τις απαντήσεις της πρότασης σύμφωνα με τις πολιτικές έγκρισης και μεταδίδει τις εγκρινόμενες συναλλαγές στην υπηρεσία παραγγελιών. Η υπηρεσία παραγγελιών παραγγέλνει χρονολογικά ανά κανάλι και δημιουργεί block συναλλαγών ανά κανάλι. Στη συνέχεια, τα blocks συναλλαγών παραδίδονται σε όλους τους ομότιμους κόμβους ανά κανάλι για επικύρωση. Κάθε ομότιμος προσθέτει το block στην αλυσίδα και η εγγραφή EMR αποθηκεύεται στην τρέχουσα βάση δεδομένων. Τέλος ένα συμβάν εκπέμπεται στην CA για να ενημερώσει τον ασθενή ότι το EMR δημιουργείται στο blockchain. Για την κοινή χρήση του EMR με έναν συγκεκριμένο γιατρό, ο ασθενής πρέπει να ορίσει το αναγνωριστικό του γιατρού, για να καθοριστεί ποιος μπορεί να έχει πρόσβαση στο αρχείο EMR μέσω της CA. Το υπόλοιπο των διαδικασιών συναλλαγής είναι παρομοιάζει με τη διαδικασία συναλλαγής για την παραγωγή EMR. Τέλος, ένα γεγονός εκπέμπεται για να ενημερώσει τον

ασθενή ότι το EMR έχει κοινοποιηθεί σε έναν συγκεκριμένο γιατρό και πως η συναλλαγή έχει συνδεθεί στο blockchain.

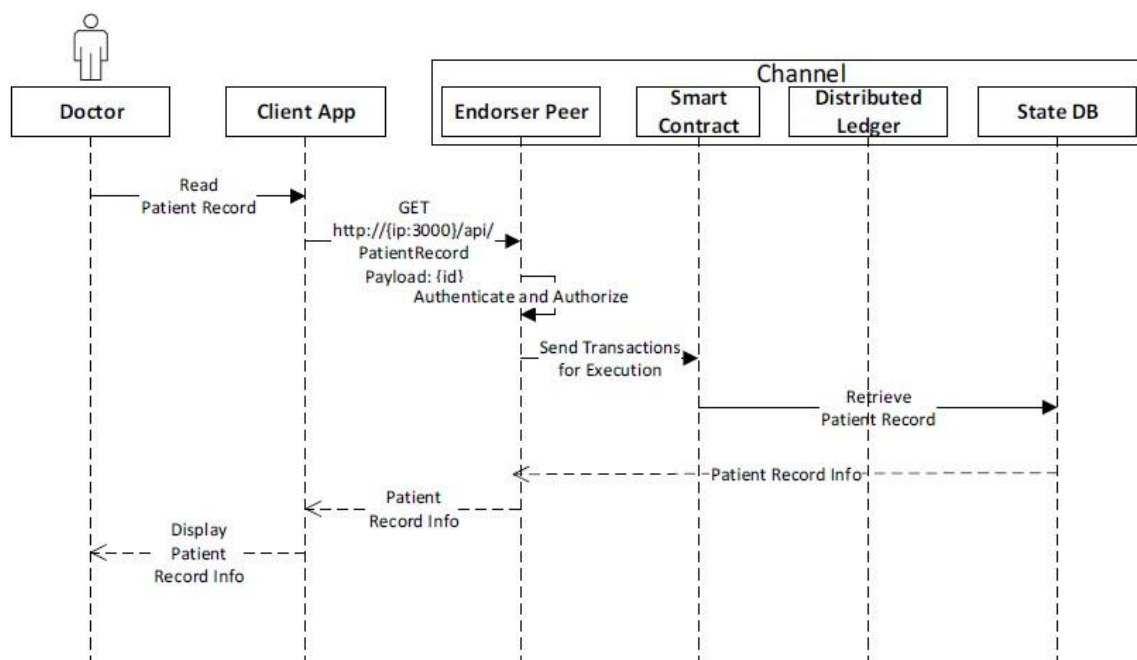


Εικόνα 3.30α: Δημιουργία και κοινή χρήση ενός EMR σε ένα blockchain (α μέρος), [153]



Εικόνα 3.30β: Δημιουργία και κοινή χρήση ενός EMR σε ένα blockchain (β μέρος) [153]

Στην τελευταία εικόνα απεικονίζονται οι διαδικασίες που εκτελεί ένας γιατρός όταν επιθυμεί να ρωτήσει το κοινόχρηστο EMR. Ο γιατρός μπορεί να ζητήσει το τελικό σημείο API, χρησιμοποιώντας τη μέθοδο GET για να ζητήσει την εγγραφή EMR από τη βάση δομένων χρησιμοποιώντας το ID του ασθενούς. Καθώς το έξυπνο συμβόλαιο ζητά μόνο το ledger, η πλατφόρμα δεν θα υποβάλλει την συναλλαγή προς την υπηρεσία συναίνεσης, αφού όλοι οι ομότιμοι κόμβοι διατηρούν ένα τοπικό αντίγραφο του ledger, έτσι δεν απαιτείται καμία διαδικασία συναίνεσης και επομένως το αποτέλεσμα του ερωτήματος σε ένα EMR επιστρέφεται αμέσως [153].



Εικόνα 3.31: Ερώτηση στο EMR σε ένα blockchain [153]

3.11) Διαχείριση απαιτήσεων τιμολογίων (Claims and Billing Management)

Η υπηρεσία της υγειονομικής περίθαλψης έχει το δικό της κόστος, που ήδη κάνει ολόκληρη τη βιομηχανία να αξίζει 1 τρισεκατομμύριο δολάρια και αυξάνεται με ταχύ ρυθμό [154]. Η διαδικασία της ιατρικής τιμολόγησης (medical billing) αποτελεί αναπόσπαστο κομμάτι του τομέα της υγειονομικής περίθαλψης. Αυτό συμβαίνει διότι, χωρίς τιμολόγηση δε μπορεί να εξασφαλιστεί η σωστή παράδοση υπηρεσιών.

Αυτή η διαδικασία ξεκινά από τη στιγμή που ο ασθενής γίνεται δεκτός στο νοσοκομείο, μέχρι τη στιγμή που θα βγει. Η διαδικασία περιλαμβάνει διάφορα βήματα όπως: check-in, confirming financial responsibility (επιβεβαίωση οικονομικής ευθύνης), coding and billing compliance (κωδικοποίηση και τιμολόγηση), transmitting the claim (διαβίβαση των αξιώσεων), receiving payment from insurance companies (πληρωμή από ασφαλιστικές εταιρίες) [155]. Το όλο σύστημα χρέωσης μπορεί να είναι πρόκληση καθώς ορισμένα από τα τέλη καλύπτονται πλήρως ή εξ'ολοκλήρου, από το ατομικό σχέδιο ασφάλειας υγείας του ασθενούς ή καταβάλλονται από τον ίδιο τον ασθενή.

Ένα από τα βασικά ζητήματα στην Ιατρική Τιμολόγηση, είναι η υπερβολική τιμολόγηση, εξαιτίας της έλλειψης διαφάνειας και εμπιστοσύνης μεταξύ των γιατρών, ασθενών και ασφαλιστικών εταιριών. Οι απαιτήσεις και οι χρεώσεις στον τομέα της υγείας υφίστανται συνεχή

κατάχρηση, αλλά μπορεί να μειωθεί με τη χρήση ενός διαφανούς συστήματος για κάθε ενδιαφερόμενο (stakeholders). Το Blockchain μπορεί να εξασφαλίσει τη διαφάνεια ενός τέτοιου συστήματος, καθ'όλη τη διαδικασία και καταργώντας τη δυσπιστία μεταξύ των ενδιαφερομένων, [154].

3.12) Εντοπισμός απάτης (fraud detection) και Διαχείριση Ποιότητας (Quality management)

Σύμφωνα με μια έκθεση του Guardian [156] που δημοσιεύτηκε από τον Παγκόσμιο Οργανισμό Υγείας (WHO), « ένα στα δέκα ιατρικά προϊόντα που κυκλοφορούν στην αγορά σε χώρες χαμηλού και μεσαίου εισοδήματος, είναι είτε υποβαθμισμένα είτε παραποιημένα». Επίσης, ο Παγκόσμιος Οργανισμός Υγείας ξοδεύει 30 δισεκατομμύρια δολάρια στον αγώνα κατά της παραποίησης και απομίμησης των φαρμάκων.

Ένα φάρμακο θεωρείται παραποιημένο (counterfeit), αν περιέχει ακατάλληλα συστατικά και εμπορεύεται με πρόθεση να κρύψει ή να μιμηθεί την προέλευση, την αυθεντικότητα, ή ακόμη και την αποτελεσματικότητα του φαρμάκου [157], [158]. Επιπλέον, τα πλαστά προϊόντα και τα παραποιημένα φάρμακα επηρεάζουν σε μεγάλο βαθμό τη διαχείριση της εφοδιαστικής αλυσίδας (SCM) [159]. Οι επιδόσεις τους στη φαρμακοβιομηχανία είναι ανταγωνιστικοί παράγοντες που διαταράσσουν την αποδοτικότητα, την αυθεντικότητα και την ισχυρή κερδοφορία, σε μια συγκεκριμένη βιομηχανία υγειονομικής περίθαλψης [160].

Οι πελάτες συχνά δεν γνωρίζουν την ακριβή πηγή των φαρμάκων που αγοράζουν και καταναλώνουν [161]. Δεδομένου ότι αυτός ο τύπος φαρμάκου είναι κακόβουλος για έναν ασθενή, είναι ένα απειλητικό θέμα για τη ζωή σε όλο τον κόσμο [162]. Αυτό μπορεί να προκαλέσει την απειλή δυσφήμισης των φαρμακευτικών εταιρειών, αναγκάζοντας τους κατασκευαστές φαρμάκων και τους διανομείς να επενδύσουν ένα τεράστιο χρηματικό ποσό σε αντίμετρα [157]. Σε μια μελέτη που δημοσιεύθηκε στο “Counterfeit Drug Detection: Recent Strategies and analytical perspectives” , βρέθηκαν οι τεχνικές όπως Φασματογραφία και Χρωματογραφία , ότι είναι αποτελεσματικές για την ανίχνευση των παραποιημένων φαρμάκων, με τη μέθοδο ανίχνευσης των δραστικών συστατικών και της σύνθεσης δείγματος της εικόνας. Ωστόσο, υπάρχουν περιορισμοί καθώς βασίζονται σε ηλεκτρομηχανικές συσκευές, γεγονός που αυξάνει το γενικό κόστος.

Το blockchain έχει τη δυνατότητα να αντιμετωπίσει πολλές προκλήσεις της φαρμακευτικής εφοδιαστικής αλυσίδας, χάρη στην εφαρμογή της για την καταπολέμηση ψευδεπίγραφων και υποβαθμισμένων φαρμάκων [163, 164, 165, 166] . Η αντιμετώπιση αυτού του προβλήματος επικεντρώνεται στην ανάπτυξη λύσεων blockchain που μπορούν να επιτρέψουν την επαλήθευση των δεδομένων της εφοδιαστικής αλυσίδας, καθώς τα φάρμακα διασχίζουν την παγκόσμια αλυσίδα εφοδιασμού, ενώ παράλληλα επιτρέπουν στους συμμετέχοντες να εντοπίζουν πιθανές διεισδύσεις πλαστών φαρμάκων, μέσω μεγαλύτερης προβολής των δεδομένων συναλλαγής στην εφοδιαστική αλυσίδα [163, 164]. Μια μεγάλη πρόκληση για την ασφάλεια και τις ρυθμίσεις των φαρμάκων σε ένα blockchain, είναι η διακυβέρνηση, δηλαδή ποιος θα συμμετάσχει στο

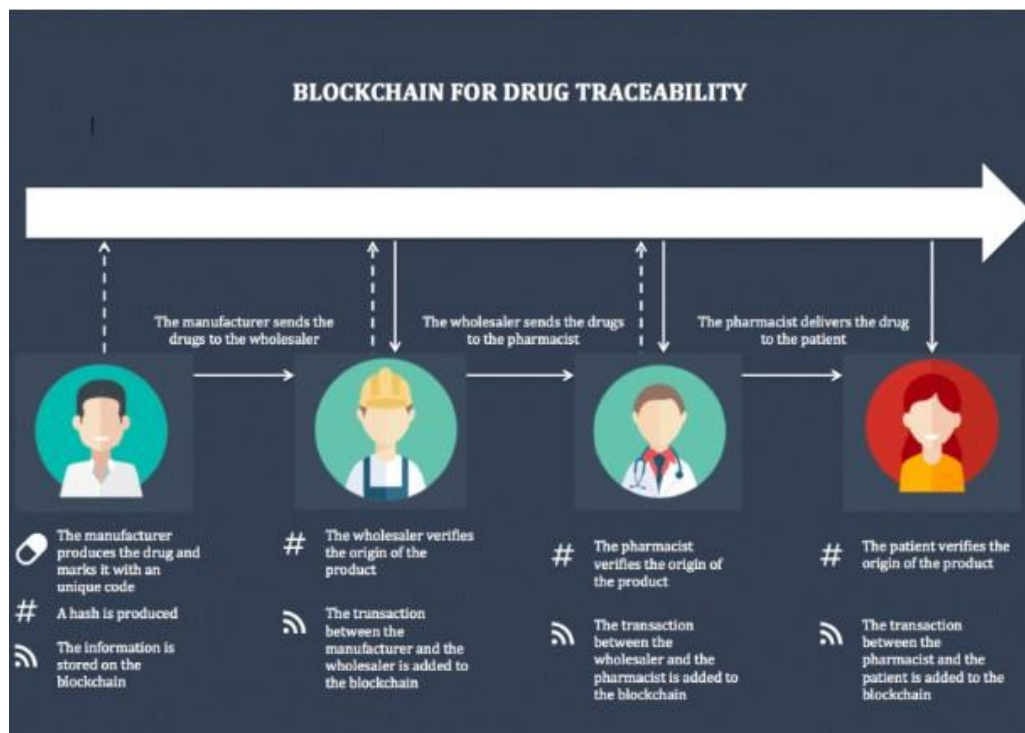
blockchain, πώς θα επικυρωθούν τα δεδομένα και κυρίως πώς θα γίνει η κοινή χρήση των ευαίσθητων και εμπιστευτικών δεδομένων της φαρμακευτικής εφοδιαστικής αλυσίδας μεταξύ των συμμετεχόντων. Πολλές από αυτές τις προκλήσεις απαιτούν τη δημιουργία μιας κοινοπραξίας από ενδιαφερόμενους που θα μπορούσαν να συμφωνήσουν με αυτούς τους κανόνες πριν ακόμη αναπτυχθεί μια λύση.

Αρκετά μεγάλες και νέες εταιρείες blockchain ξεκινούν να δραστηριοποιούνται στην ανάπτυξη των blockchain λύσεων για την φαρμακευτική εφοδιαστική αλυσίδα. Επίσης, έχουν πραγματοποιηθεί έρευνες και πειράματα σχετικά με ένα δημοσιευμένο πρωτόκολλο, το οποίο προβλέπει blockchain σύστημα φαρμακοεπαγρύπνησης σε ένα δίκτυο προσομοίωσης, χρησιμοποιώντας κατανεμημένες εφαρμογές, έξυπνες συμβάσεις και στιγμιότυπα πρωτοτύπων (prototype), τα οποία είναι χτισμένα στις πλατφόρμες blockchain, Ethereum και Hyperledger. Ωστόσο, τα στάδια σχεδιασμού για να διασφαλιστεί ότι αυτά τα blockchains είναι κατάλληλα για χρήση, επεκτάσιμα και πως μπορούν να αντέξουν σε πραγματικές δοκιμές, παραμένουν σε αρχικά στάδια.

Επίσης, οι παγκόσμιες αλυσίδες εφοδιασμού φαρμάκων διανύουν μια περίοδο εκσυγχρονισμού πολιτικής. Συγκεκριμένα, ο νόμος περί ασφάλειας της εφοδιαστικής αλυσίδας της FDA (FDA’s Drug Supply Chain Security Act), περιγράφει τα απαραίτητα μέτρα για την εφαρμογή ενός ηλεκτρονικού και διαλειτουργικού συστήματος για τον εντοπισμό και την ανίχνευση συνταγογραφούμενων φαρμάκων που διανέμονται στις ΗΠΑ [167]. Αυτό θα ενισχύσει την ικανότητα του FDA να προστατεύει τους καταναλωτές, ακόμη και από φάρμακα που μπορεί να είναι παραποιημένα, κλεμμένα, μολυσμένα ή επιβλαβή με άλλο τρόπο. Ο Νόμος για την ασφάλεια της εφοδιαστικής αλυσίδας, Drug Supply Chain Security Act, έχει επίσης κάτι αντίστοιχο και στην Ευρωπαϊκή Ένωση, όπου η οδηγία για τα ψευδεπίγραφα φάρμακα της Ε.Ε (EU Falsified Medicines Directive), απαιτεί μέτρα για την πρόληψη της εισόδου ψευδεπίγραφων φαρμάκων στη νόμιμη εφοδιαστική αλυσίδα, απαιτώντας χαρακτηριστικά ασφαλείας για να εξασφαλιστεί η ταυτοποίηση και η αυθεντικοποίηση [168].

Είναι σημαντικό πως και τα δύο αυτά μέσα πολιτικής έχουν ρυθμιστικές απαιτήσεις που μπορούν να διευκολυνθούν μέσω της τεχνολογίας blockchain. Οι δύο αυτές πολιτικές απαιτούν ένα μοναδικό αναγνωριστικό στοιχείο (μέσω της χρήσης σειριοποίησης), για την επαλήθευση της γνησιότητας των φαρμάκων, προκειμένου να αποτρέψουν την παραλαβή παραποιημένων ή οποιουδήποτε άλλου ύποπτου φαρμάκου από τους ασθενείς. Ωστόσο υπάρχουν διαφορές σχετικά με την οδηγία για τα ψευδεπίγραφα φάρμακα της Ε.Ε., η οποία χρησιμοποιεί μια κεντρική προσέγγιση, όπου οι κατασκευαστές φαρμάκων φορτώνουν σειριακούς αριθμούς σε μια κεντρική βάση δεδομένων των ρυθμιστικών αρχών της Ε.Ε, επιτρέποντας στους διανομείς να συνδέουν και να επαληθεύουν την αυθεντικότητα των φαρμάκων. Στις ΗΠΑ δεν υπάρχει προγραμματισμένη κεντρική βάση δεδομένων ρυθμιστικών αρχών και είναι λογική πρόκληση να αμφισβητηθούν οι διανομείς οι οποίοι θα ενσωματώσουν τα δεδομένα τους σε εκείνα των κατασκευαστών φαρμάκων. Έτσι, το blockchain προσφέρει μια πιθανή λύση για να ικανοποιήσει τις ανάγκες και των δύο αγορών και να εξασφαλίσει καλύτερα την ακεραιότητα της σειριοποίησης των δεδομένων και την προέλευση των γενεαλογικών πληροφοριών. Τα συστήματα blockchain θα μπορούσαν να επιτρέψουν στους κατασκευαστές φαρμάκων να μοιράζονται τους σειριακούς αριθμούς στο blockchain, όπου οι χονδρέμποροι, οι φαρμακοποιοί και οι συνταγογράφοι θα έχουν πρόσβαση, με σκοπό να επαληθεύουν την προέλευση του φαρμάκου. Η παρακάτω εικόνα μας

δείχνει μια απλοποιημένη εφοδιαστική αλυσίδα φαρμάκων βασισμένη στην τεχνολογία blockchain. Αυτή η διαδικασία εξασφαλίζει τον ποιοτικό έλεγχο χαμηλού κόστους, την καταγραφή των προϊόντων, την παρακολούθηση των φαρμάκων και την αποφυγή των παραποιημένων φαρμάκων, μέσω ολόκληρης της διαδικασίας διαχείρισης της εφοδιαστικής αλυσίδας (SCM) [169].



Εικόνα 3.32:Απλοποιημένη εφοδιαστική αλυσίδα φαρμάκων βασισμένη στην τεχνολογία blockchain, (<https://sphinxsolutionblogs.wordpress.com/2018/07/12/how-can-blockchain-efficiently-manage-medicine-supply-chain/>).

Ωστόσο, η τεχνολογία blockchain δεν είναι πανάκεια για την καταπολέμηση του παγκόσμιου εγκλήματος του εμπορίου ψευδεπίγραφων και υποβαθμισμένων φαρμάκων. Αν και είναι ένας σημαντικός στόχος, οι μοναδικές προκλήσεις που συνδέονται με την εγκληματική φύση αυτού του εμπορίου, η παρουσία της γκρίζας αγοράς (Internet), και η ανάγκη για άλλες μορφές τεχνολογίας για την κατάλληλη ταυτοποίηση και επαλήθευση του φυσικού προϊόντος, μπορεί να καταστήσει τα blockchains αποτελεσματικά στον πραγματικό κόσμο και εναντίον κακοποιών παραγόντων [165],[170]. Άλλες περιπτώσεις χρήσης συμπεριλαμβάνουν: την ενίσχυση των φαρμακευτικών δημοσίων συμβάσεων, την φαρμακοεπαγρύπνηση, την ενσωμάτωση της διαχείρισης της αλυσίδας με το IoT και μπορεί να έχουν βραχυπρόθεσμη ή και μακροπρόθεσμη χρησιμότητα από ότι η περίπτωση των παραποιημένων φαρμάκων.

Η υιοθέτηση του blockchain στις εφοδιαστικές αλυσίδες υγείας κινείται πιο αργά από ότι σε άλλες βιομηχανίες (εφοδιαστική αλυσίδα τροφίμων και διαμαντιών). Οι μελέτες που διεξήχθησαν από την Ένωση Προτύπων IEEE το 2017, σχετικά με την εξέλιξη της εφοδιαστικής αλυσίδας

φαρμάκων, διαπίστωσαν ότι : 3 από τους πιο συχνά αναφερόμενους φραγμούς υιοθεσίας μεταξύ 300 ειδικών ερωτηθέντων (34% κατασκευαστές 33% διανομείς, 33% λιανοπωλητές) ήταν α) η ενδοεπικοινωνία και η αποδοχή των χρηστών, β) η ενσωμάτωση στα υφιστάμενα δίκτυα, γ) οι προκλήσεις εκπαίδευσης στην εφαρμογή νέων τεχνολογιών [171]. Το κόστος της υιοθέτησης και της υλοποίησης είναι μια πρωταρχική πρόκληση για τους εμπλεκόμενους παράγοντες της εφοδιαστικής αλυσίδας, δεδομένου ότι οι λύσεις blockchain ενδέχεται να μην οδηγήσουν εγγενώς σε έσοδα, αλλά θα ενισχύσουν τη συμμόρφωση, τη μείωση του κόστους και το μετριασμό των κινδύνων. Η πραγματική αξία ενός φαρμακευτικού blockchain δεν μπορεί να περιοριστεί σε συγκεκριμένες περιπτώσεις χρήσης. Η απελευθέρωση του δυναμικού του blockchain θα μπορούσε να χρησιμοποιηθεί για ευρύτερους στόχους, όπως: επιτάχυνση του εκσυγχρονισμού της εφοδιαστικής αλυσίδας, απελευθέρωση των δεδομένων για τη βελτίωση της απόδοσης και της διαχείρισης της εφοδιαστικής αλυσίδας, αύξηση της διαφάνειας για τη βελτίωση της διακυβέρνησης και της υπευθυνότητας, ζητήματα τα οποία σχετίζονται με τα εμπόδια που αφορούν στην πρόσβαση, στην ποιότητα και στην ευθύνη στον τομέα των φαρμάκων.

3.13) Μοντέλα πρόβλεψης για την προστασία της ιδιωτικής ζωής (privacy-preserving predictive models)

Η διαχείριση των αρχείων καταγραφής της υγειονομικής περίθαλψης στο blockchain, επικεντρώνεται στην κοινή χρήση και ανταλλαγή των δεδομένων, μεταξύ διαφορετικών φορέων, στον τομέα της υγειονομικής περίθαλψης, διατηρώντας παράλληλα την πηγή, την προέλευση, και συχνά το απόρρητο τέτοιων δεδομένων, κατά τρόπο που να επιτρέπει την πιο ισχυρή ανάλυση τους [172]. Μεταξύ των εφαρμογών υγειονομικής περίθαλψης, υπάρχει ένα μοντέλο βασισμένο σε blockchain που προβλέπει αποτελέσματα, διαφυλάττοντας το απόρρητο. Σε αυτή τη συγκεκριμένη περίπτωση χρήσης, τα νοσοκομεία ή τα ιδρύματα υγειονομικής περίθαλψης, στοχεύουν στην εκπαίδευση ενός μοντέλου μηχανικής μάθησης M.L., από τα αρχεία υγείας που είναι αποθηκευμένα σε EHRs συστήματα. Στη συνέχεια χρησιμοποιώντας αυτό το εκπαιδευμένο μοντέλο προβλέπονται τα αποτελέσματα των ασθενών, όπως ο κίνδυνος εμφάνισης κάποιας πάθησης ή ασθένειας. Συγκεκριμένα, αν το ενδιαφέρον είναι στραμμένο σε σπάνιες ασθένειες, ενδέχεται να μην υπάρχουν αρκετά αρχεία ασθενών σε ένα μόνο νοσοκομείο ή ίδρυμα για να μάθουν ένα γενικευμένο μοντέλο αποκλειστικά από τα δικά του δεδομένα. Για να λυθεί αυτό το πρόβλημα, τα νοσοκομεία και τα ιδρύματα μπορούν να μοιράζονται τα δεδομένα τους με σκοπό να διευρύνουν τον αριθμό των αρχείων. Η άμεση ανταλλαγή των δεδομένων των ασθενών, μπορεί να οδηγήσει σε κινδύνους που αφορούν το απόρρητο και την προστασία της ιδιωτικής ζωής. Ως εκ τούτου, έχουν προταθεί αρκετές μέθοδοι μοντελοποίησης πρόβλεψης και διατήρησης του απορρήτου (privacy-preserving predictive modeling methods), επιτρέποντας στα νοσοκομεία/ιδρύματα να συνεργαστούν με σκοπό να εκπαιδεύσουν ένα μοντέλο πρόβλεψης, μοιράζοντας μόνο μερικώς εκπαιδευμένα μοντέλα μηχανικής μάθησης αντί για αρχεία ασθενών [128].

Ωστόσο, αυτές οι state-of-the-art μέθοδοι, είναι κυρίως με αρχιτεκτονική διακομιστή-πελάτη (client-server), οι οποίες μπορεί να βοηθήσουν σε αρκετά προβλήματα, όπως το <<single-point-

of-failure>>, στον server. Για το μετριασμό αυτών των προβλημάτων, ο συνδυασμός blockchain και privacy-preserving prediction modeling, παρέχει μια λύση για τα νοσοκομεία/ιδρύματα για συνεργασία, ώστε να εκπαιδεύσουν ένα προγνωστικό μοντέλο, χωρίς να ανταλλάξουν δεδομένα ασθενών, ενώ παράλληλα θα επωφελούνται από μια κατακεταμημένη peer-to-peer αρχιτεκτονική, χωρίς ανησυχίες για προβλήματα όπως το <<single-point-of-failure>>. Σε αυτή την προσέγγιση για λύση που βασίζεται σε blockchain, οι χρήστες είναι τα νοσοκομεία/ιδρύματα υγειονομικής περίθαλψης, που συμμετέχουν στο μοντέλο μάθησης. Τα δεδομένα που εισάγουν οι χρήστες, είναι τα δεδομένα σε επίπεδο ασθενών από το EHR, με την ίδια μορφή. Είναι σημαντικό ότι τα άμεσα δεδομένα δεν μοιράζονται σε νοσοκομεία/ιδρύματα, ενώ μόνο τα μοντέλα πρόβλεψης αντλούνται από τα EHR δεδομένα και κοινοποιούνται μέσω του δικτύου blockchain. Σε ένα τέτοιο δίκτυο blockchain, οι ομότιμοι κόμβοι είναι οι ίδιοι οι χρήστες. Για να επικυρώσουμε τα δεδομένα και να εκπαιδεύσουμε ένα μοντέλο πρόβλεψης, κάθε ομότιμος κόμβος ενσωματώνει κομμάτια μοντέλων στις συναλλαγές, σε επίπεδο μεταδεδομένων. Σκοπός η δημιουργία blocks, η ανάκτηση μοντέλων από άλλους ομότιμους κόμβους και στη συνέχεια η ενημέρωση του μοντέλου, χρησιμοποιώντας τα δικά τους EHR δεδομένα. Η διαδικασία εκμάθησης διεξάγεται σε απευθείας σύνδεση (Online), έτσι ώστε το μοντέλο να ενημερώνεται χρησιμοποιώντας μόνο μερικά δεδομένα σε διαδοχική σειρά. Επιπλέον, χρησιμοποιούνται εκπαιδευτικά λάθη (training errors), για να καθοδηγήσουν τη σειρά της απευθείας μάθησης (online learning) στο blockchain, με βάση ένα ίδρυμα, το οποίο περιέχει πληροφορίες με υψηλότερα σφάλματα (higher errors), και μπορεί να παρέχει περισσότερες πληροφορίες για τη βελτίωση του μοντέλου. Αυτή η επαναληπτική διαδικασία μάθησης, επαναλαμβάνεται μέχρι να προσδιοριστεί ένα προγνωστικό μοντέλο συναίνεσης για όλους τους ομότιμους κόμβους. Με τον τρόπο αυτό, το blockchain παρέχει συγκεκριμένα οφέλη για την επίλυση προβλημάτων, όπως η προστασία της ιδιωτικής ζωής και απορρήτου με την ανταλλαγή μοντέλων μόνο, την αποφυγή του <<single-point-of-failure>> και τη δημιουργία αμετάβλητων αρχείων καταγραφής για την διαδικασία μάθησης.

Ο τύπος σχεδιασμού βασίζεται με ιδιωτικό blockchain. Όσον αφορά την κοινή χρήση δεδομένων, τα μοντέλα και τα μεταδεδομένα, μοιράζονται επί της αλυσίδας (on-chain), ενώ δεν υπάρχει ανταλλαγή εκτός της αλυσίδας (off-chain). Στο blockchain δίκτυο, συμπεριλαμβάνονται μόνο τα συμμετέχοντα νοσοκομεία και ιδρύματα και το κίνητρο των χρηστών/ομότιμων κόμβων για να συμμετάσχουν είναι η βελτιωμένη προγνωστική δύναμη του μοντέλου, ώστε να αποκτήσουν νέες γνώσεις σχετικά με τα αποτελέσματα της υγείας των ασθενών και του πληθυσμού.

Τελικά, οι στόχοι αυτής της μεθόδου μάθησης βασισμένης στο blockchain, για τη διαχείριση των ιατρικών αρχείων, περιλαμβάνουν την υποστήριξη μελετών που συγκρίνουν την αποτελεσματικότητα, της βιοϊατρικής έρευνας και τελικά της φροντίδας των ασθενών [128].

ΚΕΦΑΛΑΙΟ 4 : ΠΡΟΚΛΗΣΕΙΣ

Το blockchain είναι μια αναδύομενη τεχνολογία, η οποία όπως μελετήσαμε και στο προηγούμενο κεφάλαιο εξαπλώνεται σε διάφορους κλάδους του τομέα βιοϊατρικής και υγειονομικής περίθαλψης και γενικότερα του τομέα Υγείας. Το υψηλό ποσοστό σε οφέλη και ευκαιρίες δεν πρέπει να μας εφησυχάζει, καθώς η τεχνολογία blockchain έχει το δικό της σύνολο προκλήσεων οι οποίες πρέπει να αντιμετωπιστούν. Οι προκλήσεις που θα μελετήσουμε μπορούν να μετριάσουν α) με προσεκτικό σχεδιασμό και β) υλοποίηση των συστημάτων εφαρμογής της υγειονομικής περίθαλψης.

Οι πιο σημαντικές προκλήσεις παρατίθενται παρακάτω.

4.1) Διαφάνεια (transparency) - Εμπιστευτικότητα (confidentiality)

Η φράση «everyone can see everything» στο δίκτυο blockchain μας επιστρά την προσοχή για την αυξημένη Διαφάνεια και τη μειωμένη Εμπιστευτικότητα του δικτύου.

Οι πληροφορίες κατά τη διάρκεια της μεταφοράς τους εμφανίζουν έντονη διαφάνεια , γεγονός περιοριστικό για το blockchain .

Επίσης, το δίκτυο blockchain παρέχει “ψευδωνυμία” (pseudonymity) και όχι “ανωνυμία” (anonymity) στους χρήστες. Ο κάθε χρήστης χρησιμοποιεί ως διεύθυνση hash values και μπορεί να επαναπροσδιοριστεί μέσω της ανάλυσης των διαθέσιμων πληροφοριών των συναλλαγών του στο δίκτυο blockchain [173], [174], [175], [176].

Τα δεδομένα των ασθενών στους τομείς βιοϊατρικής / υγειονομικής περίθαλψης είναι πολύ ευαίσθητα και οι δύο προκλήσεις πολύ κρίσιμες.

ΛΥΣΕΙΣ : Για να μετριάσουν τα ζητήματα διαφάνειας και εμπιστευτικότητας, συμπεριλαμβάνονται τεχνικές , όπως: α) κρυπτογράφηση των ευαίσθητων δεδομένων [177],[178], [179], β) αποθήκευση των ευαίσθητων δεδομένων off-chain (on-chain να διαδίδονται μόνο τα κρυπτογραφημένα links ή οι πληροφορίες σχετικά με τις άδειες του blockchain) , γ) αυτοματοποίηση πρωτοκόλλων διαχείρισης δεδομένων με τη χρήση έξυπνων συμβολαίων [180], [181], [182].

4.2) Ταχύτητα (speed)

Η συναλλαγή μεταξύ των ενδιαφερομένων μπορεί να διαρκέσει πολύ ώρα , ανάλογα με το πρωτόκολλο που θα χρησιμοποιηθεί. Ένας τέτοιος περιορισμός ταχύτητας μπορεί να περιορίσει την επεκτασιμότητα των εφαρμογών που βασίζονται στο blockchain.

Για το Bitcoin με το πρωτόκολλο PoW , υπάρχουν κατά μέσο όρο περίπου 288.000 συναλλαγές/ημέρα (ή περίπου 3,3 συναλλαγές/δευτερόλεπτο) , λόγω του φόρτου εργασίας υπολογισμού.

Για τη πιστωτική κάρτα, όπως η Visa , υπάρχουν περίπου 150 εκατομμύρια. Συναλλαγές/ημέρα (ή περίπου 2000 συναλλαγές/δευτερόλεπτο) [183], [184].

Η θεωρητική μέγιστη ταχύτητα συναλλαγής του Bitcoin είναι 7 συναλλαγές/δευτερόλεπτο , λόγω περιορισμού στο τρέχον πρωτόκολλο για μέγεθος block στο 1 megabyte , ενώ η θεωρητική μέγιστη ταχύτητα συναλλαγής για τη Visa είναι 4.000 συναλλαγές/δευτερόλεπτο [183], [184].

Αυτό το ζήτημα είναι εξίσου σοβαρό κατά την κατασκευή και δημιουργία των εφαρμογών blockchain σε πραγματικό χρόνο και με δυνατότητα κλιμάκωσης όπως είδαμε στις IoMT (internet of medical things) εφαρμογές.

4.3) Επεκτασιμότητα (scalability)

Λόγω της αποκεντρωμένης αρχιτεκτονικής, το ζήτημα της επεκτασιμότητας είναι λιγότερο σοβαρό. Ωστόσο, οι ιδιωτικές κλινικές, τα κέντρα υγειονομικής περίθαλψης τα αγροτικά νοσοκομεία,, οι οργανισμοί που ερευνούν τις επιχειρήσεις, οι ασφαλιστικές εταιρείες, οι μεμονωμένοι ασθενείς και οι νεοϊδρύνμενες IoT εταιρείες έχουν εκατομμύρια χρήστες με διαφορετική υποδομή. Είναι εξαιρετικά απίθανο ότι όλοι τους είναι ικανοί να διατηρήσουν την ίδια αποκεντρωμένη αρχιτεκτονική blockchain.

Η τεχνολογία blockchain χρειάζεται επίσης υψηλότερη υπολογιστική ισχύ , η οποία απαιτεί υψηλότερη κατανάλωση ηλεκτρικής ενέργειας για τον εξοπλισμό του δικτύου [185].

Το ζήτημα της επεκτασιμότητας για τα μεγάλα δεδομένα της υγειονομικής περίθαλψης (big data) πρέπει να ληφθεί σοβαρά υπόψη, για να κάνει το blockchain δημοφιλές.

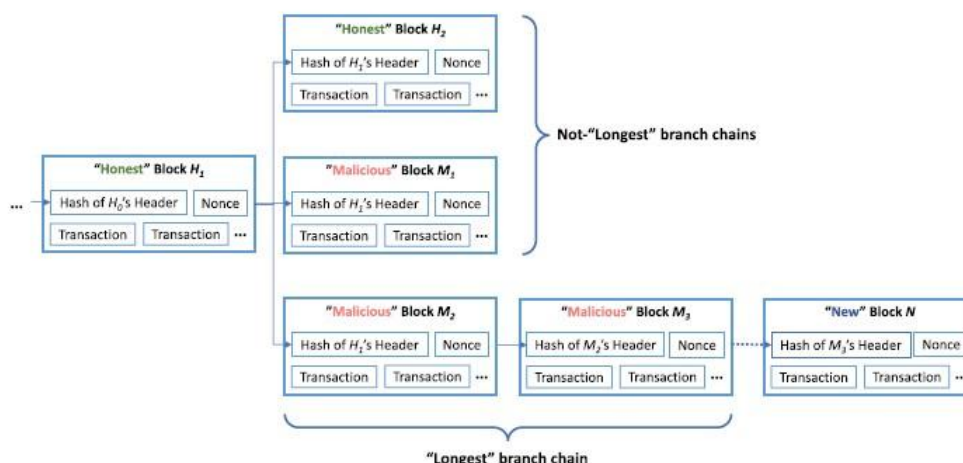
ΛΥΣΕΙΣ : Για τα ζητήματα ταχύτητας και επεκτασιμότητας, προτείνονται λύσεις που εκμεταλλεύονται το blockchain όχι ως αποθετήριο όλων των αρχείων , αλλά ως ευρετήριο των δεδομένων υγειονομικής περίθαλψης [186] και αποθηκεύοντας μόνο τις τρέχουσες επιβεβαιωμένες συναλλαγές , αντί για το πλήρες ιστορικό του blockchain [187].

Επίσης, η εφαρμογή BigChainDB [188],[189] παρέχει σημαντικά υψηλότερη ταχύτητα συναλλαγής σε σχέση με το Bitcoin, και θα μπορούσε έτσι να λυθεί το πρόβλημα της ταχύτητας και επεκτασιμότητας.

4.4) Απειλή επίθεσης 51% (threat of 51% attack)

Σε ένα δίκτυο blockchain υπάρχει η πιθανότητα οι “honest nodes” να είναι λιγότεροι από τους “malicious nodes” . Αυτό είναι η «Απειλή επίθεσης 51%» , διότι το δίκτυο καταλαμβάνεται εξ ολοκλήρου από τους κακόβουλους χρήστες [190], [191], [192].

Αντιλαμβανόμαστε την κρισιμότητα του ζητήματος σε θέματα ασφάλειας των εφαρμογών βιοϊατρικής/υγειονομικής περίθαλψης. Ας δούμε την παρακάτω εικόνα.



Εικόνα 4.1: Απειλή επίθεσης 51% [12]

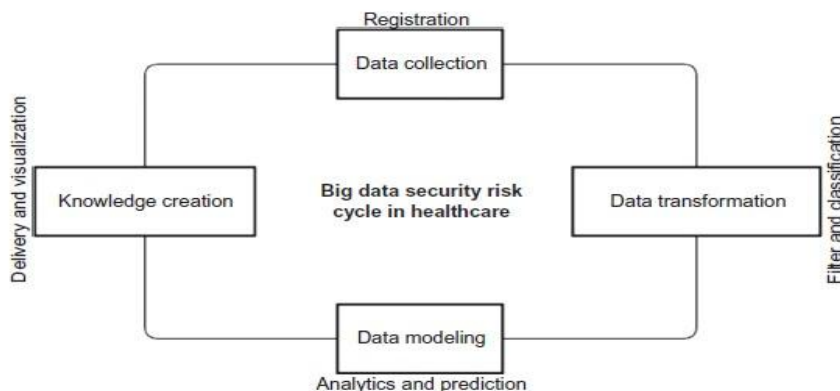
Σε αυτό το σενάριο, οι επιτιθέμενοι δημιούργησαν κακόβουλα blocks (M_1 και M_2) για να ανταγωνιστούν με ένα έντιμο block (H_2). Στόχος τους η κατάληψη του έντιμου block H_1 και όλων των blocks πριν το H_1 . Αυτή τη φορά η υπολογιστική ισχύς των έντιμων κόμβων είναι μικρότερη από την υπολογιστική ισχύ των κακόβουλων κόμβων, καθώς το 51% του δικτύου καταλαμβάνεται από τους κακόβουλους. Έτσι, ένα κακόβουλο block M_3 δημιουργείται αμέσως μετά το M_2 . Με βάση το μηχανισμό του blockchain, τα νέα block N θα δημιουργηθούν στο τέλος της μακρύτερης αλυσίδας $H_1 \rightarrow M_2 \rightarrow M_3$. Ο επιτιθέμενος έχει τροποποιήσει επιτυχώς τα αρχεία του blockchain (από το H_2 στο M_2) και καταλαμβάνει ολόκληρη την αλυσίδα, κερδίζοντας την πλειοψηφία των ψήφων [12].

ΛΥΣΕΙΣ : Η απειλή της 51% επίθεσης στο δίκτυο blockchain μπορεί να ελαττωθεί δραστικά χρησιμοποιώντας ένα εικονικό ιδιωτικό δίκτυο (a virtual private network), για τη διάδοση των δεδομένων και την ανάπτυξη ορισμένων στοιχείων του συστήματος σε private HIP (Health Insurance Portability) καθώς και υποχρέωση λογοδοσίας σε υπολογιστικά περιβάλλοντα cloud (Accountability Act- compliant cloud computing environments), όπως το iDash (Integrating Data for Analysis, Anonymization, Sharing) [193], [194].

4.5) Ασφάλεια (Security)

Το όλο σκεπτικό της χρήσης της τεχνολογίας blockchain είναι οι άνθρωποι που δεν γνωρίζονται μεταξύ τους και δεν εμπιστεύονται ο ένας τον άλλο, να μπορούν να μοιράζονται δεδομένα με έναν ασφαλή και απαραβίαστο τρόπο. Ωστόσο, η ασφάλεια ακόμα και του βέλτιστου μοντέλου blockchain μπορεί να αποτύχει. Είναι αναγκαίο να δημιουργηθούν επαρκείς μηχανισμοί πριν από την προετοιμασία ώστε να μετριαστούν ή να αποτραπούν οι παραβιάσεις ασφαλείας στο blockchain [2].

Ο επιστήμονας Abouelmehdi [195], ανέφερε τον κύκλο κινδύνου ασφαλείας των μεγάλων δεδομένων υγειονομικής περίθαλψης (Risk cycle of healthcare big data security). Αυτή η μελέτη χαρακτήρισε το στάδιο μοντελοποίησης των δεδομένων (data modeling) , ως το πιο επικίνδυνο στάδιο του κύκλου.



Εικόνα 4.2 : Κύκλος κινδύνου για την ασφάλεια των μεγάλων δεδομένων υγειονομικής περίθαλψης [23]

4.6) Αποθήκευση (Storage)

Τα ιατρικά αρχεία και τα αρχεία υγειονομικής περίθαλψης (healthcare and medical data) παράγουν μια τεράστια ποσότητα από EMR και Sensor data , από τους ασθενείς και τις φορητές IoT συσκευές τους. Αντιθέτως, η αρχιτεκτονική του blockchain υποστηρίζει πολύ περιορισμένη αποθήκευση δεδομένων επί της αλυσίδας (on-chain data storage). Η αποκεντρωμένη και κατακερματισμένη αρχιτεκτονική του blockchain έχει πολύ υψηλό κόστος για αποθήκευση δεδομένων. Παρομοίως, η πρόσβαση στα δεδομένα (data access), η διαχείριση δεδομένων (data storage) και οι λειτουργίες στο blockchain μπορεί να είναι δαπανηρή διαδικασία , εάν το μέγεθος των δεδομένων είναι μεγαλύτερο [23].

Επομένως, οι blockchain εφαρμογές πρέπει να σχεδιάζονται λαμβάνοντας υπόψη αυτό τον παράγοντα.

4.7) Τροποποίηση (modification)

Από τη μια πλευρά, το χαρακτηριστικό του blockchain για τη μη μεταβλητότητα των δεδομένων (data immutability) ασφαλίζουν το σύστημα, αλλά από την άλλη πλευρά, δεν αφήνει καμία επιλογή για τροποποίηση και διαγραφή των δεδομένων. Η τροποποίηση των δεδομένων και οι αλλαγές είναι σε αρκετές περιπτώσεις αναπόφευκτες [23].

Είτε χρειάζεται να δημιουργήσουμε ένα νέο block με συναίνεση από όλους τους κόμβους ή να δημιουργήσουμε μια νέα αλυσίδα. Αυτές οι μέθοδοι είναι δαπανηρές και δεν είναι εφικτές.

Επομένως, η ανάπτυξη των εφαρμογών blockchain πρέπει να είναι κατά τέτοιο τρόπο, ώστε η ανάγκη τροποποίησης των δεδομένων να είναι μικρότερη.

4.8) Προστασία της ιδιωτικότητας και κανονισμοί (Privacy and Regulations)

Το blockchain μεγιστοποιεί την ασφάλεια του περιεχομένου του. Η κρυπτογραφημένη, αποκεντρωμένη, ανεξάρτητη, αμετάβλητη αρχιτεκτονική του μπορεί να εξασφαλίσει την υψηλότερη ασφάλεια των περιεχομένων του. Τα μεγάλα δεδομένα υγειονομικής περίθαλψης αφορούν τις ευαίσθητες πληροφορίες του ασθενούς, για τον ασθενή και από τον ασθενή. Η διατήρηση ενός αντιγράφου αυτών των δεδομένων σε κάθε κόμβο, μπορεί να είναι επικίνδυνη [23]. Το πιο κρίσιμο ζήτημα της τεχνολογίας blockchain είναι η αποθήκευση των PII και των EHRs για πάντα.

Αρκετές χώρες και τυποποιημένοι οργανισμοί δεν ακολουθούν αυτή την πρακτική. Πρόκειται για ένα σοβαρό ζήτημα στο οποίο εμπλέκεται και ο Ευρωπαϊκός Κανονισμός GDPR. Κάθε χώρα έχει τους δικούς της κανονισμούς για την προστασία της Ιδιωτικότητας καθώς επίσης και τεχνικές. Το blockchain συμπεριφέρεται μοναδικά και χωρίς διακρίσεις μεταξύ των χωρών.

Country	Law	Key Factor
Angola	Information Protection Law	For sensitive information storing, processing, and collection, legal permission is needed.
United States	<ul style="list-style-type: none"> • HIPAA (Health Insurance Portability and Accountability Act started in 1996) • The Health Information Technology for Economic and Clinical Health (HITECH) Act, February 17, 2009 	<ol style="list-style-type: none"> 1. Right to medical record and health insurance privacy record from 12 to 18 year old citizen. 2. Meaningful use of all Electronic Health Records (EHRs).
Brazil	Law of the Constitution	Personal data and private life and citizen's image are considered as highly sensitive and secured information.
EU	Data Protection Law from Government	Protection of people's personal information during storing and processing.
Russia	Personal Data Act by Russian Federal Law	Data operators are to take all responsibility regarding any unlawful access to data.
United Kingdom	Data Protection Act (DPA)	The individual has huge power in controlling the movement of personal data. Privacy information must follow the country's territorial boundary.
India	IT Act	Any kind of breaching of personal data should compensate the victim.
South Korea	Personal Information Protection Act September 30, 2011	Right, interest, and dignity of the citizen are taken care of. No territorial scope is defined.
EU	General Data Protection Regulation (GDPR)	Personal information protection regulation, in which key factors are consent from the owner, right to forget, and the territorial boundary of data.
United States	National Institute of Standards and Technology (NIST)	Security automation, public awareness, and harmonized security rules are key factors.
New Zealand	Health Information Privacy Code	Special rules of medical institutions on collection, storage, and processing of health data.
Commonwealth	National Electronic Health Transition Authority (NEHTA)	NEHTA aims to unlock eHealth system aspects to improve the electronic health record collecting and exchanging ways.

Πίνακας 4.1 : Κανονισμοί προστασίας της Ιδιωτικότητας για τις διάφορες χώρες και οργανισμούς [23]

4.8.1) Blockchain και GDPR

Το πρόβλημα – πρόκληση σε αυτή τη «σχέση» είναι να εναρμονιστεί η υπόσχεση διαφάνειας του blockchain με τους πολύ αυστηρούς κανόνες για την προστασία της διωτικής ζωής που ισχύουν στα πλαίσια του GDPR της Ευρωπαϊκής Ένωσης [2].

Στο επίκεντρο του GDPR είναι η διασφάλιση των πληροφοριών του ατόμου. Οι οργανισμοί και οι οργανώσεις πρέπει να δίνουν ιδιαίτερη προσοχή σε δύο ζητήματα : α)στη συγκατάθεση των ατόμων και β)στην ανταλλαγή των δεδομένων. Απαιτείται *συναίνεση* προτού αναλυθούν τυχόν ιδιωτικά δεδομένα και υπάρχει επίσης υποχρέωση *λογοδοσίας*, για να επιβεβαιωθεί ότι αυτά τα δεδομένα μπορούν να αποσύρονται ή να διαγράφονται [23].

Το blockchain αντιθέτως, στηρίζεται στη μη μεταβλητότητα των δεδομένων (data immutability) , ενώ ο GDPR απαιτεί όλα τα προσωπικά δεδομένα ή ΠΙ να είναι μεταβλητά ή διαγράψιμα, από οποιονδήποτε οργανισμό, σύμφωνα με την επιθυμία των χρηστών [23].

Στο άρθρο 17, εδάφιο 2 , του GDPR , αναφέρεται : « Η υποχρέωση διαγραφής δεδομένων προσωπικού χαρακτήρα χωρίς αδικαιολόγητη καθυστέρηση».

Η φράση «the right to be forgotten» (το δικαίωμα να ξεχαστεί) , εκφράζει την επιθυμία του GDPR [23].

Αυτή τη στιγμή, οι εγκαταστάσεις αποθήκευσης δεδομένων στο blockchain ακολουθούν την «Αρχή CRAB», (Create Retrive Append Burn, δηλαδή, δημιουργία ανάκτησης για την προσάρτηση εγγραφής). Το ενδιαφέρον κομμάτι είναι το τελευταίο, Burn, δηλαδή να πετάς μακριά το κρυπτογραφικό κλειδί για την πρόσβαση στα δεδομένα του blockchain [23]. Ωστόσο, το GDPR δεν δέχεται αυτή την πράξη ως εξασφάλιση των δεδομένων (ensure of data).

Οι βασικές αλλαγές του GDPR είναι :

- α) Κάθε είδος προσωπικών δεδομένων , πρέπει να συγκεντρώνεται , να αποθηκεύεται και να επεξεργάζεται εντός των εδαφικών ορίων της Ευρωπαϊκής Ένωσης.
- β) Το GDPR μπορεί να επιβάλλει πρόστιμο έως και 4% των κερδών ή 20 εκατομμύρια Ευρώ.
- γ) Ο χρήστης πρέπει να δίνει την συγκατάθεσή του για κάθε είδους συναλλαγή προσωπικών δεδομένων. Η συγκατάθεση πρέπει να είναι απλή και κατανοητή.
- δ) Θα πρέπει να διασφαλίζονται 3 δικαιώματα:
 - Δικαίωμα πρόσβασης (right to access)
 - Δικαίωμα να ξεχαστεί (right to be forgotten)
 - Δικαίωμα παραβίασης της κοινοποίησης (right to breach notification).

ΛΥΣΕΙΣ : Πάνω από όλα , το blockchain πρέπει να συμμορφωθεί με το GDPR, προκειμένου να δουλέψει στην Ευρωπαϊκή Ένωση και με τους πολίτες της Ευρωπαϊκής Ένωσης.

Κάποιες πιθανές λύσεις είναι:

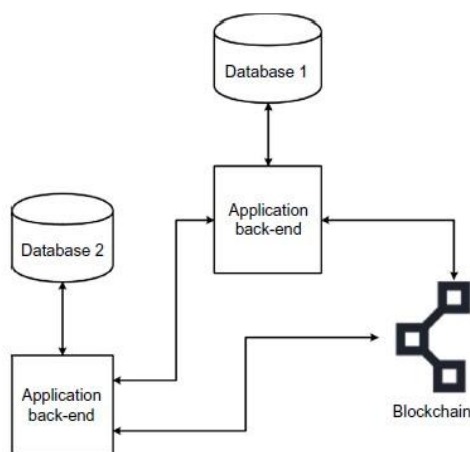
- α) να μην αποθηκεύονται τα προσωπικά δεδομένα στο blockchain,
- β) να καταγράφονται οι προσωπικές πληροφορίες με ψευδο-ανωνυμία,

γ) να αποθηκεύονται πληροφορίες στην αναφερόμενη τοπική κρυπτογραφημένη Β.Δ.

Αρκετές μελέτες πρότειναν μια τροποποιημένη αρχιτεκτονική blockchain, προκειμένου να ικανοποιηθεί το GDPR. Ο Humbeeck [196], πρότεινε μια *off-chain blockchain* αρχιτεκτονική, προκειμένου να ικανοποιηθεί το GDPR. Ο Peterson [197], πρότεινε μια αρχιτεκτονική κοινοτικού δικτύου (*community-based network architecture*) για έναν μηχανισμό ανταλλαγής πληροφοριών υγείας.

A) off-chain blockchain αρχιτεκτονική

Αυτή η μελέτη της *off-chain blockchain* αρχιτεκτονικής, προτείνει έναν μηχανισμό αποθήκευσης δεδομένων δύο επιπέδων. Στην τοπική βάση δεδομένων, οι database1 και database2, θα αποθηκεύσουν εκτός αλυσίδας (*off-chain*) κάθε είδος από τα ευαίσθητων δεδομένων GDPR. Με τη βοήθεια μιας συνδεδεμένης εφαρμογής, αυτό το σύστημα, θα αποθηκεύσει τη σύνδεση (*link*) και το hash των δεδομένων στην αλυσίδα (*on-chain*), δηλαδή στο blockchain. Με αυτό τον τρόπο, το σύστημα μπορεί να διαγράψει δεδομένα από την τοπική βάση δεδομένων οποιαδήποτε στιγμή. Ταυτοχρόνως, το hash των δεδομένων που παραμένει δεν έχει πλέον καμία χρησιμότητα [23].



Εικόνα 4.3: off-chain blockchain αρχιτεκτονική [23]

Πλεονεκτήματα της off-chain blockchain αρχιτεκτονικής :

Η προαναφερθείσα προσέγγιση είναι σύμφωνη με το GDPR, διότι τα προσωπικά δεδομένα μπορούν να διαγραφούν εντελώς. Ομοίως, καθώς ο κατακερματισμός των δεδομένων (*hash of the data*) αποθηκεύεται επί της αλυσίδας (*on-chain*), η ασφάλεια των δεδομένων διατηρείται.

Μειονεκτήματα της off-chain blockchain αρχιτεκτονικής :

Το κύριο μειονέκτημα του προαναφερθέντος συστήματος είναι ότι οποιοσδήποτε μπορεί να συνδεθεί με αυτή τη συγκεκριμένη τοπική Β.Δ. Οι κάτοχοι των δεδομένων μπορούν να έχουν πρόσβαση σε άλλα δεδομένα χωρίς να υπάρχει συγκατάθεση από τους κόμβους. Τα δικαιώματα των κατόχων δεδομένων διακυβεύονται. Η τοπική Β.Δ. είναι ανοιχτή σε περισσότερους φορείς

επίθεσης. Τέλος, η διαχείριση του hash με API, προσθέτει πολυπλοκότητα σε επίπεδο διαχείρισης [23].

Αναπάντητα ερωτήματα για την off-chain blockchain αρχιτεκτονική :

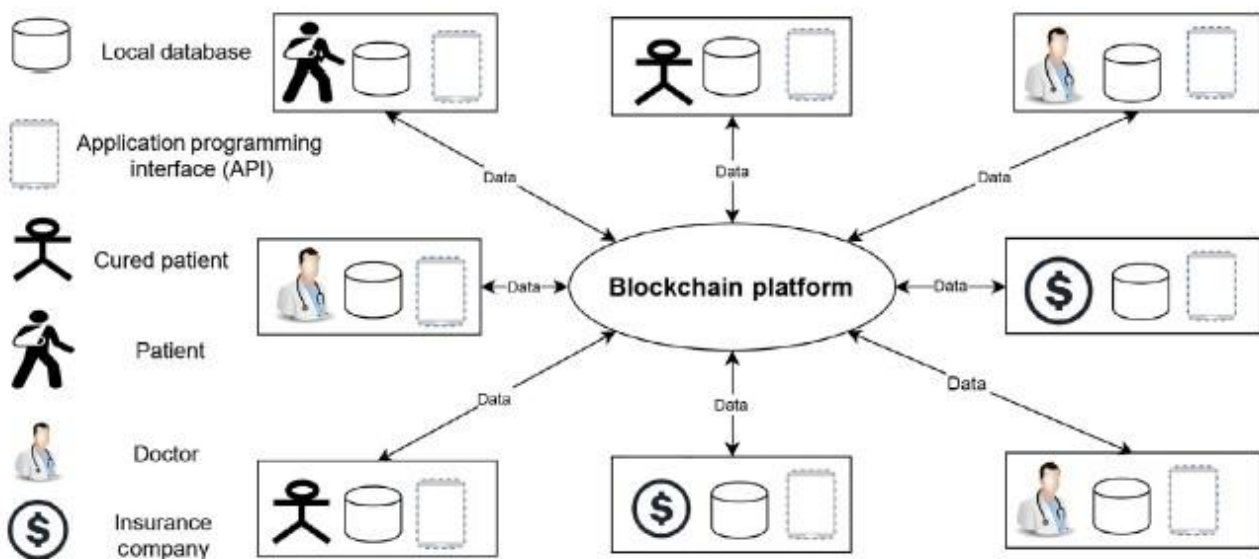
Μπορεί ο μηχανισμός που προτάθηκε να είναι σύμφωνος με το GDPR, παρά όλα αυτά, υπάρχουν μερικές ερωτήσεις που πρέπει να απαντηθούν για να είμαστε σίγουροι για την εφαρμογή αυτής της αρχιτεκτονικής.

- Ποιος είναι ο ιδιοκτήτης των off-chained data;
- Είναι δυνατή η κρυπτογράφηση των off-chained data;
- Είναι η πρόσβαση στα δεδομένα ελεγχόμενη ή όχι;
- Τι γίνεται στην περίπτωση που τα off-chained data αντιγράφονται παράνομα;

B) community-based network αρχιτεκτονική

Αυτή η μελέτη της αρχιτεκτονικής κοινοτικού δικτύου, προτείνει ένα σύστημα, όπου όλα τα δεδομένα, για έναν συγκεκριμένο κόμβο, έχουν πρόσβαση, εάν και μόνο αν η δομή και σημασιολογία των δεδομένων κατανοούνται και εγκρίνονται από όλα τα μέλη της κοινότητας. Οι ασθενείς έχουν τον πλήρη έλεγχο του privacy και των κανονισμών αυτών των δεδομένων που μοιράζονται. Ωστόσο, η άμεση αποθήκευση των προσωπικών δεδομένων είναι το κύριο μειονέκτημα.

Παρακάτω θα δούμε μια συνολική εικόνα της μελλοντικής διαχείρισης των μεγάλων δεδομένων και της αρχιτεκτονικής για τη συλλογή ιατρικών αποφάσεων.



Εικόνα 4.4: Συνεργασία του blockchain συμβατή με το GDPR για τα μεγάλα δεδομένα υγειονομικής περίθαλψης [23]

ΚΕΦΑΛΑΙΟ 5 : ΕΠΙΛΟΓΟΣ

5.1) Μελλοντικές προοπτικές:

Η τεχνολογία blockchain έχει πολλά πλεονεκτήματα που προσφέρει στον τομέα της Υγείας. Ο τρόπος με τον οποίο το Διαδίκτυο έφερε την επανάσταση στην υγειονομική περίθαλψη και εισήγαγε την τηλεϊατρική παρομοιάζει με την εξέλιξη της τεχνολογίας blockchain η οποία είναι πιθανόν να οδηγήσει μελλοντικά την ιατρική επιστήμη σε άλλο επίπεδο. Η χρήση του blockchain σε κλινικά περιβάλλοντα θα μειώσει το κόστος παρακολούθησης, θα βελτιώσει τη διαχείριση των ιατρικών δεδομένων και θα μειώσει δραστικά το χρόνο επεξεργασίας τους. Με την εγγραφή ενός ασθενούς, θα είναι διαθέσιμη η πλήρης συλλογή των δεδομένων του, ταυτόχρονα, στο καταναεμημένο καθολικό.

Επιπλέον, οι θεράποντες ιατροί δεν θα ανησυχούν πλέον για την εγκυρότητα και ειλικρίνεια του ιατρικού ιστορικού των ασθενών τους, λόγω της ικανότητάς τους να προβάλλουν τα πρωτότυπα, αυθεντικά, και τεκμηριωμένα δεδομένα σε πραγματικό χρόνο και φυσικά επιτυγχάνεται και η μείωση πιθανών σφαλμάτων στο ιατρικό ιστορικό. Ομοίως, οι ασθενείς δεν θα πρέπει να απασχολούνται και να ανησυχούν για μια δεύτερη γνώμη από άλλο γιατρό, λόγω της διαφάνειας των δεδομένων που επικρατεί στο blockchain. Επίσης, μέσω των ιατρικών τους αρχείων σε ένα δίκτυο blockchain, οι ασθενείς θα μπορούν να γνωρίζουν και άλλα άτομα, από όλο τον κόσμο, με παρόμοιες ιατρικές παθήσεις. Αυτή η επικοινωνία θα βοηθήσει τους ασθενείς να αισθάνονται πιο αποδεκτοί, υποστηριζόμενοι, και θα ενισχύσει τη θέλησή τους για να καταπολεμήσουν την ασθένεια που τους ταλαιπωρεί. Αξίζει να επισημάνουμε ότι οι ασθενείς θα έχουν πλήρη αυτονομία στα δεδομένα τους και θα μπορούν να αποφασίζουν οι ίδιοι με ποιον θα τα μοιραστούν.

5.2) Επιπτώσεις και συμπεράσματα:

Παρά το γεγονός ότι ο τομέας της υγειονομικής περίθαλψης καθυστερεί αρκετές φορές στη λήψη και διαχείριση νέων εξελίξεων, μπορεί να υπάρξει κίνητρο για υιοθέτηση του blockchain στην υγειονομική περίθαλψη στο εγγύς μέλλον. Η διαχείριση των ηλεκτρονικών αρχείων υγείας στο blockchain έχει σημεία στα οποία αξίζει ιδιαίτερη προσοχή. Η εφαρμογή των έξυπνων συμβάσεων μας ενθαρρύνει να τα υιοθετήσουμε για όλες τις συναλλαγές στον κλάδο της υγειονομικής περίθαλψης. Οι έξυπνες συμβάσεις θα κάνουν την αλυσίδα των blocks άθραυστη που θα λαμβάνει εξατομικευμένη φροντίδα, χωρίς να σπάει τα κλινικά πλαίσια. Με την ενσωμάτωση των κλινικών συστημάτων σε έξυπνα συμβόλαια blockchain, θα επιτευχθεί η αντίσταση στην παραγωγή οποιουδήποτε διπλού αντιγράφου στο μητρώο του συστήματος. Η βοήθεια που παρέχει το blockchain στους ερευνητές, είναι ότι παρέχει επιστημονικές μελέτες

επαληθευμένες και με χρονική σήμανση. Όπως τα έξυπνα συμβόλαια επιτρέπουν στους ασθενείς να ελέγχουν τα δεδομένα τους, έτσι και το αρχείο blockchain επιτρέπει στους ερευνητές να έχουν ένα πλήρες ιστορικό των ευρημάτων τους.

Στον τεράστιο τομέα της φαρμακευτικής βιομηχανίας, το blockchain είναι απολύτως απαραίτητο. Με το blockchain μπορούμε να παρακολουθήσουμε όλες τις αναφερόμενες διαδρομές των φαρμακευτικών προϊόντων. Αυτή η ρύθμιση θα επεκτείνει την ταχύτητα προετοιμασίας των δεδομένων, την εγγύηση της διάδοσης των αρχείων και τη μείωση της πιθανότητας απώλειας, βλάβης ή τροποποίησης των αρχείων. Αυτά τα κρίσιμα σημεία ελέγχονται από την ίδια την τεχνολογία. Το κάθε block που δημιουργήθηκε και προστέθηκε στην αλυσίδα δεν μπορεί να τροποποιηθεί αλλά ούτε και να διαγραφεί. Το blockchain εγγυάται ότι τα δεδομένα δεν μπορούν να νοθευτούν καθώς απορρίπτει τα παραποιημένα φάρμακα. Αυτό επιτυγχάνεται με μέσω του ελέγχου όλων των διαδικασιών στην αλυσίδα παραγωγής, εφοδιαστικής και πώλησης των φαρμακευτικών προϊόντων.

Η χρήση της τεχνολογίας blockchain στον τομέα της Υγείας θα ωφελήσει ένα μεγάλο αριθμό ατόμων, γιατρούς, παρόχους υγειονομικής περίθαλψης, βιοιατρικούς ερευνητές, ασθενείς να διαχειριστούν αποτελεσματικά τον τεράστιο όγκο δεδομένων, να μοιραστούν τη γνώση και να επικοινωνήσουν μεταξύ τους με μεγαλύτερη ασφάλεια και προστασία του απορρήτου. Η επιτυχής εφαρμογή της τεχνολογίας σε κλινικά ζητήματα θα ανοίξει νέους ορίζοντες για την πρόοδο της βιοιατρικής έρευνας. Από τη άλλη πλευρά, αυτή η ασφαλής αποθήκευση και ανταλλαγή αυτών των κλινικών δεδομένων θα βοηθήσει στην ανάπτυξη πιθανών στρατηγικών για τη διάγνωση και θεραπεία διαφόρων ασθενειών. Ένα blockchain θα μπορούσε να χρησιμοποιηθεί για συστήματα νευρικού ελέγχου καθώς και για την ψηφιοποίηση του εγκεφάλου. Η νευροτεχνολογία παραμένει σε πειραματικό στάδιο και μόνο ελάχιστες εταιρίες έχουν φτάσει στο βαθμό να επιβεβαιώνουν τη χρήση της τεχνολογίας blockchain στις έρευνές τους.

Το ερώτημα βέβαια είναι για το πόσο ασφαλή θα είναι τα προσωπικά δεδομένα του εγκεφάλου σε ένα blockchain. Η αποκεντρωμένη και διαφανής φύση της τεχνολογίας σίγουρα εμποδίζει την τροποποίηση ή την κλοπή αυτών των δεδομένων, αλλά εξακολουθούν να υφίστανται πολλές από τις γενικές ανησυχίες σχετικά με τη συλλογή δεδομένων μεγάλης κλίμακας. Αυτά τα ευαίσθητα δεδομένα ενδέχεται να καταλήξουν να πωλούνται σε τρίτους για αμφισβητήσιμους σκοπούς και αυτοί οι χρήστες ενδέχεται να εξακολουθούν να είναι έμμεσα αναγνωρίσιμοι μέσω ψευδωνύμων.

Κατά συνέπεια, αυτό το πλαίσιο υγειονομικής περίθαλψης που βασίζεται σε blockchain θα προσελκύσει περισσότερα άτομα στην υγειονομική περίθαλψη και τελικά θα βελτιώσει την ποιότητα ζωής όλων με πιο ασφαλή και σίγουρο τρόπο.

ΒΙΒΛΙΟΓΡΑΦΙΑ

- [1] D. Munro, Data Breaches in Healthcare Totaled Over 112 Million Records in 2015, vol. 31, Forbes, New York, NY, 2015.
In: Md. Mehedi Hassan Onik, Satyabrata Aich, Jinhong Yang, Chul-Soo Kim, Hee-Cheol Kim, Blockchain in healthcare: Challenges and solutions
- [2] Maged N. Kamel Boulos, James T. Wilson and Kevin A. Clauson (2018), Geospatial blockchain: promises, challenges, and scenarios in health and healthcare.
- [3] McConaghy T, Marques R, Muller A, et al. BigchainDB (2016): A Scalable Blockchain Database. <https://www.bigchaindb.com/whitepaper/>. Accessed July 30, 2016,
Meunier S. (2017) Blockchain Technology—a Very Special Kind of Distributed Database. Medium. <https://medium.com/@sbmeunier/blockchain-technology-a-very-special-kind-of-distributed-database-e63d00781118>. Accessed April 6, 2017.
Martin L. Blockchain vs. Relational Database: Which is right for your Application? TechBeacon. <https://techbeacon.com/Blockchain-relational-database-which-right-for-your-application>. Accessed April 6, 2017.
In: Tsung-Ting Kuo, Hyeon-Eui Kim, and Lucila Ohno-Machado,(2017), Blockchain distributed ledger technologies for biomedical and health care applications.
- [4] Kuo T-T, Hsu C-N, Ohno-Machado L. ModelChain (2016): Decentralized Privacy-Preserving Healthcare Predictive Modeling Framework on Private Blockchain Networks. ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST; 2016.
McConaghy T, Marques R, Muller A, et al. BigchainDB (2016): A Scalable Blockchain Database. <https://www.bigchaindb.com/whitepaper/>. Accessed July 30, 2016.
ONC/NIST Use of Blockchain in Healthcare and Research Workshop (2016). <https://oncprojectracking.healthit.gov/wiki/display/TechLabI/Useof+Blockchain+in+Healthcare+and+Research+Workshop>. Accessed December 20, 2016.
In: Tsung-Ting Kuo, Hyeon-Eui Kim, and Lucila Ohno-Machado,(2017), Blockchain distributed ledger technologies for biomedical and health care applications.
- [5] McConaghy T, Marques R, Muller A, et al. BigchainDB (2016): A Scalable Blockchain Database. <https://www.bigchaindb.com/whitepaper/>. Accessed July 30, 2016.
In: Tsung-Ting Kuo, Hyeon-Eui Kim, and Lucila Ohno-Machado, (2017), Blockchain distributed ledger technologies for biomedical and health care applications.
- [6] Lorenz J-T, Munstermann B, Higginson M, Olesen PB, Bohlken N, Ricciardi V. (2017). Blockchain in Insurance – Opportunity or Threat? McKinsey & Company. <https://www.mckinsey.com/~media/McKinsey/Industries/Financial%20Services/Our%20Insights/Blockchain%20in%20insurance%20opportunity%20or%20threat/Blockchain-in-insurance-opportunity-or-threat.ashx> . Accessed April 21, 2017.
In: Tsung-Ting Kuo, Hyeon-Eui Kim, and Lucila Ohno-Machado, (2017), Blockchain distributed ledger technologies for biomedical and health care applications.

- [7] Martin L.(2017) Blockchain vs. Relational Database: Which is right for your Application? TechBeacon. <https://techbeacon.com/Blockchain-relational-database-which-right-for-your-application>. Accessed April 6, 2017.
In: Tsung-Ting Kuo, Hyeon-Eui Kim, and Lucila Ohno-Machado, (2017), Blockchain distributed ledger technologies for biomedical and health care applications.
- [8] Bitcoin Wiki. SHA-256. <https://en.bitcoin.it/wiki/SHA-256> . Accessed April 6, 2017.
In: Tsung-Ting Kuo, Hyeon-Eui Kim, and Lucila Ohno-Machado,(2017), Blockchain distributed ledger technologies for biomedical and health care applications.
- [9] Bitcoin Wiki. Elliptic Curve Digital Signature Algorithm. https://en.bitcoin.it/wiki/Elliptic_Curve_Digital_Signature_Algorithm. Accessed April 6, 2017.
In: Tsung-Ting Kuo, Hyeon-Eui Kim, and Lucila Ohno-Machado, (2017), Blockchain distributed ledger technologies for biomedical and health care applications.
- [10] Dr Celine Herweijer, Dominic Waughray, Sheila Warren, (2018). Building Block(chain)s for a Better Planet. In World Economic Forum : Fourth Industrial Revolution for the Earth Series
- [11] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. <https://bitcoin.org/bitcoin.pdf>. 2008. Accessed July 30, 2016.
Davis J. The Crypto-currency: Bitcoin and Its Mysterious Inventor.The New Yorker. <http://www.newyorker.com/magazine/2011/10/10/the-crypto-currency>. Accessed January 11, 2017.
Calvery JS. Statement of Jennifer Shasky Calvery, Director Financial Crimes Enforcement Network United States Department of the Treasury. Vienna, Virginia, United States: Financial Crimes Enforcement Network; 2013.
Dillet R. Bitcoin Ticker Available On Bloomberg Terminal For Employees. TechCrunch. <https://techcrunch.com/2013/08/09/bitcoin-tickeravailable-on-bloomberg-terminal/> . Accessed December 14, 2016.
XE.COM INC. Currency Encyclopedia - XBT Bitcoin. <http://www.xe.com/currency/xbt-bitcoin>. Accessed February 15, 2017.
CoinDesk. Bitcoin Price. <http://www.coindesk.com/price/> . Accessed April 13, 2017.
CoinMarketCap. Crypto-Currency Market Capitalizations. <https://coinmarketcap.com/> . Accessed April 13, 2017.
Draupnir M. What Can You Buy with Bitcoin. WeUseCoins. <https://www.weusecoins.com/what-can-you-buy-with-bitcoin/>. Accessed December 14, 2016.
CoinDesk. What Can You Buy with Bitcoin. <http://www.coindesk.com/information/what-can-you-buy-with-bitcoins/>. Accessed December 14, 2016.
Coinbase.com.Where Can I Spend Bitcoin. <https://support.coinbase.com/customer/portal/articles/1834716>. Accessed December 14, 2016.
Hughes M. What Are Bitcoins Actually Used For Now in 2016. MakeUseOf. <http://www.makeuseof.com/tag/bitcoins-actually-used-now-2016/> . Accessed December 14, 2016.
In: Tsung-Ting Kuo, Hyeon-Eui Kim, and Lucila Ohno-Machado,(2017), Blockchain distributed ledger technologies for biomedical and health care applications.
- [12] Tsung-Ting Kuo, Hyeon-Eui Kim, and Lucila Ohno-Machado, (2017), Blockchain distributed ledger technologies for biomedical and health care applications
- [13] Kuo T-T, Hsu C-N, Ohno-Machado L.ModelChain, (2016): Decentralized Privacy-Preserving Healthcare Predictive Modeling Framework on Private Blockchain Networks. ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST; 2016.

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

[14] Lamport L. Password authentication with insecure communication. Commun ACM 1981;24(11):770–72.

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

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

[16] Kelsey J. (2016) Introduction to Blockchains. ONC/NIST Use of Blockchain for Healthcare and Research Workshop . Gaithersburg, Maryland, United States: ONC/NIST; 2016.

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

[17] Bitcoin.org. Bitcoin Developer Guide. <https://bitcoin.org/en/developerguide>. Accessed February 1 , 2017.

Blockchain Luxembourg S.A. Unconfirmed Transactions: Live Updating List of New Bitcoin Transactions. <https://blockchain.info/unconfirmedtransactions>. Accessed February 10, 2017.

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

[18] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. <https://bitcoin.org/bitcoin.pdf> . 2008. Accessed July 30, 2016.

Garay J, Kiayias A, Leonardos N. The bitcoin backbone protocol: Analysis and applications. Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin, Heidelberg: Springer; 2015:281–310.

Eyal I, Sirer EG. Majority is not enough: Bitcoin mining is vulnerable. International Conference on Financial Cryptography and Data Security. Springer; 2014:436–54.

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

[19] Blockchain definition. https://en.bitcoin.it/wiki/Block_chain. Accessed 20 Dec 2016

Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money Gareth W. Peters, Efstathios Panayi, CoRR abs/1511.05740. 2015. <http://arxiv.org/pdf/1511.05740.pdf>.

<https://en.wikipedia.org/wiki/Blockchain>.

In: Mehdi Benchoufi and Philippe Ravaud (2017), Blockchain technology for improving clinical research quality : DOI 10.1186/s13063-017-2035-z

[20] Bitcoin NS. A peer-to-peer electronic cash system. Bitcoin.org (online). 2009. <https://bitcoin.org/bitcoin.pdf>. Accessed 14 June 2018.

Buterin V. Ethereum white paper. GitHub (online). 2018. <https://github.com/ethereum/wiki/wiki/White-Paper> . Accessed 14 June 2018.

In: Maged N. Kamel Boulos, James T. Wilson and Kevin A. Clauson (2018), Geospatial blockchain: promises, challenges, and scenarios in health and healthcare, <https://doi.org/10.1186/s12942-018-0144-x>

- [21] Ribitzky R, St Clair J, Houlding DI, McFarlane CT, Ahier B, Gould M, Flannery HL, Pupo E, Clauson KA. Pragmatic, interdisciplinary perspectives on blockchain and distributed ledger technology: paving the future for healthcare. *Blockchain Healthc Today*. 2018;1:24.
<https://doi.org/10.30953/bhty.v1.24>.
In: Maged N. Kamel Boulos, James T. Wilson and Kevin A. Clauson (2018), *Geospatial blockchain: promises, challenges, and scenarios in health and healthcare*, <https://doi.org/10.1186/s12942-018-0144-x>
- [22] Sedgwick K. You can now 51% attack a coin for as little as \$500. *Bitcoin.com* (online). 2018 May. <https://news.bitcoin.com/you-can-now-51-attack-a-coin-for-as-little-as-500/>. Accessed 14 June 2018.
(Anonymous). PoW 51% attack cost—this is a collection of coins and the theoretical cost of a 51% attack on each network. *Crypto51* (online). 2018. <https://www.crypto51.app/>. Accessed 14 June 2018.
In: Maged N. Kamel Boulos, James T. Wilson and Kevin A. Clauson (2018), *Geospatial blockchain: promises, challenges, and scenarios in health and healthcare*, <https://doi.org/10.1186/s12942-018-0144-x>
- [23] Md. Mehedi Hassan Onik, Satyabrata Aich, Jinhong Yang, Chul-Soo Kim, Hee-Cheol Kim (2019), *Big Data Analytics for Intelligent Healthcare Management*, chapter 8 : blockchain in healthcare-challenges and solutions (pp 203) # 2019 Elsevier Inc. All rights reserved.
<https://doi.org/10.1016/B978-0-12-818146-1.00008-8>
- [24] McConaghy T, Marques R, Müller A, et al. *BigchainDB: A Scalable Blockchain Database*. <https://www.bigchaindb.com/whitepaper/>. Accessed July 30, 2016.
Greenspan G. *MultiChain Private Blockchain*. <http://www.multichain.com/download/MultiChain-White-Paper.pdf>. Accessed July 30, 2016.
Vukolić M. The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. *International Workshop on Open Problems in Network Security*. Zurich, Switzerland: Springer; 2015:112–25.
Mainelli M, Smith M. Sharing ledgers for sharing economies: an exploration of mutual distributed ledgers (aka blockchain technology). *J Financial Perspect*. 2015;3(3):38–69.
MultiChain. *MultiChain open platform for blockchain applications*. <http://www.multichain.com/>. Accessed December 16, 2016.
BigchainDB GmbH. *BigchainDB The scalable blockchain database*. <https://www.bigchaindb.com/>. Accessed December 16, 2016.
In: Tsung-Ting Kuo, Hyeon-Eui Kim, and Lucila Ohno-Machado,(2017), *Blockchain distributed ledger technologies for biomedical and health care applications*.
- [25] Buterin V. *A Next-generation Smart Contract and Decentralized Application Platform*. <https://github.com/ethereum/wiki/wiki/White-Paper>. Accessed July 31, 2016.
Wood G. *Ethereum: A Secure Decentralised Generalised Transaction Ledger*. <http://www.cryptopapers.net/papers/ethereum-yellowpaper.pdf>. Accessed October 11, 2016. 2014.
Ethereum Foundation. *The Ethereum Project*. <https://www.ethereum.org/>. Accessed December 16, 2016.
Del Castillo M. *Microsoft Doubles Down on Ethereum With New Blockchain Product*. *CoinDesk*. <http://www.coindesk.com/microsoft-launching-new-ethereum-blockchain-product/>. Accessed December 16, 2016.
In: Tsung-Ting Kuo, Hyeon-Eui Kim, and Lucila Ohno-Machado,(2017), *Blockchain distributed ledger technologies for biomedical and health care applications*.
- [26] Md. Mehedi Hassan Onik, Satyabrata Aich, Jinhong Yang, Chul-Soo Kim, Hee-Cheol Kim (2019), *Big Data Analytics for Intelligent Healthcare Management*, chapter 8 : blockchain in healthcare-challenges and solutions # 2019 Elsevier Inc. All rights reserved.

<https://doi.org/10.1016/B978-0-12-818146-1.00008-8>

[27] Mettler M. (2016), Blockchain technology in healthcare: the revolution starts here. IEEE 18th International Conference on e-Health Networking, September 14–16, 2016. Piscataway, NJ: IEEE. <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7749510> . Accessed March 3, 2017.

In: Suveen Angraal, MBBS; Harlan M. Krumholz, MD, SM; Wade L. Schulz, MD, PhD (2017) Cardiovascular Perspective : blockchain technology-applications in healthcare.

Buldas A, Kroonmaa A, Laanoja R. Keyless Signatures’ Infrastructure: how to build global distributed hash-trees. <https://eprint.iacr.org/2013/834.pdf> .

Guardtime secures over a million Estonian healthcare records on the blockchain. <http://www.ibtimes.co.uk/guardtime-secures-over-million-estonian-healthcare-records-blockchain1547367> Accessed 25 Jan 2017.

In: Mehdi Benchoufi and Philippe Ravaud (2017), Blockchain technology for improving clinical research quality : DOI 10.1186/s13063-017-2035-z

[28] <https://www.healthbank.coop/>

[29] <https://patientory.com/>

[30] <https://isolve.io/>

[31] M. Hahnel, Blockchain Enabled Genome Security From the Moment It Is Sequenced, Retrieved from: <https://www.genomes.io/wp-content/uploads/2018/03/The-genomes.io-Whitepaper-V-1.1.4.pdf>, 2018. Accessed 14 June 2018.

In: Md. Mehedi Hassan Onik, Satyabrata Aich, Jinhong Yang, Chul-Soo Kim, Hee-Cheol Kim (2019), Big Data Analytics for Intelligent Healthcare Management, chapter 8 : blockchain in healthcare-challenges and solutions # 2019 Elsevier Inc. All rights reserved.

<https://doi.org/10.1016/B978-0-12-818146-1.00008-8>

[32] G. Jones, Universal Health Coin (UHC), Retrieved from: <https://www.universalhealthcoin.com/>, 2017. Accessed 14 June 2018.

In: Md. Mehedi Hassan Onik, Satyabrata Aich, Jinhong Yang, Chul-Soo Kim, Hee-Cheol Kim (2019), Big Data Analytics for Intelligent Healthcare Management, chapter 8 : blockchain in healthcare-challenges and solutions # 2019 Elsevier Inc. All rights reserved.

<https://doi.org/10.1016/B978-0-12-818146-1.00008-8>

[33] <https://modum.io/>

[34] <https://enterprise.gem.co/health/>

[35] T.T. Kuo, L. Ohno-Machado, ModelChain (2018): Decentralized Privacy-Preserving Healthcare Predictive Modeling Framework on Private Blockchain Networks, 2018. arXiv preprint arXiv:1802.01746.

In: Md. Mehedi Hassan Onik, Satyabrata Aich, Jinhong Yang, Chul-Soo Kim, Hee-Cheol Kim (2019), Big Data Analytics for Intelligent Healthcare Management, chapter 8 : blockchain in healthcare-challenges and solutions # 2019 Elsevier Inc. All rights reserved.

<https://doi.org/10.1016/B978-0-12-818146-1.00008-8>

[36] <https://pokitdok.com/>

- [37] Burst IQ, Retrieved from: <https://www.burstiq.com/>, 2015. Accessed 14 June 2018.
- [38] <https://medicalchain.com/en/>
- [39] J. Robinson, M. Leonard Kish, YouBase Whitepaper, Retrieved from: <https://legacy.gitbook.com/book/joshrobinson/youbase/details>, 2016. Accessed 14 June 2018
- [40] Healthcombix, Retrieved from: <https://healthcombix.com/>, 2016. Accessed 14 June 2018.
- [41] B. Smith, DokChain, Retrieved from: <https://pokitdok.com/dokchain/>, 2016. Accessed 14 June 2018.
- [42] Md. Mehedi Hassan Onik, Satyabrata Aich, Jinhong Yang, Chul-Soo Kim, Hee-Cheol Kim (2019), Big Data Analytics for Intelligent Healthcare Management, chapter 8 : blockchain in healthcare-challenges and solutions # 2019 Elsevier Inc. All rights reserved.
<https://doi.org/10.1016/B978-0-12-818146-1.00008-8>
A. Azaria, A. Ekblaw, T. Vieira, A. Lippman, Medrec: using blockchain for medical data access and permission management, in: International Conference on Open and Big Data (OBD), IEEE, 2016, pp. 25–30.
In: Md. Mehedi Hassan Onik, Satyabrata Aich, Jinhong Yang, Chul-Soo Kim, Hee-Cheol Kim (2019), Big Data Analytics for Intelligent Healthcare Management, chapter 8 : blockchain in healthcare-challenges and solutions # 2019 Elsevier Inc. All rights reserved.
<https://doi.org/10.1016/B978-0-12-818146-1.00008-8>
- Suveen Angraal, MBBS; Harlan M. Krumholz, MD, SM; Wade L. Schulz, MD, PhD(2017) Cardiovascular Perspective : blockchain technology-applications in healthcare.
- Angraal S, Krumholz HM, Schulz WL. Blockchain technology: Applications in health care. *Circ Cardiovasc Qual Outcomes*. 2017;10(9):1–4. <https://doi.org/10.1161/CIRCO.UTCOMES.117.00380>.
- Lippman A, Narula N. Building a Blockchain for medical data management MIT Technology Review (online). 2018 Apr. <https://event.technologyreview.com/video/watch/andre-w-lippman-mit-block-chain-healthcare/>. Accessed 14 June 2018.
- Bell L, Buchanan WJ, Cameron J, Lo O. Applications of Blockchain within healthcare. *Blockchain Healthc Today*. 2018;1:8. <https://doi.org/10.30953/bhty.v1.8>.
- In: Maged N. Kamel Boulos, James T. Wilson and Kevin A. Clauson (2018), Geospatial blockchain: promises, challenges, and scenarios in health and healthcare, <https://doi.org/10.1186/s12942-018-0144-x>
- [43] Castaldo, L.; Cinque, V. Blockchain-based logging for the cross-border exchange of ehealth data in Europe. In International ISCSIS Security Workshop; Springer: Cham, Switzerland, 2018; pp. 46–56.
In: Seyednima Khezr, Md Moniruzzaman, Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, *Appl. Sci.* **2019**, 9, 1736; doi:10.3390/app9091736
- [44] 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. [CrossRef] [PubMed]
In: Seyednima Khezr, Md Moniruzzaman, Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, *Appl. Sci.* **2019**, 9, 1736; doi:10.3390/app9091736

- [45] Patel, V. A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. *Health Inform. J.* **2018**. [[CrossRef](#)]
In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, *Appl. Sci.* **2019**, 9, 1736; doi:10.3390/app9091736
- [46] Fan, K.; Wang, S.; Ren, Y.; Li, H.; Yang, Y. Medblock: Efficient and secure medical data sharing via blockchain. *J. Med. Syst.* **2018**, 42, 136. [[CrossRef](#)]
In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, *Appl. Sci.* **2019**, 9, 1736; doi:10.3390/app9091736
- [47] Ji, Y.; Zhang, J.; Ma, J.; Yang, C.; Yao, X. BMPLS: Blockchain-based multi-level privacy-preserving locationsharing scheme for telecare medical information systems. *J. Med. Syst.* **2018**, 42, 147. [[CrossRef](#)]
In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, *Appl. Sci.* **2019**, 9, 1736; doi:10.3390/app9091736
- [48] Shen, B.; Guo, J.; Yang, Y. MedChain: Efficient Healthcare Data Sharing via Blockchain. *Appl. Sci.* **2019**, 9, 1207. [[CrossRef](#)]
In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, *Appl. Sci.* **2019**, 9, 1736; doi:10.3390/app9091736
- [49] Zhu, L.; Wu, Y.; Gai, K.; Choo, K.K.R. Controllable and trustworthy blockchain-based cloud data management. *Future Gen. Comput. Syst.* **2019**, 91, 527–535. [[CrossRef](#)]
In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, *Appl. Sci.* **2019**, 9, 1736; doi:10.3390/app9091736
- [50] Genestier, P.; Zouarhi, S.; Limeux, P.; Excoffier, D.; Prola, A.; Sandon, S.; Temerson, J.M. Blockchain for consent management in the ehealth environment: A nugget for privacy and security challenges. *J. Int. Soc. Telemed. eHealth* **2017**, 5, GKR-e24.
In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, *Appl. Sci.* **2019**, 9, 1736; doi:10.3390/app9091736
- [51] Al Omar, A.; Bhuiyan, M.Z.A.; Basu, A.; Kiyomoto, S.; Rahman, M.S. Privacy-friendly platform for healthcare data in cloud based on blockchain environment. *Future Gen. Comput. Syst.* **2019**, 95, 511–521. [[CrossRef](#)]
In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, *Appl. Sci.* **2019**, 9, 1736; doi:10.3390/app9091736
- [52] Kaur, H.; Alam, M.A.; Jameel, R.; Mourya, A.K.; Chang, V. A Proposed Solution and Future Direction for Blockchain-Based Heterogeneous Medicare Data in Cloud Environment. *J. Med. Syst.* **2018**, 42, 156.

[CrossRef]

In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

[53] Chen, Y.; Ding, S.; Xu, Z.; Zheng, H.; Yang, S. Blockchain-Based Medical Records Secure Storage and Medical Service Framework. J. Med. Syst. **2018**, 43, 5. [CrossRef]

In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

[54] Guo, R.; Shi, H.; Zhao, Q.; Zheng, D. Secure attribute-based signature scheme with multiple authorities for Blockchain in electronic health records systems. IEEE Access **2018**, 776, 1–12. [CrossRef]

In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

[55] Wang, H.; Song, Y. Secure cloud-based EHR system using attribute-based cryptosystem and blockchain. J. Med. Syst. **2018**, 42, 152. [CrossRef]

In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

[56] Roehrs, A.; da Costa, C.A.; da Rosa Righi, R. OmniPHR: A distributed architecture model to integrate personal health records. J. Biomed. Inform. **2017**, 71, 70–81. [CrossRef]

In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

[57] Hussein, A.F.; ArunKumar, N.; Ramirez-Gonzalez, G.; Abdulhay, E.; Tavares, J.M.R.; de Albuquerque, V.H.C. A Medical Records Managing and Securing Blockchain Based System Supported by a Genetic Algorithm and DiscreteWavelet Transform. Cognit. Syst. Res. **2018**, 52, 1–11. [CrossRef]

In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

[58] Benchoufi, M.; Porcher, R.; Ravaud, P. Blockchain protocols in clinical trials: Transparency and traceability of consent. F1000Research **2017**, 6, 66. [CrossRef] [PubMed]

Nugent, T.; Upton, D.; Cimpoesu, M. Improving data transparency in clinical trials using blockchain smart contracts. F1000Research **2016**, 5, 2541. [CrossRef]

Shae, Z.; Tsai, J.J. On the design of a blockchain platform for clinical trial and precision medicine. In Proceedings of the 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), Atlanta, GA, USA, 5–8 June 2017; pp. 1972–1980.

In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

[59] Sylim, P.; Liu, F.; Marcelo, A.; Fontelo, P. Blockchain Technology for Detecting Falsified and Substandard Drugs in Distribution: Pharmaceutical Supply Chain Intervention. JMIR Res. Protoc. **2018**, 7, e10163. [CrossRef]

Mackey, T.K.; Liang, B.A. The global counterfeit drug trade: Patient safety and public health risks. J. Pharm. Sci. **2011**, 100, 4571–4579. [CrossRef] [PubMed]

Toyoda, K.; Mathiopoulos, P.T.; Sasase, I.; Ohtsuki, T. A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain. IEEE Access **2017**, 5, 17465–17477.

[CrossRef]

In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

[60] Rahman, M.A.; Hassanain, E.; Rashid, M.M.; Barnes, S.J.; Hossain, M.S. Spatial Blockchain-Based Secure Mass Screening Framework for Children With Dyslexia. IEEE Access **2018**, 6, 61876–61885. [[CrossRef](#)]

In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

[61] Jo, B.; Khan, R.; Lee, Y.S. Hybrid Blockchain and Internet-of-Things Network for Underground Structure Health Monitoring. Sensors **2018**, 18, 4268. [[CrossRef](#)]

In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

[62] Zhang, J.; Xue, N.; Huang, X. A secure system for pervasive social network-based healthcare. IEEE Access **2016**, 4, 9239–9250. [[CrossRef](#)]

In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

[63] Ichikawa, D.; Kashiyama, M.; Ueno, T. Tamper-resistant mobile health using blockchain technology. JMIR mHealth uHealth **2017**, 5, e111. [[CrossRef](#)]

In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

[64] Nikoloudakis, Y.; Pallis, E.; Mastorakis, G.; Mavromoustakis, C.X.; Skianis, C.; Markakis, E.K. Vulnerability assessment as a service for fog-centric ICT ecosystems: A healthcare use case. Peer-to-Peer Netw. Appl. **2019**, 1–9. [[CrossRef](#)]

In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

[65] Nausheen, F.; Begum, S.H. Healthcare IoT: Benefits, vulnerabilities and solutions. In Proceedings of the 2018 IEEE 2nd International Conference on Inventive Systems and Control (ICISC), Coimbatore, India, 19–20 January 2018; pp. 517–522.

In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

[66] Otoum, S.; Kantarci, B.; Mouftah, H. Adaptively supervised and intrusion-aware data aggregation for wireless sensor clusters in critical infrastructures. In Proceedings of the 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 20–24 May 2018; pp. 1–6.

In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

[67] Otoum, S.; Kantarci, B.; Mouftah, H.T. On the Feasibility of Deep Learning in Sensor Network Intrusion Detection. IEEE Netw. Lett. **2019**. [[CrossRef](#)]

In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

[68] Catarinucci, L.; De Donno, D.; Mainetti, L.; Palano, L.; Patrono, L.; Stefanizzi, M.L.; Tarricone, L. An IoT-aware architecture for smart healthcare systems. IEEE Internet Things J. **2015**, 2, 515–526. [CrossRef]

In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

[69] Saia, R. Internet of Entities (IoE): A Blockchain-based Distributed Paradigm to Security. arXiv **2018**, arXiv:1808.08809.

Saia, R.; Carta, S.; Recupero, D.; Fenu, G. Internet of Entities (IoE): A Blockchain-based Distributed Paradigm for Data Exchange between Wireless-based Devices. In Proceedings of the 8th International Conference on Sensor Networks (SENSORNETS 2019), Prague, Czech Republic, 26–27 January 2019.

In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

[70] Esposito, C.; De Santis, A.; Tortora, G.; Chang, H.; Choo, K.K.R. Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? IEEE Cloud Comput. **2018**, 5, 31–37. [CrossRef]

Dorri, A.; Kanhere, S.S.; Jurdak, R. Blockchain in internet of things: Challenges and solutions. arXiv **2016**, arXiv:1608.05187.

Dorri, A.; Kanhere, S.S.; Jurdak, R. Towards an optimized blockchain for IoT. In Proceedings of the ACM Second International Conference on Internet-of-Things Design and Implementation, Pittsburgh, PA, USA, 18–21 April 2017; pp. 173–178.

In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

[71] Khan, M.A.; Salah, K. IoT security: Review, blockchain solutions, and open challenges. Future Gen. Comput. Syst. **2018**, 82, 395–411. [CrossRef]

Top 10 Biggest Healthcare Data Breaches of All Time. Available online: <https://www.healthcareitnews.com/news/3-phishing-hacks-breach-20000-catawba-valley-patient-records> (accessed on 20 April 2019).

In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

[72] Kuo, T.T.; Ohno-Machado, L. ModelChain: Decentralized Privacy-Preserving Healthcare Predictive Modeling Framework on Private Blockchain Networks. arXiv **2018**, arXiv:1802.01746.

In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

[73] Wang, S.; Wang, J.; Wang, X.; Qiu, T.; Yuan, Y.; Ouyang, L.; Guo, Y.; Wang, F.Y. Blockchain-Powered Parallel Healthcare Systems Based on the ACP Approach. IEEE Trans. Comput. Soc. Syst. **2018**, 5, 942–950. [CrossRef]

In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

[74] Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/

[75] Saraf, C.; Sabadra, S. Blockchain platforms: A compendium. In Proceedings of the 2018 IEEE International Conference on Innovative Research and Development (ICIRD), Bangkok, Thailand, 11–12 May 2018; pp. 1–6.

Ethereum. Available online: <https://www.ethereum.org/> (accessed on 20 March 2019).

Ripple. Available online: <https://ripple.com/> (accessed on 20 March 2019).

Hyperledger. Available online: <https://www.hyperledger.org/> (accessed on 20 March 2019).

In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

[76] Dimitrov, D.V. Blockchain Applications for Healthcare Data Management. Healthc. Inform. Res. **2019**, 25, 51–56. [[CrossRef](#)] [[PubMed](#)]

In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

[77] Panesar, A. Machine Learning and AI for Healthcare: Big Data for Improved Health Outcomes; Springer: Emeryville, CA, USA, 2019.

In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

[78] Frost, J.H.; Massagli, M.P. Social uses of personal health information within PatientsLikeMe, an onlinepatient community: What can happen when patients have access to one another’s data. J. Med. Internet Res. **2008**, 10, e15. [[CrossRef](#)] [[PubMed](#)]

In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

[79] Hien, D.T.T.; Hien, D.H.; Pham, V.H. A survey on opportunities and challenges of Blockchain technology adoption for revolutionary innovation. In Proceedings of the ACM Ninth International Symposium on Information and Communication Technology, Danang City, Vietnam, 6–7 December 2018; pp. 200–207.

In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

[80] Liang, X.; Zhao, J.; Shetty, S.; Liu, J.; Li, D. Integrating blockchain for data sharing and collaboration immobile healthcare applications. In Proceedings of the 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, Canada, 8–13 October 2017; pp. 1–5.

In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

[81] Vo, H.T.; Kundu, A.; Mohania, M.K. Research Directions in Blockchain Data Management and Analytics; EDBT: Lisbon, Portugal, 2018; pp. 445–448.

In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

[82] Zhang, R.; Liu, L. Security models and requirements for healthcare application clouds. In Proceedings of the 2010 IEEE 3rd International Conference on cloud Computing, Miami, FL, USA, 5–10 July 2010; pp. 268–275.

In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

[83] Wang, H.; Song, Y. Secure cloud-based EHR system using attribute-based cryptosystem and blockchain. J. Med. Syst. **2018**, 42, 152. [[CrossRef](#)]

In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

[84] Wang, S.J.; Middleton, B.; Prosser, L.A.; Bardon, C.G.; Spurr, C.D.; Carchidi, P.J.; Kittler, A.F.; Goldszer, R.C.; Fairchild, D.G.; Sussman, A.J. A cost-benefit analysis of electronic medical records in primary care. Am. J. Med. **2003**, 114, 397–403. [[CrossRef](#)]

In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

[85] C. Lee, Z. Luo, K.Y. Ngiam, M. Zhang, K. Zheng, G. Chen, W.L.J. Yip, Big healthcare data analytics: challenges and applications, in: Handbook of Large-Scale Distributed Computing in Smart Healthcare, Springer, Cham, 2017, pp. 11–41.

In: Md. Mehedi Hassan Onik, Satyabrata Aich, Jinhong Yang, Chul-Soo Kim, Hee-Cheol Kim (2019), Big Data Analytics for Intelligent Healthcare Management, chapter 8 : blockchain in healthcare-challenges and solutions (pp 203) # 2019 Elsevier Inc. All rights reserved.

<https://doi.org/10.1016/B978-0-12-818146-1.00008-8>

[86] Stanford Medicine, Retrieved from:<https://med.stanford.edu/content/dam/sm/sm-news/documents/StanfordMedicineHealthTrendsWhitePaper2017.pdf>, 2017.

In: Md. Mehedi Hassan Onik, Satyabrata Aich, Jinhong Yang, Chul-Soo Kim, Hee-Cheol Kim (2019), Big Data Analytics for Intelligent Healthcare Management, chapter 8 : blockchain in healthcare-challenges and solutions (pp 203) # 2019 Elsevier Inc. All rights reserved.

<https://doi.org/10.1016/B978-0-12-818146-1.00008-8>

[87] Healthcare Analytics, Medical Analytics Market by Type (predictive, prescriptive) Application (Clinical, RCM, Claim, Fraud, Waste, Supply Chain, PHM) Component (Service, Software) Delivery (On demand, Cloud) End User (Payer, Hospital, ACO)—Global Forecast to 2022, Retrieved from:<https://www.marketsandmarkets.com/Market-Reports/healthcare-data-analytics-market-905.html>, 2017.

In: Md. Mehedi Hassan Onik, Satyabrata Aich, Jinhong Yang, Chul-Soo Kim, Hee-Cheol Kim (2019), Big Data Analytics for Intelligent Healthcare Management, chapter 8 : blockchain in healthcare-challenges and solutions (pp 203) # 2019 Elsevier Inc. All rights reserved.

<https://doi.org/10.1016/B978-0-12-818146-1.00008-8>

[88] Miller, R.H.; Sim, I. Physicians’ use of electronic medical records: barriers and solutions. Health Affairs **2004**, 23, 116–126. [[CrossRef](#)]

In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

- [89] Terry, A.L.; Thorpe, C.F.; Giles, G.; Brown, J.B.; Harris, S.B.; Reid, G.J.; Thind, A.; Stewart, M. Implementing electronic health records: Key factors in primary care. *Can. Fam. Phys.* **2008**, *54*, 730–736.
In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, *Appl. Sci.* **2019**, *9*, 1736; doi:10.3390/app9091736
- [90] S. Aich, M. Sain, J. Park, K.W. Choi, H.C. Kim, A text mining approach to identify the relationship between gait-Parkinson’s disease (PD) from PD based research articles, in: *International Conference on Inventive Computing and Informatics (ICICI), IEEE, 2017, pp. 481–485.*
In: Md. Mehedi Hassan Onik, Satyabrata Aich, Jinhong Yang, Chul-Soo Kim, Hee-Cheol Kim (2019), *Big Data Analytics for Intelligent Healthcare Management*, chapter 8 : blockchain in healthcare-challenges and solutions (pp 203) # 2019 Elsevier Inc. All rights reserved.
<https://doi.org/10.1016/B978-0-12-818146-1.00008-8>
- [91] S. Aich, P.M. Pradhan, J. Park, H.C. Kim, A machine learning approach to distinguish Parkinson’s disease (PD) patient’s with shuffling gait from older adults based on gait signals using 3D motion analysis, *Int. J. Eng. Technol.* *7* (3.29) (2018) 153–156.
In: Md. Mehedi Hassan Onik, Satyabrata Aich, Jinhong Yang, Chul-Soo Kim, Hee-Cheol Kim (2019), *Big Data Analytics for Intelligent Healthcare Management*, chapter 8 : blockchain in healthcare-challenges and solutions (pp 203) # 2019 Elsevier Inc. All rights reserved.
<https://doi.org/10.1016/B978-0-12-818146-1.00008-8>
- [92] S. Aich, H.C. Kim, Auto detection of Parkinson’s disease based on objective measurement of gait parameters using wearable sensors, *Artif. Intell.* *117* (2018) 103–112.
In: Md. Mehedi Hassan Onik, Satyabrata Aich, Jinhong Yang, Chul-Soo Kim, Hee-Cheol Kim (2019), *Big Data Analytics for Intelligent Healthcare Management*, chapter 8 : blockchain in healthcare-challenges and solutions (pp 203) # 2019 Elsevier Inc. All rights reserved.
<https://doi.org/10.1016/B978-0-12-818146-1.00008-8>
- [93] Lee, S.M.; Lee, D.; Schniederjans, M.J. Supply chain innovation and organizational performance in the healthcare industry. *Int. J. Oper. Prod. Manag.* **2011**, *31*, 1193–1214. [CrossRef]
Dehgani, R.; Jafari Navimipour, N. The impact of information technology and communication systems on the agility of supply chain management systems. *Kybernetes* **2019**. [CrossRef]
In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, *Appl. Sci.* **2019**, *9*, 1736; doi:10.3390/app9091736
- [94] Kim, C.; Kim, H.J. A study on healthcare supply chain management efficiency: Using bootstrap data envelopment analysis. *Health Care Manag. Sci.* **2019**, 1–15. [CrossRef]
Clauson, K.A.; Breeden, E.A.; Davidson, C.; Mackey, T.K. Leveraging blockchain technology to enhance supply chain management in healthcare. *Blockchain Healthc. Today* **2018**. . [CrossRef]
In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, *Appl. Sci.* **2019**, *9*, 1736; doi:10.3390/app9091736
- [95] Jayaraman, R.; AlHammadi, F.; Simsekler, M.C.E. Managing Product Recalls in Healthcare Supply Chain. In *Proceedings of the 2018 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), Bangkok, Thailand, 16–19 December 2018*; pp. 293–297.
In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, *Appl. Sci.* **2019**, *9*, 1736; doi:10.3390/app9091736
- [96] Dujak, D.; Sajter, D. *Blockchain Applications in Supply Chain*. In *SMART Supply Network*; Springer: Cham, Switzerland, 2019; pp. 21–46.

In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

[97] Narayanaswami, C.; Nooyi, R.; Raghavan, S.G.; Viswanathan, R. Blockchain Anchored Supply Chain Automation. IBM J. Res. Dev. **2019**. [[CrossRef](#)]

In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

[98] Isojarvi, J.; Wood, H.; Lefebvre, C.; Glanville, J. Challenges of identifying unpublished data from clinical trials: Getting the best out of clinical trials registers and other novel sources. Res. Synth. Methods **2018**, 9, 561–578. [[CrossRef](#)]

Benchoufi, M.; Ravaud, P. Blockchain technology for improving clinical research quality. Trials **2017**, 18, 335. [[CrossRef](#)] [[PubMed](#)]

In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

[99] Benchoufi, M.; Ravaud, P. Blockchain technology for improving clinical research quality. Trials **2017**, 18, 335. [[CrossRef](#)] [[PubMed](#)]

Benchoufi, M.; Porcher, R.; Ravaud, P. Blockchain protocols in clinical trials: Transparency and traceability of consent. F1000Research **2017**, 6, 66. [[CrossRef](#)] [[PubMed](#)]

In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

[100] Schöner, M.M.; Kourouklis, D.; Sandner, P.; Gonzalez, E.; Förster, J. Blockchain Technology in the Pharmaceutical Industry; Frankfurt School Blockchain Center: Frankfurt, Germany, 2017.

In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

[101] Maruchek, A.; Greis, N.; Mena, C.; Cai, L. Product safety and security in the global supply chain: Issues, challenges and research opportunities. J. Oper. Manag. **2011**, 29, 707–720. [[CrossRef](#)]

In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

[102] Xu, X.; Lu, Q.; Liu, Y.; Zhu, L.; Yao, H.; Vasilakos, A.V. Designing blockchain-based applications a case study for imported product traceability. Future Gen. Comput. Syst. **2019**, 92, 399–406. [[CrossRef](#)]

Westerkamp, M.; Victor, F.; Kupper, A. Tracing manufacturing processes using blockchain-based token compositions. Dig. Commun. Netw. **2019**, in press. [[CrossRef](#)]

In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

[103] 60 of Pharma Companies Using or Trying Blockchain Survey. Available online: <https://pharmaphorum.com/news/60-of-pharma-companies-using-or-trying-blockchain-survey/> (accessed on 12 March 2019).

In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

- [104] Chiuchisan, I.; Costin, H.N.; Geman, O. Adopting the internet of things technologies in health care systems. In Proceedings of the 2014 International Conference and Exposition on Electrical and Power Engineering (EPE), Iasi, Romania, 16–18 October 2014; pp. 532–535.
In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736
- [105] Aloqaily, M.; Otoum, S.; Al Ridhawi, I.; Jararweh, Y. An intrusion detection system for connected vehicles in smart cities. Ad Hoc Netw. **2019**, in press. [[CrossRef](#)]
In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736
- [106] Moosavi, S.R.; Gia, T.N.; Rahmani, A.M.; Nigussie, E.; Virtanen, S.; Isoaho, J.; Tenhunen, H. SEA: A secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. Procedia Comput. Sci. **2015**, 52, 452–459. [[CrossRef](#)]
In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736
- [107] Haggi, M.; Thurow, K.; Stoll, R. Wearable devices in medical internet of things: Scientific research and commercially available devices. Healthc. Inform. Res. **2017**, 23, 4–15. [[CrossRef](#)]
In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736
- [108] Yuce, M.R. Implementation of wireless body area networks for healthcare systems. Sens. Actuators Phys. **2010**, 162, 116–129. [[CrossRef](#)]
Crosby, G.V.; Ghosh, T.; Murimi, R.; Chin, C.A. Wireless body area networks for healthcare: A survey. Int. J. Ad Hoc Sens. Ubiquitous Comput. **2012**, 3, 1. [[CrossRef](#)]
Rani, A.A.V.; Baburaj, E. Secure and intelligent architecture for cloud-based healthcare applications in wireless body sensor networks. Int. J. Biomed. Eng. Technol. **2019**, 29, 186–199. [[CrossRef](#)]
Elhayatmy, G.; Dey, N.; Ashour, A.S. Internet of Things based wireless body area network in healthcare. In Internet of Things and Big Data Analytics Toward Next-Generation Intelligence; Springer: Cham, Switzerland, 2018; pp. 3–20.
In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736
- [109] Zanjali, S.V.; Talmale, G.R. Medicine reminder and monitoring system for secure health using IOT. Procedia Comput. Sci. **2016**, 78, 471–476. [[CrossRef](#)]
Dimitrov, D.V. Medical internet of things and big data in healthcare. Healthc. Inform. Res. **2016**, 22, 156–163. [[CrossRef](#)]
In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736
- [110] 3 Phishing Hacks Breach 20,000 Catawba Valley Patient Records. Available online: <https://www.healthcareitnews.com/news/3-phishing-hacks-breach-20000-catawba-valley-patient-records> (accessed on 20 April 2019).

In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

[111] Mamoshina, P.; Ojomoko, L.; Yanovich, Y.; Ostrovski, A.; Botezatu, A.; Prikhodko, P.; Izumchenko, E.; Aliper, A.; Romantsov, K.; Zhebrak, A.; et al. Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare. *Oncotarget* **2018**, 9, 5665. [[CrossRef](#)]

In: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

[112] Mack, H., Remote patient monitoring market grew by 44 percent in 2016, report says. <http://www.mobihealthnews.com/content/remote-patient-monitoring-market-grew-44-percent-2016-reportsays,2017>.

In: Kristen N. Griggs, Olya Ossipova, Christopher P. Kohlios, Alessandro N. Baccarini, Emily A. Howson, Thaier Hayajneh, (2018) , Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring, Received: 21 March 2018 / Accepted: 18 May 2018

© Springer Science+Business Media, LLC, part of Springer Nature 2018, <https://doi.org/10.1007/s10916-018-0982-x>

[113] Daniel, J. G., and Uppaluru, M., New reimbursement for remotepatient monitoring and telemedicine. <https://www.cmhealthlaw.com/2017/11/new-reimbursement-for-remote-patient-monitoring-and-telemedicine/>, 2017.

In: Kristen N. Griggs, Olya Ossipova, Christopher P. Kohlios, Alessandro N. Baccarini, Emily A. Howson, Thaier Hayajneh, (2018) , Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring, Received: 21 March 2018 / Accepted: 18 May 2018

© Springer Science+Business Media, LLC, part of Springer Nature 2018, <https://doi.org/10.1007/s10916-018-0982-x>

[114] Kristen N. Griggs, Olya Ossipova, Christopher P. Kohlios, Alessandro N. Baccarini, Emily A. Howson, Thaier Hayajneh, (2018) , Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring, Received: 21 March 2018 / Accepted: 18 May 2018

© Springer Science+Business Media, LLC, part of Springer Nature 2018, <https://doi.org/10.1007/s10916-018-0982-x>

[115] Consensus, A visit to the oracle. <https://media.consensys.net/a-visit-to-the-oracle-de9097d38b2f>, 2016.

In: Kristen N. Griggs, Olya Ossipova, Christopher P. Kohlios, Alessandro N. Baccarini, Emily A. Howson, Thaier Hayajneh, (2018) , Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring, Received: 21 March 2018 / Accepted: 18 May 2018

© Springer Science+Business Media, LLC, part of Springer Nature 2018, <https://doi.org/10.1007/s10916-018-0982-x>

[116] Naseem Naqvi, Mureed Hussain, (2018), Medical Education on the Blockchain, Received: 5 October 2018 Accepted: 25 October 2018, Published: 15 November 2018,

[https://doi.org/10.31585/jbba-1-2-\(10\)2018](https://doi.org/10.31585/jbba-1-2-(10)2018)

[117] Neame, Roderick et al. “Universities without Walls: Evolving Paradigms in Medical Education.” *BMJ: British Medical Journal* 319.7220 (1999): 1296. Print. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1129074/>

Athol, K: “Medical Schools without walls.” *Medical Education* (2009)

<https://doi.org/10.1111/j.1365-2923.1997.tb02558.x>

Hou Jianlin et al. “Transformation of the education of health professionals in China: progress and challenges. The LANCET (2014) <https://www.sciencedirect.com/science/article/pii/S0140673614613076> 89

In: Naseem Naqvi, Mureed Hussain, (2018), Medical Education on the Blockchain, Received: 5 October 2018 Accepted: 25 October 2018, Published: 15 November 2018,

[https://doi.org/10.31585/jbba-1-2-\(10\)2018](https://doi.org/10.31585/jbba-1-2-(10)2018)

[118] Sony wants to digitize education records using the blockchain: (2017) <https://techcrunch.com/2017/08/09/sony-education-blockchain>

Providing Pathways for Refugees: Practical Tips for Credential Assessment: (2016)

<https://wenr.wes.org/2016/04/providing-pathways-for-refugees-practical-tips-for-credential-assessment>

In: Naseem Naqvi, Mureed Hussain, (2018), Medical Education on the Blockchain, Received: 5 October 2018 Accepted: 25 October 2018, Published: 15 November 2018,

[https://doi.org/10.31585/jbba-1-2-\(10\)2018](https://doi.org/10.31585/jbba-1-2-(10)2018)

[119] Continuing Professional Development – A guidance for all doctors:

https://www.gmc-uk.org/g/Continuing_professional_development_guidance_for_all_doctors_0316.pdf_56438625.pdf

In: Naseem Naqvi, Mureed Hussain, (2018), Medical Education on the Blockchain, Received: 5 October 2018 Accepted: 25 October 2018, Published: 15 November 2018,

[https://doi.org/10.31585/jbba-1-2-\(10\)2018](https://doi.org/10.31585/jbba-1-2-(10)2018)

[120] Blockchain and Education: A Big Idea in need of bigger thinking:

<https://www.coindesk.com/blockchain-education-big-idea-need-bigger-thinking/>

In: Naseem Naqvi, Mureed Hussain, (2018), Medical Education on the Blockchain, Received: 5 October 2018 Accepted: 25 October 2018, Published: 15 November 2018,

[https://doi.org/10.31585/jbba-1-2-\(10\)2018](https://doi.org/10.31585/jbba-1-2-(10)2018)

[121] How Can Blockchain Technology Innovate Your Education:

<https://hackernoon.com/how-can-blockchain-technology-innovate-your-education-d1cd80c26f08>

In: Naseem Naqvi, Mureed Hussain, (2018), Medical Education on the Blockchain, Received: 5 October 2018 Accepted: 25 October 2018, Published: 15 November 2018,

[https://doi.org/10.31585/jbba-1-2-\(10\)2018](https://doi.org/10.31585/jbba-1-2-(10)2018)

[122] What Happens When You Combine Blockchain and Education?

<https://hackernoon.com/what-happens-when-you-combine-blockchain-and-education-d533ef6d4862>

In: Naseem Naqvi, Mureed Hussain, (2018), Medical Education on the Blockchain, Received: 5 October 2018 Accepted: 25 October 2018, Published: 15 November 2018,

[https://doi.org/10.31585/jbba-1-2-\(10\)2018](https://doi.org/10.31585/jbba-1-2-(10)2018)

[123] Your MD may have a phony degree 2017

<https://www.cbsnews.com/news/your-md-may-have-a-phony-degree/>

In: Naseem Naqvi, Mureed Hussain, (2018), Medical Education on the Blockchain, Received: 5 October 2018 Accepted: 25 October 2018, Published: 15 November 2018,

[https://doi.org/10.31585/jbba-1-2-\(10\)2018](https://doi.org/10.31585/jbba-1-2-(10)2018)

[124] Axact CEO, 22 others receive 20 years in jail for fake degrees case: 2018

<https://www.dawn.com/news/1418156>

In: Naseem Naqvi, Mureed Hussain, (2018), Medical Education on the Blockchain, Received: 5 October 2018 Accepted: 25 October 2018, Published: 15 November 2018,

[https://doi.org/10.31585/jbba-1-2-\(10\)2018](https://doi.org/10.31585/jbba-1-2-(10)2018)

[125] How easy is it to fake it as a doctor? 2017

<https://www.bbc.com/news/uk-40861475>

In: Naseem Naqvi, Mureed Hussain, (2018), Medical Education on the Blockchain, Received: 5 October 2018 Accepted: 25 October 2018, Published: 15 November 2018,

[https://doi.org/10.31585/jbba-1-2-\(10\)2018](https://doi.org/10.31585/jbba-1-2-(10)2018)

[126] Dennis Grishin, Kamal Obbad, Preston Estep, Kevin Quinn, Sarah Wait Zaranek, Alexander Wait Zaranek, Ward Vandewege, Tom Clegg, Nico César, Mirza Cifric, George Church, Accelerating Genomic Data Generation and Facilitating Genomic Data Access Using Decentralization, Privacy-Preserving Technologies and Equitable Compensation, (In: *Blockchain in Healthcare Today*, ISSN 2573-8240, online <https://doi.org/10.30953/bhty.v1.34>)

[127] Illumina Promises to Sequence Human Genome For \$100—But Not Quite Yet. 2017. [cited 2018 Oct 10]. Available from: <https://www.forbes.com/sites/matthewherper/2017/01/09/illumina-promises-to-sequence-human-genome-for-100-but-not-quite-yet/#672a5d72386d>

IN: Dennis Grishin, Kamal Obbad, Preston Estep, Kevin Quinn, Sarah Wait Zaranek, Alexander Wait Zaranek, Ward Vandewege, Tom Clegg, Nico César, Mirza Cifric, George Church, Accelerating Genomic Data Generation and Facilitating Genomic Data Access Using Decentralization, Privacy-Preserving Technologies and Equitable Compensation, (In: *Blockchain in Healthcare Today*, ISSN 2573-8240, online <https://doi.org/10.30953/bhty.v1.34>)

[128] Tim K. Mackey, Tsung-Ting Kuo, Basker Gummadi, Kevin A. Clauson, George Church, Dennis Grishin, Kamal Obbad, Robert Barkovich and Maria Palombini, (2019), ‘Fit-for-purpose?’ – challenges and opportunities for applications of blockchain technology in the future of healthcare, Mackey et al. *BMC Medicine* (2019) 17:68, <https://doi.org/10.1186/s12916-019-1296-7>

[129] Church GM. The personal genome project. *Mol Syst Biol.* 2005;1:2005.0030.

Ball MP, Bobe JR, Chou MF, Clegg T, Estep PW, Lunshof JE, et al. Harvard Personal Genome Project: lessons from participatory public research. *Genome Med.* 2014;6:10.

IN: Tim K. Mackey, Tsung-Ting Kuo, Basker Gummadi, Kevin A. Clauson, George Church, Dennis Grishin, Kamal Obbad, Robert Barkovich and Maria Palombini, (2019), ‘Fit-for-purpose?’ – challenges and opportunities for applications of blockchain technology in the future of healthcare, Mackey et al. *BMC Medicine* (2019) 17:68, <https://doi.org/10.1186/s12916-019-1296-7>

[130] Global Alliance for Genomics and Health. GENOMICS. A federated ecosystem for sharing genomic, clinical data. *Science.* 2016 Jun 10;352(6291):1278–80.

IN: Dennis Grishin, Kamal Obbad, Preston Estep, Kevin Quinn, Sarah Wait Zaranek, Alexander Wait Zaranek, Ward Vandewege, Tom Clegg, Nico César, Mirza Cifric, George Church, Accelerating Genomic Data Generation and Facilitating Genomic Data Access Using Decentralization, Privacy-Preserving Technologies and Equitable Compensation, (In: *Blockchain in Healthcare Today*, ISSN 2573-8240, online <https://doi.org/10.30953/bhty.v1.34>)

[131] Weber GM, Murphy SN, McMurry AJ, et al. The Shared Health Research Information Network (SHRINE): A prototype federated query tool for clinical data repositories. *J Am Med Inform Assoc.* 2009 Sep;16(5):624–30.

IN: Dennis Grishin, Kamal Obbad, Preston Estep, Kevin Quinn, Sarah Wait Zaranek, Alexander Wait Zaranek, Ward Vandewege, Tom Clegg, Nico César, Mirza Cifric, George Church, Accelerating Genomic Data Generation and Facilitating Genomic Data Access Using Decentralization, Privacy-Preserving Technologies and Equitable Compensation, (In: *Blockchain in Healthcare Today*, ISSN 2573-8240, online <https://doi.org/10.30953/bhty.v1.34>)

[132] Raisaro JL, Troncoso-Pastoriza J, Misbach M, et al. MedCo: Enabling secure and privacy-preserving exploration of distributed clinical and genomic data. *IEEE/ACM Trans Comput Biol Bioinform* [Internet]. 2018 Jul 13; Available from: <http://dx.doi.org/10.1109/TCBB.2018.2854776>

IN: Dennis Grishin, Kamal Obbad, Preston Estep, Kevin Quinn, Sarah Wait Zaranek, Alexander Wait Zaranek, Ward Vandewege, Tom Clegg, Nico César, Mirza Cifric, George Church, Accelerating Genomic Data Generation and Facilitating Genomic Data Access Using Decentralization, Privacy-Preserving Technologies and Equitable Compensation, (In: Blockchain in Healthcare Today , ISSN 2573-8240, online <https://doi.org/10.30953/bhty.v1.34>)

[133] Chen F, Wang S, Jiang X, et al. PRINCESS: Privacy-protecting rare disease International Network Collaboration via encryption through software guard extensions. *Bioinformatics*. 2017 Mar 15;33(6):871–8. IN: Dennis Grishin, Kamal Obbad, Preston Estep, Kevin Quinn, Sarah Wait Zaranek, Alexander Wait Zaranek, Ward Vandewege, Tom Clegg, Nico César, Mirza Cifric, George Church, Accelerating Genomic Data Generation and Facilitating Genomic Data Access Using Decentralization, Privacy-Preserving Technologies and Equitable Compensation, (In: Blockchain in Healthcare Today , ISSN 2573-8240, online <https://doi.org/10.30953/bhty.v1.34>)

[134] Molteni M, Allain R, Chen S, Thompson A, Simon M, Gonzalez R. Genos will sequence your genes—And help you sell them to science. *Wired* [Internet]. 2016 Dec 15 [cited 2018 Oct 6]; Available from: <https://www.wired.com/2016/12/genos-will-sequence-genes-help-sell-science/> IN: Dennis Grishin, Kamal Obbad, Preston Estep, Kevin Quinn, Sarah Wait Zaranek, Alexander Wait Zaranek, Ward Vandewege, Tom Clegg, Nico César, Mirza Cifric, George Church, Accelerating Genomic Data Generation and Facilitating Genomic Data Access Using Decentralization, Privacy-Preserving Technologies and Equitable Compensation, (In: Blockchain in Healthcare Today , ISSN 2573-8240, online <https://doi.org/10.30953/bhty.v1.34>)

[135] Brown KV. Share your DNA, get shares: Startup files an unusual offering. *Bloomberg News* [Internet]. 2018 Oct 5 [cited 2018 Oct 6]; Available from: <https://www.bloomberg.com/news/articles/2018-10-05/illumina-backed-startup-asks-sec-to-let-it-pay-people-for-dna> IN: Dennis Grishin, Kamal Obbad, Preston Estep, Kevin Quinn, Sarah Wait Zaranek, Alexander Wait Zaranek, Ward Vandewege, Tom Clegg, Nico César, Mirza Cifric, George Church, Accelerating Genomic Data Generation and Facilitating Genomic Data Access Using Decentralization, Privacy-Preserving Technologies and Equitable Compensation, (In: Blockchain in Healthcare Today , ISSN 2573-8240, online <https://doi.org/10.30953/bhty.v1.34>)

[136] Arvados Documentation [Internet]. [cited 2018 Oct 10]. Available from: doc.arvados.org Zaranek AW, Clegg T, Vandewege W, Church GM. Free factories: Unified infrastructure for data intensive web services. *Proc USENIX Annu Tech Conf*. 2008 May 1;2008:391–404. IN: Dennis Grishin, Kamal Obbad, Preston Estep, Kevin Quinn, Sarah Wait Zaranek, Alexander Wait Zaranek, Ward Vandewege, Tom Clegg, Nico César, Mirza Cifric, George Church, Accelerating Genomic Data Generation and Facilitating Genomic Data Access Using Decentralization, Privacy-Preserving Technologies and Equitable Compensation, (In: Blockchain in Healthcare Today , ISSN 2573-8240, online <https://doi.org/10.30953/bhty.v1.34>)

[137] Exonum Documentation [Internet]. [cited 2018 Oct 10]. Available from: exonum.com/doc IN: Dennis Grishin, Kamal Obbad, Preston Estep, Kevin Quinn, Sarah Wait Zaranek, Alexander Wait Zaranek, Ward Vandewege, Tom Clegg, Nico César, Mirza Cifric, George Church, Accelerating Genomic Data Generation and Facilitating Genomic Data Access Using Decentralization, Privacy-Preserving Technologies and Equitable Compensation, (In: Blockchain in Healthcare Today , ISSN 2573-8240, online <https://doi.org/10.30953/bhty.v1.34>)

- [138] Robinson PN, Köhler S, Bauer S, et al. The human phenotype ontology: A tool for annotating and analyzing human hereditary disease. *Am J Hum Genet.* 2008 Nov;83(5):610–5.
IN: Dennis Grishin, Kamal Obbad, Preston Estep, Kevin Quinn, Sarah Wait Zaranek, Alexander Wait Zaranek, Ward Vandewege, Tom Clegg, Nico César, Mirza Cifric, George Church, Accelerating Genomic Data Generation and Facilitating Genomic Data Access Using Decentralization, Privacy-Preserving Technologies and Equitable Compensation,
(In: Blockchain in Healthcare Today , ISSN 2573-8240, online <https://doi.org/10.30953/bhty.v1.34>)
- [139] Ghemawat S, Gobioff H, Leung S-T. The Google file system. In: *Proceedings of the Nineteenth ACM Symposium on Operating Systems Principles (SOSP '03)*. New York: ACM; 2003. pp. 29–43.
IN: Dennis Grishin, Kamal Obbad, Preston Estep, Kevin Quinn, Sarah Wait Zaranek, Alexander Wait Zaranek, Ward Vandewege, Tom Clegg, Nico César, Mirza Cifric, George Church, Accelerating Genomic Data Generation and Facilitating Genomic Data Access Using Decentralization, Privacy-Preserving Technologies and Equitable Compensation,
(In: Blockchain in Healthcare Today , ISSN 2573-8240, online <https://doi.org/10.30953/bhty.v1.34>)
- [140] Amstutz P, Crusoe M, Tijanić N, et al. *Common Workflow Language, v1.0. Specification, Common Workflow Language working group.* 2016. [Internet]. [cited 2018 Oct 10]. Available from: https://figshare.com/articles/Common_Workflow_Language_draft_3/3115156/2
IN: Dennis Grishin, Kamal Obbad, Preston Estep, Kevin Quinn, Sarah Wait Zaranek, Alexander Wait Zaranek, Ward Vandewege, Tom Clegg, Nico César, Mirza Cifric, George Church, Accelerating Genomic Data Generation and Facilitating Genomic Data Access Using Decentralization, Privacy-Preserving Technologies and Equitable Compensation,
(In: Blockchain in Healthcare Today , ISSN 2573-8240, online <https://doi.org/10.30953/bhty.v1.34>)
- [141] Ioannidis JP. Why most published research findings are false. *PLoS Med.*2005;2:e124.
Ioannidis JP. Genetic associations: False or true? *Trends Mol Med.* 2003;9:135–8.
In: Mehdi Benchoufi and Philippe Ravaud (2017), Blockchain technology for improving clinical research quality : DOI 10.1186/s13063-017-2035-z
- [142] Benchoufi M, Porcher R, Ravaud P. Blockchain protocols in clinical trials: Transparency and traceability of consent. *F1000Research.* 2017;6:66.
Nugent T, Upton D, Cimpoesu M. Improving data transparency in clinical trials using blockchain smart contracts [version 1; referees: 3 approved].
F1000Research. 2016;5:2541. doi:10.12688/f1000research.9756.1.
In: Mehdi Benchoufi and Philippe Ravaud (2017), Blockchain technology for improving clinical research quality : DOI 10.1186/s13063-017-2035-z
- [143] Mehdi Benchoufi and Philippe Ravaud (2017), Blockchain technology for improving clinical research quality : DOI 10.1186/s13063-017-2035-z
- [144] CONSolidated Standards of Reporting Trials Guidelines, (Consort Guidelines). <http://www.consort-statement.org/consort-2010> .
WHO Trial Registration Data Set (Version 1.2.1), International Clinical Trials Registry Platform (ICTRP). <http://www.who.int/ictrp/network/trds/en/> . Accessed 20 Dec 2016.
In: Mehdi Benchoufi and Philippe Ravaud (2017), Blockchain technology for improving clinical research quality : DOI 10.1186/s13063-017-2035-z
- [145] Sandve GK, Nekrutenko A, Taylor J, Hovig E. Ten simple rules for reproducible computational research. *PLoS Comput Biol.* 2013;9(10):e1003285.
Giles C. Financial Times. 2014. [October 17, 2014]. (Thomas Piketty's exhaustive inequality data turn out to be flawed). <http://www.ft.com/cms/s/0/c9ce1a54-e281-11e3-89fd-00144feabdc0> .

IOM (Institute of Medicine). Evolution of translational omics: Lessons learned and the path forward. Washington, DC: The National Academies Press; 2012.

In: Mehdi Benchoufi and Philippe Ravaut (2017), Blockchain technology for improving clinical research quality : DOI 10.1186/s13063-017-2035-z

[146] Zipline—Lifesaving Deliveries by Drone (2018). <http://www.flyzipline.com/>. Accessed 14 June 2018.

IN: Maged N. Kamel Boulos, James T. Wilson and Kevin A. Clauson (2018), Geospatial blockchain: promises, challenges, and scenarios in health and healthcare.

[147] Dasgupta A. The Game Changer of Geospatial Systems—Blockchain. Geospatial World (online). 2017 Sep. <https://www.geospatialworld.net/article/blockchain-geospatial-systems/>. Accessed 14 June 2018.

Anderson J. FOAM: The Future of Geospatial Data, on the Ethereum Blockchain. Steemit (online). 2017 July <https://steemit.com/ethereum/@protegeaa/foam-the-future-of-geospatial-data-on-the-ethereum-blockchain>. Accessed 14 June 2018.

Tewelow W. Bitcoin, blockchain and GIS could change the world. Geospatial Solutions (online). 2018 Mar. <http://geospatial-solutions.com/bitcoin-blockchain-and-gis-could-change-the-world/>. Accessed 14 June 2018.

IN: Maged N. Kamel Boulos, James T. Wilson and Kevin A. Clauson (2018), Geospatial blockchain: promises, challenges, and scenarios in health and healthcare.

[148] Javaria Tahir, Nadeem Javaid, (2019), Smart Ambulance: Blockchain technology in health-care for emergency patients, Department of Computer Science

[149] (https://hitconsultant.net/2014/12/02/ambulance-drone-could-transform-emergency-response/#.Xz_mjsAzblU)

[150] (<https://www.iotforall.com/drone-delivery-system/>)

[151] Asad Ali Siyal, Aisha Zahid Junej, Muhammad Zawis, Kainat Ahmed, Aiman Khalil and Georgia Soursou, (2019), Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives, Published: 2 January 2019

[152] Iezzoni, L.I. Assessing quality using administrative data. *Ann. Internal Med.* **1997**, 127, 666–674. [CrossRef]

IN: Seyednima Khezr, Md Moniruzzaman, Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, *Appl. Sci.* **2019**, 9, 1736; doi:10.3390/app9091736

[153] Lei Hang, Eunchang Choi and Do-Hyeun Kim, (2019), A Novel EMR Integrity Management Based on a Medical Blockchain Platform in Hospital, Published: 25 April 2019

[154] Dhillon, V.; Metcalf, D.; Hooper, M. Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make It Work for You; Springer: Emeryville, CA, USA, 2017.

IN: Seyednima Khezr, Md Moniruzzaman, Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, *Appl. Sci.* **2019**, 9, 1736; doi:10.3390/app9091736

[155] Course 2: The Medical Billing Process. Available online: <https://www.medicalbillingandcodingonline.com/medical-coding-for-billers/> (accessed on 12 March 2019).
IN: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091

[156] Guardian (WHO), 10% of Drugs in Poor Countries are Fake, Says WHO, Retrieved from:<https://www.theguardian.com/global-development/2017/nov/28/10-of-drugs-in-poor-countries-are-fake-says-who>,2017. Accessed 13 June 2018.

In: Md. Mehedi Hassan Onik, Satyabrata Aich, Jinhong Yang, Chul-Soo Kim, Hee-Cheol Kim (2019), Big Data Analytics for Intelligent Healthcare Management, chapter 8 : blockchain in healthcare-challenges and solutions (pp 203) # 2019 Elsevier Inc. All rights reserved.

[157] Counterfeit Medications. Available online: https://en.wikipedia.org/wiki/Counterfeit_medications (accessed on 14 March 2019).

IN: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

[158] Deisingh, A.K. Pharmaceutical counterfeiting. Analyst **2005**, 130, 271–279. [[CrossRef](#)]

IN: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

[159] Zhu, Q.; Kouhizadeh, M. Blockchain Technology, Supply Chain Information, and Strategic Product Deletion Management. IEEE Eng. Manag. Rev. **2019**, 47, 36–44. [[CrossRef](#)]

IN: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

[160] Plotnikov, V.; Kuznetsova, V. The Prospects for the Use of Digital Technology “Blockchain” in the Pharmaceutical Market. In MATEC Web of Conferences; EDP Sciences: Ho Chi Minh, Vietnam, 2018; Volume 193, p. 02029.

IN: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

[161] Montecchi, M.; Plangger, K.; Etter, M. It’s real, trust me! Establishing supply chain provenance using blockchain. Bus. Horiz. **2019**, in press. [[CrossRef](#)]

IN: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

[162] Kumar, R.; Agarwal, A.; Shubhankar, B. Counterfeit Drug Detection: Recent Strategies and Analytical Perspectives. *Int. J. Pharma Res. Health Sci.* **2018**, 6, 2351–2358.

IN: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

[163] Sylim P, Liu F, Marcelo A, Fontelo P. Blockchain technology for detecting falsified and substandard drugs in distribution: pharmaceutical supply chain intervention. *JMIR Res Protoc.* 2018;7:e10163.

IN:Tim K. Mackey, Tsung-Ting Kuo, Basker Gummadi, Kevin A. Clauson, George Church, Dennis Grishin, Kamal Obbad, Robert Barkovich and Maria Palombini, (2019), ‘Fit-for-purpose?’ – challenges and opportunities for applications of blockchain technology in the future of healthcare, Mackey et al. *BMC Medicine* (2019) 17:68, <https://doi.org/10.1186/s12916-019-1296-7>

[164] Tseng JH, Liao YC, Chong B, Liao SW. Governance on the drug supply chain via gcoin blockchain. *Int J Environ Res Public Health.* 2018;15(6):1055.

IN:Tim K. Mackey, Tsung-Ting Kuo, Basker Gummadi, Kevin A. Clauson, George Church, Dennis Grishin, Kamal Obbad, Robert Barkovich and Maria Palombini, (2019), ‘Fit-for-purpose?’ – challenges and opportunities for applications of blockchain technology in the future of healthcare, Mackey et al. *BMC Medicine* (2019) 17:68, <https://doi.org/10.1186/s12916-019-1296-7>

[165] Mackey TK, Nayyar G. A review of existing and emerging digital technologies to combat the global trade in fake medicines. *Expert Opin Drug Saf.* 2017;16(5): 587–602. <https://doi.org/10.1080/14740338.2017.1313227>.

IN:Tim K. Mackey, Tsung-Ting Kuo, Basker Gummadi, Kevin A. Clauson, George Church, Dennis Grishin, Kamal Obbad, Robert Barkovich and Maria Palombini, (2019), ‘Fit-for-purpose?’ – challenges and opportunities for applications of blockchain technology in the future of healthcare, Mackey et al. *BMC Medicine* (2019) 17:68, <https://doi.org/10.1186/s12916-019-1296-7>

[166] Vriddhula S. Application of on-dose identification and blockchain to prevent drug counterfeiting. *Pathog Glob Health.* 2018;112(4):161.

IN:Tim K. Mackey, Tsung-Ting Kuo, Basker Gummadi, Kevin A. Clauson, George Church, Dennis Grishin, Kamal Obbad, Robert Barkovich and Maria Palombini, (2019), ‘Fit-for-purpose?’ – challenges and opportunities for applications of blockchain technology in the future of healthcare, Mackey et al. *BMC Medicine* (2019) 17:68, <https://doi.org/10.1186/s12916-019-1296-7>

[167] U.S. Food and Drug Administration. Drug Supply Chain Security Act (DSCSA). <https://www.fda.gov/Drugs/DrugSafety/DrugIntegrityandSupplyChainSecurity/DrugSupplyChainSecurityAct/>. Accessed 18 Feb 2019.

IN:Tim K. Mackey, Tsung-Ting Kuo, Basker Gummadi, Kevin A. Clauson, George Church, Dennis Grishin, Kamal Obbad, Robert Barkovich and Maria Palombini, (2019), ‘Fit-for-purpose?’ – challenges and opportunities for applications of blockchain technology in the future of healthcare, Mackey et al. BMC Medicine (2019) 17:68, <https://doi.org/10.1186/s12916-019-1296-7>

[168] European Commission. Public Health. https://ec.europa.eu/health/sites/health/files/files/eudralex/vol-1/reg_2016_161/reg_2016_161_en.pdf. Accessed 4 Mar 2019.

IN:Tim K. Mackey, Tsung-Ting Kuo, Basker Gummadi, Kevin A. Clauson, George Church, Dennis Grishin, Kamal Obbad, Robert Barkovich and Maria Palombini, (2019), ‘Fit-for-purpose?’ – challenges and opportunities for applications of blockchain technology in the future of healthcare, Mackey et al. BMC Medicine (2019) 17:68, <https://doi.org/10.1186/s12916-019-1296-7>

[169] Plotnikov, V.; Kuznetsova, V. The Prospects for the Use of Digital Technology “Blockchain” in the Pharmaceutical Market. In MATEC Web of Conferences; EDP Sciences: Ho Chi Minh, Vietnam, 2018; Volume 193, p. 02029.

IN: Seyednima Khezr , Md Moniruzzaman , Abdulsalam Yassine and Rachid Benlamri, (2019) Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research, Appl. Sci. **2019**, 9, 1736; doi:10.3390/app9091736

[170] Kovacs S, et al. Technologies for Detecting Falsified and Substandard Drugs in Low and Middle-Income Countries. PLoS One. 2014;9(3):e90601.

IN:Tim K. Mackey, Tsung-Ting Kuo, Basker Gummadi, Kevin A. Clauson, George Church, Dennis Grishin, Kamal Obbad, Robert Barkovich and Maria Palombini, (2019), ‘Fit-for-purpose?’ – challenges and opportunities for applications of blockchain technology in the future of healthcare, Mackey et al. BMC Medicine (2019) 17:68, <https://doi.org/10.1186/s12916-019-1296-7>

[171] State of Blockchain Adoption on the Pharmaceutical Supply Chain. 2017. IEEE Standards Association. <https://blockchain.ieee.org/standards/2017-sbapsc>. Accessed 18 Feb 2019.

IN:Tim K. Mackey, Tsung-Ting Kuo, Basker Gummadi, Kevin A. Clauson, George Church, Dennis Grishin, Kamal Obbad, Robert Barkovich and Maria Palombini, (2019), ‘Fit-for-purpose?’ – challenges and opportunities for applications of blockchain technology in the future of healthcare, Mackey et al. BMC Medicine (2019) 17:68, <https://doi.org/10.1186/s12916-019-1296-7>

[172] Mettler M. Blockchain technology in healthcare: The revolution starts here. In: 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom) 2016;1-3. IEEE. <https://ieeexplore.ieee.org/document/7749510>.

IN:Tim K. Mackey, Tsung-Ting Kuo, Basker Gummadi, Kevin A. Clauson, George Church, Dennis Grishin, Kamal Obbad, Robert Barkovich and Maria Palombini, (2019), ‘Fit-for-purpose?’ – challenges and opportunities for applications of blockchain technology in the future of healthcare, Mackey et al. BMC Medicine (2019) 17:68, <https://doi.org/10.1186/s12916-019-1296-7>

[173] Moser M. Anonymity of Bitcoin Transactions. Münster Bitcoin Conference. Münster, Germany: MBC; 2013:17–18.

IN:Tsung-Ting Kuo, Hyeon-Eui Kim, and Lucila Ohno-Machado, (2017), Blockchain distributed ledger technologies for biomedical and health care applications

[174] Biryukov A, Khovratovich D, Pustogarov I. Deanonymisation of clients in Bitcoin P2P network. 2014 ACM SIGSAC Conference on Computer and Communications Security. Scottsdale, Arizona, United States: ACM; 2014.

IN:Tsung-Ting Kuo, Hyeon-Eui Kim, and Lucila Ohno-Machado, (2017), Blockchain distributed ledger technologies for biomedical and health care applications

[175] Ludwin A. How Anonymous is Bitcoin? Coin Center. <https://coincenter.org/entry/how-anonymous-is-bitcoin> . Accessed April 6, 2017.

IN:Tsung-Ting Kuo, Hyeon-Eui Kim, and Lucila Ohno-Machado, (2017), Blockchain distributed ledger technologies for biomedical and health care applications

[176] Abbas A. Understanding Privacy: How Anonymous can Bitcoin Payments be? Bitcoinist.net. <http://bitcoinist.com/understanding-privacy-anonymous-bitcoin/> . Accessed April 6, 2017

IN:Tsung-Ting Kuo, Hyeon-Eui Kim, and Lucila Ohno-Machado, (2017), Blockchain distributed ledger technologies for biomedical and health care applications

[177] Prakash R. Adoption of blockchain to enable the scalability and adoption of accountable care. ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/ NIST; 2016.

IN:Tsung-Ting Kuo, Hyeon-Eui Kim, and Lucila Ohno-Machado, (2017), Blockchain distributed ledger technologies for biomedical and health care applications

[178] Azaria A, Ekblaw A, Vieira T, Lippman A. MedRec: using blockchain for medical data access and permission management. International Conference on Open and Big Data (OBD). Vienna, Austria: IEEE; 2016:25–30.

IN: Tsung-Ting Kuo, Hyeon-Eui Kim, and Lucila Ohno-Machado, (2017), Blockchain distributed ledger technologies for biomedical and health care applications

[179] Kish LJ, Topol EJ. Unpatients [mdash] why patients should own their medical data. Nat Biotechnol. 2015;33(9):921–24.

IN: Tsung-Ting Kuo, Hyeon-Eui Kim, and Lucila Ohno-Machado, (2017), Blockchain distributed ledger technologies for biomedical and health care applications

[180] Ekblaw A, Azaria A, Halamka JD, Lippman A. A Case Study for Blockchain in Healthcare:“MedRec” Prototype for Electronic Health Records and Medical Research Data. Use of Blockchain for Healthcare and Research Workshop. 2016.

IN:Tsung-Ting Kuo, Hyeon-Eui Kim, and Lucila Ohno-Machado, (2017), Blockchain distributed ledger technologies for biomedical and health care applications

[181] Azaria A, Ekblaw A, Vieira T, Lippman A. MedRec: using blockchain for medical data access and permission management. International Conference on Open and Big Data (OBD). Vienna, Austria: IEEE; 2016:25–30.

IN:Tsung-Ting Kuo, Hyeon-Eui Kim, and Lucila Ohno-Machado, (2017), Blockchain distributed ledger technologies for biomedical and health care applications

[182] Peterson K, Deeduvanu R, Kanjamala P, Boles K. A blockchain-based approach to health information exchange networks. ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST; 2016.

IN: Tsung-Ting Kuo, Hyeon-Eui Kim, and Lucila Ohno-Machado, (2017), Blockchain distributed ledger technologies for biomedical and health care applications

[183] Blockchain Luxembourg S.A. Confirmed Transactions Per Day. <https://blockchain.info/charts/n-transactions> . Accessed December 14, 2016.

IN: Tsung-Ting Kuo, Hyeon-Eui Kim, and Lucila Ohno-Machado, (2017), Blockchain distributed ledger technologies for biomedical and health care applications

[184] Visa Inc. Visa Acceptance for Retailers. <https://usa.visa.com/run-yourbusiness/small-business/tools/retail.html> . Accessed December 14,

2016. IN:Tsung-Ting Kuo, Hyeon-Eui Kim, and Lucila Ohno-Machado, (2017), Blockchain distributed ledger technologies for biomedical and health care applications

[185] M.M.H. Onik, N. Al-Zaben, H. Phan Hoo, C.S. Kim, MUXER—a new equipment for energy saving in ethernet, *Technologies* 5 (4) (2017) 74.

IN: Md. Mehedi Hassan Onik, Satyabrata Aich, Jinhong Yang, Chul-Soo Kim, Hee-Cheol Kim (2019), Big Data Analytics for Intelligent Healthcare Management, chapter 8 : blockchain in healthcare-challenges and solutions # 2019 Elsevier Inc. All rights reserved.

<https://doi.org/10.1016/B978-0-12-818146-1.00008-8>

[186] Linn LA, Koo MB. Blockchain for health data and its potential use in health IT and health care related research. ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST; 2016.

IN:Tsung-Ting Kuo, Hyeon-Eui Kim, and Lucila Ohno-Machado, (2017), Blockchain distributed ledger technologies for biomedical and health care applications

[187] Attili S, Ladwa SK, Sharma U, Trenkle AF. Blockchain: the chain of trust and its potential to transform healthcare – our point of view. ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST; 2016.

IN:Tsung-Ting Kuo, Hyeon-Eui Kim, and Lucila Ohno-Machado, (2017), Blockchain distributed ledger technologies for biomedical and health care applications

[188] McConaghy T, Marques R, Müller A, et al. BigchainDB: A Scalable Blockchain Database. <https://www.bigchaindb.com/whitepaper/>. Accessed July 30, 2016.

IN:Tsung-Ting Kuo, Hyeon-Eui Kim, and Lucila Ohno-Machado, (2017), Blockchain distributed ledger technologies for biomedical and health care applications

[189] BigchainDB GmbH. BigchainDB The scalable blockchain database. <https://www.bigchaindb.com/> . Accessed December 16, 2016.

IN: Tsung-Ting Kuo, Hyeon-Eui Kim, and Lucila Ohno-Machado, (2017), Blockchain distributed ledger technologies for biomedical and health care applications

[190] Buterin V. A Next-generation Smart Contract and Decentralized Application Platform. <https://github.com/ethereum/wiki/wiki/White-Paper>. Accessed July 31, 2016.

IN: Tsung-Ting Kuo, Hyeon-Eui Kim, and Lucila Ohno-Machado, (2017), Blockchain distributed ledger technologies for biomedical and health care applications

[191] Greenspan G. MultiChain Private Blockchain. <http://www.multichain.com/download/MultiChain-White-Paper.pdf>. Accessed July 30, 2016.

IN: Tsung-Ting Kuo, Hyeon-Eui Kim, and Lucila Ohno-Machado, (2017), Blockchain distributed ledger technologies for biomedical and health care applications

[192] Meiklejohn S, Pomarole M, Jordan G, Levchenko K, McCoy D, Voelker GM, Savage S. A fistful of bitcoins: characterizing payments among men with no names. 2013 Internet Measurement Conference. Barcelona, Spain: ACM; 2013:127–140.

IN: Tsung-Ting Kuo, Hyeon-Eui Kim, and Lucila Ohno-Machado, (2017), Blockchain distributed ledger technologies for biomedical and health care applications

[193] Ohno-Machado L, Bafna V, Boxwala AA, et al. iDASH. Integrating data for analysis, anonymization, and sharing. *J Am Med Inform Assoc.* 2012;19:196–201

IN: Tsung-Ting Kuo, Hyeon-Eui Kim, and Lucila Ohno-Machado, (2017), Blockchain distributed ledger technologies for biomedical and health care applications

[194] Ohno-Machado L. To share or not to share: that is not the question. *Sci Transl Med.* 2012;4(165):165cm15.

IN: Tsung-Ting Kuo, Hyeon-Eui Kim, and Lucila Ohno-Machado, (2017), Blockchain distributed ledger technologies for biomedical and health care applications

[195] K. Abouelmehdi, A. Beni-Hessane, H. Khaloufi, Big healthcare data: preserving security and privacy, *J. Big Data* 5 (1) (2018) 1.

IN: Md. Mehedi Hassan Onik, Satyabrata Aich, Jinhong Yang, Chul-Soo Kim, Hee-Cheol Kim (2019), Big Data Analytics for Intelligent Healthcare Management, chapter 8 : blockchain in healthcare-challenges and solutions # 2019 Elsevier Inc. All rights reserved.

<https://doi.org/10.1016/B978-0-12-818146-1.00008-8>

[196] A.V. Humbeeck, The Blockchain-GDPR Paradox—Wearetheledger—Medium, Retrieved from: <https://medium.com/wearetheledger/the-blockchain-gdpr-paradox-fc51e663d047>, 2017. Accessed 14 June 2018.

IN: Md. Mehedi Hassan Onik, Satyabrata Aich, Jinhong Yang, Chul-Soo Kim, Hee-Cheol Kim (2019), Big Data Analytics for Intelligent Healthcare Management, chapter 8 : blockchain in healthcare-challenges and solutions # 2019 Elsevier Inc. All rights reserved.

<https://doi.org/10.1016/B978-0-12-818146-1.00008-8>

[197] K. Peterson, R. Deeduvanu, P. Kanjamala, K. Boles, A blockchain-based approach to health information exchange networks, in: *Proc. NIST Workshop Blockchain Healthcare*, vol. 1, 2016, pp. 1-10.

IN: Md. Mehedi Hassan Onik, Satyabrata Aich, Jinhong Yang, Chul-Soo Kim, Hee-Cheol Kim (2019), Big Data Analytics for Intelligent Healthcare Management, chapter 8 : blockchain in healthcare-challenges and solutions # 2019 Elsevier Inc. All rights reserved.

<https://doi.org/10.1016/B978-0-12-818146-1.00008-8>

