ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

Η συμβολή της τεχνολογίας Blockchain στο χώρο της υγείας.

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της

ΤΣΑΦΟΥ ΑΠΟΣΤΟΛΟΠΟΥΛΟΥ ΣΤΕΛΛΑΣ

Επιβλέπων : Δημήτριος - Διονύσιος Κουτσούρης
Καθηγητής Ε.Μ.Π.

Αθήνα, Ιανουάριος 2020

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ ΣΧΟΛΗ
ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ
ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ
ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

Η συμβολή της τεχνολογίας Blockchain στο χώρο της υγείας.

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της

ΤΣΑΦΟΥ ΑΠΟΣΤΟΛΟΠΟΥΛΟΥ ΣΤΕΛΛΑΣ

Επιβλέπων : Δημήτριος - Διονύσιος Κουτσούρης
Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 20η Ιανουαρίου 2020

(Υπογραφή)	*(Υπογραφή)*	*(Υπογραφή)*
.....	.....	.....
Δ. – Δ. Κουτσούρης Καθηγητής Ε.Μ.Π.	Γ. Ματσόπουλος Καθηγητής Ε.Μ.Π.	Π. Τσανάκας Καθηγητής Ε.Μ.Π.

Αθήνα, Ιανουάριος 2020

(Υπογραφή)

.....

ΤΣΑΦΟΥ ΑΠΟΣΤΟΛΟΠΟΥΛΟΥ ΣΤΕΛΛΑ

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

Περίληψη

Σκοπός αυτής της διπλωματικής είναι η παρουσίαση της τεχνολογίας Blockchain και η ανάδειξη των δυνατοτήτων της, στην ανάπτυξη καινοτόμων εφαρμογών. Η παρούσα διπλωματική εστιάζει το ενδιαφέρον της κυρίως στη χρήση της τεχνολογίας blockchain στο χώρο της υγείας.

Η μελέτη ακολουθεί μια λογική πορεία από πιο γενικές έννοιες σε πιο εξειδικευμένες και περιλαμβάνει σφαιρική πληροφόρηση από διάφορες οπτικές και πηγές, ώστε να εξασφαλισθεί η σταδιακή εξοικείωση και η όσο το δυνατόν πληρέστερη ενημέρωση για την Τεχνολογία Blockchain στο χώρο της υγείας, με συνοχή και συνέχεια από το ένα κεφάλαιο στο άλλο.

Η διπλωματική εργασία είναι οργανωμένη σε 5 κεφάλαια. Στο πρώτο κεφάλαιο πραγματοποιείται η παρουσίαση της τεχνολογίας Blockchain και των βασικών χαρακτηριστικών που διαθέτει . Στο δεύτερο κεφάλαιο περιγράφεται η αρχιτεκτονική των Blockchains και επισημαίνονται η δομή και τα χρήσιμα στοιχεία αυτής της τεχνολογίας. Στο τρίτο κεφάλαιο αφού αναλυθούν τα πλεονεκτήματα και οι δυνατοί τρόποι εφαρμογής των blockchains στο χώρο της υγείας δίνονται παραδείγματα εφαρμοσμένων συστημάτων στον ιατρικό κλάδο. Στο στάδιο αυτό γίνεται εκτενής βιβλιογραφική αναζήτηση τόσο σε ερευνητικές όσο και σε εμπορικές εφαρμογές. Στο τέταρτο κεφάλαιο παρουσιάζεται η εξέλιξη της τεχνολογίας Blockchain στο χώρο της υγείας και αναλύονται τα παραδείγματα μελλοντικών εφαρμογών Blockchains. Τέλος, στο πέμπτο κεφάλαιο παρουσιάζονται συνοπτικά τα πλεονεκτήματα και τα μειονεκτήματα εφαρμογής της τεχνολογίας blockchain στον ιατρικό τομέα και παρατίθενται οι αντίστοιχες παρατηρήσεις και τα συμπεράσματα .

Συνολικά, καταδεικνύεται ότι η εφαρμογή της τεχνολογίας blockchain έχει ιδιαίτερη αξία. Αυτό φαίνεται και από το συνεχώς αυξανόμενο ερευνητικό ενδιαφέρον γύρω από το blockchain, σε τομείς όπου παραδοσιακά δεν είχε εφαρμογή. Ειδικά στον τομέα της υγείας, το blockchain μπορεί να δημιουργήσει πιο αξιόπιστα και ανθεκτικά δίκτυα, βοηθώντας παράλληλα στην απρόσκοπτη επικοινωνία ανάμεσα στα διάφορα ενδιαφερόμενα μέρη (γιατροί, ασθενείς, νοσοκομεία κτλ.).

Λέξεις κλειδιά: τεχνολογία Blockchain, τεχνολογία κατανεμημένου καθολικού, αποκεντρωμένο σύστημα, συναρτήσεις κατακερματισμού, κρυπτογραφία, έξυπνα συμβόλαια, ζεύγος κλειδιών, πρωτόκολλα ομοφωνίας.

Abstract

The purpose of this thesis is to present Blockchain technology and showcase its potential in developing innovative applications. This thesis focuses mainly on the use of blockchain technology in the field of health.

The study follows a rational course from more general concepts to more specialized ones and includes comprehensive information from various perspectives and sources to ensure gradual familiarization and as comprehensive as possible information on Blockchain Technology in the health field, with coherence and continuity from one chapter to another.

The thesis is organized into 5 chapters. The first chapter introduces Blockchain technology and its key features. The second chapter describes the architecture of the Blockchains and highlights the structure and useful elements of this technology. In the third chapter, after analyzing the advantages and possible ways of applying blockchains in the field of health, examples of applied systems in the medical industry are given. At this stage, extensive bibliographical searches are carried out in both research and commercial applications. The fourth chapter describes the evolution of Blockchain technology in the field of health and analyzes the examples of future Blockchains applications. Finally, the fifth chapter gives a brief overview of the advantages and disadvantages of blockchain technology in the medical field and presents the respective observations and conclusions.

Overall, it is demonstrated that the application of blockchain technology is of particular value. This is also evidenced by the growing research interest around blockchain, in areas where it has not traditionally been implemented. Especially in the health sector, blockchain can create more reliable and robust networks, while helping seamless communication between various stakeholders (doctors, patients, hospitals, etc.).

Keywords: Blockchain technology, distributed ledger technology, decentralized system, hash functions, cryptography, smart contracts, key pair, consensus protocols.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω θερμά όλους εκείνους που με βοήθησαν και με στήριξαν στην ολοκλήρωση της διπλωματικής μου εργασίας, αλλά και στην επιτυχή περάτωση της φοίτησής μου στη Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Εθνικού Μετσόβιου Πολυτεχνείου. Πρώτα από όλα την οικογένεια μου για την αμέριστη ηθική και υλική τους συμπαράσταση καθ' όλη τη διάρκεια των σπουδών μου, έπειτα όλους τους φίλους μου και συμφοιτητές μου για την ανιδιοτελή βοήθεια που μου προσέφεραν σε όλες τις δυσκολίες που αντιμετώπισα κατά τη διάρκεια της φοίτησής μου.

Θα ήθελα να ευχαριστήσω θερμά τον καθηγητή κ. Δημήτριο Κουτσούρη που μου έδωσε την ευκαιρία να αναπτύξω τη διπλωματική μου εργασία, καθώς και την υποψήφια διδάκτορα κα. Ουρανία Μαντά για την υποστήριξή της και την καθοδήγησή της κατάμτη διάρκεια της εκπόνησης της παρούσας εργασίας. Η συνεργασία μας ήταν άψογη και οι συμβουλές τους πολύτιμες σε όλα τα στάδια και τη διάρκεια της εργασίας μου, υποδεικνύοντάς μου την ορθή και επιστημονική προσέγγιση του θέματος.

Πίνακας περιεχομένων

Πίνακας εικόνων

1.

1.1 Εισαγωγή στην τεχνολογία Blockchain.

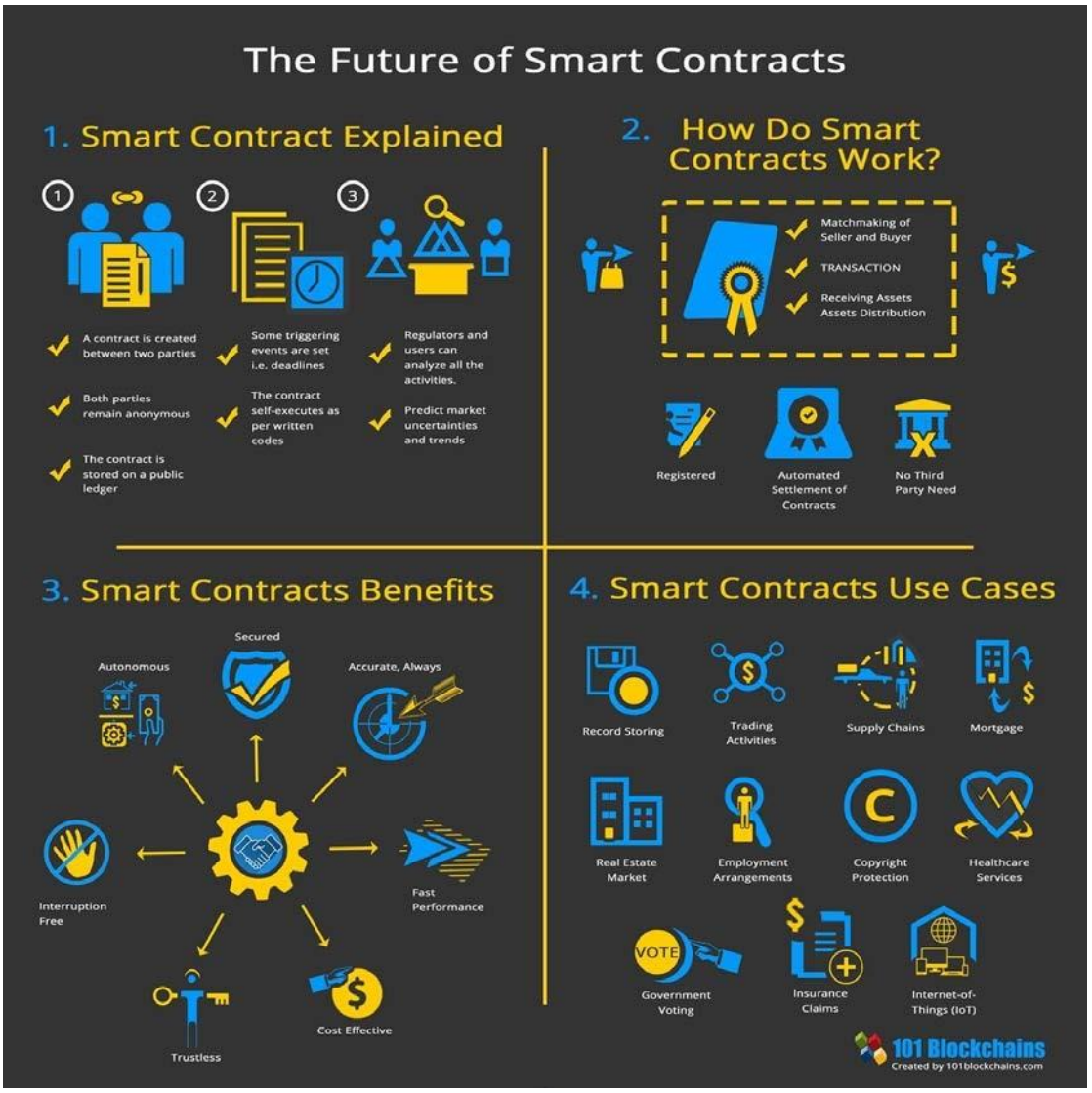
Σε αυτό το κεφάλαιο, θα οριστεί η τεχνολογία Blockchain και οι τύποι της, θα γίνει μια σύντομη επισκόπηση στην ιστορία της, ενώ παράλληλα θα εντοπιστούν τα πλεονεκτήματα της σε σχέση με τεχνολογίες παλαιού τύπου. Επίσης, θα παρουσιαστεί η γενική χρήση της τεχνολογίας αυτής τόσο στον τομέα της υγείας όσο και στην ευρύτερη βιομηχανία. Τέλος, θα αναπτυχθούν τα κύρια χαρακτηριστικά της, και οι λόγοι που την αναδεικνύουν και την καθιστούν ιδιαίτερα χρήσιμη σε πολλούς τομείς ,καθώς και το ερευνητικό ενδιαφέρον που παρουσιάζει.

1.1.1 Ορισμός του Blockchain.

Το Blockchain είναι ένας **τύπος Τεχνολογίας Κατανεμημένου Λογαριασμού που μπορεί να καταγράφει όλες τις συναλλαγές και να τις μοιράζεται μέσω ενός δικτύου υπολογιστών peer-to-peer (P2P)**, χρησιμοποιώντας κρυπτογραφικούς μηχανισμούς εμπιστοσύνης και διασφάλισης [1]. Η τεχνολογία κατανεμημένου λογαριασμού αναφέρεται στα πρωτόκολλα και στην υποστήριξη της υποδομής που επιτρέπει σε υπολογιστές σε διαφορετικές τοποθεσίες να προτείνουν, να επικυρώνουν τις συναλλαγές και να ενημερώνουν τις εγγραφές με συγχρονισμένο τρόπο σε ένα δίκτυο. Η βασική ιδέα του Blockchain είναι η ύπαρξή ενός κοινού χώρου διατήρησης και γνωστοποίησης δεδομένων συναλλαγής προσιτού σε όλα τα μέλη μιας κοινότητας. Για να γίνει κατανοητή η κύρια και διαχρονική ανάγκη που καλύπτει το blockchain, παρουσιάζεται ένα απλό παράδειγμα μιας προσπάθειας που έχει καταγραφεί πολύ πριν την δημιουργία του, αυτό είναι οι πέτρες Rai που χρησιμοποιούνταν στο νησί Yap του Ειρηνικού Ωκεανού το 500 μ.Χ. Οι πέτρες αυτές ήταν μια μορφή ασβεστολιθικού νομίσματος που συμβόλιζαν διαπραγματεύσεις που επικυρώνονταν με προφορική συμφωνία. Κατά τη διάρκεια μιας συναλλαγής, οι πέτρες δεν άλλαζαν χέρια (μερικές ζύγιζαν 4 τόνους), αλλά η ιδιοκτησία καταγραφόταν πάνω σε αυτές και στη συνέχεια λεκτικά γινόταν γνωστή η συναλλαγή σε όλη τη κοινότητα. Έτσι, δημιουργήθηκε ένα κοινό βιβλίο το οποίο ενημερωνόταν με ομαδική συναίνεση χωρίς την εμπλοκή ενδιάμεσων[2]. Μια πιο σύγχρονη αλλά παρόμοιας λογικής προσπάθεια, είναι η δημιουργία του blockchain **ως αμετάβλητη, αποκεντρωμένη και ψηφιοποιημένη καταγραφή των δεδομένων συναλλαγής με χρονολογική σειρά, ανοιχτά προσβάσιμη στους συμμετέχοντες.** Πρόκειται δηλαδή για τη δημιουργία ενός δικτύου ανταλλαγής για τη διαχείριση συναλλαγών(transactions), αξιών και περιουσιακών στοιχείων (assets) μεταξύ ισότιμων συμμετεχόντων.

Μέσα σε ένα blockchain, κάθε συμπεριλαμβανόμενος κόμβος στο δίκτυο περιέχει ένα πλήρες αντίγραφο στο καθολικό/μητρώο (ledger). Χρησιμοποιεί έναν αλγόριθμο που ονομάζεται **μοντέλο συναίνεσης** για την αποτροπή προβλημάτων συγχρονισμού μεταξύ κόμβων, συμπεριλαμβανομένων των προβλημάτων "διπλής δαπάνης". Το πρόβλημα της **διπλής δαπάνης** ουσιαστικά αναφέρεται στο γεγονός ότι οι ψηφιακές πληροφορίες μπορούν να αντιγραφούν χρησιμοποιώντας το Διαδίκτυο. Αν, για παράδειγμα, κάποιος στείλει ένα ψηφιακό στοιχείο όπως ένα ψηφιακό χαρτί ιδιοκτησίας ενός αυτοκινήτου σε κάποιον άλλο, στη συνέχεια υπάρχει ο κίνδυνος ο αποστολέας να αποστέλλει ένα αντίγραφο μέσω του διαδικτύου και να διατηρεί ακόμα το πρωτότυπο έγγραφο ιδιοκτησίας. Παραδοσιακά, ο κίνδυνος αυτός έχει μετριαστεί με την επικύρωση από αξιόπιστα τρίτα μέρη ή διαχειριστές, όπως οι τράπεζες, οι οποίοι ενεργούν ως κεντρική αρχή παρακολούθηση όλων των συναλλαγών. Η κατανεμημένη βάση δεδομένων (distributed ledger database) μεταθέτει αυτή την ευθύνη της επικύρωσης της μεταφοράς του περιουσιακού στοιχείου, σε ολόκληρο το δίκτυο χρησιμοποιώντας προσεκτικά σχεδιασμένους αλγόριθμους [3]. Αυτό εξαλείφει την ανάγκη για μια κεντρική βάση δεδομένων. Κάθε χρήστης στο δίκτυο έχει ένα αντίγραφο του μητρώου συναλλαγών και κάθε αλλαγή κυριότητας των ψηφιακών στοιχείων στο σύστημα απαιτεί επικύρωση από τους χρήστες του.

Χρησιμοποιώντας τα **έξυπνα συμβόλαια**, το blockchain μπορεί να υποστηρίξει μια ευρεία γκάμα χρήσεων και περιπτώσεων που ισχύουν τόσο στον χρηματοπιστωτικό τομέα, όσο και στο τομέα της υγειονομικής περίθαλψης, της ενέργειας, της βιομηχανίας και της έρευνας με την παροχή ενός μηχανισμού που επιτρέπει σε μη αξιόπιστες οντότητες να αλληλεπιδρούν και να συνεργάζονται. Τα έξυπνα συμβόλαια είναι κομμάτια λογισμικού που εκτελούν μια συγκεκριμένη ενέργεια με βάση την κατάσταση του συστήματος ή μια συναλλαγή που συμβαίνει. Μια έξυπνη σύμβαση είναι ένα πρόγραμμα ή ένα πρωτόκολλο που διευκολύνει, επαληθεύει ή εκτελεί τους όρους μιας σύμβασης. Τα έξυπνα συμβόλαια λειτουργούν σε αποκεντρωμένο μητρώο, είναι ανεξάρτητα από την ανθρώπινη παρέμβαση και εκτελούνται αυτόματα. Οι έξυπνες συμβάσεις μπορούν να θεωρηθούν ιδιωτικά πλαίσια κανονισμών - ένα σύστημα κανόνων που διέπουν τις συναλλαγές μεταξύ των ενδιαφερομένων και τα συμβαλλόμενα μέρη. Μόλις καθιερωθούν, οι έξυπνες συμβάσεις είναι αμετάκλητες και δεσμευτικές [4].



Εικόνα 1. Έξυπνα συμβόλαια , πλεονεκτήματα και χρήσεις του**[5]**.

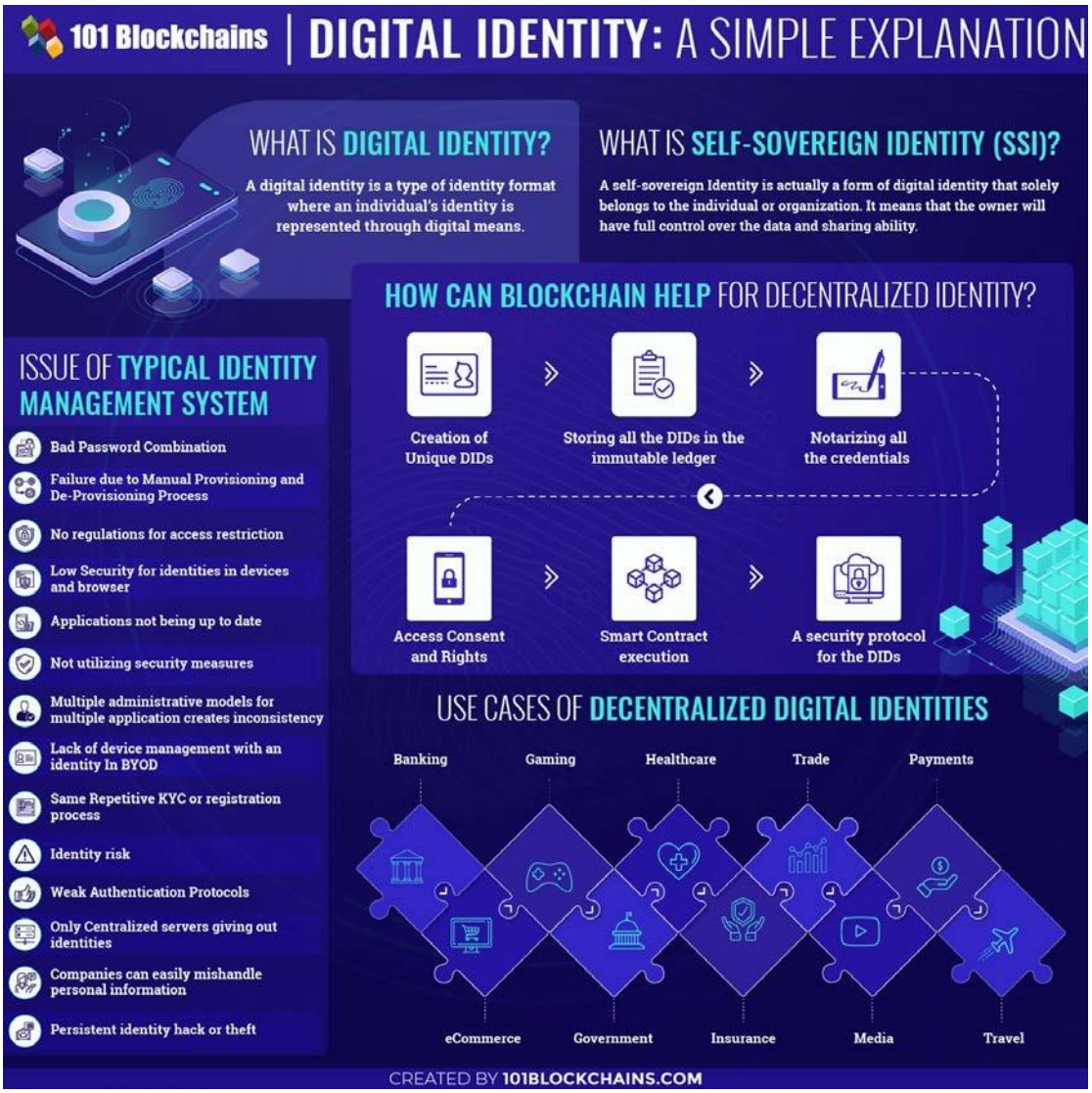
Η τεχνολογία Blockchain έχει γίνει δεχτή με ιδιαίτερη θέρμη, ωστόσο, πολλοί κλάδοι πέρα από τον χρηματοπιστωτικό, εξακολουθούν να είναι σε αρχικό στάδιο κατανόησης των δυνατοτήτων που τους προσφέρει. Στον τομέα της υγειονομικής περίθαλψης, η τεχνολογία blockchain θα μπορούσε να βελτιώσει τον τρόπο με τον οποίο οι πληροφορίες κυκλοφορούν σε ολόκληρη την αλυσίδα υγείας από τη δημιουργία φαρμάκων, τις κλινικές δοκιμές και τη συλλογή ιατρικών δεδομένων, έως την κατασκευή, τις πωλήσεις και το μάρκετινγκ.

1.1.2 Κύρια Χαρακτηριστικά του Blockchain.

Ένα από τα κύρια χαρακτηριστικά του Blockchain είναι ότι είναι δύσκολο να αλλοιωθεί η πληροφορία που περιέχει. Αυτό όπως αναφέραμε και παραπάνω, συμβαίνει διότι ο κάθε συμπεριλαμβανόμενος κόμβος στο δίκτυο έχει **ένα ακριβές αντίγραφο στο ψηφιακό καθολικό**. Για να προστεθεί μια καινούργια συναλλαγή στο δίκτυο θα πρέπει ο κάθε κόμβος να ελέγξει την εγκυρότητα της. Εφόσον γίνει ο έλεγχος και εγκριθεί ως γνήσια συναλλαγή, τότε μόνο προστίθεται στο δίκτυο. Με

πολλαπλούς συμμετέχοντες ταυτόχρονα για την έγκριση διαφορετικών τμημάτων συναλλαγών, θα ήταν δυνητικά δύσκολο να εντοπιστεί το αντίγραφο του καθολικού που θα ακολουθήσει [6]. Οι συναλλαγές περιέχουν μια αναφορά στο προηγούμενο μπλοκ, ο σύνδεσμος αυτός κρυπτογραφείται χρησιμοποιώντας μια συνάρτηση κατακερματισμού (hash function) και με τον τρόπο αυτό δημιουργείται μια "αλυσίδα" μπλοκ. Η επιλογή του επόμενου έγκυρου block γίνεται με την χρήση ενός μοντέλου συναίνεσης, που καθορίζει το δίκτυο των κόμβων θα πρέπει να υιοθετηθούν από το blockchain σε όλο το δίκτυο.

Ακόμα ένα ισχυρό χαρακτηριστικό στα blockchains, είναι ότι η ταυτότητα καθορίζεται χρησιμοποιώντας ένα ζευγάρι αριθμών που ονομάζεται **ζεύγος κλειδιών**, το οποίο αποτελείται από ένα δημόσιο κλειδί και ένα ιδιωτικό κλειδί. **Το ιδιωτικό κλειδί** είναι μυστικό και γνωστό μόνο στον ιδιοκτήτη, ενώ το **δημόσιο κλειδί** (ή μια διεύθυνση που προέρχεται από αυτό) είναι ορατό σε άλλους στο blockchain. Η ιδιοκτησία ενός ιδιωτικού κλειδιού είναι αυτό που ορίζει την **ταυτότητα** σε ένα blockchain. Πριν υποβάλει ένα άτομο συναλλαγή σε blockchain, πρέπει να υπογράψει τη συναλλαγή χρησιμοποιώντας το ιδιωτικό κλειδί του. Η υπογραφή είναι αυτή που επιτρέπει στο blockchain να επαληθεύσει την αυθεντικότητα της συναλλαγής. Είναι δυνατόν να συσχετιστεί ένα ιδιωτικό κλειδί με πολλά δημόσια κλειδιά[7]. Στο blockchain δεν υπάρχει κάποια αρμόδια αρχή που επιμελείται τη δομή του ,αντί αυτού, υπάρχει ένα **σύμπλεγμα κόμβων που διατηρεί το δίκτυο** και το καθιστά αποκεντρωμένο. Εξαιτίας της απουσίας κεντρικής επιτήρησης, μας παρέχεται μια ενισχυμένη αίσθηση ασφάλειας διότι δεν δύναται ο οποιοσδήποτε να επέμβει στο δίκτυο αλλάζοντας τα χαρακτηριστικά του προς όφελος του, ενώ η χρήση της κρυπτογράφησης αυξάνει την ασφάλεια του συστήματος. Επιπλέον το καθολικό του δικτύου διατηρείται από όλους του χρήστες του συστήματος, αυτή η κατανομή της υπολογιστικής ενέργειας δια μέσου των υπολογιστών διευκολύνει τις συναλλαγές και τις καθιστά πλήρως γνωστοποιημένες ακόμη και σε μεγάλα και πολύπλοκα συστήματα. Τα blockchains χάρη στην αποκέντρωση του δικτύου προσφέρουν επιπλέον, ταχύτερη διευθέτηση συναλλαγών συγκριτικά με το παραδοσιακό τραπεζικό σύστημα. Έτσι ένας χρήστης είναι σε θέση να μεταφέρει χρηματικά ποσά πιο άμεσα, γεγονός που διευκολύνει τις συναλλαγές και μακροπρόθεσμα του εξοικονομεί χρόνο.



Εικόνα 2. Αποκεντρωμένο καθολικό**[8].**

1.1.3 Τύποι Blockchain.

Υπάρχουν τρεις τύποι blockchain, τα δημόσια τα ιδιωτικά και τα κοινοπρακτικά blockchains. **Τα δημόσια blockchains (Open blockchains)** είναι ανοικτά και επομένως δίνεται η δυνατότητα εκμετάλλευσης των ιδιοτήτων της κατανομής του δικτύου από πληθώρα ανθρώπων εφόσον δεν υπάρχουν περιορισμοί ως προς την πρόσβαση. Ακόμη, ο κάθε χρήστης δύναται να συμμετέχει στα πρωτόκολλα ομοφωνίας, ενώ συνήθως για τη σωστή λειτουργία και την ασφάλεια του συστήματος δίνονται χρηματικές αμοιβές στους συμμετέχοντες ειδικά όταν χρησιμοποιούνται αλγόριθμοι **Proof of Work (PoW)**[9]. Ο αλγόριθμος PoW δομεί τη διαδικασία με την οποία επιλέγεται το επόμενο μπλοκ, δίνει το κίνητρο για την εξεύρεση σωστής λύσης στο κρυπτογραφικό παζλ από τους συμμετέχοντες, επειδή παρέχεται μια ανταμοιβή. Αυτό το διακριτικό ή το κρυπτοεγχειρίδιο ενισχύει τη δημιουργία αξίας, η οποία είναι μια πολύ σημαντική έννοια στο blockchain και το διαφοροποιεί από τις παραδοσιακές, κεντρικές υπηρεσίες εφαρμογών. Τέλος, τα δημόσια blockchains έχουν το πλεονέκτημα ότι παρέχουν μια ασπίδα προστασίας των χρηστών από τους

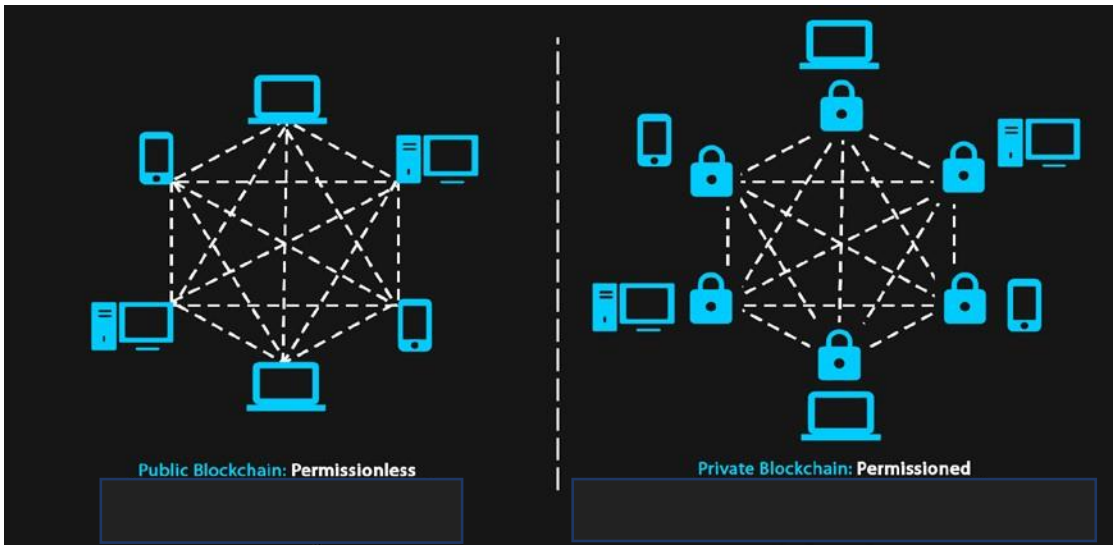
προγραμματιστές, διασφαλίζοντας ότι υπάρχουν ορισμένες σταθερές που ούτε οι ίδιοι οι δημιουργοί μιας εφαρμογής δεν έχουν τη δυνατότητα/εξουσιοδότηση να αλλάξουν.

Στην περίπτωση των **ιδιωτικών blockchains (Private blockchains)** δεν προσφέρουν ελεύθερη είσοδο σε όλους. Για να αποκτήσει κάποιος πρόσβαση σε αυτά θα έπρεπε να δοθεί έγκριση από τον κάτοχο του συστήματος. Η ομάδα ανθρώπων ή η εταιρεία που το αξιοποιεί έχει το δικαίωμα ελέγχου και δύναται να επέμβει όταν το επιθυμεί, μετατρέποντας τους κανόνες, ανατρέποντας τις συναλλαγές, τροποποιώντας τα ισοζύγια κλπ. Επιπλέον, στην περίπτωση αυτή, μειώνεται το κόστος τον συναλλαγών σε σύγκριση με ένα δημόσιο, διότι η συναλλαγή πρέπει να επαληθευτεί μόνο από κάποιους κόμβους που μπορούν να εμπιστευτούν την πολύ υψηλή επεξεργαστική ισχύ τους και δεν χρειάζεται να επαληθεύονται από χιλιάδες υπολογιστές. Επιπρόσθετα, οι επικυρωτές είναι συγκεκριμένοι, οπότε μειώνεται ο κίνδυνος επίθεσης. Ένα ακόμη πλεονέκτημα ενός ιδιωτικού Blockchain είναι η ταχύτερη επιδιόρθωση βλαβών χάρη στον γρηγορότερο εντοπισμό του προβλήματος που επιτρέπει την πιο άμεση επέμβαση για την επίλυση του. Αυτό συμβαίνει εξαιτίας της καλής σύνδεσης των κόμβων, που επιτρέπουν τη χρήση αλγορίθμων συναίνεσης καταλήγοντας στο τελικό αποτέλεσμα ταχύτερα. Τέλος, τα ιδιωτικά blockchains παρέχουν μεγαλύτερη προστασία των προσωπικών δεδομένων εφόσον τα δικαιώματα ανάγνωσης είναι περιορισμένα[10].

Τα **κοινοπρακτικά blockchains (Consortium blockchains),** παρουσιάζουν πολλές ομοιότητες στον τρόπο λειτουργιάς τους με τα ιδιωτικά blockchains, διαφοροποιούνται όμως στο γεγονός ότι ο έλεγχος δεν ανήκει σε μια μόνο εταιρία ή σε έναν οργανισμό αλλά σε ένα σύμπλεγμα εταιριών. Όλες οι επιμέρους εταιρίες μπορούν να έχουν έναν κόμβο στο δίκτυο και οι διαχειριστές ολόκληρου του δικτύου είναι υπεύθυνοι να επιλέγουν σε ποιους κόμβους θα παρέχουν δικαίωμα συμμετοχής στα πρωτόκολλα ομοφωνίας.

Συμπερασματικά, είναι φανερό ότι όλα τα είδη έχουν θετικά και αρνητικά στοιχεία, οπότε η επιλογή θα πρέπει να εξαρτάται από τη χρήση που απαιτείται να γίνει. Αν κάποιος επιθυμεί τη μεταφορά ψηφιακών στοιχείων μεταξύ μιας κλειστής ομάδας ανθρώπων και τη διατήρηση του απορρήτου των συναλλαγών ή να έχει μεγάλο όγκο συναλλαγών ανά δευτερόλεπτο, τότε φαίνεται καταλληλότερη μια ιδιωτική μπλοκ αλυσίδα. Τα ιδιωτικά blockchains, έχουν συχνή εφαρμογή στη διατήρηση ιστορικών συμβάντων και για λογιστικούς σκοπούς γιατί με αυτή την επιλογή εξαλείφεται ο κίνδυνος απουσίας ελέγχου ή διαρροής ευαίσθητων δεδομένων στο γενικότερο δίκτυο. Αν αυτό που αναζητά είναι μια ανοιχτή και διαλειτουργική πλατφόρμα όπως το διαδίκτυο, είναι προτιμότερο να επιλέξει το δημόσιο blockchain. Τον **επαγγελματικό και χρηματοοικονομικό** τομέα φαίνεται να τον ενδιαφέρει περισσότερο οι εξελίξεις στο **ιδιωτικό** τύπο blockchain ,διότι εστιάζει στις δυνατότητες της τεχνολογίας αλλά δεν επιθυμεί τον μειωμένο έλεγχο που έχουν τα δημόσια δίκτυα. Οι σημαντικότερες **εξελίξεις της τεχνολογίας** blockchain στηρίζονται σε όλα τα προτερήματα που προέρχονται από το κοινό, το **«ανοιχτό»**

blockchain.[9]



Εικόνα 3. Διαφορές δημόσιου με Ιδιωτικού blockchain **[12].**

Στο δημόσιο τύπο blockchain ο οποιοσδήποτε μπορεί να καταγράψει δεδομένα χωρίς άδεια απο κάποια αρχή και ο οποιοσδήποτε μπορεί να διαβάσει τα δεδομένα .Στον ιδιωτικό τύπο blockchainμοι συμμετέχοντες στην αλυσίδα είναι γνωστοί και έμπιστοι .Οι ιδιωτικές αλυσίδες αυτές είναι πιο μικρές και γρήγορες ενώ το proof of work σχετικά πιο απλό ανάλογα με την επιχειρηματική απόφαση.

1.1.4 Ιστορία του Blockchain.

Η προέλευση της τεχνολογίας blockchain χρονολογείται από το 2008 όταν προτάθηκε ως σχεδιασμός της επιστήμης των υπολογιστών για να επιτρέψει την ασφαλή και άμεση διαπραγμάτευση περιουσιακών στοιχείων μεταξύ των χρηστών που μπορεί να μην έχουν επαρκή εμπιστοσύνη μεταξύ τους. Αυτή η νέα αποκεντρωμένη τεχνολογία εξαλείφει την ανάγκη διατήρησης των αρχείων από κάποια κεντρική αρχή ή ενδιάμεσους φορείς [4].

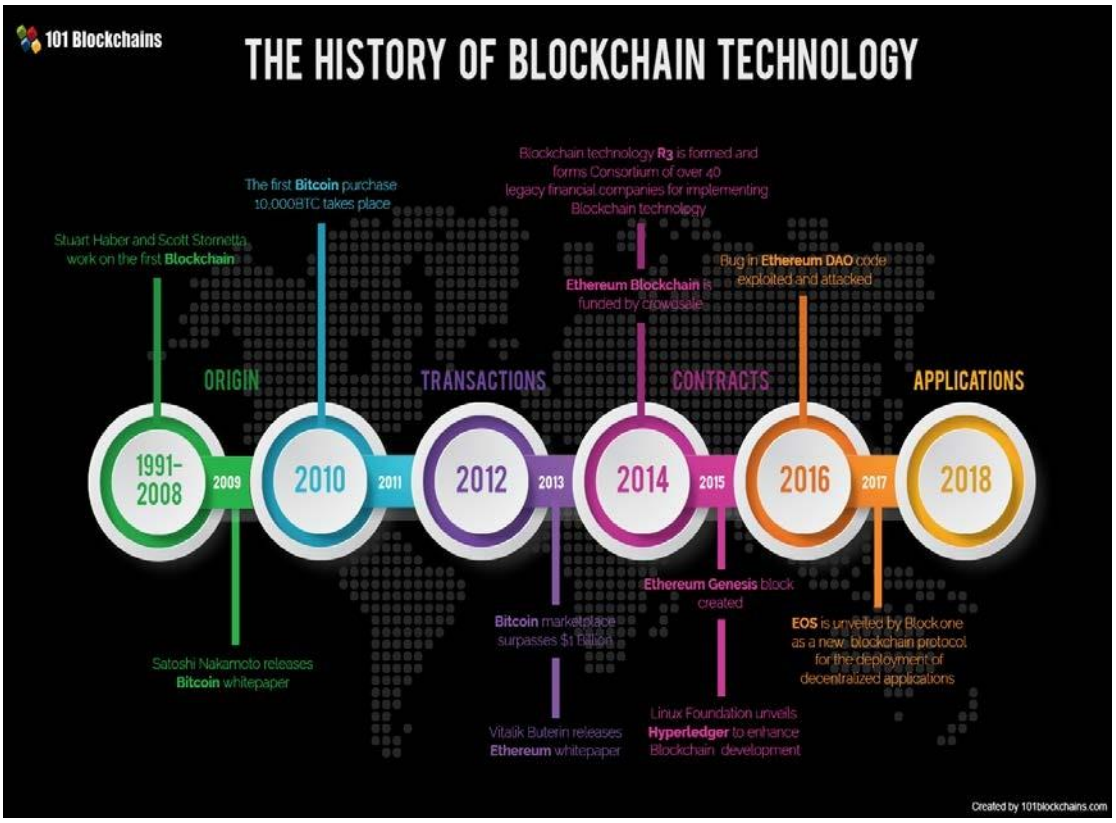
Το Blockchain εμφανίζεται για πρώτη φορά σε ένα έγγραφο που δημοσιεύεται από τον συντάκτη, ο οποίος είναι γνωστός με το ψευδώνυμο Satoshi Nakamoto. Σε αυτή την εργασία, η ιδέα ενός **Bitcoin** εισήχθη ως καθαρά peer-to-peer (P2P) δίκτυο ηλεκτρονικών συναλλαγών[13]. Αυτό το δίκτυο επέτρεπε άμεσες χρηματοπιστωτικές συναλλαγές χωρίς την μεσολάβηση κάποιου χρηματοπιστωτικού ιδρύματος. Για να απλοποιηθεί, η τεχνολογία blockchain επιτρέπει σε δύο παράγοντες του συστήματος (που ονομάζονται κόμβοι) να συναλλάσσονται σε ένα peer-to-peer (P2P) δίκτυο και αποθηκεύει αυτές τις συναλλαγές με κατανεμημένο τρόπο σε ολόκληρη την περιοχή. Σύμφωνα με την ευρέως αποδεκτή σύμβαση, το όνομα του δικτύου blockchain που χρησιμοποιεί τα πρωτόκολλα του Satoshi είναι γραμμένο με το κεφάλαιο «B» (Bitcoin) για να το διακρίνει από το νόμισμα που παράγεται στο εσωτερικό του συστήματος (bitcoin) [14]. Καταχωρεί τους ιδιοκτήτες των περιουσιακών στοιχείων που αποτελούν αντικείμενο συναλλαγών. Μια συναλλαγή επαληθεύεται από το δίκτυο με έναν «μηχανισμό συναίνεσης», ο οποίος επιτρέπει στους χρήστες στο δίκτυο P2P την επικύρωση των συναλλαγών και την ενημέρωση του μητρώου στο σύνολό του.

Ο **μηχανισμός συναίνεσης** χρησιμοποιείται για την εδραίωση της εμπιστοσύνης και την ακρίβεια των δεδομένων στο σύστημα, η οποία είχε παραδοσιακά καθιερωθεί από έναν μεσάζοντα ή έναν διαχειριστή σε ένα κεντρικό σύστημα. Ο μηχανισμός συναίνεσης είναι μια διαδικασία όπου οι κόμβοι σε ένα κατανεμημένο δίκτυο συμφωνούν για τις προτεινόμενες συναλλαγές [6]. Αυτός ο μηχανισμός προάγει την καταγραφή πληροφοριών κατά τρόπο που εξασφαλίζει την ακεραιότητα, τη μετατόπιση και την ακρίβεια των δεδομένων. Οι μηχανισμοί συναίνεσης είναι **κανόνες και πρωτόκολλα διακυβέρνησης** στο κατανεμημένο δίκτυο που επιτρέπουν την καταγραφή, την ολοκλήρωση και την εκτέλεση των συναλλαγών υπό ορισμένες προϋποθέσεις. Ως εκ τούτου, μπορεί να συναχθεί μια συμφωνία επί της προηγούμενης συναλλαγής, σχηματίζοντας μια ακολουθία συναλλαγών, παρόμοια με ένα ημερολόγιο. Στα blockchains, οι πολλαπλές συναλλαγές συγκεντρώνονται σε ένα μπλοκ το οποίο αναφέρεται μαθηματικά στο προηγούμενο μπλοκ. Στην περίπτωση του Bitcoin, μετά από ένα καθορισμένο χρονικό διάστημα, δημιουργείται ένα νέο μπλοκ με τις πραγματοποιηθείσες συναλλαγές που περιλαμβάνονται στο μπλοκ και επικυρώνονται στο δίκτυο. Αυτό σχηματίζει μια αλυσίδα μπλοκ: εξού και η ονομασία "blockchain".

Το **Bitcoin** ήταν ο πρώτος μηχανισμός που εφάρμοσε αυτό το αποκεντρωμένο, κατανεμημένο καθολικό συναλλαγών κρυπτογράφησης, παρόλα αυτά έχουν εισαχθεί πολλές εναλλακτικές λύσεις από τότε. Ενώ ο όρος blockchain αναφέρεται σε μια συγκεκριμένη στοίβα τεχνολογίας, χρησιμοποιείται όλο και περισσότερο για να αναφερθεί σε ένα χαλαρά συνδυασμένο σύνολο τεχνολογιών και διαδικασιών που καλύπτουν το μεσαίο λογισμικό, τη βάση δεδομένων, την ασφάλεια, την τεχνητή νοημοσύνη (AI), και τη νομισματική ταυτότητα. Ένα άλλο βασικό χαρακτηριστικό που αξιοποιούν οι πολλαπλές μπλοκ αλυσίδες είναι τα έξυπνα συμβόλαια. Έτσι το Blockchain μπορεί να οριστεί και ως ένας τύπος κατανεμημένου βιβλίου στο οποίο οι συναλλαγές ανταλλαγής αξίας (σε bitcoin ή άλλο διακριτικό) ταξινομούνται διαδοχικά σε μπλοκ. Κάθε μπλοκ είναι αλυσοδεμένο στο προηγούμενο μπλοκ και καταγεγραμμένο με άκαμπτο τρόπο σε έναν ομότιμο χρήστη μέσω κρυπτογραφικών μηχανισμών εμπιστοσύνης και διασφάλισης δεδομένων. Εξαρτάται από την υλοποίηση, αν οι συναλλαγές μπορούν να περιλαμβάνουν προγραμματιζόμενη συμπεριφορά.

Μετά το Bitcoin, **το Ethereum** δημιουργήθηκε τον Ιούλιο του 2015 και είναι η δεύτερη μεγαλύτερη πλατφόρμα blockchain της αγοράς, και ένα από τα δημοφιλέστερα δημόσια πρωτόκολλα blockchain για τα συστήματα επιχειρήσεων. Το Ethereum είναι ειδικά κατασκευασμένο για την εκτέλεση των έξυπνων συμβάσεων και την αυτοματοποίηση των ενεργειών κατά την τήρηση των κριτηρίων αξιολόγησης. Το Blockchain του Ethereum είναι επίσης χαμηλής αδειοδότησης και ανοιχτό. Έχει το δικό του νόμισμα (ETH) για να πραγματοποιεί συναλλαγές στο πλαίσιο του Ethereum. Εφαρμογές υγειονομικής περίθαλψης χρησιμοποιούν ιδιωτικά δίκτυα Ethereum με μοντέλα συναίνεσης που περιλαμβάνουν υλοποιήσεις των αλγορίθμων **Proof of Authority (PoA)** και **Proof of Stake** (**PoS)**[15]. Λόγω της χρήσης της κρυπτογράφησης, το Ethereum θα μπορούσε να προσφέρει ένα blockchain για την παροχή κινήτρων για τη συμμετοχή στην ανταλλαγή δεδομένων ασθενών. Το **PoA** αναφέρεται στα ιδιωτικά δίκτυα, και πρόκειται για ένα από τα πιο δημοφιλή μοντέλα συναίνεσης, όπου ένα υποσύνολο των κόμβων δικτύου επιλέγεται ως αρχή και καθορίζεται το επόμενο μπλοκ. Το Ethereum, για παράδειγμα, υποστηρίζει το πρωτόκολλο Clique PoA και άλλες ομάδες όπως η Parity έχουν

αναπτύξει τις δικές τους εφαρμογές του PoA, συμπεριλαμβανομένου του Tendermint και του Aura. Το **PoS** αναφέρεται στη σύνδεση της ασφάλεια του μοντέλου συναίνεσης με την αξία της κρυπτογράφησης επειδή οι κόμβοι με το μεγαλύτερο ποσό αξίας είναι οι κόμβοι που έχουν το σημαντικότερο λόγο στην απόφαση για το επόμενο έγκυρο μπλοκ [9]. Ο συλλογισμός στηρίζεται στο ότι κυριότερης σημασίας είναι οι κόμβοι που έχουν τα περισσότερα να χάσουν αν κάτι πάει στραβά. Αν η υποκείμενη κρυπτογράφηση έχει μηδενική αξία, τότε το PoS πάσχει από αυτό που ονομάστηκε πρόβλημα "τίποτα σε κίνδυνο".



Εικόνα 4. Ιστορία του Blockchain**[16]**.

Πλέον υπάρχουν πολλά άλλα πρωτόκολλα στην αγορά όπως τα Hyperledger, Corda, και άλλα. Το **Hyperledger**, είναι μια ανοιχτή πηγή και συνεργατική προσπάθεια υπό την ηγεσία του Linux Foundation® και της IBM, που περιλαμβάνει πλαίσια με ποικίλες περιπλοκές ώστε να επιτρέπονται συναλλαγές με κεντρικό άξονα. Περιέχει ένα μεγάλο αριθμό από διαφορετικά frameworks και εργαλεία τα οποία βοηθούν στην ανάπτυξη συγκεκριμένων και διαφορετικών blockchain ανά εφαρμογή.

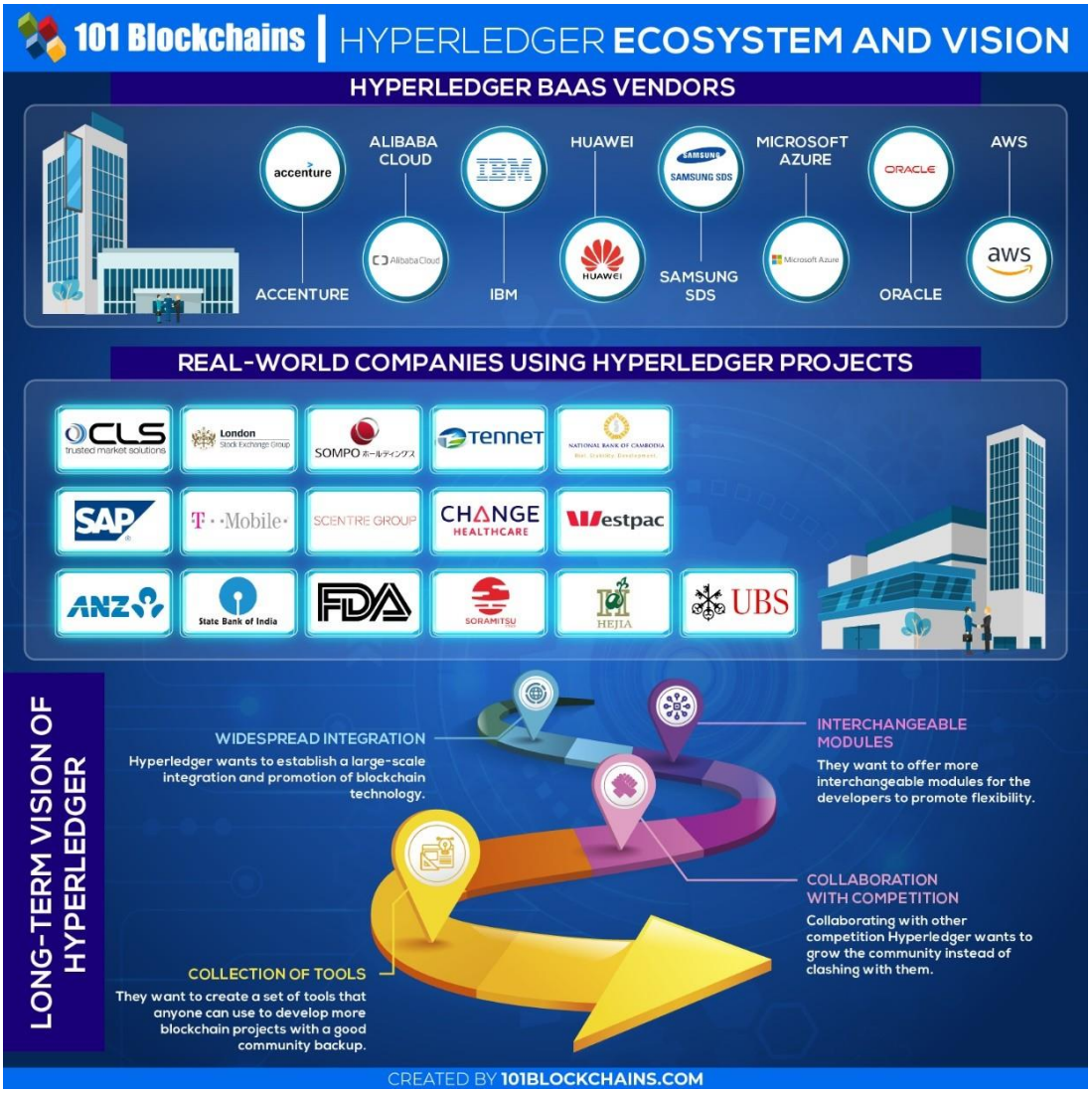
Το **Hyperledger** περιλαμβάνει τα εξής λογισμικά συναίνεσης Fabric, Sawtooth, Iroha, Burrow και Indy7. Το **Fabric** είναι το πιο ενεργό έργο του Hyperledger μέχρι σήμερα και το ξεκίνησε η IBM. Αποτελεί θεμέλιο για την ανάπτυξη εφαρμογών λογισμικού κατανεμημένων σε blockchain με αρθρωτή αρχιτεκτονική. Επιτρέπει τα εργαλεία, όπως η συναίνεση και οι υπηρεσίες προσχώρησης, να είναι **plug-and-play** (τοποθέτησης και άμεσης λειτουργίας) [17]. Ο πυρήνας της πλατφόρμας είναι γραμμένος στη γλώσσα προγραμματισμού Go. Ένα μοναδικό χαρακτηριστικό του Fabric είναι ότι η κατανεμημένη βιβλιοθήκη και η έξυπνη πλατφόρμα συμβολαίου επιτρέπουν ιδιωτικά κανάλια. Το έργο **Sawtooth** προήλθε αρχικά από την Intel.

Περιλαμβάνει έναν νέο συναινετικό αλγόριθμο που ονομάζεται απόδειξη εξαντλημένου χρόνου (Proof of Elapsed Time) [13]. Η συναίνεση όλων των μπλοκ που περιλαμβάνουν οι αλυσίδες έχει σημαντικό ρόλο στην περίπτωση αυτή.Γενικά, είναι η τεχνική με την οποία οι νέες πληροφορίες εξετάζονται και επιβεβαιώνονται πριν γίνουν δεκτές ως η επόμενη εγγραφή στο μητρώο. Το λογισμικό συναίνεσης Sawtooth στοχεύει σε μεγάλους κατανεμημένους πληθυσμούς επικύρωσης με ελάχιστη κατανάλωση πόρων.

Το λογισμικό συναίνεσης **Indy** προήλθε αρχικά από τη μη κερδοσκοπική ομάδα του Ιδρύματος Sovrin. Το Hyperledger Indy είναι μια κατανεμημένη βιβλιοθήκη, σχεδιασμένη για τη δημιουργία της αποκεντρωμένης ταυτότητας. Η κεντρική ιδέα του έργου αυτού, είναι η δημιουργία ψηφιακών ταυτοτήτων στα άτομα, με την δυνατότητα να μπορούν να την μοιραστούν όταν το επιθυμούν. Έτσι, οι εταιρείες δεν χρειάζεται να αποθηκεύουν όλο τον όγκο των προσωπικών δεδομένων αφού μπορούν να αποθηκεύσουν ένα δείκτη στην ταυτότητα. Το λογισμικό blockchain της Indy βασίζεται στην ελαχιστοποίηση των δεδομένων. Παρέχει εργαλεία, βιβλιοθήκες και επαναχρησιμοποιήσιμα στοιχεία για τη δημιουργία και χρήση ανεξάρτητων ψηφιακών ταυτοτήτων που υπάρχουν στα blockchains, έτσι ώστε να είναι διαλειτουργικά μεταξύ διαχειριστικών τομέων, εφαρμογών και οποιουδήποτε άλλου. Επειδή οι κατανεμημένοι λογαριασμοί δεν μπορούν να τροποποιηθούν ύστερα από την καταγραφή του συμβάντος, είναι σημαντικό οι περιπτώσεις χρήσης για ταυτότητα βασισμένη στο μητρώο να εξετάζουν προσεκτικά τα θεμελιώδη συστατικά, συμπεριλαμβανομένης της απόδοσης, της κλίμακας, του μοντέλου εμπιστοσύνης και της ιδιωτικότητας. Ειδικότερα, οι τεχνολογίες προστασίας της ιδιωτικής ζωής είναι εξαιρετικά σημαντικές για ένα δημόσιο μητρώο ταυτότητας, όπου η συσχέτιση μπορεί να γίνει σε παγκόσμια κλίμακα. Για όλους αυτούς τους λόγους, το Hyperledger Indy έχει αναπτύξει προδιαγραφές, ορολογία και πρότυπα σχεδίασης για αποκεντρωμένη ταυτότητα μαζί με την εφαρμογή αυτών των εννοιών που μπορούν να αξιοποιηθούν και να καταναλωθούν τόσο εντός όσο και εκτός της Consortium Hyperledger[18]. Η τεχνολογία **Burrow** περιλαμβάνει έναν εξουσιοδοτημένο, έξυπνο συμβόλαιο διερμηνέα ενσωματωμένο εν μέρει στις προδιαγραφές της εικονικής μηχανής Ethereum[19]. Η πλατφόρμα Ethereum χρησιμοποιείται τόσο για κρυπτογράφηση όσο και για έξυπνες συμβάσεις. Είναι γραμμένο με τη γλώσσα προγραμματισμού Solidity. Στο πλαίσιο του προγράμματος Burrow, το EVM είναι ο διερμηνέας για έξυπνα συμβόλαια (που δεν σχετίζονται με την κρυπτογράφηση) που διατρέχουν το δίκτυο Ethereum. Πολλές γνωστές εταιρείες ανήκουν στην Enterprise Ethereum Alliance, συμπεριλαμβανομένων των JPMorgan, της Microsoft, της Accenture, της BP και της Cisco. Τέλος, το λογισμικό συναίνεσης **Iroha** είναι ένα κομμάτι από μια απόκλιση μέσα στο Hyperledger. Προέρχεται από μερικούς προγραμματιστές στην Ιαπωνία που είχαν κατασκευάσει τη δική τους τεχνολογία blockchain για μερικές περιπτώσεις κινητής χρήσης. Εφαρμόζει ως γλώσσα προγραμματισμού τη C ++, η οποία μπορεί να έχει πιο υψηλή απόδοση για μικρά δεδομένα και επικεντρωμένες περιπτώσεις χρήσης[20].

Η ιδιωτική άδεια blockchain χρησιμοποιεί αλφαριθμητικό κώδικα που μπορεί να επιτρέψει την αυτοματοποίηση στις διαδικασίες της αλυσίδας εφοδιασμού με προκαθορισμένη αναφορά. Για παράδειγμα, επειδή το Hyperledger Fabric είναι μια ιδιωτική άδεια blockchain, επιτρέπει μόνο στους συμμετέχοντες με άδεια πρόσβασης να είναι μέρος του οικοσυστήματος. Ο υποκείμενος αλγόριθμος συναίνεσης, παρέχει διαφάνεια και συγκεκριμένο τρόπο λειτουργίας για όλα τα μέλη του συστήματος

blockchain ενώ απορρίπτει κακόβουλα και μη συνυφασμένα με τους κανόνες μέλη . Εντός του πλαισίου της περίπτωσης χρήσης δεδομένων ασθενούς, μια αλυσιδωτή άδεια θα επέτρεπε την κατάλληλη ανταλλαγή δεδομένων και την εφαρμογή των συμμετεχόντων κόμβων σε όλα τα νοσοκομεία. Λόγω διαφόρων νομικών διατάξεων εντός των ΗΠΑ και της ΕΕ (Γενικός Κανονισμός Προστασίας Δεδομένων - GDPR), τα δεδομένα δεν θα ήταν εύκολα διαθέσιμα. Το Hyperledger θα μπορούσε να είναι ένα δίκτυο εσωτερικών κόμβων που παρέχουν περισσότερα δεδομένα καθώς και την ασφάλεια και την προστασία από επιθέσεις ransomware σε σύγκριση με τα συστήματα επιχειρήσεων. Το ransomware είναι ένα είδος κακόβουλου λογισμικού που απειλεί να δημοσιοποιήσει τα προσωπικά δεδομένα του θύματος ή να διακόψει την πρόσβασή του θύματος σε αυτά, μέχρι να δοθούν λύτρα από το θύμα. Ωστόσο, αυτό το πρωτόκολλο δεν θα ήταν ευνοϊκό για το μοντέλο ανταλλαγής δεδομένων καθότι δεν παρέχει ούτε το υποκείμενο νόμισμα.



Εικόνα 5. Το οικοσύστημα Hyperledger **[21]**.

Η **Corda** είναι παρόμοια με τη πλατφόρμα hyperledger, η Corda σκοπεύει να φτιάξει ένα framework, το οποίο θα στοχεύει στη λειτουργία των επιχειρήσεων και πιο συγκεκριμένα στη διατήρηση κοινών ιστορικών για τις λειτουργίες των εταιριών. Έτσι αυξάνεται η εμπιστοσύνη ανάμεσα στις επιχειρήσεις και διευκολύνεται ο έλεγχος των συναλλαγών. Η Corda είναι μια πλατφόρμα ανοιχτού κώδικα επιχειρησιακού, οικονομικού χαρακτήρα που επιτρέπει την πραγματοποίηση συναλλαγών άμεσα και με απόλυτη προστασία της ιδιωτικής ζωής χρησιμοποιώντας έξυπνες συμβάσεις, μειώνοντας το κόστος συναλλαγών και εξορθολογίζοντας τις επιχειρήσεις [22]. Σε έναν κόσμο χωρίς πλατφόρμες blockchain, όπου όλα τα δεδομένα μοιράζονται με όλα τα μέρη, το αυστηρό μοντέλο προστασίας της ιδιωτικής ζωής της Corda επιτρέπει στις επιχειρήσεις να πραγματοποιούν συναλλαγές χωρίς προβλήματα. Η Corda R3 είναι blockchain που παρέχει δύο διαλειτουργικές και πλήρως συμβατές διανομές της πλατφόρμας Corda, μια δωρεάν λήψη βασισμένη στον κώδικα που διατίθεται στις GitHub και Corda Enterprise, μια εμπορική έκδοση που προσφέρει δυνατότητες και υπηρεσίες προσαρμοσμένες στις σύγχρονες επιχειρήσεις.

1.1.5 Ερευνητικό ενδιαφέρον της τεχνολογία του blockchain.

Η τεχνολογία του blockchain παρουσιάζει μεγάλο ενδιαφέρον εξαιτίας των κρυπτογραφικών αλγορίθμων, των δομών δεδομένων και άλλων στοιχείων που εμπεριέχει και επιτυγχάνονται τεχνικές βελτιώσεις. Πολλές από αυτές τις τεχνολογίες εξελίσσονται και βελτιώνονται καθημερινά. Επίσης ανάλογα με τη συγκεκριμένη χρήση του κάθε blockchain, προσαρμόζονται οι αλγόριθμοι, παρόλο που μεμονωμένες οι αλλαγές μπορεί να μην είναι ευδιάκριτες (δεδομένου ότι αλλάζει ο σκοπός), μπορούν να αλλάξουν δραματικά την αποδοτικότητα του συστήματος. Γενικότερα, οι βελτιώσεις είναι χρήσιμες, όμως συνήθως είναι μικρές και δεν αλλάζουν σημαντικά τις δυνατότητες της τεχνολογίας.

Ένα πεδίο που φαίνεται ότι δύναται να δημιουργήσει νέες δυνατότητες στην τεχνολογία των blockchain είναι οι δυνατότητες κλιμάκωσης. Η αποθήκευση, η αποδοτικότητα δικτύου, η ποσότητα δεδομένων που στέλνονται και οι αλγόριθμοι ομοφωνίας καταναλώνουν πολλούς πόρους σε δίκτυα με πολλούς κόμβους. Σε μικρότερες υλοποιήσεις δεν αποτελούν πρόβλημα αλλά με την πρόσθεση νέων κόμβων, οι πόροι που χρησιμοποιούνται αυξάνονται εκθετικά, με αποτέλεσμα να δημιουργούνται δυσκολίες. Επίσης ένα άλλο πρόβλημα που δημιουργείται λόγω της αδύναμης κλιμάκωσης είναι αυξημένοι χρόνοι απόκρισης του συστήματος, με αποτέλεσμα, εφαρμογές που απαιτούν χρονικά ευαίσθητες λειτουργίες να μην μπορούν να λειτουργήσουν σωστά. Κάποιες λύσεις που ήδη υπάρχουν και προσπαθούν να λύσουν τα θέματα αυτά είναι το Lightning Network και το Universal Payment channels.

Άλλες ερευνητικές προσεγγίσεις σκοπεύουν να αλλάξουν ριζικά και να εξελίξουν την λειτουργία του blockchain, μετατρέποντας τον τρόπο που αλληλεπιδρούν οι χρήστες με εκείνο και τις λειτουργίες που προσφέρει. Ένα τέτοιο πεδίο προσέγγισης είναι τα δικαιώματα πρόσβασης Αυτό συμβαίνει διότι περιορίζοντας τα **δικαιώματα πρόσβασης** σε ένα δίκτυο blockchain, ή περιορίζοντας τον αριθμό των χρηστών που μπορούν να προσθέσουν δεδομένα δημιουργήθηκαν νέοι τύποι blockchain, ανοιχτοί ή κλειστοί, με δικαιώματα ή χωρίς. Ακόμη ένα πεδίο ενασχόλησης είναι η **ιδιωτικότητα** όπου απλές λύσεις όπως τα ιδιωτικά blockchain, αν και διασφαλίζουν

την ιδιωτικότητα των δεδομένων, δεν υπόσχονται στους χρήστες την ακεραιότητα των δεδομένων τους. Σε άλλες περιπτώσεις, υπάρχουν επιπλέον πρωτόκολλα που διασφαλίζουν την ιδιωτικότητα και εφαρμόζονται στην ήδη υπάρχουσα αρχιτεκτονική, όπως αποδείξεις μηδενικής γνώσης (**Zero Knowledge Proof**) που επιτρέπουν την απόδειξη της ακεραιότητας κάποιων δεδομένων χωρίς τη γνώση των ιδίων των δεδομένων τους[23]. Μια κύρια λειτουργία του blockchain είναι η **δυνατότητα συμφωνίας των κόμβων** σε ένα κοινό ιστορικό συναλλαγών που επιτυγχάνεται με τους αλγόριθμους ομοφωνίας. Ο πιο διαδεδομένος είναι ο proof-of-work, ο οποίος αν και δουλεύει ικανοποιητικά σε μικρά δίκτυα, με την πάροδο του χρόνου και τους αυξημένους χρήστες γίνεται λιγότερο αποδοτικός, τόσο χρονικά όσο και χρηματικά. Επίσης δημιουργούνται προβλήματα όπου ένας μόνο χρήστης ή ομάδα χρηστών μπορούν να επηρεάσουν όλο το δίκτυο. Νέοι αλγόριθμοι όπως οι proof-of-stake ή proof-of-stake-velocity προσφέρουν παρόμοια πλεονεκτήματα χωρίς κάποια από τα μειονεκτήματα του proofofwork. Η δημιουργία νέων αλγορίθμων είναι δύσκολη γιατί ακόμα κι ένα μικρό λάθος στη λογική μπορεί να καταστρέψει όλο το σύστημα[6].

Ένα πεδίο που απασχολεί είναι ο τρόπος που γίνονται οι **συναλλαγές**. Για την ολοκλήρωση μιας συναλλαγής δεν χρησιμοποιούνται απλά δεδομένα αλλά έξυπνες συμβάσεις , οι οποίες περιέχουν όλα τα δεδομένα μιας συναλλαγής σε μορφή αντιλήψιμη για ένα blockchain. Με αυτό τον τρόπο δημιουργούνται πολλές καινούριες υλοποιήσεις και αποσαφηνίζονται οι δυνατότητες του blockchain. Για να καθοριστεί ο ιδιοκτήτης σε κάθε περίοδο εκτός από την παρακολούθηση των δεδομένων, απαιτείται η παρακολούθηση όλου του ιστορικού των συναλλαγών (**Inventorydata**), το οποίο με τη βοήθεια των smartcontracts, δείχνει τον ιδιοκτήτη τους[24]. Τέλος οι **δομές δεδομένων** παρουσιάζουν ενδιαφέρον καθώς δεν αποθηκεύουν σειριακά τα δεδομένα αλλά σε μορφή δέντρου με πολλά διαφορετικά κλαδιά. Το πρόβλημα είναι ότι οι κόμβοι δεν μπορούν σταθερά να επιλέξουν το ίδιο κλαδί ως το κύριο.

2.

2.1. Αρχιτεκτονική του Blockchain.

Η εσωτερική λειτουργία ενός blockchain περιλαμβάνει **λογική ιδιοκτησίας**. Αυτό σημαίνει ότι ελέγχεται ο τρόπος με τον οποίο μια ιδιοκτησία ορίζεται και διανέμεται στο σύστημα. Η καταγραφή των συναλλαγών στο σύστημα γίνεται ξεχωριστά και αξιοποιείται για τον καθορισμό της ιδιοκτησίας. Για να μπορεί να εφαρμοστεί η λειτουργία αυτή, χρησιμοποιείται η **λογική αποθήκευσης,** η οποία είναι υπεύθυνη για τη διατήρηση του ιστορικού των συναλλαγών και την προστασία τους από κακόβουλες κινήσεις. Η λογική αποθήκευσης ουσιαστικά εγγυάται ότι η ιδιοκτησία δεν θα αλλοιωθεί από λάθη ή επιθέσεις. Αυτό το καταφέρνει διατηρώντας μια δομή που επιτρέπει μόνο την πρόσθεση νέων πληροφοριών και όχι την μετατροπή ή την αφαίρεσή τους, και υλοποιείται με κρυπτογραφικούς αλγόριθμους και τεχνικές.

Ακόμη, για την ασφάλεια και την εγκυρότητα των συναλλαγών στηρίζεται στην **λογική επεξεργασίας συναλλαγών** και στη **λογική ομοφωνίας,** οι οποίες είναι υπεύθυνες για την ασφαλή ολοκλήρωση των συναλλαγών. Η **λογική επεξεργασίας των συναλλαγών** επιβλέπει την διαδικασία με την οποία υλοποιούνται οι συναλλαγές, ελέγχει την εγκυρότητα των δεδομένων και τα προσθέτει στο ιστορικό των συναλλαγών. Το ενδεχόμενο πρόσθεσης ενός κόμβου εξαιτίας κάποιου λάθους ή μίας κακόβουλης προσπάθειας δύναται να προσθέσει ψεύτικα ή λανθασμένα δεδομένα, γεγονός που απειλεί την ακεραιότητα του συστήματος. Για να αποφευχθεί αυτό, η λογική επεξεργασίας συναλλαγών βασίζεται σε πολύπλοκους αλγορίθμους peertopeer επικοινωνίας, οι οποίοι επιβεβαιώνουν τα δεδομένα επικοινωνίας ανάμεσα στους κόμβους. Επίσης χρησιμοποιούνται αλγόριθμοι, όπως η απόδειξη εργασίας(PoW). Εφόσον όλοι οι κόμβοι διατηρούν το ιστορικό των συναλλαγών ανεξάρτητα από τους υπόλοιπους, το περιεχόμενό τους μπορεί να διαφέρει ελαφρώς λόγω καθυστερήσεων ή άλλων δύσκολων καταστάσεων μέσα στο σύστημα. Έτσι μπορούμε να καταλήξουμε με παραπάνω μορφές της "πραγματικότητας". Η λειτουργία της **λογικής ομοφωνίας** όμως, μπορεί να βεβαιώνει τελικά ότι κάθε κόμβος θα έχει πανομοιότυπα δεδομένα, επιλέγοντας την έκδοση της "πραγματικότητας" των δεδομένων που αντικατοπτρίζουν την περισσότερη συλλογική δουλεια.

Η **ασφάλεια συναλλαγών** επιτρέπει μόνο στον πραγματικό ιδιοκτήτη να έχει πρόσβαση και να διαχειρίζεται τους πόρους (assets) του. Η λειτουργία της βασίζεται σε κρυπτογραφικές τεχνικές και αλγόριθμους, όπως η ασύμμετρη κρυπτογραφία και οι ψηφιακές υπογραφές

Η **αρχιτεκτονική peer-to-peer** χρησιμοποιείται στην τεχνολογία blockchain και περιγράφει πως οι διάφοροι κόμβοι του συστήματος συνδέονται μεταξύ τους. Κάθε

κόμβος δουλεύει ανεξάρτητα από τους υπόλοιπους και ο καθένας διατηρεί ένα δικό του αντίγραφο των δεδομένων του blockchain. Το πρωτόκολλο που χρησιμοποιούν για την επικοινωνία, βεβαιώνει ότι τελικά ο κάθε κόμβος θα ενημερωθεί για τις αλλαγές που γίνονται στο σύστημα.

Υπάρχει η πλήρως κατανεμημένη peer-to-peer αρχιτεκτονική που αποτελεί τη βάση του συστήματος και επιτρέπει την επικοινωνία ανάμεσα στους ανεξάρτητους κόμβους. Υπάρχει η σειρά τεχνολογιών Blockchain η οποία περιλαμβάνει τη λογική αποθήκευσης, τη λογική ομοφωνίας και τη κρυπτογραφία που δεν σχετίζονται με το σκοπό της εφαρμογής, οπότε μπορούν να χρησιμοποιηθούν κοινά σε όλες τις εφαρμογές με τον ίδιο ακριβώς τρόπο. Τέλος, υπάρχουν τα υπόλοιπα συστατικά, όπως η λογική ιδιοκτησίας και η λογική επικύρωσης συναλλαγών που είναι στενά συνδεδεμένα με τον σκοπό της εκάστοτε εφαρμογής και πρέπει να προσαρμόζονται αναλόγως.

Εικόνα 6. Σχημα ολοκληρωμένης εφαρμογής σε blockchain.

2.2. Τεχνολογία του Blockchain.

Το Blockchain είναι ένας συγκεκριμένος τύπος ή υποσύνολο της τεχνολογίας κατανεμημένου καθολικού (DLT). Το DLT είναι ο τρόπος καταγραφής και ανταλλαγής πληροφοριών σε πολλαπλά « καταστήματα » δεδομένων, όπου το καθένα περιέχει πανομοιότυπα αρχεία δεδομένων τα οποία ελέγχονται από ένα κατανεμημένο δίκτυο διακομιστών υπολογιστών, που ονομάζονται κόμβοι [6]. Το Blockchain είναι ένας μηχανισμός που χρησιμοποιεί την μέθοδο κρυπτογράφησης γνωστή ως **κρυπτογραφία** και χρησιμοποιεί μαθηματικούς αλγορίθμους για τη δημιουργία και επαλήθευση μιας συνεχώς **αυξανόμενης δομής δεδομένων**. Στη δομή αυτή μπορούν μόνο να προστεθούν δεδομένα αλλά δεν γίνεται να καταργηθούν τα ήδη υπάρχοντα, έτσι δημιουργείται η μορφή μιας αλυσίδας "μπλοκ συναλλαγών", η οποία λειτουργεί ως διανεμημένος λογαριασμός. Εάν κάποια από τις συναλλαγές σε ένα μπλοκ

μεταβληθεί ελαφρώς, η αντίστοιχη έξοδος εξαγωγής θα αλλάξει δραστικά, πράγμα που θα σπάσει την αλυσίδα στο επόμενα μπλοκ στον blockchain. Επομένως, οποιαδήποτε μεταβολή στο περιεχόμενο ενός μπλοκ στο blockchain ανιχνεύεται εύκολα στο δίκτυο. Για το λόγο αυτό, μόλις μια συναλλαγή προστεθεί σε ένα blockchain, η συναλλαγή αυτή δεν μπορεί να μεταβληθεί ή να ακυρωθεί. Έτσι, πληροφορίες στο blockchain λέγεται ότι είναι αμετάβλητες. Η μετατόπιση είναι μια σημαντική ιδιότητα του blockchain η οποία εξασφαλίζει ότι τα αρχεία, όταν δημιουργηθούν, δεν μπορούν να ανακληθούν ή να τροποποιηθούν.

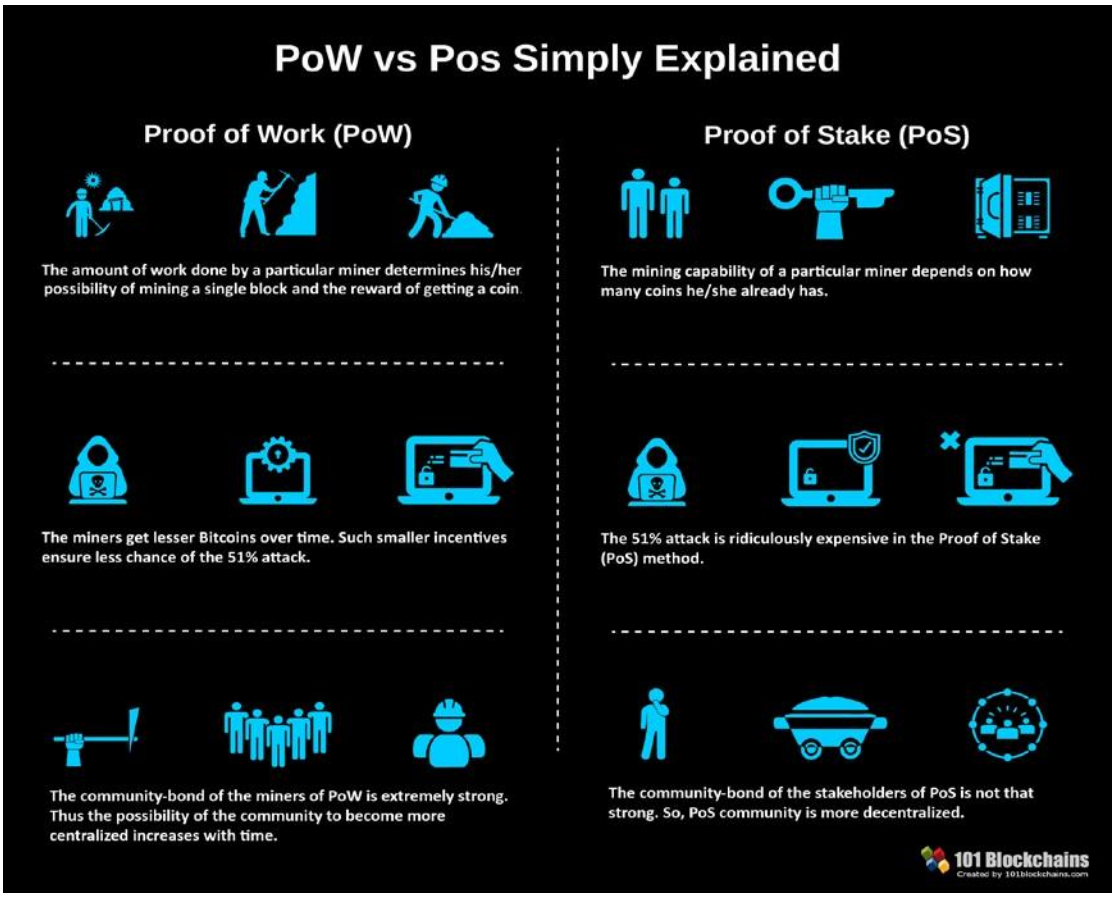
Το blockchain μπορεί να θεωρηθεί ως κατανεμημένη βάση δεδομένων όπου οι προσθήκες ξεκινούν από ένα μέλος (δηλ. έναν από τους κόμβους του δικτύου), ο οποίος δημιουργεί ένα νέο "μπλοκ" που μπορεί να περιέχει κάθε είδους πληροφορία. Αυτό το νέο μπλοκ μεταδίδεται στη συνέχεια σε όλα τα μέρη του δικτύου με κρυπτογραφημένη μορφή έτσι ώστε οι λεπτομέρειες της συναλλαγής να μην δημοσιοποιούνται. Όλοι οι κόμβοι του δικτύου (δηλαδή όλοι οι συμμετέχοντες στο δίκτυο) ορίζουν συλλογικά την ισχύ των μπλοκ σύμφωνα με μια προκαθορισμένη μέθοδο αλγοριθμικής επικύρωσης, κοινώς αναφερόμενη ως "Μηχανισμός συναίνεσης". Μόλις επικυρωθεί, το νέο "μπλοκ" προστίθεται στο blockchain, το οποίο ουσιαστικά οδηγεί σε ενημέρωση του μητρώου συναλλαγών που διανέμεται σε όλο το δίκτυο. Ο μηχανισμός αυτός μπορεί να χρησιμοποιηθεί για οποιαδήποτε συναλλαγή αξίας και δύναται να εφαρμοστεί σε οποιαδήποτε στοιχείο μπορεί να μετατραπεί σε ψηφιακή μορφή. Τα "μπλοκ" συναλλαγών υπογράφονται με ψηφιακή υπογραφή χρησιμοποιώντας ιδιωτικό κλειδί. Κάθε χρήστης στο δίκτυο blockchain έχει ένα ιδιωτικό κλειδί, το οποίο χρησιμοποιείται ως ψηφιακή υπογραφή σε μια συναλλαγή κι ένα δημόσιο κλειδί, το οποίο είναι γνωστό σε όλους στο δίκτυο. Το δημόσιο κλειδί χρησιμεύει ως διεύθυνση στο δίκτυο blockchain. και ως επαλήθευση της ψηφιακής υπογραφής / επικύρωσης της ταυτότητας του αποστολέα.

Ο οποιοσδήποτε κόμβος σε ένα δίκτυο μπορεί να προτείνει την προσθήκη νέων πληροφοριών στο blockchain. Για να επιβεβαιωθεί ότι η προσθήκη πληροφοριών είναι νόμιμη, οι κόμβοι πρέπει να φτάσουν σε κάποια μορφή συμφωνίας. Ο μηχανισμός συναίνεσης είναι μια προκαθορισμένη, συγκεκριμένη (κρυπτογραφική) μέθοδος επαλήθευσης που εξασφαλίζει τη σωστή ανάλυση της αλληλουχίας των συναλλαγών στο blockchain. Στην περίπτωση των κρυπτονομισμάτων, η αλληλουχία απαιτείται για την αντιμετώπιση του ζητήματος της "διπλής δαπάνης" όπου μεταφέρονται περισσότερες από μία φορές εάν οι μεταφορές δεν καταχωρούνται και ελέγχονται κεντρικά[25]. Ένας **μηχανισμός συναίνεσης** μπορεί να δομηθεί με διάφορους τρόπους. Οι δύο πιο γνωστοί - στο πλαίσιο των κρυπτονομισμάτων είναι ο **μηχανισμός της απόδειξης εργασίας (PoW) και της απόδειξης συμμετοχής (PoS).**

Σε ένα σύστημα **PoW**, οι συμμετέχοντες στο δίκτυο πρέπει να επιλύσουν τα αποκαλούμενα "κρυπτογραφικά παζλ" για να προσθέσουν νέα "μπλοκ" στο blockchain. Αυτή η διαδικασία επίλυσης παζλ αναφέρεται συνήθως ως "**εξόρυξη**"[6]. Τα κρυπτογραφικά παζλ αποτελούνται από όλες τις προηγούμενες πληροφορίες που καταγράφονται στο blockchain και ένα νέο σύνολο συναλλαγών που θα προστεθούν στο επόμενο μπλοκ [9]. Η είσοδος κάθε παζλ γίνεται μεγαλύτερη με την πάροδο του χρόνου (με αποτέλεσμα πιο περίπλοκο υπολογισμό), ο PoW μηχανισμός απαιτεί τεράστιο όγκο υπολογιστικών πόρων, οι οποίοι καταναλώνουν σημαντικό ποσό

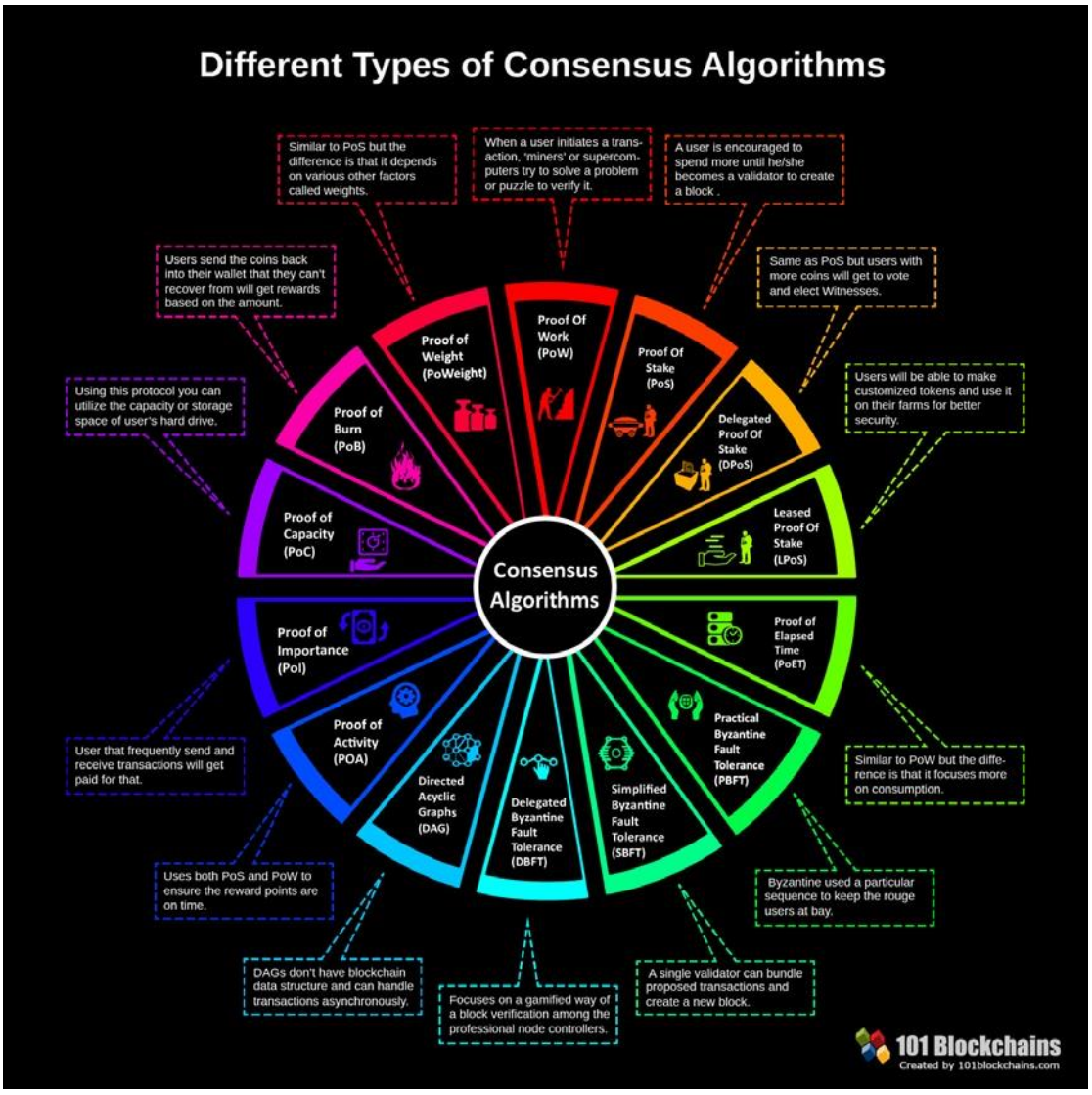
ηλεκτρικής ενέργειας [26]. Εάν ένας συμμετέχων στο δίκτυο (δηλαδή ένας κόμβος) επιλύσει ένα κρυπτογραφικό παζλ, αποδεικνύει ότι έχει ολοκληρώσει το έργο, και ανταμείβεται με ψηφιακή μορφή αξίας (ή στην περίπτωση κρυπτογράφησης, με μια νέα εξόρυξη νομίσματος). Αυτή η ανταμοιβή χρησιμεύει ως κίνητρο για την υποστήριξη του δικτύου [27]. Η Bitcoin κρυπτογράφηση βασίζεται σε μηχανισμό συναίνεσης PoW. Άλλα παραδείγματα περιλαμβάνουν τα Litecoin, Bitcoin Cash, Monero, κλπ.

Σε ένα σύστημα **PoS**, ένας επικυρωτής συναλλαγής (δηλ. Ένας κόμβος δικτύου) πρέπει να αποδείξει την ιδιοκτησία ενός συγκεκριμένου στοιχείου (ή στην περίπτωση κρυπτονομισμάτων, μια ορισμένη ποσότητα κερμάτων) προκειμένου να συμμετάσχει στην επικύρωση των συναλλαγών. Αυτή η πράξη επικύρωσης των συναλλαγών ονομάζεται "**σφυρηλάτηση**" [9] αντί για "εξόρυξη". Για παράδειγμα, στην περίπτωση κρυπτονομισμάτων, ένας επικυρωτής συναλλαγών θα πρέπει να αποδείξει το "ποντάρισμα" (share) όλων των υφιστάμενων κερμάτων που επιτρέπεται να επικυρώσουν μια συναλλαγή. Ανάλογα με το μέγεθος του ποσού που κατέχει, θα έχει περισσότερες πιθανότητες να είναι αυτός που θα επικυρώσει το επόμενο μπλοκ (μεγαλύτερη αρχαιότητα στο δίκτυο, που σημαίνει πιο αξιόπιστη θέση). Ο επικυρωτής συναλλαγών καταβάλλει τέλη συναλλαγής για τις υπηρεσίες επικύρωσής του από τα συμβαλλόμενα μέρη. Τα κρυπτονομίσματα όπως τα Neo και Ada (Cardano) χρησιμοποιούν ένα μηχανισμό συμφωνίας PoS [28].



Εικόνα 7. Μηχανισμοί συναίνεσης PoW και PoS**[29]**.

Εκτός από τους μηχανισμούς PoW και PoS υπάρχουν και άλλοι όπως η απόδειξη της διάρκειας του χρόνου (proof of elapsed time) και την απόδειξη της ικανότητας (proof of capacity). Ακόμα υπάρχουν οι αλγόριθμοι **επίτευξης συμφωνίας** όπου ο μηχανισμός αυτός συγκεντρώνει όλες τις συμφωνίες από την ομάδα στο μέγιστο δυνατό βαθμό. Υπάρχει ο μηχανισμός **συνεργασίας(1)** όπου κάθε μέλος στοχεύει σε μια καλύτερη συμφωνία που έχει ως αποτέλεσμα την προαγωγή των συμφερόντων της ομάδας στο σύνολό της και ο μηχανισμός **συνεργασίας(2)** όπου κάθε άτομο εργάζεται ως μέλος της ομάδας ανεξάρτητα από το προσωπικό του συμφέρον. Υπάρχουν μηχανισμοί για τη διασφάλιση **ίδιων δικαιωμάτων** όπου κάθε συμμετέχων έχει την ίδια αξία στην ψηφοφορία. Αυτό σημαίνει ότι η ψήφος κάθε ατόμου είναι σημαντική. Επιπρόσθετα, υπάρχει ο μηχανισμός **συμμετοχής** όπου όλοι στο εσωτερικό του δικτύου πρέπει να συμμετέχουν στην ψηφοφορία και δεν μπορεί κανείς να παραλειφθεί ή να απέχει χωρίς ψήφο. Τέλος, υπάρχει ο μηχανισμός **δραστηριότητα**ς που διασφαλίζει ότι κάθε μέλος της ομάδας είναι εξίσου ενεργό ,και ότι δεν υπάρχει κανείς με μεγαλύτερη ευθύνη στην ομάδα.



Εικόνα 8. Διαφορετικοί τύποι μηχανισμών συναίνεσης **[30]**.

2.2.1 Χρήσιμα χαρακτηριστικά της τεχνολογίαςBlockchain.

Το blockchain είναι μια κατανεμημένη βάση δεδομένων που χρησιμοποιεί αναπαραγωγή κρατικής μηχανής, με ατομικές αλλαγές στη βάση δεδομένων που αναφέρονται ως συναλλαγές ομαδοποιημένες σε μπλοκ. Η ακεραιότητα και η αντίσταση παραβίασης του αρχείου καταγραφής των συναλλαγών εξασφαλίζεται μέσω των συνδέσεων κατακερματισμού μεταξύ των μπλοκ. Η έννοια του blockchain εισήχθη για το Bitcoin στο πλαίσιο δημιουργίας ενός αποκεντρωμένου ηλεκτρονικού νομίσματος. Το blockchain θεωρείται αποκεντρωμένο, συντηρείται από μια πλειάδα ανεξάρτητων μερών (διατηρητές), με την υπόθεση ασφαλείας ότι ένα ορισμένο ποσοστό αυτών των μερών μπορεί να μην ανταποκρίνεται ή να τίθεται σε κίνδυνο οποιαδήποτε στιγμή κατά τη διάρκεια της λειτουργίας blockchain όπως η βυζαντινή ανοχή σφάλματος [31].

Το blockchain από το σχεδιασμό του καθιστά δυνατή την παροχή μιας επαληθεύσιμης απόδειξης ύπαρξης ή απουσίας ορισμένων δεδομένων ή μιας μεταβατικής κατάστασης στη βάση δεδομένων blockchain [32]. Τα μέτρα λογοδοσίας (π.χ. απόδειξη εργασίας [33]) θα μπορούσαν να καταστήσουν απαγορευτικά δαπανηρή τη δημιουργία τέτοιων αποδείξεων για οποιονδήποτε, συμπεριλαμβανομένων και των ίδιων των διαχειριστών. Τέτοιες αποδείξεις για μικρά κομμάτια αποθηκευμένων δεδομένων θα μπορούσαν να είναι συμπαγή και δεν χρειάζεται να αποκαλύπτουν άλλες πληροφορίες (μόνο μαθηματικά απρόσωπες πληροφορίες). Οι ρουτίνες εφαρμοσμένης κρυπτογραφίας (π.χ. ψηφιακές υπογραφές δημόσιου κλειδιού) χρησιμοποιούνται για την αποκέντρωση της εξακρίβωσης της ταυτότητας και της εξουσιοδότησης των συναλλαγών που πραγματοποιούνται εντός του δικτύου.

Οι χρήστες blockchain χωρίζονται συνήθως σε τρία μέρη ανάλογα με τους ρόλους τους.

1. **Οι συντηρητές της υποδομής** blockchain, οι οποίοι αποφασίζουν την επιχειρησιακή λογική στο blockchain. Οι συντηρητές αποθηκεύουν ολόκληρο το αντίγραφο ολόκληρου του μπλοκ αλφαριθμητικού κώδικα, έτσι έχουν πλήρη πρόσβαση στην ανάγνωση και αποφασίζουν για τους κανόνες επεξεργασίας συναλλαγών και είναι ενεργά συμμετέχοντες στον αλγόριθμο συναίνεσης στο blockchain, με άλλα λόγια έχουν πρόσβαση εγγραφής στο blockchain. Είναι σημαντικό ότι οι διαχειριστές δεσμεύονται με μια επίσημη ή ανεπίσημη σύμβαση με τους άλλους χρήστες σχετικά με την επιχειρησιακή λογική που κωδικοποιείται στο blockchain. Δηλαδή, οι διαχειριστές δεν μπορούν να καθορίσουν ή να αλλάξουν αυθαίρετα τους κανόνες επεξεργασίας συναλλαγών. Πράγματι, παρέχουν τα μέσα για τους εξωτερικούς χρήστες να ελέγξουν τη λειτουργία μπλοκ αλυσίδας για την αντιστοιχία αυτών των κανόνων.
2. **Οι Εξωτερικοί ελεγκτές** της επιχείρησης είναι οι ρυθμιστικές αρχές, οι μη κυβερνητικές οργανώσεις, οι αρχές επιβολής του νόμου, οι οποίοι επαληθεύουν την ορθότητα ολόκληρης της επεξεργασίας συναλλαγών σε πραγματικό χρόνο ή / και αναδρομικά. Οι ελεγκτές θεωρείται ότι

αποθηκεύουν αντίγραφα ολόκληρων μπλοκς δεδομένων, ή τουλάχιστον ένα λογικά πλήρες τμήμα τους, και εχουν τη δυνατότητα ανάγνωσης αυτού για να είναι σε θέση να εκτελέσουν πλήρη έλεγχο. Από τεχνική άποψη, οι ελεγκτές δεν συμμετέχουν ενεργά στη συναίνεση, αλλά κατά τα άλλα δρουν παρόμοια με τους διαχειριστές, διότι αντιγράφουν ολόκληρο το αρχείο καταγραφής συναλλαγών.

3. **Οι πελάτες** είναι οι τελικοί χρήστες των υπηρεσιών που παρέχονται από τους διαχειριστές. Κάθε πελάτης μπορεί να έχει πρόσβαση σε ένα σχετικά μικρό τμήμα δεδομένων blockchain, αλλά το λογισμικό του μπορεί να χρησιμοποιεί κρυπτογραφικές αποδείξεις για να επαληθεύει, με εύλογη ακρίβεια, την αυθεντικότητα των δεδομένων blockchain που παρέχονται από τους διαχειριστές και τους ελεγκτές.

Στο Bitcoin, οι υπεύθυνοι συντήρησης αντιστοιχούν σε λογισμικό εξόρυξης, οι ελεγκτές σε πλήρεις κόμβους μη εξόρυξης και οι πελάτες αντιστοιχούν σε λογισμικό διαχείρισης κλειδιού πελάτη. Με τη γενίκευση της ταξινόμησης δικτύου Bitcoin, θα αναφερθούν οι κόμβοι που έχουν πρόσβαση ανάγνωσης σε ολόκληρο το blockchain ως πλήρεις κόμβοι, οι οποίοι υποδιαιρούνται σε κόμβους επικύρωσης και κόμβους ελέγχου σύμφωνα με τους ρόλους που περιγράφονται παραπάνω.

Χρησιμοποιώντας μέτρα κρυπτογραφικής λογοδοσίας και ελέγχου, τα blockchains θα μπορούσαν να ελαχιστοποιήσουν την έλλειψη εμπιστοσύνης και τον συναφή κίνδυνο αντισυμβαλλομένου μεταξύ των συμμετεχόντων στο σύστημα.

2.3 Ορισμός Κρυπτονομισμάτων.

Η καθιέρωση ενός ορισμού των **κρυπτονομισμάτων (cryptocurrencies)** δεν είναι εύκολη υπόθεση. Μοιάζει πολύ με cryptocurrencies blockchain, που έχουν γίνει δημοφιλή σε ένα ευρύ φάσμα τεχνολογικών εξελίξεων και χρησιμοποιούν μια τεχνική γνωστή ως κρυπτογραφία .Η κρυπτογραφία είναι η τεχνική που προστατεύει τις πληροφορίες μετατρέποντάς τες σε μορφή μη αναγνώσιμη που μπορεί μόνο να αποκρυπτογραφηθεί από κάποιον που διαθέτει ένα μυστικό κλειδί [34]. Κρυπτονομίσματα όπως το Bitcoin, εξασφαλίζονται μέσω αυτής της τεχνικής κρυπτογραφίας χρησιμοποιώντας ένα έξυπνο σύστημα δημόσιων και ιδιωτικών ψηφιακών κλειδιών [35].Ο ορισμός των κρυπτονομισμάτων βασίζεται στη χάραξη πολιτικής σε ευρωπαϊκό και διεθνές επίπεδο. Οι υπεύθυνοι για τη χάραξη πολιτικής είναι η Ευρωπαϊκή Κεντρική Τράπεζα το Διεθνές Νομισματικό Ταμείο, τη Τράπεζα Διεθνών Διακανονισμών ,η Ευρωπαϊκή Αρχή Τραπεζών, η Ευρωπαϊκή Αρχή Κινητών Αξιών και Αγορών ,η Παγκόσμια Τράπεζα και η Ομάδα Χρηματοοικονομικής Δράσης από την εμφάνιση του Bitcoin το 2009[36], το θέμα των κρυπτονομισμάτων έχει εξεταστεί λεπτομερώς από διάφορους υπεύθυνους, οι οποίοι έχουν προσεγγίσει το θέμα με διαφορετικό τρόπο.

Η Ευρωπαϊκή Κεντρική Τράπεζα έχει ταξινομήσει τα κρυπτονομίσματα ως υποσύνολο **εικονικών νομισμάτων**. Σε μία έκθεση σχετικά με τα εικονικά νομίσματα του 2012, όρισε αυτά τα νομίσματα ως μορφή μη ελεγχόμενων ψηφιακών χρημάτων, τα οποία συνήθως εκδίδονται και ελέγχονται από τους προγραμματιστές. Τα ψηφιακά νομίσματα χρησιμοποιούνται και γίνονται αποδεκτά μεταξύ των μελών μιας συγκεκριμένης εικονικής κοινότητας[37]. Υπάρχουν **τρεις τύποι εικονικών**

νομισμάτων που μπορούν να διακριθούν ανάλογα με την αλληλεπίδραση τους με τα παραδοσιακά νομίσματα και την πραγματική οικονομία. Υπάρχουν τα εικονικά νομίσματα που μπορούν να χρησιμοποιηθούν μόνο **σε κλειστό εικονικό σύστημα**, συνήθως σε online παιχνίδια (π.χ. World of Warcraft Gold). Υπάρχουν επιπλέον τα εικονικά νομίσματα που συνδέονται **μονομερώς με την πραγματική οικονομία**, δηλαδή υπάρχει συντελεστής μετατροπής του νομίσματος (από παραδοσιακά χρήματα) και το αγορασμένο νόμισμα μπορεί να μεταφερθεί και στη συνέχεια να χρησιμοποιηθεί για την αγορά εικονικών αγαθών και υπηρεσιών (π.χ. Credits Facebook). Τέλος υπάρχουν τα εικονικά νομίσματα που είναι **διμερώς συνδεδεμένα με την πραγματική οικονομία** δηλαδή υπάρχουν ποσοστά μετατροπής τόσο για την αγορά εικονικού νομίσματος όσο και για την πώληση αυτού του νομίσματος. Το αγορασμένο νόμισμα μπορεί να χρησιμοποιηθούν για την αγορά τόσο των εικονικών όσο και των πραγματικών αγαθών και υπηρεσιών.

Τα κρυπτονομίσματα, όπως το Bitcoin, είναι εικονικά νομίσματα του τελευταίου τύπου, μπορούν δηλαδή να αγοραστούν με παραδοσιακά χρήματα όπως πωλούνται έναντι παραδοσιακών χρημάτων και μπορούν να χρησιμοποιηθούν για να αγοράσουν ψηφιακά και πραγματικά αγαθά και υπηρεσίες [38]. Σε μια πιο πρόσφατη έκθεση του 2015 με τίτλο «Σχέδια εικονικών νομισμάτων» έγινε μια περαιτέρω ανάλυση, που πρότεινε ένα "δεύτερο", και πιο ενημερωμένο ορισμό των εικονικών νομισμάτων. Ορίζει τα εικονικά νομίσματα ως **ψηφιακές παραστάσεις αξίας**, που δεν έχουν εκδοθεί από κεντρική τράπεζα, πιστωτικό ίδρυμα ή ίδρυμα ηλεκτρονικού χρήματος, τα οποία σε ορισμένες περιπτώσεις μπορεί να χρησιμοποιηθούν ως εναλλακτική λύση χρημάτων[7]. Ακόμα, διευκρίνισε ότι τα κρυπτονομίσματα, όπως το Bitcoin, αποτελούν ένα αποκεντρωμένο αμφίδρομο (δηλαδή διμερές) εικονικό νόμισμα.

Το Διεθνές Νομισματικό Ταμείο έχει κατηγοριοποιήσει τα κρυπτονομίσματα ως υποσύνολο εικονικών νομισμάτων, τα οποία ορίζει ως ψηφιακές αναπαραστάσεις αξίας, που εκδίδονται από ιδιώτες προγραμματιστές και εκφράζονται στη δική τους λογιστική μονάδα [39]. Σύμφωνα με το ΔΝΤ, η έννοια των εικονικών νομισμάτων καλύπτει μια ευρύτερη σειρά «νομισμάτων», που κυμαίνονται από απλά **IOUs** (Άτυπα πιστοποιητικά χρέους), **από εκδότες** (όπως κουπόνια μέσω Διαδικτύου ή κινητά και μίλια αεροπορικών εταιρειών), εικονικά νομίσματα που υποστηρίζονται από **περιουσιακά στοιχεία** όπως ο **χρυσός** και τα κρυπτονομίσματα όπως το **Bitcoin**.

Συμπερασματικά, το κρυπτονόμισμα είναι μια ψηφιακή αναπαράσταση τιμής που προορίζεται να αποτελέσει εναλλακτική λύση peer-to-peer (P2P) δικτύου του νόμιμου νομίσματος που εκδίδεται από το κράτος, και χρησιμοποιείται ως μέσο ανταλλαγής γενικού σκοπού (ανεξάρτητο από οποιοδήποτε κεντρική τράπεζα). Εξασφαλίζεται με μηχανισμό γνωστό ως κρυπτογραφία και μπορεί να μετατραπεί σε νόμιμη προσφορά και αντίστροφα . Τα κρυπτονομίσματα και τα blockchains έχουν κεντρίσει το ενδιαφέρον τα τελευταία χρόνια. Το blockchain είναι ένας τύπος κατανεμημένης τεχνολογίας χαρτονομισμάτων που διαμορφώνει τη ραχοκοκαλιά της κρυπτογραφικής αγοράς. Είναι η τεχνολογία πίσω από τη μεγάλη ποικιλία κρυπτονομισμάτων που κυκλοφορούν σήμερα. Το blockchain μπορεί να εφαρμοστεί σε διάφορους τομείς και μπορεί να έχει μια μεγάλη ποικιλία εφαρμογών.

2.3.1 Ορισμός κρυπτογραφικών μαρκών (token) και των cryptosecurities.

Ο όρος κρυπτονομίσματα χρησιμοποιείται λανθασμένα με πολύ ευρεία έννοια. [40] Για καλύτερη αποσαφήνιση πρέπει να διακριθεί από τις μάρκες (tokens) και τα cryptosecurities. Οι **κρυπτογραφικές "μάρκες"**, προσφέρουν πολλές λειτουργίες και δεν χρησιμοποιούνται μόνο ως μέσο ανταλλαγής γενικού σκοπού. Οι μάρκες εκδόθηκαν στο πλαίσιο μιας αρχικής προσφοράς ζεύγους[41] για την άντληση κεφαλαίων για ένα συγκεκριμένο έργο ή επιχείρηση. Αποτελούν μια νέα κατηγορία **κρυπτογραφικών περιουσιακών στοιχείων** (δηλαδή ψηφιακών στοιχείων που καταγράφονται σε κατανεμημένα τα οποία εξασφαλίζονται με την κρυπτογραφία [42]) που ενσωματώνουν κάποιο είδος αξίωσης και προκύπτουν από τη χρήση της blockchain τεχνολογίας. Ορισμένες μάρκες μοιάζουν με παραδοσιακά μέσα όπως μετοχές ή ομόλογα και αναφέρονται συνήθως ως **«μάρκες ασφαλείας»** ή **«επενδυτικές μάρκες»**. Άλλες μάρκες παρέχουν στους κατόχους (μελλοντική) πρόσβαση σε συγκεκριμένα προϊόντα ή υπηρεσίες και αναφέρονται συνήθως ως **"μάρκες χρησιμότητας".** Μπορούν να χρησιμοποιηθούν για να αποκτήσουν ορισμένα προϊόντα ή υπηρεσίες, αλλά δεν αποτελούν μέσο γενικού σκοπού ανταλλαγής, επειδή μπορούν να χρησιμοποιηθούν μόνο στην πλατφόρμα token[43].

Τα κρυπτονομίσματα πρέπει επίσης να διακριθούν από μια ιδέα που υπήρξε πρόσφατα και αναφέρονται ως **cryptosecurities**. Υποστηρίχθηκε ότι θα μπορούσε να χρησιμοποιηθεί η τεχνολογία blockchain για να χρησιμοποιηθούν για την εγγραφή, την έκδοση και τη μεταβίβαση τακτικών μετοχών και λοιπών εταιρικών χρεογράφων, ούτως ώστε η ο πίνακας κεφαλαιοποίησης μιας εταιρείας είναι πάντα ακριβής και ενημερωμένος [44]. Επειδή αυτή η διαδικασία εξασφαλίζεται με κρυπτογράφηση, έχει προταθεί η οριοθέτηση αυτών των τίτλων ως cryptosecurities. Η μόνη σύνδεση μεταξύ της νέας έννοιας cryptosecurities και των κρυπτονομισμάτων, είναι ότι και οι δύο χρησιμοποιούν την τεχνολογία blockchain.

2.4 Ορισμός συναρτήσεων κατακερματισμου(Hash Functions).

Ένα **hash** είναι ένα είδος "**υπογραφής**" για μια ροή δεδομένων που αναπαριστά περιεχόμενο. Μία συνάρτηση hash είναι μία μέθοδος **μετατροπής δεδομένων τυχαίου μεγέθους σε μία ψηφιακή αλφαριθμητική ακολουθία με προκαθορισμένο σταθερό μήκος.** Οι κρυπτογραφικές συναρτήσεις κατακερματισμού **(cryptographic hash functions)** είναι αυτές μέσω των οποίων είναι εύκολο να υπολογίζεται ένα hash αλλά δύσκολο (πρακτικά αδύνατον) να υπολογιστούν τα στοιχεία από τα οποία προέκυψε. Αυτές οι συναρτήσεις μετατρέπουν τα δεδομένα εισόδου με τόσο σύνθετο τρόπο ώστε πρακτικά ο αντίστροφος υπολογισμός να είναι αδύνατος. Οι πιο γνωστές κρυπτογραφικές συναρτήσεις είναι οι **MD4**,**MD5, SHA 1 και SHA 2**.

Όταν ένα hash τροφοδοτείται εκ νέου ως είσοδος σε μία συνάρτηση κατακερματισμού ,προκύπτει ένα νέο hash. Όταν αυτή η διαδικασία επαναλαμβάνεται και τα αποτελέσματά της συνδυάζονται σε μία ακολουθία, προκύπτει ένα **Hashchain**. Πολλά συστήματα Unix και Linux παρέχουν το πρόγραμμα md5sum, το οποίο διαβάζει μια ροή δεδομένων και παράγει έναν σταθερό αριθμό 128-bit που συνοψίζει τη ροή χρησιμοποιώντας τη δημοφιλή μέθοδο "MD5".

Οι ροές δεδομένων(streams of data) είναι αρχεία από τα οποία τα δύο είναι άμεσα ορατά, και το ένα είναι πολύ μεγάλο με αποτέλεσμα να μην μπορει να εμφανιστεί.

```
$ cat smallfile
$ cat bigfile
This is a larger file that contains more characters.
This demonstrates that no matter how big the input
stream is, the generated hash is the same size (but
of course, not the same value). If two files have
a different hash, they surely contain different data.

$ ls -l empty-file smallfile bigfile linux-kernel
-rw-rw-r--  1 steve steve       0 2008-04-20 08:58 empty-
file
-rw-rw-r--  1 steve steve      48 2008-04-20 08:48 smallfile
-rw-rw-r--  1 steve steve     260 2008-04-20 08:48 bigfile
-rw-r--r--  1 root  root  1122363 2003-02-27 07:12 linux-
kernel

$ md5sum empty-file smallfile bigfile linux-kernel
d41d8cd98f00b204e9800998ecf8427e  empty-file
75cdbfeb70a06d42210938da88c42991  smallfile
6e0b7a1676ec0279139b3f39bd65e41a  bigfile
c74c812e4d2839fa9acf0aa0c915e022  linux-kernel
```

Εικόνα 9.Οι ροές εισόδου παράγουν hashes του ίδιου μήκους **[45].**

Ακόμα και πολύ μικρές αλλαγές στην είσοδο αποδίδουν μεγάλες αλλαγές στην αξία του κατακερματισμού (**avalanche effect).** Στην κρυπτογραφία, το αποτέλεσμα του **avalanche effect** είναι η επιθυμητή ιδιότητα των κρυπτογραφικών αλγορίθμων, συνήθως σε μπλοκ με κρυφές κρυπτογραφικές λειτουργίες [46] και κρυπτογραφικούς κατακερματισμούς, όπου εάν μια είσοδος αλλάξει ελαφρώς (για παράδειγμα, αναστροφή ενός μόνο bit), η έξοδος αλλάζει σημαντικά (π.χ. τα bits εξόδου). Στην περίπτωση κρυπτογραφημάτων υψηλής ποιότητας, μια τέτοια μικρή αλλαγή είτε στο κλειδί είτε στο απλό κείμενο θα να προκαλέσει μια δραστική αλλαγή στο κρυπτοκείμενο .Το φαινόμενο avalanche μπορεί να φανεί καλύτερα με την απόκτηση δύο αρχείων με σχεδόν ταυτόσημο περιεχόμενο.

```
T -> 0x54 -> 0 1 0 1  0 1 0 0
t -> 0x74 -> 0 1 1 1  0 1 0 0
```

Εικόνα 10. Παράδειγμα αλλαγής του πρώτου χαρακτήρα ενός αρχείου από T σε t, όπου οι δυαδικές τιμές για αυτούς τους χαρακτήρες ASCII διαφέρουν μόνο κατά ένα bit **[47]**.

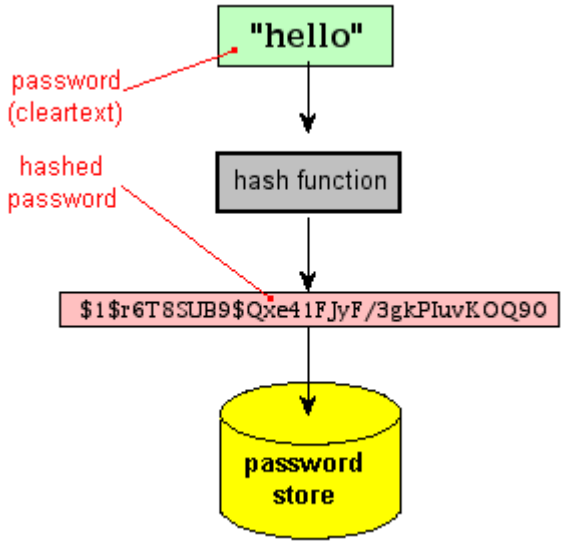
```
$ cat file1
This is a very smallfile with a few characters

$ cat file2
thisisaverysmallfilewitha few characters

$ md5sum file?
75cdbfeb70a06d42210938da88c42991 6  file1
fbe37f1eea0f802bd792ea885cd03e2  file2
```

Εικόνα 11. Η διαφορά ενός μόνο bit στην είσοδο, επιφέρει σημαντική διαφορά στο αποτέλεσμα της εξόδου ενός hash **[45]**.

Τα hashes ουσιαστικά είναι μια σύνοψη (digest) όχι κρυπτογράφηση. Η κρυπτογράφηση μετατρέπει τα δεδομένα από ένα αναγνώσιμο κείμενο σε ένα κωδικοποιημένο και αντίστροφα (με τα σωστά κλειδιά). Τα δύο κείμενα πρέπει να αντιστοιχούν κατά προσέγγιση σε μέγεθος δηλαδή όσο μεγαλύτερο είναι το αναγνώσιμο κείμενο τόσο μεγαλύτερο θα πρέπει να είναι και το κωδικοποιημένο

κείμενο που αποδίδει κ.ο.κ. . Η "κρυπτογράφηση" είναι μια αμφίδρομη λειτουργία Hashes. Αντίθετα τα hashes καταρτίζουν μια ροή δεδομένων σε μια σύνοψη (digest), και είναι αυστηρά μια λειτουργία μονής κατεύθυνσης. Επίσης, όλα τα hashes ίδιου τύπου έχουν το ίδιο μέγεθος ανεξάρτητα από το μέγεθος των εισροών[47].

Η κυριότερη χρήση ενός hash είναι η επαλήθευση της ακεραιότητας ενός αρχείου. Για παράδειγμα αν κάποιος κατεβάσει ένα κομμάτι λογισμικού από έναν ιστότοπο, για να γνωρίζει ότι δεν έχει παραβιαστεί, θα μπορούσε να ξανακατεβάσει το αρχείο για να συγκρίνει τα δυαδικά ψηφία του. Εάν τα ψηφία είναι διαφορετικά ,για να γίνει η εύρεση για τα ποια κομμάτια είναι έγκυρα, θα πρέπει να ξανακατεβάσει και να συγκρίνει πάλι τα ψηφία. Η διαδικασία αυτή είναι κουραστική και χρονοβόρα. Αντίθετα, εάν ο ιστότοπος δημοσιεύει τις τιμές κατακερματισμού των δεσμών λήψης, δύναται ο καθένας να τον ελέγξει.

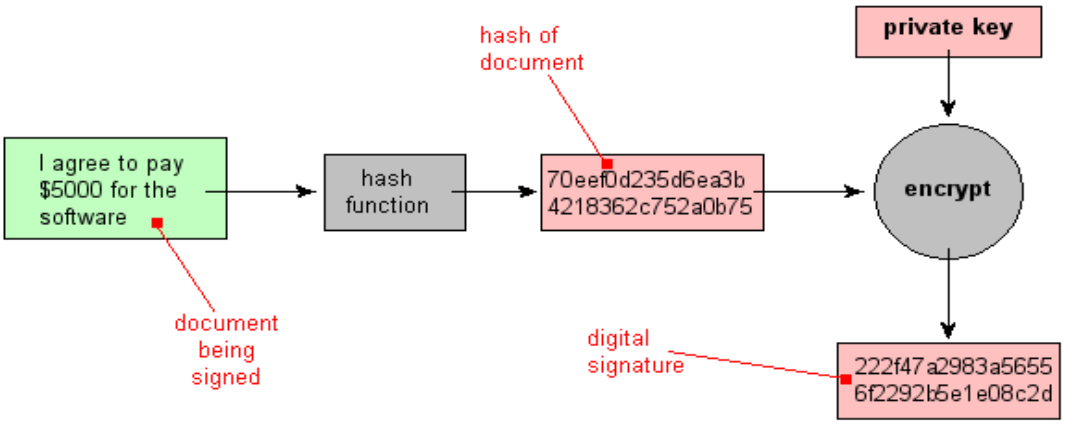


Εικόνα 12. Διαδικασία επαλήθευσης της ακεραιότητας ενός αρχείου **[45]**.

Μια ακόμη χρήση ενός hash είναι ο **κατακερματισμός των κωδικών πρόσβασης**. Η αποθήκευση των κωδικών πρόσβασης σε καθαρό κείμενο (στην αρχική τους μορφή) στα συστήματα ηλεκτρονικών υπολογιστών αντενδείκνυται , γιατί αν κάποιος μπορεί να φτάσει στο σημείο όπου αποθηκεύονται, μπορεί να εκμαιεύσει τους κωδικούς. Ένας πιο ασφαλής τρόπος είναι η αποθήκευση ενός hash του κωδικού πρόσβασης, αντί του ίδιου του κωδικού πρόσβασης. Δεδομένου ότι δεν είναι αντιστρέψιμο, δεν υπάρχει τρόπος για να βρεθεί "ποιος κωδικός πρόσβασης παρήγαγε το συγκεκριμένο hash". Βέβαια δεδομένου ότι πρόκειται για μια λειτουργία μονής κατεύθυνσης, για να μπορεί κάποιος μελλοντικός χρήστης να δώσει τον ίδιο κωδικό πρόσβασης σε μια γραμμή σύνδεσης, θα πρέπει να τρέξει τον προτεινόμενο κωδικό - σε καθαρό κείμενο - με την ίδια λειτουργία κατακερματισμού. Αν το αποτέλεσμα ταιριάζει με το αποθηκευμένο hash που υπάρχει στον χώρο αποθήκευσης των κωδικών πρόσβασης, τότε ο χρήστης γνωρίζει τον σωστό κωδικό πρόσβασης και του παρέχεται πρόσβαση, αλλά εάν τα hashes δεν είναι πανομοιότυπα, η πρόσβαση απορρίπτεται.

Η ηλεκτρονική υπογραφή ενός εγγράφου είναι το ψηφιακό ισοδύναμο της τοποθέτησης μιας υπογραφής σε χαρτί. Ο τρόπος με τον οποίο εκπροσωπείται η

υπογραφή είναι ένα στίγμα (sign) το οποίο κρυπτογραφεί το hash του εγγράφου με το ιδιωτικό κλειδί του χρήστη. Έτσι η ψηφιακή υπογραφή είναι σε θέση να επικυρώνει την εγκυρότητα του εγγράφου[48].



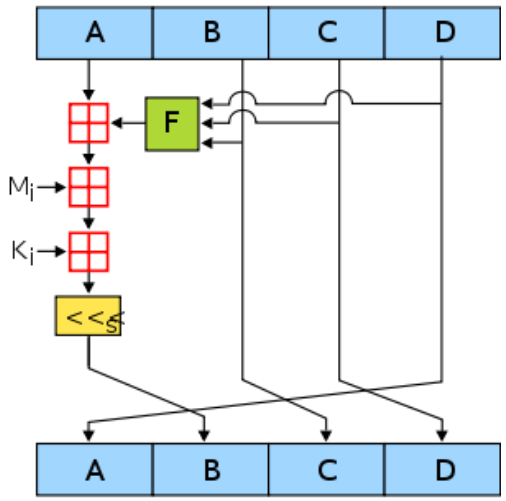
Εικόνα 13. Διαδικασία κρυπτογράφησης της ψηφιακής υπογραφής **[45].**

Ένα κρυπτογραφικό hash, περιλαμβάνει πολλούς μαθηματικούς υπολογισμούς. Μια περιγραφή του εσωτερικού ενός hash είναι πως όλα τα κομμάτια χύνονται σε ένα δοχείο και ανακατεύονται. Υπάρχουν πολλοί πόροι που δείχνουν την εσωτερική λειτουργία ενός αλγόριθμου κατακερματισμού, σχεδόν όλοι περιλαμβάνουν μετατόπιση και περιστροφή μέσω πολλαπλών επαναλήψεων [49].

Όπως προαναφέρθηκε, οι πιο γνωστοί αλγόριθμοι είναι οι MD4,MD5, SHA 1 και SHA 2. Ο αλγόριθμος **MD4** (Message-Digest) είναι μια κρυπτογραφική λειτουργία κατακερματισμού που αναπτύχθηκε από τον Ronald Rivest το 1990 [50]. Το μήκος αφομοίωσης του είναι 128 bit. Ο αλγόριθμος αυτός, έχει επηρεάσει τους μεταγενέστερους αλγορίθμους MD5, SHA-1 και RIPEMD.

2.4.1Περιγραφή του αλγορίθμου MD4.

Ο αλγόριθμος MD4 αποτελείται από 48 πράξεις, που ομαδοποιούνται σε τρεις γύρους 16 πράξεων. Το παρακάτω σχήμα απεικονίζει τη λειτουργία του.



Εικόνα 14. Το κύκλωμα του αλγορίθμου MD4 **[51].**

Το F είναι μια μη γραμμική συνάρτηση, μία λειτουργία που χρησιμοποιείται σε κάθε επανάληψη. Το Mi υποδηλώνει ένα μπλοκ 32 δυαδικών ψηφίων της εισόδου του μηνύματος και το Κι δηλώνει μία σταθερά 32 δυαδικών ψηφίων διαφορετική για κάθε λειτουργία.

Τα 128 bit (16 byte) του MD4 (που ονομάζονται επίσης digests messages) αντιπροσωπεύονται τυπικά ως δεκαεξαδικοί αριθμοί 32 ψηφίων. Τα παρακάτω παρουσιάζουν μια είσοδο ASCII 43 byte και τον αντίστοιχο κατακερματισμό MD4 [51] :

```
MD4("The quick brown fox jumps over the lazy dog")
= 1bee69a46ba811185c194762abaeae90
```

Μια μικρή αλλαγή στην είσοδο επιφέρει αλλαγή στην έξοδο όπως φαίνεται παρακάτω [51].

```
MD4("The quick brown fox jumps over the lazy cog")
= b86e130ce7028da59e672d56ad0113df
```

Το hash της συμβολοσειράς μηδενικού μήκους (zero-length string) είναι [52]:

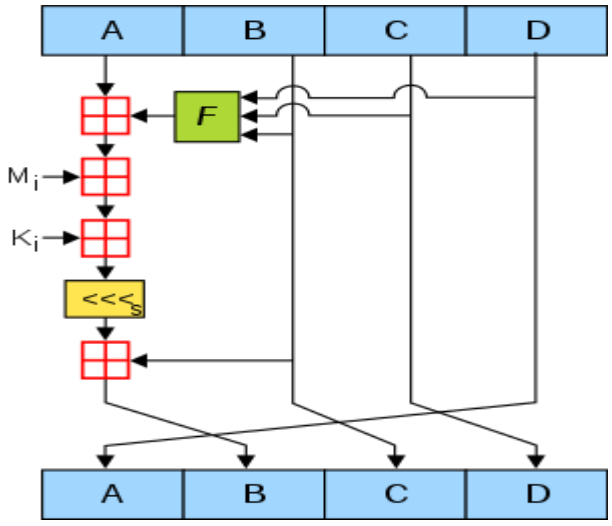
```
MD4("") = 31d6cfe0d16ae931b73c59d7e0c089c0
```

Η ασφάλεια του MD4 έχει υπονομευθεί σοβαρά. Η πρώτη επίθεση πλήρους σύγκρουσης κατά του MD4 δημοσιεύθηκε το 1995 και από τότε έχουν δημοσιευθεί αρκετές νεότερες επιθέσεις [53]. Μια παραλλαγή του MD4 χρησιμοποιείται στο ed2k URI για να παρέχει ένα μοναδικό αναγνωριστικό για ένα αρχείο στα δημοφιλή δίκτυα P2P eDonkey2000 / eMule.

2.4.2 Περιγραφή του αλγορίθμου MD5.

Ο αλγόριθμος **MD5-digest** είναι μια ευρέως χρησιμοποιούμενη λειτουργία κατακερματισμού που παράγει μια **τιμή κατακερματισμού 128-bit**. Το MD5 επεξεργάζεται ένα μήνυμα μεταβλητού μήκους σε μια έξοδο σταθερού μήκους 128 bit. Το μήνυμα εισόδου χωρίζεται σε κομμάτια μπλοκ 512 bit (δεκαέξι λέξεις 32 bit). το μήνυμα είναι γεμισμένο έτσι ώστε το μήκος του να διαιρείται από τα 512 bit. Το κύκλωμα πρώτα παίρνει ένα απλό bit, που προσαρτάται στο τέλος του μηνύματος και ακολουθείται από όσα μηδενικά απαιτούνται για να φτάσει το μήκος του μηνύματος μέχρι τα 64 bit μικρότερα από ένα πολλαπλάσιο του 512. Τα υπόλοιπα δυαδικά ψηφία γεμίζονται με 64 bits που αντιπροσωπεύουν το μήκος του αρχικού μηνύματος.

Ο κύριος αλγόριθμος MD5 λειτουργεί σε κατάσταση 128 δυαδικών ψηφίων, χωρισμένη σε τέσσερις λέξεις 32 bit, που χαρακτηρίζονται ως A, B, C και D. Αυτές αρχικοποιούνται σε ορισμένες σταθερές. Ο κύριος αλγόριθμος χρησιμοποιεί στη συνέχεια κάθε μπλοκ μηνυμάτων 512-bit με τη σειρά του για να τροποποιήσει την κατάσταση. Η επεξεργασία ενός μπλοκ μηνύματος αποτελείται από τέσσερα παρόμοια στάδια.Κάθε στάδιο αποτελείται από 16 παρόμοιες λειτουργίες που βασίζονται σε μια μη γραμμική συνάρτηση F, αρθρωτή προσθήκη και αριστερή περιστροφή. Το παρακάτω σχήμα απεικονίζει τη λειτουργία του σε μια επανάληψη.



Εικόνα 15.Κύκλωμα του αλγορόιθμου MD5 **[54] .**

*Το MD5 αποτελείται από 64 από αυτές τις λειτουργίες, που ομαδοποιούνται σε τέσσερις επαναλήψεις 16 λειτουργιών. Το F είναι μια μη γραμμική συνάρτηση. Το Mi υποδηλώνει ένα μπλοκ 32 δυαδικών ψηφίων της εισόδου μηνύματος και το Ki δηλώνει μία σταθερά 32 δυαδικών ψηφίων διαφορετική για κάθε λειτουργία. Το <<< s υποδηλώνει μια περιστροφή του αριστερού δυαδικού ψηφίου.Υπάρχουν τέσσερις πιθανές λειτουργίες, μια διαφορετική χρησιμοποιείται σε κάθε επανάληψη. Οι λογικές αυτές πράξεις είναι το XOR, το AND, το OR και το **NOT** .*

$$F(B,C,D) = (B \wedge C) \vee (\neg B \wedge D)$$
$$G(B,C,D) = (B \wedge D) \vee (C \wedge \neg D)$$
$$H(B,C,D) = B \oplus C \oplus D$$
$$I(B,C,D) = C \oplus (B \vee \neg D)$$

Οι μίξεις MD5 είναι 128 bit (16 byte) MD5 (που ονομάζονται επίσης digests μηνυμάτων) αντιπροσωπεύονται συνήθως ως μια ακολουθία 32 δεκαεξαδικών ψηφίων. Τα παρακάτω δείχνουν μια είσοδο ASCII 43 byte και τον αντίστοιχο κατακερματισμό MD5 [54] :

```
MD5("The quick brown fox jumps over the lazy dog") =
9e107d9d372bb6826bd81d3542a419d6
```

Με μια μικρή αλλαγή κατά την είσοδο φαίνεται ότι και σε αυτή την περίπτωση αλλάζει ριζικά η έξοδος [54].

```
MD5("The quick brown fox jumps over the lazy dog.") =
e4d909c290d0fb1ca068ffaddf22cbd0
```

Το hash της συμβολοσειράς μηδενικού μήκους (zero-length string) είναι [54] :

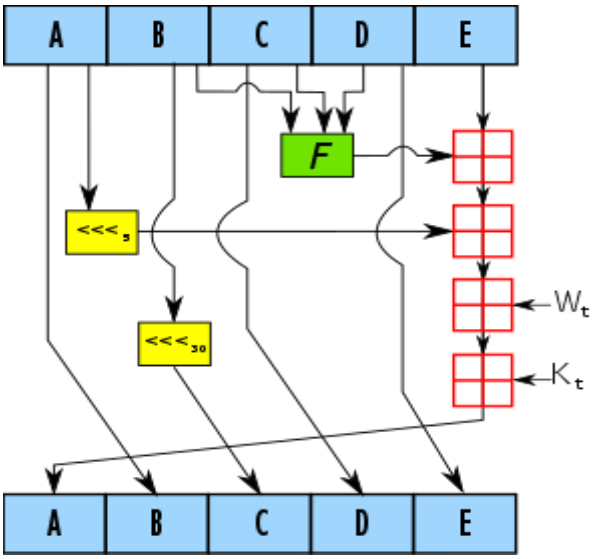
```
MD5("") =
d41d8cd98f00b204e9800998ecf8427e
```

Ο MD5 σχεδιάστηκε αρχικά για να χρησιμοποιηθεί ως κρυπτογραφική λειτουργία κατακερματισμού, έχει βρεθεί όμως ότι έχει εκτεταμένες ευπάθειες. Μπορεί να χρησιμοποιηθεί και ως έλεγχος για την επαλήθευση της ακεραιότητας των δεδομένων, αλλά μόνο ενάντια στην ακούσια διαφθορά. Παραμένει κατάλληλος για μη κρυπτογραφικούς σκοπούς (για παράδειγμα για τον καθορισμό του διαμερίσματος για ένα συγκεκριμένο κλειδί σε μια διαχωρισμένη βάση δεδομένων)[55]. Μία βασική απαίτηση οποιασδήποτε κρυπτογραφικής συνάρτησης κατακερματισμού είναι ότι θα πρέπει να είναι υπολογιστικά ανέφικτο να βρεθούν δύο διαφορετικά μηνύματα που έχουν κατακερματιστεί στην ίδια τιμή. Το MD5 αποτυγχάνει στην απαίτηση αυτή.

Τις αδυναμίες του MD5 έχει εκμεταλλευτεί το κακόβουλο λογισμικό Flame το 2012. Το Ινστιτούτο Τεχνολογίας Λογισμικού της CMU θεωρεί το MD5 ουσιαστικά «κρυπτογραφικά σπασμένο και ακατάλληλο για περαιτέρω χρήση»[56]. Το MD5 εξακολουθεί να χρησιμοποιείται ευρέως, παρά τις καλά τεκμηριωμένες αδυναμίες του ,από τους εμπειρογνώμονες ασφαλείας [57] για τον εντοπισμό κωδικών πρόσβασης. Ο αλγόριθμος MD5 εξακολουθεί να χρησιμοποιείται επίσης στην έρευνα για την ασφάλεια και από εταιρείες για την προστασία τους από ιούς[58] .

2.4.3 Περιγραφή τουαλγορίθμου SHA-1.

Ο **SHA-1** (Secure Hash Algorithm 1) είναι μια κρυπτογραφική συνάρτηση κατακερματισμού η οποία παίρνει μια είσοδο και παράγει μια τιμή κατακερματισμού 160 bit (20 byte).Τυπικά αποδίδεται ως δεκαεξαδικός αριθμός 40 χαρακτήρων. Σχεδιάστηκε από τον Οργανισμό Εθνικής Ασφάλειας των Ηνωμένων Πολιτειών και αποτελεί Πρότυπο Ομοσπονδιακής Επεξεργασίας Πληροφοριών των Η.Π.Α. [49].



Εικόνα 16.Κύκλωμα που παρουσιάζει τη λειτουργία του SHA-1 **[49].**

Τα A, B, C, D και E είναι 32-bit λέξεις.Το F είναι μια μη γραμμική συνάρτηση που ποικίλλει. Το <<<n δηλώνει περιστροφή αριστερού δυαδικού ψηφίου από n θέσεις. Το n ποικίλλει για κάθε λειτουργία.Wt είναι η εκτεταμένη λέξη μηνύματος του κύκλου t. Kt είναι η στρογγυλή σταθερά του κύκλου t .

Το SHA-1 σε δεκαεξαδική μορφή και σε κωδικοποίηση κειμένου ASCII από δυαδικό σε Base64 φαίνεται παρακάτω [49].

```
SHA1("The quick brown fox jumps over the lazy dog")
gives hexadecimal: 2fd4e1c67a2d28fced849ee1bb76e7391b93eb12
gives Base64 binary to ASCII text encoding:
L9ThxnotKPzthJ7hu3bnORuT6xI=
```

Μια μικρή αλλαγή στην είσοδο επιφέρει και εδώ αλλαγή στην έξοδο [59].

```
SHA1("The quick brown fox jumps over the lazy cog")
gives hexadecimal: de9f2c7fd25e1b3afad3e85a0bd17d9b100db4b3
gives Base64 binary to ASCII text encoding:
3p8sf9JeGzr60+haC9F9mxANtLM=
```

Το hash της συμβολοσειράς μηδενικού μήκους (zero-length string) είναι [59]:

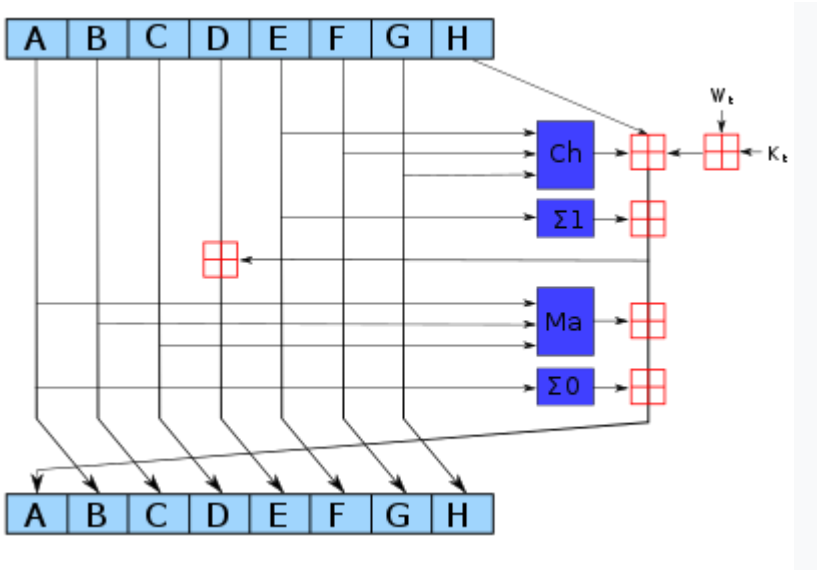
```
SHA1("")
gives hexadecimal: da39a3ee5e6b4b0d3255bfef95601890afd80709
gives Base64 binary to ASCII text encoding:
2jmj7l5rSw0yVb/vlWAYkK/YBwk=
```

Λόγω της επαναληπτικής δομής των αλγορίθμων και της απουσίας επιπρόσθετων τελικών βημάτων, όλες οι λειτουργίες SHA (εκτός από το SHA-3) είναι ευάλωτες στις επιθέσεις σύγκρουσης επέκτασης μήκους και μερικών μηνυμάτων [60]. Αυτές οι

επιθέσεις επιτρέπουν σε έναν εισβολέα να δημιουργήσει ένα μήνυμα που υπογράφεται μόνο από κλειδωμένο SHA (message || key) ή SHA (key || message) , εκτείνοντας το μήνυμα και επανυπολογίζοντας το hash χωρίς να γνωρίζει το κλειδί. Μια απλή βελτίωση για να αποφευχθούν αυτές οι επιθέσεις είναι να κατακερματιστεί δύο φορές: SHAd (message) = SHA (SHA (0b || message)) (το μήκος 0b ή μηδενικό μπλοκ είναι ίσο με το μέγεθος του μπλοκ της συνάρτησης κατακερματισμού).

2.4.4Περιγραφή του αλγορίθμου SHA-2.

Ο **SHA-2** (Secure Hash Algorithm 2) είναι ένα σύνολο κρυπτογραφικών λειτουργιών κατακερματισμού σχεδιασμένων από τον Οργανισμό Εθνικής Ασφάλειας των Ηνωμένων Πολιτειών (NSA) [61]. Κατασκευάζονται χρησιμοποιώντας τη δομή Merkle-Damgård, από μία λειτουργία συμπίεσης μονής κατεύθυνσης η οποία κατασκευάστηκε με τη δομή Davies-Meyer από έναν (ταξινομημένο) εξειδικευμένο αποκλεισμό κρυπτογράφησης .



Εικόνα 17. Κύκλωμα που παρουσιάζει τη λειτουργία του SHA-2 **[62].**

Στο παραπάνω παράδειγμα φαίνετα μια επανάληψη σε μια λειτουργία συμπίεσης της οικογενείας SHA-2. Η περιστροφή με δυαδικά ψηφία χρησιμοποιεί διαφορετικές σταθερές για το SHA-512. Οι αριθμοί αυτοί αφορούν το SHA-256. Μια επανάληψη σε μια λειτουργία συμπίεσης της οικογενείας SHA-2.Τα εξαρτήματα με μπλε χρώμα.Τα εξαρτήματα με μπλε χρώμα εκτελούν τις ακόλουθες λειτουργίες:

$$Ch(E,F,G)= (E \cap F) \oplus (E' \cap G)$$

$$Ma(A,B,C)=(A \cap B) \oplus (A \cap C) \oplus$$

$$(B \cap C)\ \Sigma 0(A>>>2) \oplus (A>>>13)$$

$$\oplus (A>>>22)\ \Sigma 1(E)=(E>>>6) \oplus (E>>>11)$$

$$\oplus (E>>>25)$$

Το SHA-2 περιλαμβάνει σημαντικές αλλαγές από το SHA-1. Το SHA-2 αποτελείται από έξι λειτουργίες κατακερματισμού με τιμές κατακερματισμού που είναι 224, 256, 384 ή 512 bits: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512 / -512 / 256

αντίστοιχα.Τα SHA-256 και SHA-512 είναι νέες λειτουργίες κατακερματισμού που υπολογίζονται με λέξεις 32-bit και 64-bit αντίστοιχα. Χρησιμοποιούν διαφορετικές ποσότητες μετατόπισης και πρόσθετες σταθερές, αλλά οι δομές τους είναι σχεδόν ίδιες, διαφέρουν μόνο στον αριθμό επαναλήψεων. Τα SHA-224 και SHA-384 είναι εκδοχές των SHA-256 και SHA-512 αντιστοίχως, υπολογισμένες με διαφορετικές αρχικές τιμές. Τα SHA-512/224 και SHA-512/256 είναι επίσης εκδοχές του SHA-512, αλλά οι αρχικές τιμές δημιουργούνται χρησιμοποιώντας τη μέθοδο που περιγράφεται στο Federal FIPS PUB 180-4. Το SHA-256 συμμετέχει στη διαδικασία εξακρίβωσης της ταυτότητας των πακέτων λογισμικού του Debian και στο πρότυπο υπογραφής μηνύματος DKIM. Το SHA-512 αποτελεί μέρος ενός συστήματος για την εξακρίβωση της ταυτότητας του αρχειακού βίντεο από το Διεθνές Ποινικό Δικαστήριο για τη γενοκτονία στη Ρουάντα. Τα SHA-256 και SHA-512 προτείνονται για διαχείριση στη DNSSEC. Οι προμηθευτές Unix και Linux κινούνται με τη χρήση SHA-2 256 και 512 bit για ασφαλή αντιστάθμιση κωδικού πρόσβασης. Αρκετά κρυπτοσυστήματα όπως το Bitcoin χρησιμοποιούν το SHA-256 για την επαλήθευση των συναλλαγών και τον υπολογισμό της απόδειξης εργασίας ή της απόδειξης συμμετοχής [63].

2.4.5 Χρήση συναρτήσεων κατακερματισμου (Hash Functions) σε συστήματα Blockchains.

Μέσα στο **blockchain** χρησιμοποιούνται αλγόριθμοι κατακερματισμού για τον **προσδιορισμό της μοναδικής κατάστασης της αλυσίδας σε κάθε χρονική στιγμή**. Τα blocks είναι συνδεδεμένοι κατάλογοι που περιέχουν δεδομένα και έναν δείκτη κατακερματισμού που δείχνει το προηγούμενο μπλοκ, δημιουργώντας μια αλυσίδα. Τα μπλοκ συνδέονται μεταξύ τους μέσω δεικτών κατακερματισμού, οι οποίοι αναπαριστούν τον κατακερματισμό των δεδομένων μέσα στα προηγούμενα μπλοκ μαζί με τη διεύθυνση τους. Με τη σύνδεση των μπλοκ δεδομένων σε αυτή τη μορφή, κάθε προκύπτων κατακερματισμός του προηγούμενου μπλοκ αντιπροσωπεύει ολόκληρη την κατάσταση του μπλοκ αλυσίδας αφού όλα τα δεδομένα των προηγούμενων μπλοκ έχουν αναπαρασταθεί σε ένα hash.

2.5 Δομική σύσταση των μπλοκ.

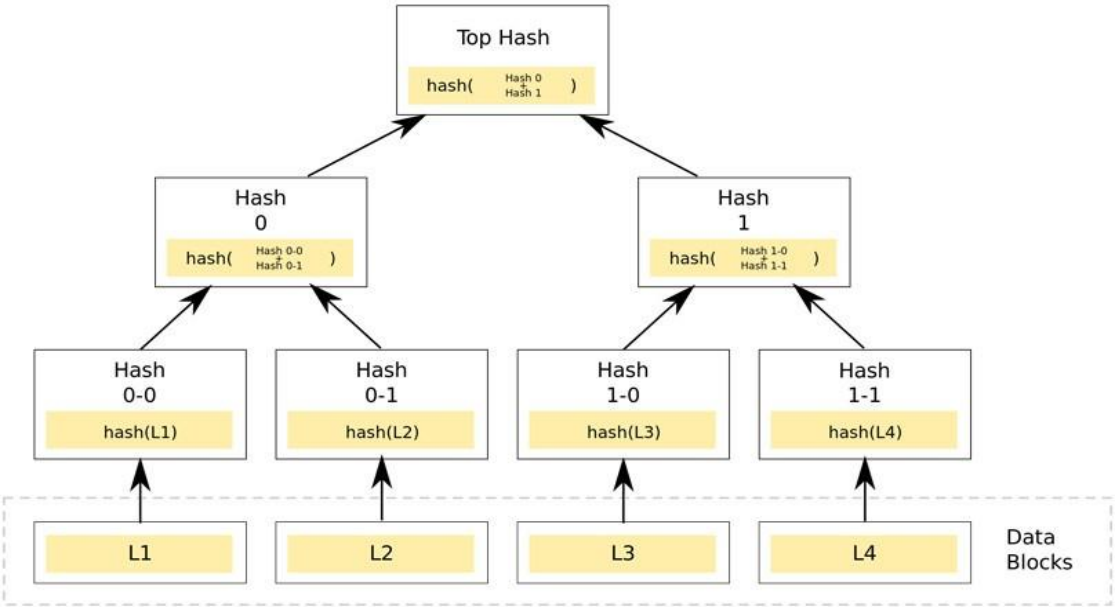
Η αλυσίδα των συνεχόμενων μπλοκ που συνθέτουν το δίκτυο του Bitcoin είναι μία χρονολογικά άρρηκτη κατασκευή. Κάθε μπλοκ αποτελείται από την κεφαλή (block header) και το σώμα (block body) [64]. Η κεφαλή του μπλοκ περιλαμβάνει τις απαραίτητες πληροφορίες που καθορίζουν την μοναδικότητα του μπλοκ, όπως η κατακερματισμένη του αξία(merkle root block hash), η κατακερματισμένη αξία του προηγούμενου μπλοκ(parent block hash), μία χρονική ένδειξη-σφραγίδα που δηλώνει τη χρονική δημιουργία του μπλοκ (block timestamp), έναν τυχαίο ακέραιο αριθμό που χρησιμοποιείται στην επίλυση των μαθηματικών διαδικασιών κατά την εξόρυξη(nonce), έναν αριθμό έκδοσης που ελέγχει πιθανές αναβαθμίσεις (version number), το μέγεθος του μπλοκ (block size) και ένα αριθμητικό όριο που χρησιμεύει στην διατήρηση του ρυθμού δημιουργίας του επόμενου μπλοκ στα επιθυμητά χρονικά όρια(difficulty target), το οποίο μεταβάλλεται περιοδικά και αναλογικά με την αύξηση της υπολογιστικής ισχύος εξόρυξης. Το σώμα του μπλοκ περιλαμβάνει μία λίστα συναλλαγών.Κάθε μπλοκ συνδέεται με το προηγούμενο μέσω συνάρτησης κατακερματισμού, δημιουργώντας μία αλληλένδετη και αδιάσπαστη αλυσίδα. Με

αυτό τον τρόπο κατακερματιστικής διασύνδεσης οποιαδήποτε τροποποίηση σε κάποιο μπλοκ της αλυσίδας μεταδίδεται στην πιο πρόσφατη εκδοχή του συστήματος παρέχοντας τη δυνατότητα εντοπισμού κακόβουλων ενεργειών [65].

2.5.1 Χρήση των δεντρών Merkle σε συστήματα Blockchains.

Το σχήμα του Merkle Tree (Εικόνα 18) χρησιμοποιείται στο σύστημα του Bitcoin για να εξασφαλίζει τον εντοπισμό οποιασδήποτε εισερχόμενης αλλαγής σε κάποια συναλλαγή. Συγκεκριμένα ένα δένδρο τύπου Merkle είναι ένα δυαδικό δένδρο στο οποίο οι πληροφορίες αποθηκεύονται στα φύλλα του.Τα δέντρα Merkle επιτρέπουν την ασήμαντη ανάλυση της ακεραιότητας των δεδομένων καθώς και τη χαρτογράφηση αυτών των δεδομένων μέσω ολόκληρου του δέντρου με τη χρήση δοκιμαστικών στοιχείων Merkle. Η δομή του δέντρου επιτρέπει την αποτελεσματική χαρτογράφηση ανεξάρτητα των μεγάλων ποσοτήτων δεδομένων και επιτρέπει την εύκολη αναγνώριση του σημείου πού συμβαίνουν οι αλλαγές στα δεδομένα αυτά.

Εφόσον το hash της ρίζας είναι δημόσια γνωστό και αξιόπιστο, σε μια αναζήτηση βασικής αξίας σε βάση δεδομένων μπορεί να χρησιμοποιήσει μια απόδειξη Merkle για να επαληθεύσει τη θέση και την ακεραιότητα ενός δεδομένου σε μια βάση δεδομένων που έχει μια συγκεκριμένη ρίζα. Ένα από τα σημαντικότερα οφέλη της δομής δέντρου Merkle είναι η δυνατότητα επαλήθευσης αυθαίρετων μεγάλων συνόλων δεδομένων μέσω ενός παρόμοιου μηχανισμού αντιστάθμισης που χρησιμοποιείται για την επαλήθευση πολύ μικρότερων ποσοτήτων δεδομένων. Το δέντρο είναι επωφελές για τη διανομή μεγάλων συνόλων δεδομένων σε διαχειρίσιμα μικρότερα τμήματα όπου το εμπόδιο για την επαλήθευση της ακεραιότητας μειώνεται σημαντικά παρά το συνολικά μεγαλύτερο μέγεθος δεδομένων.



Εικόνα 18. Σχήμα Merkle tree **[66]**.

3.

3.1 Η τεχνολογία Blockchain στο χώρο της υγείας.

Η τεχνολογία blockchain είναι ιδιαίτερα χρήσιμη στο χώρο της υγείας. Συγκεκριμένα χρησιμοποιείται σε περιπτώσεις διευθέτησης ενός θέματος όπου χρειάζεται η **εμπλοκή πολλών συμβαλλόμενων μελλών** και επιπρόσθετα σε διαδικασίες όπου απαιτείται μεγαλύτερη **εμπιστοσύνη** από την ήδη υπάρχουσα μεταξύ των συμμετεχόντων, η χρήση της κρίνεται βοηθητική. Ακόμα η τεχνολογία blockchain μπορεί να εφαρμοστεί σε καταστάσεις όπου **η διαμεσολάβηση τρίτων ατόμων δύναται να παραλειφθεί**, ενισχύοντας έτσι την εμπιστοσύνη ή την αποτελεσματικότητα του συστήματος. Τέλος η χρήση της είναι δόκιμη, όταν είναι αναγκαία η **αξιόπιστη παρακολούθηση των δραστηριοτήτων του συστήματος** ή όταν τα δεδομένα πρέπει να παραμείνουν αξιόπιστα με την **πάροδο του χρόνου** [67].

Το Blockchain δύναται να χρησιμοποιηθεί ως αποκεντρωμένο δίκτυο διαχείρισης ιατρικών δεδομένων, κοινό σε όλους τους ενδιαφερόμενους, με ελεγχόμενη πρόσβαση σε ιατρικά αρχεία, χωρίς την επίβλεψη κάποιας κεντρικής αρχής. Η **ιδιότητα του αμετάβλητου** του blockchain βελτιώνει σημαντικά την **ασφάλεια των δεδομένων υγείας** που είναι αποθηκευμένα σε αυτό, διότι αφού αποθηκευτούν στο blockchain δεν μπορούν να αλλοιωθούν ή να.ανακληθούν. Όλα τα δεδομένα για την υγεία στο blockchain είναι κρυπτογραφημένα, με χρονοσήμανση και η προσάρτηση τους στο δίκτυο γίνεται με χρονολογική σειρά. Επιπλέον, τα ιατρικά δεδομένα αποθηκεύονται σε blockchain χρησιμοποιώντας **κρυπτογραφικά κλειδιά** που βοηθούν στην προστασία της ταυτότητας ή της ιδιωτικής ζωής των ασθενών. Η διαβεβαίωση ότι δεν γίνεται κακή χρήση των δεδομένων των ασθενών ενισχύεται μέσω των blockchains χάρη στην ισχυρή κρυπτογράφηση, τα πρωτόκολλα και τις καθορισμένες έξυπνες συμβάσεις που περιλαμβάνει [68].

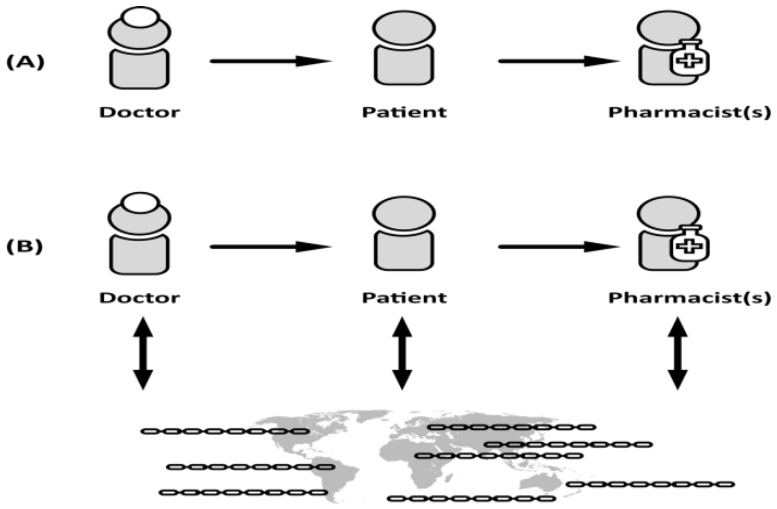
Οι εγγραφές στο blockchain αντιγράφονται σε πολλαπλούς κόμβους, έτσι η **διαθεσιμότητα των δεδομένων υγείας** που είναι αποθηκευμένα σε μπλοκ αλυσίδα είναι εγγυημένη καθώς το σύστημα είναι ανθεκτικό στις απώλειες ή στη διαφθορά δεδομένων και στην επαλήθευση αυτών ακόμη και χωρίς πρόσβαση στο απλό κείμενο των αρχείων που είναι αποθηκευμένα σε blockchain. Αυτό είναι ένα πολύ χρήσιμο στοιχείο στους τομείς υγειονομικής περίθαλψης, όπως στη διαχείριση αλυσίδας εφοδιασμού φαρμακευτικών προϊόντων και στην επεξεργασία ασφαλιστικών απαιτήσεων.

3.2 Εφαρμογές Blockchain στο χώρο της υγείας.

3.2.1 Εφαρμογές Blockchain για την καταπολέμηση της παραχάραξης φαρμάκων.

Περιγραφή-ανάλυση προβλήματος

Η χρήση της τεχνολογίας Blockchain στην **ιχνηλασιμότητα των φαρμάκων** είναι μια σαφώς καθορισμένη πρόκληση στην οποία μπορεί να εφαρμοστεί η τεχνολογία blockchain. Η εταιρεία **Nuco** θέλησε να αντιμετωπίσει την παραχάραξη των φαρμάκων που συμβαίνει με την **τροποποίηση των αριθμών και την αλλαγή της αρχικής συνταγής, το διπλασιασμό συνταγών** (π.χ. φωτοτυπία) και των λεγόμενων **«ιατρικών αγορών»,** όπου ορισμένα άτομα επισκέπτονται πολλούς γιατρούς για να συγκεντρώσουν όσο το δυνατόν περισσότερες αρχικές συνταγές [67]. Για να το καταφέρει αυτό, ζήτησε να εγκατασταθούν προγράμματα παρακολούθησης που θα βελτιώνουν την πρόσβαση και τον χρόνο απόκρισης, θα σαρώνουν τα δεδομένα για να επισημαίνουν ύποπτα πρότυπα αγορών και θα ενημερώνουν τους γιατρούς και τους φαρμακοποιούς για τα αποτελέσματα. Η εταιρία Nuco αναγνωρίζει το πρόβλημα ως πρόβλημα "ανοικτού βρόχου", αυτό σημαίνει ότι υπάρχει ατέρμονη ανατροφοδότηση μεταξύ των γιατρών και των φαρμακοποιών.



Εικόνα 19. Παραδοσιακός τρόπος αλληλεπίδρασης ιατρών-ασθενών-φαρμακοποιών και η διαδικασία με χρήση τεχνολογίας blockchain **[69]**.

Το παραπάνω σχήμα είναι παράδειγμα ενός ανοικτού βρόχου, όπου Α) ο ασθενής λαμβάνει ιατρική συνταγή από έναν γιατρό, ο οποίος στη συνέχεια τη παραδίδει σε έναν (ή περισσότερους) φαρμακοποιούς. Ένας φαρμακοποιός δεν γνωρίζει εάν η συνταγή είναι πρωτότυπη, ακριβής ή έχει συμπληρωθεί προηγουμένως. (Β) Για να κλείσει ο βρόχος, οι συναλλαγές αποθηκεύονται σε ένα blockchain Κάθε ενδιαφερόμενος μπορεί να έχει πρόσβαση και να προσθέσει δεδομένα στα blockchains, ανάλογα με την περίπτωση. Για παράδειγμα, ένας γιατρός μπορεί να προσθέσει την εγγραφή της αρχικής συνταγής και ένας φαρμακοποιός μπορεί να ελέγξει ότι η συνταγή είναι αναλλοίωτη. ένας φαρμακοποιός μπορεί να καταγράψει τις ενέργειες που έχουν συμβεί και ο γιατρός ή άλλος φαρμακοποιός μπορεί να ελέγξει την κατάστασή του.

Προτεινόμενη λύση βασισμένη σε τεχνολογία Blockchain

Η εταιρία Nuco ανέπτυξε μια λύση βασισμένη στη τεχνολογία blockchain για το πρόβλημα παραποίησης των συνταγογραφούμενων φαρμάκων. Η διαδικασία ξεκινάει όταν μια ιατρική συνταγή συνταγογραφείται από έναν γιατρό, την ίδια στιγμή επισυνάπτεται ένας μη αναγνώσιμος από τον υπολογιστή κωδικός ο οποίος λειτουργεί ως μοναδικό αναγνωριστικό σύμβολο. Αυτό το **μοναδικό αναγνωριστικό σύμβολο** συνδέεται στη συνέχεια με ένα μπλοκ πληροφοριών που περιλαμβάνει το **όνομα του φαρμάκου**, την **ποσότητα,** την **ανώνυμη ταυτότητα του ασθενούς** και μια **χρονική σήμανση.** Όταν η συνταγή ελέγχεται από το φαρμακοποιό, σαρώνεται το σύμβολο, και η απόπειρα έγκρισης της συνταγής καταγράφεται και συγκρίνεται με τα δεδομένα που περιέχονται στο blockchain. Έτσι, ο φαρμακοποιός ενημερώνεται γρήγορα εάν η συνταγή είναι έγκυρη ώστε να ολοκληρωθεί η διαδικασία. Αντίγραφα του blockchain, διατηρούνται από πολλούς ενδιαφερόμενους σε ένα αποκεντρωμένο δίκτυο. Αυτά τα ενδιαφερόμενα μέρη συμπεριλαμβάνουν αλυσίδες φαρμακείων, ασφαλιστικές εταιρείες, ελεγκτές ή νοσοκομεία, καθένα από τα οποία έχει συμφέρον να επιλύσει απάτες με συνταγογραφούμενα φάρμακα.

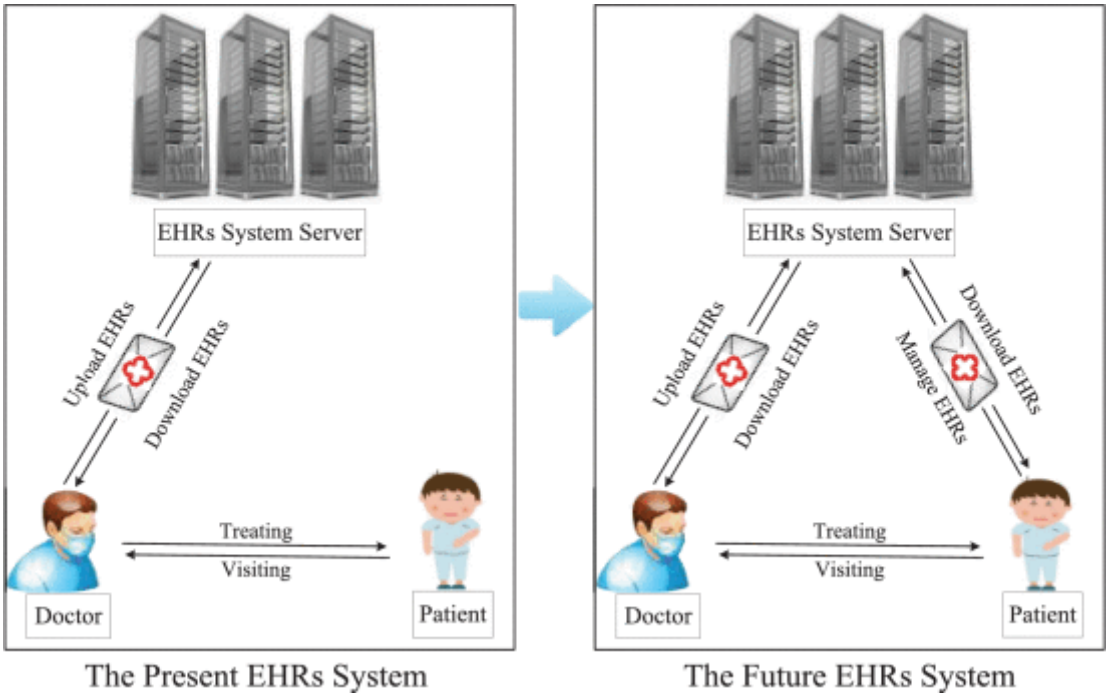
Πλεονεκτήματα

Το εύρος των δεδομένων που μπορούν να παρέχουν οι συμμετέχοντες είναι αρκετά μεγάλο για να καλύψει τους απαιτούμενους πόρους που χρειάζεται η συγκεκριμένη τεχνολογία πληροφορικής. Λόγω της κρυπτογράφησης των πληροφοριών blockchain, η προστασία της ιδιωτικής ζωής διατηρείται, διότι κάθε ενδιαφερόμενος μπορεί να έχει πρόσβαση μόνο στις πληροφορίες στις οποίες δικαιούται με την κατοχή των σωστών κρυπτογραφικών κλειδιών. Οι πληροφορίες που περιέχονται στο blockchain είναι ακριβείς, και καταγράφονται με κοινό τρόπο για όλους, η καθεμία πληροφορία περιέχει μια αδιάσπαστη αλυσίδα, πανομοιότυπη με τις άλλες αλυσίδες που περιλαμβάνονται στο δίκτυο ,οι οποίες μπορούν να ελέγχονται προκειμένου να εξασφαλιστεί η ακεραιότητα των δεδομένων. Αυτή η λύση περιγράφει τη μορφή ενός εξουσιοδοτημένου τύπου blockchain, στο οποίο μόνο συγκεκριμένα μέρη μπορούν να διαβάσουν πληροφορίες και να συναλλάσσονται. Η λύση Nuco χρησιμοποιεί τις ήδη υπάρχουσες τεχνολογίες (π.χ. ο φαρμακοποιός χρειάζεται μόνο ένα smartphone ή παρόμοια συσκευή για να διαβάσει το μοναδικό αναγνωριστικό) και παρέχει διαλειτουργικότητα με τα υπάρχοντα πρωτόκολλα. Η **διαλειτουργικότητα** είναι ένα σημαντικό στοιχείο δεδομένου ότι τα νέα έργα blockchain διεπικοινωνούν με την τρέχουσα και τη νέα τεχνολογία για την αποθήκευση πληροφοριών.

3.2.2 Εφαρμογές Blockchain για τη δημιουργία Ιατρικών Φακέλων.

Περιγραφή

Η τεχνολογία blockchain δίνει τη δυνατότητα στους ασθενείς να **ασκούν προσωπικό έλεγχο** στα δεδομένα που συλλέγονται για εκείνους. Αυτό καθιστά τη λειτουργία ενός γιατρού ευκολότερη, δημιουργώντας ένα υψηλότερο επίπεδο οργάνωσης και προσβασιμότητας με τη χρήση ψηφιακών εργαλείων που εξοικονομούν χρόνο και ταυτόχρονα δημιουργούν μια αμεσότερη επαφή του ασθενή με την κατάσταση της υγείας του.



Εικόνα 20. Παραδοσιακός και μελλοντικός τρόπος ενημέρωσης των ασθενών για την κατάσταση της υγείας τους **[70].**

Μία από τις πιο δημοφιλείς περιπτώσεις χρήσης blockchain στην υγειονομική περίθαλψη είναι η διαχείριση **ηλεκτρονικών ιατρικών φακέλων** (Electronic Medical Record-EMR), τα οποία χρησιμοποιούνται για την ηλεκτρονική δημιουργία, αποθήκευση και διαχείριση των ιατρικών δεδομένων των ασθενών.

Πλεονεκτήματα

Το Blockchain καθίσταται κατάλληλο για την αποθήκευση και τη διαχείριση των ηλεκτρονικών ιατρικών αρχείων των ασθενών. Αυτό συμβαίνει, εξαιτίας της ιδιότητας της αποκέντρωσης, της αμεταβλητότητας, και της αξιοπιστίας της προέλευσης των δεδομένων που παρέχουν τα έξυπνα συμβόλαια [71]. Το blockchain συμμορφώνεται με την ευρωπαϊκή πολιτική για τα προσωπικά δεδομένα (GDPR), η οποία απαγορεύει την επεξεργασία ευαίσθητων προσωπικών δεδομένων ασθενών, εκτός εάν δοθεί ρητή συγκατάθεση από τους εκείνους [72].Το blockchain είναι ευρέως προτεινόμενο ως βιώσιμη τεχνολογία για την οικοδόμηση μιας πλατφόρμας υγειονομικής περίθαλψης που μπορεί να εξουσιοδοτήσει τους ασθενείς να ελέγχουν το πώς και με ποιους θα μοιράζονται τα δεδομένα τους [73].

Εφαρμοσμένα παραδείγματα

Η εταιρία **Guardtime**, χρησιμοποιεί μια πλατφόρμα βασισμένη σε blockchain για την ασφάλεια των αρχείων πάνω από 1 εκατομμύριο ασθενών στην Εσθονία [74].

Παρομοίως η **πλατφόρμα MedRec** [75], έργο του MIT Media Lab και του ιατρικού κέντρου Beth Israel Deaconess, στοχεύει στην παροχή των υπηρεσιών της, στους ίδιους τους ασθενείς για να καθορίσουν ποιος μπορεί να έχει πρόσβαση στα δεδομένα

τους, μέσω κάποιων λειτουργιών παροχής δικαιωμάτων πρόσβασης χτισμένο σε μπλοκ αλυσίδα.

Το **Δίκτυο Υγείας Gem (GHN)** είναι ένα ακόμα παράδειγμα, το οποίο αναπτύσσεται από την εκκίνηση των Ηνωμένων Πολιτειών, χρησιμοποιώντας την πλατφόρμα **blockbuster** της Ethereum. Το Δίκτυο Υγείας Gem επιτρέπει στους επαγγελματίες να έχουν κοινή πρόσβαση στα ίδια δεδομένα [75].

Η **Healthbank**, μια ελβετική εταιρεία ψηφιακής υγείας, εργάζεται κατά τον ίδιο τρόπο για να εξουσιοδοτήσει τους ασθενείς να ελέγχουν πλήρως τα δεδομένα τους χρησιμοποιώντας blockchain.

Το **HealthChain**[76] είναι μια εφαρμογή ηλεκτρονικών ιατρικών φακέλων που αναπτύχθηκε ως ένα εξουσιοδοτημένο, ιδιωτικό δίκτυο blockchain χρησιμοποιώντας το Hyperledger Fabric . Η αρθρωτή αρχιτεκτονική του Hyperledger [77] επιτρέπει στην HealthChain να επιτύχει την **εμπιστευτικότητα των δεδομένων για την υγεία, την επεκτασιμότητα και την ασφάλεια αυτών**. Το HealthChain περιλαμβάνει επίσης αλυσιδωτούς κώδικες (έξυπνες συμβάσεις) που ελέγχουν τις άδειες και τα δικαιώματα πρόσβασης στο δίκτυο blockchain. Υπάρχει επίσης άλλη μια πλατφόρμα η **Ancile**[78], η οποία χρησιμοποιεί επίσης έξυπνα συμβόλαια, αλλά είναι χτισμένη στην πλατφόρμα Blockhouse του Etherum για την επίτευξη του ελέγχου πρόσβασης, την ασφάλεια των δεδομένων, την προστασία της ιδιωτικής ζωής και τη διαλειτουργικότητα των ηλεκτρονικών ιατρικών φακέλων.

Η MedRec [75] αποτελεί ένα παραδείγμα υλοποιήσης των ηλεκτονικών ιατρικών αρχείων που χρησιμοποιούν την πλατφόρμα Ethereum blockchain. Η πλατφόρμα **Medrec** παρέχει στους χρήστες, τη συλλογή των ιατρικών ιστορικών από όλους τους διαφορετικούς παρόχους[79]. Με την πάροδο του χρόνου και εξαιτίας των περιορισμένων δυνατοτήτων των ιατρικών φακέλων που υπάρχουν στην αγορά, τα προσωπικά δεδομένα των χρηστών καταλήγουν στην επιμέλεια πολλών διαφορετικών οργανισμών οι οποίοι αποτελούν τους κύριους υπεύθυνους για τη διαχείριση τους. Αυτό έχεις ώς αποτέλεσμα την δύσκολη και χρονοβόρα χρήση τους. Η Medrec δίνει τη δυνατότητα για μια ομοιόμορφη πρόσβαση στα διάφορα διασκορπισμένα δεδομένα, όπως και τον έλεγχο της χρήσης τους. Το δεύτερο πρόβλημα που επιχειρεί να διορθώσει είναι ότι τα ιατρικά δεδομένα δεν έχουν κάποια εύκολα αντιληπτή αξία ούτε εύκολο τρόπο απόκτησης από ερευνητές που τα χρειάζονται. Στην πλατφόρμα αυτή, οι ερευνητές που προσφέρουν υπολογιστική δύναμη για τη διατήρηση και επέκταση του blockchain, ως αντάλλαγμα θα δέχονται ανωνυμοποιημένα ιατρικά δεδομένα που θα μπορούν να χρησιμοποιήσουν. Η υποστηριζόμενη τεχνολογία είναι βασισμένη σε Blockchain, το οποίο υποστηρίζει διανεμημένες βάσεις δεδομένων, μόνιμο ιστορικό όλων των συμβάντων και ασφαλή πρόσβαση στα δεδομένα. Τα χρήσιμα στοιχεία που περιλαμβάνει αυτή η προσπάθεια είναι ότι χρησιμοποιεί ήδη υπάρχουσες τεχνολογίες και αρχιτεκτονικές (όπως του ηλεκτρονικού φακέλου) και εγκαταστάσεις, το οποίο κάνει την εφαρμογή του πιο εύκολη και επιθυμητή. Επιπλέον**,** το κόστος διατήρησης του backend μέρους της εφαρμογής μειώνεται σημαντικά, γίνεται ως και μηδαμινό.Τέλος, απαιτεί συμφωνία με πολλούς ιατρικούς οργανισμούς για να λειτουργήσει σε ιδανική κατάσταση.

Η πλατφόρμα **Medibloc** έχει σκοπό να προσφέρει στους χρήστες μια συλλογή των ιατρικών ιστορικών από προσωπικές τους ηλεκτρονικές συσκευές όπως κινητά και προσωπικοί υπολογιστές [80]. Η **Medibloc** δίνει τη δυνατότητα για ομοιόμορφη πρόσβαση στα διάφορα διασκορπισμένα δεδομένα, όπως και τον έλεγχο για τη χρήση τους αλλά και το σημαντικότερο εξασφάλιση της υπαρξής τους Όλες οι συναλλαγές στην εφαρμογή θα υποστηρίζονται από ένα κρυπτονόμισμα που θα επιτρέπει όλες τις λειτουργίες της πλατφόρμας και τη χρήση των διαφόρων υπηρεσιών της. Στους διάφορους κόμβους (συμμετέχοντες) του συστήματος που διατηρούν το blockchain, θα τους παρέχονται κρυπτονομίσματα. Περιλαμβάνει ένα επίπεδο δεδομένων βασισμένο σε Blockchain, το οποίο υποστηρίζει διανεμημένες βάσεις δεδομένων, μόνιμο ιστορικό όλων των συμβάντων και ασφαλή πρόσβαση στα δεδομένα. Οι συναλλαγές θα πραγματοποιούνται με τη χρήση κτυπτονομίσματος και τα έσοδα των λειτουργιών θα καλύπτουν το κόστος των servers των κλινικών. Σε αντίθεση με πολλές άλλες πλατφόρμες ο κώδικας είναι ανοιχτός γεγονός που δίνει ξεκάθαρη εικόνα στην ανάπτυξη του προϊόντος και στον άμεσο, δημόσιο έλεγχο των δεδομένων.

Η πλατφόρμα **Iryo** σκοπεύει να δώσει λύση στο μεγάλο όγκο ιατρικών δεδομένων που παράγεται κάθε χρόνο. Για την αντιμετώπιση του προβλήματος αυτού η πλατφόρμα Iryo βασίζεται στο πρότυπο πλαίσιο openEHR για λειτουργία των ηλεκτρονικών φακέλων σε διαφορετικά συστήματα [81]. Η **Iryo** δίνει σε πρώτο στάδιο τη δυνατότητα ομοιόμορφης πρόσβασης στα διασκορπισμένα δεδομένα, και στη συνέχεια παρέχει τη δυνατότητα ελέγχου της σωστής χρήσης τους. Τα δεδομένα αποθηκεύονται σε τρία διαφορετικά μέρη [στο κινητό του πελάτη, στους εξυπηρετητές (servers) των κλινικών που κρατούν τα δεδομένα και στους εξυπηρετητές (servers) της ίδια της εταιρίας], έτσι τα δεδομένα είναι πάντα προσβάσιμα και είναι πρακτικά αδύνατο να χαθούν. Επίσης δίνει τη δυνατότητα να χρησιμοποιηθούν ανωνυμοποιημένα τα δεδομένα αυτά σε ερευνητικά προγράμματα. Όλες οι συναλλαγές στην εφαρμογή υποστηρίζονται από ένα κρυπτονόμισμα που διευκολύνει όλες τις λειτουργίες. Οι υποστηριζόμενες τεχνολογίες που χρησιμποποιούνται είναι βασισμένες σε τεχνολογία Blockchain, η οποία υποστηρίζει και σε αυτή την περίπτωση, διανεμημένες βάσεις δεδομένων, μόνιμο ιστορικό όλων των συμβάντων και ασφαλή πρόσβαση στα δεδομένα. Επιπλέον περιλαμβάνει μια εφεδρική αποθήκευση που διασφαλίζει τα δεδομένα των χρηστών. Η υποστήριξη κρυπτονομίσματος καθιστά δυνατές τις συναλλαγές και δύναται να καλύψει το κόστος των servers των κλινικών. Τέλος, εξασφαλίζει τη διαλειτουργικότητα των υπαρχόντων συστημάτων των ηλεκτρονικών ιατρικών φακέλων. Σημαντικά στοιχεία της εφαρμογής αυτής είναι ότι βασίζεται σε ήδη υπάρχουσες τεχνολογίες και προσφέρει διαλειτουργικές λύσεις που κάνουν ευκολότερη τη χρήση του. Το κόστος διατήρησης των servers της πλατφόρμας είναι ιδιαίτερα μειωμένο έως και μηδαμινό. Παρέχει μεγάλη ασφάλεια δεδομένων αλλά απαιτει μεγαλύτερο κόστος χρήσης. Η αρχική προσφορά του κρυπτονομίσματος(ICO) αναβλήθηκε μέχρι νεωτέρας, το οποίο μπορεί να σηματοδοτεί τη μη βιωσιμότητα του συστήματος αυτού.

Η **Medicalchain** στοχεύει να αντιμετωπίσει τα προβλήματα της αλληλοεπικάλυψης και της παραποίησης των δεδομένων καθώς και τον μεγάλο όγκο των μη προσβάσιμων πληροφοριών που προκύπτουν από τον παραδοσιακό τρόπο μεταφοράς των ιατρικών αρχείων [69]. Η Medicalchain εισήγαγε μια ψηφιοποιημένη λύση που οδηγεί τους γιατρούς μέσω μιας δομημένης διαδικασίας στη μείωση των

λανθασμένων στοιχείων και παραλείψεων των ιατρικών δεδομένων και επιταχύνει την αναθεώρηση των ιατρικών εγγράφων από τα ανώτερα στελέχη. Για να το επιτύχει αυτό χρησημοποιεί blockchain, το οποίο επιτρέπει την **αποτελεσματική αποκεντρωμένη ανταλλαγή δεδομένων μεταξύ των ενδιαφερομένων** (π.χ. νοσοκομεία σε διαφορετικά δίκτυα και φορείς παροχής ασφάλισης υγείας) και παρέχει εμπιστοσύνη για την προφύλαξη της ιδιωτικότητας των δεδομένων των ασθενών **λόγω της κρυπτογράφησης.** Η πλατφόρμα **Medical chain** δίνει τη δυνατότητα να χρησιμοποιηθούν ανωνυμοποιημένα τα δεδομένα αυτά για λόγους έρευνας από ερευνητές. Η ανάπτυξη ενός blockchain το οποίο είναι **κοινόχρηστο σε ένα δίκτυο αξιόπιστων διεθνών οργανισμών υγειονομικής περίθαλψης** δημιουργήθηκε για να βοηθήσει τους ασθενείς να λαμβάνουν φροντίδα διεθνώς χωρίς περίπλοκη συλλογή και μεταφορά ιατρικών αρχείων. Η ενεργοποίηση των διεθνών μπλοκ αλυσίδων δύναται να βρεί λύσεις και στην αποθήκευση πληροφοριών σε ένα blockchain. Η αποθήκευση των ιατρικών στοιχείων ορισμένες φορές αποτελεί πρόβλημα διότι σε κάποιες περιπτώσεις δεν επιτρέπεται από τους κανονισμούς η **αποθήκευση** δεδομένων ιδιωτικής υγειονομικής περίθαλψης. Για να κατασκευαστεί μια διεθνής κοινή δομή δεδομένων θα πρέπεί να υπάρχει μια **κρυπτογραφημένη υπογραφή** που θα επιτρέπει σε κάθε μπλοκ του blockchain να προσδιορίσει με μοναδικό τρόπο το μπλοκ που ακολουθεί. Ομοίως, κάθε μπλοκ μπορεί να περιέχει κρυπτογραφημένες υπογραφές απομακρυσμένων αποθηκευμένων εγγράφων που μπορούν να χρησιμοποιηθούν για να αποδειχθεί ότι ένα έγγραφο δεν έχει αλλοιωθεί. Τα δεδομένα μπορούν να διατηρούνται σε κάθε νοσοκομείο και στη συνέχεια, όταν μεταφέρονται από τον ασθενή, αποδεδειγμένα μέσω των υπογραφών που έχουν καταγραφεί και μοιραστεί μέσω του blockchain να γίνεται η πλήρης και ακριβής καταγραφή του ιατρικού ιστορικού του ασθενούς. Μόνο με την πιστοποίηση ότι το έγγραφο είναι γνήσιο αποθηκεύεται στο blockchain. Τα πραγματικά έγγραφα μπορούν να παραμείνουν (σε κρυπτογραφημένη μορφή) στις εγχώριες δικαιοδοσίες έως ότου ο ιδιοκτήτης των δεδομένων (ο ασθενής) αποφασίσει να τα μοιραστεί. Η αποθήκευση κρυπτογραφικών υπογραφών με τον τρόπο αυτό είναι γνωστή ως "**αποθήκευση εκτός αλυσίδας**" και είναι ένα κοινό θέμα στην τεχνολογία blockchain για τον τομέα της υγείας, τόσο για την αντιμετώπιση ρυθμιστικών εμποδίων όσο και λόγω της ύπαρξης μεγάλων σε όγκο αρχείων δεδομένων όπως δεδομένα απεικόνισης, όπου η κοινή χρήση τους στην μπλοκ αλυσίδα δεν αποτελεί μια βελτιωμένη λύση.

Η **Healthcoin**, ανέπτυξε μια πρωτοβουλία βασισμένη σε blockchain για να βοηθήσει τους επιστήμονες να συνεργαστούν για τη βελτίωση των συμπτωμάτων του διαβήτη. Στη συνέχεια οικοδόμησε ένα **σύστημα για την κατασκευή ενός παγκόσμιου ηλεκτρονικού συστήματος αρχείων υγείας** [67]. Έχει προσδιορίσει μια πρόταση για τον έλεγχο των πληροφοριών με βάση τον ασθενή που αποτελείται από τρεις αρχές, να δίνει τα πλήρη δεδομένα στον χρήστη , να επιτρέπει στον χρήστη να διοχετεύσει τα δεδομένα του στην καλύτερη δυνατή χρήση και να επιτρέπει στους χρήστες να μεταδίδουν τα αποτελέσματα. Παρόμοια προγράμματα για τη σύνδεση των πληροφοριών των ασθενών μεταξύ των ενδιαφερόμενων μερών επιχειρούνται από πολλές εταιρίες, όπως οι BurstIQ, Factom, GemOS, HealthCombix, MedRec.

Η πλατφόρμα **BurstIQ** παρέχει στους χρήστες τη συλλογή των ιατρικών ιστορικών από όλους τους διαφορετικούς παρόχους. Την πλατφόρμα αυτή μπορούν να τη χρησιμοποιήσουν τόσο οι απλοί χρήστες όσο και γιατροί που μπορούν να γνωρίζουν εύκολα το ολοκληρωμένο ιατρικό ιστορικό των χρηστών. Η λειτουργία του μπορεί

να μειώσει το κόστος του δικτύου επειδή δε χρειάζεται η μεταφορά πολύπλοκων ιατρικών αρχείων και δύναται να προσφέρει εξειδικευμένες θεραπευτικές αγωγές μέσω της αγοράς που περιέχεται στην εφαρμογή. Οι ασφαλιστικές μπορούν να χρησιμοποιήσουν τα αποτελεσματα από την ανάλυση δεδομένων , η οποία βασίζεται σε βαθιάς μάθησης (deep learning) αλγορίθμους για καλύτερες προβλέψεις. Περιλαμβάνει ένα επίπεδο δεδομένων βασισμένο σε Blockchain, το οποίο υποστηρίζει διανεμημένες βάσεις δεδομένων, μόνιμο ιστορικό όλων των συμβάντων και ασφαλή πρόσβαση στα δεδομένα. Τέλος, έχει την υποστήριξη ενός κρυπτονομίσματος που θα κάνει δυνατές όλες τις συναλλαγές και θα καλύπτει το κόστος των servers των κλινικών. Η **BurstIQ** εστιάζει στις δυνατότητες της τεχνολογίας blockchain όταν γίνει ο κύριος τρόπος αποθήκευσης των ιατρικών δεδομένων των ασθενών. Εστιάζει στο μέλλον της φροντίδας ,της ιατρικής ακριβείας, παρέχοντας θεραπευτικές αγωγές ειδικά για τις ανάγκες ενός συγκεκριμένου ασθενή και μ**ηχανική μάθηση με συστήματα τεχνητής νοημοσύνης**, επικεντρωμένες στον τομέα της υγείας και τις ιδιαιτερότητες των ασθενών [67].

Η **HealthCombix**, σε συνεργασία με τη **PointNurse**, προσπαθούν να αντιμετωπίσουν το πρόβλημα της μετατόπισης ευθύνης στους ασθενείς για την παρακολούθηση των ιατρικών δεδομένων τους. Για την επιβεβαίωση των δεδομένων που καταλήγουν στο αμετάβλητο αρχείο blockchain και την έγκριση της ακρίβειάς τους, εισήγαγαν ένα νεό επίπεδο που περιλαμβάνει τη μεσολάβηση των νοσοκόμων που επικυρώνουν τη σωστή μεταφορά των δεδομένων στον ασθενή . Ένα άλλο χαρακτηριστικό διαφοροποίησης του HealthCombix είναι η προσπάθεια τους να συνδέσουν το σύστημά που διαχειρίζοντια με **ένα εξειδικευμένο εξάρτημα υλικού** το οποίο μπορεί να χρησιμοποιηθεί για **την αξιόπιστη παρακολούθηση των ασθενών και να εισαγάγει τα αρχεία ποιότητας στο blockchain.** Το **Bowhead** είναι μια άλλη πρωτοβουλία που ενδιαφέρεται να χρησιμοποιήσει μια συνιστώσα υλικού για να τροφοδοτήσει αξιόπιστες πληροφορίες σε ένα blockchain [67].

Άλλες εφαρμογές ηλεκτονικών ιατρικών φακέλων που βασίζονται σε blockchain είναι η **MedBlock** [82]**,** η **BlockHIE** , η **FHIRChain** [83], και η **MeDShare** [84].

3.2.2.1. Λύσεις για την ασφάλεια των ιατρικών δεδομένων στους Ιατρικούς Φακέλους.

Περιγραφή και ανάλυση λύσεων

Στην παρούσα υποενότητα συνίστανται ορισμένα κρυπτογραφικά συστήματα που έχουν ως στόχο την ενίσχυση της ασφάλειας και της εγκυρότητας των αποθηκευμένων ιατρικών δεδομένων του blockchain που είναι αποθηκευμένα στο block-based των ηλεκτονικών ιατρικών αρχείων. Αναλυτικότερα έχει προταθεί μια μέθοδος ελέγχου πρόσβασης που βασίζεται σε blockchain και χρησιμοποιεί **μετασχηματισμό διακριτού μήκους κύματος** και **γενετικό αλγόριθμο για τη βελτιστοποίηση της απόδοσης του συστήματος**[85].

Μια ακόμα λύση είναι η δημιουργία ενός σχήματος υπογραφής στην οποία ο ασθενής να είναι σε θέση να υποστηρίξει ένα μήνυμα που θα προστεθεί στο blockchain με βάση τα χαρακτηριστικά του μηνύματος, χωρίς να αποκαλύπτει καμία ευαίσθητη πληροφορία. Αυτό το πρωτόκολλο αποδεικνύεται ότι αντιστέκεται στην επίθεση αθέμιτης σύμπραξης και ότι είναι ασφαλές από υπολογιστική άποψη[86]. Με κρυπτογράφηση βάσει χαρακτηριστικών ,κρυπτογράφηση με βάση της ταυτότητα και

βάση ταυτότητας υπογραφής προτείνεται να χρησιμοποιηθεί από το blockchain στο χώρο της υγείας[87].

Άλλες προτάσεις σχετικές με την ασφάλεια των ηλεκτρονικών ιατρικών αρχείων βασίζονται σε blockchain που περιλαμβάνουν σχέδια διαχείρισης κλειδιών[88]. Έχει προταθεί για την προστασία της ιδιωτικής ζωής, ένα ασφαλές και προστατευμένο ιδιωτικό απόρρητο σύστημα ηλεκτρονικών ιατρικών αρχείων το οποίο χρησιμοποιεί **ιδιωτικά μπλοκ** και **κοινοπραξίες** για να αποθηκεύσει τα δεδομένα των ασθενών [89]. Το σύστημα αυτό βασίζεται στην ασύμμετρη κρυπτογράφηση, αλλά εφαρμόζει και μηχανισμούς για τη διεξαγωγή δοκιμών συμμόρφωσης για τη διασφάλιση της διαθεσιμότητας του συστήματος. Προτάθηκε επίσης μια πλατφόρμα διατήρησης της ιδιωτικής ζωής, που χρησιμοποιεί κρυπτογραφικές λειτουργίες για την εξακρίβωση της ταυτότητας των δεδομένων των ασθενών σε συστήματα ιατρικών αρχείων που βασίζονται σε blockchain[68].

Τέλος, υποδεικνύεται μια αρχιτεκτονική που ονομάζεται **Healthcare Data Gateway** (HDG) για εφαρμογές ιατρικών αρχείων που βασίζονται σε blockchain και επιτρέπει στους ασθενείς να κατέχουν, να ελέγχουν και να επιλέγουν πώς θα μοιράζονται τα δεδομένα τους με τρόπο που προστατεύεται η ιδιωτικότητα τους[90]. Σχετική αρχιτεκτονική προτείνεται για τη διαχείριση και την ανταλλαγή ιατρικών δεδομένων ασθενών με διαβήτη χρησιμοποιώντας συμβάσεις blockchain πολλαπλών υπογραφών για την επίτευξη του ελέγχου πρόσβασης και ιδιωτικού απορρήτου των δεδομένων [91].

Δεδομένου ότι οι λύσεις αυτές αναπτύσσονται παράλληλα και ελλείψει προτύπων, αναδύεται ένα νέο πρόβλημα διαλειτουργικότητας. Η **QBRICS** και η **Nuco** (Aion) έχουν ξεκινήσει έργα για την ανάπτυξη τεχνολογιών βασισμένων σε blockchain για να μεταφράσουν και να παγιώσουν πληροφορίες από πολλαπλές πηγές για την ανασυγκρότηση των δεδομένων ασθενών σε κατακερματισμένες πλατφόρμες.

3.2.3 Εφαρμογές Blockchain στην οδοντιατρική βιομηχανία.

Περιγραφή πρωτοβουλίας Dentacoin

Η **Dentacoin** είναι μια πρωτοβουλία που στοχεύει στη χρήση τεχνολογίας blockchain για να συνδέσει τους οδοντιάτρους, τους ασθενείς και τους προμηθευτές (κατασκευαστές και εργαστήρια) παγκοσμίως[67]. Η πρώτη φάση του έργου τους ήταν η υλοποίηση μιας πλατφόρμας αναθεώρησης που βασίζεται στην αμετάβλητη αποκέντρωση των μπλοκ αλυσίδων και στη διαφάνεια και την αξιοπιστία των έξυπνων συμβολαίων που συνδέονται με το blockchain για τη δημιουργία εμπιστοσύνης στη διαδικασία αναθεώρησης. Οι επιθυμητές ενέργειες, όπως η σύνταξη μιας επισκόπησης, επιβραβεύονται με τη μεταφορά **κρυπτονομίσματος** στον ασθενή, η οποία στη συνέχεια μπορεί να χρησιμοποιηθεί για την αγορά οδοντιατρικών υπηρεσιών από συμμετέχοντες ιατρούς. Οι οδοντίατροι ανταμείβονται για τη συμμετοχή τους μέσω της πρόσβασης σε έρευνα αγοράς και κρυπτογράφησης αποδεκτών από τους κατασκευαστές.

Προτεινόμενη λύση βασισμένη σε τεχνολογία Blockchain

Η Dentacoin ασχολείται με την ανάπτυξη μιας οικονομίας όπου μεταξύ των συμμετεχόντων μερών δεν απαιτούνται πρόσθετοι διαμεσολαβητές για τη διαχείριση των αλληλεπιδράσεων μεταξύ των επιμέρους τμημάτων του δικτύου. Αξίζει να σημειωθεί ότι αυτή η προσπάθεια τεχνολογίας blockchain ήδη διαθέτει δύο κλινικές αποδεικτικών ιδεών που δέχονται πληρωμές στο νόμισμα Dentacoin .Οι μελλοντικές φάσεις του σχεδίου του προγράμματος Dentacoin θα χρησιμοποιήσουν τη στρατηγική κινήτρων για να ενθαρρύνουν τους ασθενείς να εκπαιδεύονται για την οδοντιατρική περίθαλψη, να συνάπτουν ασφαλιστικές συμβάσεις μεταξύ ασθενών και οδοντιάτρων, που να επιβραβεύουν τους ασθενείς που εκτελούν ελάχιστη οδοντιατρική συντήρηση και να χρησιμεύουν ως ιατρικός φάκελος ασθενούς. Οι δημιουργοί της Dentacoin επέλεξαν να εφαρμόσουν ένα **δημόσιο blockchain** επειδή θεώρησαν ότι ένα πιο συγκεντρωτικό ιδιωτικό blockchain θα ήταν λιγότερο αξιόπιστο λόγω του πιο περιορισμένου αριθμού των επαληθευτών που εξασφαλίζουν την πιστότητα των συναλλαγών.

3.2.4 Εφαρμογές Blockchain σε Βιοιατρική έρευνα και εκπαίδευση.

Περιγραφή και ανάλυση πλεονεκτημάτων.

Σε κλινικές δοκιμές, το blockchain μπορεί να βοηθήσει στην **εξάλειψη της πλαστογραφίας των δεδομένων** και τον **αποκλεισμό των ανεπιθύμητων αποτελεσμάτων της κλινικής έρευνας**[92]. Το Blockchain διευκολύνει τους ασθενείς να επιτρέπουν την χορήγηση των δεδομένων τους για να χρησιμοποιούνται σε κλινικές δοκιμές λόγω της ανωνυμίας που παρέχει η κωδικοποίση των δεδομένων τους [93]. Επιπρόσθετα, η ιδιότητα του αμετάβλητου του blockchain πιστοποιεί την ακεραιότητα των δεδομένων που συλλέγονται μέσω blockchain για κλινική μελέτη. Όλα αυτά είναι μερικοί από τους λόγους blockchain αναμένεται να φέρει επανάσταση στη βιοϊατρική έρευνα[67].

Εφαρμοσμένα παραδείγματα

Το Blockchain παρέχει τη δυνατότητα βελτίωσης της διαδικασίας αξιολόγησης από ομοτίμους συμμετέχοντες των δημοσιεύσεων κλινικών ερευνών εξαιτίας του αποκεντρωμένου και αμετάβλητου χαρακτήρα του [94]. Μια άλλη πιθανή εφαρμογή [95] για τη χρήση blockchain είναι η κατασκευή ενός συστήματος που θα βασίζεται στην αξία, με βάση την ικανότητα και την προσφορά χωρίς να βασίζεται σε τρίτους. Παρομοίες, έρευνες παρουσιάζουν [96] πώς τα έξυπνα συμβόλαια στην πλατφόρμα blockbuster της Ethereum μπορούν να χρησιμοποιηθούν για τη βελτίωση της διαφάνειας των δεδομένων σε κλινικές δοκιμές. Η πλατφόρμα Ethereum χρησιμοποιείται επίσης για την υλοποίηση μιας άλλης λύσης που βασίζεται σε blockchain που προτείνεται να επισημαίνονται τα έγγραφα που ανακτώνται από βιοϊατρικές βάσεις δεδομένων[97].

3.2.5 Εφαρμογές Blockchain για την παρακολούθηση απομακρυσμένων ασθενών.

Περιγραφή και ανάλυση πλεονεκτημάτων

Ένας ακόμη τομέας στον οποίο μπορεί να φανεί χρήσιμη η τεχνολογία blockchain, είναι η **παρακολούθηση της υγείας απομακρυσμένων ασθενών**. Η απομακρυσμένη παρακολούθηση ασθενών περιλαμβάνει τη συλλογή βιοϊατρικών δεδομένων μέσω αισθητήρων στην περιοχή του σώματος και κινητές συσκευές ώστε να μπορούν να παρακολουθούν από απόσταση την κατάσταση του ασθενούς εκτός παραδοσιακών περιβάλλοντων υγειονομικής περίθαλψης όπως το νοσοκομείο. Το Blockchain έχει προταθεί ως μέσο για την αποθήκευση, την ανταλλαγή και την ανάκτηση των απομακρυσμένων βιοϊατρικών δεδομένων[98].

Εφαρμοσμένα παραδείγματα

Οι έξυπνες συμβάσεις στην πλατφόρμα **blockbuster της Ethereum** μπορούν να υποστηρίξουν εφαρμογές παρακολούθησης ασθενών σε πραγματικό χρόνο με τη δυνατότητα παροχής αυτοματοποιημένων παρεμβάσεων σε ασφαλές περιβάλλον.[99] Επίσης μια εφαρμογή βασισμένη στο **Hyperledger** δίνει τη δυνατότητα συλλογής και ανταλλαγής δεδομένων μεταξύ των φορέων της υγειονομικής περίθαλψης μέσω ενός κινητού. Παρομοίως, το blockchain χρησιμοποιείται για την ανάπτυξη συσκευής ενίσχυσης SMEAD με δυνατότητα κινητής τηλεφωνίας για την παρακολούθηση των ασθενών με διαβήτη. Ένα άλλο παράδειγμα εφαρμογής είναι οι συσκευές κινητών(smartphones) που χρησιμοποιήθηκαν με επιτυχία για τη μετάδοση δεδομένων σε μια εφαρμογή που βασίζεται σε blockchain Hyperledger Fabric[100]. Επίσης έχει αναπτυχθεί μια εφαρμογή όπου ένας κεντρικός παράγοντας που βασίζεται σε μπλοκ αλυσίδας πετυχαίνει ολοκληρωμένη ασφάλεια δεδομένων και ιδιωτικού απορρήτου για συνεχή παρακολούθηση απομακρυσμένων ασθενών [101].

3.2.6 Εφαρμογές Blockchain σε Ασφάλιση Υγείας.

Περιγραφή και ανάλυση πλεονεκτημάτων

Η επεξεργασία των ασφαλιστικών απαιτήσεων είναι ένας χώρος όπου η εφαρμογή του blockchain μπορεί να φανεί ιδιαίτερα βοηθητική[102]. Η διαδικασία της ασφάλισης της υγείας χρειάζεται τη διαφάνεια, την αποκέντρωση, την αμετάβλητη συμπεριφορά και τη δυνατότητα ελέγχου των αρχείων που είναι αποθηκευμένα σε ένα blockchain[93]. Εντούτοις, τα παραδείγματα υλοποιήσεων τέτοιων συστημάτων είναι πολύ περιορισμένα.

Εφαρμοσμένα παραδείγματα

Ένα καλό παράδειγμα διεκπεραίωσης των **ασφαλιστικών απαιτήσεων** στην υγειονομική περίθαλψη είναι **το MIStore** το οποίο είναι ένα πακέτο ιατροφαρμακευτικής ασφάλισης που βασίζεται σε σύστημα blockchain και αναπτύσσεται σε πλατφόρμα του Ethereum [103]. Επιπλέον, μια πρωτοβουλία μιας εταιρείας με την επωνυμία **Pokitdok** στοχεύει να συνεργαστεί με την Intel για να χτίσει ένα blockchain-based σύστημα που θα διευκολύνει την επίλυση των ασφαλιστικών απαιτήσεων στην υγειονομική περίθαλψη [67].

3.2.7 Εφαρμογές Blockchain στις Αναλύσεις Δεδομένων Υγείας.

Περιγραφή και ανάλυση πλεονεκτημάτων

Το Blockchain παρέχει επίσης μια μοναδική ευκαιρία **να αξιοποιήσει τη δύναμη των άλλων αναδυόμενων τεχνολογιών** όπως οι τεχνικές μεταφοράς μάθησης για την πραγματοποίηση προγνωστικών αναλύσεων των δεδομένων της υγειονομικής περίθαλψης και να προωθήσει την έρευνα στον τομέα της ιατρικής ακριβείας [104]. Αυτή η χρήση του μπλοκ αλυσίδας παρέχει έναν ολοκληρωμένο οδικό χάρτη για το πώς μπορεί αυτό να πραγματοποιηθεί[94],[105]. Τέλος έχει διεξαχθεί πειραματική έρευνα στην οποία το blockchain χρησιμοποιείται στην αρχιτεκτονική για την ταξινόμηση της αρρυθμίας [106].

3.2.8 Εφαρμογές Blockchain στη Ψηφιακή Ιατρική και στην παροχή φροντίδας.

Εφαρμοσμένο παράδειγμα

Η **Patientory** απευθύνεται σε ασθενείς, κλινικούς ιατρούς και οργανισμούς φροντίδας υγείας προσφέροντας μια πλατφόρμα η οποία επιτρέπει την πρόσβαση, την αποθήκευση και την ασφαλή μεταφορά πληροφοριών, βελτιώνοντας την συνεργασία των οργανισμών ενώ επιβεβαιώνει και την ασφάλεια των δεδομένων[107]. Η πλατφόρμα αποτελείται από δύο υπομονάδες μια για τους ιατρικούς επαγγελματίες και μία για τους απλούς χρήστες , από τις οποίες μόνο η δεύτερη έχει κυκλοφορήσει σε μια πρώτη πειραματική έκδοση. Οι υποστηριζόμενες προδιαγραφές περιλαμβάνουν ένα επίπεδο δεδομένων βασισμένο σε Blockchain, το οποίο υποστηρίζει διανεμημένες βάσεις δεδομένων,ως μόνιμο ιστορικό όλων των συμβάντων και ασφαλή πρόσβαση στα δεδομένα. Επιπλέον, περιέχουν διαχειριστές κλειδιών και κρυπτογραφικές τεχνικές οι οποίες συνδέουν με ασφάλεια το blockchain backend του συστήματος με τον χρήστη. Απαιτεί τη χρήση μιας εφαρμογής για κινητά με λογισμικό iOS, η οποία αποτελεί τη διεπαφή των απλών χρηστών και τη χρήση μιας εφαρμογής σε υπολογιστή, για τους ιατρικούς επαγγελματίες, ή οποία προσφέρει λειτουργίες διαχείρισης γραφείου.

Πλεονεκτήματα χρήσης της παλτφόρμας Patientory

Τα πλεονεκτήματα που παρέχει η πλατφόρμα Patientory είναι ότι ενισχύει την εφαρμογή κινητών συσκευών για τους χρήστες. Ακόμη, επιτρέπει την συλλογή των ιατρικών πληροφοριών των χρηστών όπως και ολοκληρου του ιατρικού ιστορικού δίνοντας τη δυνατότητα μεταφοράς των πληροφοριών αυτών σε συγγενεις και ιατρικούς συμβούλους. Μελλοντικά θα δίνεται η δυνατότητα απόκτησης ενός καινούριου κρυπτονομίσματος, το οποίο θα χρησιμοποιείται σε συναλλαγές μέσα στην εφαρμογή και θα υπάρχει εφαρμογή για τους κλινικούς οργανισμούς και τους γιατρούς.που θα προσφέρει όλες τις δυνατότητες που περιέχονται σε συνηθισμένες εφαρμογές διοίκησης και οργάνωσης ιατρείων, όπως ημερολόγια, ηλεκτρονικές συνταγογραφήσεις και αυτόματες ειδοποιήσεις. Τέλος ,θα προσφέρει τη δυνατότητα πρόσβασης στις πληροφορίες των χρηστών που τις μοιράζονται μαζί τους, όπως ιατρικά ιστορικα και τη δυνατότητα ανταλλαγής μηνυμάτων με τους ασθενείς τους.

Εφαρμοσμένο παράδειγμα

Ακόμα ένα εφαρμοσμένο παράδειγμα αποτελεί η πλατφόρμα **Bowhead health,** η οποία έχει σκοπό τη συλλογή των ιατρικών ιστορικών των χρηστών αλλά και την καθημερινή παρακολούθηση των συνηθειών τους και της υγείας τους με σκοπό τη εξατομικευμένη προσφορά φροντίδας υγείας μέσω συμπληρωμάτων διατροφής και

φαρμάκων[108]. Ο σχεδιασμός της εφαρμογής είναι έντονα συνδεδεμένος με τη παιχνιδοποίηση(gamification), μέσω συστημάτων ψυχολογικής επιβράβευσης αλλά και οικονομικής υποστήριξης μέσω ενός κρυπτονομίσματος. Οι υποστηριζόμενες προδιαγραφές περιλαμβάνουν ένα επίπεδο βάσης δεδομένων βασισμένο σε Blockchain, το οποίο υποστηρίζει διανεμημένες βάσεις δεδομένων, μόνιμο ιστορικό όλων των συμβάντων και ασφαλή πρόσβαση στα δεδομένα. Επιπλέον περιέχει κρυπτονόμισμα το οποίο χρησιμοποιείται για συναλλαγές μες την εφαρμογή. Το gamification αποτελεί αναπόσπαστο μέρος της εφαρμογής των χρηστών, ειδικά στη συμμετοχή σε βάθος χρόνου. Η διατήρηση του backend της πλατφόρμας έχει διατεθεί σε τρίτες εταιρείες χάρη των δυνατοτήτων της τεχνολογίας blockchain και των κρυπτονομισμάτων χωρίς επιπλέον κόστος. Τέλος ,περιέχονται αυτόματα φυσικά μηχανήματα που αναλύουν την υγεία των χρηστών.

Πλεονεκτήματα χρήσης της παλτφόρμας Bowhead health

Τα πλεονεκτήματα μιας τέτοιας εφαρμογής είναι ότι το κόστος της διατήρησης του backend μέρους της εφαρμογής μειώνεται σημαντικά και ότι η καθημερινή επαφή του χρήστη με την εφαρμογή, φροντίζει την συνεχόμενη χρήση της. Ακόμα ένα χρήσιμο στοιχείο της εφαρμογής αυτής είναι η ιδιαίτερα λεπτομερής εκτέλεση του συστήματος παρακολούθησης του ιστορικού του blockchain. Επιπλέον ,τα δεδομένα αποθηκεύονται σε ένα σύστημα βασισμένο σε τεχνολογία blockchain,το οποίο επιτρέπει στους χρήστες την παρακολούθηση και τον έλεγχο όλου του ιστορικού τους. Τέλος δίνεται ενσωματωμένη η δυνατότητα αγοράς συγκεκριμένων προϊόντων από το Amazon , με τα κρυπτονομίσματα που κερδίζουν οι χρήστες απλά με την χρήση της εφαρμογής. Στο μέλλον η διατήρηση του backend της εφαρμογής θα μπορεί να αναληφθεί από τρίτους οργανισμούς με αντάλλαγμα, το καινούργιο κρυπτονόμισμα. Αυτή η ανάθεση είναι δυνατή μόνο χάρη στην τεχνολογία blockchain. Επιπλέον οι πληροφορίες που μαζεύονται θα χρησιμοποιούνται για την πώληση συμπληρωμάτων διατροφής και φαρμάκων μέσω αυτόματων πωλητών σε δημοφιλή σημεία στην πόλη αλλά και στο σπίτι.

3.2.9 Εφαρμογές Blockchain στις Αναλύσεις υγειονομικής περίθαλψης.

Εφαρμοσμένο παράδειγμα

Η πλατφόρμα **Doc.ai** βασίζεται στα δεδομένα τα οποία της προσφέρουν οι ίδιοι οι χρήστες, όπως δεδομένα από κλινικές, γενετικούς ελέγχους αλλά και δεδομένα για την προσωπική τους υγεία ,όπως η διατροφή και η άσκηση. Τα δεδομένα αυτά χρησιμοποιούνται μέσω μιας αναλυτικής μονάδας , η οποία χρησιμοποιεί τεχνητή νοημοσύνη για να δώσει προβλέψεις και αναλύσεις για την υγεία των ίδιων των χρηστών [109]. Επιπλέον, δίνει απόλυτο έλεγχο στους ίδιους τους χρήστες για τη χρήση των προσωπικών δεδομένων τους, μέσω ενός συστήματος το οποίο λειτουργεί σε συνέπεια με όλους τους σχετικούς νόμους περί διαχείρισης δεδομένων, εξασφαλίζοντας ταυτόχρονα την ασφάλειά τους, μέσω της τεχνολογίας blockchain. Τέλος με τη χρήση αυτού του συστήματος προσφέρεται στους χρήστες η δυνατότητα να συμμετάσχουν, μέσω των ανωνυμοποιημένων δεδομένων τους, σε ιατρικές έρευνες σε όλον τον κόσμο.

Στόχος της πλατφόρμας αυτής είναι η εξέλιξη του επιπέδου ανάλυσης των δεδομένων σε ένα δίκτυο εκπαίδευσης τεχνητής νοημοσύνης στο οποίο θα συμμετάσχουν οι

χρήστες μέσω ενός νέου κρυπτονομίσματος. Τα υποστηριζόμενα πρότυπα που περιλαμβάνουν είναι βασισμένα σε τεχνολογία Blockchain, η οποία βοηθάει στην συγκέντρωση όλων των δεδομένων όπως και στην ασφαλή πρόσβαση των χρηστών μέσω ενός κινητού. Περιλαμβάνει, ένα επίπεδο ανάλυσης δεδομένων το οποίο βασίζεται σε τεχνολογίες τεχνητής νοημοσύνης, ώστε μέσω της ανάλυσης τους, να προσφέρει χρήσιμες πληροφορίες για την υγεία των ασθενών.

Πλεονεκτήματα

Τα πλεονεκτήματα της προσπάθειας αυτής, είναι ότι προσφέρονται έτοιμα, τυποποιημένα δεδομένα σε ερευνητές. Αυτό αποτελεί ένα σημαντικό στοιχείο γιατί η απόκτηση ιατρικών δεδομένων είναι συνήθως δύσκολη και χρονοβόρα. Επιπλέον, ο σχεδιασμός της εφαρμογής στο κινητό είναι ιδιαίτερα καλός. Η ανάλυση ιατρικών δεδομένων έχει ήδη αποδειχθεί από άλλες υπηρεσίες (όπως αυτές που αναλύουν ιατρικά δεδομένα) ότι ενδιαφέρουν σημαντικά τους χρήστες και χρησιμοποιούνται εκτεταμένα.

3.2.10 Εφαρμογές Blockchain σε ιατρικές συσκευές και ασφάλεια Internet of Things (IoT).

Εφαρμοσμένα παραδείγματα

Ένα μεγάλο μέρος τις ιατρικής φροντίδας στο οποίο δεν δίνεται αρκετή προσοχή είναι ο εξοπλισμος και οι εγκαταστάσεις που χρησιμοποιούνται. Στην ασφάλεια και λειτουργία αυτών των συσκευών επικεντρώνεται η **Neuromesh**[110]. Η Neuromesh μπορεί να εφαρμοστεί σε κάθε είδους εγκαταστάσεις στις οποίες εφαρμόζονται τοίχοι προστασίας κατά κακόβουλων λογισμικών. Συγκεντρώνει δεδομένα τα οποία αναλύονται μέσω νευρωνικών δικτύων και deep learning αλγόριθμων (βαθιάς μάθησης αλγορίθμων), οι αλγόριθμοι αυτοί προειδοποιούν για ύποπτες ή λανθασμένες λειτουργίες του συστήματος. Επιπλέον προσφέρει και ένα δίκτυο που συνδέεται με τις ιατρικές, οικιακές αλλά και νοσοκομειακές συσκευές. Η σύνδεση αυτή επιτρέπει την ασφαλή εικοσιτετράωρη παρακολούθηση των συσκευών. Τις ίδιες λειτουργίες μπορεί να προσφέρει και σε κυκλώματα κλειστών καμερών αλλά και συστήματα βιομηχανικού ελέγχου. Οι υποστηριζόμενες προδιαγραφές είναι βασισμένες σε Blockchain, το οποίο προσφέρει ασφάλεια αληθινού χρόνου στα δίκτυα και επιτρέπει τη λειτουργία των δικτύων ελέγχου των συσκευών με ασφαλή τρόπο. Επιπλέον περιέχει ένα επίπεδο μηχανικής μάθησης το οποίο αναλύει τις λειτουργίες του δικτύου και παράγει αναφορές για την λειτουργία τους. Τέλος, περιέχει ένα επίπεδο παρακολούθησης και ελέγχου ιατρικών και άλλων συσκευών .

Πλεονεκτήματα

Τα πλεονεκτήματα της συγκεκριμένης εφαρμογής είναι ότι η τεχνολογία της μπορεί να εφαρμοστεί σε πολλές διαφορετικές βιομηχανίες και εταιρείες, ενώ υπάρχουν χρήσεις ακόμα και σε οικιακές συσκευές.

3.2.11 Εφαρμογές Blockchain στις Αλυσίδες εφοδιασμού και στη συμβουλευτική.

Εφαρμοσμένα παραδείγματα

Η εταιρία **Chronicled** προσφέρει πολλές υπηρεσίες σε εταιρείες και βιομηχανίες. Μερικές από αυτές τις υπηρεσίες περιλαμβάνουν διαχείριση αποθεμάτων , διαχείριση λογαριασμών των πολιτών, εκθέσεις ελέγχων από τρίτες εταιρείες ,διαχείριση εσόδων και τέλος μπορεί να χρησιμοποιηθεί ως αρχείο όλων των συμβάντων που συμβαίνουν στην αλυσίδα εφοδιασμού[111]. Όλες αυτές οι υπηρεσίες έχουν χρήσεις σε πολλές διαφορετικές βιομηχανίες αλλά ιδιαίτερα οι μεγάλες εταιρείες ιατρικής φροντίδας, μπορούν να έχουν μεγάλα κέρδη από τη χρήση των εφαρμογών αυτών. Όλες αυτές οι υπηρεσίες βασίζονται σε blockchain δίκτυα τα οποία επικεντρώνονται σε διαφορετικούς τομείς όπως σε παρακολούθηση αποθεμάτων είτε σε βεβαιώσεις για την ασφαλή μεταφορά αρχείων. Τα περισσότερα από τα πρωτόκολλα και χαρακτηριστικά της εφαρμογής βασίζονται σε τεχνολογία blockchain για τη χρήση τους.

Πλεονεκτήματα χρήσης της πλατφόρμας Chronicled

Ένα θετικό στοιχείο της εφαρμογής Chronicled είναι η επικοινωνία με δημοφιλείς τεχνολογίες για ταυτοποίηση προϊόντων και ελέγχου για την αυθεντικότητά τους, όπως QR codes, barcodes και λοιπά. Επιπλέον περιλαμβάνει πλατφόρμες για ενδοεταιρική διαχείριση χρηστών και παρέχει ασφαλή επικοινωνία ανάμεσα στους χρήστες. Δύναται να αποτελέσει ένα αρχείο και ιστορικό για προϊόντα, μέλη και συμβάντα της εταιρείας. Η μέθοδος αυτή απαιτεί αρκετά μεγάλο προϋπολογισμό. Επιπλέον, διαθέτει μεγάλη ποικιλία από διαφορετικές υπηρεσίες δίνοντας την επιλογή για συγκεκριμένες λύσεις.

Η εταιρία **Consensys**, έχει ως στόχο να φέρει την τεχνολογία blockchain στις επιχειρήσεις [112]. Συνδυάζοντας τις δυνατότητες της τεχνολογίας blockchain με ειδικούς σε πολλούς τομείς που ασχολούνται με τη λειτουργία διαφόρων υπηρεσιών, μπορούν να προσφέρουν προσωποποιημένες λύσεις ανά επιχείρηση. Οι ειδικοί μπορεί να είναι από μηχανικοί μέχρι χρηματοοικονομικοί επαγγελματίες. Όλοι οι οργανισμοί που λειτουργούν στον τομέα της υγείας μπορούν να χρησιμοποιήσουν και να επωφεληθούν από τις υπηρεσίες αυτές. Συγκεκριμένα η Consensys , δημιουργεί πλατφόρμες σε συνεργασία με τις εταιρίες βασισμένες σε blockchain ,ανάλογα την εφαρμογή τους. Επίσης μπορεί να βοηθήσει στην δημιουργία ενός νέου κρυπτονομίσματος, το οποίο είναι βασικό για τη λειτουργία των εφαρμογών και μπορεί να χρησιμοποιηθεί για χρηματοδότηση εταιρειών. Τα περισσότερα από τα πρωτόκολλα και τις υπηρεσίες της εφαρμογής βασίζονται σε τεχνολογία blockchain για τη χρήση τους και συγκεκριμένα είναι βασισμένα στην τεχνολογία ethereum. Τέλος, περιλαμβάνει ειδίκευση σε ανάπτυξη κρυπτονομισμάτων και διαχείρισή τους σε διαφορετικούς τομείς λειτουργίας των επιχειρήσεων.

3.2.12 Εφαρμογές Blockchain στην Υγειονομική υποδομή δεδομένων.

Εφαρμοσμένο παράδειγμα

Η εταιρεία **Deepmind-Health**, προσφέρει πολλές υπηρεσίες σε εταιρείες και στο δημόσιο σύστημα φροντίδας υγείας του Ηνωμένου Βασιλείου(NHS)[113].Παρέχει πολλές υπηρεσίες με σκοπό τη βελτίωση της λειτουργίας των νοσοκομείων και μια απο αυτές είναι το Verifiable Data Audit. Χρησιμοποιεί εργαλεία που ελέγχουν τη χρήση των δεδομένων ώστε να επιβεβαιώνεται ότι η χρήση αυτών γίνεται στο πλαίσιο των νόμων και της ηθικής. Η εταιρία deepmind ήδη προσφέρει υπηρεσίες που λειτουργούν με δεδομένα από τα νοσοκομεία. Το σύστημα verifiable data audit θα καταγράφει κάθε συναλλαγή και τη χρήση των δεδομένων σε ένα σύστημα blockchain, βεβαιώνοντας το αληθινό ιστορικό για την χρήση της κάθε πληροφορίας.

Πλεονεκτήματα

Σε αντίθεση με πιο συνηθισμένες αποκεντροποιημένες εφαρμογές blockchain, δε χρειάζεται η προστασία του συστήματος με proof-of-work αλγόριθμους, επειδή τα ιδρύματα που συμμετέχουν το εμπιστεύονται ήδη ,έτσι το σύστημα δουλεύει πιο γρήγορα και οικονομικά. **Οι υποστηριζόμενες τεχνολογίες** παρέχουν ένα επίπεδο δεδομένων βασισμένο σε Blockchain, το οποίο προσφέρει ασφάλεια σε επιθέσεις και τροποποιήσεις, δίνοντας τη δυνατότητα διατήρησης ενός αδιάλλακτου ιστορικού. Η μη χρήση των proof-of-work αλγόριθμων στο blockchain, οδηγεί σε πιο γρήγορη, οικονομική και τελικά πιο ασφαλή χρήση του δικτύου. Εφαρμόζεται ήδη σε υπάρχοντα συστήματα επικοινωνίας μεταξύ εταιρειών και ιδρυμάτων φροντίδας υγείας.

3.2.13 Εφαρμογές Blockchain σε άλλους τομείς.

Υπάρχουν δύο περιπτώσεις που δεν μπορούν να ταξινομηθούν σε καμία κατηγορία των προσδιορισμένων περιπτώσεων χρήσης blockchain, αλλά παρουσιάζουν σχετικές προοπτικές έρευνας. Η μία εστιάζει στον **εντοπισμό των μετρήσεων για την αξιολόγηση εφαρμογών υγειονομικής περίθαλψης** που βασίζονται σε blockchain [114] ενώ η άλλη περίπτωση [115] **μελετά τις κοινωνικο-τεχνικές συνέπειες της χρήσης τεχνολογίας blockchain στην υγειονομική περίθαλψη.**

3.3 Εφαρμογές Blockchain σε ερευνητικά ευρωπαικά έργα.

3.3.1 Εφαρμογές Blockchain σε υποδομές τεχνολογίας πληροφοριών και επικοινωνίας.

Περιγραφή

Η ψηφιακή επανάσταση και ιδιαίτερα τα μεγάλα δεδομένα (big data) και η τεχνητή νοημοσύνη(AI), προσφέρουν νέες ευκαιρίες για τη βελτίωση της υγειονομικής περίθαλψης. Ωστόσο, ενέχουν κινδύνους για την ασφάλεια των ευαίσθητων κλινικών δεδομένων που είναι αποθηκευμένα σε υποδομές Τεχνολογίας Πληροφοριών και Επικοινωνίας(ΤΠΕ), κρίσιμης σημασίας για την υγειονομική περίθαλψη. Συγκεκριμένα, η ανταλλαγή δεδομένων μέσω του Διαδικτύου θεωρείται απαραίτητη και αποτελεί ένα οδόφραγμα που παρεμποδίζει τις μεγάλες ιατρικές καινοτομίες που βασίζονται σε δεδομένα.

Εφαρμοσμένο παράδειγμα

Το μετασχηματιστικό χαρακτηριστικό της **FeatureCloud**, έχει ως στόχο την ελαχιστοποίηση του δυναμικού του εγκλήματος στον κυβερνοχώρο και θα δώσει τη δυνατότητα πρώτης διασφάλισης διασυνοριακών συνεργατικών προσπαθειών εξόρυξης δεδομένων [116]. Συλλογικά, η ιδιαίτερα διεπιστημονική κοινοπραξία του έργου, από την τεχνολογία της πληροφορίας στην ιατρική, καλύπτει όλες τις πτυχές, την αξιολόγηση των κινδύνων στον κυβερνοχώρο, τις νομικές παραμέτρους και τις διεθνείς πολιτικές, την ανάπτυξη της ομοσπονδιακής τεχνολογίας τεχνητής νοημοσύνης (AI) σε συνδυασμό με το Blockchaining, τις συσκευές, την αξιολόγηση και τη μετάφραση στην κλινική πρακτική, την εμπορική εκμετάλλευση, καθώς και τη διάδοση και τη μεγιστοποίηση της εμπιστοσύνης των ασθενών.

Πλεονεκτήματα

Το FeatureCloud θα εφαρμοστεί σε ένα εργαλείο λογισμικού για τη σημαντική μείωση των κινδύνων στον κυβερνοχώρο, για την υποδομή υγειονομικής περίθαλψης, χρησιμοποιώντας την πρώτη παγκόσμια προσέγγιση απόρρητου προς αρχιτεκτονική, η οποία έχει δύο βασικά χαρακτηριστικά ότι δεν διαβιβάζονται ευαίσθητα δεδομένα μέσω οποιωνδήποτε διαύλων επικοινωνίας, και ότι τα δεδομένα δεν αποθηκεύονται σε ένα κεντρικό σημείο. Η ενοποιημένη μηχανική μάθηση (για εξοικονόμηση δεδομένων που προστατεύει την ιδιωτική ζωή) ενσωματωμένη στην τεχνολογία Blockchain (για αμεταβλητότητα και διαχείριση των δικαιωμάτων των ασθενών) θα εφαρμόσει με ασφάλεια την τεχνολογία AI επόμενης γενιάς για ιατρικούς σκοπούς.Είναι σημαντικό να δοθούν στους ασθενείς αποτελεσματικά μέσα ανάκλησης προηγούμενης συγκατάθεσης ανά πάσα στιγμή. Η πρωτοποριακή νέα υποδομή για cloud AI ανταλλάσσει μόνο τις μαθησιακές αναπαραστάσεις μοντέλων που είναι ανώνυμα από προεπιλογή.

3.3.2 Εφαρμογές Blockchain για την ασφάλεια της ιδιωτικότητας των ιατρικών δεδομένων.

Εφαρμοσμένο παράδειγμα

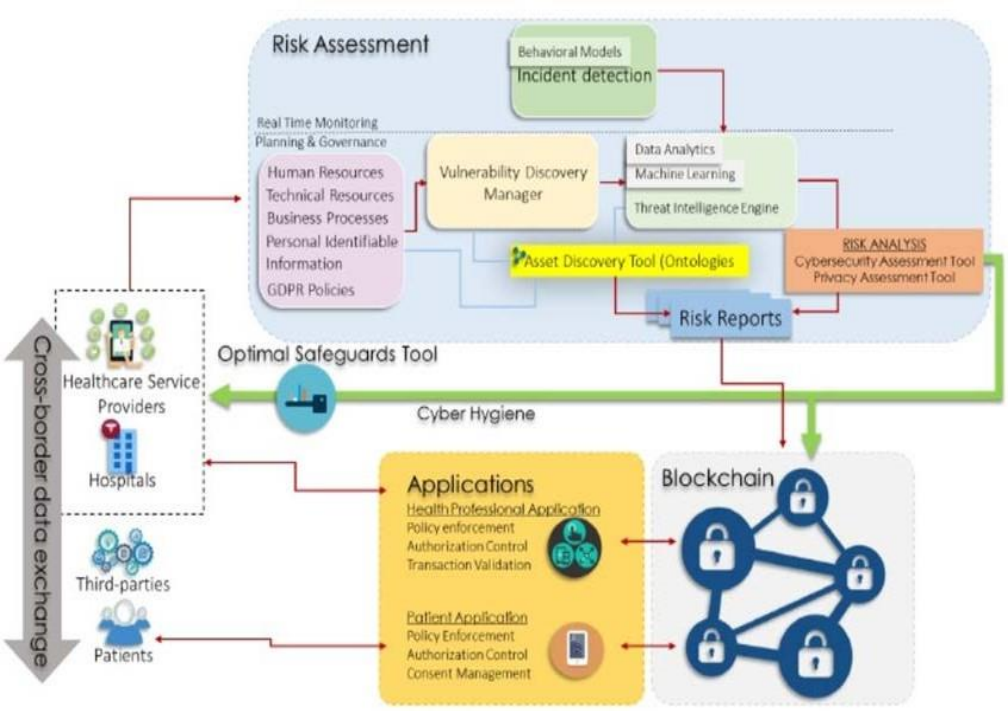
Η εφαρμογή **CUREX** στοχεύει στην προστασία της εμπιστευτικότητας και της ακεραιότητας των δεδομένων υγείας, δημιουργώντας μια ευέλικτη πλατφόρμα προσαρμοσμένη στην εκάστοτε κατάσταση[117]. Επιτρέπει σε έναν πάροχο υγειονομικής περίθαλψης να εκτιμήσει τους ρεαλιστικούς κινδύνους στον κυβερνοχώρο και τους κινδύνους ιδιωτικής ζωής στους οποίους εκτίθεται και προτείνει μαθηματικά βέλτιστες στρατηγικές αντιμετώπισης αυτών των κινδύνων, με διασφαλίσεις προσαρμοσμένες ειδικά για κάθε επιχειρηματική περίπτωση και εφαρμογή.

Η CUREX στοχεύει να είναι απόλυτα συμβατή με το GDPR. Στον πυρήνα της, μια αποκεντρωμένη αρχιτεκτονική, ενισχυμένη με μια ιδιωτική τεχνολογία Blockchain, διασφαλίζει την ακεραιότητα της διαδικασίας εκτίμησης κινδύνου και όλων των συναλλαγών των δεδομένων που συμβαίνουν μεταξύ του ποικίλου φάσματος εμπλεκομένων ενδιαφερομένων. Προβλέπεται ότι το CUREX θα επηρεάσει την ευρωπαϊκή αγορά, αναπτύσσοντας μία από τις πρώτες πλατφόρμες διαχείρισης

κινδύνων στο πλαίσιο του GDPR. Στόχος της πλατφόρμας αυτής είναι να παρασχεθούν τα εργαλεία για την αξιολόγηση των κινδύνων στον κυβερνοχώρο, που συνδέονται με την ανταλλαγή δεδομένων στο χώρο της υγείας. Να παρασχεθεί επιπλέον, ένα εργαλείο υποστήριξης αποφάσεων για τη χάραξη βέλτιστης ασφάλειας στον κυβερνοχώρο και προστασίας της ιδιωτικής ζωής. Τελικός στόχος είναι η παράδοση μιας πλατφόρμας βασισμένης σε τεχνολογία Blockchain για την ενίσχυση της εμπιστοσύνης στην ανταλλαγή δεδομένων για την υγεία και η ενίσχυση της ασφάλειας στον κυβερνοχώρο για τις οργανώσεις υγειονομικής περίθαλψης. Αξιοποιώντας καινοτόμες μεθόδους για την μοντελοποίηση δεδομένων υγείας, την ανακάλυψη ευπάθειας στις πληροφορίες που απειλούν την ασφάλεια στον κυβερνοχώρο, τις μεθοδολογίες αξιολόγησης κινδύνου ιδιωτικού απορρήτου, καθώς και την τεχνολογία αιχμής σε συστήματα Blockchain για τα δεδομένα υγείας, το CUREX στοχεύει στη διευκόλυνση της ασφαλούς και εξουσιοδοτημένης ανταλλαγής δεδομένων υγείας.

Η πλατφόρμα CUREX αποτελείται από μια σειρά στοιχείων (εργαλεία, εφαρμογές, τεχνολογία Blockchain). Αυτά τα στοιχεία, καθώς και οι αλληλεξαρτήσεις τους παρουσιάζονται παρακάτω και απεικονίζουν την αρχιτεκτονική του βασικού συστήματος που πρέπει να βελτιωθεί περαιτέρω κατά τη διάρκεια του έργου. Η ενσωματωμένη πλατφόρμα CUREX θα βασίζεται σε μια ευέλικτη και επιδέξια αρχιτεκτονική που αποτελείται από τέσσερα ξεχωριστά επίπεδα.

Το πρώτο επίπεδο αποτελεί η ανίχνευση οφέλους, το οποίο περιλαμβάνει τα εργαλεία και τις μεθοδολογίες που εξετάζουν τη χαρτογράφηση των δεδομένων, των τεχνικών και των ανθρώπινων πόρων σε οντολογικά μοντέλα.Το δεύτερο είναι το επίπεδο πληροφοριών (νοημοσύνης) για απειλές, το οποίο περιλαμβάνει την ανακάλυψη τρωτών σημείων και την ανάλυση διαφόρων πόρων που θα εντοπίσουν πιθανές απειλές.Το επόμενο επίπεδο περιλαμβάνει τη διαχείριση των κινδύνων, το οποίο αναλύει και δημιουργεί στοιχεία ποσοτικοποιημένων κινδύνων που λαμβάνονται υπόψη τόσο στην ασφάλεια του κυβερνοχώρου όσο και στην προστασία της ιδιωτικής ζωής. Επιπλέον αξιοποιούνται και στην εύρεση βέλτιστων διασφαλίσεων και τεχνικών βελτίωσης της υγιεινής στον κυβερνοχώρο με βάση τα συστήματα υποστήριξης αποφάσεων.Τέλος υπάρχει το επίπεδο ενίσχυσης της εμπιστοσύνης, το οποίο περιλαμβάνει την ανάπτυξη ενός Blockchain που βασίζεται στην επιχειρηματική συναίνεση, το οποίο θα αποθηκεύει τις αναφορές για τα συγκεντρωμένα ρίσκα από τα προηγούμενα επίπεδα και θα ενσωματώνει τα εργαλεία CUREX και τις εφαρμογές τελικών χρηστών σε μια πλήρως συμβατή πλατφόρμα με το GDPR.



Εικόνα 21. Απεικόνιση της εφαρμογής CUREX και των εργαλείων της[118].

Πλεονεκτήματα

Το CUREX επεκτείνεται πέρα από τα τεχνικά μέτρα και δίνει έμφαση και στη βελτίωση της υγιεινής στον κυβερνοχώρο μέσω της κατάρτισης και της ευαισθητοποίησης του προσωπικού υγειονομικής περίθαλψης. Η αξιοποίησή του επικεντρώνεται στην εξαιρετικά δύσκολη κατάσταση της (διασυνοριακής) ανταλλαγής δεδομένων για την υγεία, η οποία καλύπτει τη διασυνοριακή κινητικότητα των ασθενών, την απομακρυσμένη υγειονομική περίθαλψη και την ανταλλαγή δεδομένων για έρευνα. Το CUREX θα επιτύχει τους στόχους του με την παροχή εξουσιοδότησης στα ιδρύματα υγειονομικής περίθαλψης να αξιολογούν αποτελεσματικά και με ακρίβεια τους κινδύνους για την ασφάλεια του κυβερνοχώρου και την ιδιωτική ζωή, που συνδέονται με την ανταλλαγή δεδομένων για την υγεία και να ενισχύουν την προστασία του κυβερνοχώρου και της ιδιωτικής ζωής. Αξιοποιώντας τις τεχνολογίες που αναπτύχθηκαν για το γνωστό έργο H2020 MyHealth - MyData (MH - MD), το CUREX θα προσφέρει ένα επιχειρησιακό δίκτυο ασφαλούς σχεδιασμού, βασισμένο στις τεχνολογίες και το λογισμικό Blockchain του MH - MD, που θα παρέχει λειτουργίες υπευθυνότητας και ελεγκτικής ικανότητας.

3.3.3 Εφαρμογές Blockchain για την Ανάλυση του δικτύου του Αθλητισμού σε πραγματικό χρόνο.

Περιγραφή προβλήματος

Η αυξανόμενη παρουσία και χρήση φορητών συσκευών ανίχνευσης και ποσοτικοποιημένων φορητών συσκευών και η αύξηση των ενσωματωμένων και φορητών υπολογιστών, αναμένεται να φέρει την επόμενη επανάσταση του διαδικτύου

των αθλημάτων, βελτιώνοντας την φυσική κατάσταση, την απόδοση της υγείας, την παραγωγικότητα και την ασφάλεια, καθώς και τη δημιουργία νέων θέσεων εργασίας και το άνοιγμα νέων αγορών. Παρ 'όλα αυτά, σε ευρωπαϊκό επίπεδο, υπάρχει αναγνωρισμένη έλλειψη ερευνητών υψηλής εξειδίκευσης, επιστημόνων και μηχανικών με μεταβιβάσιμες δεξιότητες και επιχειρηματική εμπειρία, εκπαιδευμένων στην κατασκευή πλατφορμών πληροφορικής .

Εφαρμοσμένο παράδειγμα

Η κοινοπραξία **RAIS**, αποτελούμενη από 6 δικαιούχους και 7 πλήρως οργανωμένους εταίρους, φιλοδοξεί να δημιουργήσει τον πυρήνα μιας εύφορης πολυεπιστημονικής κοινότητας έρευνας και καινοτομίας με ισχυρή επιχειρηματική κουλτούρα που θα προωθήσει φορητές συσκευές ανίχνευσης, ποσοτικοποιημένες αυτο-συσκευές και συνοδευτικά μεσαία λογισμικά, τεχνολογίες εξόρυξης και ανάλυσης μεγάλων δεδομένων, που απαιτούνται για τη συλλογή ευρέος φάσματος πληροφοριών σχετικά με τον αθλητισμό και την ευεξία των χρηστών [119]. Η RAIS φιλοδοξεί να παράσχει σε 14 διδακτορικούς φοιτητές μια παγκόσμια εκπαίδευση σε ένα ευρύ φάσμα θεμάτων που δημιουργούν μια εύφορη διεπιστημονική κοινότητα έρευνας και καινοτομίας που θα προωθήσει τη **φορητή τεχνολογία** δηλαδή φορητές συσκευές ανίχνευσης, ποσοτικά προσδιορισμένες συσκευές και συνοδευτικό μεσαίο λογισμικό. Ακόμα θα προωθεί το **Block-chain Powered IoT,** δηλαδή αποκεντρωμένες πλατφόρμες IoT τροφοδοτούμενες με Blockchain (δημιουργώντας εκατοντάδες δισεκατομμύρια συναλλαγές ανά ημέρα) για την εξόρυξη των μεγάλων δεδομένων (Big Data) .Τέλος θα ενισχύει την **ανάλυση Edge πραγματικού χρόνου** και την πρόβλεψη μοντέλων για την καταγραφή ενός ευρέος φάσματος δεδομένων και τάσεων που σχετίζονται με τον αθλητισμό .

Οι υποψήφιοι της RAIS θα λάβουν εμπεριστατωμένη έρευνα «πρακτικής εξάσκησης» καθώς και σημαντική έκθεση σε μη ακαδημαϊκά περιβάλλοντα μέσω βιομηχανικών αποσπάσεων. Το πλούσιο σύνολο εκδηλώσεων σε όλο το δίκτυο, συμπεριλαμβανομένων διαδραστικών online σεμιναρίων, επιχειρηματικών εκδηλώσεων, hackathons, σεμιναρίων και διασκέψεων, θα διασφαλίσει τη συνεργασία των υποτρόφων ως μια σταθερή ομάδα και την ανάπτυξη ατόμων ως εμπειρογνώμονες. Το δίκτυο κατάρτισης RAIS θα χρηματοδοτήσει 14 Ευρωπαϊκές Εταιρίες Έρευνας για τον ύπνο (ESRs), 3 εργαστήρια, 1 εκδήλωση Hackathlon, 1 εκδήλωση επιχειρηματικότητας, 3 θερινά σχολεία και ένα τελικό συνέδριο. **Για να επιτύχει αυτό το στόχο, η RAIS θα επικεντρωθεί στην** ανάπτυξη νέων τεχνολογιών σε αναλυτικά στοιχεία Edge σε μεγάλα δεδομένα, στην επεξεργασία ροής δεδομένων, στην κατανεμημένη και αποκεντρωμένη Μηχανική Μάθηση και στην τεχνολογία Blockchain **Οι ερευνητικές περιοχές** που εστιάζει η RAIS είναι η κατανεμημένη υποδομή ανίχνευσης & δικτύωση για το διαδίκτυο του αθλητισμού, η ασφάλεια,η προστασία της ιδιωτικής ζωής και η εμπιστοσύνη για φορητές συσκευές,η εξόρυξη δεδομένων και ανάλυση Edge για τον αθλητισμό και την ευημερία και οι προγνωστικές αναλύσεις για το διαδίκτυο της εξαγωγής γνώσεων για αθλήματα.

Πλεονεκτήματα

Το κύριο προτέρημα της RAIS είναι ότι δύναται να παρέχει εκπαίδευση παγκόσμιας κλάσης για την επόμενη γενιά ερευνητών και μηχανικών με έμφαση σε έναν ισχυρό συνδυασμό προηγμένης κατανόησης τόσο σε θεωρητικές όσο και σε πειραματικές

προσεγγίσεις, μεθοδολογίες και εργαλεία που απαιτούνται για την ανάπτυξη αποκεντρωμένων, κλιμακωτών και ασφαλών υποδομών και πλατφόρμων συλλογικής ανίχνευσης

3.3.4 Εφαρμογές Blockchain για την προστασία των νοσοκομειακών και υγειονομικών υποδομών.

Περιγραφή προβλήματος

Η υγειονομική περίθαλψη εξελίσσεται ολοένα και περισσότερο προς την ψηφιοποίηση, από την ανάπτυξη ηλεκτρονικών ιατρικών αρχείων έως την τηλεπισκόπηση και τηλε-εμπειρογνωμοσύνη και τα συνδεδεμένα αντικείμενα αυξάνονται. Είναι προφανές ότι οι απειλές και οι ενδεχόμενες ζημίες σε κρίσιμες υποδομές υγειονομικής περίθαλψης που οφείλονται σε κυβερνοεπιθέσεις, απαιτούν την ενίσχυση των χαρακτηριστικών ασφάλειας της βιομηχανίας.

Εφαρμοσμένο παράδειγμα

Το **PANACEA** αποτελεί μια προσπάθεια απόδειξης ότι η ασφάλεια πηγάζει από την ατομική ευαισθητοποίηση για τις ευπάθειες του κυβερνοχώρου, επιτρέποντας στις μονάδες υγειονομικής περίθαλψης να εκτιμούν τη φύση και τη σοβαρότητα μιας απειλής και αποφασίζοντας με βιώσιμο τρόπο να υιοθετήσουν στρατηγικές για την ενίσχυση της ετοιμότητας και της αντίδρασής της [120]. Το PANACEA θα παράσχει μια Δυναμική Πλατφόρμα Διαχείρισης Κινδύνου, μέσω δοκιμών αξιολόγησης και διείσδυσης που υποστηρίζουν την ανταλλαγή πληροφοριών σε όλα τα οργανωτικά ορία. Τα δεδομένα θα συλλέγονται όχι μόνο από τις τοπικές τεχνολογίες πληροφοριών (IT), αλλά και από απομακρυσμένη υποδομή και από συσκευές IoT που βασίζονται στην πλατφόρμα κοινής χρήσης πληροφοριών (SISP). Από την μια πλευρά, το PANACEA θα αντιμετωπίσει την ανάγκη να ανταποκριθεί γρήγορα σε ένα περίπλοκο, πολυδιάστατο τοπίο απειλής στον κυβερνοχώρο, από την άλλη πλευρά, θα προσθέσει την ανάγκη επαγγελματιών στον τομέα της ασφάλειας στον κυβερνοχώρο με υψηλό βαθμό εξειδίκευσης, ώστε να μειωθούν οι κίνδυνοι στον κυβερνοχώρο για την υγειονομική περίθαλψη.

Πλεονεκτήματα

Το έργο αυτό έχει πολλαπλά πλεονεκτήματα , ένα απο αυτά θα είναι η ενίσχυση της θέσης της Ευρώπης ως βασικού φορέα παροχής ασφάλειας για συστήματα πληροφορικής της υγειονομικής περίθαλψης. Ακόμα θα ενισχύσει τη συνεχή ανάπτυξη και βελτίωση της πλήρως προσαρμοσμένης διαχείρισης ταυτότητας και των ασφαλών λύσεων διαχείρισης δεδομένων για την Υγειονομική Περίθαλψη. Θα συντελέσει στην ανάπτυξη νέων προϊόντων, όπως οι συνδεδεμένες πλατφόρμες διαχείρισης αντικειμένων, για τη διασφάλιση των συνδεδεμένων ιατρικών συσκευών. Επιπλέον θα επιταχύνει την ανάπτυξής της στο οικοσύστημα Υγείας για να προσελκύσει περισσότερους πελάτες και να αυξήσει το μερίδιο αγοράς της, με στόχο να φτάσει σε έσοδα ύψους 2 δισ. δολαρίων έως το 2020. Επιπρόσθετα θα επεκτείνει και ενισχύσει το ευρωπαϊκό δίκτυο των ενδιαφερομένων και των υπευθύνων λήψης αποφάσεων. Επιπλέον, θα ενεργοποιήσει μια αντιπροσωπευτική κοινότητα

ενδιαφερομένων και θα προσδιορίσει μια πορεία βιωσιμότητας για το όραμα της PANACEA. Τέλος, η PANACEA παρέχει ένα ολοκληρωμένο εργαλείο για την ασφάλεια στον κυβερνοχώρο, παρέχοντας μια ολιστική προσέγγιση για τα ιδρύματα υγειονομικής περίθαλψης, που αποτελείται από ένα συνδυασμό τεχνικών (πλατφόρμες SW για δυναμική αξιολόγηση κινδύνων, ασφαλή ανταλλαγή πληροφοριών και ασφάλεια βάσει σχεδιασμού) και μη τεχνικών (διαδικασίες, μοντέλα διοίκησης, εργαλεία συμπεριφοράς των ανθρώπων). Συγκεντρωτικά στα πλαίσια της υλοποίησης του έργου θα υπάρξει ανάπτυξη και επικύρωση εργαλείων για τη δυναμική αξιολόγηση και μετριασμό των κινδύνων εργαλείων για την ασφαλή κοινή χρήση των πληροφοριών, εργαλείων για την ασφάλεια του συστήματος από τον σχεδιασμό του και πιστοποίηση**,** εργαλείων ταυτοποίησης και ελέγχου ταυτότητας**,** εκπαιδευτικών πακέτων για την ασφάλεια του κυβερνοχώρου στον τομέα της υγείας**,** εργαλείων για ανθεκτικότητα διοίκησης και κατευθυντήριες γραμμές εφαρμογής για την υιοθέτηση λύσεων για την ασφάλεια στον κυβερνοχώρο**.**

3.3.5 Εφαρμογές Blockchain στη διανομή των ιατρικών δεδομένων.

Εφαρμοσμένο παράδειγμα

Το **MyHealth - MyData (MH-MD)** είναι μια ενέργεια έρευνας και καινοτομίας του προγράμματος Horizon 2020 που στοχεύει στην ουσιαστική αλλαγή του τρόπου με τον οποίο μοιράζονται τα ευαίσθητα δεδομένα [121]. Το MH-MD πρόκειται να είναι το πρώτο ανοιχτό δίκτυο βιοϊατρικής πληροφόρησης με επίκεντρο τη σύνδεση μεταξύ οργανώσεων και ατόμων, ενθαρρύνοντας τα νοσοκομεία να αρχίσουν να διαθέτουν ανώνυμα τα δεδομένα για ανοιχτή έρευνα, παροτρύνοντας τους πολίτες να γίνουν οι τελικοί ιδιοκτήτες και ελεγκτές των δεδομένων υγείας τους. Το MH-MD προορίζεται να γίνει μια πραγματική αγορά πληροφοριών, βασισμένη σε νέους μηχανισμούς εμπιστοσύνης και σχέσεις αξίας μεταξύ πολιτών της Ευρωπαικής Ένωσης , νοσοκομείων, ερευνητικών κέντρων και επιχειρήσεων. Το My Health - My Data (MH-MD) στοχεύει στη χρήση της τεχνολογίας Blockchain για να επιτρέπει την αποθήκευση και τη μετάδοση των ιατρικών δεδομένων με ασφάλεια και αποτελεσματικότητα.

Πλεονεκτήματα

Η ανάπτυξη μιας πλατφόρμας δεδομένων για την υγεία, βασισμένης σε τεχνολογία Blockchain έχει ως αποτέλεσμα να επιτρέπει στους πολίτες της ΕΕ να διαχειρίζονται και να μοιράζονται με ασφάλεια τα κλινικά δεδομένα τους, για τη βελτίωση της ποιότητας της υγειονομικής περίθαλψης και την προώθηση κλινικής έρευνας και καινοτομίας. Το My Health - My Data στοχεύει να δημιουργήσει μια πλατφόρμα που βασίζεται σε τεχνολογία Blockchain, ένα ψηφιακό βιβλίο όπου οι συναλλαγές δεδομένων είναι ορατές σε ολόκληρο το δίκτυο των ενδιαφερομένων, ελαχιστοποιώντας κάθε πιθανότητα ανεπιθύμητης χρήσης. Μια διεπαφή δυναμικής συγκατάθεσης, θα επιτρέψει στους χρήστες να δίδουν, να αρνούνται ή να ανακαλούν τη συγκατάθεσή τους για πρόσβαση σε δεδομένα, για διαφορετικές χρήσεις, σύμφωνα με τις προτιμήσεις τους. Το έργο θα διερευνήσει τη σκοπιμότητα των εφαρμογών αξιοποιώντας την αξία των μεγάλων συνόλων κλινικών δεδομένων, ιδιαίτερα τις

προηγμένες αναλύσεις δεδομένων, τις μηχανές ανάκτησης ιατρικών σχολιασμών και τα μοντέλα συγκεκριμένων ασθενών για φυσιολογική πρόβλεψη.

3.3.6 Εφαρμογές Blockchain στην Προστασία των Υδάτινων Υποδομών ενάντια στις κυβερνο-φυσικές Απειλές.

Περιγραφή προβλήματος

Οι υποδομές ύδατος είναι απαραίτητες για την ανθρώπινη κοινωνία, τη ζωή και την υγεία. Μπορούν να απειληθούν από φυσικές ή κυβερνο απειλές με σοβαρές κοινωνικές συνέπειες. Για να αντιμετωπιστεί αυτό, το πρόγραμμα **STOP-IT** που χρηματοδοτείται από το H2020 συγκεντρώνει μια ισχυρή ομάδα 23 εταίρων, συμπεριλαμβανομένων επιχειρήσεων κοινής ωφέλειας για νερό, κατασκευαστές βιομηχανικών τεχνολογιών, μικρομεσαίες επιχειρήσεις υψηλής τεχνολογίας και κορυφαίους προμηθευτές έρευνας και ανάπτυξης από όλη την Ευρώπη. Μαζί η κοινοπραξία αναπτύσσει λύσεις στις πιό πιεστικές απειλές κατά τη διάρκεια των επόμενων τεσσάρων ετών[122].

Εφαρμοσμένο παράδειγμα

Η ομάδα **STOP-IT** εντοπίζει τους τρέχοντες και τους μελλοντικούς κινδύνους και αναπτύσσει ταυτόχρονα ένα πλαίσιο διαχείρισης όλων των κινδύνων για τη φυσική και κυβερνητική προστασία κρίσιμων υποδομών ύδρευσης. Η πρόληψη, η ανίχνευση, η αντίδραση και ο μετριασμός των σχετικών κινδύνων σε στρατηγικό, τακτικό και επιχειρησιακό επίπεδο σχεδιασμού θα ληφθούν υπόψη για τη δημιουργία τεχνολογιών, εργαλείων και οδηγιών, που θα ενσωματωθούν σε μια ολοκληρωμένη, κλιμακούμενη, προσαρμόσιμη και αρθρωτή πλατφόρμα λογισμικού. Το κύριο αποτέλεσμα STOP-IT θα είναι μια ολοκληρωμένη, αρθρωτή πλατφόρμα που υποστηρίζει το στρατηγικό / τακτικό προγραμματισμό, τη λήψη επιχειρησιακών αποφάσεων σε πραγματικό χρόνο και την εκ των υστέρων αξιολόγηση των βασικών τμημάτων της υποδομής ύδρευσης.

Πλεονεκτήματα

Οι λύσεις του STOP-IT βασίζονται σε βελτιωμένες ώριμες τεχνολογίες μέσω του συνδυασμού και της ενσωμάτωσής τους (συμπεριλαμβανομένων των συστημάτων δημόσιας προειδοποίησης, των έξυπνων κλειδαριών) και νέες τεχνολογίες των οποίων το επίπεδο ετοιμότητας της τεχνολογίας (TRL) θα αυξηθεί (συμπεριλαμβάνονται υπηρεσίες κατά της απειλής στον κυβερνοχώρο, ασφαλείς ασύρματες μονάδες επικοινωνίας αισθητήρων, τεχνολογίες ανίχνευσης ανωμαλιών με γνώμονα το περιβάλλον, στρατηγικές ελέγχου ανθεκτικότητας σε σφάλματα για ενσωματωμένους αισθητήρες SCADA, προστασία όγκου δεδομένων αισθητήρων σε πραγματικό χρόνο μέσω συστημάτων Blockchain, αδειοδότηση κινητήρων, ανίχνευση ανωμαλιών στον άνθρωπο με τη χρήση νέων μεθόδων ηλεκτρονικής όρασης και WiFi και αποτελεσματικοί αλγόριθμοι ανίχνευσης μόλυνσης νερού).Η πλατφόρμα θα είναι κλιμακούμενη (κλιμάκωση από μικρές επιχειρήσεις σε μεγάλες) , προσαρμόσιμη (συμπεριλαμβανομένων των διαφόρων ενοτήτων που καλύπτουν διαφορετικές ανάγκες, με επέκταση για μελλοντικές ενότητες) και ευέλικτη (οι

διαχειριστές των υπηρεσιών ύδρευσης μπορούν να αποφασίσουν πώς να την χρησιμοποιήσουν και θα χρησιμοποιείται από εμπειρογνώμονες, αρχάριους ή ακόμα και μη τεχνικό προσωπικό.

4.

4.1 Μελλοντικές εξελίξεις της τεχνολογίας Blockchain στο χώρο της υγείας.

Η αυξημένη διαθεσιμότητα δεδομένων και οι πρόσφατες εξελίξεις στην τεχνητή νοημοσύνη παρουσιάζουν πρωτοφανείς ευκαιρίες στην υγειονομική περίθαλψη και μείζονες προκλήσεις για τους ασθενείς και τους προγραμματιστές. Οι καινοτόμες τεχνικές μάθησης μετατρέπουν οποιαδήποτε δεδομένα του ατόμου σε ιατρικά δεδομένα και μετασχηματίζουν απλές εικόνες προσώπου και βίντεο σε ισχυρές πηγές δεδομένων για προγνωστικές αναλύσεις. Επί του παρόντος, οι ασθενείς δεν έχουν τον έλεγχο πρόσβασης στα ιατρικά τους αρχεία και δεν γνωρίζουν την πραγματική αξία των δεδομένων που έχουν.

Σε αυτό το κεφάλαιο, παρουσιάζεταιι μια επισκόπηση των τεχνολογιών τεχνητής νοημοσύνης και μπλοκ αλυσίδων επόμενης γενιάς που παρέχουν καινοτόμες λύσεις στη βιοϊατρική έρευνα. Επιπλέον με τη χρήση των παραπάνω στοιχείων δίνεται η δυνατότητα σε ασθενείς με νέα εργαλεία να ελέγχουν και να επωφελούνται από τα προσωπικά τους δεδομένα καθώς και να υποβάλλονται κίνητρα για τη συνεχή παρακολούθηση της υγείας τους. Επιπρόσθετα, εισάγονται νέες ιδέες για την αξιολόγηση των προσωπικών αρχείων, συμπεριλαμβανομένης της συνδυαστικής, χρονικής και σχέσης αξίας των δεδομένων. Παρουσιάζεται επίσης ένας χάρτης πορείας για ένα αποκεντρωμένο οικοσύστημα δεδομένων προσωπικού χαρακτήρα που επιτρέπει την ανάπτυξη νέων μεθόδων για την ανακάλυψη φαρμάκων, την ανάπτυξη βιοδεικτών και την προληπτική υγειονομική περίθαλψη. Μια ασφαλής και διαφανής κατανεμημένη αγορά προσωπικών δεδομένων που χρησιμοποιεί τεχνολογίες blockchain μπορεί να είναι σε θέση να επιλύσει τις προκλήσεις που αντιμετωπίζουν οι ρυθμιστικές αρχές και να επιστρέψει στον ιδιώτη τον έλεγχο των προσωπικών δεδομένων, συμπεριλαμβανομένων των ιατρικών αρχείων.

4.2 Μελλοντικές εφαρμογές της τεχνολογίας Blockchain στο χώρο της υγείας.

4.2.1 Εφαρμογές Blockchain στη δημιουργία νέων κρυπτονομισμάτων.

Πλεονεκτήματα blockchain

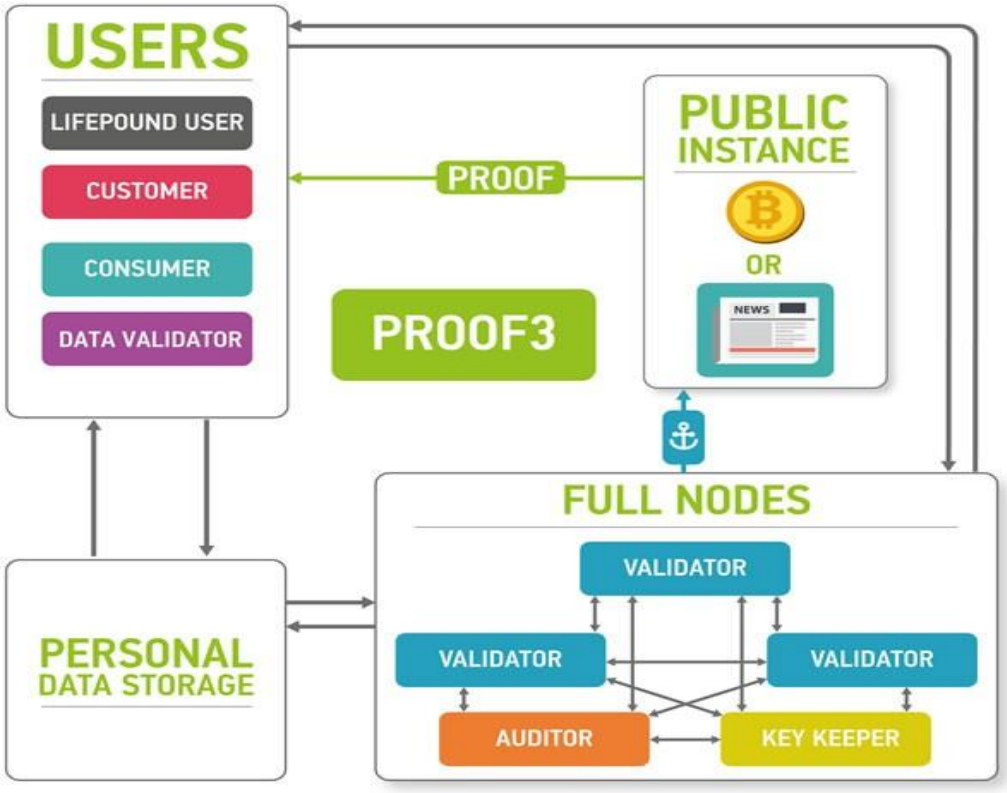
Η διαδικασία απόκτησης δεδομένων μπορεί να απλοποιηθεί δραματικά με τη χρήση ενός συστήματος βασισμένο σε blockchain. Ένα τέτοιο σύστημα επιτρέπει στον χρήστη την άμεση φόρτωση των δεδομένων του απευθείας στο σύστημα και την

αδειοδότηση χρήσης των δεδομένων αυτών από όποιους συμμετέχοντες αυτός επιθυμεί. Επίσης, μπορεί να εγγυηθεί την παρακολούθηση όλων των δραστηριοτήτων χρήσης των δεδομένων. Η υπόσχεση μιας τέτοιας λύσης είναι η δυνατότητα των χρηστών να αποκτήσουν την κυριότητα των δεδομένων τους και να αποκτήσουν πρόσβαση στα προνόμια που μπορούν να τους προσφέρουν .Επιπλέον, επιτρέπεται οι ίδιοι να μπορούν να διαχειριστούν π.χ. να πουλήσουν τα δεδομένα τους απευθείας στους καταναλωτές. Ωστόσο, η ανταλλαγή δεδομένων με ένα νόμισμα ενδέχεται να είναι προβληματική για πολλούς λόγους, μεταξύ των οποίων είναι η ανάγκη πραγματοποίησης μεγάλου αριθμού μικροτραπεζών σε πολλές χώρες και μεταξύ μεγάλου αριθμού διαφορετικών τύπων συμμετεχόντων στην αγορά δεδομένων.

Μελλοντικά παραδείγματα

Μια νέα μορφή κρυπτογραφικού νομίσματος ονομάζεται **LifePound** και μπορεί είτε να δημιουργηθεί είτε να εξορύσσεται με την τοποθέτηση των δεδομένων στην αγορά [105]. Η LifePound χρησιμοποιεί blockchain για την διευκόλυνση των συναλλαγών και την εισαγώγη νέων προγραμμάτων παροχής κινήτρων.

Η αρχιτεκτονική της προτεινόμενης πλατφόρ μας περιγράφεται στο παρακάτω σχήμα:



Εικόνα 22. Το οικοσύστημα της αγοράς LifePound [123].

Το οικοσύστημα της αγοράς αποτελείται από τέσσερα μέρη: μπλοκ αλυσίδα, αποθήκευση δεδομένων, τους χρήστες και τις δημόσιες εκδηλώσεις. Το blockchain χρησιμοποιείται για την επεξεργασία νέων μπλοκ συναλλαγών, την αποθήκευση και αποστολή κλειδιών και τον ίδιο τον έλεγχο. Η αποθήκευση δεδομένων περιέχει

κρυπτογραφημένα δεδομένα. Οι χρήστες στέλνουν και πωλούν τα δεδομένα τους χρησιμοποιώντας την αγορά (χρήστες), επικυρώνουν δεδομένα (επικυρώσεις δεδομένων), αγοράζουν προσωπικά ιατρικά δεδομένα (πελάτες) και χρησιμοποιούν το LifePound ως κρυπτονόμισμα (χρήστες LifePound). Το σύστημα δεν είναι πλήρως ανοιχτό και οι δημόσιες περιπτώσεις χρησιμοποιούνται σε κρυπτογραφικές αποδείξεις για τους χρήστες ώστε να εγγυώνται την ορθότητα λειτουργίας των αγορών.

Οι συμμετέχοντες και οι στόχοι τους.

Οι **χρήστες** της εφαρμογής αυτής μπορούν να διαχειρίζονται (να αποθηκεύουν και να πωλούν) τα βιοϊατρικά τους δεδομένα προκειμένου να λαμβάνουν προηγμένες εκθέσεις υγείας από τα αποτελέσματα της ανάλυσης δεδομένων. Οι χρήστες επιτρέπεται να διατηρούν τα δεδομένα τους ιδιωτικά και ασφαλιζόμενα. Επιπλέον μπορούν να παρέχουν πρόσβαση στα δεδομένα τους μόνο στους οργανισμούς τους οποίους επιλέγουν . Οι **πελάτες** προτίθενται να αγοράσουν τα δείγματα δεδομένων τα οποία συγκεντρώνονται από πολλούς χρήστες. Για να εξασφαλιστεί η ποιότητα των δεδομένων που παρέχονται από τους χρήστες, απαιτείται η επικύρωση των δεδομένων από εμπειρογνώμονες οι οποίοι είναι οι πρώτοι αγοραστές των δεδομένων. Οι **επικυρωτές δεδομένων** ελέγχουν την ποιότητα των δεδομένων και παρέχουν στους πελάτες την εγγύηση της εγκυρότητάς τους. Οι **χρήστες του LifePound** διαχειρίζονται την αγορά κρυπτογράφησης (πιθανώς χωρίς να υπάρχει αλληλεπίδραση με τα προσωπικά δεδομένα).

Τρόπος λειτουργίας

Οι αλληλεπιδράσεις στην αγορά καταχωρούνται σε blockchain με τη μορφή συναλλαγών. Το Blockchain δεν περιέχει καμία ανοιχτή προσωπική πληροφορία. Περιέχει κρυπτογραφικές συναρτήσεις που θα μπορούσαν να χρησιμοποιηθούν ως σφραγίδα ένδειξης χρόνου ενώ παρέχεται και ένα λογικό επίπεδο μη αποδοχής των ενεργειών που υπάρχουν στην αγορά. Η πρώτη ενέργεια επιτυγχάνεται με τη βοήθεια ενός blockchain anchoring[124] και άλλων τεχνικών χρονοσειρών[125]. Η τελευταία ενέργεια πραγματοποιείται με τη βοήθεια της ψηφιακής υπογραφής και ενός δημόσιου κλειδιού που βασίζεται σε ένα blockchain πιστοποίησης της συναλλαγής .

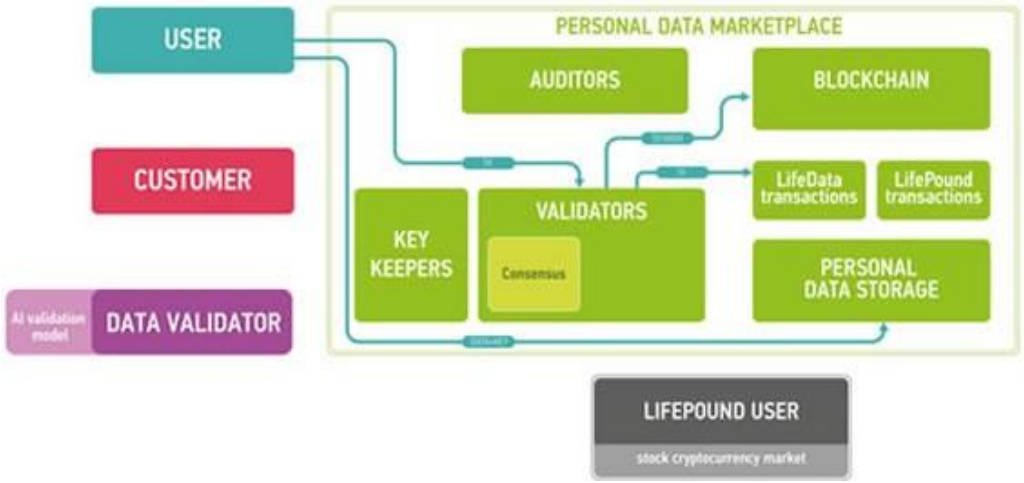
Οι πλήρεις κόμβοι Blockchain και το Storage Cloud είναι μέρη του οικοσυστήματος. Το Storage Cloud θα μπορούσε να είναι ένα υπάρχον αποθηκευτικό cloud, για παράδειγμα το Amazon Web Services , το οποίο επιτρέπει την κατασκευή εφαρμογών συμβατών με τον Νόμο περί φορητότητας και λογοδοσίας για την ασφάλιση υγείας (Health Insurance Portability and Accountability Act, HIPAA) ή η πλατφόρμα Google Cloud. Ένας από τους κύριους λόγους της αποθήκευσης σε cloud είναι η λύση της αποθήκευσης εκτός αλυσίδας που παρέχει και είναι ιδιαίτερα σημαντική ειδικά όταν πρόκειται για μεγάλα αρχεία βιοϊατρικών δεδομένων, όπου το μέγεθος ενός αρχείου θα μπορούσε να φθάσει τα 50 Mb. Η αποθήκευση σε cloud μπορεί να απαιτεί τον έλεγχο ταυτότητας για την πρόσβαση ανάγνωσης και εγγραφής σε δεδομένα, η οποία σε μια προτιμώμενη εγκατάσταση θα βασίζεται στο δημόσιο κλειδί που είναι εγκατεστημένο στο blockchain της αγοράς. Για να διασφαλιστεί η ασφάλεια και το απόρρητο του συστήματος, τα δεδομένα που μεταφορτώνονται από τους χρήστες στο χώρο αποθήκευσης του cloud θα είναι κρυπτογραφημένα χρησιμοποιώντας ένα σχήμα κρυπτογράφησης κατωφλίου[126]. Καθώς η τεχνολογία

αποθήκευσης θα ωριμάζει, μπορεί να είναι δυνατή η αντικατάσταση της αποθήκευσης του cloud με τα συστήματα προσωπικής αποθήκευσης, όπου όλα τα προσωπικά δεδομένα θα ανήκουν στο άτομο και επίσης θα βρίσκονται σε ατομική μονάδα αποθήκευσης. Τα άτομα ενδέχεται επίσης να είναι σε θέση να δανείζουν τα δεδομένα τους στα άλλα μέρη για εκπαιδευτικούς σκοπούς.

Οι κόμβοι του Blockchain θα πρέπει να είναι υπεύθυνοι οργανισμοί οι οποίοι θα έχουν πρόσβαση σε όλες τις πληροφορίες του blockchain. Διακρίνονται σε τρεις κατηγορίες, στους υπεύθυνους για την εξακρίβωση του Blockchain, οι οποίοι δεσμεύουν τα νέα μπλοκ με συναλλαγές στο blockchain ,τους ελεγκτές της αγοράς και τους διαχειριστές κλειδιών. Οι τελευταίοι διατηρούν τα κοινόχρηστα στοιχεία με ένα συγκεκριμένο πρόγραμμα κρυπτογράφησης κατωφλίου που είναι απαραίτητο για την αποκρυπτογράφηση δεδομένων του χρήστη στο χώρο αποθήκευσης. Σε μία πιθανή εγκατάσταση,τα κλειδιά μπορούν να περιλάμβάνουν κρυπτογραφικές ταυτότητες υποστηριζόμενες από ένα δημόσιο κλειδί (PKI) βασισμένο σε blockchain. Το γεγονός αυτό θα τους επέτρεπε να δημιουργήσουν αυθεντικά κανάλια επικοινωνίας με άλλους συμμετέχοντες του περιγραφόμενου πρωτοκόλλου για τη μετάδοση βασικών μεριδίων. Σε αυτή τη ρύθμιση, οι κατόχοι ενδέχεται να χρησιμοποιούν συνήθεις μηχανισμούς ασφαλείας για την εγγύηση της ασφάλειας των δεδομένων τους.

Ενέργειες του χρήστη του συστήματος.

Ο χρήστης επιλέγει τον τύπο δεδομένων και την τοπική διαδρομή χρησιμοποιώντας τη διεπαφή του συστήματος .Ο χρήστης κρυπτογραφεί τα δεδομένα χρησιμοποιώντας έναν συμμετρικό κρυπτογράφο. Η τεχνική μυστικής κοινής χρήσης του Shamir [127] [128] χρησιμοποιείται στη συνέχεια για να διαιρέσει το μυστικό κλειδί για να διανεμηθεί μεταξύ των κατόχων κλειδιών έτσι ώστε όλοι οι κάτοχοι K μαζί να είναι σε θέση να αποκρυπτογραφήσουν τα δεδομένα. Όπου το K είναι σταθερά μικρότερο από τον αριθμό των κλειστών κατόχων N. Η επιλογή της σταθερής K εξαρτάται από το μοντέλο ασφαλείας blockchain. Ο χρήστης διανέμει τα βασικά μερίδια μεταξύ των κατόχων κλειδιών, χρησιμοποιώντας ένα απευθείας κανάλι επικοινωνίας που έχει ταυτοποιηθεί με κάθε κάτοχο. Αφού ο χρήστης μεταφορτώσει τα κρυπτογραφημένα δεδομένα σε ένα cloud, θεωρούνται LifeData. Ο χρήστης δημιουργεί μια συναλλαγή για τη μεταφόρτωση των δεδομένων, προκειμένου να ειδοποιήσει τους συμμετέχοντες στο οικοσύστημα (ιδίως τους επικυρωτές δεδομένων) ότι έχει πραγματοποιηθεί η μεταφόρτωση. Η συναλλαγή περιέχει το δημόσιο κλειδί του χρήστη, τον τύπο δεδομένων και έναν σύνδεσμο στα δεδομένα του χώρου αποθήκευσης του cloud. Ο χρήστης υπογράφει τη συναλλαγή και την εκπέμπει στους κόμβους του blockchain . Η συναλλαγή περιλαμβάνεται στο blockchain μέσω ενός αλγόριθμου συναίνεσης. Το επόμενο στάδιο ,είναι η αγορά των δεδομένων αυτών από τους επικυρωτές .



Εικόνα 23. Παράδειγμα ροής εργασίας για χρήστες της αγοράς[123].

Ο χρήστης ανεβάζει δεδομένα και παίρνει το LifePounds ως ανταμοιβή , το ποσό εξαρτάται από την αξία των δεδομένων.

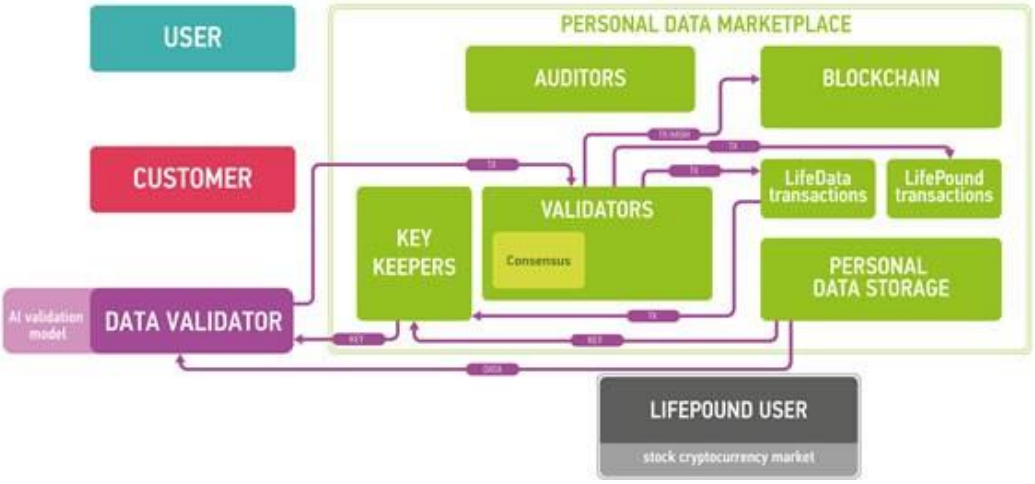
Ενέργειες του επικυρωτή του συστήματος.

Ο επικυρωτής δεδομένων έχει ως στόχο την έγκριση των δεδομένων. Επιλέγει τα μη έγκυρα δεδομένα και παράγει μια συναλλαγή για να τα αγοράσει για επικύρωση. Υπογράφει τη συναλλαγή και τη μεταδίδει στους κόμβους blockchain. Η συναλλαγή περιλαμβάνεται στο blockchain μέσω αλγόριθμου συναίνεσης. Εάν ο επικυρωτής διαθέτει τα LifePounds για την αγορά των δεδομένων για επικύρωση, τα LifePounds του επικυρωτή δεδομένων αποστέλλονται σε μια έξυπνη σύμβαση επικύρωσης και η ροή εργασίας συνεχίζεται. Διαφορετικά, ο επικυρωτής αποτυγχάνει να επικυρώσει τα δεδομένα και πηγαίνει στο αρχικό στάδιο.

Οι κάτοχοι των κλειδιών βλέπουν τις συναλλαγές επικύρωσης δεδομένων στο blockchain. Κάθε κάτοχος κλειδιού παραδίδει τα αποθηκευμένα κοινόχρηστα κλειδιά για κάθε κομμάτι δεδομένων στην παρτίδα στον επικυρωτή,μέσω ενός πιστοποιημένου καναλιού επικοινωνίας. Ο επικυρωτής μεταφορτώνει κρυπτογραφημένα δεδομένα από την αποθήκευση του cloud και μόλις λάβει αρκετά κοινόχρηστα κλειδιά από τους κατόχους κλειδιών, αποκρυπτογραφεί τα δεδομένα.

Το αποτέλεσμα είναι ένας φορέας των τιμών boolean, που σηματοδοτεί εάν τα αντίστοιχα κομμάτια των δεδομένων στην παρτίδα είναι έγκυρα ή άκυρα. Ο χρόνος επικύρωσης είναι περιορισμένος. Τα έξυπνα συμβόλαια για την επικύρωση δεδομένων έχουν ως προεπιλογή να θεωρούν ότι όλα τα δεδομένα στην παρτίδα είναι έγκυρα. Ο επικυρωτής διαμορφώνει και υπογράφει τη συναλλαγή για την επικύρωση των δεδομένων. Η συναλλαγή περιέχει κρυπτογραφικές συναρτήσεις για τα δεδομένα και για το αποτέλεσμα της επικύρωσης. Εάν το αποτέλεσμα για ένα συγκεκριμένο στοιχείο δεδομένων στην παρτίδα είναι "έγκυρο", τότε τα δεδομένα LifePounds διανέμονται μεταξύ των λογαριασμών των υποβαλόντων. Επιπλέον, τα επικυρωμένα δεδομένα διατίθενται προς πώληση στην πλατφόρμα. Ο επικυρωτής θα λάβει μέρος των εσόδων από τρίτους που θα αγοράσουν τα δεδομένα από την παρτίδα στο μέλλον . Εάν το αποτέλεσμα για ένα συγκεκριμένο στοιχείο δεδομένων στην παρτίδα είναι "μη έγκυρο", τότε τα LifePounds από το έξυπνο συμβόλαιο

επιστρέφονται στο λογαριασμό του επικυρωτή και τα δεδομένα δεν είναι διαθέσιμα προς πώληση στην πλατφόρμα.

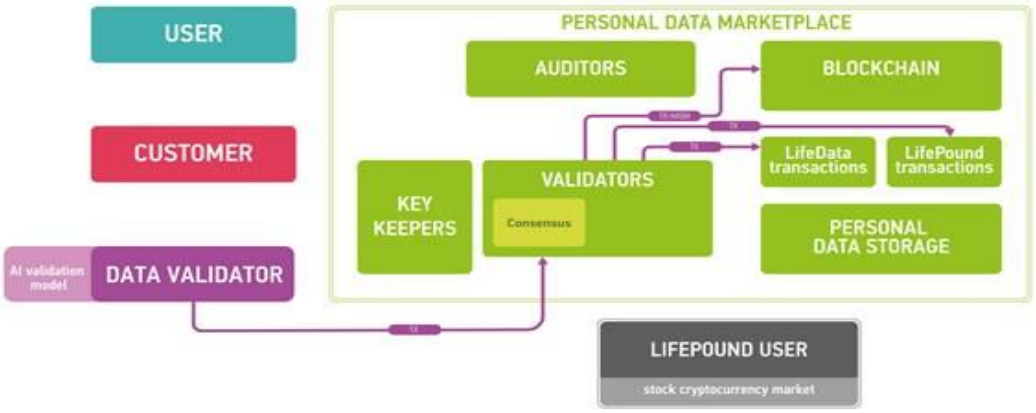


Εικόνα 24.Παράδειγμα της ροής εργασίας των επικυρωτών δεδομένων της αγοράς [105].

Οι επικυρωτές δεδομένων είναι αγοραστές ενδιάμεσων δεδομένων, οι οποίοι παρέχουν υπηρεσίες επικύρωσης στα ορυχεία Lifepounds.

Ενέργειες του πελάτη στο σύστημα.

Ο πελάτης επιλέγει τα επικυρωμένα δεδομένα και προτείνει μια συναλλαγή για να τα αποκτήσει .Ο πελάτης επικυρώνει τη συναλλαγή και την διανέμει στους κόμβους blockchain. Η συναλλαγή περιλαμβάνεται στο blockchain μέσω ενός αλγόριθμου συναίνεσης. Εάν ο πελάτης κατέχει την απαραίτητη ποσότητα LifePounds που απαιτείται για την απόκτηση των συγκεκριμένων δεδομένων, η ροή εργασίας συνεχίζεται. Διαφορετικά, ο πελάτης αδυνατεί να αγοράσει τα δεδομένα και η διαδικασία επιστρέφει στο αρχικό στάδιο. Οι κατόχοι κλειδιών βλέπουν μια συναλλαγή αγοράς δεδομένων που μπορεί να προβληθεί στο blockchain. Κάθε κάτοχος κλειδιού στέλνει τα κοινόχρηστα κλειδιά για όλα τα δεδομένα της συναλλαγής και τα μεταδίδει με ασφάλεια στον πελάτη (π.χ. μέσω ενός πιστοποιημένου καναλιού επικοινωνίας). Ο πελάτης κατεβάζει τα κρυπτογραφημένα δεδομένα από την αποθήκευση του cloud. Μόλις ο πελάτης λάβει αρκετά βασικά μερίδια από τους κατόχους κλειδιών, αποκρυπτογραφεί τα δεδομένα.



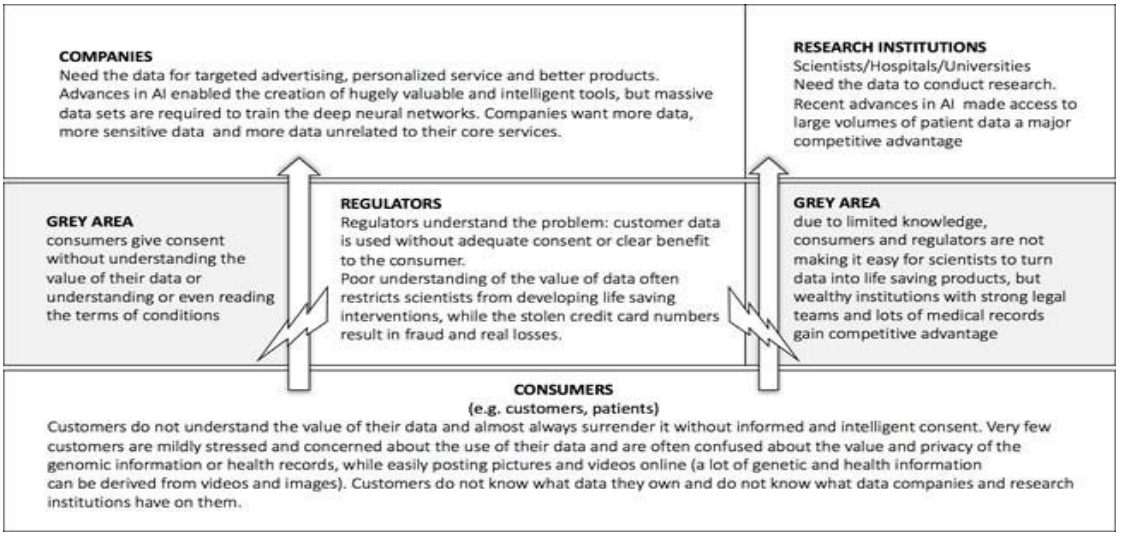
Εικόνα 25.Παράδειγμα ροής εργασίας για τους πελάτες της αγοράς **[105].**

Οι πελάτες αγοράζουν δεδομένα για το LifePounds. Το μοντέλο τιμής δεδομένων καθορίζει το κόστος δεδομένων.

4.2.2 Εφαρμογές Blockchain για την ασφάλεια των δεδομένων και προστασία της ιδιωτικότητας.

Περιγραφή του προβλήματος

Μία από τις σημαντικότερες προκλήσεις της υγειονομικής περίθαλψης είναι η ασφάλεια των δεδομένων και της ιδιωτικής ζωής. Τόσο οι καταναλωτές, όσο και οι εταιρείες υγείας και έρευνας απαιτούν τα δεδομένα πολλών ατόμων για να εκπαιδεύσουν τα βαθιά νευρωνικά τους δίκτυα. Οι εταιρείες με το μεγαλύτερο όγκο δεδομένων αποκτούν τα δεδομένα αυτά με τρόπους που μπορεί να μην είναι πολύ διαφανείς για τα άτομα και συχνά οι εταιρείες και τα άτομα δεν αντιλαμβάνονται την αξία αυτών των δεδομένων. Οι ρυθμιστικές αρχές συχνά καθιέρωσαν εμπόδια στη συλλογή και αποθήκευση δεδομένων από τους καταναλωτές.



Εικόνα 26. Η ροή δεδομένων από τα άτομα προς τις εταιρείες και τα ερευνητικά ιδρύματα **[105]**.

Η εισαγωγή του οικοσυστήματος δεδομένων βασισμένου σε blockchain μπορεί να βοηθήσει στη διασφάλιση ότι τα άτομα θα αναλάβουν τον έλεγχο των δεδομένων τους και οι εταιρείες και τα ερευνητικά ιδρύματα μπορούν να αποκτήσουν δεδομένα πιο ελεύθερα μειώνοντας την ανάγκη για παρέμβαση των ρυθμιστικών αρχών.

Τρόπος λειτουργίας

Η ασφάλεια της περιγραφόμενης ρύθμισης εξαρτάται από την ασφάλεια των χρησιμοποιούμενων crypto-primitives, τη λειτουργία κατακερματισμού και το σχήμα υπογραφής του δημόσιου κλειδιού που χρησιμοποιείται στην κατασκευή blockchain της αγοράς, καθώς και το συμμετρικό κρυπτογράφο και το σύστημα μυστικής κατανομής που χρησιμοποιούνται για την κρυπτογράφηση των δεδομένων χρήστη.

Το δημόσιο κλειδί (PKI) που βασίζεται σε blockchain για «γνωστούς» χρήστες (π.χ.επικυρωτές blockchain, επικύρωση δεδομένων κλπ.) Θα μπορούσε να βασιστεί σε καλά εδραιωμένα μέτρα για ασφαλή διαχείριση κλειδιών (π.χ. αποθήκευση κλειδιών κλπ.). Αυτά τα μέτρα θα μπορούσαν να ενισχυθούν με έξυπνη αναθέτουσα σύμβαση (π.χ. πολλαπλές υπογραφές) με βάση το blockchain. Επιπλέον, το blockchain θα μπορούσε να παράσχει ασφαλείς εγκαταστάσεις για την παρακολούθηση της βασικής ανάκλησης και έκδοσης, οι οποίες παραμένουν τα πιο αδύναμα σημεία για συγκεντρωτικές ρυθμίσεις των δημόσιων κλειδιών.

Επιπλέον, η χρήση της κρυπτογράφησης κατωφλίου θα μπορούσε να επιτρέψει την ανακούφιση ενός μόνο σημείου αποτυχίας στη μακροπρόθεσμη αποθήκευση δεδομένων. Καθώς τα δεδομένα στην αποθήκευση θα κρυπτογραφηθούν, ο συμβιβασμός της αποθήκευσης δεν θα οδηγήσει στη διαρροή δεδομένων (ωστόσο, η πρόσβαση στο χώρο αποθήκευσης θα πρέπει να περιοριστεί επιπλέον, π.χ. με την εξακρίβωση της ταυτότητας των χρηστών αποθήκευσης με τη βοήθεια του PKI που είναι εγκατεστημένο στο blockchain της αγοράς) .

Η χρήση αυθεντικών καναλιών επικοινωνίας για τη μετάδοση βασικών συναλλαγών θα μπορούσε να επιτρέψει την επίτευξη εμπιστευτικής μυστικότητας, ακόμη και αν τα μακροπρόθεσμα ασύμμετρα κλειδιά των βασικών κατόχων θα υπονομεύονταν .

Η διαχείριση του κλειδιού από την πλευρά του χρήστη για την κρυπτογράφηση δεδομένων και την εξακρίβωση της ταυτότητας των συναλλαγών blockchain μπορεί να είναι επιρρεπής σε διάφορους κινδύνους. Η ελαχιστοποίηση αυτών των κινδύνων απαιτεί προσεκτικό σχεδιασμό του λογισμικού πελάτη και των υλικών υποστήριξης. Οι υπάρχουσες λύσεις για κρυπτοσυχνότητες και / ή διαχείριση γενικών κλειδιών μπορούν να προσαρμοστούν για τη μείωση των κινδύνων.

Η περιγραφόμενη ρύθμιση δεν αφορά την ασφάλεια των δεδομένων (ειδικότερα, την προστασία από τη διαρροή) αφού τα δεδομένα έχουν αγοραστεί και μεταφερθεί στον αγοραστή. Η προστασία αυτή θα μπορούσε να επιτευχθεί με τη βοήθεια των υφιστάμενων μέτρων ασφαλείας για τα δεδομένα σε κατάσταση ηρεμίας και χρήσης και κατά συνέπεια δεν εμπίπτει στο πεδίο εφαρμογής του παρόντος εγγράφου.

4.2.3 Εφαρμογές εξωτερικού πλαισιού για έργα Blockchains.

Περιγραφή

Το Exonum είναι ένα blockchain ανοιχτού κώδικα προσανατολισμένο προς τις εξουσιοδοτημένες εφαρμογές blockchain με ευρεία πρόσβαση στην ανάγνωση των δεδομένων blockchain. Η αρχιτεκτονικη που χρησιμοποιεί το Exonum είναι προσανατολισμένη στις υπηρεσίες (SOA) [128] και αποτελείται αρχικά από τρία μέρη: υπηρεσίες, πελάτες και μεσαία λογισμικά.

Οι **υπηρεσίες** είναι το κύριο σημείο επέκτασης του πλαισίου, και ενσωματώνει την επιχειρησιακή λογική των εφαρμογών blockchain. Ένα αποκλειστικό blockchain anchoring που λειτουργεί με Exonum μπορεί να περιλαμβάνει πληθώρα υπηρεσιών. Οι υπηρεσίες έχουν ένα βαθμό αυτονομίας γιατί κάθε υπηρεσία προορίζεται για την επίλυση ενός συγκεκριμένου έργου. Η διεπαφή τους επιτρέπει την επαναχρησιμοποίηση τους και τη δυνατότητα σύνθεσης.

Οι **πελάτες** προορίζονται να είναι οι δημιουργοί των περισσότερων συναλλαγών. Έχουν τη δυνατότητα να διαβάζουν τις αιτήσεις στο σύστημα και τους παρέχονται βοηθητικά προγράμματα διαχείρισης κρυπτογραφικού κλειδιού, καθώς και εργαλεία δημιουργίας συναλλαγών και επαλήθευσης των απαντήσεων στις αιτήσεις ανάγνωσης.

Τα **μεσαία λογισμικά** (Middleware) παρέχουν την ακεραιότητα των συναλλαγών και τη διαλειτουργικότητα μεταξύ υπηρεσιών και πελατών και την αναπαραγωγή υπηρεσιών μεταξύ των κόμβων στο δίκτυο (που προορίζεται τόσο για την ανοχή σφαλμάτων υπηρεσιών όσο και για τον έλεγχο μέσω κόμβων ελέγχου). Επιπλέον, διαχειρίζονται τον κύκλο ζωής των υπηρεσιών (π.χ. ο έλεγχος πρόσβασης, η παροχή βοήθειας για τη δημιουργία απαντήσεων στις αιτήσεις ανάγνωσης κλπ). Δηλαδή, το μεσαίο λογισμικό μειώνει την πολυπλοκότητα του συστήματος από την άποψη των κατασκευαστών υπηρεσιών.

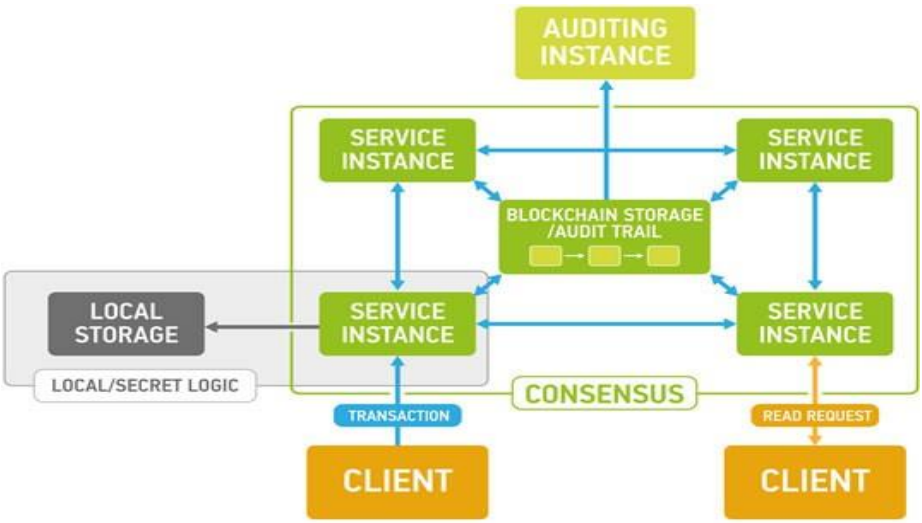
Πλεονεκτήματα εφαρμογής

Τα κύρια πλεονεκτήματα του Exonum για την περιγραφείσα εφαρμογή σε σύγκριση με τα εναλλακτικά εξουσιοδοτημένα πλαίσια είναι ότι χάρη στο σχεδιασμό των δομών αποθήκευσης δεδομένων, το Exonum θα μπορούσε να διευκολύνει τους πελάτες και τους ελεγκτές (συμπεριλαμβανομένων εκείνων με ελλειπή πρόσβαση στην πρόσβαση σε δεδομένα) να ελέγχουν το σύστημα τόσο σε πραγματικό χρόνο όσο και αναδρομικά.

Επιπλέον, με τη χρήση της αρχιτεκτονικής ,η οποία είναι προσανατολισμένη στις υπηρεσίες, η εφαρμογή θα μπορούσε εύκολα να επαναχρησιμοποιήσει τις ήδη αναπτυγμένες υπηρεσίες για άλλες εφαρμογές του Exonum, να προσθέσει και να επαναπροσδιορίσει υπηρεσίες που χρησιμοποιούνται για την εφαρμογή κλπ. Ο προσανατολισμός στις υπηρεσίες και η άμεση χρήση κοινών μεταφορών (όπως το REST + JSON) επιτρέπουν τον εξορθολογισμό της ενσωμάτωσης εφαρμογών τρίτων μερών στο οικοσύστημα που παρέχεται από το Marketplace. Επιπλέον, ο προσανατολισμός της υπηρεσίας θα μπορούσε θεωρητικά να παρέχει απρόσκοπτη διαλειτουργικότητα με άλλα μπλοκ με βάση το Exonum.

Σε σύγκριση με τα αδέσμευτα μπλοκ αλφάδια και τα πλαίσια με συγκεκριμένη γλώσσα / εικονική μηχανή, η Exonum παρέχει σημαντικά υψηλότερη παραγωγική

ικανότητα (σειρά 1.000 συναλλαγών ανά δευτερόλεπτο) και δυνατότητα κωδικοποίησης περίπλοκων λογικών συναλλαγών, και αλληλεπίδραση με εξωτερικά εξαρτήματα. Το Exonum χρησιμοποιεί απαισιόδοξες υποθέσεις ασφαλείας ως προς τη λειτουργία κόμβου επικύρωσης. Ο αλγόριθμος συναίνεσης που χρησιμοποιείται στο Exonum δεν εισάγει μεμονωμένα σημεία αποτυχίας (π.χ. αποκλειστικούς ενορχηστρωτικούς κόμβους / κόμβους παραγγελίας συναλλαγών). Επιπλέον, το σύνολο των κόμβων επικύρωσης είναι επαναρυθμίσιμο, επιτρέποντας την κλιμάκωση της ασφάλειας προσθέτοντας νέα επικυρώματα, περιστρεφόμενα πλήκτρα για επικυρώσεις, κλείδωμα των συμβιβασμένων επικυρωτών κ.λπ.



Εικόνα 27. Σχεδιασμός υπηρεσίας Exonum [105].

Κάθε παράμετρος Υπηρεσίας και Έλεγχος έχει τοπικό αντίγραφο της αποθήκευσης μπλοκ αλυσίδων για να εξασφαλίσει την αυθεντικότητα των δεδομένων και το φορτίο εξισορρόπησης.

Αποθήκευση

Η κατάσταση Blockchain στο Exonum είναι μια επίμονη αποθήκευση κλειδιού-τιμής ,όπου τα κλειδιά και οι τιμές είναι, στις πιο γενικές περιπτώσεις, ακολουθίες byte ενός αυθαίρετου μήκους, με καθορισμένες λειτουργίες. Οι λειτουργίες αυτές είναι η εισαγωγή μιας τιμής κάτω από ένα συγκεκριμένο πλήκτρο (δημιουργώντας το πλήκτρο εάν χρειάζεται), η αφαιρέση ενός ζεύγος κλειδιού-τιμής από το πλήκτρο και η επεξήγηση των πλήκτρων στη λεξικογραφική σειρά, συμπεριλαμβανομένης της έναρξης από ένα συγκεκριμένο κλειδί.

Λειτουργία Exonum

Το Exonum επιτρέπει τη διάσπαση του κεντρικού χώρου της κοινής αποθήκευσης κλειδιού-τιμής στην ιεραρχία των πληκτρολογημένων συλλογών με λίστες, σύνολα και χάρτες, ενώ τα στοιχεία των συλλογών (ή ζεύγη κλειδιών-τιμών στην περίπτωση των χαρτών) είναι δυαδικά σειριοποιήσιμα σύμφωνα με τη μορφή σειριοποίησης Exonum. Οι λειτουργίες σε αυτές τις συλλογές αντιστοιχίζονται στις ανάλογες λειτουργίες της υποκείμενης αποθήκευσης κλειδιού-τιμής. Τα δύο ανώτατα επίπεδα

ιεραρχίας αντιστοιχούν σε υπηρεσίες και συλλογές δεδομένων εντός της συγκεκριμένης υπηρεσίας. Το δεύτερο επίπεδο ιεραρχίας περιλαμβάνει τα στοιχεία συλλογών υπηρεσιών του ανώτατου επιπέδου. Πρόσθετα επίπεδα ιεραρχίας θα μπορούσαν να δημιουργηθούν χρησιμοποιώντας τις συλλογές ως στοιχεία συλλογών ανώτατου επιπέδου.

Οι συλλογές μπορούν να δηλωθούν ως Merkelized. Οι Merkelized συλλογές εισάγουν μια νέα λειτουργία,την είσοδο κατακερματισμένων συναρτήσεων. Με τον τρόπο αυτόν ενισχύεται η δέσμευση κατακερματισμού για όλα τα στοιχεία της συλλογής. Αυτή η δομή επιτρέπει τη δημιουργία κρυπτογραφικών αποδείξεων παρουσίας (και απουσίας στην περίπτωση συνόλων / χαρτών) αντικειμένων στη συλλογή.

Παρόμοια με την ιεραρχική δομή των συλλογών μέσα στο blockchain που περιγράφηκε παραπάνω, όλες οι Merkelised συλλογές μιας συγκεκριμένης υπηρεσίας θα μπορούσαν να δεσμευτούν σε ένα ενιαίο digest hash. Ομοίως, οι δεσμεύσεις όλων των υπηρεσιών εντός του blockchain θα μπορούσαν να συγκεντρωθούν σε ένα ενιαίο κατακερματισμό, ο οποίος θα αφορούσε όλα τα δεδομένα σε όλες τις Merkel συλλογές εντός της κατάσταση του blockchain. Για όλες τις προθέσεις και τους σκοπούς, η προκύπτουσα χώνευση στο επίπεδο blockchain είναι το hash (δέσμευση) ολόκληρης της κατάστασης blockchain. Αυτό θα επιτρέψει να δημιουργηθούν αποδείξεις ύπαρξης ή απουσίας που συνδέονται με αυτό το ενιαίο hash ως ρίζα εμπιστοσύνης.

Προκειμένου να μειωθούν οι κίνδυνοι αναθεώρησης ιστορικού και αμφισβήτησης, μπορεί να αποθηκευτεί σε ένα αδέσμευτο blockchain με ισχυρές εγγυήσεις υπευθυνότητας (π.χ. Bitcoin) και οι αποδείξεις που θα παρέχονται στους πελάτες να αυξάνονται αναλόγως. Πρέπει να σημειωθεί ότι το σχήμα αγκυροβόλησης θα επέτρεπε την αξιόπιστη επιβεβαίωση των δηλώσεων σχετικά με την κατάσταση blockchain αναδρομικά, ακόμα και αν το ίδιο το blockchain έχει καταστεί μη διαθέσιμο (π.χ. λόγω συμβιβασμού ευρείας κλίμακας ή συμπαιγνίας των validator blockchain).

Σύνδεση εφαρμογής με το Δίκτυο

Οι υπηρεσίες μπορούν να επικοινωνούν με τον εξωτερικό κόσμο μέσω δύο ειδών αλληλεπιδράσεων. Το πρώτο είδος αλληλεπίδρασης είναι οι συναλλαγές να παρουσιάζονται ως ο μόνος τρόπος για να τροποποιηθεί η κατάσταση blockchain. Οι συναλλαγές εκτελούνται ασύγχρονα, με την παραγγελία τους και τα αποτελέσματα εκτέλεσης υπόκεινται στον αλγόριθμο συναίνεσης που εκτελείται στο blockchain. Για το λόγο αυτό, οι εισερχόμενες συναλλαγές μεταδίδονται μεταξύ των πλήρων κόμβων στο δίκτυο.

Το δεύτερο είδος αλληλεπίδρασης είναι οι αιτήσεις ανάγνωσης να επιτρέπουν την ανάκτηση πληροφοριών από την κατάσταση blockchain, η οποία μπορεί να συνοδεύεται από τις αντίστοιχες αποδείξεις ύπαρξης / απουσίας. Οι αιτήσεις ανάγνωσης μπορούν να επεξεργαστούν τοπικά από οποιοδήποτε πλήρη κόμβο (ή, γενικότερα, από οποιονδήποτε κόμβο που έχει επαρκή πρόσβαση ανάγνωσης στα αντίστοιχα πλήκτρα κλειδιών της κατάστασης blockchain).

Στρώμα μεταφοράς

Λόγω του καθολικού επαληθεύσιμου των συναλλαγών και των αποδείξεων, οι πελάτες μπορούν να συνδεθούν με έναν μόνο κόμβο για όλα τα αιτήματα τους. Ο κακόβουλος ενεργός κόμβος δεν μπορεί να δημιουργήσει αποδείξεις για αιτήσεις ανάγνωσης. Θα μπορούσε όμως, να καθυστερήσει την επεξεργασία των συναλλαγών μη μεταδίδοντας τις συναλλαγές που έλαβε από τον πελάτη. Το πρωτόκολλο μεταφοράς δεν προορίζεται να προσκολληθεί με την προδιαγραφή Exonum. Πράγματι, όπως συμβαίνει με τις υπηρεσίες ιστού σε πλαίσια όπως το Java EE και το CORBA, το επίπεδο των μεσαίων λογισμικών έχει την ευθύνη να αφαιρεθεί η λειτουργικότητα του στρώματος μεταφοράς από τους υπεύθυνους ανάπτυξης υπηρεσιών, έτσι ώστε η επίκληση των τελικών σημείων υπηρεσίας να μπορεί να αντιστοιχιστεί στις τοπικές επικλήσεις μεθόδων. Από το Exonum 0.2, η μεταφορά RESTful JSON υποστηρίζεται για την αλληλεπίδραση πλήρων κόμβων Exonum με τους πελάτες και το TCP με προσαρμοσμένο δυαδικό σχήμα χρησιμοποιείται στην επικοινωνία μεταξύ πλήρων κόμβων.

Έλεγχος ταυτότητας και εξουσιοδότηση

Οι συναλλαγές επιβεβαιώνονται υποχρεωτικά από τους δημιουργούς τους με τη βοήθεια ψηφιακών υπογραφών δημόσιου κλειδιού για την εξασφάλιση της ακεραιότητάς τους, καθώς και της καθολικής επαλήθευσης σε πραγματικό χρόνο και εκ των υστέρων. Η υποδομή δημόσιου κλειδιού (PKI) θα μπορούσε να χτιστεί στην κορυφή για να επιτευχθεί πληρέστερος έλεγχος πρόσβασης χωρίς απόρριψη ή / και έλεγχο πρόσβασης, εάν είναι απαραίτητο.

Καθώς οι αιτήσεις ανάγνωσης είναι τοπικές, ο έλεγχος ταυτότητας / εξουσιοδότηση για αυτούς μπορεί να είναι συγκεκριμένος για τις μεταφορές, επιτυγχάνεται π.χ. με υπογραφές ιστού (κυρίως για αιτήσεις ανάγνωσης που υλοποιούνται με τη μέθοδο HTTP GET) .

Ενέργειες ενός πελάτη στο Exonum.

Ένας πελάτης στο Exonum κατέχει μια βιβλιοθήκη που παρέχει τη δυνατότητα επικοινωνίας με πλήρεις κόμβους (δηλ. να καλέσει τα τελικά σημεία της υπηρεσίας και να λάβει απαντήσεις) και να επαληθεύσει κρυπτογραφικά τις απαντήσεις. Ένας πελάτης θα μπορούσε να χαρακτηριστεί από τις βασικές δυνατότητες διαχείρισης και την εμμονή των απαντήσεων από τους πλήρεις κόμβους. Το πρώτο θα μπορούσε να χρησιμοποιηθεί για την εξακρίβωση της ταυτότητας των αιτημάτων και το τελευταίο θα μπορούσε να βοηθήσει στην αποδοχή και να επαληθεύσει τη συνοχή μεταξύ των διαφορετικών απαντήσεων .

Ανάγκη ομοφωνίας.

Το Exonum χρησιμοποιεί έναν αλγόριθμο συναίνεσης με βάση τη βυζαντινή ανοχή σφάλματος (Byzantine fault-tolerant ,BFT) [129] για να παραγγείλει συναλλαγές στο αρχείο καταγραφής συναλλαγών και να συμφωνήσει για το αποτέλεσμα της συναλλαγής. Το δίκτυο Exonum θα συνεχίσει να λειτουργεί μέχρι το 1/3 των επικυρωτών να έχει συμβιβαστεί ή να έχει απενεργοποιηθεί. Ως εκ τούτου, δεν υπάρχει κανένα σημείο αποτυχίας στο δίκτυο και όλη η διαδικασία επεξεργασίας συναλλαγών είναι αποκεντρωμένη. Ο αλγόριθμος συναίνεσης λειτουργεί με την παραδοχή των αξέχαστων ψηφιακών υπογραφών δημόσιου κλειδιού και ενός μερικώς

σύγχρονου δικτύου. Υπό αυτές τις συνθήκες, ο αλγόριθμος παρέχει ασφάλεια [130] που δεν εξαρτάται από τη μερική συγχρονικότητα. Παρόμοια με άλλους μερικούς σύγχρονους αλγόριθμους BFT όπως PBFT ή Tendermint, ο αλγόριθμος χρησιμοποιεί τρεις τύπους μηνυμάτων συναίνεσης - προτάσεις μπλοκ, προβλέψεις και προ-δεσμεύσεις. Ο αλγόριθμος αυτός είναι επικυρωμένος με ψηφιακές υπογραφές, ώστε να επιτρέπεται η μεταφορά μηνυμάτων μεταξύ των επικυρωτών.

Χαρακτηριστικά αλγοριθμού BFT

Σε σύγκριση με άλλους αλγόριθμους BFT, ο αλγόριθμος που χρησιμοποιείται στο Exonum περιέχει κάποια διακριτικά χαρακτηριστικά. Οι επαναλήψεις ψηφοφορίας έχουν σταθερό χρόνο έναρξης, αλλά δεν έχουν ορισμένο χρόνο λήξης. Ένας γύρος τελειώνει μόνο όταν το επόμενο μπλοκ έχει ληφθεί ή δεσμευτεί τοπικά. Αυτό συμβάλλει στη μείωση των καθυστερήσεων όταν η σύνδεση δικτύου μεταξύ των επικυρωτών είναι ασταθής.

Επιπλέον, οι προτάσεις αποκλεισμού περιλαμβάνουν μόνο κρυπτογραφικές συναρτήσεις συναλλαγών. Επιπλέον, η εκτέλεση των συναλλαγών καθυστερεί. Οι συναλλαγές εφαρμόζονται μόνο τη στιγμή που ένας κόμβος λαμβάνει επαρκείς προεπισκοπήσεις για μια πρόταση. Η καθυστερημένη επεξεργασία συναλλαγών μειώνει την αρνητική επίδραση των κακόβουλων κόμβων στη διακίνηση και την καθυστέρηση του συστήματος.

Ακόμα, ο αλγόριθμος αιτήσεων επιτρέπει σε έναν επικυρωτή να αποκαταστήσει πληροφορίες συναίνεσης από άλλους επικυρωτές χρησιμοποιώντας το γεγονός ότι όλα τα μηνύματα υπογράφονται ψηφιακά. Αυτό έχει θετική επίδραση στη ζωντάνια του συστήματος.

Το σετ επικύρωσης είναι επαναπροσδιορίσιμο. οι επικυρωτές θα μπορούσαν να προστεθούν ή να καταργηθούν από την υπάρχουσα συμφωνία υπερσύγχρονης ισχύος των υφιστάμενων επικυρωτών. Η ίδια διαδικασία θα μπορούσε να χρησιμοποιηθεί για την εναλλαγή κλειδιών για τους επικυρωτές.

Bitcoin anchoring

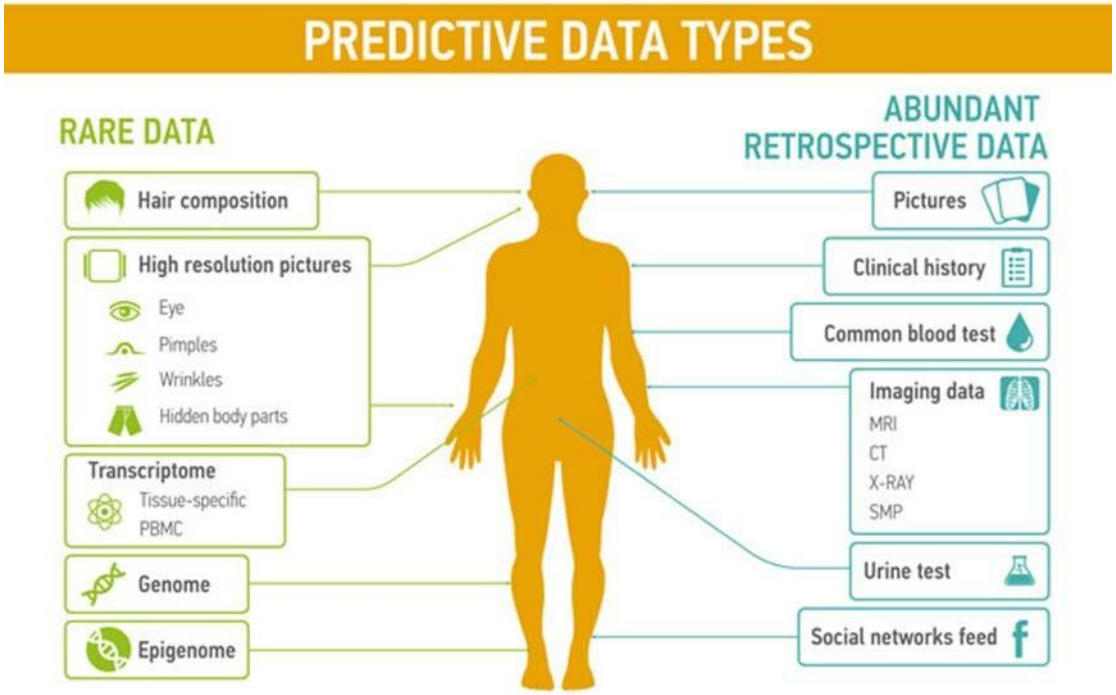
Το Exonum χρησιμοποιεί έναν αλγόριθμο αγκύρωσης BFT Bitcoin, ο οποίος δημιουργείται ως ξεχωριστή υπηρεσία. Ο αλγόριθμος εκπέμπει περιοδικά την καταγραφή κατακερματισμού ενός πρόσφατου μπλοκ σε ένα μπλοκ αλυσίδα Exonum, το οποίο δεσμεύεται σε ολόκληρη την κατάσταση blockchain και το ιστορικό συναλλαγών σε μια συναλλαγή στο blockchain Bitcoin. Η συναλλαγή αγκύρωσης έχει μια σαφώς καθορισμένη μορφή και πρέπει να επικυρωθεί από μια υπερπληθώρα επικυρωτών στην αγκυροβολημένη αλυσίδα Exonum. Οι επικυρωτές θα πρέπει να χρησιμοποιούν μεμονωμένους πλήρεις κόμβους Bitcoin για να λαμβάνουν πληροφορίες από το μπλοκ αλφάδι Bitcoin, προκειμένου να εξαλειφθούν τα μεμονωμένα σημεία αποτυχίας που σχετίζονται με πιθανές επιθέσεις έκλειψης [btc-eclipse] στους κόμβους. Οι συναλλαγές αγκύρωσης σχηματίζουν μια ακολουθία. κάθε μεταγενέστερη συναλλαγή αγκύρωσης ξοδεύει μια έξοδο που δημιουργήθηκε από την προηγούμενη. Η εξακρίβωση της ταυτότητας και η αλυσιδωτή σύνδεση των συναλλαγών αγκύρωσης καθιστούν την περιγραφόμενη διαδικασία αγκύρωσης παρόμοια με τα χαρακτηριστικά ασφαλείας της με την αγκύρωση [131].

4.2.4 Εφαρμογές για το συνδυασμό των πληροφοριών.

Περιγραφή

Οι πάροχοι υγειονομικής περίθαλψης σε όλο τον κόσμο παρακολουθούν τις αντιλήψεις των ασθενών μέσω ενός ηλεκτρονικού συστήματος ιατρικών αρχείων, δημιουργώντας terabytes των ιατρικών αρχείων ασθενών. Αυτή η γιγαντιαία ποσότητα ιατρικών δεδομένων είναι πολύτιμες πληροφορίες για την υγεία.

Κάθε είδος δεδομένων (βασική εξέταση αίματος, βασική εξέταση ούρων, μαγνητική τομογραφία, ηλεκτροεγκεφαλογράφημα, ηλεκτροκαρδιογράφημα, γονιδίωμα, μεταγραφικό μόριο, μικροβιοκτόνο κλπ.) και οι συνδυασμοί τους έχουν σχετική αξία ανάλογα με την ποιότητα των ιατρικών αρχείων και τη βιολογική τους σημασία για ορισμένες ασθένειες. Οι διαφορετικοί τύποι ιατρικών δεδομένων έχουν τη δική τους προγνωστική αξία, την αντιπροσωπευτική ευαισθησία, και αποτελούν ένα ποσοστό πρόβλεψης. Τα μοτίβα που αντικατοπτρίζουν τις αλλαγές στην κατάσταση του ασθενούς είναι πιο ευανάγνωστα όταν ο γιατρός χρησιμοποιεί σύνθετες πληροφορίες, παρουσιάζοντας την κατάσταση υγείας του ασθενούς σε διαφορετικά επίπεδα στην τρέχουσα χρονική περίοδο. Μερικοί από τους τύπους δεδομένων, όπως φωτογραφίες, βίντεο, ηχογράφηση φωνής, μπορούν επίσης να έχουν σημαντική προγνωστική αξία για την ιατρική κατάσταση. Για παράδειγμα, αρκετές ερευνητικές ομάδες έχουν ήδη μελετήσει την εφαρμογή αναγνώρισης φωνής και ομιλίας για τη διάγνωση της νόσου του Parkinson και την πρόβλεψη της σοβαρότητας της κατάστασης [132].



Εικόνα 28**. Οι τύποι προγνωστικών δεδομένων** [123].

Οι τύποι προγνωστικών δεδομένων θα μπορούσαν να χωριστούν σε δύο ομάδες: σπάνια δεδομένα, όπως τα μεταγραφικά προφίλ, σύνθεση τρίχας και άφθονα αναδρομικά δεδομένα, συμπεριλαμβανομένων κοινών εξετάσεων αίματος ή ζωοτροφών από κοινωνικά δίκτυα.

Ο παραδοσιακός αγωγός διάγνωσης είναι βασισμένος στις ιατρικές εξετάσεις, ειδικά όταν οι ειδικοί της υγειονομικής περίθαλψης προσπαθούν να διαγνώσουν σοβαρές και σύνθετες παθήσεις όπως ογκολογικές, αυτοάνοσες ή νευροεκφυλιστικές ασθένειες. Ο συνδυασμός τύπων δεδομένων, ειδικά το άθροισμα των δεδομένων χαμηλής διάγνωσης, παρέχει μια επισκόπηση πολλαπλών επιπέδων και καλύτερη κατανόηση των σύνθετων συνθηκών και οδηγεί επίσης σε ταχύτερη διάγνωση [133] .Η αναζήτηση και ο εντοπισμός των κατάλληλων ομάδων βιοδεικτών με βάση τα δεδομένα πολλαπλών επιπέδων παραμένει μια σημαντική πρόκληση. Λαμβάνοντας υπόψη τους διάφορους μηχανισμούς ανάπτυξης της νόσου, οι βιοδείκτες μπορούν να αποκτήσουν διάφορες μορφές. Υπάρχει κοινή τάση να χρησιμοποιούνται διάφοροι τύποι ιατρικών εξετάσεων για ουσιαστικά ευρύτερες διαγνωστικές εφαρμογές από αυτές που ήταν διαθέσιμες κατά την έναρξη της εφαρμογής τους.

Παρά τον μεγάλο αριθμό διαφόρων διαγνωστικών εξετάσεων, δεν είναι λογικό να χρησιμοποιείται κάθε είδος ιατρικών δεδομένων για την περιγραφή της κατάστασης της υγείας του ασθενούς. Για παράδειγμα, η ανάλυση του γονιδιώματος παρέχει μια σημαντική πληροφορία σχετικά με την κληρονομικότητα, αλλά λόγω της σχετικής σταθερότητας έχει χαμηλή τιμή για την πρόβλεψη δυναμικών αλλαγών στον οργανισμό σε σύγκριση με το επιγονιδίωμα[134] ή το μεταγραφικό [135]. Ο χρόνος δειγματοληψίας είναι ένα σημαντικό στοιχείο οποιασδήποτε ιατρικής ανάλυσης, που επιτρέπει να περιγραφεί με ακρίβεια η κατάσταση της ανθρώπινης υγείας αυτή τη στιγμή. Σύμφωνα με τις αρχές της υγείας των 360ο που εισάγει το National Health Service NHS[136], όσο οι περισσότερες διαφορετικές παράμετροι αναλύονται ταυτόχρονα, τόσο πιο λεπτομερής και ογκώδης είναι η συνολική εικόνα. Ο μοναδικός συνδυασμός ημερομηνίας παρέχει μια πολύ θρεπτική τροφή για τη τεχνητή νοημοσύνη, επιτρέποντας τη δημιουργία ισχυρών αλγορίθμων αποτελεσματικής και ακριβούς ανίχνευσης διαφορετικών καταστάσεων ανθρώπινης υγείας.

Στο παρόν έγγραφο εισάγουμε ένα επίσημο μοντέλο που επιτρέπει την αξιολόγηση της τιμής των δεδομένων που λαμβάνει υπόψη τις συνδυαστικές και τις χρονικές παραμέτρους των δεδομένων. Με βάση το μοντέλο αξίας μπορούμε να καθορίσουμε ένα σωστό κόστος για τη χρήση του δεδομένου συνδυασμού δεδομένων και αυτό με τη σειρά του επιτρέπει τη δημιουργία ενός τυπικού μοντέλου συναλλαγών ιατρικών δεδομένων για τη δημιουργία αγοράς ιατρικών δεδομένων.

4.2.5 Εφαρμογές για την πρόβλεψη της ηλικίας των ασθενών και την αξιολόγηση της προσδιοριστικής αξίας των δεδομένων.

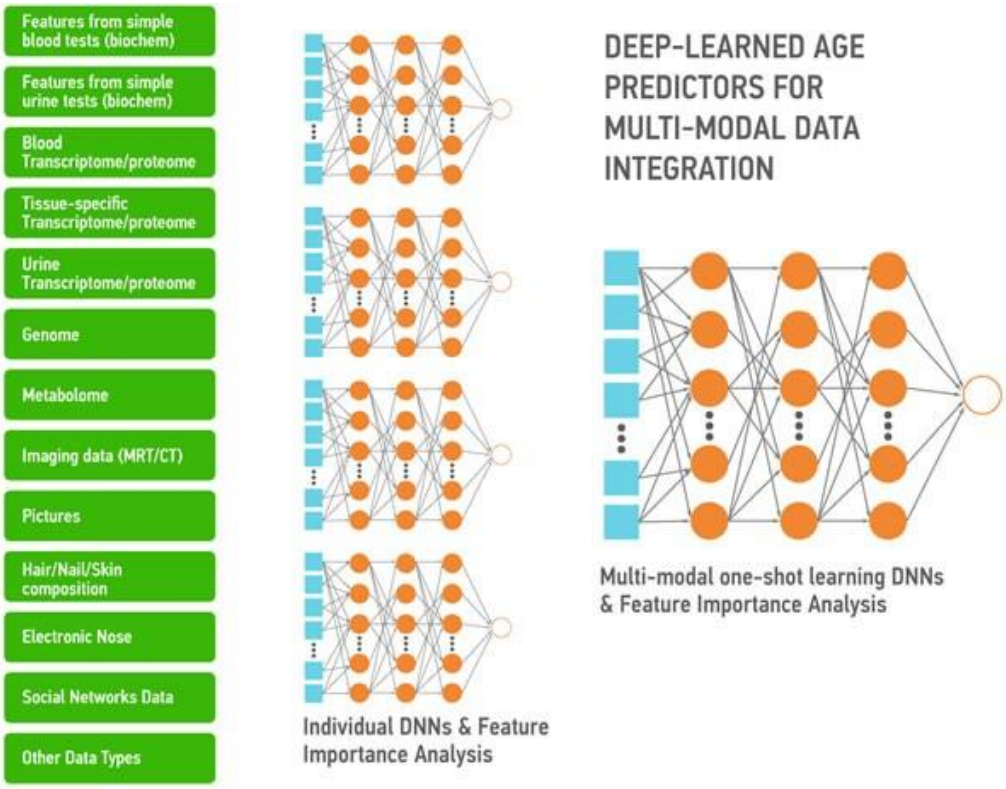
Περιγραφή

Η χρονολογική ηλικία είναι ένα χαρακτηριστικό γνώρισμα του κάθε ζωντανού οργανισμού και ένας από τους σημαντικότερους παράγοντες που επηρεάζουν τη νοσηρότητα και τη θνησιμότητα στους ανθρώπους. Το πλήθος των βιοδεικτών που συνδέονται με τη νόσο σχετίζεται έντονα με την ηλικία. Για παράδειγμα, τα τριγλυκερίδια, η γλυκοζυλιωμένη αιμοσφαιρίνη (HbA1c), η περιφέρεια μέσης, η IL-6

αυξάνεται με την ηλικία, αλλά άλλες παράμετροι όπως η λευκωματίνη, η IGF και η κάθαρση κρεατινίνης κινούνται προς την αντίθετη κατεύθυνση [137]. Έχουν γίνει πολλές προσπάθειες για την ενσωμάτωση των βιοδεικτών σε διάφορους δείκτες υγείας / κινδύνου όπως ο δείκτης υγιούς γήρανσης [138], ο δείκτης κινδύνου Framingham [139], ο δείκτης ευθραυστότητας [140] και ο φυσιολογικός δείκτης συνυπολογισμών. Τελικά, η ηλικία είναι η πλησιέστερη εκτίμηση της κατάστασης υγείας ενός ατόμου. Ως εκ τούτου, ο συνδυασμός διαφόρων βιολογικών δεικτών και η σύνδεσή τους με την ηλικία θα αποτελέσουν τη βάση για πλατφόρμα ικανή να παράσχει ολοκληρωμένη ανάλυση της κατάστασης της υγείας, να αξιολογήσει την ποιότητα των δεδομένων και ακόμη να προσδιορίσει τα πλαστά δεδομένα. Επιπλέον, η αντιμετώπιση της γήρανσης ως ασθένειας (για τη σύλληψη των σημαντικότερων βιολογικών ιδιοτήτων των αλλαγών που σχετίζονται με την ηλικία και εμφανίζονται κατά τη διάρκεια της γήρανσης) διευκολύνει τη μεταφορά της μάθησης σε μεμονωμένες ασθένειες χρησιμοποιώντας ένα πολύ μικρότερο αριθμό δειγμάτων.

Λειτουργία εφαρμογής.

Η γήρανση είναι επίσης μια συνεχής διαδικασία που σταδιακά οδηγεί σε απώλεια της λειτουργίας και στις ασθένειες που συνδέονται με την ηλικία. Οι τεχνικές μηχανικής μάθησης που χρησιμοποιούν τα Deep Neural Networks (DNN) έχουν εκπαιδευτεί στα πολυτροπικά δεδομένα που κυμαίνονται από φωτογραφίες, βίντεο, εξετάσεις αίματος, "omics", δραστηριότητα, ακόμη και μυρωδιά και ιδρώτα κατά τη γήρανση, συλλαμβάνουν τα πολλά βιολογικά χαρακτηριστικά σχετικά με την ομάδα και το άτομο. Αυτά τα DNNs μπορούν να χρησιμοποιηθούν για να εξαγάγουν τα χαρακτηριστικά που εμπλέκονται περισσότερο στη γήρανση και συγκεκριμένες ασθένειες για να χρησιμοποιηθούν ως στόχοι ή να δημιουργήσουν δίκτυα σύνδεσης και αιτιακές γραφές. Αυτά τα DNNs μπορούν επίσης να επανεκπαιδευθούν σε πολύ μικρότερο αριθμό συνόλων δεδομένων συγκεκριμένων ασθενειών εντός του ίδιου τύπου δεδομένων ή χρησιμοποιώντας τους πολλούς τύπους βιολογικών δεδομένων. Εδώ προτείνουμε μια αρχιτεκτονική υψηλού επιπέδου που φέρει τους διάφορους τύπους δεδομένων (Σχήμα 6). Πρώτον, για κάθε τύπο δεδομένων χτίζουμε έναν πρόλογο DNN χρονολογικής ηλικίας για τα σχετικά υγιή άτομα. Τα μεμονωμένα DNN θα επιτρέπουν την ανίχνευση των απομειώσεων και τον έλεγχο ποιότητας των δεδομένων. Στη συνέχεια, όλα τα μεμονωμένα DNNs θα χρησιμοποιηθούν για την εκπαίδευση πολλαπλών τρόπων μονόπλευρης εκμάθησης DNN. Αυτή η αρχιτεκτονική επιτρέπει όχι μόνο την ακριβή πρόβλεψη ηλικίας, αλλά και την ανάλυση σημαντικών χαρακτηριστικών. Τα αποτελέσματα μιας τέτοιας ανάλυσης σε όλους τους παράγοντες πρόβλεψης θα δείξουν τη σημασία κάθε μεμονωμένου βιοδείκτη και μπορεί να ενημερώσουν το σχετικό «κόστος» του. Δεδομένου ότι πολλοί από τους βιοδείκτες που σχετίζονται με την ηλικία (Αλβουμίνη, Γλυκόζη, Νορεπινεφρίνη, WBC, Il-6 κ.λπ.) μετρώνται συνήθως στη κλινική σε ξεχωριστές δοκιμές διαφορετικού βαθμού διεισδυτικότητας, είναι σημαντικό να γνωρίζουμε ποιες είναι πιο προβλέψιμες.



Εικόνα 29. Μια απλή απεικόνιση των βαθιών νευρωνικών δικτύων [105].

Τα νευρωνικά δίκτυα έχουν εκπαιδευτεί για την πρόβλεψη της χρονολογικής ηλικίας μέσα στον τύπο δεδομένων και τη χρήση των χαρακτηριστικών που εξάγονται χρησιμοποιώντας τη σημασία των χαρακτηριστικών και την επιλογή βαθιών χαρακτηριστικών για τους πολυτροπικούς παράγοντες πρόβλεψης ηλικίας. Αυτοί οι παράγοντες πρόβλεψης μπορούν να χρησιμοποιηθούν για την ολοκλήρωση, την επαλήθευση και τη μεταφορά δεδομένων.

5.

5.1 Συμπεράσματα συμβολής της τεχνολογίας Blockchain στο χώρο της υγείας.

Η εφαρμογή της τεχνολογίας blockchain στην υγειονομική περίθαλψη εξακολουθεί να είναι ένα αναδυόμενο πεδίο. Υπάρχει ανάγκη ανάπτυξης περισσότερων πρωτότυπων και αποδεικτικών στοιχείων για την κατανόηση και τη διαπίστωση της ωριμότητας της τεχνολογίας σε σχέση με την εφαρμογή της στην υγειονομική περίθαλψη. Πολλά από τα προτεινόμενα πλαίσια, ιδέες, μοντέλα και αρχιτεκτονικές, [105], πρέπει να εφαρμοστούν και να δοκιμαστούν για να αξιολογηθούν τα δυνατά σημεία τους και οι αδυναμίες τους. Για να διασφαλιστεί η διαλειτουργικότητα μεταξύ των διαφόρων προϊόντων blockchain, υπάρχει ανάγκη για ανοικτά πρότυπα. Επί του παρόντος, η εστίαση είναι στη δοκιμή της λειτουργικότητας των prototypes blockchain. Ωστόσο, για την πλήρη υιοθέτηση και επέκταση του blockchain στην επιχειρησιακή υγειονομική περίθαλψη χρειάζονται ανοικτά πρότυπα και το στοιχείο της διαλειτουργικότητας. Είναι επομένως σημαντικό οι ερευνητές να αρχίσουν να εξετάζουν ζητήματα διαλειτουργικότητας και τις διαδικασίες τυποποίησης. Υπάρχει ήδη μια ομάδα προτύπων στην οποία οι ερευνητές μπορούν να στείλουν τις συνεισφορές τους [69].

Οι προκλήσεις της ασφάλειας των δεδομένων και της ιδιωτικής ζωής, της διαλειτουργικότητας, της επεκτασιμότητας και της ταχύτητας χαρακτηρίζουν τις εφαρμογές υγειονομικής περίθαλψης που βασίζονται σε blockchain. Ολες οι παραπάνω προκλήσεις απαιτούν περαιτέρω συντονισμό και ερευνητικές δεσμεύσεις προκειμένου να βελτιωθεί η εμπιστοσύνη των ενδιαφερομένων μερών στη χρήση της τεχνολογίας στην υγειονομική περίθαλψη. Η υπόσχεση της τεχνολογίας blockchain είναι να επιτρέψει την αποτελεσματική ανταλλαγή πληροφοριών με τα ενδιαφερόμενα μέρη, εξασφαλίζοντας παράλληλα την ακεραιότητα των δεδομένων και την προστασία της ιδιωτικής ζωής των ασθενών. Οι υποστηρικτές ελπίζουν ότι η τεχνολογία αυτή θα ενισχύσει την δύναμη των ανθρώπων και θα τους επιτρέψει να βελτιώσουν την κατάσταση της υγείας τους.

Αν αντιμετωπιστούν οι προκλήσεις της διαλειτουργικότητας και δημιουργηθεί ένα αξιόπιστο ιδιωτικό απόρρητο, αναπτυχθούν πρωτόκολλα ανωνυμίας και υπάρξει συναίνεση για τα είδη των συμβάσεων που απαιτούνται στον έλεγχο των πληροφοριών, τότε θα ξεκινήσει μια νέα εποχή στο τομέα της υγειονομικής περίθαλψης. Αυτές είναι σημαντικές προκλήσεις και οι εταιρείες έχουν ήδη κάνει σημαντικές προσπάθειες αντιμετώπισής τους ακόμη και σε αυτό το πρώιμο στάδιο. Οι γίγαντες της τεχνολογίας του αιώνα μας έχουν δείξει ήδη ότι ανταποκρίνονται στη χρήση της τεχνητής νοημοσύνης για την άντληση δεδομένων.

Η τεχνολογία blockchain αποτελεί ένα σημαντικό βήμα προς την κατεύθυνση της εξατομικευμένης υγείας με παροχή υγειονομικής περίθαλψης με βάση την βαθιά κατανόηση της προσωπικής βιολογίας του κάθε ατόμου.

Το δυναμικό της τεχνολογίας blockchain διερευνάται σε πολλές εφαρμογές του τομέα της υγειονομικής περίθαλψης. Η πορεία της τεχνολογίας (και το μάρκετινγκ) είναι ανοδική. Είναι μια συναρπαστική στιγμή, με πολλές νέες εφαρμογές που ανακαλύπτονται ,αναπτύσσονται, και ύποσχονται πολλές εξελίξεις στο χώρο της υγείας.

5.2 Τρόπος εφαρμογής της τεχνολογίας Blockchain και η λήψη μέτρων για την λειτουργία της στο χώρο της υγείας.

Η χρήση της τεχνολογίας blockchain τοποθετεί τον ασθενή στο επίκεντρο της προσοχής. Για τους περισσότερους ασθενείς, η διατήρηση της υγείας συνεπάγεται αλληλεπιδράσεις με διάφορους παρόχους υγειονομικής περίθαλψης και εργαλεία συλλογής δεδομένων, τα οποία παράγουν πληροφορίες κρίσιμες για την λήψη κατάλληλων αποφάσεων. Υπάρχει αυξανόμενη τάση για τη συμφωνία ότι οι πληροφορίες πρέπει να είναι διαθέσιμες στους ασθενείς έτσι ώστε να μπορούν να είναι ενεργοί παράγοντες στην περίθαλψή τους και η συμμετοχή και εμπλοκή των ασθενών αποτελούν τον ακρογωνιαίο λίθο της σύγχρονης ιατρικής πρακτικής .Οι συντηρητές του συστήματος έχουν επίσης πρόσβαση σε ιατρικές πληροφορίες, ωστόσο, οι ασθενείς επιθυμούν να ελέγχουν ποιες πληροφορίες λαμβάνουν οι φροντιστές και υπό ποιες συνθήκες.

Εξίσου σημαντικό στοιχείο είναι ότι πρέπει να ληφθεί υπόψη ο στενός και άκρως προσωπικός χαρακτήρας των πληροφοριών υγείας. Οι πληροφορίες για την υγεία πρέπει να είναι ιδιωτικές και προσιτές μόνο από τα κατάλληλα συμβαλλόμενα μέρη, για τους κατάλληλους λόγους, τη κατάλληλη στιγμή. Ορισμένες δικαιοδοσίες έχουν θεσπιστεί από τη νομοθεσία για την προστασία προσωπικών πληροφοριών (π.χ. Καναδάς: Υπουργός Δικαιοσύνης, 2015, Ηνωμένες Πολιτείες: Υπουργείο Υγείας και Ανθρωπίνων Υπηρεσιών, 2013), τις οποίες πρέπει να λάβουν υπόψη οι νέες τεχνολογίες. Παρά την πολυπλοκότητα του προβλήματος ,καταβάλλονται προσπάθειες ώστε κάθε ενήλικος να έχει πλήρη πρόσβαση στα δικά τους ιατρικά αρχεία.

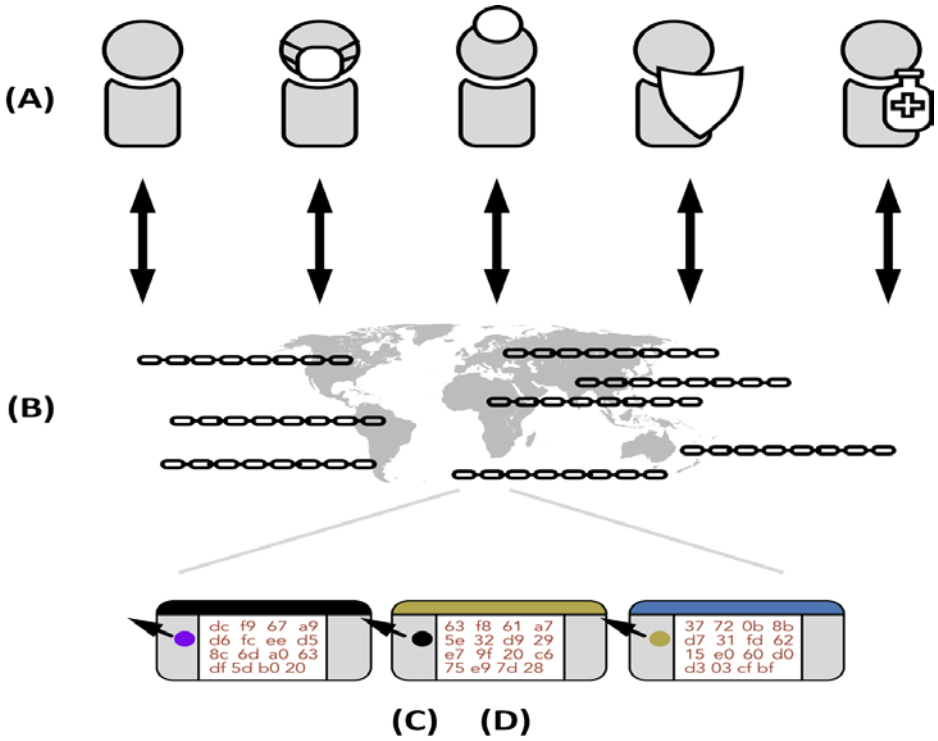
Επί του παρόντος, οι ιατρικές πληροφορίες παρέχονται συχνά από μεμονωμένους παρόχους ή συλλέκτες δεδομένων χωρίς πλήρη πρόσβαση ασθενών . Αυτό περιορίζει την ικανότητα των ασθενών να διερευνούν επιλογές, να συνεισφέρουν και να διορθώνουν λάθη στα δικά τους δεδομένα και να μοιράζονται τις πληροφορίες τους με νέους επαγγελματίες για να καθορίσουν πλήρως ένα ενημερωμένο ιατρικό ιστορικό. Η ανταλλαγή πληροφοριών θα πρέπει να επιτρέπει στον ασθενή αυξημένο έλεγχο εξασφαλίζοντας ότι οι πλήρεις πληροφορίες για την υγεία του είναι διαθέσιμες στους κατάλληλους ανθρώπους την κατάλληλη στιγμή. Η έλλειψη της διαλειτουργικότητας των πληροφοριών είναι επιζήμια για τη χρήση νέων διαγνωστικών τεχνολογιών με βάση δεδομένα.

Υπάρχει ένας περιορισμός στο κόστος της υγειονομικής περίθαλψης, και τα έξοδα αυξάνονται σε κάθε συζήτηση που αφορά αλλαγές του παραδοσιακού τρόπου εφαρμογής της. Οι κατά κεφαλήν δαπάνες για την υγεία αυξήθηκαν κατά 60% τα τελευταία 10 χρόνια σύμφωνα με τη Παγκόσμια Τράπεζα. Σε χώρες όπως η Αυστραλία, το Ηνωμένο Βασίλειο και ο Καναδάς, οι δαπάνες για την υγεία αντιπροσωπεύουν περίπου το 10% του ΑΕΠ. στις Ηνωμένες Πολιτείες, ο αριθμός αυτός είναι πιο κοντά στο 17%. Παραδόξως, τα αποτελέσματα στις Ηνωμένες Πολιτείες είναι χειρότερα από ό, τι αλλού ,γεγονός που δείχνει ότι υπάρχουν σπατάλες στο σύστημα[69]. Πρόσφατη μελέτη έδειξε ότι οι ηλικιωμένοι με διάγνωση χρόνιων παθήσεων αντιμετωπίζουν τεράστιες δαπάνες για την υγεία ακόμη και σε ορισμένες από τις πλουσιότερες χώρες της Ευρώπης .Πρέπει να σημειωθεί ότι ο πληθυσμός στις ανεπτυγμένες χώρες, κατά μέσο όρο, γηράσκει και επομένως η κατάσταση αυτή αναμένεται εύλογα να επιδεινωθεί στο μέλλον. Η τεχνολογία μπορεί να είναι μέρος της λύσης. Η τεχνολογία blockchain έχει τη δυνατότητα να διατηρεί και να ελέγχει την πρόσβαση σε τεράστιες ποσότητες ανώνυμων δεδομένων υγείας, επιτρέποντας νέες έρευνες και νέες ιδέες, προστατεύοντας ταυτόχρονα την ιδιωτικότητα των ασθενών. Είναι σημαντικό το γεγονός ότι η τεχνολογία blockchain χρησιμεύει ως πρωτόκολλο για τη σύνδεση σημαντικών ενδιαφερομένων με τα δεδομένα, χωρίς να απαιτείται ακριβό στρώμα μεσολαβητών δεδομένων και υπηρεσιών εγγύησης για τη διασφάλιση της εμπιστοσύνης, την απομάκρυνση της μεσαίας διαχείρισης και του σχετικού κόστους από την εξίσωση κοινής χρήσης δεδομένων. Η καλύτερη ανταλλαγή δεδομένων μεταξύ των ενδιαφερόμενων μερών θα πρέπει επίσης να μειώσει το κόστος, για παράδειγμα, λόγω διπλών δοκιμών που συμβαίνουν όταν οι πάροχοι υγειονομικής περίθαλψης δεν γνωρίζουν τις ενέργειες του άλλου.

5.3 Πλεονεκτήματα της τεχνολογίας Blockchain στο χώρο της υγείας.

Στον πυρήνα της, η τεχνολογία blockchain αποτελείται από μερικές απλές ιδέες με ενδιαφέρουσες ιδιότητες που ευθυγραμμίζονται σημαντικά με τις σημαντικές προκλήσεις της υγειονομικής περίθαλψης.

Τα Blockchains είναι κατανεμημένα βιβλία - διαδοχικοί κατάλογοι συναλλαγών με πανομοιότυπα αντίγραφα που μοιράζονται και συντηρούνται από πολλά μέρη. Δεν υπάρχει μια ενιαία πηγή που να διεκδικεί την εξουσία πάνω στα πραγματικά δεδομένα, ενώ οι συναλλαγές ολοκληρώνονται με τη συναίνεση των πολλαπλών μερών που κατέχουν τα δεδομένα . Εξαιτίας αυτού, τα blockchains αναφέρονται ως αποκεντρωμένα. Αυτή η διάταξη προστατεύει τα δεδομένα από παραβιάσεις όχι μόνο από μεμονωμένους κατόχους του blockchain, αλλά και από εξωτερικές προσπάθειες βλάβης [69].



Εικόνα 30. Εμπλεκόμενοι φορείς και οι ρόλοι τους σε συστήματα blockchains **[69]**.

Οι εμπλεκόμενοι φορείς (Α) έχουν επιλεκτική και ελεγχόμενη πρόσβαση σε στοιχεία δεδομένων που είναι αποθηκευμένα σε ένα σύνολο ταυτόσημων επαληθευμένων μπλοκ αλυσίδων που διατηρούνται σε πολλαπλές τοποθεσίες (Β), όπου κάθε μπλοκ περιέχει ελεγχόμενες πληροφορίες σχετικά με τη δημιουργία και την αλληλούχιση (C). Οι πληροφορίες σχετικά με την αλληλούχιση θα μπορούσαν να έχουν τη μορφή κατακερματισμού που λειτουργεί ως υπογραφή για να περιγράψει με μοναδικό τρόπο ένα ή περισσότερα προηγούμενα μπλοκ στην αλυσίδα. Παρόλο που όλα τα βέλη μεταξύ των (Α) και (Β) εμφανίζονται ως διπλής κεφαλίδας, η πρόσβαση ανάγνωσης και εγγραφής στο blockchain θα εξαρτηθεί από τους ενδιαφερόμενους, όπως ορίζεται στις έξυπνες συμβάσεις.

Κάθε εγγραφή στην αλυσίδα περιλαμβάνει ακριβείς πληροφορίες σχετικά με το πότε δημιουργήθηκε και την κρυπτογραφική υπογραφή της προηγούμενης εγγραφής στην αλυσίδα μαζί με πρόσθετες αυθαίρετες πληροφορίες. Η υπογραφή - ή το hash - αποτελείται από μια κρυπτογραφικά δημιουργούμενη ακολουθία γραμμάτων και αριθμών καθορισμένου μήκους που αναγνωρίζει με μοναδικό τρόπο οποιαδήποτε ψηφιακή οντότητα. Η αλλαγή οποιουδήποτε αρχείου θα αλλάξει την υπογραφή του και θα δημιουργήσει έτσι ένα εύκολα ανιχνεύσιμο σπάσιμο στην αλυσίδα. Τα αρχεία μπορούν να προστεθούν, να μην καταργηθούν και μόνο με συναίνεση των διαχειριστών των κατανεμημένων αντιγράφων. Οι μπλοκ αλυσίδες είναι επομένως αμετάβλητες.

Οι πληροφορίες σε κάθε μπλοκ μπορούν να κρυπτογραφηθούν έτσι ώστε μόνο οι κάτοχοι των σωστών κρυπτογραφικών κλειδιών να έχουν πρόσβαση στις πληροφορίες που περιέχονται σε αυτό. Το μπλοκ αλυσίδων είναι επομένως ιδιωτικό.

Μια αναδυόμενη ιδιότητα αυτών των δομημένων και κοινών δεδομένων είναι ότι εξαλείφει την ανάγκη για μεσίτες εμπιστοσύνης μεταξύ των μερών που απαιτούν πρόσβαση σε δεδομένα. Ακόμη και αν δεν είναι δυνατή η πρόσβαση σε όλα τα δεδομένα σε ένα blockchain λόγω περιορισμών της ιδιωτικής ζωής, κάθε ενδιαφερόμενος μπορεί να αποδείξει με μαθηματική βεβαιότητα ότι κατέχει το

ακριβές και μη τροποποιημένο αντίγραφο της ροής ιστορικών δεδομένων. Ο καθένας έχει ισότιμη πληροφόρηση και καλά κατασκευασμένα blockchains διασφαλίζουν ότι όλοι οι ενδιαφερόμενοι μπορούν να δουν όλα τα δεδομένα που απαιτούνται για τον έλεγχο των συναλλαγών στην αλυσίδα. Ο αποκεντρωμένος και αμετάβλητος χαρακτήρας των υλοποιήσεων του blockchain σε συνδυασμό με αυτή τη διαφάνεια σημαίνει ότι φέρουν εμπιστοσύνη.

Πρόσθετοι κανόνες, συχνά αναφερόμενοι ως έξυπνες συμβάσεις, μπορούν να ενσωματωθούν σε αυτούς τους αποκεντρωμένους, αμετάβλητους, ιδιωτικούς και αξιόπιστους λογαριασμούς για τη ρύθμιση του τρόπου με τον οποίο μπορούν να χρησιμοποιηθούν τα δεδομένα. Οι έξυπνες συμβάσεις δεν αποτελούν βασικό χαρακτηριστικό κάθε μπλοκ αλυσίδας, αλλά είναι συχνά βασικές για τη χρήση τους στον περίπλοκο κόσμο της υγειονομικής περίθαλψης. Αυτές οι συμβάσεις επωφελούνται από τις ιδιότητες του blockchain: ένα έξυπνο συμβόλαιο ενσωματωμένο σε ένα blockchain είναι αμετάβλητο και μπορεί να διασφαλίσει ότι λειτουργεί με τον ίδιο τρόπο, χρησιμοποιώντας αξιόπιστες πληροφορίες που μοιράζονται εξίσου μεταξύ όλων των μερών, επ 'αόριστον.

Φαίνεται σημαντικό να προσθέσουμε ότι τα blockchains είναι εργαλεία με χρήσιμες ιδιότητες που μπορούν να εφαρμοστούν σε πολλούς τομείς, αλλά δεν μπορούν από μόνα τους να λύσουν τα πανευρωπαϊκά ζητήματα των θεσμικών οργάνων. Ακόμη και με τέλεια τεχνολογία, οι πληροφορίες που τίθενται σε μπλοκ αλυσίδα μπορούν να περιέχουν ακόμη σφάλματα και πρέπει πρώτα να δημιουργηθούν και να συμφωνηθούν όλοι οι κανόνες για την πρόσβαση και την προσθήκη νέων πληροφοριών από τους κατόχους της. Τα οφέλη από την εφαρμογή τεχνολογίας blockchain μπορούν να υλοποιηθούν πλήρως μόνο μετά από επενδύσεις με προσεκτικό τεχνικό και διοικητικό σχεδιασμό που περιλαμβάνει όλους τους ενδιαφερόμενους.

5.4 Κίνδυνοι της τεχνολογίας Blockchain στο χώρο της υγείας.

Η τεχνολογία Blockchain είναι τόσο αποδοτική όσο οι χρήστες της. Εάν τίθενται στην αλυσίδα χαμηλής ποιότητας ή λανθασμένες πληροφορίες, τότε αυτό που μπορεί να διασφαλιστεί μέσω της αμεταβλητότητας και της αποκέντρωσης είναι ότι η αλυσίδα θα παραμείνει χαμηλής ποιότητας και θα περιέχει λανθασμένες πληροφορίες. Το Blockchain και οι υποστηρικτικές τεχνολογίες προσφέρουν πολλές νέες ευκαιρίες, αλλά πρέπει να ληφθεί μέριμνα για την αξιολόγηση ολόκληρης της υλοποίησης, συμπεριλαμβανομένου του τι συμβαίνει με τις πληροφορίες πριν και μετά από ένα blockchain. Οι λύσεις διαλειτουργικότητας θα πρέπει να είναι επιμελείς όσον αφορά τις πληροφορίες που αποθηκεύονται και να περιλαμβάνουν λύσεις για την επίλυση των αποκλίσεων λαμβάνοντας διαφορετικά είδη πληροφοριών. Επίσης, η μεταφορά πληροφοριών και ο έλεγχος των δεδομένων από τον ασθενή πρέπει να συνοδεύεται από σωστή εκπαίδευσή του.

Η τεχνολογία αυτή αναμένεται να επωφεληθεί από τη σημερινή διαφημιστική εκστρατεία και να εδραιωθεί στο χώρο της υγείας, αλλά δεν σταματά να θέτει δύσκολες ερωτήσεις. Οι εταιρίες θα πρέπει να κινηθούν συνετά και όχι πολύ γρήγορα για να αποφευχθεί η παροχή ανολοκλήρωτων ή μη ελεγμένων εφαρμογών στην αγορά.

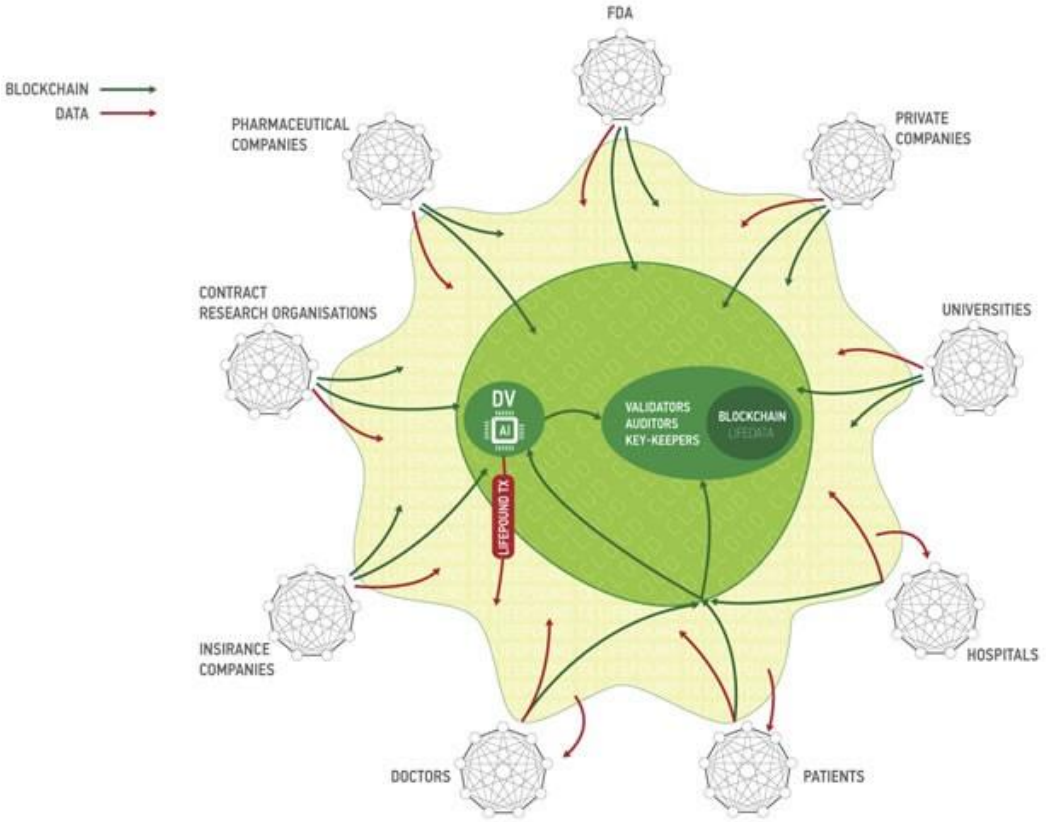
Ένα ενδιαφέρον πρόβλημα είναι ότι η δυνατότητα πρόσβασης στα δεδομένα στο blockchain είναι μέσω ενός "κλειδιού", το οποίο είναι μια μοναδική ακολουθία χαρακτήρων και ψηφίων. Εάν χαθεί ένα κλειδί, τότε τα δεδομένα στα οποία γίνεται πρόσβαση χάνονται. Η απώλεια πρόσβασης σε πληροφορίες διάρκειας λόγω της απώλειας ενός από αυτά τα κλειδιά είναι πρόβλημα και θα πρέπει να εφαρμοστούν λύσεις για την επανασύνδεση των χρηστών με τα δεδομένα τους

5.5 Εκτίμηση των μελλοντικών εφαρμογών της τεχνολογίας Blockchain στο χώρο της υγείας.

Σε αυτή την εργασία παρουσιάσαμε την προσπάθεια αξιολόγησης της αξίας του χρόνου και της αξίας του συνδυασμού των προσωπικών δεδομένων στο πλαίσιο μιας ανταλλαγής δεδομένων υγείας που τροποποιείται μέσω της τεχνητής νοημοσύνης (AI) σε blockchain. Προβλέπεται ακόμα η εμφάνιση ενός νέου επαγγέλματος του "οικονομολόγου δεδομένων" και η δημιουργία ερευνητικών ιδρυμάτων οικονομικών δεδομένων υγείας [123].

Οι πρόσφατες εξελίξεις στην τεχνητή νοημοσύνη επέτρεψαν τη δημιουργία υψηλής ακρίβειας προγνωστικών βιολογικών χαρακτηριστικών, όπως η ηλικία, η φυλή και το φύλο, από πολύ απλούς τύπους δεδομένων, όπως οι αιματολογικές εξετάσεις κ.λ.π. . Η αξία των διαφόρων τύπων δεδομένων μπορεί να εξαρτάται από την εφαρμογή. Για παράδειγμα, για τις ασφαλιστικές εταιρείες, το κόστος της δημιουργίας δεδομένων για το γονιδίωμα μπορεί να είναι σημαντικά υψηλό, όπως και η αξία της πρόσφατης εικόνας του ασθενούς, αφού μπορεί να περιλαμβάνει στοιχεία της ηλικίας, της υγείας και της θνησιμότητας του ασθενούς [123].

Το Blockchain και η τεχνητή νοημοσύνη ανοίγουν νέα παραδείγματα για τα οικοσυστήματα δεδομένων υγείας. Η τεχνολογία Blockchain επιτρέπει τη δημιουργία ενός κατανεμημένου και ασφαλούς ημερολογίου προσωπικών δεδομένων, όπου οι ασθενείς έχουν τον έλεγχο, κατέχουν τα δεδομένα τους και παρακολουθούν τα προνόμια πρόσβασης και την κατανόηση της κατάστασης της υγείας τους. Το πιο σημαντικό είναι ότι η τεχνολογία blockchain επιτρέπει τη δημιουργία μιας αγοράς με βάσεις δεδομένων, όπου οι ασθενείς μπορούν να λαμβάνουν απτές ανταμοιβές για τη διάθεση των δεδομένων τους στην κοινότητα ανάπτυξης εφαρμογών, στις φαρμακευτικές και καταναλωτικές εταιρείες και στα ερευνητικά ιδρύματα. Επί του παρόντος, μόνο λίγοι ασθενείς παγκοσμίως διαθέτουν τα πλήρη δεδομένα που περιέχουν το κλινικό ιστορικό τους σε συνδυασμό με τα γενετικά χαρακτηριστικά, τη βιοχημεία του αίματος και τα προφίλ καταμέτρησης κυττάρων, τα δεδομένα για τον τρόπο ζωής, τη χρήση ναρκωτικών και συμπληρωμάτων και άλλους τύπους δεδομένων, επειδή δεν βλέπουν την αξία σε αυτά τα δεδομένα και δεν εξετάζονται τακτικά. Από την άλλη πλευρά, οι φαρμακευτικές και καταναλωτικές εταιρείες είναι πρόθυμες να διαθέσουν σημαντικά ποσά για τη συλλογή μεγάλου αριθμού αρχείων προσωπικών δεδομένων που απαιτούνται για την κατάρτιση του AI. Αυτά τα κεφάλαια μπορούν να χρησιμοποιηθούν για την επιδότηση των τακτικών εξετάσεων από τους ασθενείς, για να αποκαλυφθούν οι νέες χρήσεις για τους διάφορους τύπους δεδομένων και να αναπτυχθούν εξελιγμένα εργαλεία διάγνωσης και θεραπείας.



Εικόνα 31. Προτεινόμενη οικονομία με βάση δεδομένα προσωπικού χαρακτήρα [141].

Τα άτομα έχουν πλήρη γνώση και έλεγχο των δεδομένων τους και επιβραβεύονται για τη δημιουργία νέων δεδομένων και την παροχή δεδομένων για ερευνητικούς ή εμπορικούς σκοπούς. Ένα τέτοιο οικοσύστημα μπορεί να επιτρέψει στις ρυθμιστικές αρχές συμπεριλαμβανομένης της Υπηρεσίας Τροφίμων και Φαρμάκων και των φαρμακευτικών και καταναλωτικών εταιρειών να ανταλλάξουν τα δεδομένα τους

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] "2. Cryptocurrencies and Blockchain | Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion | Better Regulation." [Online]. Available: https://service.betterregulation.com/document/344397. [Accessed: 30-Oct-2019].

[2] A. J. Mount, "Bitcoin's status isn't as simple as ruling if it is more a private token or a public ledger," *Win-Vector Blog*, 07-Nov-2015. [Online]. Available: http://www.win-vector.com/blog/2015/11/bitcoins-status-isnt-as-simple-as-ruling-if-it-is-more-a-private-token-or-a-public-ledger/. [Accessed: 22-Oct-2019].

[3] "5 - 01 Houben statement.pdf.".

[4] D. R. Houben and A. Snyers, "Cryptocurrencies and blockchain," p. 103.

[5] "Smart Contracts: The Ultimate Guide for the Beginners," *101 Blockchains*, 19-Jul-2018. [Online]. Available: https://101blockchains.com/smart-contracts/. [Accessed: 17-Dec-2019].

[6] "122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf." .

[7] European Central Bank, *Virtual currency schemes: a further analysis.* Frankfurt am Main: European Central Bank, 2015.

[8] "Blockchain for Digital Identity: The Decentralized and Self-Sovereign Identity (SSI)," *101 Blockchains*, 02-Oct-2019. [Online]. Available: https://101blockchains.com/digital-identity/. [Accessed: 17-Dec-2019].
[9] "IFRS: Accounting for crypto-assets," p. 24.
[10] "The difference between public and private blockchain - Blockchain Pulse: IBM Blockchain Blog." [Online]. Available: https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/. [Accessed: 25-Oct-2019].
[11] "The difference between public and private blockchain," *Blockchain Pulse: IBM Blockchain Blog*, 31-May-2017. [Online]. Available: https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/. [Accessed: 25-Oct-2019].
[12] "Introduction to Permissioned Blockchains," *101 Blockchains*, 02-Jun-2019. [Online]. Available: https://101blockchains.com/permissioned-blockchain/. [Accessed: 19-Dec-2019].
[13] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," p. 9.
[14] "State of Blockchain: Q3 2016 - CoinDesk." [Online]. Available: https://www.coindesk.com/research/state-of-blockchain-q3-2016#. [Accessed: 29-Oct-2019].
[15] "Use Ethereum | Ethereum." [Online]. Available: https://www.ethereum.org/use/. [Accessed: 29-Oct-2019].
[16] "Blockchain Technology History: Ultimate Guide," *101 Blockchains*, 03-Nov-2018. [Online]. Available: https://101blockchains.com/history-of-blockchain-timeline/. [Accessed: 17-Dec-2019].
[17] "Hyperledger Fabric – Hyperledger." [Online]. Available: https://www.hyperledger.org/projects/fabric. [Accessed: 29-Oct-2019].
[18] "Hyperledger Indy – Hyperledger." [Online]. Available: https://www.hyperledger.org/projects/hyperledger-indy. [Accessed: 29-Oct-2019].
[19] "Hyperledger Burrow – Hyperledger." [Online]. Available: https://www.hyperledger.org/projects/hyperledger-burrow. [Accessed: 29-Oct-2019].
[20] "Hyperledger Iroha – Hyperledger." [Online]. Available: https://www.hyperledger.org/projects/iroha. [Accessed: 29-Oct-2019].
[21] "Hyperledger: The Enterprise Blockchain." [Online]. Available: https://101blockchains.com/hyperledger-blockchain/#prettyPhoto. [Accessed: 15-Dec-2019].
[22] "GitHub - corda/corda: Corda is an open source blockchain project, designed for business from the start. Only Corda allows you to build interoperable blockchain networks that transact in strict privacy. Corda's smart contract technology allows businesses to transact directly, with value." [Online]. Available: https://github.com/corda/corda. [Accessed: 29-Oct-2019].
[23] "A Zero-Knowledge Proof: Improving Privacy on a Blockchain | Altoros." [Online]. Available: https://www.altoros.com/blog/zero-knowledge-proof-improving-privacy-for- a-blockchain/. [Accessed: 29-Oct-2019].
[24] "How manufacturers can use blockchain for inventory management." [Online]. Available: https://www.allerin.com/blog/how-manufacturers-can-use-blockchain-for-inventory-management. [Accessed: 29-Oct-2019].
[25] "4. EU Regulatory Framework | Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion | Better Regulation." [Online]. Available: https://service.betterregulation.com/document/344399. [Accessed: 31-Oct-2019].

[26] "Bitcoin Energy Consumption Index," *Digiconomist*. [Online]. Available: https://digiconomist.net/bitcoin-energy-consumption. [Accessed: 31-Oct-2019].
[27] "Bitcoin Could Consume as Much Electricity as Denmark by 2020 - VICE." [Online]. Available: https://www.vice.com/en_us/article/aek3za/bitcoin-could-consume-as-much-electricity-as-denmark-by-2020. [Accessed:29-Oct-2019].
[28] "Ethereum's Proof of Stake Protocol in Review," *CryptoSlate*, 23-Apr-2018. [Online]. Available: https://cryptoslate.com/ethereums-proof-of-stake-protocol-in-review/. [Accessed: 31-Oct-2019].
[29] "Consensus Algorithms: The Root Of The Blockchain Technology," *101 Blockchains*, 25- Aug-2018. [Online]. Available: https://101blockchains.com/consensus-algorithms- blockchain/. [Accessed: 17-Dec-2019].
[30] "Consensus Algorithms: The Root Of The Blockchain Technology," *101 Blockchains*, 25- Aug-2018. [Online]. Available: https://101blockchains.com/consensus-algorithms- blockchain/. [Accessed: 17-Dec-2019].
[31] "Lamport et al. - The Byzantine Generals Problem.pdf." .
[32] "bitfury-digital_assets_on_public_blockchains-1.pdf." .
[33] "On Blockchain Auditability.pdf." .
[34] "Cryptography in .NET Succinctly ⋆ Programming and Tech Blog." [Online]. Available: https://dirkstrauss.com/cryptography-succinctly/. [Accessed: 31-Oct-2019].
[35] "FAQ - Bitcoin." [Online]. Available: https://bitcoin.org/en/faq#general. [Accessed: 31- Oct-2019].
[36] G. Hileman and M. Rauchs, "2017 Global Cryptocurrency Benchmarking Study," *SSRN Electron. J.*, 2017, doi: 10.2139/ssrn.2965436.
[37] European Central Bank, *Virtual currency schemes*. Frankfurt am Main: European Central Bank, 2012.
[38] "Page de recherche," *Banque de France*. [Online]. Available: https://www.banque-france.fr/search-es. [Accessed:01-Nov-2019].
[39] D. He *et al.*, "Virtual Currencies and Beyond: Initial Considerations," *Staff Discuss. Notes*, vol. 16, no. 03, p. 1, 2016, doi: 10.5089/9781498363273.006.
[40] M. the C. F. Aziz, "Altcoins vs. Tokens: What's the Difference?," *Master The Crypto*, 07- Aug-2017. [Online]. Available: https://masterthecrypto.com/differences-between-cryptocurrency-coins-and-tokens/. [Accessed:04-Nov-2019].
[41] J. Rohr and A. Wright, "Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets," Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 3048104, Oct. 2017.
[42] "IFRS Accounting for crypto-assets.pdf." .
[43] D. A. Zetzsche, R. P. Buckley, D. W. Arner, and L. Föhr, "The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators," Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 3072298, Jul. 2018.
[44] "Delaware Passes Law Permitting Companies to Use Blockchain Technology to Issue and Track Shares - Publications - Allen & Overy." [Online]. Available: http://www.allenovery.com/publications/en-gb/Pages/Delaware-Passes-Law-Permitting-Companies-to-Use-Blockchain-Technology-to-Issue-and-Track-Shares-.aspx. [Accessed: 04-Nov-2019].
[45] "An Illustrated Guide to Cryptographic Hashes." [Online]. Available: http://www.unixwiz.net/techtips/iguide-crypto-hashes.html. [Accessed: 17-Dec-2019].
[46] "Cryptography and Computer Privacy." [Online]. Available: https://www.apprendre-en-ligne.net/crypto/bibliotheque/feistel/index.html. [Accessed: 05-Nov-2019].
[47] "An Illustrated Guide to Cryptographic Hashes." [Online]. Available: http://unixwiz.net/techtips/iguide-crypto-hashes.html. [Accessed: 05-Nov-2019].

[48] "crypto-hash-3.gif (600×271)." [Online]. Available: http://unixwiz.net/images/crypto-hash-3.gif. [Accessed: 05-Nov-2019].
[49] "SHA-1," *Wikipedia*. 30-Oct-2019.
[50] "RSA Laboratories - 3.6.6 What are MD2, MD4, and MD5?" [Online]. Available: https://web.archive.org/web/20110901034903/http://www.rsa.com/rsalabs/node.asp?id=2253. [Accessed: 06-Nov-2019].
[51] "MD4," *Wikipedia*. 26-Sep-2019.
[52] "MD4," *Wikipedia*. 26-Sep-2019.
[53] "Sasaki et al. - 2007 - New Message Difference for MD4.pdf." .
[54] "MD5," *Wikipedia*. 22-Dec-2019.
[55] "International Standard Book Number," *Wikipedia*. 30-Oct-2019.
[56] "The ProFTPD Project: MD5 sums and PGP signatures of release files." .
[57] C. Cimpanu, "A quarter of major CMSs use outdated MD5 as the default password hashing scheme," *ZDNet*. [Online]. Available: https://www.zdnet.com/article/a-quarter- of-major-cmss-use-outdated-md5-as-the-default-password-hashing-scheme/. [Accessed: 06-Nov-2019].
[58] "Poisonous MD5 – Wolves Among the Sheep – Silent Signal Techblog." [Online]. Available: https://blog.silentsignal.eu/2015/06/10/poisonous-md5-wolves-among-the- sheep/. [Accessed: 07-Nov-2019].
[59] "SHA-1," *Wikipedia*. 23-Dec-2019.
[60] "Schneier on Security: Cryptography Engineering." .
[61] "Wayback Machine." .
[62] "SHA-2," *Wikipedia*. 19-Nov-2019.
[63] I. T. L. Computer Security Division, "NIST Policy on Hash Functions - Hash Functions | CSRC," *CSRC | NIST*, 04-Jan-2017. [Online]. Available: https://csrc.nist.gov/projects/hash-functions/nist-policy-on-hash-functions. [Accessed: 10-Nov-2019].
[64] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Gener. Comput. Syst.*, vol. 82, pp. 395–411.
[65] R. Böhme, N. Christin, B. Edelman, and T. Moore, "Bitcoin: Economics, Technology, and Governance," *J. Econ. Perspect.*, vol. 29, no. 2, pp. 213–238, May 2015, doi: 10.1257/jep.29.2.213.
[66] E. Swenson-Healey, *laser/go-merkle-tree*. 2019.
[67] "Hitching Healthcare to the Chain: An Introduction to Blockchain Technology in the Healthcare Sector | TIM Review." .
[68] C. C. Agbo, Q. H. Mahmoud, and J. M. Eklund, "Blockchain Technology in Healthcare: A Systematic Review," *Healthc. Basel Switz.*, vol. 7, no. 2, Apr. 2019, doi: 10.3390/healthcare7020056.
[69] "Hitching Healthcare to the Chain: An Introduction to Blockchain Technology in the Healthcare Sector | TIM Review." [Online]. Available: https://timreview.ca/article/1111. [Accessed: 13-Nov-2019].
[70] R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain in Electronic Health Records Systems," *IEEE Access*, vol. 6, pp. 11676–11686, 2018, doi: 10.1109/ACCESS.2018.2801266.
[71] "Blockchain distributed ledger technologies for biomedical and healthcare applications | Journal of the American Medical Informatics Association | Oxford Academic." [Online]. Available: https://academic.oup.com/jamia/article/24/6/1211/4108087. [Accessed: 13- Nov-2019].
[72] "Patients and Privacy: GDPR Compliance for Healthcare Organizations - Security News - Trend Micro DK." .

[73] "Blockchain Technology | Circulation: Cardiovascular Quality and Outcomes." [Online]. Available: https://www.ahajournals.org/doi/10.1161/CIRCOUTCOMES.117.003800. [Accessed: 13-Nov-2019].
[74] "Blockchain technology in healthcare: The revolution starts here - IEEE Conference Publication." .
[75] "MedRec: Using Blockchain for Medical Data Access and Permission Management— MIT Media Lab." .
[76] "Blockchain technology innovations - IEEE Conference Publication." .
[77] "Hyperledger fabric." .
[78] "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology - ScienceDirect." .
[79] "MedRec." .
[80] "Medibloc," *MediBloc*. [Online]. Available: https://medibloc.org. [Accessed: 17-Nov-2019].
[81] "IRYO.IO." .
[82] "MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain | SpringerLink." .
[83] "FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data - ScienceDirect." .
[84] "MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain - IEEE Journals & Magazine." .
[85] "A medical records managing and securing blockchain based system supported by a Genetic Algorithm and Discrete Wavelet Transform - ScienceDirect." .
[86] "Secure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain in Electronic Health Records Systems - IEEE Journals & Magazine." .
[87] "Secure Cloud-Based EHR System Using Attribute-Based Cryptosystem and Blockchain | SpringerLink." [Online]. Available: https://link.springer.com/article/10.1007%2Fs10916- 018-0994-6. [Accessed: 14-Nov-2019].
[88] "Current Links for doi: 10.1049/trit.2018.0014." .
[89] "Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain | SpringerLink." .
[90] "Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control | SpringerLink." .
[91] "How to Use Blockchain for Diabetes Health Care Data and Access Management: An Operational Concept - Simon Lebech Cichosz, Mads Nibe Stausholm, Thomas Kronborg, Peter Vestergaard, Ole Hejlesen, 2019." [Online]. Available: https://journals.sagepub.com/doi/10.1177/1932296818790281. [Accessed: 14-Nov- 2019].
[92] I. Radanović and R. Likić, "Opportunities for Use of Blockchain Technology in Medicine," *Appl. Health Econ. Health Policy.*, vol. 16, no. 5, pp. 583–590, Oct. 2018, doi: 10.1007/s40258-018-0412-8.
[93] M. N. Kamel Boulos, J. T. Wilson, and K. A. Clauson, "Geospatial blockchain: promises, challenges, and scenarios in health and healthcare," *Int. J. Health Geogr.*, vol. 17, no. 1, p. 25, Jul. 2018, doi: 10.1186/s12942-018-0144-x.
[94] "How blockchain technology can change medicine: Postgraduate Medicine: Vol 130, No 4." .
[95] "Blockchain Technology: A Data Framework to Improve Validity, Trust, and Accountability of Information Exchange in Health Professions Education." .
[96] T. Nugent, D. Upton, and M. Cimpoesu, "Improving data transparency in clinical trials using blockchain smart contracts," *F1000Research*, vol. 5, p. 2541, Oct. 2016, doi: 10.12688/f1000research.9756.1.
[97] "ScienceDirect Full Text PDF." .

[98] “IEEE Xplore Abstract Record.” .
[99] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, “Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring,” *J. Med. Syst.*, vol. 42, no. 7, p. 130, Jun. 2018, doi: 10.1007/s10916- 018-0982-x.
[100] “JMU - Tamper-Resistant Mobile Health Using Blockchain Technology | Ichikawa | JMIR mHealth and uHealth.” .
[101] “Continuous Patient Monitoring With a Patient Centric Agent: A Block Architecture - IEEE Journals & Magazine.” .
[102] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, and V. Santamaría, “Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough?,” *Future Internet*, vol. 10, no. 2, p. 20, Feb. 2018, doi: 10.3390/fi10020020.
[103] L. Zhou, L. Wang, and Y. Sun, “MIStore: a Blockchain-Based Medical Insurance Storage System,” *J. Med. Syst.*, vol. 42, no. 8, p. 149, Jul. 2018, doi: 10.1007/s10916-018- 0996-4.
[104] J. Tsai, “Transform Blockchain into Distributed Parallel Computing Architecture for Precision Medicine,” *2018 IEEE 38th Int. Conf. Distrib. Comput. Syst. ICDCS*, pp. 1290–1299, 2018, doi: 10.1109/icdcs.2018.00129.
[105] P. Mamoshina *et al.*, “Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare,” *Oncotarget*, vol. 9, no. 5, pp. 5665–5690, Nov. 2017, doi: 10.18632/oncotarget.22345.
[106] A. Juneja and M. Marefat, “Leveraging blockchain for retraining deep learning architecture in patient-specific arrhythmia classification,” 2018, pp. 393–397, doi: 10.1109/BHI.2018.8333451.
[107] “doc.ai - Get the full picture of your health.” [Online]. Available: https://doc.ai/. [Accessed: 17-Nov-2019].
[108] “Bowhead Health - Optimize Your Health.” .
[109] “Full Text PDF.” .
[110] G. Falco, C. Li, P. Fedorov, C. Caldera, R. Arora, and K. Jackson, “NeuroMesh: IoT Security Enabled by a Blockchain Powered Botnet Vaccine,” 2019, doi: 10.1145/3312614.3312615.
[111] “Chronicled.” [Online]. Available: https://www.chronicled.com/. [Accessed: 17-Nov-2019].
[112] “Blockchain Technology Solutions | Ethereum Solutions | ConsenSys.” [Online]. Available: https://consensys.net/. [Accessed: 17-Nov-2019].
[113] “DeepMind’s health team joins Google Health | DeepMind.” .
[114] “Zhang et al. - 2017 - Metrics for assessing blockchain-based healthcare .pdf.” .
[115] M. C. Wong, K. C. Yee, and C. Nøhr, “Socio-Technical Considerations for the Use of Blockchain Technology in Healthcare,” *Stud. Health Technol. Inform.*, vol. 247, pp. 636– 640, 2018.
[116] “Project Feature Cloud - Federated Machine Learning.” .
[117] “CUREX | Secure and Private Health Data Exchnage.” .
[118] “CUREX Platform | CUREX.” [Online]. Available: https://curex-project.eu/content/curex-platform. [Accessed: 19-Dec-2019].
[119] “RAIS - Home.” .
[120] “PANACEA Research.” .
[121] “MyHealthMyData,” *MyHealthMyData*. [Online]. Available: http://www.myhealthmydata.eu/. [Accessed: 17-Nov-2019].
[122] “STOP-IT » project about protection of critical water infrastructures.” .

[123] P. Mamoshina *et al.*, "Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare," *Oncotarget*, vol. 9, no. 5, pp. 5665–5690, Nov. 2017, doi: 10.18632/oncotarget.22345.

[124] N. Cory, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?," Information Technology and Innovation Foundation, May 2017.

[125] O. for C. Rights (OCR), "Your Rights Under HIPAA," *HHS.gov*, 07-May-2008. [Online]. Available: https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html. [Accessed: 02-Dec-2019].

[126] "Full Text PDF." .

[127] A. J. Menezes, P. C. van Oorschot, S. A. Vanstone, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. CRC Press, 2018.

[128] T. Erl, *Service-oriented architecture: concepts, technology, and design*. Upper Saddle River, NJ: Prentice Hall Professional Technical Reference, 2005.

[129] "Reaching Agreement in the Presence of Faults." [Online]. Available: https://dl.acm.org/citation.cfm?id=322188. [Accessed: 02-Dec-2019].

[130] "Kwon - Tendermint Consensus without Mining.pdf." .

[131] "Public Key Cryptography | SpringerLink." [Online]. Available: https://link.springer.com/book/10.1007%2Fb75033#page=304. [Accessed: 02-Dec- 2019].

[132] M. Asgari and I. Shafran, "Predicting Severity of Parkinson's Disease from Speech," *Conf. Proc. Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. IEEE Eng. Med. Biol. Soc. Conf.*, vol. 2010, pp. 5201–4, Aug. 2010, doi: 10.1109/IEMBS.2010.5626104.

[133] F. Jiang, W. Huang, Y. Wang, P. Tian, X. Chen, and Z. Liang, "Nucleic Acid Amplification Testing and Sequencing Combined with Acid-Fast Staining in Needle Biopsy Lung Tissues for the Diagnosis of Smear-Negative Pulmonary Tuberculosis," *PloS One*, vol. 11, no. 12, p. e0167342, 2016, doi: 10.1371/journal.pone.0167342.

[134] "Environmental Epigenomics in Health and Disease - Epigenetics and Disease Origins | Randy L Jirtle | Springer." [Online]. Available: https://www.springer.com/gp/book/9783642233791. [Accessed: 02-Dec-2019].

[135] G. A. Passos, Ed., *Transcriptomics in Health and Disease*. Springer International Publishing, 2014.

[136] "360˚ of Health Data: Harnessing big data for better health | ABPI." [Online]. Available: https://www.abpi.org.uk/publications/360-of-health-data-harnessing-big-data-for-better-health/. [Accessed: 02-Dec-2019].

[137] D. A. Glei, N. Goldman, Y.-H. Lin, and M. Weinstein, "Age-Related Changes in Biomarkers: Longitudinal Data from a Population-Based Sample," *Res. Aging*, vol. 33, no. 3, pp. 312–326, May 2011, doi: 10.1177/0164027511399105.

[138] J. L. Sanders *et al.*, "Heritability of and mortality prediction with a longevity phenotype: the healthy aging index," *J. Gerontol. A. Biol. Sci. Med. Sci.*, vol. 69, no. 4, pp. 479–485, Apr. 2014, doi: 10.1093/gerona/glt117.

[139] "Aging." [Online]. Available: https://www.aging-us.com/article/101227/text. [Accessed: 02-Dec-2019].

[140] "Aging | Frailty and inflammatory markers in older adults with cancer - Full Text." [Online]. Available: https://www.aging-us.com/article/101162/text. [Accessed: 02-Dec-2019].

[141] P. Mamoshina *et al.*, "Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare," *Oncotarget*, vol. 9, no. 5, pp. 5665–5690, Jan. 2018, doi: 10.18632/oncotarget.22345.