ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΚΑΤΑΝΕΜΗΜΕΝΕΣ ΕΦΑΡΜΟΓΕΣ BLOCKCHAIN ΣΤΟΝ ΤΟΜΕΑ ΤΗΣ ΥΓΕΙΑΣ

ΚΑΨΗΣ ΠΑΝΑΓΙΩΤΗΣ
Α.Μ. 71347137

Εισηγητής: ΚΑΡΚΑΖΗΣ ΠΑΝΑΓΙΩΤΗΣ, Αναπληρωτής Καθηγητής

(κενό φύλλο)

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Σχεδίαση ολοκληρωμένου συστήματος συγγραφής διπλωματικής εργασίας

ΚΑΤΑΝΕΜΗΜΕΝΕΣ ΕΦΑΡΜΟΓΕΣ BLOCKCHAIN ΣΤΟΝ ΤΟΜΕΑ ΤΗΣ ΥΓΕΙΑΣ
Α.Μ. 71347137

Ημερομηνία εξέτασης 29/07/2024

Μέλη Εξεταστικής Επιτροπής συμπεριλαμβανομένου και του Εισηγητή

Α/α	ΟΝΟΜΑ ΕΠΩΝΥΜΟ	ΒΑΘΜΙΔΑ/ΙΔΙΟΤΗΤΑ	ΥΠΟΓΡΑΦΗ
1	Καρκαζής Παναγιώτης	Αναπληρωτής Καθηγητής	PANAGIOTIS KARKAZIS Digitally signed by PANAGIOTIS KARKAZIS Date: 2024.08.02 12:22:34 +03'00'
2	Μυριδάκης Νικόλαος	Αναπληρωτής Καθηγητής	Nikolaos Myridakis Digitally signed by Nikolaos Myridakis Date: 2024.08.02 19:49:40 +03'00'
3	Μαυρομάτης Κωνσταντίνος	Λέκτορας	Konstantinos Mavrommatis Digitally signed by Konstantinos Mavrommatis Date: 2024.08.02 22:46:16 +03'00'

(κενό φύλλο)

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΠΤΥΧΙΑΚΗΣ/ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος Καψής Παναγιώτης του Ιωάννη, με αριθμό μητρώου 71347137 φοιτητής του Πανεπιστημίου Δυτικής Αττικής της Σχολής Μηχανικών του Τμήματος Μηχανικών Πληροφορικής και Υπολογιστών, δηλώνω υπεύθυνα ότι:

«Είμαι συγγραφέας αυτής της πτυχιακής/διπλωματικής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.

Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου».

Ο/Η Δηλών/ούσα

(κενό φύλλο)

ΕΥΧΑΡΙΣΤΙΕΣ

Η παρούσα διπλωματική εργασία ολοκληρώθηκε μετά από επίμονες προσπάθειες, σε ένα ενδιαφέρον γνωστικό αντικείμενο, όπως αυτό της εφαρμογής της τεχνολογίας Blockchain στην υγειονομική περίθαλψη. Την προσπάθειά μου αυτή υποστήριξε ο επιβλέπων καθηγητής μου, τον οποίο θα ήθελα να ευχαριστήσω. Ακόμα θα ήθελα να ευχαριστήσω την οικογένειά μου για τη συμπαράσταση κατά τη διάρκεια των σπουδών μου.

(κενό φύλλο)

ΠΕΡΙΛΗΨΗ

Η τεχνολογία έχει πραγματικά εισβάλει στη ζωή μας τα τελευταία χρόνια. Η τεχνολογία Blockchain είναι μια από τις πιο σημαντικές ανακαλύψεις και δημιουργικές εξελίξεις που διαδραματίζουν σημαντικό ρόλο στον επαγγελματικό κόσμο σήμερα. Το blockchain ως ολοκληρωμένη έννοια προέκυψε με το πρώτο κρυπτονόμισμα, το Bitcoin, ως τρόπος διατήρησης δεδομένων, διασφαλίζοντας πάντα τη μοναδικότητα και την εγκυρότητά του, χωρίς να εμπλέκεται καμία κεντρική ελεγκτική αρχή. Αυτή η τεχνολογία αναπτύσσεται προς την κατεύθυνση της συνεχούς επανάστασης και αλλαγής. Είναι ένα blockchain που επικαλύπτει πληροφορίες και διατηρεί την εμπιστοσύνη μεταξύ των ατόμων ανεξάρτητα από το πόσο μακριά βρίσκονται. Η άνοδος της τεχνολογίας ανάγκασε τους ακαδημαϊκούς και τους ειδικούς να εξετάσουν εξονυχιστικά νέους τρόπους εφαρμογής της τεχνολογίας blockchain σε ένα ευρύ φάσμα τομέων. Η τεχνολογία είναι σχετικά νέα, έχει αναπτυχθεί την τελευταία δεκαετία και χρησιμοποιείται στη νομοθεσία, τις ασφάλειες, στις επιστήμες υγείας, τις αλυσίδες εφοδιασμού, τη διαχείριση πνευματικών δικαιωμάτων και πολλούς άλλους τομείς πέρα από αυτόν που απέκτησε φήμη από τα κρυπτονομίσματα. Επιδεικνύει επίσης τις δυνατότητες της τεχνολογίας blockchain να φέρει επανάσταση στον κλάδο της υγειονομικής περίθαλψης. Στην παρούσα εργασία αναλύεται η τεχνολογία του Blockchain καθώς και οι εφαρμογές της στις επιστήμες υγείας. Στη συνέχεια αναφέρονται τύποι πρωτοκόλλων συναίνεσης και παρουσιάζονται διάφορα παραδείγματα χρήσης τους. Επιπλέον, αναλύεται ο ρόλος του κάθε ατόμου στην επιλογή μιας πλατφόρμας ανάπτυξης εφαρμογών blockchain καθώς και μερικές από τις πιο δημοφιλείς πλατφόρμες ανάπτυξης εφαρμογών.

ABSTRACT

Technology has really invaded our lives in recent years. Blockchain technology is nowadays one of the most important breakthroughs and creative developments that play an important role in the professional world. Blockchain as a comprehensive concept emerged with the first cryptocurrency, Bitcoin, as a way of storing data, always ensuring its uniqueness and validity, without any central controlling authority involved. This technology is developing in the direction of constant revolution and change. It is a blockchain that overlays information and maintains trust between individuals no matter how far apart they are. The rise of the technology has forced academics and experts to scrutinize new ways of applying blockchain technology in a wide range of fields. The technology is relatively new, having been developed in the last decade and used in law, insurance, health sciences, supply chains, copyright management and many other areas beyond the one gained fame from cryptocurrencies. It also demonstrates the potential of blockchain technology to revolutionize the healthcare industry. In this paper, the blockchain technology and its applications in healthcare are analyzed. Types of consensus protocols are mentioned and various examples of their use are presented. In addition, the role of each individual in choosing a blockchain application development platform as well as some of the most popular application development platforms are analyzed.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 1: Εισαγωγή 15
1.1 Επισκόπηση του Blockchain 15
1.2 Λειτουργία του Blockchain 17
1.3 Κρυπτογραφία στο Blockchain 19
1.4 Είδος Δικτύου και Εξέλιξη του Blockchain 21
1.5 Χαρακτηριστικά του Blockchain 24
ΚΕΦΆΛΑΙΟ 2: Διαδικασία Συναλλαγών 26
2.1 Διαδικασία Συναλλαγής του Blockchain 26
2.2 Διαδικασία Συναλλαγής του Bitcoin 27
2.3 Διαδικασία Συναλλαγής του Ethereum 28
ΚΕΦΑΛΑΙΟ 3: Consensus Αλγόριθμοι 29
3.1 Proof of Work (PoW) 30
3.2 Proof of Stake (PoS) 32
3.3 Delegated Proof of Stake (DPoS) 33
3.4 Πλεονεκτήματα και Μειονεκτήματα 33
3.5 Άλλοι Consensus Αλγόριθμοι 34
ΚΕΦΑΛΑΙΟ 4: Εφαρμογές Blockchain 35
4.1 Εισαγωγή 35
4.2 Internet of Things 38
4.2.1 Ενίσχυση Ασφάλειας Συνδεδεμένων Συσκευών 38
4.2.2 Διατήρηση Ανωνυμίας 39
4.2.3 Έξυπνα Συμβόλαια 39
4.2.4 Μηχανισμοί Διαχείρισης Συσκευών και Πρωτοκόλλων 42
4.2.5 Ασφάλεια Δικτύου 43
4.3 Blockchain και Ενέργεια 44
4.3.1 Έλεγχος της Αγοράς Ηλεκτρικής Ενέργειας μεταξύ Μηχανών 44
4.3.2 Διευκόλυνση του Εμπορίου Ενέργειας 44
4.3.3 Αύξηση Ασφάλειας των Ενεργειακών Δικτυών 45
4.3.4 Βοήθεια στη Διάχυση της Πράσινης Ενέργειας 45
4.4 Blockchain και Οικονομία 46
4.4.1 Καλύτερη Επεξεργασία Συναλλαγών 46
4.4.2 Βιώσιμες Τραπεζικές και Χρηματοοικονομικές Συναλλαγές 47
4.4.3 Ενίσχυση της Οικονομικής Ασφάλειας 47
4.4.4 Απόρρητο και Αυτοματοποιημένα Οικονομικά Συμβόλαια 48
4.4.5 Βιομηχανία Τυχερών Παιχνιδιών 48

4.5 Blockchain και Κυβέρνηση 49
4.5.1 Ηλεκτρονική Διακυβέρνηση 49
4.5.2 Πραγματοποίηση μιας Ψηφιακής Ταυτότητας 50
4.5.3 Ηλεκτρονική Ψηφοφορία 50
4.5.4 Ενίσχυση του Ελέγχου των Συσκευών Μέτρησης 51
4.6 Blockchain και Υγειονομική Περίθαλψη 52
4.6.1 Blockchains στα Ηλεκτρονικά Αρχεία Υγείας 53
4.6.2 Απόκτηση και Αποθήκευση Δεδομένων στον Κλάδο της Ιατρικής 55
4.6.3 Λύσεις Blockchain για Τήρηση Ιατρικών Αρχείων 56
4.6.4 Κοινή Χρήση Δεδομένων και Διαλειτουργικότητα 57
4.6.5 Λύσεις Blockchain για Κοινή Χρήση Δεδομένων 58
4.6.6 Ασφάλεια Δεδομένων και Διαχείριση Ταυτότητας 58
4.6.7 Λύσεις Blockchain για Ασφάλεια Δεδομένων και Διαχείριση Ταυτότητας 59
4.6.8 Blockchain στην Κλινική Ερευνά 59
4.6.9 Blockchain και Νευροεπιστημη 60
4.6.10 Blockchain και Μεταμόσχευση Οργάνων 61
4.6.11 Φαρμακευτικός Κλάδος 62
4.6.12 Λύσεις Blockchain στον Φαρμακευτικό Κλάδο 62
ΚΕΦΑΛΑΙΟ 5: Προκλήσεις 63
5.1 Ασφάλεια και Ιδιωτικό Απόρρητο των Δεδομένων 63
5.2 Διαχείριση Χωρητικότητας Αποθήκευσης 64
5.3 Προκλήσεις Τυποποίησης 64
5.4 Κοινωνικές Προκλήσεις 65
ΚΕΦΑΛΑΙΟ 6: Σχεδίαση Πρότυπης Εφαρμογής Υγείας 65
6.1 Στόχοι 66
6.2 Επισκόπηση 66
6.3 Πλεονεκτήματα του Εφαρμοζόμενου Συστήματος 66
6.4 Αρχιτεκτονική του Συστήματος και Στοιχεία 69
6.5 Use – Case Σεναριο 74
6.6 Συμπερασματα και Μελοντικες Εξελιξεις 78
ΚΕΦΑΛΑΙΟ 7: Επίλογος 80
ΒΙΒΛΙΟΓΡΑΦΙΑ 81

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

Εικόνα 1. Ψηφιακή υπογραφή και κατακερματισμός που χρησιμοποιούνται στις συναλλαγές blockchain [127] 20
Εικόνα 2. Κρυπτογραφία δημόσιου κλειδιού και συνάρτηση κατακερματισμού για τη διεύθυνση Bitcoin [127] 21
Εικόνα 3. Δημόσια, Υβριδικά και Ιδιωτικά Blockchain [131] 22
Εικόνα 4. Αρχιτεκτονική του Blockchain [128] 23
Εικόνα 5. Χαρακτηριστικά του Blockchain [130] 26
Εικόνα 6. Τομείς εφαρμογής της τεχνολογίας Blockchain [125] 36
Εικόνα 7. Πλήθος εφαρμογών Blockchain ανά τομέα [126] 37
Εικόνα 8. Ethereum, Nem, Neo, Cardano και Hyperledger Blockchain 42
Εικόνα 9. Τομείς εφαρμογής Blockchain [127] 43
Εικόνα 10. Πλεονεκτήματα και Μειονεκτήματα Blockchain στην Κυβέρνηση [129] 50
Εικόνα 11. Εφαρμογές Blockchain στην Υγειονομική Περίθαλψη [124] 55
Εικόνα 12. Πλεονεκτήματα και Μειονεκτήματα Blockchain στην Υγεία [124] 63
Εικόνα 13. SWOT Ανάλυση [124] 65
Εικόνα 14. Κρυπτογραφία Δεδομένων 67
Εικόνα 15. Αποτελέσματα Bscscan 68
Εικόνα 16. Αρχιτεκτονική Εφαρμογής 69
Εικόνα 17. Use - Case διάγραμμα 69
Εικόνα 18. Φόρμα Σύνδεσης 74
Εικόνα 19. MetaMask Interaction 75
Εικόνα 20. Φόρμα Ασθενών 75
Εικόνα 21. Φόρμα Γιατρών 76
Εικόνα 22. Πληροφορίες Ασθενούς 76
Εικόνα 23. Πληροφορίες Γιατρού 76
Εικόνα 24. Δέσμευση Ασθενή - Γιατρού 76
Εικόνα 25. Προφίλ Γιατρού 77
Εικόνα 26. Ενημέρωση Κατάστασης Ασθενή 77
Εικόνα 27. Στοιχεία Ασθενή 78

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

PoW	Proof of Work
PoS	Proof of Stake
ECDSA	Elliptic Curve Digital Signature Algorithm
zkSNARKS	Zero-Knowledge Succinct Non-Interactive Argument of Knowledge
P2PKH	Pay To Public Key Hash
SoC	Speed of Consensus
TA	Trust Authority
SHA-256	Secure Hash Algorithm 256-bit
UTXO	Unspent Transaction Output
BTC	Bitcoin
EOA	Externally Owned Account
CA	Certificate Authority
SC	Smart Contract
Wei	Weekly Economic Index
BGP	Byzantine Generals Problem
PoA	Proof of Activity
PoC	Proof of Capacity
PoI	Proof of Importance
PoSt	Proof of Storage
PoD	Proof of Deposit
BFT	Byzantine Fault Tolerance
PKI	Public key infrastructure
PoET	Proof of Elapsed Time
SGX	Software Guard Extensions
PoR	Proof of Reputation
IoT	Internet of Things
RFID	Radio-Frequency Identification
EC20	Ethereum Request for Comment 20
dApp	decentralized Application
P2P	Peer to Peer
EHRs	Electronic Health Records
IoMT	Internet of Medical Things
QoE	Quality of Experience
UI	User Interface
HIV	Human Immunodeficiency Virus
HIPAA	Health Insurance Portability and Accountability Act
AR/VR	Augmented Reality/Virtual Reality
Gcoin	Global Governance Coin
SWOT	Strengths, Weaknesses, Opportunities, and Threats
ML	Machine Learning
TN	Τεχνητή Νοημοσύνη

ΚΕΦΑΛΑΙΟ 1: Εισαγωγή

1.1 Επισκόπηση του Blockchain

Το blockchain, σε αντίθεση με τις συμβατικές τεχνικές, επιτρέπει τις άμεσες μεταφορές ψηφιακών περιουσιακών στοιχείων από ομότιμο σε ομότιμο [1]. Η τεχνολογία που ονομάζεται blockchain αναπτύχθηκε αρχικά για την εξυπηρέτηση του γνωστού χρήματος Bitcoin. Ο Satoshi παρουσίασε το Bitcoin για πρώτη φορά το 2008 και το λάνσαρε το 2009 [2]. Έκτοτε, το χρηματιστήριο γνώρισε τεράστια ανάπτυξη, φτάνοντας τα 10 δισεκατομμύρια δολάρια το 2016. Η αλυσίδα μπλοκ είναι ουσιαστικά μια σειρά από μπλοκ που χρησιμοποιεί ένα δημόσιο βιβλίο για να κρατήσει όλα τα δεσμευμένα γεγονότα [3]. Το blockchain λειτουργεί σε ένα αυτόνομο περιβάλλον που καθίσταται δυνατό με τη συμπερίληψη διαφόρων βασικών τεχνολογιών, συμπεριλαμβανομένων των διασκορπισμένων μεθόδων συμφωνίας, των κρυπτογραφικών κατακερματισμών και των ψηφιακών υπογραφών. Δεν υπάρχει ανάγκη για μεσάζοντες που να επιβεβαιώνουν ή να ελέγχουν οποιαδήποτε από τις συναλλαγές, επειδή όλες λαμβάνουν χώρα αποκεντρωμένα [4].

Η τεχνολογία blockchain έχει ορισμένους τεχνικούς περιορισμούς, παρά το γεγονός ότι έχει τη δυνατότητα να αντικαταστήσει πολλά από τα υπάρχοντα ψηφιακά δίκτυα. Οι πλατφόρμες που βασίζονται στο κρυπτονόμισμα αντιμετωπίζουν σημαντικές προκλήσεις κλιμάκωσης [5]. Τα προβλήματα κλιμάκωσης με το Bitcoin μπορούν να αποδοθούν στο περιορισμένο μέγεθος και την κανονικότητα των μπλοκ, καθώς και στον μέγιστο αριθμό συναλλαγών που μπορεί να υποστηρίξει το δίκτυο [6]. Η απόδοση του δικτύου περιορίζεται από τον περιορισμό του μεγέθους των μπλοκ του 1 megabyte και την τυπική περίοδο δημιουργίας μπλοκ των 10 λεπτών στο δίκτυο Bitcoin [7].

Η ικανότητα ανάπτυξης του Bitcoin καθορίζεται από το μέγεθος των μπλοκ, ανεξάρτητα από τους κόμβους του δικτύου. Σε γενικές γραμμές, το Bitcoin μπορεί να διαχειριστεί μεταξύ 3 και 7 συναλλαγές ανά δευτερόλεπτο [8]. Ωστόσο, η απόδοση συναλλαγών περιορίζεται ουσιαστικά σε 2-4 συναλλαγές ανά δευτερόλεπτο, η οποία δεν επαρκεί για συναλλαγές υψηλής συχνότητας λόγω του μεγαλύτερου μεγέθους των νεοπαραγόμενων μπλοκ. Αυτή τη στιγμή υπάρχουν πάνω από 36 εκατομμύρια χρήστες Bitcoin, και καθώς ο αριθμός αυτός αυξάνεται με την πάροδο του χρόνου, θα έχει αρνητική επίδραση στη χωρητικότητα του δικτύου. Ανησυχίες θα δημιουργηθούν από διάφορα προβλήματα, όπως το ζήτημα της συμφόρησης της αλυσίδας μπλοκ, τις καθυστερήσεις των συναλλαγών και το υψηλότερο κόστος συναλλαγών. Εξαιτίας αυτού, η χρήση της τεχνολογίας για να βασιστεί μια επιχειρηματική στρατηγική της κυβέρνησης ή του ιδιωτικού τομέα στο δίκτυο blockchain μπορεί να μην είναι βιώσιμη. Επιπλέον, τα μεγαλύτερα μπλοκ απαιτούν περισσότερο αποθηκευτικό χώρο και διαδίδονται πιο αργά μέσω του δικτύου blockchain [9], γεγονός που θα οδηγήσει σε ζητήματα συγκεντρωτισμού και εμπιστοσύνης καθώς οι χρήστες θα προσπαθούν να τρέξουν και να διατηρήσουν ένα τόσο μεγάλο blockchain. Η αντιμετώπιση του συμβιβασμού μεταξύ του μεγέθους της αλυσίδας μπλοκ και της εμπιστοσύνης έχει γίνει έτσι πολύ δύσκολη.

Άλλα προβλήματα με το blockchain περιλαμβάνουν τη συνδεσιμότητα, την ανωνυμία, τη χρήση ενέργειας, την εξόρυξη selsh, την ασφάλεια και τη ρυθμιστική πολιτική. Η απουσία ενός τυποποιημένου συστήματος για την εταιρική υιοθέτηση και ενσωμάτωση των λύσεων που βασίζονται στην αλυσίδα μπλοκ δημιουργεί το πρόβλημα της συμβατότητας. Παρόλο που η αλυσίδα μπλοκ ισχυρίζεται ότι είναι εξαιρετικά ασφαλής και οι χρήστες διενεργούν συναλλαγές μόνο με τη χρήση ψηφιακών υπογραφών που συνδέονται με κρυπτογραφία δημόσιου-ιδιωτικού κλειδιού, διαρροές της ιδιωτικής ζωής μπορεί ακόμη να προκύψουν εντός του συστήματος [10]. Επιπλέον, μπορεί να βρεθεί η πραγματική διεύθυνση IP του χρήστη. Σοβαρά ζητήματα εγείρονται επίσης με τις μεθόδους συναίνεσης όπως η απόδειξη εργασίας (PoW) και η απόδειξη συμμετοχής (PoS).

Για παράδειγμα, η PoW είναι γνωστή για τη χρήση σημαντικής ποσότητας ηλεκτρικής ενέργειας επειδή οι ανθρακωρύχοι ανταγωνίζονται για τη δημιουργία μπλοκ επιλύοντας απαιτητικά μαθηματικά προβλήματα [11]. Στο PoS, οι πλούσιοι γίνονται προοδευτικά πλουσιότεροι επειδή η πιθανότητα να αποκτήσουν ένα μπλοκ εξαρτάται από το μέγεθος του στοιχήματος των ανθρακωρύχων [12]. Η εξόρυξη Selsh, κατά την οποία οι miners επωφελούνται περισσότερο από το εύλογο μερίδιό τους κρατώντας τα μπλοκ τους μυστικά, είναι ένα άλλο μειονέκτημα της τεχνολογίας blockchain [13]. Σε μια επίθεση 51%, ένας κόμβος αποκτά τον έλεγχο της πλειοψηφίας σε ένα δίκτυο και το εκμεταλλεύεται. Επιπλέον, λόγω των αβεβαιοτήτων που περιβάλλουν τις πιθανές κυβερνητικές ρυθμίσεις, θεωρείται ότι η τεχνολογία blockchain ενδέχεται να μην φτάσει στο ζενίθ της ή στην αναμενόμενη ευρεία χρήση από τους ενδιαφερόμενους φορείς [14]. Μία από τις κύριες υποκείμενες αιτίες μπορεί να είναι ότι οι κεντρικές τράπεζες δεν είναι πλέον σε θέση να επηρεάζουν την οικονομία μέσω μεσαζόντων χάρη στον αποκεντρωμένο χαρακτήρα του blockchain, γεγονός που αποτελεί κακό νέο για τις κυβερνήσεις. Ως εκ τούτου, πρέπει να ληφθούν μέτρα για την επίλυση αυτών των προβλημάτων στο κρυπτονόμισμα.

Τι είναι το blockchain; Το blockchain (αλυσίδα μπλοκ) είναι μια αποκεντρωμένη ψηφιακή τεχνολογία καταγραφής και αποθήκευσης δεδομένων, η οποία επιτρέπει τη διαφανή και ασφαλή καταγραφή συναλλαγών. Τα δεδομένα οργανώνονται σε μπλοκ, τα οποία συνδέονται διαδοχικά και κρυπτογραφούνται, δημιουργώντας έτσι μια αμετάβλητη και ανθεκτική σε παραβιάσεις αλυσίδα. Η τεχνολογία αυτή χρησιμοποιείται κυρίως για την καταγραφή συναλλαγών κρυπτονομισμάτων, αλλά βρίσκει εφαρμογή και σε άλλους τομείς όπως οι αλυσίδες εφοδιασμού, οι έξυπνες συμβάσεις και η πιστοποίηση δεδομένων[15]. Τα νέα μπλοκ μπορούν να υποβληθούν στο παγκόσμιο blockchain μόνο μετά από επιτυχημένο διαγωνισμό αποκεντρωμένης διαδικασίας συναίνεσης.

Συγκεκριμένα, εκτός από τις πληροφορίες εγγραφής συναλλαγών, ένα μπλοκ διατηρεί επίσης την τιμή κατακερματισμού ολόκληρου του μπλοκ, η οποία μπορεί να θεωρηθεί ως η κρυπτογραφημένη του εικόνα, συν την τιμή κατακερματισμού του προηγούμενου μπλοκ, η οποία αποτελεί τον κρυπτογραφικό σύνδεσμο για το προηγούμενο μπλοκ στο blockchain. Το δίκτυο επιβάλλει μια αποκεντρωμένη διαδικασία συναίνεσης που ελέγχει (i) την είσοδο νέων μπλοκ στο blockchain, (ii) την ανάγνωση πρωτοκόλλων για επαλήθευση ασφάλειας του blockchain και (iii) την συνοχή των δεδομένων των αρχείων συναλλαγών που περιέχεται σε κάθε αντίγραφο του blockchain που διατηρείται σε κάθε κόμβο. Επομένως, το blockchain διασφαλίζει ότι μόλις προστεθεί μια εγγραφή συναλλαγής σε ένα μπλοκ και το μπλοκ έχει δημιουργηθεί και υποβληθεί επιτυχώς στο blockchain, το αρχείο συναλλαγής δεν μπορεί να αλλάξει ή να καταστραφεί αναδρομικά. Η ακεραιότητα του περιεχομένου δεδομένων σε κάθε αλυσίδα μπλοκ είναι εγγυημένο ότι από τη στιγμή που ένα μπλοκ δεσμευτεί στο blockchain, δεν μπορεί να παραβιαστεί με κανέναν τρόπο. Έτσι, το blockchain χρησιμεύει ως ένα ασφαλές κατανεμημένο καθολικό που αρχειοθετεί αποτελεσματικά, διαρκώς και επαληθεύσιμα όλες τις συναλλαγές μεταξύ οποιωνδήποτε δύο μερών σε ένα ανοιχτό σύστημα δικτύου.

Στο πλαίσιο του συστήματος bitcoin, το blockchain χρησιμοποιείται ως το ασφαλές, ιδιωτικό και αξιόπιστο δημόσιο αρχείο του για όλες τις συναλλαγές που πραγματοποιούν συναλλαγές με bitcoin στο δίκτυο bitcoin. Αυτό διασφαλίζει ότι όλες οι συναλλαγές Bitcoin καταγράφονται, οργανώνονται και αποθηκεύονται σε κρυπτογραφικά ασφαλή μπλοκ που συνδέονται μεταξύ τους με επαληθεύσιμο και ανθεκτικό τρόπο. Το blockchain είναι ο βασικός φύλακας των συναλλαγών Bitcoin έναντι πολλών γνωστών και σκληρών ζητημάτων ασφάλειας, απορρήτου και εμπιστοσύνης, όπως διπλή δαπάνη, μη εξουσιοδοτημένη αποκάλυψη ιδιωτικών συναλλαγών, εξάρτηση από αξιόπιστες κεντρικές αρχές και αποκεντρωμένος υπολογισμός αναξιοπιστίας. Οι χρηματοπιστωτικές υπηρεσίες, η υγειονομική περίθαλψη, η κυβέρνηση, η παραγωγή και η διανομή είναι μερικοί μόνο από τους πολυάριθμους

τομείς στους οποίους η αλυσίδα μπλοκ έχει βρει ευρεία υιοθέτηση [16]. Η αλυσίδα μπλοκ είναι έτοιμη να καινοτομήσει και να μετασχηματίσει ένα ευρύ φάσμα εφαρμογών, όπως η κατανεμημένη πιστοποίηση, η μεταφορά αγαθών (αλυσίδα εφοδιασμού), η μεταφορά ψηφιακών μέσων (πωλήσεις έργων τέχνης), η παροχή απομακρυσμένων υπηρεσιών (ταξίδια και τουρισμός) και πλατφόρμες όπως για παράδειγμα, τη μετακίνηση υπολογιστών σε πηγές δεδομένων [17]. Οι κατανεμημένοι πόροι όπως η παραγωγή και ο διαμοιρασμός της ηλεκτρικής ενέργειας, η ηλεκτρονική ψηφοφορία, η διαχείριση ταυτότητας και ο έλεγχος των δημόσιων εγγράφων αποτελούν πρόσθετες χρήσεις της τεχνολογίας blockchain. Το οικοσύστημα blockchain αναπτύσσεται ραγδαία με αυξημένες επενδύσεις και ενδιαφέρον από τη βιομηχανία, την κυβέρνηση και τον ακαδημαϊκό κόσμο.

1.2 Λειτουργία του Blockchain

Το Blockchain λειτουργεί ως κατανεμημένη ασφαλής βάση δεδομένων καταγραφής αρχείων συναλλαγών. Στο δίκτυο bitcoin, εάν ο πελάτης Α θέλει να στείλει μερικά bitcoin σε έναν άλλο πελάτη Β, θα εναπόκειται στον πελάτη Α να δημιουργήσει μια συναλλαγή bitcoin. Η συναλλαγή πρέπει να εγκριθεί από τους miners για να μπορέσει να δεσμευτεί στο δίκτυο Bitcoin. Για να ξεκινήσει η διαδικασία εξόρυξης (mining), οι συναλλαγές μεταδίδονται σε κάθε κόμβο του δικτύου. Αυτοί οι κόμβοι που λειτουργούν ως miners θα συλλέγουν συναλλαγές σε ένα μπλοκ, θα επαληθεύουν τις συναλλαγές στο μπλοκ και θα χρησιμοποιούν το πρωτόκολλο συναίνεσης (Proof of Work) για να κερδίσει την αναγνώριση από το δίκτυο. Ένα μπλοκ μπορεί να προστεθεί στην αλυσίδα μπλοκ όταν άλλοι κόμβοι επαληθεύουν ότι όλες οι συναλλαγές που περιέχονται στο μπλοκ είναι έγκυρες. Η μεταφορά των bitcoin από το Α στο Β είναι οριστικοποιημένη και νόμιμη μόνο όταν το «μπλοκ» που περιέχει τις συναλλαγές εγκριθεί από άλλους κόμβους και προστεθεί στο blockchain.

Οι τρεις βασικές και σημαντικές δυνατότητες που υποστηρίζονται από την εφαρμογή του blockchain στο Bitcoin είναι:

- Αλυσιδωτά συνδεόμενος χώρος αποθήκευσης κατακερματισμού
- Ψηφιακές υπογραφές
- Συναίνεση δέσμευσης για την προσθήκη νέων μπλοκ στον αλυσιδωτά συνδεόμενο παγκόσμιο χώρο αποθήκευσης

Συνδυάζοντας κατάλληλα μια σειρά από δημοφιλείς τεχνολογίες ασφάλειας, όπως αλυσίδες κατακερματισμού, δέντρα Merkle και ψηφιακές υπογραφές με μηχανισμούς συναίνεσης, το blockchain Bitcoin μπορεί όχι μόνο να αποτρέψει το πρόβλημα διπλής δαπάνης του Bitcoin, αλλά και να αποτρέψει οποιαδήποτε αναδρομική τροποποίηση των δεδομένων συναλλαγών σε ένα μπλοκ από την στιγμή που το μπλοκ έχει εισαχθεί με επιτυχία στο blockchain.

Αλυσιδωτά συνδεόμενος χώρος αποθήκευσης κατακερματισμού. Οι δείκτες κατακερματισμού και τα δέντρα Merkle είναι τα δύο βασικά δομικά στοιχεία για την εφαρμογή του blockchain στο Bitcoin χρησιμοποιώντας τον αλυσιδωτά συνδεόμενο χώρο αποθήκευσης κατακερματισμού.

Δείκτης κατακερματισμού. Ο δείκτης κατακερματισμού είναι ο κατακερματισμός των δεδομένων μέσω κρυπτογραφίας, ο οποίος δείχνει τη θέση όπου είναι αποθηκευμένα τα δεδομένα. Επομένως, ο δείκτης κατακερματισμού μπορεί να χρησιμοποιηθεί για να ελέγξουμε εάν τα δεδομένα έχουν παραβιαστεί. Το blockchain οργανώνεται συνδέοντας τα μπλοκ δεδομένων μεταξύ τους χρησιμοποιώντας τους δείκτες κατακερματισμού.

Κάθε μπλοκ υποδεικνύει μια διεύθυνση όπου αποθηκεύονται τα δεδομένα του προηγούμενου μπλοκ μέσω ενός δείκτη κατακερματισμού, ο οποίος δείχνει προς το μπλοκ που έχει προηγηθεί. Επιπλέον,

η τιμή κατακερματισμού των αποθηκευμένων δεδομένων μπορεί να επαληθευτεί δημόσια από τον χρήστη, αποδεικνύοντας ότι τα αποθηκευμένα δεδομένα δεν έχουν παραβιαστεί. Εάν ένας κακόβουλος χρήστης προσπαθήσει να αλλάξει τα δεδομένα σε οποιοδήποτε μπλοκ σε ολόκληρη την αλυσίδα, προκειμένου να συγκαλύψει την παραβίαση, θα πρέπει να αλλάξει τους δείκτες κατακερματισμού όλων των προηγούμενων μπλοκ. Τελικά, ο χρήστης πρέπει να σταματήσει να παραποιεί, γιατί δεν θα μπορέσει να πλαστογραφήσει τα δεδομένα στην κεφαλή της αλυσίδας, η οποία δημιουργήθηκε στην αρχή με την κατασκευή του συστήματος. Αυτό το αρχικό μπλοκ στην αλυσίδα αποκαλείται ως μπλοκ γένεσης. Στο τέλος, η παραβίαση του κακόβουλου χρήστη θα αποκαλυφθεί, γιατί με την εγγραφή αυτού του ενιαίου δείκτη κατακερματισμού του μπλοκ γένεσης, ολόκληρη η αλυσίδα μπορεί να γίνει αποτελεσματικά ανθεκτική στην παραβίαση. Οι χρήστες έχουν την δυνατότητα να επιστρέψουν σε ένα συγκεκριμένο μπλοκ και να το επαληθεύσουν από την αρχή της αλυσίδας.

Δέντρο Merkle. Ένα δέντρο Merkle ορίζεται ως ένα δυαδικό δέντρο αναζήτησης του οποίου οι κόμβοι συνδέονται μεταξύ τους χρησιμοποιώντας δείκτες κατακερματισμού. Είναι μια άλλη χρήσιμη δομή δεδομένων για την κατασκευή ενός blockchain. Με τη σειρά τους, αυτοί οι κόμβοι ομαδοποιούνται σε χωριστές ομάδες, έτσι ώστε κάθε φορά που δύο κόμβοι χαμηλότερου επιπέδου ομαδοποιούνται ως ένας στο γονικό επίπεδο, και για κάθε ζεύγος κόμβων χαμηλότερου επιπέδου, ο αλγόριθμος κατασκευής δέντρου Merkle δημιουργεί ένα νέο κόμβο δεδομένων που περιέχει μια τιμή κατακερματισμού για το καθένα. Επαναλαμβάνεται αυτή τη διαδικασία μέχρι να φτάσει στη ρίζα του δέντρου.

Το δέντρο Merkle έχει τη δυνατότητα να διασχίζει προς τα κάτω σε οποιονδήποτε κόμβο του δέντρου μέσω του δείκτη κατακερματισμού, αποτρέποντας έτσι την παραβίαση δεδομένων. Συγκεκριμένα, όταν ένας αντίπαλος προσπαθήσει να παραβιάσει τα δεδομένα ενός κόμβου φύλλου, θα προκληθεί η αλλαγή της τιμής κατακερματισμού του γονικού κόμβου του. Ακόμα κι αν συνεχίσει να παραποιεί τους επάνω κόμβους, πρέπει να αλλάξει όλους τους κόμβους στη διαδρομή από κάτω προς τα πάνω. Δεδομένου ότι ο δείκτης κατακερματισμού του ριζικού κόμβου δεν ταιριάζει με τον αποθηκευμένο δείκτη κατακερματισμού, είναι εύκολο να εντοπιστεί ότι τα δεδομένα έχουν παραβιαστεί.

Ένα πλεονέκτημα ενός δέντρου Merkle είναι ότι μπορεί να αποδείξει αποτελεσματικά και συνοπτικά τη συμμετοχή ενός κόμβου δεδομένων δείχνοντας αυτόν τον κόμβο δεδομένων και όλους τους προγόνους του στην ανοδική πορεία του μέχρι τον κόμβο ρίζα. Η συμμετοχή στο δέντρο Merkle μπορεί να επαληθευτεί σε λογαριθμικό χρόνο υπολογίζοντας τον κατακερματισμό στη διαδρομή και ελέγχοντας τον κατακερματισμό έναντι της ρίζας.

Ψηφιακή Υπογραφή. Οι ψηφιακές υπογραφές καθορίζουν την εγκυρότητα των δεδομένων χρησιμοποιώντας έναν κρυπτογραφικό αλγόριθμο. Είναι επίσης ένα σχέδιο για την επαλήθευση ότι ένα τμήμα δεδομένων δεν έχει παραβιαστεί. Υπάρχουν τρία βασικά συστατικά για την δημιουργία ενός σχήματος ψηφιακών υπογραφών. Το πρώτο συστατικό είναι ο αλγόριθμος δημιουργίας κλειδιού, ο οποίος δημιουργεί δύο κλειδιά - το ένα χρησιμοποιείται για την υπογραφή του μηνύματος αλλά και τη διατήρηση του μυστικού, που ονομάζεται ιδιωτικό κλειδί (private key)· το άλλο αποδεσμεύεται στο κοινό, το λεγόμενο δημόσιο κλειδί (public key), και χρησιμοποιείται για την επαλήθευση ότι το μήνυμα έχει υπογραφή υπογεγραμμένη με το αντίστοιχο ιδιωτικό κλειδί. Το δεύτερο βασικό συστατικό είναι ο αλγόριθμος υπογραφής. Δημιουργεί υπογραφές σε μηνύματα εισαγωγής που εγκρίνονται με ένα δεδομένο ιδιωτικό κλειδί. Το τρίτο βασικό συστατικό είναι ο αλγόριθμος επαλήθευσης. Λαμβάνει ως είσοδο μια υπογραφή, ένα μήνυμα και ένα δημόσιο κλειδί το οποίο και χρησιμοποιεί για να επαληθεύσει την υπογραφή του μηνύματος και επιστρέφει μια δυαδική τιμή.

Ένας καλά καθορισμένος και ασφαλής αλγόριθμος υπογραφής πρέπει να έχει δύο ιδιότητες. Η πρώτη ιδιότητα είναι ότι μια έγκυρη υπογραφή πρέπει να είναι επαληθεύσιμη. Η δεύτερη ιδιότητα είναι ότι η υπογραφή δεν είναι πλαστογραφημένη. Αυτό σημαίνει ότι ένας αντίπαλος που έχει στην κατοχή του το δημόσιο κλειδί κάποιου χρήστη δεν μπορεί να πλαστογραφήσει μια υπογραφή σε κάποιο μήνυμα.

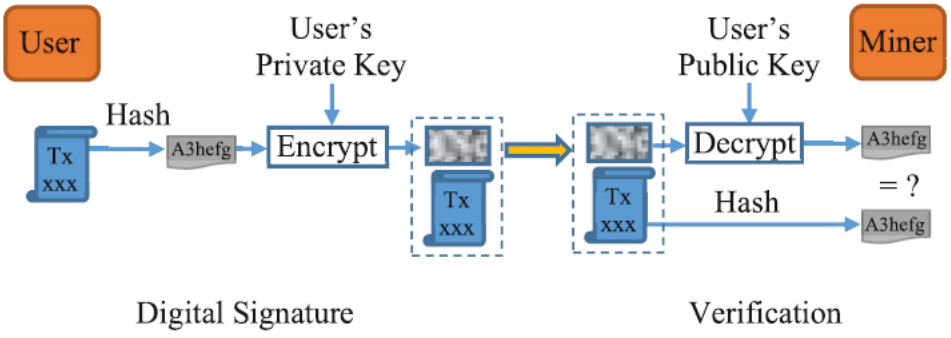
1.3 Κρυπτογραφία στο Blockchain

Για να επιτρέψει ασφαλή και αξιόπιστα αρχεία και συναλλαγές, η αλυσίδα μπλοκ προσφέρει ένα επίπεδο εμπιστοσύνης μεταξύ άγνωστων. Χωρίς το blockchain απαιτείται ένας ενδιάμεσος τρίτος για την παραγωγή αξιόπιστων εγγράφων και αλληλεπιδράσεων. Η αλυσίδα μπλοκ αντικαθιστά την ανάγκη για έναν ενδιάμεσο κεντρικό οργανισμό, δημιουργώντας εμπιστοσύνη μέσω της κρυπτογραφίας και της συνεργασίας. Το blockchain χρησιμοποιεί κρυπτογράφηση για την καταγραφή των δεδομένων στο καθολικό. Ακολουθούν ορισμένα δομικά στοιχεία κρυπτογράφησης που χρησιμοποιούνται από το blockchain [18]:

- Χρήση κρυπτογραφίας δημόσιου κλειδιού για κρυπτογράφηση και ψηφιακή πιστοποίηση.
- Απόδειξη μηδενικής γνώσης: Μεταφορά πληροφοριών ενός μυστικού χωρίς να το αποκαλύπτει.
- Μονόδρομες ψευδοτυχαίες συναρτήσεις κατακερματισμού των μαθηματικών. Ως μέρος της επικεφαλίδας μπλοκ, τα δέντρα Merkle υιοθέτησαν τη συνάρτηση κατακερματισμού.

Κρυπτογράφηση δημόσιου κλειδιού. Χρησιμοποιείται για να αποδείξει ποιος ξεκίνησε μια συμφωνία. Το ιδιωτικό κλειδί αποθηκεύεται σε ένα ψηφιακό πορτοφόλι για blockchain, το οποίο μπορεί να είναι ένα πορτοφόλι (ένα φυσικό αντικείμενο για τη φύλαξη του ιδιωτικού κλειδιού) ή οποιοδήποτε πορτοφόλι λογισμικού (όπως ένα πρόγραμμα πορτοφολιού γραφείου, μια εφαρμογή πορτοφολιού για smartphone ή ένα πορτοφόλι στο διαδίκτυο). Ένας χρήστης χρησιμοποιεί το δημόσιο κλειδί του για να επαληθεύσει ότι το μήνυμα προέρχεται πραγματικά από αυτόν, και το ιδιωτικό του κλειδί για να σφραγίσει ένα μήνυμα γνωστό ως ψηφιακή υπογραφή που θα σταλεί στην αλυσίδα μπλοκ. Για παράδειγμα, στην Εικόνα 1, ο χρήστης δημιουργεί μια τιμή κατακερματισμού Α από τα δεδομένα της συναλλαγής του και τη σφραγίζει χρησιμοποιώντας το ιδιωτικό του κλειδί για να δημιουργήσει μια ψηφιακή υπογραφή. Στη συνέχεια, το άτομο διαβιβάζει τα δεδομένα της συναλλαγής του και την ψηφιακή του ταυτότητα στο δίκτυο blockchain. Ο ανθρακωρύχος (miner) κάνει κατακερματισμό των δεδομένων συναλλαγής που έλαβε για να παράγει μια άλλη τιμή κατακερματισμού Β και χρησιμοποιεί το δημόσιο κλειδί του χρήστη για να αποκωδικοποιήσει τη ληφθείσα ψηφιακή υπογραφή για να παράγει την τιμή κατακερματισμού Α. Στη συνέχεια, ο ανθρακωρύχος καθορίζει αν η τιμή κατακερματισμού Α είναι ίση ή όχι με την τιμή κατακερματισμού Β. Ο ανθρακωρύχος επιβεβαιώνει τη συναλλαγή του χρήστη αν είναι ισοδύναμες.

Η συνοδευτική ψηφιακή υπογραφή διασφαλίζει την κυριότητα της συναλλαγής, επειδή το ιδιωτικό κλειδί μπορεί να φυλάσσεται με ασφάλεια μόνο από τον ιδιοκτήτη του. Ανάλογα με το μοναδικό ιδιωτικό κλειδί κάθε χρήστη, η μέθοδος επιτρέπει την ψηφιακή υπογραφή σε κάθε συναλλαγή. Ο συνδυασμός δημόσιου και ιδιωτικού κλειδιού λειτουργεί ως θεμέλιο του blockchain και χρησιμοποιείται για την επιβεβαίωση και την επικύρωση των συναλλαγών των χρηστών.



Εικόνα 1. Ψηφιακή υπογραφή και κατακερματισμός που χρησιμοποιούνται στις συναλλαγές blockchain [127]

Οι ψηφιακές υπογραφές χρησιμοποιούνται σε συναλλαγές και μπλοκ τόσο στο Ethereum όσο και στο Hyperledger Fabric για να επαληθεύσουν την ταυτότητα του δημιουργού και ότι τα δεδομένα δεν έχουν αλλάξει μετά την υπογραφή. Πολλοί χρησιμοποιούν τον αλγόριθμο ψηφιακής υπογραφής με ελλειπτική καμπύλη (ECDSA) για τη δημιουργία ενός συνόλου δημόσιων και ιδιωτικών κλειδιών.

Δεδομένου ότι το δημόσιο κλειδί ενός χρήστη πρέπει να είναι γνωστό προκειμένου να επαληθευτεί μια ψηφιακή υπογραφή, το δημόσιο κλειδί του χρήστη μπορεί εύλογα να επιλεγεί ως ταυτοποίησή του. Πρόκειται για μια τεχνική για τη διατήρηση ατομικών ταυτοτήτων στην αλυσίδα μπλοκ χωρίς να αποκαλύπτονται οι πραγματικές ταυτότητες.

Αποδείξεις μηδενικής γνώσης. Τα παρακάτω απεικονίζουν μία από τις κύριες εφαρμογές των αποδείξεων μηδενικής γνώσης στην τεχνολογία blockchain. Η αλυσίδα μπλοκ επιθυμεί να βεβαιωθεί ότι ο χρήστης που μεταφέρει χρήματα έχει αρκετά κεφάλαια πριν δεσμεύσει τη συναλλαγή όταν ένας χρήστης ζητά να στείλει χρήματα σε έναν άλλο χρήστη. Η αλυσίδα μπλοκ, ωστόσο, ενδιαφέρεται λιγότερο για το ποιος ξοδεύει τα χρήματα παρά για το πόσα χρήματα διαθέτει συνολικά. Το blockchain σε αυτή την περίπτωση δεν γνωρίζει ποιος ή πόσα χρήματα μεταφέρει ο χρήστης και σε ποιον τα στέλνει. Ορισμένα blockchains χρησιμοποιούν την κρυπτογραφική έννοια των αποδείξεων μηδενικής γνώσης για να βελτιώσουν την ανωνυμία των χρηστών. Αν και το zkSNARKS, ένα συγκεκριμένο είδος απόδειξης μηδενικής γνώσης, περιλαμβάνεται επί του παρόντος στο σχέδιο ανάπτυξης του Ethereum, το Ethereum δεν επιτρέπει επί του παρόντος τις αποδείξεις μηδενικής γνώσης.

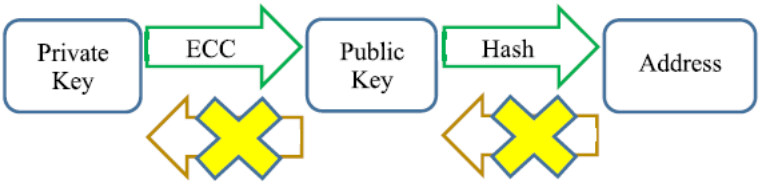
Λειτουργίες κατακερματισμού. Ένα κρίσιμο κομμάτι της τεχνολογίας blockchain είναι οι λειτουργίες κατακερματισμού. Μια αλγεβρική έκφραση γνωστή ως "συνάρτηση κατακερματισμού" έχει πέντε κρίσιμα χαρακτηριστικά για την κρυπτογραφία:

- **Σταθερό μέγεθος.** Οποιαδήποτε είσοδος μπορεί να χρησιμοποιηθεί ως σημείο εκκίνησης για μια συνάρτηση κατακερματισμού, η οποία παράγει μια έξοδο σταθερού μεγέθους. Ως αποτέλεσμα, οτιδήποτε μπορεί να αναχθεί σε ένα στοιχείο δεδομένων συγκεκριμένης διάστασης. Ως εκ τούτου, οι συναρτήσεις κατακερματισμού χρησιμοποιούνται στις αλυσίδες μπλοκ για τη συμπίεση των επικοινωνιών για την ψηφιακή πιστοποίηση.
- **Αντοχή σε προεικόνιση**. Είναι απλό να προσδιοριστεί ένα αποτέλεσμα κατακερματισμού δεδομένης μιας εισόδου. Ωστόσο, δεδομένου του αποτελέσματος κατακερματισμού, είναι πρακτικά ανέφικτο να αντιστρέψουμε την αρχική είσοδο. Στην πραγματικότητα, η μόνη μέθοδος για την επίτευξη του ίδιου αποτελέσματος είναι η τυχαία εισαγωγή των δεδομένων στη συνάρτηση κατακερματισμού.

- **2η αντοχή στην προεικόνιση**. Εάν παρέχεται μια είσοδος και η έξοδος κατακερματισμού της, η λήψη της δεύτερης εισόδου που παράγει την ίδια έξοδο κατακερματισμού είναι υπολογιστικά ανέφικτη.
- **Αντοχή στη σύγκρουση**. Είναι υπολογιστικά αδύνατο να παραχθεί το ίδιο αποτέλεσμα κατακερματισμού από δύο διαφορετικές πηγές.
- **Μεγάλη αλλαγή**. Εάν οποιοδήποτε μεμονωμένο bit της εισόδου μεταβληθεί, θα παραχθεί ένα εντελώς νέο αποτέλεσμα κατακερματισμού.

Διεύθυνση IP P2PKH. Εκτός από το δέντρο Merkle και τον αλγόριθμο εξόρυξης PoW, οι λογαριασμοί Bitcoin Pay To Public Key Hash (P2PKH) χρησιμοποιούν επίσης κρυπτογραφικές συναρτήσεις κατακερματισμού [19]. Για να μπορεί ένας χρήστης Bitcoin να μεταφέρει και να λαμβάνει χρήματα, η διεύθυνση P2PKH γίνεται με τη χρήση συναρτήσεων κατακερματισμού και κρυπτογράφησης δημόσιου κλειδιού (Εικόνα 2). Είναι ανέφικτη η αντίστροφη ανάλυση από μια διεύθυνση στο δημόσιο κλειδί και το ιδιωτικό κλειδί της λόγω της μονόδρομης λειτουργίας.

Το μήκος ενός κλειδιού διατηρείται σταθερό. Το μέγεθος ενός δημόσιου κλειδιού είναι 65 bytes, ενώ το μέγεθος ενός ιδιωτικού κλειδιού είναι 32 bytes (ή 33 bytes για ένα συμπιεσμένο δημόσιο κλειδί). Το αναγνωριστικό P2PKH έχει μέγεθος 20 bytes.



Εικόνα 2. Κρυπτογραφία δημόσιου κλειδιού και συνάρτηση κατακερματισμού για τη διεύθυνση Bitcoin [127]

1.4 Είδος Δικτύου και Εξέλιξη του Blockchain

Ένα από τα πιο θεμελιώδη χαρακτηριστικά ενός δικτύου blockchain είναι το είδος του. Υπάρχουν δύο είδη δικτύων ανάλογα με την αρχή λειτουργίας που έχει ο χρήστης. Αρχικά έχουμε δίκτυα που λειτουργούσαν χωρίς άδεια (permissionless) και με άδεια (permissioned). Ένας γρήγορος και εύκολος τρόπος για να κατανοήσουμε την άμεση διαφορά μεταξύ τους είναι να σκεφτούμε ένα απλό παράδειγμα, τη διαφορά χρήσης μεταξύ δύο ειδών δικτύων Διαδικτύου (επιχείρησης-οικιακό). Τα blockchains χωρίς άδεια είναι σαν το διαδίκτυο που έχουμε στο σπίτι μας και μπορούμε να πραγματοποιούμε ό,τι θέλουμε και όπως το θέλουμε, ενώ τα blockchains με άδεια είναι σαν το διαδίκτυο που ανήκει σε επιχειρήσεις με περιορισμούς στις δυνατότητες των χρηστών τους. Συνεπώς, τα permissioned δίκτυα περιορίζουν την ελευθερία κινήσεων των χρηστών.

Πιο συγκεκριμένα:

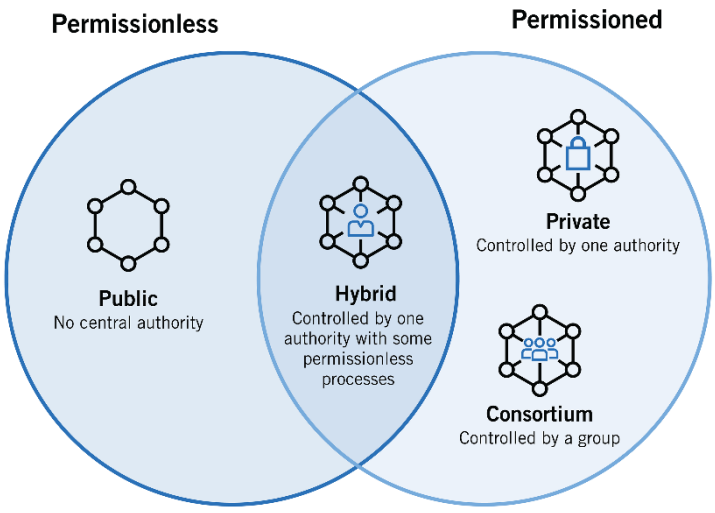
Χωρίς Άδεια - Permissionless: Τα blockchain που μπορούν και λειτουργούν χωρίς να υπάρχει άδεια έχουν ένα ψηφιακό δημόσιο καθολικό που μπορεί να έχει πρόσβαση οποιοσδήποτε χρήστης (miners, προγραμματιστές, χρήστες δικτύου). Επίσης προσφέρουν στους χρήστες τους εύρος κινήσεων, χωρίς την άδεια οποιασδήποτε κεντρικής αρχής. Αυτός ο συγκεκριμένος τύπος blockchain είναι κατά κύριο λόγο ανοιχτού κώδικα, μπορεί ο καθένας να τον κάνει λήψη και να ασχοληθεί. Λόγω της κατασκευής τους, μπορεί όποιος θέλει να κοιτάξει όλες τις συναλλαγές του δικτύου που έχουν πραγματοποιηθεί, αλλά και να προχωρήσει στην δημιουργία block. Σε κάποιο συγκεκριμένο δίκτυο, δεδομένου ότι η πρόσβαση είναι δωρεάν, ενδέχεται να υπάρξουν προσπάθειες αλλαγής των συναλλαγών που έχουν

ήδη πραγματοποιηθεί προς όφελος ενός ή περισσοτέρων χρηστών. Για να μην συμβεί αυτό, δημιουργήθηκαν πρωτόκολλα συναίνεσης τα οποία εφαρμόζουν κανόνες ανάμεσα στους χρήστες όσον αφορά τον τρόπο λειτουργίας του δικτύου.

Με Άδεια – Permissioned: Σε ένα δίκτυο που λειτουργεί με άδεια, είναι απαραίτητο ο χρήστης να συμμετέχει έχοντας λάβει άδεια από κάποια κεντρική αρχή. Δεδομένου ότι πρόκειται για κλειστά δίκτυα, δίνεται η άδεια στους χρήστες να κάνουν ό,τι μπορούν. Δηλαδή, μπορεί ο ίδιος να δει ήδη πραγματοποιημένες συναλλαγές ή και να δημιουργήσει κάποιο νέο block ή ακόμα να κάνει και τα δύο. Τα δίκτυα με άδεια χρησιμοποιούν και αυτά ένα πρωτόκολλο συναίνεσης. Εδώ όμως, εξαιτίας του γεγονότος πως τα πρωτόκολλα δεν είναι παρόμοια, η υπολογιστική ισχύς που χρειάζονται είναι πιο λίγη. Επιχειρήσεις που έχουν να κάνουν με την διαχείριση ευαίσθητων τύπων δεδομένων, στα οποία θέλουν να έχουν πρόσβαση τρίτοι, χρησιμοποιούν αυτό το είδος blockchain . Ακόμα και σε αυτό το είδος blockchain όμως μπορεί να υπάρξει αλλοίωση των δεδομένων από κάποιον χρήστη. Βέβαια, επειδή όλοι οι χρήστες είναι καταχωρημένοι μπορεί ευκολότερα να βρεθεί και να περιοριστεί κάποια απόπειρα.

Καθώς οι τεχνολογίες blockchain συνεχίζουν να εξελίσσονται, όσον αφορά τον τρόπο κατασκευής, πρόσβασης και επαλήθευσης των blockchain, ομαδοποιούνται σε τρεις μεγάλες κατηγορίες:

- **Δημόσια blockchains**, όπου ο καθένας μπορεί να διαβάσει, να στείλει ή να λάβει συναλλαγές και να επιτρέψει σε οποιονδήποτε συμμετέχοντα να συμμετάσχει σε μια διαδικασία συναίνεσης για να αποφασίσει ποια μπλοκ περιέχουν τις σωστές συναλλαγές και να τα προσθέσει στο blockchain.
- **Blockchains κοινοπραξίας ή υβριδικά blockchains**, τα οποία θέτουν ορισμένους περιορισμούς στις άδειες εγγραφής, έτσι ώστε μόνο ένα προεπιλεγμένο σύνολο συμμετεχόντων στο δίκτυο μπορεί να επηρεάσει και να ελέγξει τη διαδικασία συναίνεσης, ακόμη και αν η ανάγνωση είναι ανοιχτή σε οποιονδήποτε συμμετέχοντα στο δίκτυο.
- **Ιδιωτικά blockchain**, των οποίων η πρόσβαση εγγραφής περιορίζεται αυστηρά σε έναν μόνο συμμετέχοντα (ή οργανισμό), ακόμη και αν η πρόσβασή τους για ανάγνωση είναι ανοιχτή στο κοινό ή περιορίζεται σε ένα υποσύνολο συμμετεχόντων στο δίκτυο.

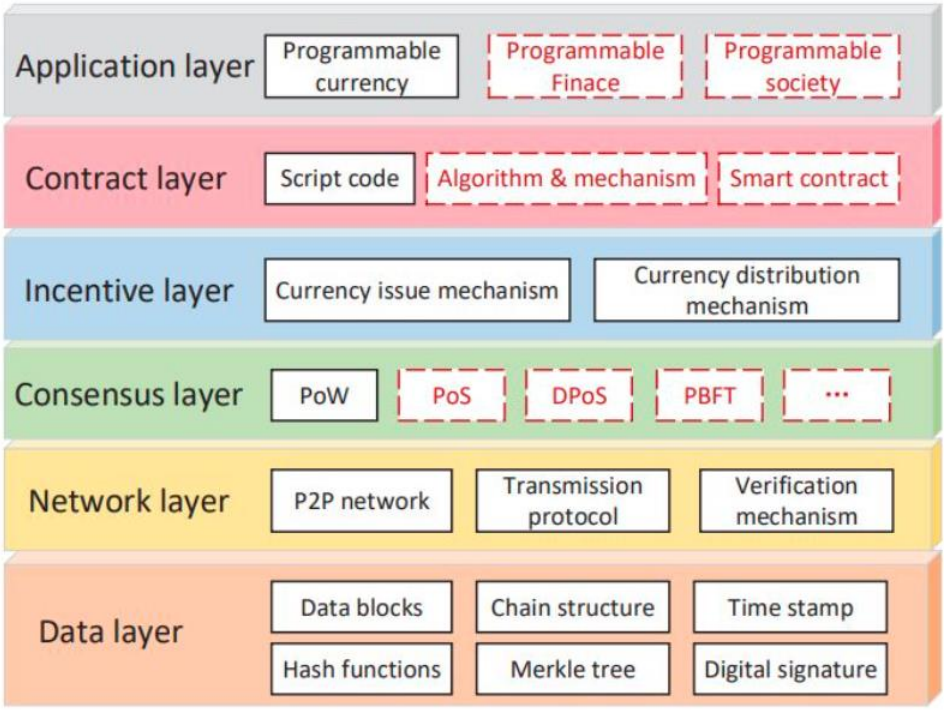


Εικόνα 3. Δημόσια, Υβριδικά και Ιδιωτικά Blockchain [131]

Αν και από άποψη ασφάλειας και απόδοσης διαφέρουν ως προς την ταχύτητα συναίνεσης (Speed of Consensus, SoC) και το κατά πόσον χρησιμοποιείται κάποια αρχή εμπιστοσύνης (Trust Authority, TA) και πόσες TA απαιτούνται. Συνεπώς, αυτοί οι τρεις τύποι blockchains μοιράζονται ορισμένα κοινά χαρακτηριστικά:

- Χρησιμοποιούν όλοι ένα αποκεντρωμένο δίκτυο peer-to-peer για συναλλαγές
- Απαιτούν κάθε συναλλαγή να υπογράφεται ψηφιακά και να προσαρτάται μόνο στο blockchain και κάθε ομότιμος κόμβος διατηρεί ένα αντίγραφο του κατανεμημένου καθολικού συναλλαγών
- Βασίζονται όλοι στη συναίνεση για τον συγχρονισμό των αντιγράφων ολόκληρου του δικτύου

Αν και το Bitcoin κυκλοφόρησε δημόσια το 2009 ως το πρώτο peer-to-peer σύστημα ψηφιακών νομισμάτων, χρησιμοποιώντας το blockchain ως δημόσιο καθολικό για όλες τις συναλλαγές του, η έννοια του ασφαλούς blockchain μέσω κρυπτογραφίας προτάθηκε για πρώτη φορά το 1991 και χρησιμοποιήθηκε το 1993 στο . Οι Bayer, Haber και Stornetta περιέγραψαν για πρώτη φορά τη βελτιστοποίηση της απόδοσης των δέντρων Merkle ως αλυσίδες κατακερματισμού. Τα τελευταία 10 χρόνια, τα blockchain έχουν εξελιχθεί από ψηφιακά νομίσματα (Blockchain 1.0) σε έξυπνα συμβόλαια (Blockchain 2.0) και πολλές άλλες μορφές αποκεντρωτικής συνεργασίας με υψηλή υπευθυνότητα και υψηλή ασφάλεια και εμπιστοσύνη (Blockchain 3.0). Καθώς η χρησιμότητα του blockchain συνεχίζει να εξελίσσεται από το blockchain 1.0 στο blockchain 3.0, γίνεται ακόμη πιο σημαντικό για τους χρήστες και τους προγραμματιστές του blockchain να κατανοήσουν καλύτερα το blockchain και τις ιδιότητες ασφάλειας και απορρήτου του.



Εικόνα 4. Αρχιτεκτονική του Blockchain [128]

1.5 Χαρακτηριστικά του Blockchain

Παρακάτω παρουσιάζονται τα κύρια χαρακτηριστικά της τεχνολογίας blockchain:

1. **Είναι αμετάβλητα.** Το αμετάβλητο σημαίνει ότι το blockchain είναι ένα μόνιμο και αμετάβλητο δίκτυο. Η τεχνολογία Blockchain λειτουργεί μέσω μιας συλλογής κόμβων.
    - Κάθε κόμβος στο δίκτυο έχει ένα αντίγραφο του ψηφιακού καθολικού. Για να προσθέσει κάποιος μια συναλλαγή, κάθε κόμβος ελέγχει την εγκυρότητα της συναλλαγής και εάν η πλειοψηφία των κόμβων πιστεύει ότι είναι έγκυρη συναλλαγή, τότε προστίθεται στο δίκτυο. Αυτό σημαίνει ότι κανείς δεν μπορεί να προσθέσει οποιοδήποτε μπλοκ συναλλαγών στο καθολικό χωρίς την έγκριση της πλειοψηφίας των κόμβων.
    - Τυχόν επαληθευμένες εγγραφές είναι μη αναστρέψιμες και δεν μπορούν να αλλάξουν. Αυτό σημαίνει ότι δεν μπορεί να υποβληθεί σε επεξεργασία, αλλαγή ή διαγραφή από κανέναν χρήστη στο δίκτυο.

2. **Είναι διανεμημένα στο δίκτυο.** Όλοι οι συμμετέχοντες στο δίκτυο έχουν αντίγραφο του καθολικού για πλήρη διαφάνεια. Το δημόσιο καθολικό θα παρέχει πλήρεις πληροφορίες για όλους τους συμμετέχοντες στο δίκτυο και τις συναλλαγές. Η κατανεμημένη υπολογιστική ισχύς μεταξύ των υπολογιστών εξασφαλίζει καλύτερα αποτελέσματα. Τα κατανεμημένα λογιστικά βιβλία είναι ένα από τα σημαντικά χαρακτηριστικά των blockchain για διάφορους λόγους, όπως:
    - Σε ένα κατανεμημένο καθολικό, είναι εύκολο να παρακολουθείτε τι συμβαίνει, επειδή οι αλλαγές διαδίδονται πολύ γρήγορα σε όλο το καθολικό.
    - Κάθε κόμβος στο δίκτυο blockchain πρέπει να διατηρεί λογιστικά βιβλία και να συμμετέχει στην επαλήθευση.
    - Οποιεσδήποτε αλλαγές στο καθολικό θα ενημερωθούν μέσα σε δευτερόλεπτα ή λεπτά και δεδομένου ότι δεν εμπλέκονται μεσάζοντες στο blockchain, η επαλήθευση των αλλαγών θα γίνει γρήγορα.
    - Εάν ένας χρήστης θέλει να προσθέσει ένα νέο μπλοκ, τότε άλλοι συμμετέχοντες κόμβοι πρέπει να επικυρώσουν τη συναλλαγή. Για να προστεθεί ένα νέο μπλοκ σε ένα δίκτυο blockchain, πρέπει να εγκριθεί από την πλειοψηφία των κόμβων του δικτύου.
    - Σε ένα δίκτυο blockchain, κανένας κόμβος δεν λαμβάνει κανενός είδους ειδική μεταχείριση ή εύνοια από το δίκτυο. Όλοι πρέπει να ακολουθούν τυπικές διαδικασίες για να προσθέσουν νέα μπλοκ στο δίκτυο.

3. **Είναι αποκεντρωμένα.** Τα δίκτυα blockchain είναι αποκεντρωμένα, που σημαίνει ότι δεν υπάρχει κεντρικό διοικητικό όργανο υπεύθυνο για όλες τις αποφάσεις. Αντίθετα, μια ομάδα κόμβων δημιουργεί και συντηρεί το δίκτυο. Κάθε κόμβος σε ένα δίκτυο blockchain έχει το ίδιο αντίγραφο του καθολικού. Η αποκεντρωμένη ιδιοκτησία προσφέρει πολλά πλεονεκτήματα σε ένα δίκτυο blockchain:
    - Δεδομένου ότι ένα δίκτυο blockchain δεν εξαρτάται από ανθρώπινους υπολογισμούς, είναι πλήρως οργανωμένο και ανεκτικό σε σφάλματα.
    - Τα δίκτυα blockchain είναι λιγότερο επιρρεπή σε αποτυχία λόγω της αποκεντρωμένης φύσης του δικτύου. Η επίθεση στο σύστημα είναι πιο ακριβή για τον κακόβουλο χρήστη, επομένως είναι λιγότερο πιθανό να αποτύχει.

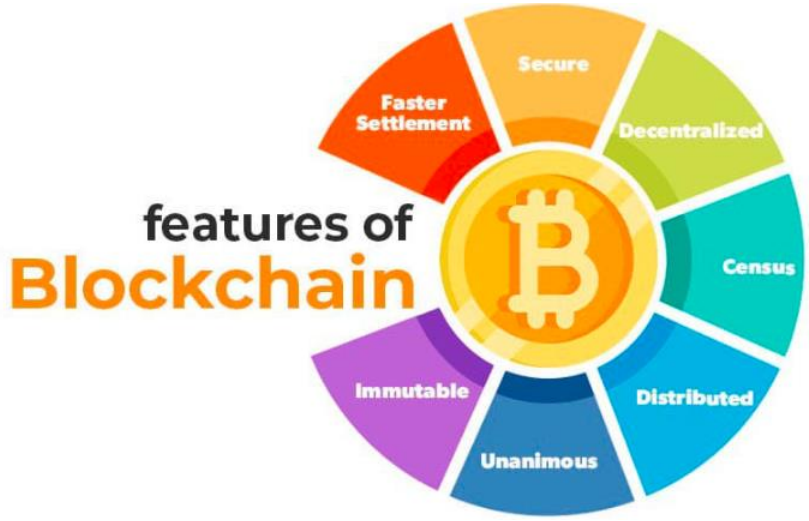
- Δεν εμπλέκεται τρίτο μέρος, επομένως δεν υπάρχει πρόσθετος κίνδυνος στο σύστημα.
- Η αποκεντρωμένη φύση του blockchain βοηθά στη δημιουργία διαφανών προφίλ για κάθε συμμετέχοντα στο δίκτυο. Επομένως, κάθε αλλαγή είναι ανιχνεύσιμη και πιο συγκεκριμένη.
- Οι χρήστες έχουν πλέον τον έλεγχο της περιουσίας τους, δεν χρειάζεται να βασίζονται σε τρίτα μέρη για τη συντήρηση και τη διαχείριση των περιουσιακών τους στοιχείων.

4. **Είναι ασφαλή.** Όλες οι εγγραφές στο blockchain είναι κρυπτογραφημένες ξεχωριστά. Η χρήση κρυπτογράφησης προσθέτει ένα άλλο επίπεδο ασφάλειας σε ολόκληρη τη διαδικασία στο δίκτυο blockchain. Εφόσον δεν υπάρχει κεντρική αρχή, δεν σημαίνει ότι τα δεδομένα μπορούν απλώς να προστεθούν, να ενημερωθούν ή να διαγραφούν στο δίκτυο. Κάθε πληροφορία στο blockchain κατακερματίζεται κρυπτογραφικά, πράγμα που σημαίνει ότι κάθε κομμάτι δεδομένων έχει μια μοναδική ταυτότητα στο δίκτυο. Όλα τα μπλοκ περιέχουν το δικό τους μοναδικό κατακερματισμό και τον κατακερματισμό του προηγούμενου μπλοκ. Λόγω αυτής της ιδιότητας, τα μπλοκ συνδέονται κρυπτογραφικά μεταξύ τους. Οποιαδήποτε προσπάθεια τροποποίησης δεδομένων σημαίνει αλλαγή όλων των αναγνωριστικών κατακερματισμού, κάτι που είναι αδύνατο.

5. **Υπάρχει συναίνεση για την λήψη αποφάσεων.** Κάθε blockchain έχει συναίνεση για να βοηθήσει το δίκτυο να λάβει γρήγορες και δίκαιες αποφάσεις. Ο Consensus αλγόριθμος είναι ένας αλγόριθμος λήψης αποφάσεων για ενεργές ομάδες κόμβων στο δίκτυο για να επιτύχουν γρήγορα μια συναίνεση για να εξασφαλίσουν την ομαλή λειτουργία του συστήματος. Οι κόμβοι μπορεί να μην εμπιστεύονται ο ένας τον άλλον, αλλά μπορούν να εμπιστεύονται τους αλγόριθμους που τρέχουν στον πυρήνα του δικτύου για τη λήψη αποφάσεων. Υπάρχουν πολλοί διαθέσιμοι αλγόριθμοι συναίνεσης, ο καθένας με τα δικά του πλεονεκτήματα και μειονεκτήματα. Κάθε blockchain πρέπει να έχει έναν αλγόριθμο συναίνεσης, διαφορετικά χάνει την αξία του.

6. **Υπάρχει ομοφωνία για την εκτέλεση αλλαγών.** Όλοι οι συμμετέχοντες στο δίκτυο συμφωνούν με την εγκυρότητα μιας εγγραφής πριν να προστεθεί στο δίκτυο. Όταν ένας κόμβος θέλει να προσθέσει ένα μπλοκ στο δίκτυο, πρέπει να λάβει πλειοψηφία, διαφορετικά το μπλοκ δεν μπορεί να προστεθεί στο δίκτυο. Οι κόμβοι δεν μπορούν απλώς να προσθέσουν, να ενημερώσουν ή να διαγράψουν πληροφορίες από το δίκτυο. Κάθε εγγραφή ενημερώνεται ταυτόχρονα και οι ενημερώσεις διαδίδονται γρήγορα στο δίκτυο. Επομένως, είναι αδύνατο να πραγματοποιηθούν αλλαγές χωρίς τη συγκατάθεση της πλειοψηφίας των κόμβων στο δίκτυο.

7. **Είναι γρηγορότερα όσον αφορά τον διακανονισμό.** Το παλαιού τύπου τραπεζικό σύστημα είναι επιρρεπές σε συνέπειες, όπως η λήψη ημερών για την επεξεργασία μιας συναλλαγής μετά την ολοκλήρωση όλων των διακανονισμών, η οποία μπορεί εύκολα να διαταραχθεί. Το Blockchain, από την άλλη, προσφέρει ταχύτερους διακανονισμούς σε σύγκριση με τα παραδοσιακά τραπεζικά συστήματα. Αυτή η λειτουργία blockchain βοηθά στη διευκόλυνση της ζωής.



Εικόνα 5. Χαρακτηριστικά του Blockchain [130]

ΚΕΦΆΛΑΙΟ 2: Διαδικασία Συναλλαγών

2.1 Διαδικασία Συναλλαγής του Blockchain

Μια μεμονωμένη εργασία που καταγράφεται σε δημόσια έγγραφα μπορεί να θεωρηθεί ως μια μικροσκοπική μονάδα σε μια συναλλαγή Blockchain. Τα μπλοκ είναι ένα άλλο όνομα για αυτά τα δεδομένα [20]. Όλοι οι ανθρακωρύχοι (miners) που είναι συνδεδεμένοι στο δίκτυο blockchain εκτελούν, εφαρμόζουν και καταγράφουν αυτά τα μπλοκ στο blockchain για επικύρωση. Ενώ οι προηγούμενες συναλλαγές μπορούν πάντα να εξεταστούν, δεν μπορούν να αλλάξουν [21]. Η υποκείμενη τεχνολογία του Bitcoin ονομάζεται blockchain και επιτρέπει αποκεντρωμένες αλληλεπιδράσεις μεταξύ ομότιμων χρηστών σε παγκόσμιο δίκτυο. Έτσι, το Bitcoin είναι μια ανθεκτική στη λογοκρισία, παγκόσμια μορφή χρήματος. Το πρωταρχικό ζήτημα με τα συμβατικά συγκεντρωτικά συστήματα, όπως οι τράπεζες, όπου οι άνθρωποι πρέπει να εμπιστευτούν σοβαρά το σύστημα, μπορεί να είναι η πίστη γενικά. Καθώς μεταφέρει την κατοχή ψηφιακών περιουσιακών στοιχείων από έναν ομότιμο σε έναν άλλο χωρίς να απαιτεί καμία εμπιστοσύνη, αυτό είναι το γλυκό σημείο για τη δημόσια τεχνολογία blockchain. Η αλυσίδα μπλοκ είναι ένα σύστημα χωρίς εμπιστοσύνη που δημιουργεί εμπιστοσύνη μέσω των μηχανισμών που διαδίδουν πληροφορίες για όλες τις δραστηριότητες του δικτύου [22]. Ένας άλλος παράγοντας που πρέπει να λαμβάνεται υπόψη κατά την έναρξη μιας συμφωνίας είναι η ασφάλεια. Οι ανησυχίες για την ασφάλεια μπορούν να επιλυθούν με τη χρήση μεθόδων συμφωνίας και εξόρυξης blockchain που εξαρτώνται σε μεγάλο βαθμό από τις κρυπτογραφικές συναρτήσεις κατακερματισμού. Για παράδειγμα, η ασφαλής μέθοδος κατακερματισμού SHA-256 χρησιμοποιείται από το Bitcoin [23]. Οποιαδήποτε μορφή εισόδου, συμπεριλαμβανομένου κειμένου, αριθμών, συμβολοσειρών ή ακόμη και ενός αρχείου που δημιουργείται από υπολογιστή οποιουδήποτε μήκους, μπορεί να χρησιμοποιηθεί από το Bitcoin για

τη δημιουργία μιας εξόδου 256 bit ή των 64 χαρακτήρων που είναι γνωστοί ως κατακερματισμός [24]. Το μετασχηματισμένο αποτέλεσμα κατακερματισμού θα είναι πάντα πανομοιότυπο δεδομένης της ίδιας εισόδου. Μια μονόδρομη συνάρτηση, η οποία σημαίνει επίσης ότι είναι αδύνατο να υπολογιστεί η είσοδος από την έξοδο, είναι μια συνάρτηση στην οποία μια μικροσκοπική αλλαγή στην είσοδο αλλάζει εντελώς την έξοδο. Κάποιος μπορεί μόνο να υποθέσει ποια ήταν η είσοδος, και οι πιθανότητες να είναι σωστή η εικασία είναι εξαιρετικά μικρές, οπότε είναι ασφαλής.

Το πρώτο στάδιο της διαδικασίας συναλλαγής είναι η επιβεβαίωση της ταυτότητας του αποστολέα, υποδεικνύοντας ότι μόνο ο αποστολέας και όχι κάποιος άλλος ζητά τη συναλλαγή μεταξύ του αποστολέα και του παραλήπτη. Ας υποθέσουμε ότι ο Bob και η Alice έχουν και οι δύο ένα ποσό σε bitcoins και ότι η Alice επιθυμεί να στείλει στον Bob 10 bitcoins. Η Alice θα διαδώσει τώρα μια ειδοποίηση στο δίκτυο blockchain με τις λεπτομέρειες της συναλλαγής προκειμένου να μεταφέρει τα χρήματα. Η αλυσίδα μπλοκ χρησιμοποιεί ψηφιακά δακτυλικά αποτυπώματα (δημόσια και ιδιωτικά κλειδιά) για να το επιτύχει αυτό [25]. Τα στοιχεία του Bob, συμπεριλαμβανομένης της δημόσιας θέσης του και του ποσού της συναλλαγής, καθώς και το δημόσιο κλειδί και η ψηφιακή υπογραφή της Alice, παρέχονται για τη μετάδοση. Η Alice δημιούργησε αυτή την ψηφιακή υπογραφή χρησιμοποιώντας το μυστικό της κλειδί. Η αλυσίδα μπλοκ χρησιμοποιεί τη μέθοδο ψηφιακής υπογραφής με ελλειπτική καμπύλη (ECDSA) [26].

Αυτό το πρόγραμμα διασφαλίζει ότι τα χρήματα μπορούν να χρησιμοποιηθούν μόνο από τους ανθρώπους που πραγματικά τα κατέχουν. Κάθε συναλλαγή έχει μια υπογραφή 256 bit. Για να πλαστογραφήσει αυτή την υπογραφή προκειμένου να πραγματοποιήσει μια δόλια συναλλαγή, ένας κακόβουλος χρήστης θα πρέπει να προβλέψει 2256 περιπτώσεις, κάτι που είναι και ανέφικτο λόγω της απώλειας πόρων [27]. Ο επαληθευτής πρέπει να επαληθεύσει όχι μόνο τη νομιμότητα του αποστολέα αλλά και τη νομιμότητα της συναλλαγής, συμπεριλαμβανομένου του αν ο αποστολέας έχει αρκετά χρήματα για να τα δώσει στον παραλήπτη ή όχι. Αυτό θα μπορούσε να γίνει με τη συμβουλή του ημερολογίου, το οποίο περιέχει λεπτομέρειες σχετικά με κάθε προηγούμενη επιτυχημένη συναλλαγή.

2.2 Διαδικασία Συναλλαγής του Bitcoin

Ο πρωταρχικός στόχος αυτού του ψηφιακού νομίσματος ήταν να επιτρέψει ένα αποκεντρωμένο σύστημα ηλεκτρονικής ανταλλαγής μετρητών μεταξύ διαφόρων μερών καταργώντας τους κεντρικούς μεσάζοντες [28]. Κατά τη διάρκεια μιας ανταλλαγής bitcoin, η κατοχή κάποιου bitcoin μεταφέρεται σε μια άλλη διεύθυνση bitcoin. Στις περισσότερες περιπτώσεις, ξεκινά από το πορτοφόλι bitcoin ενός πελάτη και στη συνέχεια διαδίδεται στο δίκτυο. Μόνο αν η συναλλαγή είναι νόμιμη, οι κόμβοι του δικτύου θα την επαναλάβουν και θα τη συμπεριλάβουν στο μπλοκ που εξορύσσουν. Η συμπερίληψη της συναλλαγής και άλλων πράξεων σε ένα μπλοκ διαρκεί περίπου 10 λεπτά [29]. Μέχρι αυτή τη στιγμή, ο παραλήπτης θα έπρεπε να είναι σε θέση να δει τη συνολική συναλλαγή στο πορτοφόλι του.

Το Unspent Transaction Output (UTXO), το οποίο αναφέρεται στο ποσό εξόδου μιας συναλλαγής που λαμβάνει ένας χρήστης και στη δυνατότητα να το ξοδέψει στο μέλλον [30], είναι το πρωταρχικό συστατικό μιας δομής bitcoin. Σκεφτείτε την πιθανότητα τα νομίσματα ή το νόμισμα σε ένα πραγματικό πορτοφόλι να μπερδευτούν, ενώ αυτό δεν συμβαίνει με το ποσό που λαμβάνεται στο Bitcoin. Το σύνολο του ληφθέντος ποσού παραμένει ένα ξεχωριστό αντικείμενο σε ένα πορτοφόλι Bitcoin. Για παράδειγμα, αν αποθηκεύσουμε δύο διαφορετικά ποσά (2 και 3 δολάρια) στο ίδιο φυσικό πορτοφόλι ή στο διαδικτυακό πορτοφόλι, θα αθροιστούν σε 5 δολάρια, ενώ θα εξακολουθούν να εμφανίζονται οι ακριβείς αριθμοί και θα συνεχίσουν να υπάρχουν ως ξεχωριστές οντότητες στο πορτοφόλι Bitcoin. Ας υποθέσουμε ότι η Alice επιθυμεί να μεταβιβάσει στον Bob 0,15

BTC (Bitcoin), αλλά έχει μόνο τρία διαφορετικά UTXO (0,01, 0,2 και 3) στο πορτοφόλι της. Το πορτοφόλι πρέπει να επιλέξει ένα από αυτά τα τρία UTXO εξόδου ως επιλογή δαπάνης για να το επιτύχει αυτό. Το πορτοφόλι θα ανοίξει αυτή την ποσότητα και θα χρησιμοποιήσει ολόκληρο το ποσό ως είσοδο UTXO για τη συναλλαγή των 0,15 BTC εάν επιλέξει το 0,2 ως έξοδο. Στη συνέχεια, 0,15 Bitcoin θα σταλούν ως UTXO εξόδου στο πορτοφόλι IP του Bob.

Έπειτα από την διαχείριση και την επαλήθευση όλων αυτών των συναλλαγών καθώς και την παραγωγή ενός νέου μπλοκ το οποίο τελικά εντάσσεται στην τρέχουσα αλυσίδα, οι miners θα ανταμείβονται για την εργασία τους [31]. Οι επιτυχημένοι miners λαμβάνουν αμοιβές συναλλαγών και αποζημίωση για τη δημιουργία μπλοκ [32]. Οι χρήστες συνήθως ορίζουν μια αμοιβή συναλλαγής κατά την υποβολή συναλλαγών στους ανθρακωρύχους μετά από έναν επιτυχή σχηματισμό μπλοκ. Δεν υπάρχουν λεπτομέρειες για την επικεφαλίδα σχετικά με τη χρέωση συναλλαγής. Στέλνοντας λιγότερα χρήματα στους αποδέκτες από το συνολικό UTXO εισόδου, οι χρήστες μπορούν να προσθέσουν μια χρέωση συναλλαγής. Όπως φαίνεται στην Εξ. 1, αυτό το μη καθορισμένο ποσό συναλλαγής μπορεί να θεωρηθεί ως χρέωση συναλλαγής.

$$Inputs - outputs = Transactionfees \quad (1)$$

Κατά την εξόρυξη ενός μπλοκ, οι ανθρακωρύχοι περιλαμβάνουν τόσο τη δική τους προσωπική συναλλαγή στην coinbase όσο και τα δεδομένα της συναλλαγής που προσπαθούν να ελέγξουν και να επιβεβαιώσουν. Ένα αποκλειστικό είδος συναλλαγής bitcoin που μπορεί να παραχθεί μόνο από έναν miner είναι μια συναλλαγή coinbase. Κάθε φορά που εξορύσσεται ένα νέο μπλοκ στο δίκτυο, παράγεται μια συναλλαγή αυτού του είδους με μόνο εξόδους. Αυτή η συναλλαγή χορηγεί σε έναν ανθρακωρύχο το block bounty ως αποζημίωση για τις προσπάθειές του. Η λειτουργία αυτή αποστέλλει επίσης τυχόν έξοδα συναλλαγής που έχει συσσωρεύσει ο ανθρακωρύχος. Το έγγραφο του κατανεμημένου καθολικού θα προστεθεί από τους εταίρους του δικτύου αφού διαπιστώσουν αν η συναλλαγή είναι ισοδύναμη. Αυτό δείχνει πώς ένας ανθρακωρύχος πρέπει να κατανέμει την πληρωμή του όταν φτιάχνει ένα μπλοκ. Ωστόσο, όπως φαίνεται στην Εξ. 2, κάθε κόμβος του δικτύου θα εξετάσει το μπλοκ για να δει αν πληρεί το κριτήριο. Ένας miner μπορεί να χρησιμοποιήσει την αμοιβή μπλοκ και το κόστος συναλλαγής μόνο όταν το μπλοκ έχει επαληθευτεί.

$$sum(BlockOutputs) \leq sum(BlockInputs) + BlockReward \quad (2)$$

2.3 Διαδικασία Συναλλαγής του Ethereum

Οι συνθήκες του UTXO, μια εφαρμογή αναφοράς του προγράμματος πορτοφολιού που διατηρούσε την αναφορά του λογαριασμού, αρνούνται την κατάσταση του Bitcoin. Από την άλλη πλευρά, το Ethereum υπήρξε πρωτοπόρος στην ιδέα ενός λογαριασμού ως πηγή και προορισμός μιας συναλλαγής. Κατά συνέπεια, οι συναλλαγές επιτρέπουν τη μετακίνηση τιμών, μηνυμάτων και δεδομένων μεταξύ των λογαριασμών που μπορεί να οδηγήσουν σε αλλαγές της κατάστασης, σε αντίθεση με τη διατήρηση της κατάστασης, όπως στην περίπτωση των UTXO του Bitcoin [33]. Ο λογαριασμός εξωτερικής κατοχής (EOA) και ο λογαριασμός συμβολαίου (CA) είναι τα δύο είδη λογαριασμών που είναι διαθέσιμα για το Ethereum.

Ο CA διαχειρίζεται από τον κώδικα και ενεργοποιείται μόνο από έναν EOA, ενώ ο EOA κατέχεται από ιδιωτικά κλειδιά [34]. Ενώ ο CA συμβολίζει ένα έξυπνο συμβόλαιο, ο EOA απαιτείται για τη συμμετοχή στο δίκτυο Ethereum και επικοινωνεί με την αλυσίδα μπλοκ χρησιμοποιώντας συναλλαγές (SC). Το SC προσθέτει ένα επίπεδο συλλογισμού και υπολογισμού στην αρχιτεκτονική εμπιστοσύνης και είναι ένα στοιχείο κώδικα που υλοποιείται στον κόμβο της αλυσίδας μπλοκ [35]. Μια κωδικοποιημένη επικοινωνία στο SC ενεργοποιεί την εκτέλεση των συναλλαγών.

Το κινητό νόμισμα στο Ethereum ονομάζεται αιθέρας. Ο αιθέρας συμβολίζεται με το σύμβολο Wei [36]. Τόσο τα μηνύματα για την ενεργοποίηση των έξυπνων συμβολαίων όσο και τα ελάσματα για τη μεταφορά του αιθέρα περιλαμβάνονται σε μια συναλλαγή στο Ethereum [37]. Παρόμοια χαρακτηριστικά χρησιμοποιούνται από το Ethereum και το Bitcoin, όπως τα στοιχεία της συναλλαγής, το nonce και το hash του προηγούμενου μπλοκ. Χρησιμοποιεί επίσης άλλα πεδία όπως το ανώτατο όριο κόστους, την κατάσταση του SC κ.ο.κ. Το ποσό προς μεταφορά, η διεύθυνση του παραλήπτη, τα τέλη, οι πόντοι αερίου και οι αντίστοιχοι λογαριασμοί καθορίζονται για μια απλή μεταφορά αιθέρα. Με την εξέταση του χρονικού ορίου, του συνδυασμού nonce και της διαθεσιμότητας επαρκών τελών για την εκτέλεση, όλες οι παραγόμενες συναλλαγές θα επαληθευτούν.

Για τη δημιουργία μπλοκ, το Ethereum χρησιμοποιεί επίσης ένα μοντέλο που βασίζεται σε κίνητρα. Το Ethereum απαιτεί κρυπτογραφικό καύσιμο ή αέριο για κάθε λειτουργία. Για απλούστερους υπολογισμούς, το αέριο χρησιμοποιείται στη θέση του αιθέρα ως αμοιβή. Η κύρια αιτιολόγηση γι' αυτό είναι ότι το αέριο είναι ένα κρυπτονόμισμα του οποίου η αξία δεν σχετίζεται με τα τέλη συναλλαγών και το κόστος υπολογισμού. Σε αντίθεση με τα σημεία αερίου, η αξία του αιθέρα κυμαίνεται με τις διακυμάνσεις της αγοράς ως νόμισμα. Οι μονάδες αερίου που απαιτούνται για την εκτέλεση μιας συναλλαγής υπολογίζονται κατά τη διάρκεια της εξόρυξης. Η συναλλαγή απορρίπτεται εάν η αμοιβή που ορίζεται στη συναλλαγή σημείου αερίου δεν επαρκεί. Τόσο το υπόλοιπο του λογαριασμού όσο και η προτεινόμενη συναλλαγή πρέπει να περιέχουν τους πόντους αερίου που απαιτούνται για την εκτέλεση προκειμένου να προχωρήσει. Ο αρχικός λογαριασμός θα λάβει τα χρήματα που θα περισσεύουν μετά την ολοκλήρωση της συναλλαγής. Στο Ethereum, οι ανθρακωρύχοι ανταγωνίζονται για τη δημιουργία μπλοκ μέσω ενός μοντέλου κινήτρων εξόρυξης. Ο νικητής είναι ο εξορύκτης που ολοκληρώνει πρώτος το παζλ, ενώ οι όμηροι είναι οι εξορύκτες που το ολοκληρώνουν μετά [38]. Το μπλοκ του νικητή προστίθεται στην κύρια αλυσίδα, και τα πρόσθετα δευτερεύοντα μπλοκ προστίθενται στην κύρια αλυσίδα ως μπλοκ ommer. Το κόστος της συναλλαγής δίνεται στο νικητήριο μπλοκ ως πόντοι αερίου επιπλέον της βασικής χρέωσης των τριών αιθέρων. Ένα μικρό μέρος των συνολικών πόντων αερίου πηγαίνει στο μπλοκ των νικητών.

ΚΕΦΑΛΑΙΟ 3: Consensus Αλγόριθμοι

Το Consensus είναι ένα πρωτόκολλο που βασίζεται σε ομάδες για τη δυναμική επίτευξη συμφωνίας μεταξύ τους. Το Consensus, σε αντίθεση με την πλειοψηφία, τονίζει ότι ολόκληρη η ομάδα μπορεί να επωφεληθεί από την επίτευξη συναίνεσης. Το πρόβλημα της δυναμικής επίτευξης συναίνεσης στις ομάδες βασίζεται στον συντονισμό που βασίζεται στην ομάδα. Με την παρουσία κακόβουλων παραγόντων και ελαττωματικών διαδικασιών, αυτή η συντονισμένη συναίνεση μπορεί να παραβιαστεί. Για παράδειγμα, οι κακόβουλοι χρήστες μπορεί να δημιουργούν κρυφά αντικρουόμενα μηνύματα που εμποδίζουν τα μέλη της ομάδας να ενεργούν από κοινού, υπονομεύοντας έτσι την αποτελεσματικότητα της δράσης της ομάδας. Αυτό το πρόβλημα είναι γνωστό ως «Πρόβλημα των Βυζαντινών Στρατηγών» (BGP) [39]. Μια συλλογή στρατηγών που είναι υπεύθυνοι για ένα τμήμα των βυζαντινών δυνάμεων περικυκλώνουν την πόλη στο πρόβλημα BGP. Εάν μόνο ορισμένοι από τους στρατηγούς επιτεθούν στην πόλη, η εισβολή θα αποτύχει. Για να αποφασίσουν αν θα επιτεθούν ή όχι, οι στρατηγοί πρέπει να συμβουλευτούν ο ένας τον άλλον. Αλλά μεταξύ των στρατηγών μπορεί να υπάρχουν κατάσκοποι. Ο προδότης θα μπορούσε να δώσει σε κάθε στρατηγό μια ξεχωριστή επιλογή. Αυτό είναι ένα αναξιόπιστο σκηνικό. Σε ένα τέτοιο σκηνικό, μπορεί να είναι δύσκολο να καταλήξει κανείς σε συμφωνία. Η αποτυχία επίτευξης συναίνεσης λόγω λανθασμένων συμμετεχόντων είναι γνωστή ως βυζαντινό σφάλμα. Οι Leslie Lamport, Marshall Pease και Robert Shostak έδειξαν το 1982 ότι η βυζαντινή ανοχή σφαλμάτων μπορεί να επιτευχθεί μόνο εάν οι έντιμοι

στρατηγοί καταφέρουν να καταλήξουν σε πλειοψηφική συμφωνία για τη στρατηγική τους. Ο αλγόριθμος συναίνεσης που χρησιμοποιείται συνήθως στο τρέχον σύστημα blockchain παρέχει μια πιθανολογική λύση για το BGP.

3.1 Proof of Work (PoW)

Το πρωτόκολλο συναίνεσης που σχεδιάστηκε από τον Satoshi Nakamoto για το Bitcoin στοχεύει στην επίτευξη μιας συντονισμένης από το δίκτυο συναίνεσης σχετικά με την εγκυρότητα κάθε συναλλαγής Bitcoin. Παρακάμπτει το BGP («Πρόβλημα των Βυζαντινών Στρατηγών») χρησιμοποιώντας το πρωτόκολλο PoW.

Περιγράφουμε το PoW με διπλές ιδιότητες:

- θα πρέπει να είναι δύσκολο και χρονοβόρο για κάποιον να παράγει αποδείξεις που ικανοποιούν ορισμένες απαιτήσεις και
- θα πρέπει να είναι εύκολο και γρήγορο για άλλους για να επαληθεύσουν την απόδειξη της ορθότητάς της.

Για την πρώτη ιδιότητα, πρέπει να επινοηθεί μια πρόκληση απόδειξης εργασίας έτσι ώστε ο υπολογισμός μιας έγκυρης απόδειξης εργασίας να είναι δύσκολος, χαμηλής πιθανότητας και κάπως τυχαίος, επομένως απαιτεί πολλές δοκιμές και σφάλματα.

Χρησιμοποιούμε το BGP για να δείξουμε πώς λειτουργεί το PoW. Όταν τα στρατεύματα στα ανατολικά της πόλης θέλουν να στείλουν ένα μήνυμα στα στρατεύματα στα δυτικά της πόλης, ακολουθούμε τα βήματα του πρωτοκόλλου PoW:

1. Προσθέτουμε ένα "nonce" (συνήθως αρχίζει με μηδέν) στο αρχικό μήνυμα, το οποίο είναι ένας τυχαίος αριθμός σε δεκαεξαδική τιμή.
2. Εφαρμόζει έναν κατακερματισμό σε ένα μήνυμα που δεν έχει βελτιωθεί και ελέγχει εάν το αποτέλεσμα κατακερματισμού είναι μικρότερο ή ίσο με μια προκαθορισμένη τιμή (όπως πέντε μηδενικά στην αρχή).
3. Εάν πληρείται η συνθήκη κατακερματισμού, ο στρατός στη μία πλευρά της πόλης στέλνει τον κατακερματισμό και το μηδενικό μήνυμα στον στρατό στην άλλη πλευρά της πόλης. Εάν όχι, αυξάνουμε το nonce κατά 1 και επαναλαμβάνουμε τη διαδικασία μέχρι να επιτευχθεί το επιθυμητό αποτέλεσμα. Η εύρεση του σωστού nonce μπορεί να είναι χρονοβόρα και υπολογιστικά εντατική.
4. Λόγω του χαρακτηριστικού κατά της σύγκρουσης της συνάρτησης κατακερματισμού, είναι δύσκολο να παραβιαστεί η τιμή κατακερματισμού του μηνύματος ακόμη και αν ο αγγελιοφόρος έχει συλληφθεί. Επειδή η τιμή κατακερματισμού του παραποιημένου μηνύματος θα είναι πολύ διαφορετική από την τιμή κατακερματισμού του αρχικού μηνύματος, ο στρατηγός του ανατολικού στρατοπέδου μπορεί να επαληθεύσει ότι το μήνυμα ξεκινά με πέντε μηδενικά και να αγνοήσει το μήνυμα εάν δεν το κάνει.
5. Επαναλαμβάνεται η παραπάνω διαδικασία για πολλαπλές επαναλήψεις, έτσι ώστε να αποστέλλονται πολλαπλοί αγγελιοφόροι από τον στρατό στα ανατολικά στον στρατό στα δυτικά μέσω της πόλης.

Αυτό το τελευταίο βήμα είναι για να αντιμετωπιστεί η πιθανή ευπάθεια της αποστολής μόνο ενός αγγελιοφόρου: εάν η πόλη συλλάβει τον αγγελιοφόρο, λάβει το μήνυμα και το παραποιήσει, τότε

κατά συνέπεια, το nonce αλλάζει μέχρι να βρεθεί η σωστή τιμή nonce έτσι ώστε το επιθυμητό κέρδος να έχει το απαιτούμενο αποτέλεσμα κατακερματισμού του επιθυμητού αριθμού μηδενικών. Αν και αυτή η διαδικασία είναι υπολογιστικά δαπανηρή και χρονοβόρα, εξακολουθεί να είναι δυνατή. Το πρωτόκολλο PoW κλείνει αυτό το κενό αυξάνοντας τον αριθμό. Πρώτον, με την προσθήκη περισσότερων αγγελιοφόρων, μειώνονται σημαντικά οι πιθανότητες να πιαστούν. Δεύτερον, ακόμα και αν συλληφθούν μερικοί από αυτούς, ο χρόνος που απαιτείται για να παραβιαστεί το συσσωρευμένο μήνυμα και να βρεθεί η αντίστοιχη nonce για το hash αυξάνεται σημαντικά. Προκειμένου ένα μπλοκ να είναι έγκυρο στο blockchain, οι miners πρέπει να μπορούν να το κατακερματίσουν σε τιμή μικρότερη ή ίση με τον τρέχοντα στόχο και στη συνέχεια να υποβάλουν τη λύση τους στο δίκτυο για επαλήθευση από άλλους κόμβους. Οι διπλές ιδιότητες του PoW διασφαλίζουν ότι η εύρεση του σωστού nonce για τον κατάλληλο στόχο κατακερματισμού είναι εξαιρετικά δύσκολη και χρονοβόρα. Ωστόσο, είναι πολύ εύκολο και απλό να επαληθευτεί το αποτέλεσμα κατακερματισμού, ώστε να μην έχει γίνει καμία παραβίαση.

Το πρωτόκολλο PoW στο Bitcoin επεκτείνει το σύστημα Hashcash με κάποιες μικρές βελτιώσεις. Πρώτον, το Bitcoin περιορίζει τον ρυθμό με τον οποίο το δίκτυο μπορεί να δημιουργήσει και να προσθέσει νέα μπλοκ σε περίπου ένα κάθε 10 λεπτά. Επιτυγχάνει αυτόν τον έλεγχο ρυθμού παρακολουθώντας αυτόματα τον χρόνο που χρειάζεται για να λυθεί κάθε πρόκληση απόδειξης εργασίας και προσαρμόζοντας ανάλογα τη δυσκολία της πρόκλησης. Δεύτερον, το Bitcoin αυξάνει τη δυσκολία πρόβλεψης για το ποιος miner στο δίκτυο θα είναι σε θέση να δημιουργήσει το επόμενο μπλοκ δημιουργώντας επιτυχώς απόδειξη εργασίας με υψηλό κόστος.

Για την επίσημη ανάλυση του PoW, οι Garay και Kiayias αρχικά εξήγαγαν και ανέλυσαν επίσημα δύο βασικές ιδιότητες του πρωτοκόλλου Bitcoin: το δημόσιο πρόθεμα και την ποιότητα της αλυσίδας. Ωστόσο, η ανάλυσή τους βασίζεται σε πολλές υποθέσεις, όπως μια σταθερή ρύθμιση με δεδομένο αριθμό παικτών, ένα πλήρως σύγχρονο κανάλι δικτύου μέσω του οποίου τα μηνύματα παραδίδονται χωρίς καθυστέρηση. Πιο πρόσφατα, οι Pass και Shi πρότειναν το FruitChain, ένα πρωτόκολλο που επεκτείνει το πρωτόκολλο Bitcoin PoW μέσω ενός μηχανισμού ανταμοιβής, ενώ παρέχει τις ίδιες ιδιότητες συνέπειας και ζωντάνιας μέσω προσεγγιστικών αποδείξεων ισορροπίας Nash.

Αν και το πρωτόκολλο PoW μπορεί να λύσει αποτελεσματικά το Πρόβλημα των Βυζαντινών Στρατηγών, έχει τρεις περιορισμούς. Πρώτον, το πρωτόκολλο είναι μια εξαιρετικά αναποτελεσματική διαδικασία λόγω της υψηλής υπολογιστικής πολυπλοκότητας και της χαμηλής πιθανότητας δημιουργίας επιτυχούς απόδειξης εργασίας. Υποστηρίχθηκε ότι μπορεί να είναι ελκυστική η διερεύνηση πιο αποτελεσματικών πρωτοκόλλων με αντισταθμίσεις μεταξύ αποτελεσματικότητας και ισχυρής συνέπειας για διαφορετικές εφαρμογές με διαφορετικά επίπεδα απαιτήσεων συνέπειας και διαφορετικά επίπεδα ανοχής κινδύνου. Δεύτερον, η ασφάλεια του PoW προέρχεται κυρίως από την ανταμοιβή μπλοκ (mining), η οποία είναι ένα ισχυρό κίνητρο για την προσέλκυση μεγάλου αριθμού miners να συμμετάσχουν στο PoW, η οποία είναι απαραίτητη για τη διασφάλιση της ισχύς του πρωτοκόλλου blockchain PoW. Η ανθεκτικότητα εγγυάται, ότι από τη στιγμή που μια συναλλαγή προσαρτηθεί σε ένα μπλοκ βαθιά στο blockchain ενός κόμβου, έτσι ώστε ένα επιπλέον *ν* ή περισσότερα μπλοκ τοποθετηθούν πάνω από αυτό, η συναλλαγή θα συμπεριληφθεί τελικά σε κάθε μπλοκ πραγματικού κόμβου σε ένα δίκτυο υψηλής πιθανότητας στο blockchain. Το Liveness διασφαλίζει, ότι κάθε συναλλαγή από έναν πραγματικό κόμβο θα αποθηκευτεί τελικά σε ένα μπλοκ μεγαλύτερο από βάθος *ν* στην αλυσίδα και θα γίνει αμετάβλητο. Μια έντιμη πλειοψηφία πρέπει να έχει και τις δύο περιουσίες. Ενώ η οικονομική συναίνεση είναι πολύ σημαντική για την προστασία της ζωντάνιας και της επιμονής βραχυπρόθεσμα, η αναζήτηση μετριοπάθειας συνδυάζοντάς την με την κοινωνική συναίνεση μπορεί να έχει υγιή και ευρεία ανάπτυξη του blockchain σε πολλές άλλες εφαρμογές, όπως αποδεικνύεται από το δυναμικό του συστήματος Bitcoin.

Συνοπτικά, οι αλγόριθμοι Proof of Work τείνουν να βασίζονται σε αποκεντρωμένα κίνητρα και σε οικονομικά κίνητρα ασφάλειας. Προωθώντας περισσότερους miners, προσφέροντας ανταμοιβές δημιουργίας μπλοκ και επιβραβεύοντάς τους απαιτώντας λύσεις σε υπολογιστικά δαπανηρές προκλήσεις, επιτυγχάνεται η αποτροπή της δημιουργίας κεντρικών καρτέλ και συμπαιγνιακών μερών καθώς και η αποτροπή της αντικοινωνικής συμπεριφοράς τους.

3.2 Proof of Stake (PoS)

Το Proof-of-stake (PoS) μπορεί να είναι μια πιο ενεργειακά αποδοτική επιλογή σε σχέση με το Proof-of-work (PoW). Ο miner δεν χρειάζεται να χρησιμοποιήσει μεγάλη επεξεργαστική ισχύ για να απαντήσει στο μαθηματικό πρόβλημα χρησιμοποιώντας αυτή την τεχνική συναίνεσης. Αντίθετα, η συμμετοχή στη διαδικασία δημιουργίας μπλοκ εξαρτάται από το αν έχει αρκετά μεγάλο ενδιαφέρον για το σύστημα [40]. Το μερίδιο ή ο πλούτος του εμπλεκόμενου διακομιστή καθορίζει πλήρως την πιθανότητα να του δοθεί η ευκαιρία να επαληθεύσει ένα μπλοκ. Ένα επαρκές μερίδιο θεωρείται ότι αποτρέπει την πιθανότητα κακόβουλης επίθεσης στο δίκτυο [41]. Η αντιπαλότητα μεταξύ των ομότιμων εξαλείφεται επειδή ο επικυρωτής επιλέγεται ανάλογα με το συμφέρον που έχει στο δίκτυο. Ως αποτέλεσμα, ένας επαληθευτής ποντάρει σε ένα μπλοκ χρησιμοποιώντας την επένδυσή του. Ο επαληθευτής θα λάβει τις αμοιβές από τις συναλλαγές στο μπλοκ, εάν το μπλοκ επιβεβαιωθεί. Επειδή το PoS εξοικονομεί περισσότερη ενέργεια και προσφέρει μεγαλύτερη καθυστέρηση και ρυθμό μετάδοσης από το PoW, μπορεί να είναι πιο βιώσιμο [42]. Αυτή η διαδικασία συμφωνίας έχει, ωστόσο, ορισμένες ελλείψεις. Ο πιο πλούσιος κόμβος μπορεί να έχει περισσότερες ευκαιρίες να επαληθεύσει ένα μπλοκ και να γίνει πιο εξέχων στο δίκτυο, επειδή ο επικυρωτής επιλέγεται με βάση τα στοιχήματα, γεγονός που μπορεί να οδηγήσει σε άδικη κατανομή ή συγκεντρωτισμό. Το PoS μπορεί να είναι πιο επιρρεπές σε κακόβουλες επιθέσεις, καθώς το κόστος εξόρυξης και η προσπάθεια είναι πολύ μικρότερο σε σύγκριση με το PoW. Ένα πρόσφατα ανακαλυφθέν μειονέκτημα αυτού του αλγορίθμου συναίνεσης ονομάζεται Nothingat-stake problem[43]. Αυτό το πρόβλημα είναι ένα επακόλουθο της να μη βασίζεται σε μια φυσική πραγματικότητα για την εξασφάλιση ενός σημείου συντονισμού για συναίνεσης.

Πρόσφατοι αλγόριθμοι PoS, όπως ο Casper του Ethereum, προσπαθούν ενεργά να τιμωρήσουν τον επικυρωτή για κακόβουλη συμπεριφορά [44]. Προκειμένου να επιλύσουν αυτές τις δυσκολίες αναπτύσσονται το ποσό του στοιχήματος και διάφορες μέθοδοι για την επιλογή του επικυρωτή που θα έχει την ευκαιρία να πλαστογραφήσει το επόμενο μπλοκ. Για παράδειγμα, οι King et al. πρότειναν το Peercoin, το οποίο επιλέγει τα στοιχήματα με βάση την ηλικία, δίνοντας προτεραιότητα στις μεγαλύτερες ομάδες νομισμάτων κατά την εξόρυξη ενός μπλοκ [45]. Το Blackcoin αναπτύχθηκε από τους Vasin et al. Χρησιμοποιεί την τύχη για την επιλογή του επόμενου δημιουργού του μπλοκ και αναζητά τη χαμηλότερη τιμή κατακερματισμού, λαμβάνοντας επίσης υπόψη το ποσό του στοιχήματος [46]. Επιπλέον, ορισμένοι αλγόριθμοι συμφωνίας χρησιμοποιούν στοιχεία τόσο του PoS όσο και του PoW, συχνά με διαφορετικό χαρακτηριστικό. Για παράδειγμα, οι Bentov et al. πρότειναν τον αλγόριθμο Proof-of-Activity (PoA), ο οποίος συνδυάζει τα χαρακτηριστικά PoW και PoS, για να εγγυηθεί ότι οι επικυρωτές επιλέγονται με ψευδοτυχαίο αλλά συνεπή τρόπο [47]. Στο PoA, ένα μπλοκ μπορεί να θεωρηθεί νόμιμο μόνο εάν συμφωνούν με αυτό N ανθρακωρύχοι. Από την άλλη πλευρά, μπορεί να κινδυνεύει κάτι άλλο εκτός από χρήματα. Στο Proof-of-Capacity(PoC) οι miners εκχωρούν χώρο στους σκληρούς τους δίσκους για την επαλήθευση ενός μπλοκ. Άλλες, ελαφρώς διαφορετικές στρατηγικές περιλαμβάνουν το Proof-of-Importance (PoI), το Proof-of-Storage (PoSt) και το Proof-of-Deposit (PoD), οι οποίες χρησιμοποιούν μάρκες, αποθήκευση και καταθέσεις, αντίστοιχα, ως περιουσιακά στοιχεία για μια ευκαιρία εξόρυξης [48]-[50].

3.3 Delegated Proof of Stake (DPoS)

Η Delegated proof-of-stake (DPoS) είναι μια μέθοδος συμφωνίας με διακριτική ευχέρεια στην οποία κάθε κόμβος με συμμετοχή στο δίκτυο μπορεί να ψηφίσει για να αναθέσει σε άλλον κόμβο την ευθύνη επικύρωσης συναλλαγών [51]. Η DPoS είναι μια αντιπροσωπευτική δημοκρατική διαδικασία, ενώ η PoS υιοθετεί μια άμεση δημοκρατική στρατηγική. Οι αντιπρόσωποι, που αναφέρονται επίσης ως μάρτυρες, επιλέγονται από τους ενδιαφερόμενους για τη δημιουργία και την επαλήθευση ενός μπλοκ [52]. Αυτοί οι επιλεγμένοι κόμβοι συγκεντρώνονται στη συνέχεια ως ομάδα που προτείνει μπλοκ και επαληθεύει τις συνθήκες των δεδομένων. Ψηφίζουν εναλλάξ για μπλοκ εκ μέρους των μελών τους και επιβεβαιώνουν την εγκυρότητα των προηγούμενων μπλοκ. Γενικά, στα περισσότερα συστήματα χρησιμοποιούνται δεξαμενές αντικατάστασης με εφεδρικούς επικυρωτές για την αντιμετώπιση των αποτυχιών των κόμβων. Σε αντίθεση με το PoS, η επικύρωση ενός μπλοκ έχει σημαντικά λιγότερους παίκτες, γεγονός που επιταχύνει τη δημιουργία μπλοκ και επιβεβαιώνει τις συναλλαγές [53]. Προκειμένου να εξασφαλιστεί η αποτελεσματικότητα, μπορούν επίσης να ρυθμιστούν παράγοντες του δικτύου, όπως το μέγεθος των μπλοκ και τα διαστήματα των μπλοκ. Η τάση συγκεντρωτισμού αυτού του μηχανισμού συμφωνίας μπορεί να είναι το κύριο μειονέκτημά του. Οι παίκτες με υψηλό βαθμό μπορούν να ρίχνουν τις δικές τους ψήφους και να επηρεάζουν τους άλλους να ρίχνουν επικυρωτικές ψήφους. Ωστόσο, εάν ένας ανέντιμος μάρτυρας επιδεικνύει οποιαδήποτε κακία, οι ενδιαφερόμενοι έχουν το δικαίωμα να τον εκδιώξουν. Ένας ιστότοπος που χρησιμοποίησε τη μέθοδο συναίνεσης DPoS είναι η Bitshare.

3.4 Πλεονεκτήματα και Μειονεκτήματα

Σε ένα δίκτυο blockchain που βασίζεται σε PoW, οι miners ανταγωνίζονται για να είναι οι πρώτοι που θα λύσουν ένα proof of work, καθώς ο νικητής που θα προσθέσει πρώτος το επόμενο μπλοκ στο blockchain ανταμείβεται. Αυτή η ανταμοιβή περιλαμβάνει ανταμοιβές δημιουργίας μπλοκ και χρεώσεις συναλλαγών. Αντίθετα, με το PoS, για να προστεθεί το επόμενο μπλοκ στο blockchain, κάθε κατάλληλος επικυρωτής πρέπει να ποντάρει σε αυτό το μπλοκ προκειμένου να είναι κατάλληλος για να είναι validator για αυτό το μπλοκ. Εάν προσαρτηθεί ένα μπλοκ, τότε όλοι οι validators θα ανταμειφθούν ανάλογα με το ποντάρισμά τους. Δεν υπάρχει ανταμοιβή για την δημιουργία μπλοκ, επομένως ο miner μπορεί να λάβει ανταμοιβές μόνο μοιράζοντας την προμήθεια συναλλαγής του μπλοκ αλλά επιπλέον λαμβάνοντας υπόψη και την αναλογία ποντάρισματος στο μπλοκ. Οι επικυρωτές από την άλλη, λαμβάνουν μικρές ανταμοιβές για να τους αποζημιώσουν για το κλείδωμα της κατάστασης, τη διατήρηση των κόμβων και τη λήψη πρόσθετων προφυλάξεων για την προστασία των ιδιωτικών κλειδιών τους. Το μεγαλύτερο μέρος του κόστους ανάκτησης προέρχεται από κυρώσεις που δημιουργούνται από τις συναλλαγές, οι οποίες μπορεί να είναι πολύ μεγαλύτερες από τις ανταμοιβές που λαμβάνουν ταυτόχρονα. Σε αντίθεση λοιπόν με το PoW που έχει "ασφάλεια από ανταμοιβές για την καύση υπολογιστικής ενέργειας", το Proof of Stake εξασφαλίζει "ασφάλεια από κυρώσεις για απώλεια οικονομικής αξίας".

Υπάρχουν πολλές εκδόσεις συναινετικών αλγορίθμων που βασίζονται σε PoS. Από αλγοριθμική προοπτική, το PoS που βασίζεται σε αλυσίδα και το PoS βυζαντινού τύπου με ανοχή σε σφάλματα (BFT) είναι οι δύο κύριοι τύποι.

Σε PoS που βασίζεται σε αλυσίδα, ο αλγόριθμος επιλέγει τυχαία έναν validator κάθε χρονική περίοδο (π.χ. κάθε 10 δευτερόλεπτα) και εκχωρεί σε αυτόν το δικαίωμα επικύρωσης να δημιουργήσει ένα μπλοκ και να συνδέσει αυτό το μπλοκ (συνήθως το τρέχον μπλοκ) με κάποιο προηγούμενο μπλοκ (το

τελευταίο μπλοκ της προηγούμενης μακρύτερης αλυσίδας). Έτσι, με την πάροδο του χρόνου, η πλειοψηφία των μπλοκ συγκλίνει σε μια αυξανόμενη αλυσίδα.

Οι πρώτες εκδόσεις του αλγορίθμου PoS που βασίζεται στην αλυσίδα ήταν αφελείς επειδή οι ανταμοιβές χρησιμοποιήθηκαν για την παραγωγή μπλοκ χωρίς ποινές και, ως εκ τούτου, υπέφεραν από το πρόβλημα της «ανιθαγένειας». Συγκεκριμένα, οι επικυρωτές μπορούν να ψηφίσουν και να παράγουν μπλοκ σε πολλαπλές ανταγωνιστικές αλυσίδες ταυτόχρονα, και μπορούν να το κάνουν χωρίς να επιβαρυνθούν με επιπλέον κόστος. Σε αυτόν τον αφελή σχεδιασμό PoS, οι πολλαπλές ανταγωνιστικές αλυσίδες είναι μεγαλύτερες από την αναμενόμενη τιμή ψηφοφορίας σε μία μόνο αλυσίδα. Ακόμη και χωρίς εισβολέα, ένα blockchain μπορεί να μην καταλήξει ποτέ σε συναίνεση.

3.5 Άλλοι Consensus Αλγόριθμοι

Sleepy Consensus. Το "παράδειγμα του ύπνου" που προτείνεται από το Sleepy Consensus [54] υποθέτει ότι οι χρήστες είναι είτε "ξύπνιοι/ενεργοί" (online) είτε "κοιμισμένοι" (offline). Οι συμμετέχοντες έχουν τη δυνατότητα να εναλλάσσονται μεταξύ του να είναι ξύπνιοι και του να είναι "κοιμισμένοι" ανά πάσα στιγμή κατά τη διάρκεια της διαδικασίας που ακολουθείται. Όταν ο αριθμός των έντιμων ατόμων είναι στην πλειονότητα, ο sleepy consensus έχει αποδειχθεί ότι είναι ανθεκτικός.

Μια PKI χρησιμοποιείται για τη δημιουργία του Sleepy Consensus. Στο πλαίσιο του μοντέλου χρονισμού του Dwork-Naor-Sahai [55], όπου το δίκτυο υποτίθεται ότι είναι χαλαρά συγχρονισμένο και υπάρχουν πολύ μικρές αποκλίσεις μεταξύ όλων των ρολογιών και του "πραγματικού χρόνου", αποδεικνύεται ότι είναι ασφαλής και συνεπής. Το πρώτο πρωτόκολλο του Sleepy αλγόριθμου αφορά το γεγονός πως είναι απλός στη χρήση, επειδή βασίζεται στη συνάρτηση hash(κατακερματισμού) που είναι ανθεκτική στις συγκρούσεις. Ωστόσο, επιτρέπει μόνο το "στατικό online χρονοδιάγραμμα" και τις στατικές αλλοιώσεις. Το δεύτερο πρωτόκολλο του Sleepy αλγόριθμου βελτιώνει την ασφάλεια με δύο τρόπους:

- Επιτρέπει ευέλικτες αλλοιώσεις.
- Είναι ανθεκτικός ακόμη και όταν ένας αντίπαλος επιλέγει τυχαία ποιοι κόμβοι είναι διαθέσιμοι και σε ποιες ώρες.

Αντί να χρησιμοποιεί PoW όπως άλλες μέθοδοι κατανεμημένης συμφωνίας, η πρωταρχική ιδέα του Sleepy αλγόριθμου βασίζεται στο πρωτόκολλο blockchain του Bitcoin PoW. Ο Sleepy consensus, ωστόσο, δεν εφαρμόζεται όταν ο κύριος όγκος των διαδικτυακών συμμετεχόντων είναι ανέντιμος.

Proof of elapsed time (PoET). Ο consensus αλγόριθμος δικτύου blockchain, που προτάθηκε από την Intel [56], επιτυγχάνει δικαιοσύνη και την ελάχιστη χρήση υπολογιστών χρησιμοποιώντας την SGX, την αξιόπιστη υπολογιστική πλατφόρμα της Intel. Κάθε εμπλεκόμενος κόμβος στο PoET απαιτείται να περιμένει για ένα αυθαίρετα επιλεγμένο χρονικό διάστημα και ο πρώτος που θα ολοκληρώσει την περίοδο αναμονής επιτρέπεται να δημιουργήσει ένα νέο μπλοκ. Όταν ένα νέο μπλοκ μεταδίδεται στο δίκτυο, το SGX επιτρέπει στον διακομιστή να παράγει μια εύκολα επαληθεύσιμη απόδειξη της περιόδου αναμονής.

Ωστόσο, το SGX δεν είναι απολύτως αξιόπιστο, όπως ακριβώς και η πλειονότητα των ασφαλών υπολογιστικών συστημάτων. Για παράδειγμα, μπορεί να μην είναι σε θέση να σταματήσει τις επιθέσεις εναντίον βασικών εχθρών που διαθέτουν τους απαιτούμενους πόρους. Μια νέα έρευνα [57] καταδεικνύει τις αδυναμίες ασφαλείας του πρωτοκόλλου blockchain, καθώς χρησιμοποιείται με την πλατφόρμα SGX της Intel. Για να μειωθούν αυτές οι αδυναμίες, προτείνονται δύο λύσεις:

- Αλλαγή της κατανομής των πιθανοτήτων
- Εφαρμογή στατιστικών ελέγχων για την απόρριψη ορισμένων μπλοκ που παράγονται από ένα συγκεκριμένο ποσοστό κόμβων

Proof of Authority (PoA). Μια μέθοδος συναίνεσης που επιτρέπει σχετικά γρήγορες συναλλαγές ονομάζεται Proof of Authority [58]. Η θεμελιώδης αρχή της PoA είναι ότι μόνο οι επικυρωτές έχουν την εξουσία να αποδέχονται νέα μπλοκ και συναλλαγές. Ένας συμμετέχων κόμβος αποκτά μια φήμη που σχετίζεται με το όνομά του και ο κόμβος μπορεί να γίνει επικυρωτής μόνο όταν η φήμη του φτάσει σε έναν υψηλό αριθμό. Για δύο λόγους, το PoA θεωρείται πιο αξιόπιστο από το PoS. Για να αποφύγουν να συνδεθεί η ταυτότητά τους με μια κακή εικόνα, οι επικυρωτές έχουν κίνητρο να ελέγχουν έντιμα τις συναλλαγές και τα μπλοκ. Από την άλλη πλευρά, ένας επικυρωτής δεν επιτρέπεται να αποδεχθεί δύο διαδοχικές συναλλαγές. Ως αποτέλεσμα, η εμπιστοσύνη δεν μπορεί να συγκεντρωθεί.

Proof of Reputation (PoR). Το PoR, το οποίο σημαίνει Evidence of Character, είναι μια επέκταση του PoA. Πολυάριθμοι οργανισμοί μελέτης και επιχειρήσεις έχουν κάνει πρόσφατα την πρόταση αυτή [59-61]. Η μέθοδος συναίνεσης PoR μπορεί να έχει διάφορες τροποποιήσεις και παράγοντες προσαρμογής, αλλά η θεμελιώδης έννοια είναι απλή. Ο χαρακτήρας οικοδομείται και προσδιορίζεται με τη χρήση προκαθορισμένων αλγορίθμων. Ένας κόμβος μπορεί να εκλεγεί στο δίκτυο ως έγκυρος κόμβος αφού επιδείξει σεβασμό και περάσει από επαλήθευση. Σε αυτό το στάδιο, το δίκτυο λειτουργεί όπως ένα PoA, με μόνο τους έγκυρους κόμβους να μπορούν να υπογράφουν και να επαληθεύουν μπλοκ.

ΚΕΦΑΛΑΙΟ 4: Εφαρμογές Blockchain

4.1 Εισαγωγή

Το Blockchain είναι μια τεχνολογία και μια μέθοδος που επιτρέπει στους χρήστες να επικυρώνουν, να διατηρούν και να συγχρονίζουν το περιεχόμενο ενός καθολικού συναλλαγών το οποίο αναπαράγεται σε πολλαπλούς χρήστες. Με άλλα λόγια, το Blockchain είναι μία αποκεντρωμένη τεχνολογία διαχείρισης συναλλαγών και δεδομένων η οποία απέκτησε δημοτικότητα το 2008, όταν ένα ανώνυμο άτομο (ή ομάδα) δημοσίευσε μια λευκή βίβλο που εισήγαγε το Bitcoin, μία Blockchain εφαρμογή ενός ψηφιακού νομίσματος [62] [63].

Η πλειονότητα των ατομικών συναλλαγών -χρηματοοικονομικές, εκπαιδευτικές, υγειονομικής περίθαλψης κ.λπ.- μέχρι σήμερα είναι συγκεντρωμένες μέσω αξιόπιστων τρίτων μερών. Μετά την αποφοίτησή, για παράδειγμα, ο εργοδότης μπορεί να ζητήσει ένα επίσημο πιστοποιητικό σπουδών ως απόδειξη της επιτυχούς ολοκλήρωσης των σπουδών. Το πανεπιστήμιο, το οποίο λειτουργεί ως αξιόπιστος μεσάζων μεταξύ του σπουδαστή και του εργοδότη για να εγγυηθεί ότι οι πληροφορίες είναι σωστές και γνήσιες, είναι το σημείο από το οποίο λαμβάνεται αυτό το πιστοποιητικό σπουδών. Γιατί όμως ο εργοδότης δεν ζητάει αντίγραφο της αναλυτικής βαθμολογίας του φοιτητή; Η βάση γι' αυτό είναι η εμπιστοσύνη, επειδή ο υποψήφιος έχει τη δυνατότητα να αλλάξει το υλικό προς όφελός του. Στην ουσία, η εμπιστοσύνη είναι το πραγματικό αγαθό ή η υπηρεσία που προσφέρει ένας τρίτος και αυτό ακριβώς υπόσχεται το blockchain.

Εικόνα 6. Τομείς εφαρμογής της τεχνολογίας Blockchain [125]

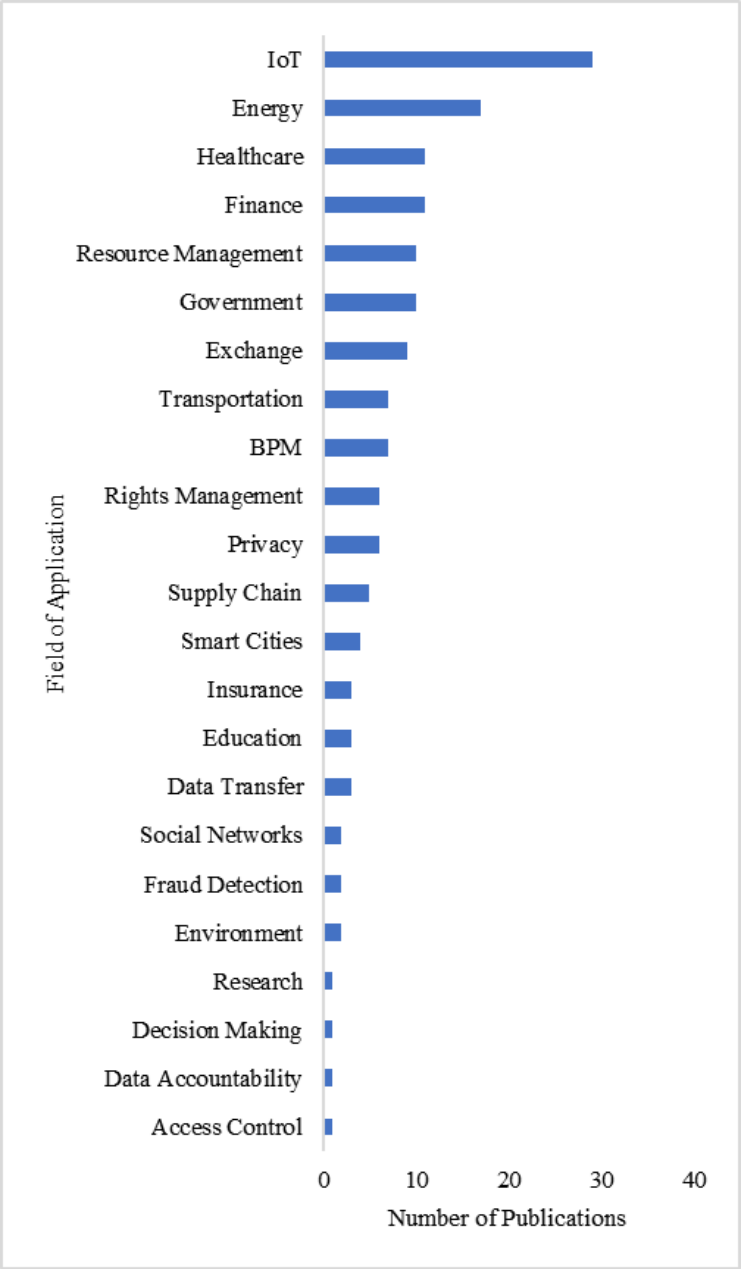
Πιο συγκεκριμένα, το blockchain προσφέρει ένα αποκεντρωμένο περιβάλλον όπου δεν είναι απαραίτητη η εμπιστοσύνη μεταξύ των ενδιαφερομένων και τα δεδομένα δεν ελέγχονται από τρίτους. Οι συναλλαγές σφραγίζονται χρονολογικά σε ένα βιβλίο με χρονολογική σειρά και αυτό επιτυγχάνεται με τη χρήση ενός μηχανισμού αυτοελέγχου που συντηρείται από ομότιμους. Το καθολικό είναι δημόσια ελέγξιμο, καθώς οι συναλλαγές μεταδίδονται σε οποιονδήποτε χρησιμοποιεί το σύστημα [63]. Η κοινότητα αντιγράφει και διατηρεί τις πληροφορίες των συναλλαγών, οπότε δεν μπορούν να αλλάξουν ή να τροποποιηθούν χωρίς τη συγκατάθεση και την ενημέρωση του καθολικού. Αυτό προφυλάσσει από την απάτη και εγγυάται μια ψηφιακή μορφή πιστοποίησης, επιτρέποντας συναλλαγές "χωρίς εμπιστοσύνη" μεταξύ ομοτίμων.

Τα μέλη του δικτύου θα επωφεληθούν από την πρόταση αυτή με διάφορους τρόπους. Πρώτον, εφόσον δεν υπάρχει ανάγκη για μια κεντρική αρχή να ελέγχει ή να πιστοποιεί τις συναλλαγές, όλοι μπορούν να το κάνουν άμεσα- δεύτερον, εφόσον δεν υπάρχει ανάγκη για έναν μεσάζοντα μεταξύ των μερών, οι συναλλαγές και οι ανταλλαγές πληροφοριών μπορούν να γίνουν ταχύτερα λόγω της ανοικτής πληροφόρησης. Τέλος, ακόμη και αν τα δεδομένα είναι δημόσια προσβάσιμα, εξακολουθούν να είναι ανώνυμα, δεδομένου ότι κάθε λογαριασμός διαθέτει ένα μοναδικό ζεύγος δημόσιου και ιδιωτικού κλειδιού. Όλοι έχουν πρόσβαση στο δημόσιο κλειδί, ενώ μόνο το άτομο έχει πρόσβαση στο ιδιωτικό κλειδί, εξασφαλίζοντας την ανωνυμία της ταυτότητας του συγκεκριμένου μέρους.

Ενώ η τεχνολογία blockchain μπορεί να έχει λαμπρό μέλλον, ο ενθουσιασμός γύρω από τις πιθανές χρήσεις της μάλλον την έχει βλάψει. Αυτή η ευφορία έδωσε τη δυνατότητα σε αμφίβολες και ανέντιμες επιχειρήσεις να τοποθετηθούν ως οι κορυφαίοι εμπειρογνώμονες στην τεχνολογία Blockchain. Παρόλο που αυτό μπορεί να μείωσε κάποια εμπιστοσύνη, ιδίως στους χρηματοπιστωτικούς και τεχνολογικούς κλάδους, είχε το πλεονέκτημα ότι προσέλκυσε μεγαλύτερη προσοχή και ενδιαφέρον του κοινού για το θέμα. Ως αποτέλεσμα, ενθάρρυνε την ακαδημαϊκή μελέτη των τεχνικών πτυχών και εφαρμογών του.

Στην παρούσα ενότητα πλαισιώνεται η αρχική χρήση της τεχνολογίας Blockchain και παρακολουθείται η μετέπειτα εξέλιξή της σε διάφορα πεδία μελέτης. Περιγράφεται επίσης η προσέγγιση για την πραγματοποίηση μιας βιβλιογραφικής ανασκόπησης και τη διαδικασία επιλογής

και χαρτογράφησης. Στη συνέχεια αναπτύσσονται τα αποτελέσματα της διαδικασίας και ακολουθεί μια ανασκόπηση της κατάστασης της έρευνας για την εφαρμογή του Blockchain. Η χρήση της τεχνολογίας Blockchain σε αυτή την ενότητα αφορά το εμπορικό και βιομηχανικό περιβάλλον.



Εικόνα 7. Πλήθος εφαρμογών Blockchain ανά τομέα [126]

4.2 Internet of Things

Το διαδίκτυο των αντικειμένων είναι μέχρι στιγμής το πιο δημοφιλή πεδίο εφαρμογών. Το είκοσι (29) τοις εκατό από τα 151 άρθρα αφορούσαν εφαρμογές blockchain. Όλα αυτά τα άρθρα καταδεικνύουν την ικανότητα του blockchain να βελτιώνει και να επαυξάνει το παράδειγμα του IoT. Κατά την ανασκόπηση αυτών των άρθρων IoT ξεχώρισαν τα παρακάτω θέματα εντός του πεδίου:

- Ενίσχυση ασφάλειας συνδεδεμένων συσκευών
- Διατήρηση ανωνυμίας
- Όροι έξυπνων συμβολαίων
- Μηχανισμοί διαχείρισης συσκευών και πρωτοκόλλων
- Ασφάλεια δικτύου

4.2.1 Ενίσχυση Ασφάλειας Συνδεδεμένων Συσκευών

Ένα σημαντικό πρόβλημα με τη διασύνδεση εκατομμυρίων συσκευών που απαιτούνται για τη διάδοση του φαινομένου IoT είναι η εκθετική αύξηση των ανησυχιών για την ασφάλεια που δημιουργούνται από τις διάφορες διεπαφές που χρησιμοποιούν οι δικτυωμένες συσκευές για την επικοινωνία. Αυτό περιλαμβάνει μια ποικιλία θεμάτων ασφαλείας που σχετίζονται με το IoT, συμπεριλαμβανομένων, ενδεικτικά, ζητημάτων χαμηλού επιπέδου, όπως η αλληλοσύνδεση αντιπάλων και οι ανασφαλείς φυσικές διεπαφές, καθώς και θέματα ασφάλειας μεσαίου επιπέδου, όπως η ανακάλυψη μη ασφαλούς γείτονα, ο έλεγχος ταυτότητας και η επικοινωνία σε προηγμένα θέματα ασφάλειας, συμπεριλαμβανομένων των μη ασφαλών διεπαφών, ασφάλεια λογισμικού/υλικολογισμικού και ενδιάμεσου λογισμικού [64].

Αντιμετωπίζονται διάφορες λύσεις σχετικές με το blockchain που σχετίζονται με ζητήματα όσον αφορά την ασφάλεια του IoT. Συγκεκριμένα, το blockchain μπορεί να εκμεταλλευτεί τον χώρο διευθύνσεών του (160 bit), μειώνοντας έτσι σημαντικά την πιθανότητα συγκρούσεων διευθύνσεων και εξαλείφοντας την ανάγκη για μια κεντρική αρχή για τη διαχείριση αριθμών που έχουν εκχωρηθεί από το Διαδίκτυο, παρέχοντας παράλληλα μια πιο επεκτάσιμη λύση με την επιλογή να έχουμε περισσότερες πολλαπλές διευθύνσεις από ότι με το IPv6.

Επιπλέον, χρησιμοποιώντας τους μηχανισμούς διαχείρισης ταυτότητας και διακυβέρνησης του blockchain, οι συσκευές που σχετίζονται με το IoT μπορούν εύκολα να εγγραφούν και να αναγνωριστούν σε ένα ενοποιημένο καθολικό με τη δυνατότητα να επισημαίνονται ως συγκεκριμένοι χρήστες έχοντας την επιλογή γρήγορης και ασφαλούς μεταφοράς των δικαιωμάτων και της ιδιοκτησίας των συσκευών μεταξύ των μελών του συστήματος.

Η ακεραιότητα των δεδομένων επιβεβαιώνεται μέσω του φυσικού σχεδιασμού της τεχνολογίας blockchain και της αμετάβλητης λογιστικής της, έτσι ώστε όλα τα δεδομένα που μεταδίδονται μέσω του δικτύου να είναι κρυπτογραφικά πιστοποιημένα, επιτυγχάνοντας έτσι την ασφαλή παρακολούθηση και την ακεραιότητα τους. Ταυτόχρονα, ο μηχανισμός ιδιωτικού/δημόσιου κλειδιού που δημιουργήθηκε μέσω του blockchain θα επιτρέψει τη δραστική απλοποίηση των πρωτοκόλλων ασφαλείας που απαιτούνται για να ενεργοποιηθεί η ασφάλεια στα παραδοσιακά πρωτόκολλα επικοινωνίας. Ωστόσο, η μελέτη αποτυγχάνει να αντιμετωπίσει ζητήματα που σχετίζονται με την υιοθέτηση του blockchain σε συσκευές, ειδικά όσον αφορά την υπολογιστική ισχύ που απαιτείται για την επαλήθευση των Proof of Work μηχανισμών σε μικρές και χαμηλού κόστους συσκευές.

4.2.2 Διατήρηση Ανωνυμίας

Από την οπτική του χρήστη, υπάρχει εγγενής έλλειψη εμπιστοσύνης στο να έχουμε συσκευές σε συνεχή επικοινωνία με τις εταιρείες που τις παράγουν και να στέλνουμε δεδομένα από ιδιώτες καταναλωτές με στοχευμένους τρόπους σε οντότητες που επιδιώκουν κέρδος. Αυτά τα ζητήματα έχουν αναφερθεί ως καθυστερήσεις στην υιοθέτηση ορισμένων οικιακών ηχείων και έξυπνων βοηθών, εν μέσω φόβου ότι οι εταιρείες θα κατασκοπεύουν τους πελάτες τους. Το Blockchain βοηθά σε αυτό, επιτρέποντας τη «διαφανή ασφάλεια», όπου πραγματοποιείται η ασφαλής μεταφορά δεδομένων μεταξύ των χρηστών, διατηρώντας παράλληλα την ανωνυμία των συγκεκριμένων ταυτοτήτων τους [16].

Το Blockchain επιλύει το δίλημμα ασφαλείας που αντιμετωπίζουν αυτή τη στιγμή οι περιορισμένες συσκευές σε ένα πλαίσιο IoT όπου οι οργανισμοί δεν μπορούν να επιβάλουν τα τρέχοντα πρότυπα ελέγχου πρόσβασης, αλλά ταυτόχρονα δεν θέλουν να συμπεριλάβουν ισχυρούς κεντρικούς μηχανισμούς (λόγω ανησυχιών για το απόρρητο και την ευαισθησία δεδομένων). Για το σκοπό αυτό, το blockchain μπορεί να εισαγάγει ένα αποκεντρωμένο πλαίσιο διαχείρισης εξουσιοδοτήσεων που αξιοποιεί τη συνέπεια της τεχνολογίας blockchain για την αντιμετώπιση ζητημάτων απορρήτου και ευαισθησίας δεδομένων [65], [66].

Ωστόσο, αυτές οι μελέτες δεν καλύπτουν τους κινδύνους από την έκθεση ταυτότητας και την απώλεια της ανωνυμίας από τη χρήση πρόσθετων πληροφοριών για την έμμεση ταυτοποίηση ατόμων που σχετίζονται με δημόσια κλειδιά.

4.2.3 Έξυπνα Συμβόλαια

Τα έξυπνα συμβόλαια αξιοποιούν την τεχνολογία blockchain για να μπορούν να δημιουργούν συμβάσεις και συμφωνίες μεταξύ των μερών τους. Αυτές οι συμφωνίες ουσιαστικά είναι προγράμματα που περιέχουν συγκεκριμένες εντολές που τους επιτρέπεται να εκτελούνται εντός του πλαισίου και της δυνατότητας εφαρμογής συγκεκριμένων παραμέτρων. Αυτές οι συμβάσεις υπάρχουν στο blockchain και αποτελούν μέρος ενός αποκεντρωμένου περιβάλλοντος που επιτρέπει την αυτοματοποίηση και την εκτέλεση διαδικασιών πολλαπλών βημάτων, διευκολύνοντας έτσι την ανταλλαγή πληροφοριών και χρημάτων στο blockchain.

Ένα παράδειγμα έξυπνου συμβολαίου μπορεί να βρεθεί στην πλατφόρμα Ethereum, όπου ο εκδότης ενός νέου κρυπτονομίσματος ορίζει μια συγκεκριμένη ισοτιμία μεταξύ του νέου κρυπτονομίσματος και του Ethereum. Αυτές οι παράμετροι εξαρτώνται από τον ίδιο τον εκδότη της σύμβασης και μπορεί να κυμαίνονται από τον όγκο συναλλαγών έως το συνολικό ποσό του νομίσματος που διανέμεται σε εκείνη τη χρονική στιγμή. Μέσω έξυπνων συμβολαίων, οι εκδότες μπορούν να αυτοματοποιήσουν τη διαδικασία των χρηστών που στέλνουν τα Ethereum token τους και λαμβάνουν ένα κατάλληλο και ισοδύναμο ποσό του σχετικού κρυπτονομίσματος.

Τα έξυπνα συμβόλαια μπορούν επίσης να χρησιμοποιηθούν για άλλους σκοπούς, όπως η διανομή περιεχομένου (Content distribution), η διαχείριση της εφοδιαστικής αλυσίδας (Supply chain management) και το Διαδίκτυο των πραγμάτων (Internet of Things). Μέσω έξυπνων συμβάσεων, η διανομή περιεχομένου μπορεί να διαχειρίζεται προσδιορίζοντας συγκεκριμένες μετρήσεις που σχετίζονται με την κατανάλωση μέσων και περιεχομένου και εφαρμόζοντας ίση αμοιβή για τη χρήση αυτή, η οποία επιτρέπει την αμοιβή για καλλιτέχνες και δημιουργούς περιεχομένου με μη ενδιάμεσο τρόπο. Ομοίως, οι αλυσίδες εφοδιασμού μπορούν να αξιοποιήσουν έξυπνα συμβόλαια για να αυτοματοποιήσουν τα βήματα που πρέπει να γίνουν κατά την αποστολή, την άφιξη ή τη μεταφόρτωση ενός αντικειμένου· αυτό μπορεί να γίνει μέσω του Διαδικτύου των πραγμάτων που

χρησιμοποιεί αισθητήρες και τσιπ RFID που επιτρέπει την ανταλλαγή πληροφοριών χωρίς επίβλεψη καθώς και την ενημερωμένη παρακολούθηση της προέλευσης των αντικειμένων και των τροφίμων [62].

Ενώ τα έξυπνα συμβόλαια προσφέρουν ορισμένα πλεονεκτήματα που συμβάλλουν στην αύξηση της ελκυστικότητας των blockchains σε σχέση με άλλα συστήματα, ζητήματα όπως τα διαφορετικά πρότυπα και η περιορισμένη λειτουργικότητα παραμένουν ένα ζήτημα. Συγκεκριμένα, δεδομένου ότι τα έξυπνα συμβόλαια είναι προγράμματα, μπορούν να γραφτούν με πολλούς τρόπους και να έχουν διαφορετικές παραμέτρους και πρότυπα, γεγονός που δυσκολεύει τους μη τεχνικούς χρήστες να κατανοήσουν και να εφαρμόσουν ή να συμφωνήσουν στη χρήση έξυπνων συμβολαίων σε συναλλαγές λόγω φόβου απάτης. Αυτό το πρόβλημα αντιμετωπίζεται επί του παρόντος χρησιμοποιώντας πρότυπα που εφαρμόζονται σε πλατφόρμα, όπως το πρότυπο διακριτικού EC20 που χρησιμοποιείται στο Ethereum, το οποίο καθορίζει τα στοιχεία και τη δομή που απαιτούνται για έξυπνες συμβάσεις.

Το δεύτερο ζήτημα περιστρέφεται γύρω από την περιορισμένη χρήση έξυπνων συμβολαίων, ειδικά στα κρυπτονομίσματα. Στην περίπτωση του Ethereum, τα συμβόλαια μπορούν να πραγματοποιούν αυτόματα ανταλλαγές μεταξύ ενός δεδομένου κρυπτονομίσματος και των διακριτικών Ethereum, αλλά δεν μπορούν να δημιουργήσουν ανταλλαγές και μεταφορές από οποιοδήποτε κρυπτονόμισμα σε άλλο, το οποίο είναι επίσης γνωστό ως sidechain. Στην περίπτωση του Ethereum, αυτό το πρόβλημα επί του παρόντος επιλύεται επιτρέποντας την ύπαρξη τέτοιων παραμέτρων στα έξυπνα συμβόλαια και επιτρέποντας στο blockchain να ενσωματώσει αυτές τις συναλλαγές.

Παρακάτω παρατίθεται μια μερική περίληψη των δημοφιλών συστημάτων που υποστηρίζουν έξυπνες συμβάσεις:

- **Ethereum**: Το Ethereum είναι μία ανοιχτή πλατφόρμα λογισμικού και κρυπτονόμισμα που βασίζεται στο blockchain και επιτρέπει στους προγραμματιστές να δημιουργούν και να διανέμουν αυτόνομες εφαρμογές (dApp). Με βάση τους διαθέσιμους πόρους από τους ομότιμους, το δίκτυο επιτρέπει την εκτέλεση αλγορίθμων που είναι πλήρεις κατά Turing και εκφράζονται στη γλώσσα υπολογιστών Solidity στην εικονική μηχανή Ethereum Virtual Machine (EVM), μια εικονική μηχανή. Ένα ευρύ φάσμα εφαρμογών που προηγουμένως ήταν αδιανόητες τροφοδοτούνται πλέον από το δίκτυο, από την ηλεκτρονική ψηφοφορία, τη συμμόρφωση, τις συναλλαγές κ.λπ.
- **NEM**: Το NEM είναι ένα διαφορετικό, αποκεντρωμένο δίκτυο ομότιμων που βασίζεται στην αλυσίδα μπλοκ και επιτρέπει σε τρίτους να δημιουργούν εφαρμογές για έξυπνα περιουσιακά στοιχεία, συμπεριλαμβανομένων, μεταξύ άλλων, νομισμάτων και crowdsourcing tokens. Το NEM διαφέρει από άλλες αλυσίδες μπλοκ στο ότι χρησιμοποιεί συμφωνία proof-of-importance αντί για proof-of-stake ή proof-of-work. Οι λογαριασμοί πολλαπλών υπογραφών, η ανωνυμία, οι επικοινωνίες, η επεκτασιμότητα και το γεγονός ότι σχεδόν κάθε μέλος της κοινότητας του NEM μπορεί να προτείνει αλλαγές και εξελίξεις είναι μερικά από τα πλεονεκτήματα του NEM.
- **NEO**: Το πρωτόκολλο NEO επιτρέπει την εκτέλεση έξυπνων συμβολαίων χωρίς εμπιστοσύνη που μπορούν να χρησιμοποιηθούν για επιχειρηματικές δραστηριότητες, καθώς και ως πλαίσιο για πιο σύνθετες. Όσον αφορά τη χρηστικότητα, ανταγωνίζεται το Ethereum. Χρησιμοποιείται κυρίως στην Ασία, όπου θεωρείται ο βασιλιάς του κλάδου.
- **Cardano**: Το Cardano, το οποίο επιτρέπει την υλοποίηση και εκτέλεση έξυπνων συμβολαίων, είναι αρκετά συγκρίσιμο με το Ethereum. Το “Ouroboros”, η μέθοδος εξόρυξης proof-of-stake που χρησιμοποιεί λιγότερη ενέργεια από εκείνη του Ethereum,

είναι το βασικό χαρακτηριστικό που το διαφοροποιεί από το Ethereum και άλλα έξυπνα συμβόλαια. Η έκδοση χρεωστικών καρτών που μπορούν να χρηματοδοτηθούν από το ηλεκτρονικό πορτοφόλι του χρήστη και να χρησιμοποιηθούν ως τυπική χρεωστική κάρτα είναι ένα άλλο χαρακτηριστικό στοιχείο του Cardano.

- **Hyperledger**: Υπό τη διαχείριση του ιδρύματος Linux, το Hyperledger είναι ένα πλαίσιο και ένα βοηθητικό πρόγραμμα ανοικτού κώδικα για την αφαίρεση της περιπλοκότητας της δημιουργίας αλυσίδων μπλοκ (συμπεριλαμβανομένων των blockchains με άδεια). Προσφέρει μια ευέλικτη δομή καθώς και μια σειρά εργαλείων για την εκτέλεση έξυπνων συμβάσεων σε κατανεμημένα λογιστικά βιβλία. Ο αλυσιδωτός κώδικας για το Hyperledger Fabric μπορεί να αναπτυχθεί σε ένα δίκτυο blockchain αφού έχουν καθοριστεί σε αυτό πολυάριθμες έξυπνες συμβάσεις. Αυτό σημαίνει ότι, ενώ ο αλυσιδωτός κώδικας χειρίζεται τις έξυπνες συμβάσεις που καθορίζονται εντός του, οι ίδιες οι έξυπνες συμβάσεις διαχειρίζονται τη συναλλακτική ή επιχειρηματική λογική.

Γίνεται σημαντική προσπάθεια για τη δημιουργία "έξυπνων πόλεων", οι οποίες θα χρησιμοποιούν την τεχνολογία ως υποδομή για την επίλυση πολλών από τα προβλήματα που αντιμετωπίζουν σήμερα οι πόλεις. Οι πόλεις αυτές θα χρησιμοποιούν πράσινη ενέργεια, ολοκληρωμένες μορφές μεταφορών, διαχείριση του νερού και της ρύπανσης, παγκόσμια ταυτοποίηση (ID), ασύρματα συστήματα διαδικτύου και προώθηση του τοπικού εμπορίου. Η πολυπλοκότητα της δημιουργίας και εκτέλεσης έξυπνων πόλεων, σύμφωνα με ορισμένους, μπορεί να αποδειχθεί η μεγαλύτερη πρόκληση του μέλλοντος και ο δρόμος προς τη γενική αποδοχή της τεχνολογίας blockchain [67].

Μπορούμε λοιπόν να συμπεράνουμε ότι τα έξυπνα συμβόλαια μπορούν να προσφέρουν αρκετά πλεονεκτήματα για το IoT, ειδικά όσον αφορά την αυτοματοποίηση της επικοινωνίας συσκευών. Ωστόσο, πρέπει να γίνουν αρκετά βήματα για να επιτευχθεί το επίπεδο ωριμότητας που απαιτείται για την αξιοποίηση αυτού του δυναμικού.

Εικόνα 8. Ethereum, Nem, Neo, Cardano και Hyperledger Blockchain

4.2.4 Μηχανισμοί Διαχείρισης Συσκευών και Πρωτοκόλλων

Με τη χρήση της τεχνολογίας blockchain, αναμένεται πλήρης αυτοματοποίηση των αλληλεπιδράσεων των συσκευών μέσω του δικτύου. Για πολλαπλές διαδραστικές συσκευές, ένα blockchain μπορεί να επιτρέψει την ανταλλαγή πληροφοριών χωρίς χρήστη μεταξύ διαφορετικών εισόδων, όπως ένας πομπός από ένα στοιχείο και ένας δέκτης από ένα άλλο. Για παράδειγμα, όταν ένα κοντέινερ επιβιβάζεται σε πλοίο, σε φορτηγό ή παραδίδεται στη διεύθυνση κατοικίας, η αλληλεπίδραση καταγράφεται αυτόματα στο blockchain και εξαλείφει το στοιχείο ανθρώπινου σφάλματος και την επιπλέον εργασία των αντικειμένων παρακολούθησης.

Η έρευνα προτείνει τη χρήση του blockchain ως μηχανισμού για τη δημιουργία και τη διαχείριση δικτύων IoT και των συσκευών που σχετίζονται με τα συστήματα συγχρονισμού και επικοινωνίας τους. Το Blockchain θα επιτρέψει τη διαχείριση των διαμορφώσεων των συσκευών και των σχετικών κλειδιών [66]-[71].

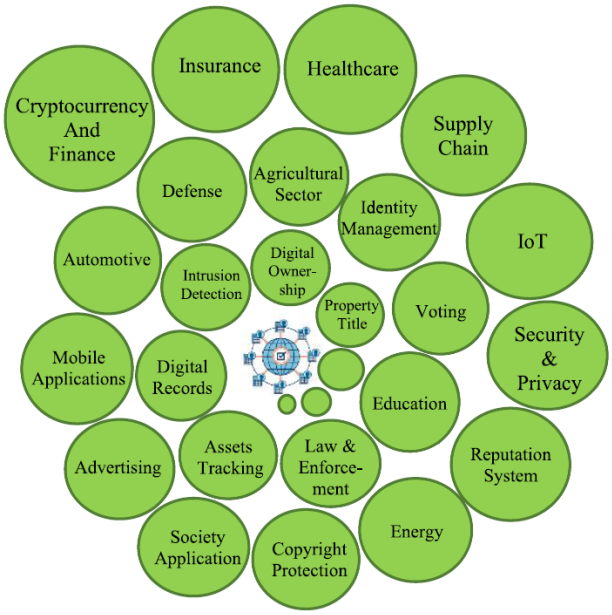
Ωστόσο, υπάρχει έλλειψη πραγματικών εφαρμογών ή ανάπτυξης επιχειρηματικών μοντέλων σχετικά με τη χρήση της διαχείρισης συσκευών και τις επιπτώσεις της, συγκεκριμένα το κόστος και τις απαιτήσεις συντήρησης της ενσωμάτωσης τέτοιων προηγμένων συσκευών επικοινωνίας σε διάφορες συσκευές.

4.2.5 Ασφάλεια Δικτύου

Η στροφή σε μια αποκεντρωμένη αρχιτεκτονική θα οδηγήσει σε ένα πιο βιώσιμο οικοσύστημα. Το τρέχον κεντρικό μοντέλο απαιτεί υπερβολικό κόστος συντήρησης, ειδικά για κάτι τόσο απλό όπως η διανομή μιας ενημέρωσης λογισμικού σε εκατομμύρια συσκευές, όχι μόνο μία φορά, αλλά σε συνεχόμενη βάση, ακόμα και αν δεν παράγονται πλέον.

Η βιβλιογραφία παρουσιάζει την ιδέα ενός πλαισίου ενημέρωσης στο οποίο ένα σύστημα που βασίζεται σε blockchain επιτρέπει χωρίς άδεια και κατανεμημένους ελέγχους την εγκυρότητα του τρέχοντος υλικολογισμικού που διατηρείται σε διάφορες συσκευές IoT. Παράλληλα ελέγχει την ακεραιότητα των εκδόσεων λογισμικού και επιτρέπει την αυτοματοποιημένη διαδικασία ενημέρωσης των κόμβων στο ίδιο το δίκτυο διεργασιών [63], [72], [73].

Λαμβάνοντας υπόψη τη νοημοσύνη και την επικοινωνία των οχημάτων, μπορεί να χρησιμοποιηθεί ένα παράδειγμα για να καταδειχθεί η εφαρμογή της ανωνυμίας χρησιμοποιώντας τις ιδιωτικές/δημόσιες λειτουργίες που βρίσκονται στα blockchains στους αλγόριθμους κατακερματισμού τους. Συγκεκριμένα, το blockchain θα χρησιμοποιεί ασύμμετρη κρυπτογραφία για τη δημιουργία δημόσιων και ιδιωτικών κλειδιών, τα οποία στη συνέχεια θα διανεμηθούν στα οχήματα, επιτρέποντάς τους να συναλλάσσονται μεταξύ τους μέσω του δημόσιου κλειδιού, διατηρώντας παράλληλα την ανωνυμία προστατεύοντας το ιδιωτικό κλειδί. Ως αποτέλεσμα, τα αυτοκίνητα θα μπορούν να ανταλλάσσουν δεδομένα απευθείας μεταξύ τους χρησιμοποιώντας υποδομές blockchain peer-to-peer (όπως αυτή που χρησιμοποιείται σήμερα για κρυπτονομίσματα αυτοκινήτων) για την ανταλλαγή πληροφοριών κίνησης και άλλων ευαίσθητων δεδομένων, διατηρώντας παράλληλα την ανωνυμία των ίδιων των οχημάτων , και μέσω επέκτασης του προγράμματος οδήγησης.



Εικόνα 9. Τομείς εφαρμογής Blockchain [127]

4.3 Blockchain και Ενέργεια

Ο ενεργειακός τομέας κατατάσσεται δεύτερος στη λίστα με τις εφαρμογές blockchain, με 17 από 151 άρθρα εφαρμογών (περίπου 11%). Υπάρχουν διάφορες κατηγορίες όσον αφορά τον τομέα της ενέργειας και εφαρμογές διαχείρισης ενέργειας βασισμένες σε blockchain, όπως

- Έλεγχος της αγοράς ηλεκτρικής ενέργειας μεταξύ μηχανών
- Διευκόλυνση του εμπορίου ενέργειας
- Αύξηση ασφάλειας των ενεργειακών δικτύων
- Βοήθεια στη διάχυση της πράσινης ενέργειας

4.3.1 Έλεγχος της Αγοράς Ηλεκτρικής Ενέργειας μεταξύ Μηχανών

Ο παραδοσιακός τρόπος χρήσης ηλεκτρικής ενέργειας μπορεί να μην ωφεληθεί πολύ από μια εφαρμογή blockchain, επειδή βασίζεται σε ένα πλαίσιο ενός προμηθευτή και όλων των πελατών. Ωστόσο, οι πρόσφατες εξελίξεις στην παραγωγή και κατανάλωση ενέργειας έχουν αρχίσει να αλλάζουν τα παραδοσιακά πρότυπα συνηθειών και αλληλεπιδράσεων με την αγορά. Συγκεκριμένα, η δυνατότητα χρήσης ανανεώσιμων πηγών ενέργειας, όπως η ηλιακή για την παραγωγή ηλεκτρικής ενέργειας στο σπίτι έχει ανοίξει το δρόμο για μια κατανεμημένη αγορά ενέργειας όπου οι πελάτες γίνονται προμηθευτές βάσει χρόνου και συνθηκών. Ως εκ τούτου, υπάρχει ανάγκη για μια πλατφόρμα που επιτρέπει την ασφαλή ανταλλαγή πληροφοριών παραγωγής και κατανάλωσης ενέργειας μεταξύ των μερών, βελτιστοποιώντας παράλληλα την ανθρώπινη συμμετοχή και διατηρώντας το απόρρητο.

Το blockchain θα μπορούσε να είναι μια λύση, καθώς προσφέρει τη δυνατότητα να ενεργοποιήσει ένα πλαίσιο για αλληλεπίδραση μηχανής με μηχανή και να δημιουργήσει μια αγορά ηλεκτρικής ενέργειας όπου οι καταναλωτές μπορούν να επιλέξουν από μια ποικιλία προμηθευτών και να επιλέξουν την κατάλληλη προσφορά αυτόνομα [50]. Ένα άλλο πρόβλημα που σχετίζεται με την εμπορία ενέργειας μεταξύ μηχανών είναι η φαινομενικά συνεχής απαίτηση πληρωμής μεταξύ κόμβων για ηλεκτρική ενέργεια που παρέχεται ή αποσύρεται. Οι μικροπληρωμές είναι συναλλαγές που πραγματοποιούνται με το μικρότερο πλασματικό ποσό νομίσματος που χρησιμοποιείται για την πληρωμή διαφόρων μικροαντικειμένων διαδοχικά. Η εισαγωγή μικροπληρωμών επιτρέπει την άμεση αλληλεπίδραση μεταξύ των μηχανών, καθώς ο έλεγχος ταυτότητας όλων των μερών είναι αυτοματοποιημένος και αποκεντρωμένος [15].

Ωστόσο, πρέπει να λάβουμε υπόψη την πολυπλοκότητα των παραμέτρων που εμπεριέχονται σε συναλλαγές που περιλαμβάνουν ενέργεια, όπως η απόσταση από πηγές ενέργειας και η γενική ανάγκη για γρήγορη και αποτελεσματική εναλλαγή μεταξύ πηγών ενέργειας για την αποφυγή διακοπής ρεύματος. Συνεπώς μπορεί να είναι δύσκολες υπό ορισμένους αλγόριθμους εκκαθάρισης blockchain, όπως η απόδειξη της εργασίας (proof of work).

4.3.2 Διευκόλυνση του Εμπορίου Ενέργειας

Ο μετασχηματισμός των αγορών ενέργειας που συζητήθηκε προηγουμένως ανοίγει την πόρτα σε διάφορες ανταλλαγές μεταξύ διαφορετικών ενδιαφερομένων στην ενεργειακή κοινότητα. Το blockchain έχει τη δυνατότητα να δημιουργήσει χώρο για τη δημιουργία τοπικών αγορών ηλεκτρικής ενέργειας, εκδημοκρατίζοντας την αγορά ενέργειας χρησιμοποιώντας διάφορους μηχανισμούς παραγωγής ενέργειας των χρηστών. Ωστόσο, υπάρχουν ορισμένα εμπόδια στο εμπόριο ενέργειας.

Τα ζητήματα προστασίας της ιδιωτικής ζωής στην κατανάλωση ενέργειας και η ανταλλαγή πληροφοριών στην αγορά είναι ένα άλλο ζήτημα για τα αποκεντρωμένα ενεργειακά δίκτυα, καθώς οι πληροφορίες για την παραγωγή και την κατανάλωση ενέργειας από διαφορετικά άτομα θα είναι δημόσιες. Οι λύσεις blockchain μπορούν να λύσουν αυτό το πρόβλημα δημιουργώντας μια ανταλλαγή πληροφοριών που δεν αποκαλύπτει την ταυτότητα των ατόμων που εμπλέκονται. Επιπλέον, η λύση θα επιτρέψει τη δημιουργία αυτοματοποιημένων μηχανισμών δημοπρασίας, γεγονός που θα απλοποιήσει την ανταλλαγή ενέργειας, θα ρυθμίσει τα επίπεδα ενέργειας αυξάνοντας παράλληλα την ασφάλεια [74]. Ταυτόχρονα, η εισαγωγή μηχανισμών επεξεργασίας πληρωμών στο blockchain θα διευκολύνει τις συναλλαγές μεταξύ των μικροδικτύων [15], [75].

Η εφαρμογή αυτών των μοντέλων θα πρέπει να λαμβάνει υπόψη τον σχετικό αντίκτυπο που μπορεί να έχουν τέτοιες αγορές στην ικανότητα της κυβέρνησης να προβλέπει και να ελέγχει τη ζήτηση και τις αγορές ενέργειας, επιτρέποντας κρατική παρέμβαση και ρυθμιστικούς μηχανισμούς.

4.3.3 Αύξηση Ασφάλειας των Ενεργειακών Δικτυών

Ανεξάρτητα από το μοντέλο που χρησιμοποιείται για την παράδοση και τη διαχείριση της παραγωγής της ηλεκτρικής ενέργειας, οι αγορές ενέργειας αντιμετωπίζουν συνεχείς απειλές για την ασφάλεια, που αποτελούν ένα σύγχρονο ψηφιακό δίλημμα. Η αυξημένη ψηφιοποίηση μπορεί να καταστήσει ευάλωτους τους παραγωγούς/εγκαταστάσεις ενέργειας, ενώ η έλλειψη ψηφιοποίησης μειώνει την αποδοτικότητα και την ποιότητα των υπηρεσιών.

Το Blockchain είναι μια πιθανή λύση στο δίλημμα της ψηφιοποίησης ενέργειας. Συγκεκριμένα, αποτελεί την εισαγωγή μιας προσέγγισης βασισμένης σε blockchain που χρησιμοποιεί έξυπνες συμβάσεις για τη διαχείριση της ανταλλαγής ενέργειας μεταξύ διαφόρων καταναλωτών/προμηθευτών, που θα επέτρεπε βιώσιμους και ολοένα και πιο ασφαλείς μηχανισμούς ανταλλαγής ενέργειας ενώ οδηγεί σε ένα πιο αποκεντρωμένο και ανθεκτικό πλέγμα [76]. Ταυτόχρονα, το πλαίσιο ανωνυμίας συναλλαγών εντός του blockchain θα επιτρέψει την αύξηση της ασφάλειας και της ιδιωτικής ζωής των μερών της συναλλαγής στο μικροδίκτυο [77], ενώ παράλληλα θα είναι σε θέση να προστατεύσει το ενεργειακό δίκτυο από επιθέσεις στον κυβερνοχώρο διαμορφώνοντας ένα πλαίσιο προστασίας βασισμένο στο κατανεμημένο καθολικό [78].

Ωστόσο, η έρευνα θα πρέπει να περιλαμβάνει την έλλειψη προσφυγής και το κόστος αυξημένης ασφάλειας σε περίπτωση λάθους ή απάτης, καθώς η ανωνυμία και το αμετάβλητο του καθολικού θα δυσκολέψει τις αρχές να επιδιώξουν ζητήματα. Επομένως, η έρευνα για την εφαρμογή blockchain θα πρέπει επίσης να ενσωματωθεί με το σκεπτικό του να κατανοήσουν και να γνωρίζουν τις πτυχές του πελάτη για κυβερνητικούς και επίσημους σκοπούς.

4.3.4 Βοήθεια στη Διάχυση της Πράσινης Ενέργειας

Καθώς το ενεργειακό σύστημα συνεχίζει να εξελίσσεται και οι μεμονωμένοι καταναλωτές αποκτούν μεγαλύτερη πρόσβαση σε ανανεώσιμες πηγές ενέργειας, η αγορά μπορεί να στραφεί σε ένα αποκεντρωμένο μοντέλο που περιλαμβάνει διάφορους μηχανισμούς παραγωγής και αποθήκευσης ενέργειας. Αυτό παρέχει μια ευκαιρία μείωσης των περιβαλλοντικών επιπτώσεων της παραγωγής και κατανάλωσης ενέργειας βελτιώνοντας τη συνολική απόδοση και μειώνοντας τα απόβλητα.

Η τεχνολογία Blockchain μπορεί να χρησιμοποιηθεί σε πλαίσια διαχείρισης ενέργειας. Η εισαγωγή πράσινων πιστοποιητικών μέσω μιας αλυσίδας μπλοκ που επιτρέπει την πιστοποίηση της πηγής παραγωγής ενέργειας (δηλαδή που παράγεται από ανανεώσιμες πηγές, απλώς αποθηκεύεται

συμβατικά παραγόμενη ενέργεια σε μπαταρίες ή άλλους μηχανισμούς αποθήκευσης) θα επιτρέψει στις κυβερνήσεις να σχεδιάζουν και να δημιουργούν κατάλληλα κίνητρα και οφέλη [79].

Η τρέχουσα μελέτη θα πρέπει επίσης να λάβει υπόψη την απαιτούμενη πολυπλοκότητα που απαιτείται για να δημιουργηθούν ανταλλαγές μεταξύ των αγορών για διάφορες πηγές ενέργειας.

Μπορούμε να εξετάσουμε το παράδειγμα της οικιακής παραγωγής και να το ανταλλάξουμε ενεργά στην αγορά ενέργειας για να προμηθεύουμε την περίσσεια ηλεκτρικής ενέργειας που παράγεται κατά τις ώρες αιχμής και να αναπληρώσουμε το έλλειμμα που προκαλείται λόγω της απρόβλεπτης φύσης των ανανεώσιμων πηγών ενέργειας. Ωστόσο, πολλά ζητήματα εμποδίζουν την ανάπτυξη ενός τέτοιου οικοσυστήματος, συμπεριλαμβανομένων των ανησυχιών των νοικοκυριών σχετικά με τη συντήρηση και τη συμμετοχή που απαιτείται για τη συμμετοχή στην ίδια αγορά με τους προμηθευτές και τους καταναλωτές. Η τεχνολογία Blockchain λύνει αυτό το πρόβλημα αποκεντρώνοντας την ανταλλαγή πληροφοριών μεταξύ των νοικοκυριών, εκχωρώντας δημόσια/ιδιωτικά κλειδιά σε κάθε νοικοκυριό και χρησιμοποιώντας έξυπνα συμβόλαια για τον καθορισμό συγκεκριμένων παραμέτρων κατανάλωσης και παροχής ενέργειας. Χρησιμοποιώντας έξυπνα συμβόλαια, τα νοικοκυριά μπορούν να ορίσουν προτιμήσεις σχετικά με τις τιμές προσφοράς και ζήτησης ενέργειας και να πραγματοποιούν συναλλαγές αυτόματα, οι οποίες θα προστατεύονται από την αποκέντρωση και το αμετάβλητο του blockchain. Έτσι οι ταυτότητες των νοικοκυριών θα παραμείνουν ιδιωτικές χάρη στη χρήση ασύμμετρης κρυπτογράφησης.

4.4 Blockchain και Οικονομία

Τα οικονομικά ήταν μια άλλη σημαντική κατηγορία που συγκεντρώθηκε από την ανασκόπηση της βιβλιογραφίας, με 11 (περίπου 7%) από 151 άρθρα που μελετούν την αλληλεπίδραση μεταξύ χρηματοδότησης και εφαρμογών blockchain:

- Καλύτερη επεξεργασία συναλλαγών
- Βιώσιμες τραπεζικές και χρηματοοικονομικές συναλλαγές
- Ενίσχυση της οικονομικής ασφάλειας
- Απόρρητο και αυτοματοποιημένα οικονομικά συμβόλαια

4.4.1 Καλύτερη Επεξεργασία Συναλλαγών

Ενώ τα τραπεζικά ιδρύματα βοηθούν τον κόσμο να προχωρήσει στο εμπόριο, η ταχεία επέκταση του συνολικού εμπορίου σε συνδυασμό με την ψηφιοποίηση των χρηματοπιστωτικών νομισμάτων συνεχίζει να ασκεί πίεση στους περιορισμούς του τρέχοντος συστήματος, όπου οι κεντρικές βάσεις δεδομένων διαθέτουν εξαιρετικά ευαίσθητες πληροφορίες και ακόμη και απλές συναλλαγές πληρωμής μπορεί να χρειαστούν μέρες για να διεκπεραιωθούν. Αυτό επιβραδύνει το εμπόριο και τις συναλλαγές και την εμποδίζει να αντικαταστήσει πλήρως τα παραδοσιακά fiat νομίσματα σχετικά με τις συναλλαγές [80].

Τα πλαίσια blockchain έχουν πολλά οφέλη όπως βελτιωμένη επεξεργασία συναλλαγών και απόδοση που σχετίζεται με τις τραπεζικές εργασίες. Συγκεκριμένα, το blockchain μπορεί να βοηθήσει την κυβέρνηση να δημιουργήσει μια ενιαία δομή λογαριασμού, να αυτοματοποιήσει την επεξεργασία και την εξισορρόπηση των λογαριασμών, μειώνοντας έτσι τα αδρανή ταμειακά υπόλοιπα, το περιττό κόστος δανεισμού και τη μείωση του κόστους της κεντρικής τράπεζας βελτιώνοντας τη ρευστότητα [81].

Τα συστήματα που βασίζονται στο blockchain μπορούν να δημιουργηθούν όχι μόνο ως συστατικά στοιχεία εντός των χρηματοπιστωτικών οργανισμών, αλλά και ως ανταγωνιστές, με μεγαλύτερη ενσωμάτωση και αποκέντρωση που οδηγούν σε βελτιωμένες λειτουργίες και ταχύτερη επεξεργασία των συναλλαγών [82].

Παρ' όλα αυτά, οι έρευνες θα πρέπει να λαμβάνουν υπόψη τα μειονεκτήματα που αντιμετωπίζουν το blockchain και άλλα καινοτόμα συστήματα όσον αφορά τη διάδοση και την υιοθέτηση σε σύγκριση με παλαιότερες προσεγγίσεις. Επιπλέον, σε έθνη όπου έχουν αναπτυχθεί τεχνολογίες όπως το pay pass, το Apple Pay, το Google Pay και άλλες, η ταχύτητα των συναλλαγών και η ικανότητα άμεσων συναλλαγών έχουν αυξηθεί σημαντικά. Αυτό υποδηλώνει ότι, ελλείψει αυξημένης ανωνυμίας και ασφάλειας, το πρωταρχικό όφελος της αλυσίδας μπλοκ για τους καταναλωτές θα είναι οι επιπτώσεις της στις διεθνείς μεταφορές και το εμπόριο.

4.4.2 Βιώσιμες Τραπεζικές και Χρηματοοικονομικές Συναλλαγές

Τα παραδοσιακά τραπεζικά συστήματα εξακολουθούν να αντιμετωπίζουν πρόβλημα βιωσιμότητας, παρά την ανάκαμψη της χρηματοπιστωτικής αγοράς από την κρίση του 2008. Η πτώχευση μιας τράπεζας έχει αρνητικές οικονομικές επιπτώσεις για τους πελάτες της, καθώς και αλυσιδωτές επιπτώσεις στον υπόλοιπο τομέα. Οι παγκόσμιες προεκτάσεις της χρηματοπιστωτικής κρίσης και ο επακόλουθος χαρακτηρισμός των περισσότερων χρηματοπιστωτικών ιδρυμάτων για να πτωχεύσουν έγιναν εφικτές λόγω αυτής της περίστασης.

Από τη σκοπιά της ανάπτυξης ενός βιώσιμου χρηματοπιστωτικού συστήματος στην παγκόσμια οικονομία, μπορεί κανείς να δει την όλη λειτουργία του Blockchain στο μέλλον των τραπεζικών και χρηματοπιστωτικών συναλλαγών. Ένα παγκοσμίως αποκεντρωμένο λογιστικό καθολικό θα είναι εφικτό με την αποκέντρωση της αποθήκευσης του πλούτου στους ανθρώπους που τον κατέχουν και την αποσύνδεση της αξίας του από την οικονομία (ή την οικονομική υγεία μιας συγκεκριμένης χώρας ή περιοχής), με αποτέλεσμα θεωρητικά πιο σταθερές αξίες χρηματοοικονομικού πλούτου και ένα πιο ανθεκτικό οικονομικό σύστημα [83].

Ωστόσο, οι μελέτες που εξετάζουν αυτή την πιθανή χρήση πρέπει να λαμβάνουν υπόψη τους τον τρόπο με τον οποίο θα επηρεάσει τα σημερινά επιχειρηματικά μοντέλα των χρηματοπιστωτικών διαμεσολαβητών καθώς και τον κλάδο των δανείων.

4.4.3 Ενίσχυση της Οικονομικής Ασφάλειας

Η έλλειψη ενοποιημένων συνόλων δεδομένων και πληροφοριών αποτελεί εγγενές ελάττωμα της τρέχουσας δομής δεδομένων του χρηματοπιστωτικού συστήματος. Οι τράπεζες υπόκεινται σε παραβιάσεις της ασφάλειας και κυβερνοεπιθέσεις. Ενώ αυτό μπορεί να είναι ενοχλητικό όταν πρόκειται για κοινωνικά και γενικά δημογραφικά δεδομένα, το πρόβλημα γίνεται πολύ πιο σοβαρό όταν πρόκειται για οικονομικά περιουσιακά στοιχεία και οικονομικές ταυτότητες. Ένα άλλο ζήτημα που εγείρεται από τη χρήση τρίτων χρηματοπιστωτικών ιδρυμάτων είναι η απώλεια της ανωνυμίας, με αυστηρές απαιτήσεις ταυτότητας και έλλειψη ευελιξίας στις χρηματοπιστωτικές συναλλαγές.

Δεδομένων των ιδιαίτερων χαρακτηριστικών και δυνατοτήτων της, η χρήση της τεχνολογίας blockchain έχει πολλά οφέλη από την άποψη της κυβερνοασφάλειας. Ειδικότερα, η αποκέντρωση των δεδομένων του λογιστικού βιβλίου θα καθιστούσε τα δεδομένα πιο ασφαλή και ανθεκτικά σε επιθέσεις κακόβουλων χρηστών, ενώ η αυξημένη ιδιωτικότητα και ανωνυμία που προκύπτει από τη

χρήση του ιδιωτικού/δημόσιου κλειδιού του blockchain επιτρέπει μεγαλύτερη ελευθερία και προστασία σε οικονομικές συναλλαγές όπως η κλοπή ταυτότητας [84].

Ωστόσο, οι μελέτες θα πρέπει επίσης να δώσουν προσοχή στους κινδύνους μιας τέτοιας ιδιωτικότητας και ανωνυμίας, δεδομένου ότι ο εντοπισμός του ιδιωτικού κλειδιού ενός χρήστη θα επέτρεπε στον επιτιθέμενο να κλέψει πληροφορίες και να διαπράξει απάτη χωρίς να λογοδοτήσει.

4.4.4 Απόρρητο και Αυτοματοποιημένα Οικονομικά Συμβόλαια

Η τεχνολογία blockchain καθιστά δυνατή την αυτοματοποίηση των χρηματοοικονομικών συμβάσεων, χρησιμοποιώντας το πρωτόκολλο για τη διευκόλυνση ταχύτερων και πιο αποδοτικών χρηματοοικονομικών διαδικασιών με δυνατότητα εξοικονόμησης 11 έως 12 δισεκατομμυρίων δολαρίων ετησίως. Αυτό οφείλεται στο γεγονός ότι τα συμβόλαια επιπέδου 3, τα οποία εκτελούν συγκεκριμένες ενέργειες, ενώ παράλληλα τις αυτοματοποιούν, μπορούν να υλοποιηθούν στο blockchain [85].

Σκεφτείτε ένα σενάριο όπου κάποιος προσπαθεί να στείλει χρήματα σε ένα φτωχό έθνος στο εξωτερικό. Το χρονικό διάστημα (συχνά μετριέται σε ημέρες) που απαιτείται για την ολοκλήρωση της μεταβίβασης είναι το πρώτο από τα πολλά προβλήματα που μπορεί να δυσχεράνουν τη συναλλαγή. Οι κίνδυνοι αστάθειας για τους παρόχους χρηματοπιστωτικών υπηρεσιών και τα χρηματοπιστωτικά ιδρύματα στον αναπτυσσόμενο κόσμο επιδεινώνουν την κατάσταση αυτή. Η αλυσίδα μπλοκ θα αποκεντρωθεί και θα κρυπτογραφήσει τη μετάδοση των πληροφοριών, ενώ θα επιτρέψει σε κάθε αποστολέα και παραλήπτη να έχει ένα δημόσιο και ένα ιδιωτικό κλειδί. Ως αποτέλεσμα, το άτομο θα μπορούσε να υποβάλει απευθείας την απαραίτητη πληρωμή και η συναλλαγή να διεκπεραιωθεί μέσα σε λίγα λεπτά αντί για ημέρες, διατηρώντας παράλληλα την ασφάλεια του περιουσιακού στοιχείου σε μια αποκεντρωμένη πλατφόρμα εκτός από τα τραπεζικά ιδρύματα.

4.4.5 Βιομηχανία Τυχερών Παιχνιδιών

Ένα από τα μεγαλύτερα ζητήματα που αντιμετωπίζει η επιχείρηση τυχερών παιχνιδιών στο σύνολό της είναι η εμπιστοσύνη. Ανησυχίες σχετικά με την ακεραιότητα των τυχαίων διαδικασιών που χρησιμοποιούνται (όπως στον υπολογισμό των πιθανοτήτων) και, φυσικά, την ασφάλεια των κεφαλαίων που εμπλέκονται στις συναλλαγές τυχερών παιχνιδιών υπάρχουν, ιδίως για τους παρόχους υπηρεσιών τυχερών παιχνιδιών σε απευθείας σύνδεση. Τα μοναδικά χαρακτηριστικά της τεχνολογίας blockchain μπορούν να αξιοποιηθούν για την ενημέρωση επαληθεύσιμων και διαφανών διαδικασιών παραγωγής ψευδοτυχαίων δεδομένων [86]. Οποιοσδήποτε θα μπορεί να παρακολουθεί αυτές τις διαδικασίες χωρίς τη βοήθεια μιας εξωτερικής υπηρεσίας διαχειριστή και μόνο εξετάζοντας τα δημόσια δεδομένα που έχουν καταγραφεί στο λογιστικό βιβλίο. Επιπλέον, χάρη στη συμπερίληψη έξυπνων συμβολαίων σε πολλά πρωτόκολλα που βασίζονται στο blockchain, οι παίκτες και οι διαχειριστές του διαδικτυακού τζόγου μπορούν να συνάπτουν διαφανείς, αλγοριθμικά ρυθμιζόμενες συμφωνίες που υποστηρίζουν την ιδέα των άμεσων πληρωμών με τη χρήση ψηφιακών νομισμάτων.

4.5 Blockchain και Κυβέρνηση

Η κυβέρνηση είναι ακόμα ένας δημοφιλής τομέας ακαδημαϊκού ενδιαφέροντος, αντιπροσωπεύοντας 10 (ή περίπου 6,5%) από τις 151 επιχειρηματικές εφαρμογές Blockchain. Το blockchain στην κυβέρνηση παρουσιάζει τα εξής οφέλη:

- Ηλεκτρονική διακυβέρνηση
- Πραγματοποίηση μιας ψηφιακής ταυτότητας
- Ηλεκτρονική ψηφοφορία
- Ενίσχυση του ελέγχου των συσκευών μέτρησης

4.5.1 Ηλεκτρονική Διακυβέρνηση

Ο όρος "ηλεκτρονική διακυβέρνηση" περιγράφει τον τρόπο με τον οποίο οι κυβερνητικοί αξιωματούχοι χρησιμοποιούν ψηφιακά εργαλεία και γενικότερα τεχνολογία για τη βελτίωση των συνολικών υπηρεσιών και παροχών, αυξάνοντας παράλληλα τη δέσμευση με τους ψηφοφόρους τους.

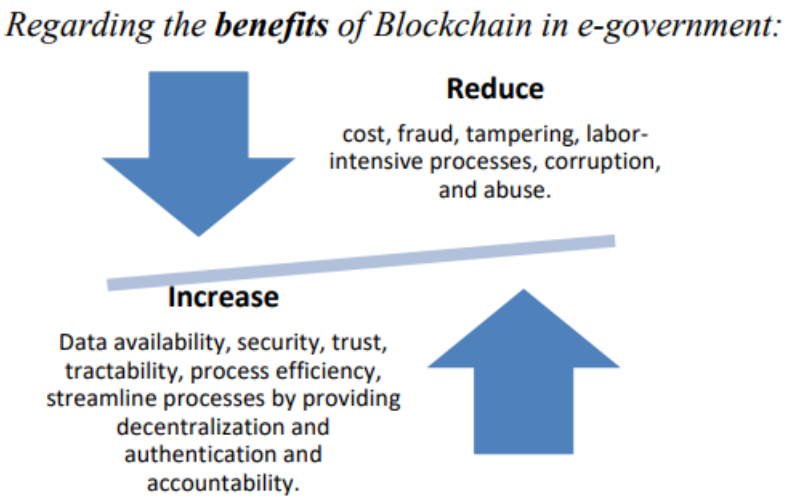
Η υιοθέτηση της τεχνολογίας blockchain από την κυβέρνηση έχει διάφορα οφέλη. Κατ' αρχάς, η συντήρηση και η διαχείριση της τεχνολογίας Blockchain είναι απλή λόγω της επεκτασιμότητάς της και του αποκεντρωμένου καθολικού [87],[88]. Επιπλέον, η εφαρμογή έξυπνων συμβάσεων θα επιτρέψει την αποτελεσματική ολοκλήρωση και εκτέλεση περίπλοκων κυβερνητικών γραφειοκρατικών δραστηριοτήτων. Αυτά τα οφέλη θα επέτρεπαν στις κυβερνήσεις να αυξήσουν την ποσότητα των παρεχόμενων υπηρεσιών, βελτιώνοντας παράλληλα τη γενική ποιότητα και τους χρόνους διεκπεραίωσης των υφιστάμενων υπηρεσιών.

Δεύτερον, η αποκέντρωση της βάσης δεδομένων Blockchain προωθεί μεγαλύτερο άνοιγμα και προσβασιμότητα μεταξύ της κυβέρνησης και των πολιτών που την απαρτίζουν. Με την ανωνυμοποίηση των δεδομένων, όλες οι κυβερνητικές συναλλαγές μπορούν να ελεγχθούν και να αναζητηθούν ανωμαλίες χωρίς να αποκαλυφθούν τα άμεσα εμπλεκόμενα μέρη, γεγονός που ενισχύει επίσης τις υπηρεσίες δικαιοσύνης συνολικά, συμβάλλοντας στην εξάλειψη της προκατάληψης [89].

Τρίτον, η αποκεντρωμένη φύση του λογιστικού καθολικού σημαίνει ότι οι πληροφορίες θα είναι πιο τυποποιημένες και προσβάσιμες σε περισσότερες περιοχές και μέρη από ό,τι πριν. Η κυβέρνηση θα είναι σε θέση να ανοίξει τις υπηρεσίες ανταλλαγής πληροφοριών σε όλους τους διάφορους οργανισμούς καθώς και στο κοινό, αξιοποιώντας έναν συνδυασμό ιδιωτικού/δημόσιου κλειδιού.

Τέλος, ο μη αναστρέψιμος χαρακτήρας του καθολικού και η ενσωμάτωση των χρηματοοικονομικών συναλλαγών επιτρέπουν στους χρήστες να δημιουργήσουν και να διατηρήσουν ένα αξιόπιστο και κοινόχρηστο χρηματοοικονομικό ιστορικό, το οποίο μπορεί να ενισχύσει τη συνολική αποτελεσματικότητα και αξιοπιστία του πιστωτικού συστήματος [90].

Για να προχωρήσει μια συναλλαγή, η έρευνα θα πρέπει, ωστόσο, να λάβει υπόψη τη σχετική σημασία των σημαντικών συναλλαγών και τον πιθανό κίνδυνο που συνδέεται με την κλοπή του ιδιωτικού κλειδιού ενός ατόμου.



Εικόνα 10. Πλεονεκτήματα και Μειονεκτήματα Blockchain στην Κυβέρνηση [129]

4.5.2 Πραγματοποίηση μιας Ψηφιακής Ταυτότητας

Η νομιμότητα των εγγράφων και τα κριτήρια επαλήθευσης της ταυτότητας του καθενός στα σημερινά κυβερνητικά συστήματα βασίζονται κυρίως σε έντυπες και συμβατικές μεθόδους. Η πλειονότητα των κρατών του κόσμου απαγορεύει τη χρήση ψηφιακών ταυτοτήτων για ευαίσθητες ή βασικές κυβερνητικές υπηρεσίες. Αυτό οφείλεται στο γεγονός ότι δεν έχουν υιοθετηθεί ευρέως τα πλαίσια και τα πρότυπα ψηφιακών ταυτοτήτων, τα οποία μπορούν να εγγυηθούν την προστασία της ιδιωτικής ζωής και την ασφάλεια, επιτρέποντας παράλληλα την ατομική ταυτοποίηση εντός μιας κοινωνίας.

Επιτρέποντας την ανάπτυξη μιας δημόσιας και ιδιωτικής ταυτότητας που θα επιτρέπει στο άτομο να επαληθεύει τον εαυτό του ανά πάσα στιγμή, ενώ παράλληλα θα επιτρέπει την ανταλλαγή δημόσιων πληροφοριών που θα παραμένουν ανώνυμες. Η τεχνολογία blockchain είναι κατάλληλη για την αντιμετώπιση αυτής της πρόκλησης. Τα αμετάβλητα και τα αποκεντρωμένα χαρακτηριστικά της διαχείρισής του εγγυώνται επίσης την ακρίβεια και τη γνησιότητα των πληροφοριών που κοινοποιούνται στις εξουσιοδοτημένες αρχές [17].

Παρ' όλα αυτά, η έρευνα σε αυτόν τον τομέα θα πρέπει να λάβει υπόψη τους σημαντικούς κινδύνους και τις επιπτώσεις της κλοπής ταυτότητας σε περίπτωση απώλειας ή απόκτησης του ιδιωτικού κλειδιού ενός ατόμου, επιτρέποντας σε παράνομες δραστηριότητες όπως η κλοπή ταυτότητας να παραμείνουν ανεξέλεγκτες.

4.5.3 Ηλεκτρονική Ψηφοφορία

Ο συγκεντρωτικός χαρακτήρας του συστήματος σημαίνει ότι υπάρχει ένας μόνο προμηθευτής που έχει τη δυνατότητα να ελέγχει και να χειρίζεται τα δεδομένα ανάλογα με τις ανάγκες. Γεγονός που μπορεί να θέσει σε κίνδυνο τα θεμέλια της δημοκρατίας μιας χώρας, καθώς η κυβέρνηση προσπαθεί να μεταβεί από τα παραδοσιακά συστήματα ψηφοφορίας που βασίζονται σε χάρτινα ψηφοδέλτια και υπογραφές σε μια πιο σύγχρονη και ψηφιακή λύση [91].

Με τη φύση του ανοιχτού κώδικα και το αποκεντρωμένο λογιστικό του καθολικού, το blockchain μπορεί να προσφέρει τη λύση, επιτρέποντας στις κυβερνήσεις να μειώσουν τον κίνδυνο αλλοίωσης των δεδομένων και να αποκρούσουν τις απειλές ασφαλείας από άλλες χώρες. Διατηρώντας πλήρη

ανωνυμία, η ικανότητα του Blockchain να παρέχει επαρκή έλεγχο ταυτότητας το καθιστά κατάλληλο για τους στόχους και τις εφαρμογές των μεθόδων ψηφοφορίας.

Παρ' όλα αυτά, δεδομένης της φύσης του εκλογικού κύκλου στο πλαίσιο του πρωτοκόλλου proof of work (PoW), η έρευνα θα πρέπει να λάβει υπόψη τις υπολογιστικές απαιτήσεις ενός τέτοιου συστήματος. Ένας άλλος παράγοντας που πρέπει να ληφθεί υπόψη είναι ο κίνδυνος κλοπής ταυτότητας που προκαλείται από την αποκάλυψη του ιδιωτικού κλειδιού του χρήστη.

4.5.4 Ενίσχυση του Ελέγχου των Συσκευών Μέτρησης

Η αύξηση της υιοθέτησης τυποποιημένων οργάνων μέτρησης σε διάφορες χώρες, και ιδίως στον αναπτυσσόμενο κόσμο, παρουσιάζει ορισμένες προκλήσεις λόγω της πολυπλοκότητας των νέων οργάνων. Καθώς η επιστήμη έχει εξελιχθεί, έχουν εξελιχθεί και τα όργανα μέτρησης που απαιτούνται για τον προσδιορισμό και την ποσοτικοποίηση των διαφόρων μεταβλητών που απαιτούνται για την επιστημονική έρευνα. Οι δυσκολίες σχετίζονται κυρίως με τον όγκο των δεδομένων που μετρούνται και τις απειλές ασφάλειας που συνδέονται με την αλλαγή και τη χειραγώγηση των δεδομένων.

Οι πόροι που απαιτούνται για τον υπολογισμό των μέτρων και την ποσοτικοποίηση του αυξανόμενου όγκου πληροφοριών που συλλέγονται, έχουν αποδειχθεί απαγορευτικοί για ορισμένες κυβερνήσεις και υποανάπτυκτα έθνη. Το blockchain χρησιμοποιεί κατανεμημένους υπολογισμούς και μετρήσεις για να λύσει αυτό το ζήτημα. Μπορεί να βοηθήσει τις κυβερνήσεις να ξεπεράσουν τους περιορισμούς και τις προκλήσεις των αυξανόμενων αναγκών σε πόρους, επιτρέποντας την αποκέντρωση των υπολογισμών μετρήσεων και τη διάδοσή τους σε ολόκληρο τον κόσμο, διατηρώντας παράλληλα την εμπιστευτικότητα και την ακεραιότητα των δεδομένων. Επιπλέον, η αποκέντρωση των δεδομένων θα καταστήσει την ασφάλεια και τις παραβιάσεις τους πολύ πιο δύσκολες. Ωστόσο το αμετάβλητο του καθολικού θα εγγυηθεί ότι η συνέπεια, η ορθότητα και η ακεραιότητα των δεδομένων διατηρούνται [92], [93].

Οι μελέτες θα πρέπει να λαμβάνουν υπόψη τις προκλήσεις που περιβάλλουν τις διαφοροποιήσεις στα παγκόσμια πρότυπα για τη μέτρηση των αξιών και τον τρόπο με τον οποίο επηρεάζουν τη βιωσιμότητα και την αποδοχή των συστημάτων αυτών από το κοινό.

Μπορούμε να χρησιμοποιήσουμε ένα παράδειγμα για να δείξουμε πώς μπορεί να εφαρμοστεί μια πραγματική ψηφιακή ταυτότητα βασισμένη στο blockchain. Σήμερα, ένας πελάτης που αγοράζει ένα αλκοολούχο ποτό σε ένα μπαρ πρέπει να επιδεικνύει μια μορφή προσωπικής ταυτότητας κατόπιν αιτήματος, προκειμένου να συμμορφώνεται με τις ισχύουσες κανονιστικές απαιτήσεις. Παρ' όλα αυτά, εκτός από την παροχή των απαιτούμενων πληροφοριών, όπως η ηλικία, ο πελάτης δίνει επίσης μια τεράστια ποσότητα προσωπικών πληροφοριών, συμπεριλαμβανομένης της ακριβούς ημερομηνίας γέννησής του, της διεύθυνσης και μιας σειράς άλλων λεπτομερειών. Στους χρήστες θα παρέχεται πάντα ένα ιδιωτικό/δημόσιο κλειδί που μπορεί να χρησιμοποιηθεί και να επικυρωθεί λόγω της αποκεντρωμένης φύσης των δεδομένων με τη χρήση της ασύμμετρης κρυπτογράφησης του blockchain. Στην περίπτωση του προστάτη, η ψηφιακή ταυτοποίηση θα επέτρεπε στο άτομο να παρέχει μόνο τις απαραίτητες πληροφορίες, όπως η ηλικία, διατηρώντας παράλληλα την ταυτότητά του.

4.6 Blockchain και Υγειονομική Περίθαλψη

Η ταχεία εξάπλωση της ψηφιοποίησης στην υγειονομική περίθαλψη είχε ως αποτέλεσμα τη δημιουργία μεγάλου αριθμού ηλεκτρονικών αρχείων για τους ασθενείς. Αυτή η ανάπτυξη θέτει άνευ προηγουμένου απαιτήσεις για την προστασία των ιατρικών δεδομένων που χρησιμοποιούνται και ανταλλάσσονται. Η άνοδος της τεχνολογίας blockchain ως υπεύθυνου και διαφανούς μηχανισμού αποθήκευσης και διαμοιρασμού δεδομένων ανοίγει νέους δρόμους για την αντιμετώπιση σοβαρών ανησυχιών που αφορούν το απόρρητο, την ασφάλεια και την ακεραιότητα των δεδομένων στην υγειονομική περίθαλψη. Η τεχνολογία Blockchain προσελκύει μεγάλη προσοχή. Τα τελευταία χρόνια έχει προσελκύσει την προσοχή της βιομηχανίας και του ακαδημαϊκού κόσμου. Στην πραγματικότητα, νέες εφαρμογές blockchain εμφανίζονται καθημερινά. Η τεχνολογία Blockchain θεωρείται τεχνολογία κατανεμημένου καθολικού για συναλλαγές ψηφιακών δεδομένων σε δίκτυο peer-to-peer (P2P), το οποίο μπορεί να διανεμηθεί δημόσια ή ιδιωτικά σε όλους τους χρήστες, επιτρέποντας την αποθήκευση οποιουδήποτε τύπου δεδομένων με αξιόπιστο και επαληθεύσιμο τρόπο.

Μια άλλη σημαντική έννοια του blockchain είναι ένα έξυπνο συμβόλαιο, μια νομικά δεσμευτική πολιτική που αποτελείται από ένα προσαρμόσιμο σύνολο κανόνων βάσει των οποίων τα μέρη συμφωνούν να αλληλεπιδρούν μεταξύ τους με αποκεντρωμένο, αυτοματοποιημένο τρόπο. Η τεχνολογία έχει ήδη δημιουργήσει πολλές εφαρμογές έξυπνων συμβάσεων σε τομείς τόσο διαφορετικούς όπως η ενέργεια, οι χρηματοοικονομικές υπηρεσίες, η ψηφοφορία και η υγειονομική περίθαλψη. Η τεχνολογία Blockchain παρέχει διαφάνεια και καταργεί την ανάγκη για τρίτους διαχειριστές ή μεσάζοντες. Χρησιμοποιεί μηχανισμούς συναίνεσης και κρυπτογραφία για την επαλήθευση της νομιμότητας των συναλλαγών σε ένα αναξιόπιστο περιβάλλον. Στο δίκτυο συναλλαγών P2P με κατανεμημένη αλυσίδα μπλοκ, ο κόμβος λήψης ελέγχει το μήνυμα, εάν το μήνυμα είναι σωστό, αποθηκεύεται σε ένα μπλοκ.

Στη συνέχεια χρησιμοποιείται ένας αλγόριθμος συναίνεσης για την επιβεβαίωση των δεδομένων σε κάθε μπλοκ, το Proof-of-work (PoW). Αφού εκτελεστεί ο αλγόριθμος συναίνεσης, το μπλοκ θα προστεθεί στην αλυσίδα και κάθε κόμβος στο δίκτυο αναγνωρίζει το μπλοκ και συνεχίζει να διαδίδει την αλυσίδα. Μία από τις πιο σημαντικές εφαρμογές της τεχνολογίας blockchain είναι η υγειονομική περίθαλψη. Η δυνατότητα του blockchain στην υγειονομική περίθαλψη έγκειται στην υπέρβαση προκλήσεων που σχετίζονται με την ασφάλεια των δεδομένων, το απόρρητο, την κοινή χρήση και την αποθήκευση.

Μία από τις απαιτήσεις του κλάδου της υγειονομικής περίθαλψης είναι η διαλειτουργικότητα. Είναι η ικανότητα δύο μερών, ανθρώπου ή μηχανής, να ανταλλάσσουν δεδομένα ή πληροφορίες με ακρίβεια, αποτελεσματικότητα και συνέπεια. Ο στόχος της διαλειτουργικότητας στην υγειονομική περίθαλψη είναι να διευκολύνει την ανταλλαγή πληροφοριών που σχετίζονται με την υγεία, όπως ηλεκτρονικά αρχεία υγείας (EHRs), μεταξύ παρόχων υγειονομικής περίθαλψης και ασθενών, έτσι ώστε τα δεδομένα να μπορούν να μοιράζονται σε όλο το περιβάλλον και να διανέμονται από διαφορετικά νοσοκομειακά συστήματα.

Επιπλέον, η διαλειτουργικότητα επιτρέπει στους παρόχους να μοιράζονται με ασφάλεια ιατρικά αρχεία ασθενών (με την άδεια του ασθενούς) ανεξάρτητα από την τοποθεσία του παρόχου και τη σχέση εμπιστοσύνης μεταξύ τους. Αυτό είναι ιδιαίτερα σημαντικό δεδομένης της ποικιλίας των πηγών για δεδομένα υγειονομικής περίθαλψης. Αυτή η πτυχή της διαλειτουργικότητας αντιμετωπίζεται μέσω της χρήσης της τεχνολογίας blockchain, η οποία έχει δείξει τη δυνατότητα να αποθηκεύει, να διαχειρίζεται και να μοιράζεται με ασφάλεια τα EHRs στην κοινότητα της υγειονομικής περίθαλψης. Επιπλέον, το αυξανόμενο κόστος των υποδομών υγειονομικής περίθαλψης και του λογισμικού για τον κλάδο ασκεί τεράστια πίεση στις οικονομίες του κόσμου. Στον

τομέα της υγειονομικής περίθαλψης, η τεχνολογία blockchain επηρεάζει θετικά τα αποτελέσματά της για εταιρείες και ενδιαφερόμενους φορείς για τη βελτιστοποίηση των επιχειρηματικών διαδικασιών, τη βελτίωση των αποτελεσμάτων των ασθενών, τη διαχείριση δεδομένων ασθενών, τη βελτίωση της συμμόρφωσης, τη μείωση του κόστους και την καλύτερη διαχείριση δεδομένων που σχετίζονται με αυτήν. Εξίσου σημαντική είναι η ικανότητα της τεχνολογίας blockchain να επηρεάζει τη ροή φαρμάκων και ιατρικού εξοπλισμού στη μακρά και πολύπλοκη αλυσίδα εφοδιασμού της υγειονομικής περίθαλψης. Το blockchain για τις εφοδιαστικές αλυσίδες υγειονομικής περίθαλψης υπόσχεται να εξαλείψει τον κίνδυνο πλαστών φαρμάκων που απειλούν να βλάψουν τους ασθενείς παγκοσμίως.

Η τεχνολογία Blockchain διερευνάται επί του παρόντος σε διάφορες εφαρμογές υγειονομικής περίθαλψης, όπως η διαχείριση δεδομένων, η αποθήκευση, η συνδεσιμότητα συσκευών και η ασφάλεια στο Internet of Medical Things (IoMT). Τα περισσότερα από τα οφέλη που προσφέρει η τεχνολογία blockchain στους προαναφερθέντες τομείς εφαρμογών έχουν θετικό αντίκτυπο στην ποιότητα της εμπειρίας (QoE) για τους περισσότερους ενδιαφερόμενους και τελικούς χρήστες, συμπεριλαμβανομένων ασθενών, φροντιστών, ερευνητών, φαρμακευτικών εταιρειών και ασφαλιστικών εταιρειών. Η δυνατότητα κοινής χρήσης δεδομένων υγειονομικής περίθαλψης χωρίς να διακυβεύεται το απόρρητο των χρηστών και οι κίνδυνοι για την ασφάλεια των δεδομένων είναι ένα σημαντικό βήμα για να γίνουν τα συστήματα εξυπνότερα, να βελτιωθεί η ποιότητα των υπηρεσιών της καθώς και η εμπειρία του χρήστη.

4.6.1 Blockchains στα Ηλεκτρονικά Αρχεία Υγείας

Οι επαγγελματίες του ιατρικού τομέα, τα νοσοκομεία και ο εξοπλισμός υγειονομικής περίθαλψης έχουν συμβάλει στην ανάγκη για σημαντική αύξηση της ψηφιοποίησης των ιατρικών αρχείων τα τελευταία δέκα χρόνια, επειδή διευκολύνει την πρόσβαση στα δεδομένα, την κοινή χρήση και τη χρήση τους ως βάση για την αποτελεσματικότερη και αποδοτικότερη λήψη αποφάσεων. Επί του παρόντος, τα μηχανογραφημένα ιατρικά δεδομένα είναι το σημείο όπου η τεχνολογία blockchain χρησιμοποιείται συχνότερα στην υγειονομική περίθαλψη.

Τα ηλεκτρονικά αρχεία υγείας (EHR) δεν σχεδιάστηκαν για να διαχειρίζονται αρχεία δια βίου σε πολλαπλά ιδρύματα, και καθώς οι συνθήκες ζωής μετακινούν τους ασθενείς από τα δεδομένα ενός παρόχου σε έναν άλλο, διασκορπίζουν τα δεδομένα τους σε διάφορα ιδρύματα, χάνοντας την απλή πρόσβαση σε ιστορικά δεδομένα [85], [94], [95]. Πολλοί ακαδημαϊκοί έχουν προτείνει τη χρήση της τεχνολογίας blockchain για τη διατήρηση των EHR ως αποτέλεσμα της επείγουσας ανάγκης για μια εφευρετική λύση για τον χειρισμό των EHR με τρόπο που να παρακινεί τους ασθενείς να αλληλοεπιδρούν με τα πρόσφατα και ιστορικά δεδομένα υγειονομικής περίθαλψης.

Ένα πρωτότυπο "MedRec" κάνει χρήση ειδικών χαρακτηριστικών blockchain για τη διαχείριση της ανταλλαγής δεδομένων, του απορρήτου και της πιστοποίησης ταυτότητας. Χρησιμοποιεί ένα αποκεντρωμένο σύστημα διαχείρισης αρχείων, υπόσχεται να δώσει στους ασθενείς ένα ενδελεχές, αμετάβλητο ιστορικό και επιτρέπει την απλή πρόσβαση στα ατομικά ιατρικά τους δεδομένα σε πολυάριθμους παρόχους και εγκαταστάσεις θεραπείας [96].

Το "MedRec" δεν διατηρεί ιατρικά δεδομένα σε αρχείο ούτε απαιτεί περίοδο αναμονής. Ειδοποιεί τον ασθενή, ο οποίος θα αποφασίσει τελικά πού μπορεί να πάει ο φάκελος, και αποθηκεύει μια σφραγίδα του φακέλου σε μια αλυσίδα μπλοκ (blockchain). Η σφραγίδα διασφαλίζει ότι αγοράστηκε ένα τέλειο αντίγραφο του δίσκου. Επιπλέον, μεταφέρει τον έλεγχο από τον οργανισμό στον ασθενή, γεγονός που δίνει στον ασθενή μεγαλύτερο βάρος και εξουσία να αναλάβει τον ρόλο του ιδιοκτήτη.

Οι ενώσεις διαχείρισης προορίζονται να ενεργούν ως εκπρόσωποι των ασθενών για εκείνους τους ασθενείς που θα προτιμούσαν να μην χειρίζονται τις πληροφορίες τους με αυτό το έργο. Η πλειονότητα των ατομικών καταχωρίσεων ασθενών που χρησιμοποιούν οι άνθρωποι σήμερα έχουν περίπλοκα σχέδια, προσθέτουν στο φόρτο εργασίας και έχουν διαφορετικές διεπαφές χρήστη για κάθε ίδρυμα. Ένα UI αποτελεί επίσης μέρος του πλαισίου MedRec, το οποίο βοηθά στη διατήρηση των συνδέσεων με τα ιατρικά δεδομένα καθώς αυτά ταξιδεύουν μεταξύ διαφορετικών ομάδων.

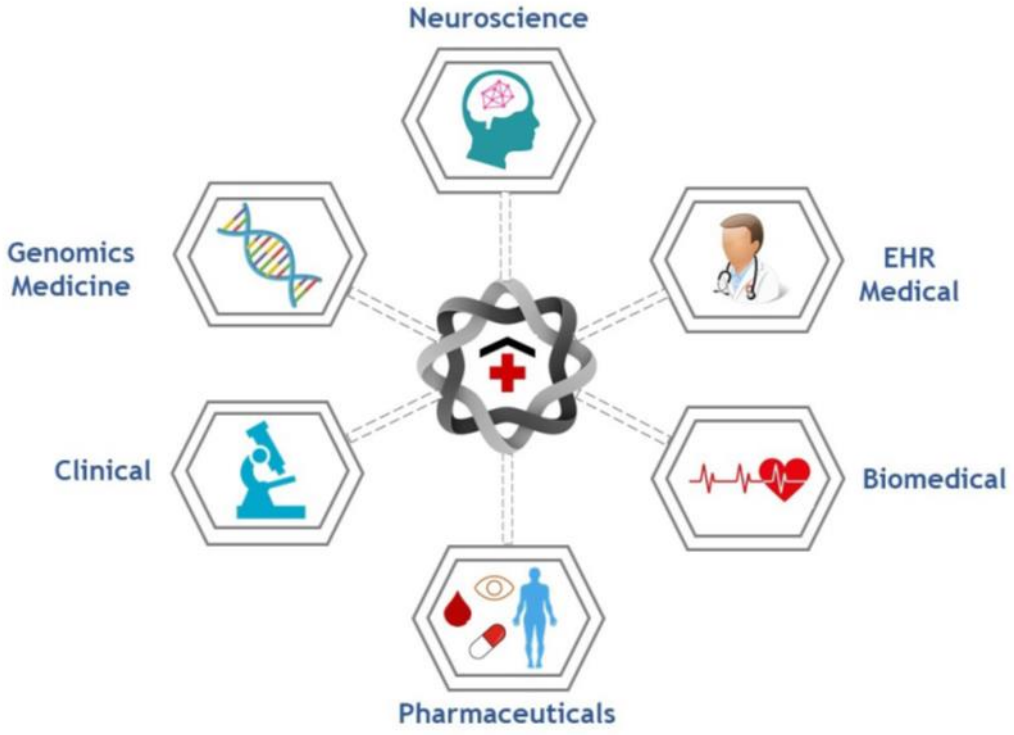
Η κοινή χρήση ιατρικών δεδομένων συναντά συχνά σοβαρά εμπόδια κατά την υιοθέτηση των EHR, συμπεριλαμβανομένης της απώλειας της διαχείρισης των δεδομένων, της προέλευσης, της παρακολούθησης και της προστατευμένης παρακολούθησής τους. Με αυτούς τους περιορισμούς κατά νου παρουσιάστηκε το MeDShare [97], ένα ασφαλές σύστημα blockchain για την ανταλλαγή ιατρικών δεδομένων μεταξύ άγνωστων μερών. Το MeDShare θα μπορούσε να χρησιμοποιηθεί για την τήρηση ηλεκτρονικών φακέλων υγείας και την ανταλλαγή ιατρικών δεδομένων μεταξύ παρόχων υπηρεσιών cloud, νοσοκομείων και ερευνητικών οργανισμών υγειονομικής περίθαλψης με μικρότερο κίνδυνο για την ασφάλεια και το απόρρητο των πληροφοριών.

Για την ακριβή διάγνωση και θεραπεία, οι γιατροί, οι ακτινολόγοι, και γενικότερα οι εργαζόμενοι στον τομέα της υγειονομικής περίθαλψης, τα φαρμακεία και οι ερευνητές ανταλλάσσουν συχνά άκρως εμπιστευτικά και σημαντικά δεδομένα ασθενών που βρίσκονται στα EHRs. Η φροντίδα του ασθενούς μπορεί να τεθεί σε κίνδυνο κατά την αποθήκευση, τη μετάδοση και τη διανομή αυτών των εξαιρετικά εμπιστευτικών πληροφοριών τους μεταξύ διαφόρων οργανισμών, γεγονός που μπορεί να θέσει σε σοβαρούς κινδύνους την υγεία του ασθενούς και τη διατήρηση του πιο πρόσφατου ιστορικού του. Λόγω του μακρόχρονου παρελθόντος των διαδικασιών προ- και μεταθεραπείας, παρακολούθησης και αποκατάστασης, η συχνότητα αυτών των κινδύνων μπορεί να γίνει μεγαλύτερη σε ασθενείς που μάχονται με χρόνιες ασθένειες (όπως ο καρκίνος και ο HIV). Προκειμένου να διασφαλιστεί η αποτελεσματική θεραπεία, η τήρηση ενημερωμένων πληροφοριών για τον ασθενή έχει καταστεί απολύτως απαραίτητη. Προτάθηκε λοιπόν ένα σύστημα βασισμένο στην αλυσίδα μπλοκ για τον έλεγχο, τη διατήρηση και την κοινή χρήση των ψηφιοποιημένων ιατρικών δεδομένων των ασθενών με καρκίνο, προκειμένου να παρακαμφθούν αυτοί οι περιορισμοί [98]. Για τον χειρισμό, την πρόσβαση και τη διατήρηση προστατευμένων δεδομένων ασθενών, εφάρμοσαν ένα σύστημα blockchain με άδεια. Για την απόκτηση και τον έλεγχο της ασφάλειας και της προστασίας των δεδομένων και των αρχείων ασθενών σε κλινικές, μπορούν να χρησιμοποιηθούν τέτοια προτεινόμενα μοντέλα για την αποτελεσματική εφαρμογή της τεχνολογίας blockchain.

Η πρωτοβουλία για τον ιατρικό φάκελο της Εσθονίας που βασίζεται στην αλυσίδα μπλοκ είναι ένα ακόμη ιστορικό ορόσημο. Όταν πρότεινε την ιδέα να διατηρηθούν εκατομμύρια ιατρικά δεδομένα ιδιωτικά και ταυτόχρονα να καταστούν ευρέως προσβάσιμα στους ιατρούς και τις ασφαλιστικές εταιρείες, η Εσθονία αναδείχθηκε ως παγκόσμιος πρωτοπόρος στην τεχνολογία blockchain το 2016 [99].

Η ισχυρή εγγύηση που παρέχεται στους ασθενείς ότι η χρήση αυτής της τεχνολογίας θα καταστήσει τα δεδομένα υγειονομικής περίθαλψης αμετάβλητα, ίσως αποτελεί την κινητήρια δύναμη πίσω από την παγκόσμια ανάπτυξη της τεχνολογίας blockchain στην ιατρική. Οποιαδήποτε προσπάθεια εισόδου ή τροποποίησης μπορεί να εντοπιστεί γρήγορα και να επισημανθεί σε όλη την αλυσίδα μπλοκ. Αυτό είναι χρήσιμο όχι μόνο για τη δεοντολογία των ασθενών αλλά και για τον εντοπισμό οποιασδήποτε παράνομης δραστηριότητας, όπως η εκτεταμένη απάτη ή η παραποίηση αρχείων. Επιπλέον, η ανταλλαγή και η αναθεώρηση αρχείων για εγκεκριμένες ιατρικές υπηρεσίες θα είναι πολύ πιο εύκολη. Όταν ένας ασθενής επισκέπτεται, η πλειονότητα των προμηθευτών του εν λόγω ασθενούς το παρατηρεί συνήθως αμέσως. Τα φαρμακευτικά σφάλματα, οι υπερευαισθησίες και οι φαρμακευτικές λύσεις μπορούν να φιλοξενηθούν πάνω σε όλα τα αρχεία blockchain εύλογα γρήγορα

με τη βοήθεια αλγορίθμων που φροντίζουν τους ασθενείς, χωρίς την ανάγκη για χρονοβόρες φαρμακευτικές φόρμες συμβιβασμού. Κατά συνέπεια, η χρήση της τεχνολογίας blockchain θα προωθήσει την καλύτερη πρόσβαση στην περίθαλψη, τη διαχείριση των ιατρικών αρχείων [12], τη γρήγορη επικύρωση των κλινικών πληροφοριών, την αυξημένη ασφάλεια και τον αποτελεσματικότερο σχεδιασμό της περίθαλψης.



Εικόνα 11. Εφαρμογές Blockchain στην Υγειονομική Περίθαλψη [124]

4.6.2 Απόκτηση και Αποθήκευση Δεδομένων στον Κλάδο της Ιατρικής

Οι τεχνολογίες παρακολούθησης της υγειονομικής περίθαλψης, συμπεριλαμβανομένων των φορητών συσκευών, δημιουργούν τεράστιες ποσότητες προσωπικών δεδομένων υγείας. Η σωστή διαχείριση και η ασφαλής ανάκτηση αυτών των δεδομένων είναι κρίσιμης σημασίας για τη λήψη αποφάσεων όσων αφορά τις βάσεις δεδομένων στο σύστημα υγείας μας. Το υπάρχον σύστημα υγειονομικής περίθαλψης μας παράγει επίσης δεδομένα μέσω των συνήθων δραστηριοτήτων διεξαγωγής επιχειρήσεων και παροχής υπηρεσιών. Οι ασθενείς αλληλεπιδρούν με πολλούς παρόχους υγειονομικής περίθαλψης καθ' όλη τη διάρκεια της ζωής τους, αφήνοντας τα δεδομένα κατακερματισμένα στα συστήματα των παρόχων. Οι πάροχοι διατηρούν συχνά τα δικαιώματα διαχείρισης πρωτογενών δεδομένων, δημιουργώντας κατακερματισμένες διαδρομές δεδομένων και μειώνοντας την ευκολία πρόσβασης των ασθενών. Τα δεδομένα υγειονομικής περίθαλψης χαρακτηρίζονται από όγκο, ετερογένεια και ταχύτητα. Είναι ανομοιόμορφα, έχουν πολλές μεταβλητές και απαιτούν ανάλυση δεδομένων σε πραγματικό χρόνο. Πολλά από αυτά τα δεδομένα είναι απρόσιτα, δεν είναι τυποποιημένα σε όλα τα συστήματα και είναι δύσκολο να κατανοηθούν, να χρησιμοποιηθούν και να μοιραστούν.

Παρακάτω φαίνεται η τρέχουσα κατάσταση της τήρησης ιατρικών αρχείων και του ιατρικού ιστορικού.

- Βασίζεται στην αλληλεπίδραση ασθενούς με γιατρό
- Αποτυγχάνει πάντα να χρησιμοποιήσει τα δεδομένα
- Δημιουργεί μια μακρά και κουραστική διαδικασία για τη φροντίδα υγείας
- Σημαντικές πληροφορίες ασθενών είναι διάσπαρτες στα συστήματα
- Δεν διαθέτει διαθεσιμότητα βασικών δεδομένων, επομένως, πολλά συστήματα υγείας δεν παρέχουν τα απαραίτητα για την θεραπεία ασθενών
- Επηρεάζει αρνητικά το σύστημα διαχείρισης, μιας και οι συσκευές αναπαραγωγής δεν είναι εξοπλισμένες με τις σωστές πληροφορίες για μια ομαλή διαδικασία
- Προσφέρει κακή ασφάλεια δεδομένων υγειονομικής περίθαλψης και αξιοπιστία

Ο κλάδος της υγειονομικής περίθαλψης είναι πολύ αναποτελεσματικός, όπου τα περισσότερα ιατρικά αρχεία εξακολουθούν να αποθηκεύονται σε χαρτί και σε αποκεντρωμένες τοποθεσίες. Δεν μπορούν να χρησιμοποιηθούν για τον συντονισμό της φροντίδας, τη μέτρηση της ποιότητας ή τη μείωση των ιατρικών λαθών. Τα δεδομένα υγειονομικής περίθαλψης συλλέγονται ψηφιακά σε διάφορα σημεία. Είναι σημαντικό να εξαχθεί το μέγιστο όφελος από αυτά τα δεδομένα χωρίς να περιπλέκεται η διαδικασία. Μια βασική πρόκληση που αντιμετωπίζει ο κλάδος της υγειονομικής περίθαλψης είναι η δυνατότητα εύκολης και οικονομικής καταγραφής και αποθήκευσης πληροφοριών και η ασφαλής κοινή χρήση τους σε διαφορετικές εφαρμογές και συστήματα. Η φορητότητα και η ομοιόμορφη συμβατότητα των δεδομένων κατά την εργασία σε διαφορετικά συστήματα είναι επίσης σημαντική.

4.6.3 Λύσεις Blockchain για Τήρηση Ιατρικών Αρχείων

Η τεχνολογία Blockchain είναι εφαρμόσιμη σε κάθε τύπο ψηφιακών δεδομένων όπου ο έλεγχος ταυτότητας και η συναίνεση για την ακεραιότητα των δεδομένων είναι σημαντική και πολλά μέρη πρέπει να μοιράζονται την πρόσβαση εγγραφής. Το blockchain μπορεί να χρησιμοποιηθεί για την ασφάλεια ζωτικής σημασίας ιατρικών δεδομένων. Το Blockchain μπορεί να δώσει λύση στα προβλήματα τήρησης αρχείων στον κλάδο της υγειονομικής περίθαλψης και είναι ιδιαίτερα χρήσιμο για την καταγραφή συναλλαγών που συνεχίζουν να αναπτύσσονται σταθερά. Επιπλέον είναι πιο κατάλληλο για ένα ανοιχτό περιβάλλον συναλλαγών καταναλωτών όπου οι παλιές πληροφορίες είναι λιγότερο σημαντικές και η ανάπτυξη δεδομένων είναι σταθερή. Η τεχνολογία Blockchain εξετάζεται για την εξασφάλιση δεδομένων DNA, προσωπικών πληροφοριών, ιατρικών αρχείων και βασικών πληροφοριών ιατρικού ιστορικού. Οι πάροχοι υγειονομικής περίθαλψης μπορούν να χρησιμοποιήσουν το blockchain για να αποθηκεύσουν λεπτομέρειες σχετικά με τα αρχεία ασθενών, τα οποία οι ασθενείς και οι γιατροί μπορούν να δουν απευθείας στον ιστό οποιαδήποτε στιγμή, οπουδήποτε.

Το Blockchain επιτρέπει την ενοποιημένη φορητότητα και το πολύπλευρο σύστημα προστασίας σε διάφορες φάσεις. Επιτρέπει στους παρόχους υγειονομικής περίθαλψης να δημιουργήσουν ένα ολοκληρωμένο σύστημα αρχείων υγείας με επίκεντρο τον ασθενή, κατέχοντας τα ιδιωτικά κλειδιά των δεδομένων τους. Οι ασθενείς ελέγχουν ποιος μπορεί να έχει πρόσβαση ή να χρησιμοποιήσει τα δεδομένα τους. Ένα ολοκληρωμένο σύστημα που τροφοδοτείται από blockchain βοηθά στο συντονισμό αρχείων και δραστηριοτήτων και βοηθά στην αποτροπή της απάτης. Το σύστημα θα βοηθά επίσης τους ασθενείς να έχουν πρόσβαση και να διαχειρίζονται τα αρχεία υγείας τους από οπουδήποτε στον κόσμο, να μοιράζονται με ασφάλεια αυτά τα αρχεία με οποιονδήποτε

επαγγελματία υγείας και να παρακολουθεί το ιατρικό τους ιστορικό, όπως αλλεργίες, χρόνιες ασθένειες και εμβόλια.

Μια πρόσφατη μελέτη προτείνει ένα σύστημα διατήρησης δεδομένων βασισμένο σε blockchain για ιατρικά δεδομένα που μπορεί να παρέχει μια αξιόπιστη λύση αποθήκευσης. Αυτή διασφαλίζει την πρωτοτυπία και την επαληθευσιμότητα των αποθηκευμένων δεδομένων προστατεύοντας παράλληλα το απόρρητο των χρηστών. Το σύστημα επεξεργασμένων δεδομένων επιτρέπει στους χρήστες να αποθηκεύουν μόνιμα σημαντικά δεδομένα. Εάν υπάρχει υποψία παραποίησης, μπορεί να επαληθευτεί η πρωτοτυπία των δεδομένων. Μια άλλη μελέτη προτείνει μια προστασία ασφάλειας και απορρήτου που βασίζεται σε blockchain για την προσωπική υγεία. Λόγω του ότι παραμένει αναλλοίωτο, το blockchain μπορεί να βοηθήσει στη βελτίωση της ακρίβειας της διάγνωσης, όπου η ασφάλεια και η προστασία της ιδιωτικής ζωής είναι βασικά ζητήματα στο σύστημα

4.6.4 Κοινή Χρήση Δεδομένων και Διαλειτουργικότητα

Η αναποτελεσματική διαλειτουργικότητα δημιουργεί δύο τύπους προβλημάτων:

- Δυσκολία στον εντοπισμό ασθενών και αποκλεισμό πληροφοριών σχετικά με το πού βρίσκονται οι πάροχοι υγειονομικής περίθαλψης
- Επιβολή αδικαιολόγητων περιορισμών στην ανταλλαγή δεδομένων ασθενών ή ηλεκτρονικών πληροφοριών υγείας

Η έλλειψη μιας καθολικά αποδεκτής πρακτικής στοιχείων αναγνώρισης ασθενών και συγκάλυψης πληροφοριών έχει προκαλέσει τεράστια ζημιά στην αποτελεσματική πρακτική υγειονομικής περίθαλψης. Επίσης, η διαλειτουργικότητα είναι σημαντική, ειδικά σε μία περίοδο πανδημίας. Ο χρόνος εμφάνισης της επιδημίας υπογραμμίζει την επείγουσα ανάγκη για μια ισχυρότερη υποδομή κοινής χρήσης δεδομένων που μπορεί να βοηθήσει στον εξορθολογισμό της επικοινωνίας ασθενών-παρόχων και στον εξορθολογισμό της ροής πληροφοριών για τη διαχείριση απειλών για τη δημόσια υγεία. Εάν ένας ασθενής επισκεφτεί έναν γιατρό που δεν είναι ο γιατρός πρωτοβάθμιας φροντίδας του, πρέπει να έχει εύκολη πρόσβαση στα ιατρικά του αρχεία. Επιπλέον, η βελτίωση της ροής δεδομένων υγείας θα επιτρέψει στους γιατρούς να διεξάγουν τηλεπαρακολούθηση και τηλεϊατρική. Καθώς μπορεί μία πανδημία να επιδεινώνεται, οι προσβάσιμες και διαφανείς πληροφορίες, συμπεριλαμβανομένων πληροφοριών σχετικά με τον τρόπο με τον οποίο οι ασθενείς αξιολογούν τον κίνδυνο, αναπτύσσουν συμπτώματα και ανταποκρίνονται στη θεραπεία, είναι κρίσιμης σημασίας. Η κρίση της δημόσιας υγείας έχει επισημάνει περαιτέρω την έλλειψη διαλειτουργικότητας των υφιστάμενων συστημάτων.

Παρακάτω φαίνεται η τρέχουσα κατάσταση της κοινής χρήσης δεδομένων.

- Τα ιατρικά αρχεία αποθηκεύονται ψηφιακά σε κεντρικά συστήματα πληροφορικής, καθιστώντας δύσκολη την κοινή χρήση
- Η αίτηση, η αποστολή, η λήψη και η συλλογή δεδομένων ασθενών είναι κουραστική, χρονοβόρα και δαπανηρή
- Η τεχνολογική ανάπτυξη στη διαχείριση δεδομένων υγειονομικής περίθαλψης ήταν αργή λόγω των κανονισμών, των ασυμβίβαστων συστημάτων υποστήριξης και των κατακερματισμένων κοινών πληροφοριών υγειονομικής περίθαλψης
- Η έλλειψη συνεργασίας και κοινής χρήσης δεδομένων μεταξύ των συστημάτων αποθήκευσης υγειονομικής περίθαλψης καθιστά δύσκολη τη μεταφορά, την ανάκτηση και την ανάλυση δεδομένων

Ως αποτέλεσμα, πολλά από τα δεδομένα περιέχονται σε βάσεις δεδομένων, περιορίζοντας την ικανότητα του ασθενούς να γνωρίζουν το ιατρικό τους ιστορικό.

4.6.5 Λύσεις Blockchain για Κοινή Χρήση Δεδομένων

Η τεχνολογία Blockchain μπορεί να απλοποιήσει σημαντικά τη διαδικασία κοινής χρήσης δεδομένων υγειονομικής περίθαλψης και να βοηθήσει στην επίλυση προβλημάτων διαλειτουργικότητας στον κλάδο της υγειονομικής περίθαλψης. Σε ένα επιτρεπόμενο blockchain, οι ασθενείς αναγνωρίζονται από το κατακερματισμένο αναγνωριστικό τους, το οποίο θα είναι και το μοναδικό αναγνωριστικό τους. Ο κατακερματισμός επιτρέπει στο αναγνωριστικό να είναι μοναδικό και προστατεύει το απόρρητο του χρήστη. Οι ασθενείς θα επιβλέπουν την κοινή χρήση των δικών τους κλειδιών αποκρυπτογράφησης για σχετικά μπλοκ δεδομένων με τον επιλεγμένο πάροχο υγειονομικής περίθαλψης. Ενισχύει την ασφάλεια, το απόρρητο και τη διαλειτουργικότητα και μπορεί να τοποθετήσει τους ασθενείς στο κέντρο του οικοσυστήματος. Οι ασθενείς και οι πάροχοι θα λαμβάνουν ακριβή, ενημερωμένα, και πλήρη ιατρικά αρχεία.

4.6.6 Ασφάλεια Δεδομένων και Διαχείριση Ταυτότητας

Πρόσφατες παραβιάσεις ασφαλείας στα ιατρικά αρχεία ασθενών έχουν επιδεινώσει τις ανησυχίες σχετικά με την ασφάλεια των δεδομένων και το απόρρητο των ασθενών. Σύμφωνα με την παγκόσμια ασφάλεια δικτύου, η ασφαλιστική εταιρεία Beazley, έβγαλε πως το 45% των επιθέσεων ransomware (κακόβουλος ιός για κρυπτογράφηση αρχείων) το 2017 στόχευσε οργανισμούς υγειονομικής περίθαλψης. Ο αριθμός των παραβιασμένων ιατρικών αρχείων και των παραβιάσεων ιατρικών δεδομένων αυξάνεται. Σύμφωνα με το HIPAA Journal, ο αριθμός των αναφερόμενων παραβιάσεων στον κλάδο της υγειονομικής περίθαλψης αυξήθηκε από λιγότερες από 20 το 2009 σε περισσότερες από 350 το 2017. Το 2018, ο αριθμός των παραβιάσεων στον κλάδο της υγειονομικής περίθαλψης είχε ως αποτέλεσμα την έκθεση 13 εκατομμυρίων ιατρικών αρχείων, σύμφωνα με το Υπουργείο Υγείας και Ανθρωπίνων Υπηρεσιών. Οι παραβιάσεις δεδομένων υγείας κατά μέσο όρο τουλάχιστον μία την ημέρα, επηρεάζοντας περισσότερα από 27 εκατομμύρια αρχεία ασθενών το 2016. Χάκερ διέρρευσαν ευαίσθητα ιατρικά αρχεία 1,4 εκατομμυρίων ασθενών το 2018 από το δίκτυο νοσοκομείων UnityPoint Health. Θεωρήθηκε η μεγαλύτερη παραβίαση δεδομένων υγειονομικής περίθαλψης στις ΗΠΑ εκείνη τη χρονιά. Τα παραβιασμένα αρχεία περιλάμβαναν εργαστηριακά αποτελέσματα, θεραπείες, αριθμούς κοινωνικής ασφάλισης ασθενών και ασφαλιστικές πληροφορίες.

Πολλοί οργανισμοί υγειονομικής περίθαλψης αποθηκεύουν πολύτιμες πληροφορίες για την υγεία σε μια κεντρική τοποθεσία σε παλαιωμένη υποδομή πληροφορικής, πρωταρχικό στόχο για ransomware και άλλες επιθέσεις στον κυβερνοχώρο. Οι οργανισμοί υγειονομικής περίθαλψης γίνονται συχνά στόχος εξελιγμένων κυβερνοεπιθέσεων λόγω του βάθους των πληροφοριών που αποθηκεύουν οι πάροχοι. Η απώλεια πρόσβασης στα αρχεία ασθενών και σε άλλες κρίσιμες πληροφορίες μπορεί να ακρωτηριάσει οποιονδήποτε πάροχο, κοστίζοντας εκατομμύρια δολάρια στην οργάνωση-θύμα. Οι οργανισμοί υγειονομικής περίθαλψης επενδύουν σε προηγμένες τεχνολογίες ασφάλειας, όπως καλύτερα αντίγραφα ασφαλείας δεδομένων, προηγμένη κρυπτογράφηση δεδομένων, τεχνητή νοημοσύνη και πλατφόρμες ασφαλείας σε πραγματικό χρόνο για να αποτρέψουν απειλές προτού αρχίσουν να προκαλούν σοβαρά προβλήματα. Οι ανησυχίες σχετικά με την ασφάλεια των δεδομένων και το απόρρητο των ασθενών, καθώς και η αύξηση του αριθμού των επιθέσεων στον κυβερνοχώρο έχουν οδηγήσει σε επείγουσα ανάγκη για καλύτερη ασφάλεια πληροφορικής.

4.6.7 Λύσεις Blockchain για Ασφάλεια Δεδομένων και Διαχείριση Ταυτότητας

Το Blockchain μπορεί να προσφέρει πολλά πλεονεκτήματα για την ασφάλεια των δεδομένων υγειονομικής περίθαλψης και τη διαχείριση ταυτότητας. Αποτρέπει τις απειλές και προστατεύει τα προσωπικά δεδομένα από το να πέσουν σε λάθος χέρια. Το Blockchain κρυπτογραφεί δεδομένα όταν προστίθενται στην αλυσίδα και τα καθιστά αμετάβλητα και μη αποκρυπτογραφημένα. Εξουσιοδοτεί συναλλαγές χρησιμοποιώντας ένα ιδιωτικό κλειδί αναγνώρισης που είναι γνωστό μόνο στο άτομο. Έτσι, σε αντίθεση με τη σημερινή τεχνολογία δεδομένων υγειονομικής περίθαλψης, οι πάροχοι της μπορούν να έχουν πρόσβαση στα ιατρικά δεδομένα ασθενών μόνο με ρητή πρόσβαση σε αρχεία blockchain. Η καλύτερη συνεργασία δεδομένων μεταξύ παρόχων αυξάνει την πιθανότητα ακριβούς διάγνωσης και την πιθανότητα επιτυχίας θεραπειών και επιτρέπουν στις εγκαταστάσεις υγειονομικής περίθαλψης να παρέχουν οικονομικά αποδοτική περίθαλψη. Το Blockchain μπορεί να διατηρήσει τις πληροφορίες των ασθενών ασφαλείς, ενώ παράλληλα τους επιτρέπει να τις μοιράζονται με οποιονδήποτε πάροχο υπηρεσιών επιλέγουν. Παρέχει απόδειξη ιδιοκτησίας ιατρικών αρχείων και εγγυάται την αυθεντικότητα της τεχνολογίας κατά της παραχάραξης.

Σύμφωνα με μια πρόσφατη μελέτη που διεξήχθη από την BIS Research, ο κλάδος της υγειονομικής περίθαλψης θα μπορούσε να εξοικονομήσει έως και 100 δισεκατομμύρια δολάρια ετησίως έως το 2025 μέσω της υιοθέτησης της τεχνολογίας blockchain. Η εξοικονόμηση πόρων θα πραγματοποιηθεί με τη μείωση του κόστους που σχετίζεται με παραβιάσεις δεδομένων, το λειτουργικό κόστος, το κόστος πληροφορικής, την απάτη που σχετίζεται με την παραχάραξη και την ασφαλιστική απάτη. Η έκθεση αναφέρει ότι η εφαρμογή του blockchain στην παγκόσμια αγορά υγειονομικής περίθαλψης αναμένεται να αυξήσει τον σύνθετο ετήσιο ρυθμό ανάπτυξης από το 2018 έως το 2025 περίπου 64% και θα έχει φτάσει σχεδόν τα 6 δισεκατομμύρια έως το 2025.

4.6.8 Blockchain στην Κλινική Ερευνά

Οι κλινικές μελέτες μπορεί να αντιμετωπίσουν ποικίλα προβλήματα, όπως η προστασία των δεδομένων, η ακεραιότητα των δεδομένων, η ανταλλαγή δεδομένων, η τήρηση εγγράφων, η εγγραφή ασθενών [100] κ.ο.κ. Το Bitcoin, η επερχόμενη τεχνολογία του διαδικτύου, μπορεί να προσφέρει εφαρμόσιμες απαντήσεις σε αυτά τα ζητήματα. Η τεχνολογία blockchain χρησιμοποιείται από ειδικούς στον τομέα της υγειονομικής περίθαλψης για την αντιμετώπιση αυτών των προβλημάτων [86, 101]. Οι εφαρμογές blockchain, μαζί με την τεχνητή νοημοσύνη (AI) και τη μηχανική μάθηση, θα φέρουν σύντομα επανάσταση στον τομέα της υγειονομικής περίθαλψης.

Το Ethereum, ένα πρωτόκολλο που προσφέρει τη δυνατότητα έξυπνων συμβολαίων στην αλυσίδα μπλοκ [101, 102], χρησιμοποιείται παράλληλα με τα συστήματα διαχείρισης δεδομένων που βασίζονται σε κλινικές στην έρευνα που παρουσιάστηκε από τους Timothy et al. Ο πρωταρχικός στόχος της μελέτης ήταν η επίλυση της πρόκλησης εγγραφής ασθενών. Τα αποτελέσματα της μελέτης έδειξαν ότι το Ethereum επέτρεπε ταχύτερες μεταφορές από το Bitcoin και το συμπέρασμα που ακολούθησε, πρότεινε τη χρήση έξυπνων συμβολαίων του Ethereum για την αύξηση της διαφάνειας των συστημάτων διαχείρισης δεδομένων σε κλινικές δοκιμές. Ως εκ τούτου, μία από τις τρέχουσες χρήσεις αυτής της τεχνολογίας στην κλινική μελέτη είναι η εγγραφή ασθενών με τη χρήση blockchain.

Ο Mehdi Benchoufi διεξήγαγε πρόσθετη έρευνα, υλοποιώντας ένα πλαίσιο για τη λήψη της εν επίγνωση άδειας των ασθενών για την παρακολούθηση και τη διατήρησή της με τρόπο ασφαλή, ανοιχτά αποδεδειγμένο και μη διαψεύσιμο [103]. Δημιούργησαν τη διαδικασία του χρησιμοποιώντας τεχνολογία blockchain.

4.6.9 Blockchain και Νευροεπιστημη

Η ποσότητα των ειδήσεων και των ερευνών που σχετίζονται με τις εφαρμογές blockchain αυξάνεται, και ο τομέας των νευροεπιστημών είναι αναμφίβολα μεταξύ αυτών [104]. Εξαλείφοντας τη μηχανική επαφή με τις υποδομές του περιβάλλοντος και επιτρέποντας τη διαχείριση συσκευών και δεδομένων μέσω νοητικών οδηγιών, οι σύγχρονες νευρωνικές τεχνολογίες στοχεύουν στη δημιουργία ενός νέου παραδείγματος. Τέτοιες νευρωνικές συσκευές έχουν την ικανότητα να διαβάζουν μοτίβα εγκεφαλικής δραστηριότητας και να μετατρέπουν τα μοτίβα αυτά σε οδηγίες για τη λειτουργία εξωτερικών συσκευών. Μπορούν επίσης να χρησιμοποιήσουν δεδομένα εγκεφαλικής δραστηριότητας για να προσδιορίσουν την παρούσα νοητική κατάσταση ενός ατόμου. Οι συσκευές νευρωνικής διεπαφής με πολλαπλούς ευαίσθητους αισθητήρες, κυκλώματα υπολογιστών και ασύρματη μετάδοση είναι σε θέση να λαμβάνουν και να αναλύουν τα εγκεφαλικά ερεθίσματα. Ερμηνεύουν την ηλεκτρική δραστηριότητα του εγκεφάλου, η οποία στη συνέχεια αναμεταδίδεται στην ελεγχόμενη συσκευή για περαιτέρω αποκωδικοποίηση. Το άτομο φοράει μια ενιαία συσκευή στο κεφάλι του που φιλοξενεί όλη αυτή την τεχνολογία. Η θεωρία του blockchain θα εφαρμοστεί με σύνθετους αλγόριθμους και μεγάλα δεδομένα για την καταγραφή αυτών των εγκεφαλικών σημάτων στη νευρωνική διεπαφή. Η Neurogress είναι μία από τις επιχειρήσεις που επιβεβαιώνουν ότι θα χρησιμοποιούν την τεχνολογία blockchain. Η εταιρεία, η οποία ιδρύθηκε το 2017 και είναι εγγεγραμμένη στην Ελβετία, ειδικεύεται στην ανάπτυξη συστημάτων νευροελέγχου που επιτρέπουν στους χρήστες να διοικούν ρομποτικούς βραχίονες, μη επανδρωμένα αεροσκάφη, έξυπνες συσκευές και AR/VR (επαυξημένη πραγματικότητα/εικονική πραγματικότητα) γκάτζετ με το μυαλό τους.

Η ακρίβεια της ανάγνωσης του εγκεφάλου από το σύστημα ελέγχου της Neurogress βελτιώνεται μέσω της μηχανικής μάθησης, η οποία απαιτεί τη διατήρηση του 90% των δεδομένων του εγκεφάλου προκειμένου να διδαχθεί η τεχνητή νοημοσύνη (AI) του συστήματος. Με άλλα λόγια, απαιτούνται "μεγάλα δεδομένα της ανθρώπινης νευρικής δραστηριότητας" και η ανάγκη του Human Brain Project για "exabytes (1 exabyte = 1 δισεκατομμύριο megabytes) μνήμης", αναφέρεται στο whitepaper της εταιρείας ως παράδειγμα του τύπου της απαιτούμενης ικανότητας αποθήκευσης. Διαπιστώνοντας ότι το blockchain "λύνει αποτελεσματικά το ζήτημα της ασφάλειας και της ανωνυμίας στην αποθήκευση δεδομένων", η Neurogress σκοπεύει να το χρησιμοποιήσει. Τα δεδομένα των χρηστών καθίστανται "ανθεκτικά σε επιθέσεις κακόβουλων χρηστών" και, ως εκ τούτου, πιο ιδιωτικά με το να αποθηκεύονται σε μια αποκεντρωμένη αλυσίδα μπλοκ (blockchain). Επιπλέον, το σύστημα της Neurogress είναι ανοικτό για τους υποψήφιους καταναλωτές των υπηρεσιών της πλατφόρμας χάρη στη χρήση της τεχνολογίας blockchain. Η μέθοδος θα διασφαλίσει την ασφάλεια και το απόρρητο των προσωπικών δεδομένων, επειδή οποιαδήποτε ανώμαλη συμπεριφορά θα είναι εύκολο να εντοπιστεί.

Ως εκ τούτου, είναι σαφές ότι τα blockchain αποτελούν ένα είδος τεχνολογίας πληροφοριών με πολλές σημαντικές πιθανές χρήσεις, συμπεριλαμβανομένης της επαύξησης του εγκεφάλου, της μοντελοποίησης του εγκεφάλου και της εγκεφαλικής σκέψης. Η ανάγκη για ένα μέσο αποθήκευσης προκύπτει κατά την ψηφιοποίηση του πλήρους ανθρώπινου εγκεφάλου. Σε αυτό το σημείο κάνει και πάλι την εμφάνισή της η τεχνολογία blockchain. Μια πρόταση είναι η αποθήκευση mindfiles, τα οποία θα λειτουργούσαν ως τα δομικά στοιχεία δεδομένων στις επιμέρους αλυσίδες σκέψης και θα μπορούσαν να διαμοιράζονται σε ένα σύστημα αρχείων δικτύου ομότιμων χρηστών που υποστηρίζει την έκδοση του ιστορικού. Ένα υπολογιστικό σύστημα με διάφορα χαρακτηριστικά που επιτρέπουν τη δυνατότητα τεχνητής νοημοσύνης, ανθρώπινης βελτίωσης και την πιθανή συγχώνευσή τους προτείνεται ως αυτό το είδος σκέψης blockchain. Προκειμένου να επαληθευτεί η προέλευση και η ειλικρίνεια ενός καθολικού, το blockchain επιτρέπει σε ένα δίκτυο συνδεδεμένων υπολογιστών να σφίγγει στα χέρια του κάθε χρονικό σημείο. Αυτού του είδους ο μηχανισμός εμπιστοσύνης θα μπορούσε να επιτρέψει στα νευρωνικά δίκτυα να αποθηκεύουν και να θυμούνται με ακρίβεια

πληροφορίες σχετικά με το τι είναι υποκειμενικό έναντι του αντικειμενικού μιας συγκεκριμένης εμπειρίας, αν κατασκευάζαμε έναν εγκέφαλο από το μηδέν. Ως εφαρμογή blockchain, ο έλεγχος ταυτότητας πολλαπλών παραγόντων που συνδέεται με μια προσωπική αλυσίδα σκέψης μπορεί να ανοίξει ευκαιρίες για την ασφαλή κατασκευή μιας κοινότητας δεδομένων μετρήσιμων για τους ανθρώπους.

Με τη βοήθεια των κοινών δεδομένων, τα απομονωμένα αρχεία στα οποία αποθηκεύονται τα ανθρώπινα δεδομένα μειώνονται. Κάθε άτομο αποκτά τον έλεγχο της ιδιωτικής του ζωής και τη δυνατότητα να μοιράζεται τις εμπειρίες του με άλλους για πιθανό οικονομικό κέρδος χωρίς τη βοήθεια τρίτου μέρους ή κεντρικής αρχής. Στο μέλλον, όταν δύο ή περισσότερα άτομα βιώνουν την ίδια στιγμή από διαφορετικές οπτικές γωνίες, μπορεί να είμαστε σε θέση να ανακατασκευάσουμε τις εμπειρίες τους προκειμένου να είμαστε πιο αμερόληπτοι σχετικά με το τι συνέβαινε εκείνη ακριβώς τη στιγμή. Ιδανικά, αυτό θα καταστήσει δυνατή τη δημιουργία ψηφιακών προσομοιώσεων παλαιών αναμνήσεων και τη δυνατότητα να βλέπουμε προσωπικά τα πράγματα από την οπτική γωνία ενός άλλου ατόμου. Αυτό θα ενσωματώσει δεδομένα από τις αισθήσεις σε αυτή την επερχόμενη αλυσίδα μπλοκ μόλις έχουμε μια πιο ελαστική αντίληψη για το πώς οι μεμονωμένες αντιστοιχίσεις σε συναισθήματα και αισθητηριακά γεγονότα συμβάλλουν σε μια συγκεκριμένη ανάμνηση (π.χ. όραση, όσφρηση κ.ο.κ.). Επιπλέον, επί του παρόντος δημιουργούνται τα απαραίτητα εργαλεία. Στο όχι πολύ μακρινό μέλλον, η σημερινή κατάσταση των συσκευών εγκεφάλου και νεύρων, η απεικόνιση με βιοανάδραση και κάθε άλλο μέσο που επιτρέπει ένα πολυπαραγοντικό αποτύπωμα μοναδικό για το αρχείο της χρονικής εμπειρίας ενός συγκεκριμένου ανθρώπου θα μας επιτρέψει να αρχίσουμε να καταγράφουμε τις αισθητηριακές μας εμπειρίες. Η έρευνα μπορεί να γίνει για τη βελτίωση της λήψης αποφάσεων, της μάθησης, της μνήμης και των διαδικασιών αποκατάστασης χρησιμοποιώντας αυτά τα εργαλεία ως σημείο εκκίνησης.

4.6.10 Blockchain και Μεταμόσχευση Οργάνων

Ένα άλλο παράδειγμα για πως το blockchain αλλάζει τον κλάδο της υγειονομικής περίθαλψης είναι στον τομέα των μεταμοσχεύσεων οργάνων. Οι μεταμοσχεύσεις οργάνων είναι περίπλοκες. Η κατάσταση των οργάνων μπορεί να χειροτερεύσει γρήγορα και τα δωρισμένα όργανα πρέπει να προέρχονται από άτομα με συμβατούς τύπους αίματος. Μια μεταμόσχευση καρδιάς ή πνεύμονα διαρκεί συνήθως λιγότερο από 10 ώρες, σύμφωνα με το Κέντρο Μεταμοσχεύσεων του Πανεπιστημίου του Μίσιγκαν. Χωρίς αποτελεσματικό σύστημα, τα σωτήρια όργανα θα πήγαιναν χαμένα. Σε αυτό το σημείο βοηθάει το blockchain, επιταχύνοντας την διαδικασία εύρεσης συμβατού δότη. Περισσότεροι από 120.000 άνθρωποι περιμένουν για μεταμόσχευση οργάνου και κατά μέσο όρο 22 από αυτούς πεθαίνουν κάθε μέρα. Η Organtree είναι η πρώτη αποκεντρωμένη εταιρεία βάσης δεδομένων δωρεών οργάνων στον κόσμο που χρησιμοποιεί τεχνολογία blockchain για τη σύνδεση δωρητών, ασθενών και ιατρικών ιδρυμάτων. Η χρήση του blockchain επιτρέπει στην Organtree να αυξήσει τον αριθμό των αντιστοιχιών και να κάνει τη μεταφορά ταχύτερη και ευκολότερη από ποτέ. Αυτό επιτυγχάνεται εύκολα γιατί το blockchain παρέχει ένα ασφαλές και αδιάβλητο αρχείο για όλες τις συναλλαγές και τις διαδικασίες που εμπλέκονται στη δωρεά και μεταμόσχευση οργάνων. Αυτή η διαφάνεια διασφαλίζει ότι όλα τα δεδομένα είναι αξιόπιστα και ακριβή, μειώνοντας τον κίνδυνο απάτης και λαθών. Επιπλέον με το blockchain, οι μεσάζοντες και οι ενδιάμεσοι που μπορούν να προκαλέσουν καθυστερήσεις και επιπλοκές στη διαδικασία εξαλείφονται. Αυτό επιτρέπει άμεση και άμεση επικοινωνία μεταξύ των δωρητών, των ληπτών και των ιατρικών φορέων. Τα έξυπνα συμβόλαια (smart contracts) στο blockchain μπορούν να αυτοματοποιήσουν τη διαδικασία ταυτοποίησης των αντιστοιχιών μεταξύ δωρητών και ληπτών. Αυτά τα συμβόλαια μπορούν να εκτελούνται αυτόματα όταν πληρούνται συγκεκριμένα κριτήρια, επιταχύνοντας τη διαδικασία. Το

blockchain επιτρέπει επίσης την εύκολη παρακολούθηση και τον έλεγχο της αλυσίδας εφοδιασμού οργάνων, από τον δωρητή έως τον λήπτη. Αυτό μειώνει την πιθανότητα απώλειας ή κακής διαχείρισης των οργάνων. Τέλος, η τεχνολογία blockchain επιτρέπει σε διάφορους φορείς, όπως νοσοκομεία, τράπεζες οργάνων και ερευνητικά κέντρα, να συνεργάζονται αποτελεσματικότερα και σε πραγματικό χρόνο, βελτιώνοντας την συνολική διαδικασία δωρεάς και μεταμόσχευσης.

Τα Ηνωμένα Αραβικά Εμιράτα (ΗΑΕ) είναι η πρώτη χώρα στον κόσμο που χρησιμοποιεί blockchain και τεχνητή νοημοσύνη για μεταμοσχεύσεις οργάνων. Τα Ηνωμένα Αραβικά Εμιράτα έχουν συνεργαστεί με την Dhonor Healthtech, μια κορυφαία εθνική εταιρεία που επικεντρώνεται σε παγκόσμιες λύσεις blockchain υγειονομικής περίθαλψης. Ο κύριος στόχος είναι η επίτευξη μιας ασφαλέστερης και βελτιστοποιημένης διαδικασίας δωρεάς οργάνων. Ένας περαιτέρω στόχος είναι η θέσπιση προτύπων για τη βελτίωση της επαλήθευσης οργάνων, της αντιστοίχισης οργάνου-ασθενούς και της βελτιστοποίησης της μεταμόσχευσης χρησιμοποιώντας τεχνητή νοημοσύνη και blockchain. Το blockchain και η τεχνητή νοημοσύνη επιτρέπουν στα νοσοκομεία να βελτιστοποιούν τη διαδικασία αντιστοίχισης οργάνων από δότη σε ασθενή.

4.6.11 Φαρμακευτικός Κλάδος

Οι φαρμακευτικές εταιρείες εργάζονται συνεχώς για να βελτιώσουν την ποιότητα των φαρμάκων και να εφεύρουν νέα φάρμακα για μια ποικιλία ασθενειών. Για να διασφαλιστεί η προστασία των διπλωμάτων ευρεσιτεχνίας, η ασφάλεια, η αποτελεσματικότητα, η στατιστική εγκυρότητα και η ρυθμιστική έγκριση των φαρμάκων, αυτά πρέπει να περάσουν από μια μακρά και περίπλοκη διαδικασία. Συνήθως, αυτή η διαδικασία διαρκεί πολλά χρόνια, από την ανακάλυψη έως την εμπορευματοποίηση, με τις κλινικές δοκιμές να καταλαμβάνουν τον περισσότερο χρόνο. Έτσι, μια τόσο χρονοβόρα διαδικασία είναι ευάλωτη σε απομιμήσεις φαρμάκων λόγω έλλειψης ασφάλειας και ιδιωτικότητας.

4.6.12 Λύσεις Blockchain στον Φαρμακευτικό Κλάδο

Το παραπάνω εμπόδιο μπορεί να αφαιρεθεί χρησιμοποιώντας τεχνολογία blockchain σε όλη τη φαρμακευτική διαδικασία. Μπορούμε να διατηρήσουμε το απόρρητο και να διασφαλίσουμε την ασφάλεια μέσω της χρήσης κατανεμημένων λογιστικών βιβλίων μέσω της αλυσίδας μπλοκ, διασφαλίζοντας ότι κάθε δοκιμαστικό συμβάν καταγράφεται σε έναν κόμβο blockchain που δεν παραβιάζεται. Θα μπορούσε να χρησιμοποιηθεί ένα ιδιωτικό blockchain για να διασφαλιστεί ότι όλα τα φάρμακα υπόκεινται σε προστασία με δίπλωμα ευρεσιτεχνίας. Αυτό μπορεί να γίνει χρησιμοποιώντας έξυπνα συμβόλαια που παρέχουν ακεραιότητα, ιχνηλασιμότητα και διαφάνεια. Σύμφωνα με μια πρόσφατη μελέτη, περίπου το 60% των φαρμακευτικών εταιρειών χρησιμοποιούν ή πειραματίζονται με το blockchain, αντανακλώντας τις δυνατότητες του blockchain σε τέτοιους κλάδους. Τα πλαστά φάρμακα αποτελούν παγκόσμιο πρόβλημα και πρόκληση, εγκυμονώντας εξαιρετικούς κινδύνους για το κοινό και τους καταναλωτές.

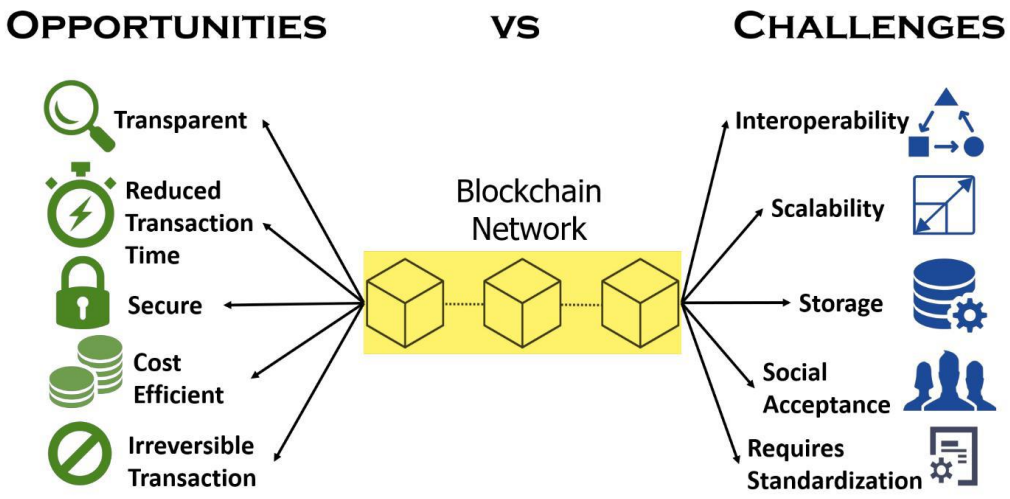
Οι Selim et al. ανέπτυξαν σύστημα blockchain παρακολούθησης φαρμάκων για να ελέγξουν την σκοπιμότητα εφαρμογής της τεχνολογίας και των αρχών της σε ένα προσομοιωμένο δίκτυο [132]. Στόχος είναι η βελτίωση της ιχνηλασιμότητας των παραποιημένων φαρμάκων. Το σύστημα αντιστέκεται στην παραδοσιακή παραποίηση της αλυσίδας εφοδιασμού φαρμάκων, η οποία αποτελεί σημαντικό πρόβλημα για ορισμένες ασιατικές χώρες. Από πολλές απόψεις, το Gcoin (Global Governance Coin), το νόμισμα παγκόσμιας διακυβέρνησης, παρέχει έναν δυναμικό ρόλο για όλους τους κόμβους, συμπεριλαμβανομένων των εκδοτών νομισμάτων, των πλήρων κόμβων, των miners ή

των συνηθισμένων κόμβων, που χρησιμοποιείται στη διαχείριση της αλυσίδας εφοδιασμού φαρμάκων.

Οι Tseng et al. σύστησαν τη χρήση του blockchain Gcoin ως βάση για τη ροή δεδομένων των φαρμάκων για τη δημιουργία διαφανών δεδομένων συναλλαγών των φαρμάκων [133]. Αυτό μοιράζεται μεταξύ κατασκευαστών, χονδρεμπόρων, λιανοπωλητών, φαρμακείων, νοσοκομείων και καταναλωτών. Τα αρχεία των συναλλαγών των φαρμάκων μπορούν να μετατρέψουν την αλυσίδα εφοδιασμού των φαρμάκων από ρύθμιση (ελεγχόμενη από την κυβέρνηση) σε επιτήρηση (συνεργασία από κάθε συμμετέχοντα). Επιπλέον, τα ρυθμιστικά μοντέλα για τις φαρμακευτικές αλυσίδες εφοδιασμού μπορεί να διαφέρουν σε ελέγχους στο μοντέλο του δικτύου παρακολούθησης. Για περισσότερο από μια δεκαετία, η τεχνολογία αναγνώρισης ραδιοσυχνοτήτων (RFID) έχει αναγνωριστεί ως ισχυρό μέτρο προστασίας ιδιοκτησίας, ωστόσο, εκτός του αξιόπιστου τομέα της RFID, όπως τα δίκτυα ταχυδρομικής αλυσίδας εφοδιασμού, είναι εύκολο να παραποιηθεί με την κλωνοποίηση αυτής της αναγνώρισης. Με την εκμετάλλευση της πλατφόρμας Ethereum, τέτοια τρωτά σημεία μπορούν να εξαλειφθούν σε όλη την αλυσίδα εφοδιασμού από τον κατασκευαστή έως τον τελικό πελάτη.

ΚΕΦΑΛΑΙΟ 5: Προκλήσεις

Το Blockchain είναι μια νέα τεχνολογία που κερδίζει έδαφος σε πολλούς κλάδους [105] και προσφέρει πολλά πλεονεκτήματα [106] και δυνατότητες [107]. Ωστόσο, η τεχνολογία αυτή έχει μια μοναδική συλλογή ζητημάτων που πρέπει να επιλυθούν (όπως απεικονίζεται στην εικόνα 12). Στο παρόν μέρος εξετάζονται μερικές από αυτές τις ουσιαστικές δυσκολίες.



Εικόνα 12. Πλεονεκτήματα και Μειονεκτήματα Blockchain στην Υγεία [124]

5.1 Ασφάλεια και Ιδιωτικό Απόρρητο των Δεδομένων

Η προστασία των δεδομένων και της ιδιωτικής ζωής είναι οι πρώτες και σημαντικότερες προκλήσεις [108]. Η ανάγκη ύπαρξης τρίτου μέρους για την ολοκλήρωση μιας συναλλαγής καταργείται με τη χρήση εφαρμογών που βασίζονται στην τεχνολογία blockchain [106]. Τα δεδομένα είναι ευάλωτα σε πιθανούς κινδύνους προστασίας της ιδιωτικής ζωής και ασφάλειας, επειδή ο μηχανισμός blockchain

επιτρέπει σε ολόκληρη την κοινότητα, σε αντίθεση με ένα μοναδικό αξιόπιστο τρίτο μέρος, να επικυρώνει τις εγγραφές σε μια αρχιτεκτονική blockchain [109]. Το απόρρητο των δεδομένων δεν θα είναι άθικτο επειδή όλοι οι κόμβοι μπορούν να δουν τα δεδομένα που μοιράζεται ένας κόμβος. Ο ασθενής πρέπει να επιλέξει έναν ή περισσότερους πράκτορες οι οποίοι, σε περίπτωση έκτακτης ανάγκης, θα μπορούν να έχουν πρόσβαση στις πληροφορίες του ή/και στο ιατρικό ιστορικό του εκ μέρους του, ελλείψει τρίτου μέρους για άδεια. Το γεγονός ότι ο εν λόγω αντιπρόσωπος μπορεί πλέον να δώσει σε μια ομάδα ατόμων πρόσβαση στις πληροφορίες του ίδιου ασθενούς αποτελεί σοβαρό κίνδυνο για την ιδιωτικότητα και την ασφάλεια των εν λόγω δεδομένων. Λόγω των δυσκολιών στη μετακίνηση των δεδομένων από το ένα μπλοκ στο άλλο όταν χρησιμοποιούνται μέθοδοι υψηλής ασφάλειας, οι παραλήπτες θα έχουν πρόσβαση μόνο σε ορισμένα ή σε όλα τα δεδομένα. Επιπλέον, οι επιθέσεις 51%, ένας τύπος παραβίασης της ασφάλειας, είναι δυνατές στα δίκτυα blockchain [110]. Σε αυτή την επίθεση εμπλέκεται μια ομάδα ανθρακωρύχων που ελέγχουν περισσότερο από το 50% των δεδομένων σε ένα δίκτυο blockchain. Αποκτώντας τον έλεγχο του δικτύου, οι ανθρακωρύχοι μπορούν να σταματήσουν κάθε νέα μεταφορά, παρακρατώντας την έγκρισή τους. Πέντε κρυπτονομίσματα έχουν πέσει πρόσφατα θύματα αυτής της επίθεσης, σύμφωνα με το coindesk [111]. Επιπλέον, ένα ιατρικό έγγραφο μπορεί να περιέχει ιδιωτικές πληροφορίες που είναι ακατάλληλες για την αλυσίδα μπλοκ [112].

5.2 Διαχείριση Χωρητικότητας Αποθήκευσης

Η διαχείριση της δυνατότητας αποθήκευσης παρουσιάζει μια άλλη δυσκολία σε αυτό το μέτωπο. Το blockchain δεν απαιτεί μεγάλη χωρητικότητα επειδή δημιουργήθηκε για την αποθήκευση και τη διαχείριση δεδομένων συναλλαγών, τα οποία έχουν συγκεκριμένο σκοπό [113]. Τα προβλήματα αποθήκευσης έγιναν εμφανή με την πάροδο του χρόνου καθώς επεκτάθηκε στον κλάδο της υγειονομικής περίθαλψης. Καθημερινά, πρέπει να γίνεται χειρισμός σημαντικής ποσότητας δεδομένων στον κλάδο της υγειονομικής περίθαλψης. Όλα τα δεδομένα, συμπεριλαμβανομένων των αρχείων ασθενών, του ιστορικού υγείας, των αποτελεσμάτων εξετάσεων, των μαγνητικών τομογραφιών, των ακτίνων Χ και άλλων ιατρικών εικόνων, θα είναι προσβάσιμα σε όλους τους κόμβους της αλυσίδας στην κατάσταση blockchain, γεγονός που καθιστά αναγκαία μια σημαντική ποσότητα αποθηκευτικού χώρου [114, 115]. Επιπλέον, επειδή οι εφαρμογές blockchain βασίζονται σε συναλλαγές, οι βάσεις δεδομένων που χρησιμοποιούνται για την υποστήριξη αυτής της τεχνολογίας έχουν την τάση να επεκτείνονται γρήγορα. Η ταχύτητα αναζήτησης και πρόσβασης σε εγγραφές επιβραδύνεται καθώς οι βάσεις δεδομένων αυξάνονται σε μέγεθος, καθιστώντας τες τρομερά ακατάλληλες για τα είδη των συναλλαγών όπου η ταχύτητα είναι ζωτικής σημασίας. Ως αποτέλεσμα, ένα σύστημα blockchain πρέπει να είναι τόσο προσαρμόσιμο όσο και ανθεκτικό [116].

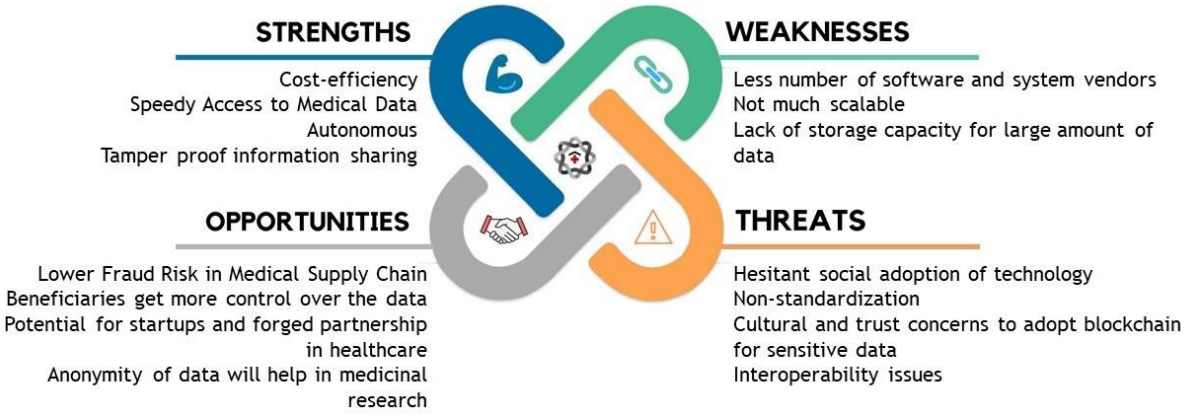
5.3 Προκλήσεις Τυποποίησης

Η τεχνολογία blockchain βρίσκεται ακόμη σε νηπιακό στάδιο, οπότε αναμφίβολα θα υπάρξουν δυσκολίες με τη ρύθμιση στην πορεία προς την πραγματική εφαρμογή της στην ιατρική και την υγειονομική περίθαλψη. Θα χρειαστούν διεθνείς οργανισμοί τυποποίησης για την παροχή μιας σειράς καλά πιστοποιημένων και επαληθευμένων προτύπων. Θα ήταν χρήσιμο να αξιολογηθεί το μέγεθος, ο τύπος δεδομένων και η μορφή των πληροφοριών που μοιράζονται στις εφαρμογές blockchain χρησιμοποιώντας αυτά τα καθιερωμένα πρότυπα. Αυτά τα πρότυπα πρέπει να λειτουργούν ως προληπτικά μέτρα ασφαλείας εκτός από τον έλεγχο των κοινών δεδομένων.

5.4 Κοινωνικές Προκλήσεις

Η τεχνολογία blockchain βρίσκεται ακόμη σε πρώιμο στάδιο, οπότε εκτός από τις προαναφερθείσες τεχνολογικές δυσκολίες, αντιμετωπίζει και κοινωνικές δυσκολίες όπως οι πολιτισμικές αλλαγές. Δεν είναι ποτέ απλό να αποδεχτείς και να αγκαλιάσεις μια τεχνολογία που είναι θεμελιωδώς διαφορετική από τον τρόπο με τον οποίο γίνονταν πάντα τα πράγματα. Παρόλο που ο ιατρικός τομέας αγκαλιάζει σταδιακά την αυτοματοποίηση, υπάρχει ακόμη πολύς δρόμος μέχρι να υιοθετήσει πλήρως τις νέες τεχνολογίες, ιδίως εκείνες όπως το blockchain, οι οποίες δεν έχουν ακόμη αποδειχθεί αποτελεσματικές σε θεραπευτικές ρυθμίσεις. Θα χρειαστεί χρόνος και προσπάθεια για να πειστούν οι γιατροί να χρησιμοποιούν την τεχνολογία αντί για χαρτιά. Η τεχνολογία και οι πολιτικές που παρέχονται είναι συγκριτικά αναξιόπιστες λόγω των χαμηλών ποσοστών χρήσης τους στον τομέα της υγείας [116]. Δεν είμαστε σε θέση να πούμε ότι είναι μια λειτουργική και ολοκληρωμένη απάντηση στα προβλήματα της υγειονομικής περίθαλψης αυτή τη στιγμή [106] λόγω όλων αυτών των εμποδίων και κινδύνων.

Χρησιμοποιήθηκε μια μέθοδο ανάλυσης SWOT για την κατανόηση, την ανάλυση και την αντιμετώπιση με καλύτερο τρόπο τα πλεονεκτήματα, τα μειονεκτήματα, τις ευκαιρίες και τους κινδύνους που αντιμετωπίζει η τεχνολογία blockchain στον κλάδο της υγειονομικής περίθαλψης (όπως απεικονίζεται στην εικόνα 13).



Εικόνα 13. SWOT Ανάλυση [124]

ΚΕΦΑΛΑΙΟ 6: Σχεδίαση Πρότυπης Εφαρμογής Υγείας

Η τεχνολογία blockchain έχει τραβήξει ενδιαφέροντα λόγω της αποκεντρωμένης, ασφαλούς και μόνιμης φύσης της. Οι εφαρμογές της σε διάφορα τμήματα, ιδίως στην υγειονομική περίθαλψη, αναμένεται να μετατρέψουν τη διαχείριση των πληροφοριών, την ασφάλεια και τη φροντίδα των ασθενών. Αυτή η έκθεση αναλύει τις εφαρμογές blockchain που περιγράφονται ειδικά για τα συστήματα υγειονομικής περίθαλψης, εστιάζοντας στην διαχείριση δεδομένων, την πιστοποίηση ταυτότητας γιατρών και την πρόσβαση στον έλεγχο.

6.1 Στόχοι

Ο μεγαλύτερος στόχος είναι να καταδειχθούν τα δυνητικά οφέλη του blockchain στην υγειονομική περίθαλψη, με έμφαση στην αξιοπιστία, την ιχνηλασιμότητα και την ασφάλεια των πληροφοριών. Η εφαρμογή της τεχνολογίας blockchain μπορεί να προσφέρει υψηλό επίπεδο ασφάλειας για την αποθήκευση και τη μετάδοση ευαίσθητων υγειονομικών δεδομένων. Η κρυπτογράφηση και η ανάθεση δικαιωμάτων πρόσβασης μπορούν να διασφαλίσουν ότι μόνο εξουσιοδοτημένα μέλη έχουν πρόσβαση στα δεδομένα. Επιπλέον, η αυτοματοποίηση διαδικασιών μέσω της τεχνολογίας blockchain μπορεί να οδηγήσει σε εξοικονόμηση χρόνου και κόστους για τους υγειονομικούς φορείς, ενώ παράλληλα εξασφαλίζεται η αξιοπιστία και η ιχνηλασιμότητα κάθε βήματος της διαδικασίας.

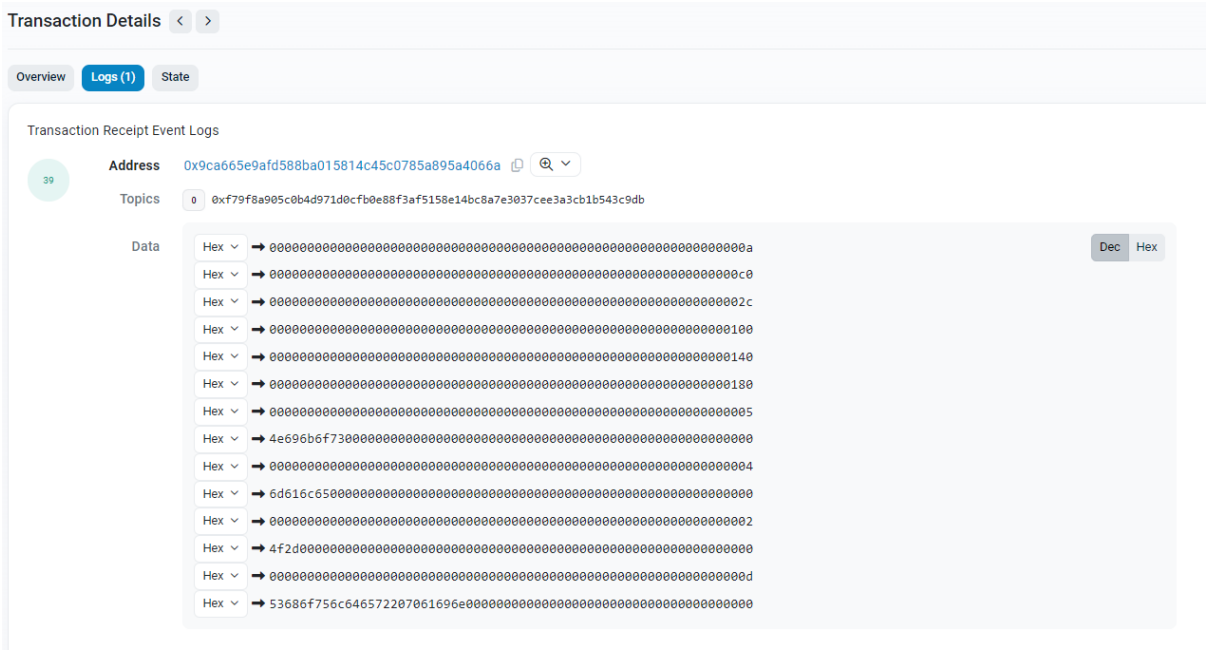
6.2 Επισκόπηση

Το παρόν σύστημα αποτελεί μία βασική εφαρμογή υγειονομικής περίθαλψης. Με την χρήση μιας εντολής ενεργοποιείται ο server και είναι διαθέσιμη η πρόσβαση στην ιστοσελίδα του συστήματος. Αρχικά δίνει την δυνατότητα σύνδεσης και πρόσβασης στην ιστοσελίδα στον Admin καθώς και στους γιατρούς. Ο πρώτος έχει την δυνατότητα εισαγωγής, αφαίρεσης και επεξεργασίας των δεδομένων των γιατρών και των ασθενών. Οι γιατροί από την μεριά τους έχουν την δυνατότητα προβολής των δεδομένων των ασθενών με τους οποίους τους έχει δικαιοδοτήσει ο Admin. Όλα τα παραπάνω πραγματοποιούνται με την χρήση του MetaMask (ψηφιακό πορτοφόλι Ethereum), το οποίο μέσω κάποιων τυπικών συναλλαγών ευθύνεται για την πιστοποίηση της οποιαδήποτε αλλαγής στην πλατφόρμα. Ο Admin, όπως και ο κάθε γιατρός έχουν την δικιά τους ηλεκτρονική ταυτότητα που είναι συνδεδεμένη με το αντίστοιχο πορτοφόλι τους στο MetaMask. Όλα τα δεδομένα είναι κρυπτογραφημένα.

6.3 Πλεονεκτήματα του Εφαρμοζόμενου Συστήματος

Αυξημένη ασφάλεια:

Η κρυπτογραφία αποτελεί έναν βασικό παράγοντα για την ασφάλεια των πληροφοριών. Καθιστά δυσκολότερη την απόσπαση ευαίσθητων δεδομένων από κακόβουλους χρήστες. Όπως φαίνεται στην παρακάτω εικόνα τα στοιχεία του ασθενή που εισήγαγε ο admin είναι όλα κρυπτογραφημένα (Εικόνα 14).



Εικόνα 14. Κρυπτογραφία Δεδομένων

Προστασία της ιδιωτικής ζωής των δεδομένων:

Οι λογαριασμοί μπορούν να εναλλάσσονται από την επέκταση του MetaMask, γεγονός που θα μπορούσε να δώσει πρόσβαση στην μεταβολή των δεδομένων από όλους τους χρήστες. Η ασφάλεια του blockchain όμως, αποτρέπει τέτοιες καταστάσεις επειδή ο κάθε χρήστης έχει τον δικό του μοναδικό λογαριασμό που έχει δεσμευθεί στην αλυσίδα για διαφορετικούς λόγους.

Ενσωμάτωση έξυπνων συμβολαίων:

Η ενσωμάτωση των έξυπνων συμβάσεων μπορεί να μηχανογραφήσει και να διατηρήσει ορισμένες μορφές. Για παράδειγμα, οι έξυπνες συμβάσεις μπορούν να ρομποτικοποιήσουν τη διαδικασία εισαγωγής στην πλατφόρμα, διασφαλίζοντας ότι η πρόσβαση επιτρέπεται ή απορρίπτεται όταν πληρούνται οι προκαθορισμένες προϋποθέσεις.

Διαφάνεια και ιχνηλασιμότητα:

Όλες οι ενέργειες στο σύστημα, από τη μεταφορά δεδομένων έως τις απαιτήσεις και τις εγκρίσεις, καταγράφονται στην αλυσίδα μπλοκ. Αυτό το απλό στοιχείο καταγραφής λειτουργεί ως αμετάβλητη διαδρομή ελέγχου.

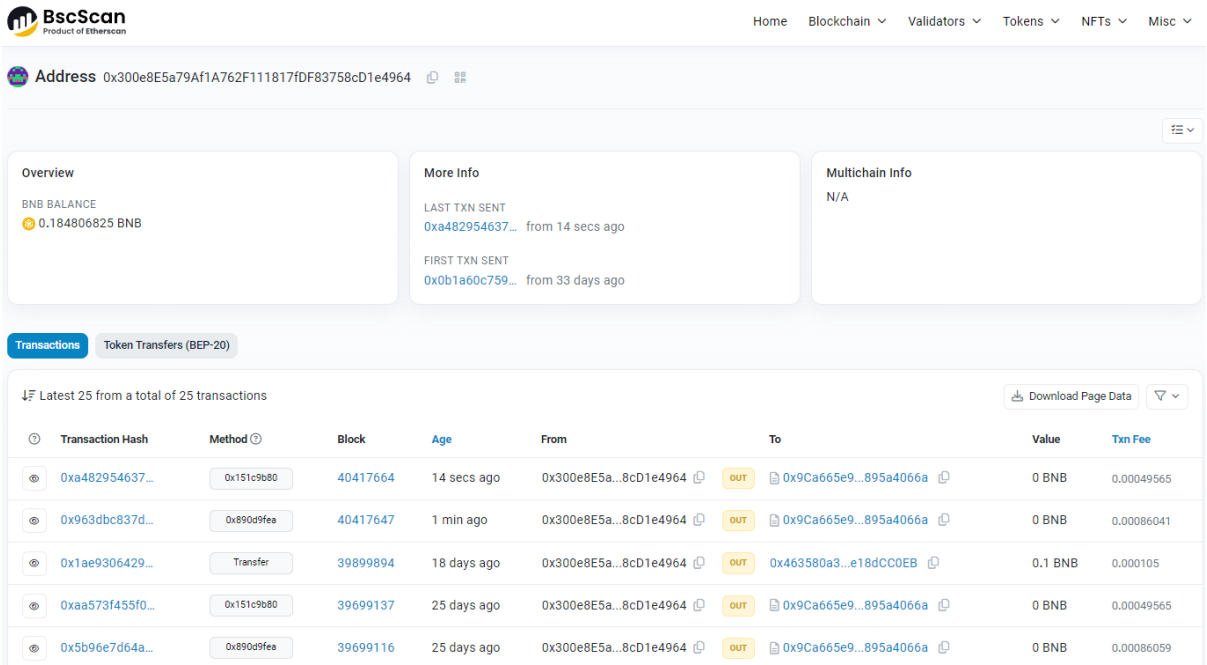
Διαρκής ενίσχυση:

Ο admin έχει τον έλεγχο των πληροφοριών και μπορεί να επιλέξει ποιος μπορεί να έχει πρόσβαση σε αυτές και για ποιους σκοπούς.

Αποτελεσματική διαχείριση δεδομένων:

Ένα από τα βασικά χαρακτηριστικά του blockchain είναι η αμετάβλητη φύση του. Μόλις ένα κομμάτι συμπεριληφθεί στην αλυσίδα, είναι υπολογιστικά αδιανόητο να μεταβληθεί η ουσία ή η διάταξή του. Με τον τρόπο αυτό αποφεύγεται η αλλοίωση αρχείων και διασφαλίζεται η διατήρηση των δεδομένων.

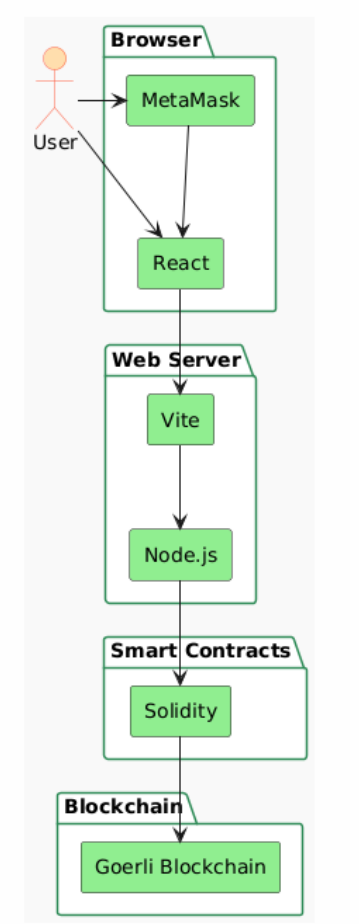
Πηγαίνοντας στο block explorer έχουμε την δυνατότητα να δούμε τα blocks που έχουν δημιουργηθεί, την χρονική στιγμή που έγινε η εξόρυξη τους καθώς και αυτά που μεταβλήθηκε η κατάστασή τους από τις παραπάνω αλλαγές (Εικόνα 27).



Εικόνα 15. Αποτελέσματα Bscscan

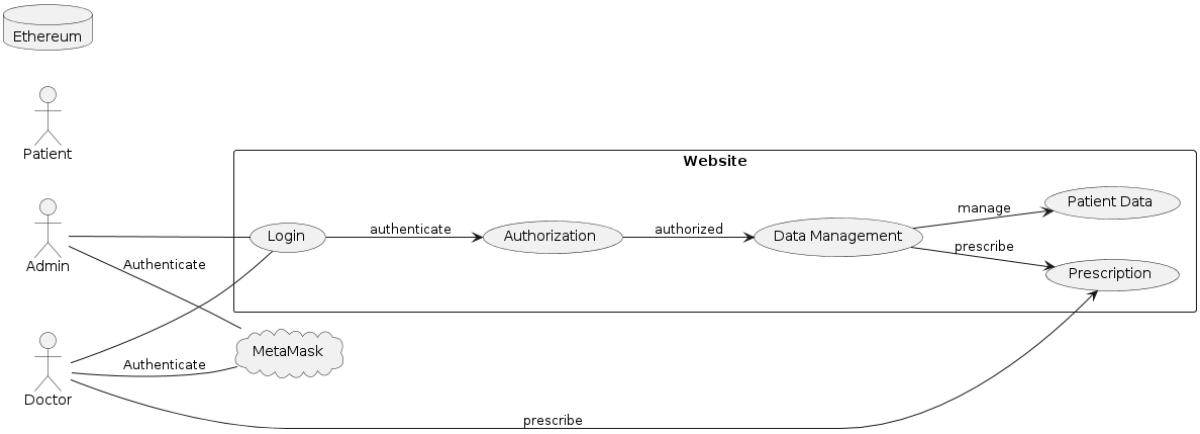
6.4 Αρχιτεκτονική του Συστήματος και Στοιχεία

Διάγραμμα Αρχιτεκτονικής Συστήματος



Εικόνα 16. Αρχιτεκτονική Εφαρμογής

Διάγραμμα Use – Case



Εικόνα 17. Use - Case διάγραμμα

Goerli Blockchain Network

Το παρόν σύστημα είναι βασισμένο στο Goerli blockchain. Το Goerli είναι ένα δοκιμαστικό δίκτυο (testnet) του Ethereum, μιας από τις πιο δημοφιλείς πλατφόρμες blockchain. Το δίκτυο Goerli χρησιμοποιείται για τη δοκιμή εφαρμογών και έξυπνων συμβολαίων χωρίς την ανάγκη πραγματικών Ether (το κρυπτονόμισμα του Ethereum). Αν και το κυρίως δίκτυο του Ethereum είναι το Mainnet, το οποίο χρησιμοποιείται για πραγματικές συναλλαγές και συμβόλαια, το Goerli λειτουργεί ως περιβάλλον δοκιμών.

Οι προγραμματιστές και οι ερευνητές χρησιμοποιούν το Goerli για να δοκιμάσουν και να επικυρώσουν τις εφαρμογές τους χωρίς να χρειάζεται να ξοδέψουν πραγματικά Ether. Επιπλέον, το Goerli δίνει τη δυνατότητα στους προγραμματιστές να εξασκηθούν σε διάφορες λειτουργίες του Ethereum χωρίς τον κίνδυνο απώλειας πραγματικών κεφαλαίων.

Το Goerli έχει την πλεονεκτική ιδιότητα ότι είναι συμβατό με τον Ethereum Virtual Machine (EVM), έτσι ώστε οι εφαρμογές που αναπτύσσονται και δοκιμάζονται σε αυτό το δίκτυο μπορούν να μεταφερθούν με ελάχιστες αλλαγές στο κυρίως δίκτυο του Ethereum. Αυτό το καθιστά ένα χρήσιμο εργαλείο για την ανάπτυξη και τον έλεγχο εφαρμογών πριν από την πραγματική τους υλοποίηση [117].

React

Η React είναι μία ανοιχτού κώδικα JavaScript βιβλιοθήκη για τη δημιουργία διεπαφών χρήστη (UI). Δημιουργήθηκε από την Facebook και έχει καθιερωθεί ως ένα από τα πιο δημοφιλή εργαλεία για την ανάπτυξη ιστοσελίδων και εφαρμογών.

Οι βασικές αρχές του React περιλαμβάνουν:

1. **Συστατικά (Components)**: Το React έχει βασιστεί στην ιδέα της δημιουργίας επαναχρησιμοποιήσιμων συστατικών. Κάθε στοιχείο (component) του React είναι μια μικρή, ανεξάρτητη μονάδα που μπορεί να περιέχει HTML, JavaScript, και CSS.
2. **Εικονικό DOM (Virtual DOM)**: Το React χρησιμοποιεί ένα εικονικό DOM για να βελτιστοποιήσει την απόδοση. Αντί να αλληλεπιδρά με τον πραγματικό DOM κάθε φορά που γίνεται μια αλλαγή, το React ενημερώνει πρώτα το εικονικό DOM και στη συνέχεια αντανακλά τις αλλαγές στον πραγματικό DOM μόνο όταν απαιτείται.
3. **Κατάσταση (State)**: Το React χρησιμοποιεί την έννοια της κατάστασης για τη διαχείριση της κατάστασης της εφαρμογής. Η κατάσταση είναι η πληροφορία που ελέγχει την εμφάνιση και τη συμπεριφορά των στοιχείων.
4. **Δέσμευση (Binding)**: Το React χρησιμοποιεί δέσμευση (binding) για να επιτρέψει τη δυναμική ενημέρωση των στοιχείων όταν η κατάσταση της εφαρμογής αλλάζει. Αυτό επιτρέπει στα στοιχεία να ενημερώνονται αυτόματα όταν αλλάζουν τα δεδομένα.

Με αυτές τις βασικές αρχές, το React προσφέρει ένα ευέλικτο και αποτελεσματικό πλαίσιο για τη δημιουργία δυναμικών και αποτελεσματικών χρήστη-κεντρικών διασταυρώσεων και διεπαφών χρήστη [118].

VITE

Το Vite είναι ένα σύγχρονο εργαλείο ανάπτυξης για την δημιουργία ιστοσελίδων. Είναι σχεδιασμένο ειδικά για την ταχύτερη και πιο αποτελεσματική ανάπτυξη ιστοσελίδων, ιδίως για έργα που χρησιμοποιούν τεχνολογίες όπως το Vue.js και το React.

Ακολουθούν ορισμένα από τα σημαντικότερα χαρακτηριστικά του Vite:

Dev Server: Το Vite διαθέτει έναν πολύ γρήγορο διακομιστή ανάπτυξης που εκμεταλλεύεται τη φυσική υποστήριξη των ES modules σε μοντέρνους περιηγητές. Αυτό επιτρέπει την πολύ γρήγορη αντικατάσταση των μονάδων (hot module replacement - HMR) και τις γρήγορες ενημερώσεις κατά τη διάρκεια της ανάπτυξης.

Build Speed: Ένα από τα κύρια χαρακτηριστικά του Vite είναι οι γρήγοροι χρόνοι κατασκευής. Αυτό επιτυγχάνεται εκμεταλλευόμενος τα ES modules και μεταγλωττίζοντας μόνο τα συγκεκριμένα modules που χρειάζονται για το έργο, αντί για τη συνολική δέσμευση του έργου όπως συμβαίνει με παραδοσιακούς bundlers όπως το webpack.

Plugin System: Το Vite προσφέρει ένα ευέλικτο σύστημα προσθέτων που επιτρέπει στους προγραμματιστές να επεκτείνουν τη λειτουργικότητά του κατά τις ανάγκες τους. Αυτό επιτρέπει την ομαλή ενσωμάτωση με διάφορα εργαλεία, προεπεξεργαστές και πλαίσια εργασίας.

Vue.js and React Support: Παρόλο που το Vite είναι συμβατό με οποιοδήποτε πλαίσιο ή βιβλιοθήκη frontend, είναι ιδιαίτερα καλό σε έργα που χρησιμοποιούν Vue.js και React. Παρέχει προεπισκοπήσεις για αυτά τα πλαίσια, διευκολύνοντας τη γρήγορη εγκατάσταση και ανάπτυξη.

Zero-config Setup: Παρέχει την δυνατότητα να ξεκινήσει κάποιος αμέσως τη δουλειά του χωρίς να χρειάζεται να σπαταλήσει χρόνο για να ρυθμίσει το περιβάλλον και τα εργαλεία κατασκευής. Αυτό επιταχύνει τη διαδικασία ανάπτυξης για τους προγραμματιστές.

ESBuild Integration: Το Vite κάνει χρήση του ESBuild, ενός JavaScript bundler γραμμένο σε Go που είναι απίστευτα γρήγορο. Το Vite δομείται γρήγορα σε μεγάλο βαθμό λόγω της ταχύτητας του ESBuild.

Optimized Production Builds: Το Vite παράγει βελτιστοποιημένα builds παραγωγής εκτός από τα γρήγορα builds ανάπτυξης. Οι web εφαρμογές θα φορτώνονται γρήγορα και αποτελεσματικά στο πρόγραμμα περιήγησης χάρη στη βελτιστοποίηση επιδόσεων, τη συμπίεση και την ελαχιστοποίηση που παρέχουν αυτά τα builds.

Συνολικά, το Vite είναι ένα αποτελεσματικό εργαλείο για τη σύγχρονη ανάπτυξη frontend, παρέχοντας ταχύτητα, αποτελεσματικότητα και δυνατότητες που είναι εύχρηστες για τους προγραμματιστές και επιταχύνουν τη διαδικασία ανάπτυξης. Αποτελεί μια πολύ αγαπητή επιλογή μεταξύ των προγραμματιστών frontend λόγω της έμφασής του στη χρήση των εγγενών δυνατοτήτων του προγράμματος περιήγησης και στον εξορθολογισμό των διαδικασιών ανάπτυξης [119].

Ganache

Το Ganache είναι ένα εργαλείο που χρησιμοποιείται για την ανάπτυξη και δοκιμή εφαρμογών blockchain βασισμένων στο Ethereum. Αρχικά δημιουργήθηκε από την Truffle Suite και προσφέρει ένα τοπικό blockchain που μπορεί να χρησιμοποιηθεί για την ανάπτυξη και δοκιμή έξυπνων συμβολαίων (smart contracts) και εφαρμογών χωρίς την ανάγκη πραγματικού Ether. Αυτό καθιστά τη διαδικασία ανάπτυξης πιο ευέλικτη και γρήγορη, καθώς μπορεί ο χρήστης να δοκιμάζει και να επαναλαμβάνει την ανάπτυξη του χωρίς να χρειάζεται να δαπανήσει πραγματικά Ether. Επιπλέον, το Ganache παρέχει εργαλεία για τη διαχείριση των συναλλαγών, των λογαριασμών και των μπλοκ του τοπικού blockchain. Στην περίπτωσή μας χρησιμοποιήθηκε για την δημιουργία των λογαριασμών στο MetaMask, οι οποίοι λογαριασμοί εισάχθηκαν με την χρήση των ιδιωτικών κλειδιών τους [120].

Metamask

Το MetaMask είναι μια από τις πιο δημοφιλείς και ευρέως χρησιμοποιούμενες επεκτάσεις προγραμματισμού περιήγησης (browser extensions) για το Ethereum blockchain. Αποτελεί ένα ψηφιακό πορτοφόλι (wallet) που επιτρέπει στους χρήστες να διαχειρίζονται τα Ether (ETH) και τα Ethereum-based tokens τους, καθώς και να αλληλεπιδρούν με ιστοσελίδες που υποστηρίζουν το Ethereum blockchain.

Ορισμένα κύρια χαρακτηριστικά του MetaMask περιλαμβάνουν:

- **Ψηφιακό Πορτοφόλι Ethereum**: Το MetaMask λειτουργεί ως ένα ηλεκτρονικό πορτοφόλι όπου οι χρήστες μπορούν να αποθηκεύουν τα ETH και τα Ethereum-based tokens τους.
- **Επικοινωνία με dApps**: Το MetaMask επιτρέπει στους χρήστες να αλληλεπιδρούν με αποκεντρωμένες εφαρμογές (dApps) που βασίζονται στο Ethereum blockchain από το πρόγραμμα περιήγησης τους, όπως το Chrome ή το Firefox.
- **Υπογραφή Συναλλαγών**: Το MetaMask επιτρέπει στους χρήστες να υπογράφουν και να αποστέλλουν συναλλαγές στο Ethereum blockchain.
- **Δημιουργία Νέων Πορτοφολιών**: Οι χρήστες μπορούν να δημιουργήσουν νέα πορτοφόλια Ethereum απευθείας από το MetaMask.
- **Επέκταση λειτουργιών μέσω Plugins**: Το MetaMask υποστηρίζει πρόσθετα (plugins) που επεκτείνουν τις λειτουργίες του, όπως η ολοκλήρωση επιπλέον ασφαλείας και η πρόσθετη δυνατότητα διαχείρισης.

Συνολικά, το MetaMask είναι ένα πολύ χρήσιμο εργαλείο για τους χρήστες που ασχολούνται με το Ethereum blockchain, καθώς τους επιτρέπει να διαχειρίζονται τα κρυπτονομίσματά τους και να αλληλεπιδρούν με διάφορες εφαρμογές και υπηρεσίες [121].

Solidity

Είναι μία γλώσσα προγραμματισμού που χρησιμοποιείται για την ανάπτυξη έξυπνων συμβολαίων (smart contracts) στο blockchain του Ethereum και άλλων πλατφορμών. Είναι σχεδιασμένη για να είναι σχετικά εύκολη στην εκμάθηση και να παρέχει ισχυρές δυνατότητες για τον προγραμματισμό έξυπνων συμβολαίων.

Η Solidity είναι μία γλώσσα με συντακτική ομοιότητα με την JavaScript, κάτι που καθιστά ευκολότερη τη μετάβαση για προγραμματιστές που είναι ήδη εξοικειωμένοι με αυτήν. Ωστόσο, υπάρχουν ορισμένες σημαντικές διαφορές και προσθήκες που η Solidity προσφέρει για την ανάπτυξη έξυπνων συμβολαίων, όπως τη δυνατότητα αναγκαστικής εξόδου από συμβόλαια (self-destruct) και τη δυνατότητα να επικοινωνεί με άλλα συμβόλαια μέσω των διεπαφών (interfaces).

Η Solidity έχει κερδίσει μεγάλη δημοτικότητα λόγω της ευελιξίας της και της ευκολίας χρήσης της στην ανάπτυξη έξυπνων συμβολαίων για το Ethereum και άλλα blockchain [122].

BscScan

Το BscScan είναι ένας εξειδικευμένος εξερευνητής blockchain για το Binance Smart Chain (BSC). Δημιουργήθηκε από την ίδια ομάδα που ανέπτυξε το Etherscan, τον πιο δημοφιλή εξερευνητή blockchain για το Ethereum.

Ακολουθούν μερικά από τα κύρια χαρακτηριστικά του BscScan:

- Παρακολούθηση Συναλλαγών:

  Παρέχει λεπτομερείς πληροφορίες για κάθε συναλλαγή που γίνεται στο Binance Smart Chain. Αυτές οι πληροφορίες περιλαμβάνουν τη διεύθυνση αποστολέα και παραλήπτη, το ποσό, τις χρεώσεις αερίου και το status της συναλλαγής.

- Αναζήτηση Διευθύνσεων:

  Επιτρέπει στους χρήστες να αναζητούν διευθύνσεις πορτοφολιών για να δουν τα υπόλοιπά τους, τις συναλλαγές που έχουν πραγματοποιήσει και άλλα σχετικά δεδομένα.

- Εξερεύνηση Συμβολαίων:

  Οι χρήστες μπορούν να δουν και να αλληλεπιδράσουν με έξυπνα συμβόλαια, να δουν τον κώδικα τους και να ελέγξουν τη δραστηριότητα τους.

- Στατιστικά Δεδομένα και Αναλύσεις:

  Προσφέρει διάφορα στατιστικά δεδομένα, όπως το συνολικό αριθμό συναλλαγών, τη δραστηριότητα των κόμβων, την κατανάλωση αερίου και άλλα σημαντικά στατιστικά.

- Κατάλογος για τα Token:

  Περιέχει μια πλήρη λίστα όλων των token που είναι διαθέσιμα στο BSC, με λεπτομερείς πληροφορίες για κάθε token, συμπεριλαμβανομένων των συμβόλων τους, της κεφαλαιοποίησης και των κατόχων τους.

- Επικυρωποίηση Συμβολαίων:

  Επιτρέπει στους προγραμματιστές να επαληθεύουν και να δημοσιεύουν τον κώδικα των έξυπνων συμβολαίων τους, καθιστώντας τα ευκολότερα στη χρήση από τους χρήστες.

Χρήσεις του BscScan

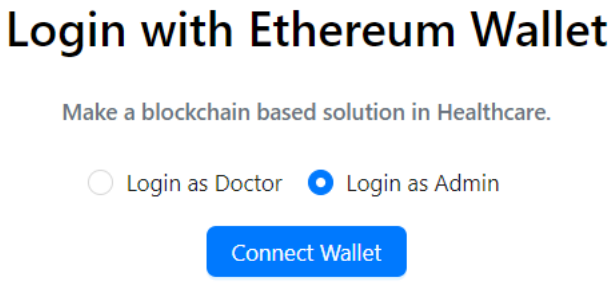
- Επενδυτές: Μπορούν να παρακολουθούν τις κινήσεις των κεφαλαίων τους και να εξετάζουν τις δραστηριότητες των token στα οποία επενδύουν.
- Προγραμματιστές: Χρησιμοποιούν το BscScan για να ελέγχουν την απόδοση των έξυπνων συμβολαίων τους.
- Χρήστες: Ελέγχουν τις συναλλαγές τους και διασφαλίζουν την επιτυχία τους.

Το BscScan είναι ένα απαραίτητο εργαλείο για όσους ασχολούνται με το Binance Smart Chain, είτε είναι προγραμματιστές, επενδυτές ή καθημερινοί χρήστες. Παρέχει τα απαραίτητα εργαλεία για να διαχειρίζεται κανείς αποτελεσματικά τις δραστηριότητες του στο blockchain [123].

6.5 Use – Case Σεναριο

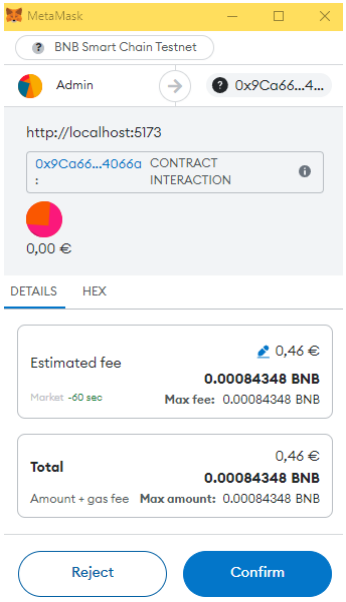
Αρχικά ενεργοποιούμε τον σέρβερ για να μπορούμε να αποκτήσουμε την δυνατότητα σύνδεσης στην πλατφόρμα. Στην συνέχεια συνδέεται ο admin μέσω του MetaMask χρησιμοποιώντας τον δικό του μοναδικό λογαριασμό. Στην αρχική σελίδα έχει την δυνατότητα πρόσθεσης ή αφαίρεσης ασθενών και γιατρών. Σε πρώτη φάση προσθέτει έναν ασθενή και έπειτα έναν γιατρό. Στο επόμενο βήμα συνδέει τον ασθενή με τον ενδιαφερόμενο γιατρό για να του δώσει πρόσβαση στην καρτέλα του. Ο γιατρός από την μεριά του συνδέεται στην πλατφόρμα με τον ίδιο τρόπο όπως ακριβώς ο admin και μπορεί στην αρχική του σελίδα να δει όλους τους καταχωρημένους σε αυτόν ασθενείς. Επιλέγει αυτόν που εκείνη την στιγμή τον ενδιαφέρει και του προσάπτει συνταγή. Τέλος βλέπει την καρτέλα του ασθενή με τα στοιχεία του. Όλες οι παραπάνω ενέργειες γίνονται με την πιστοποίηση του MetaMask.

Ενεργοποιώντας τον σέρβερ δίνεται η δυνατότητα σύνδεσης στην πλατφόρμα. Από κει και πέρα ο χρήστης μπορεί να πραγματοποιήσει σύνδεση ως γιατρός ή ως admin (Εικόνα 18).



Εικόνα 18. Φόρμα Σύνδεσης

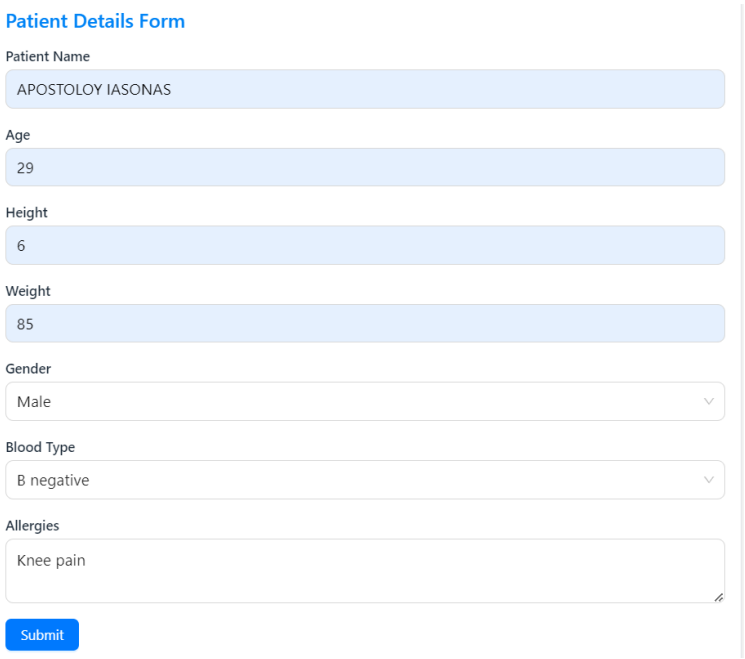
Ο Admin πραγματοποιεί σύνδεση. Εκείνη την στιγμή εμφανίζεται το παράθυρο του MetaMask για την είσοδο του στο σύστημα (Εικόνα 19). Θα εγκριθεί η είσοδος πραγματοποιώντας μια μηδαμινή συναλλαγή (entry fee) για την πιστοποίηση και την καταγραφή της ενέργειας στην αλυσίδα.



Εικόνα 19. MetaMask Interaction

Ο Admin μπορεί να είναι μόνο ένας. Στην προκειμένη περίπτωση είναι ο χρήστης με την διεύθυνση 0x300e8E5a79Af1A762F111817fDF83758cD1e4964 στο MetaMask. Αυτό το γεγονός δίνει την δυνατότητα στον Admin να έχει πρόσβαση στα δεδομένα της ιστοσελίδας.

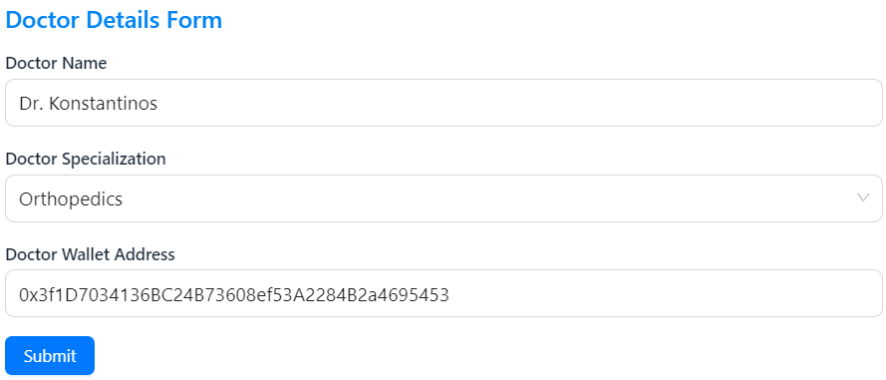
Ο Admin έχει την δυνατότητα εισαγωγής ασθενών και γιατρών. Συμπληρώνεται η φόρμα από τον ίδιο για την καταχώρηση του ασθενή στο σύστημα (Εικόνα 20).



Εικόνα 20. Φόρμα Ασθενών

Για την πραγματοποίηση οποιασδήποτε ενέργειας ενεργοποιείται το MetaMask όπως παρουσιάστηκε παραπάνω.

Με τον ίδιο τρόπο εισάγει τον ενδιαφερόμενο ιατρό (Εικόνα 21).



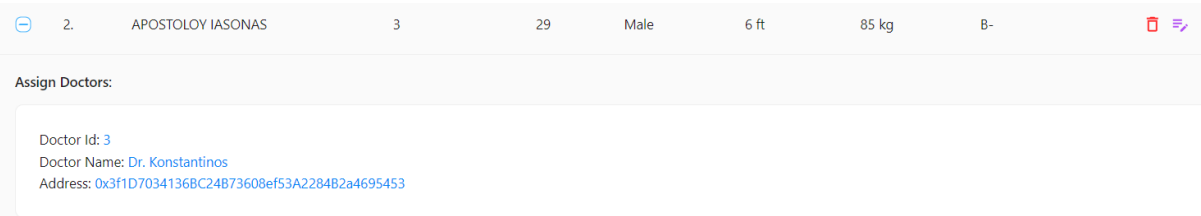
Εικόνα 21. Φόρμα Γιατρών

Εφόσον ενημερώθηκε η πλατφόρμα με τις επιθυμητές εγγραφές μπορεί ο Admin να τις δει στην αρχική σελίδα (Εικόνα 22,23).

Εικόνα 22. Πληροφορίες Ασθενούς

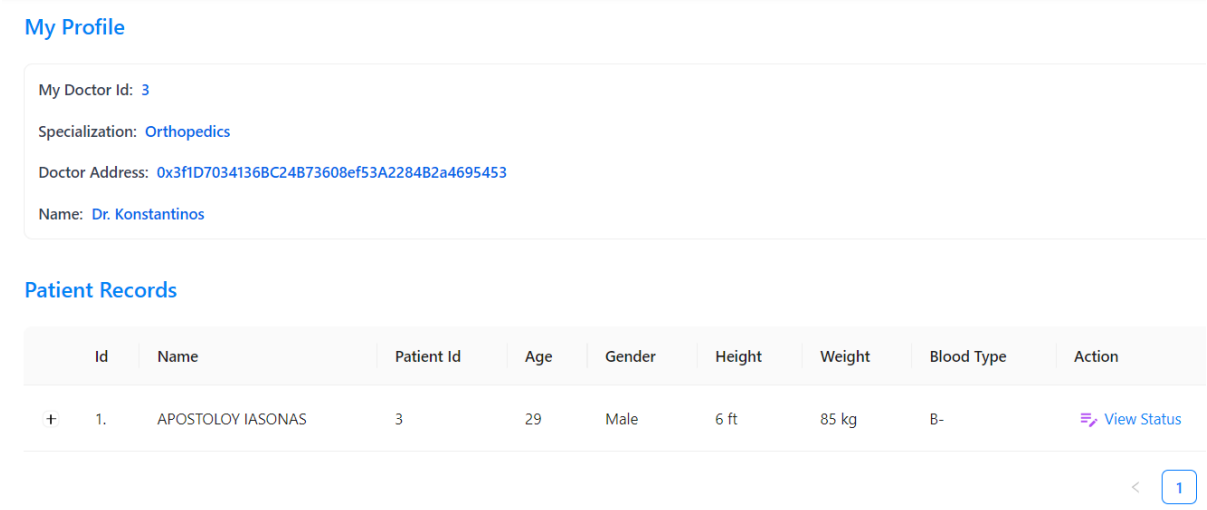
Εικόνα 23. Πληροφορίες Γιατρού

Στη συνέχεια δεσμεύει τον κατάλληλο γιατρό με τον ασθενή (Εικόνα 24). Το παράθυρο του MetaMask εμφανίζεται ξανά, όπως και σε οποιαδήποτε άλλη ενέργεια που έχει σκοπό να προκαλέσει αλλαγή στην αλυσίδα.



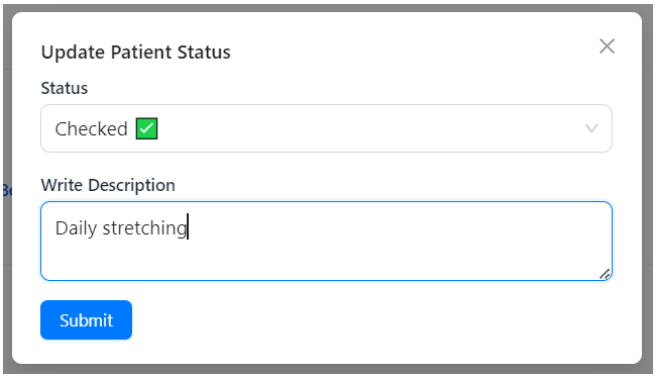
Εικόνα 24. Δέσμευση Ασθενή - Γιατρού

Από την μεριά του ο γιατρός συνδέεται στην πλατφόρμα με τον ίδιο ακριβώς τρόπο όπως και ο Admin και έχει την δυνατότητα να δει τους ασθενείς που έχει δεσμευτεί (Εικόνα 25).



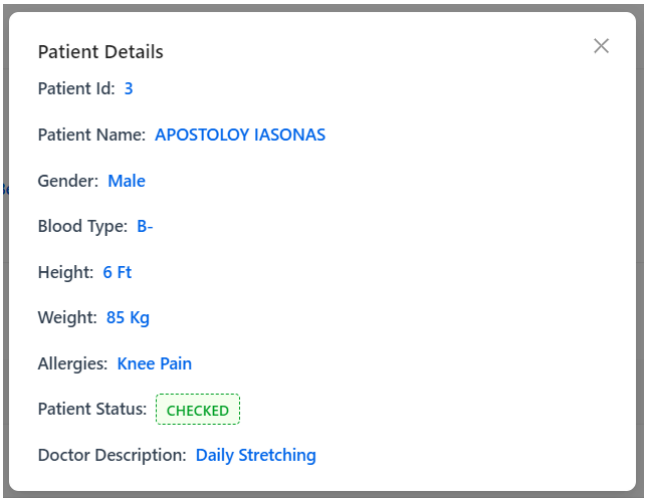
Εικόνα 25. Προφίλ Γιατρού

Έπειτα μπορεί να ενημερώσει την κατάσταση του εκάστοτε ασθενή και να χορηγήσει την ανάλογη συνταγή (Εικόνα 26).



Εικόνα 26. Ενημέρωση Κατάστασης Ασθενή

Εφόσον πραγματοποιήσει το παραπάνω βήμα, ο γιατρός έχει το δικαίωμα να δει την καρτέλα του κάθε ασθενή που του έχει ανατεθεί (Εικόνα 27).



Εικόνα 27. Στοιχεία Ασθενή

6.6 Συμπερασματα και Μελοντικες Εξελιξεις

Το σύστημα υγειονομικής περίθαλψης με βάση την αλυσίδα μπλοκ που παρουσιάζεται εδώ αντιπροσωπεύει τις δυνατότητες της τεχνολογίας να φέρει επανάσταση στη διαχείριση των πληροφοριών υγειονομικής περίθαλψης. Το σύστημα αντιμετωπίζει βασικές προκλήσεις στα πλαίσια δεδομένων ευεξίας, παρέχοντας ασφάλεια πληροφοριών, μόνιμη συγκατάθεση και απλή τήρηση αρχείων. Ενώ το μοντέλο δείχνει τη θεμελιώδη χρησιμότητα, η πραγματική εκτέλεση θα απαιτήσει ευρεία μέτρα ασφαλείας, ρυθμίσεις ευελιξίας και σχέδιο με επίκεντρο τον χρήστη. Με την ευκαιρία, η εφαρμογή της αλυσίδας μπλοκ στην υγειονομική περίθαλψη αποτελεί εγγύηση για ένα πιο ασφαλές, απλό και ασθενοκεντρικό περιβάλλον.

Επεκτασιμότητα

Καθώς αυξάνεται ο αριθμός των ασθενών και των αρχείων, ενδέχεται να προκύψουν ζητήματα ευελιξίας. Μπορούν να εξεταστούν ρυθμίσεις όπως η κατανομή και η χωρητικότητα εκτός αλυσίδας.

Εμπειρία χρήστη

Η προσθήκη εισόδου από την μεριά του ασθενή στο σύστημα θα είναι ένα αρκετά μεγάλο βήμα για την εξέλιξη της πλατφόρμας. Θα βοηθήσει στην πιο άμεση επικοινωνία μεταξύ ασθενή και γιατρού.

Μηχανισμοί συναίνεσης

Είναι σημαντικό να εξασφαλιστεί ότι οι ασθενείς μπορούν να επιβλέπουν τα δεδομένα που κατέχουν. Η διαφανής επικοινωνία με τους ασθενείς σχετικά με τη χρήση, την ικανότητα και την πρόσβαση στα δεδομένα τους είναι σημαντική. Οι ασθενείς πρέπει να ενημερώνονται πλήρως σχετικά με τον τρόπο με τον οποίο χρησιμοποιούνται τα δεδομένα τους. Θα πρέπει να δοθεί έμφαση στη συγκατάθεση των ασθενών έτσι ώστε να εγγυάται ότι η πρόσβαση σε ευαίσθητα αρχεία επιτρέπεται. Αυτή η

προσέγγιση προωθεί την πίστη μεταξύ ασθενών και προμηθευτών υγειονομικής περίθαλψης, η οποία είναι βασική για την εκτενέστερη εκτέλεση του συστήματος.

Ενσωμάτωση με προηγμένες τεχνολογίες

Τεχνητή νοημοσύνη (AI) και μηχανική μάθηση (ML):

Η ενσωμάτωση της αλυσίδας μπλοκ με τις τεχνολογίες AI και ML θα ανοίξει δυνατότητες ανάλυσης με πρόβλεψη στην υγειονομική περίθαλψη. Αναλύοντας σχέδια και μοτίβα στα αποθηκευμένα δεδομένα ασθενών, οι αλγόριθμοι της ΤΝ μπορούν να δώσουν γνώσεις σχετικά με πιθανούς κινδύνους για την υγεία, διάφορες θεραπείες και εξατομικευμένες προσεγγίσεις υγειονομικής περίθαλψης. Η αποκεντρωμένη και ασφαλής φύση της αλυσίδας μπλοκ εγγυάται τη διασφάλιση και την ανωνυμία των ευαίσθητων πληροφοριών που χρησιμοποιούνται για τέτοιου είδους αναλύσεις.

Web of Restorative Things (IoMT):

Με την επέκταση των gadgets IoMT (wearables, περαιτέρω gadgets ελέγχου), το σύνολο των πληροφοριών όσον αφορά τις θεραπείες των ασθενών που δημιουργούνται αναπτύσσεται εκθετικά. Η αποκεντρωμένη μηχανική της αλυσίδας μπλοκ ενθαρρύνει το ασφαλές και αποτελεσματικό εμπόριο πληροφοριών μεταξύ αυτών των συσκευών και δίνει τη δυνατότητα παρατήρησης σε πραγματικό χρόνο χωρίς να διακινδυνεύεται η απώλεια των πληροφοριών.

Συμπεράσματα

Συνοψίζοντας, το παρόν σύστημα υγειονομικής περίθαλψης παρέχει ένα σύγχρονο και ασφαλές πλαίσιο για τη διαχείριση ιατρικών δεδομένων μέσω της χρήσης blockchain τεχνολογίας και ψηφιακών πορτοφολιών MetaMask. Οι βασικές λειτουργίες του περιλαμβάνουν την εισαγωγή, αφαίρεση, και επεξεργασία δεδομένων από τον διαχειριστή (Admin) και την προβολή των δεδομένων από τους γιατρούς, διασφαλίζοντας την προστασία και την ιδιωτικότητα των ασθενών.

Η χρήση του MetaMask εξασφαλίζει την αυθεντικότητα και την ασφάλεια των συναλλαγών μέσω της blockchain, επιτρέποντας την πιστοποίηση οποιασδήποτε αλλαγής στην πλατφόρμα. Ο κάθε χρήστης του συστήματος διαθέτει μια μοναδική ηλεκτρονική ταυτότητα, συνδεδεμένη με το αντίστοιχο ψηφιακό πορτοφόλι του, διασφαλίζοντας ότι μόνο εξουσιοδοτημένα άτομα έχουν πρόσβαση στα δεδομένα.

Η υλοποίηση αυτή δεν αυξάνει μόνο την ασφάλεια αλλά και την ευκολία στην διαχείριση των ιατρικών αρχείων, ενώ παράλληλα μειώνει τις γραφειοκρατικές διαδικασίες. Το σύστημα προσφέρει ευκολία στην εκκίνηση και στην χρήση της πλατφόρμας.

Συνολικά, το σύστημα ενσωματώνει τις τελευταίες τεχνολογικές καινοτομίες για την βελτίωση της αποδοτικότητας και της ασφάλειας στην υγειονομική περίθαλψη, επιτρέποντας στους διαχειριστές και στους γιατρούς να επικεντρωθούν στη βελτίωση της φροντίδας των ασθενών με μεγαλύτερη ασφάλεια και αποτελεσματικότητα.

ΚΕΦΑΛΑΙΟ 7: Επίλογος

Ολοκληρώνοντας την παρούσα διπλωματική εργασία, γίνεται εμφανές ότι η τεχνολογία blockchain έχει τη δυνατότητα να φέρει επανάσταση στον τομέα της υγειονομικής περίθαλψης. Στόχος ήταν η εκτενή κάλυψη των βασικών αρχών και των χαρακτηριστικών του blockchain, των διαδικασιών των συναλλαγών, των αλγορίθμων συναίνεσης, και των διαφόρων εφαρμογών του στην υγεία.

Συγκεκριμένα, η τεχνολογία blockchain προσφέρει σημαντικά πλεονεκτήματα, όπως η ασφάλεια και η διαφάνεια των δεδομένων, η προστασία της ιδιωτικότητας και η δυνατότητα για αποκεντρωμένη διαχείριση των ιατρικών αρχείων. Επιπλέον, οι εφαρμογές blockchain στην υγειονομική περίθαλψη μπορούν να συμβάλουν στην καλύτερη διαχείριση των δεδομένων, στη μείωση των λαθών και στη βελτίωση της αποτελεσματικότητας των υπηρεσιών υγείας.

Οι εφαρμογές του blockchain στην υγειονομική περίθαλψη περιλαμβάνουν την καταγραφή των ηλεκτρονικών αρχείων υγείας (EHRs), την εξασφάλιση της διαλειτουργικότητας και της κοινής χρήσης δεδομένων μεταξύ διαφορετικών συστημάτων υγείας, καθώς και τη διασφάλιση της αυθεντικότητας και της ακεραιότητας των κλινικών δοκιμών και των φαρμακευτικών προϊόντων. Αυτές οι δυνατότητες ενισχύουν την εμπιστοσύνη των ασθενών και των επαγγελματιών υγείας στο σύστημα υγειονομικής περίθαλψης και προσφέρουν μια πιο συντονισμένη και ολοκληρωμένη προσέγγιση στη φροντίδα των ασθενών.

Ωστόσο, παρά τα πλεονεκτήματα αυτά, η τεχνολογία αντιμετωπίζει αρκετές προκλήσεις, όπως η ανάγκη για τυποποίηση, η διαχείριση της χωρητικότητας αποθήκευσης και οι κοινωνικές αντιστάσεις στην υιοθέτηση νέων τεχνολογιών. Ειδικά στον τομέα της υγειονομικής περίθαλψης, η υιοθέτηση του blockchain απαιτεί σημαντικές αλλαγές στις υπάρχουσες διαδικασίες και στη νομοθεσία. Οι προκλήσεις αυτές περιλαμβάνουν την ανάγκη για εκπαίδευση των επαγγελματιών υγείας και των διαχειριστών συστημάτων πληροφορικής, καθώς και την ανάπτυξη ολοκληρωμένων και εύχρηστων εφαρμογών που θα επιτρέπουν την εύκολη ενσωμάτωση του blockchain στις καθημερινές εργασίες.

Συνοψίζοντας, η ενσωμάτωση της τεχνολογίας blockchain στον τομέα της υγείας έχει τη δυνατότητα να προσφέρει μια πιο ασφαλή, αποτελεσματική και διαφανή διαχείριση των ιατρικών δεδομένων. Παρόλο που υπάρχουν σημαντικές προκλήσεις που πρέπει να αντιμετωπιστούν, οι προοπτικές που ανοίγονται είναι εξαιρετικά ενθαρρυντικές για το μέλλον της υγειονομικής περίθαλψης. Με τη σωστή υποστήριξη και την κατάλληλη προσαρμογή, το blockchain μπορεί να αποτελέσει το θεμέλιο για την ανάπτυξη ενός πιο βιώσιμου και αξιόπιστου συστήματος υγείας, που θα εξυπηρετεί καλύτερα τις ανάγκες των ασθενών και των επαγγελματιών υγείας.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Aste, T., Tasca, P., & Di Matteo, T. (2017). Blockchain technologies: The foreseeable impact on society and industry. *computer*, *50*(9), 18-28..

[2] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

[3] Salah, K., Rehman, M. H. U., Nizamuddin, N., & Al-Fuqaha, A. (2019). Blockchain for AI: Review and open research challenges. IEEE access, 7, 10127-10149.

[4] Litke, A., Anagnostopoulos, D., & Varvarigou, T. (2019). Blockchains for supply chain management: Architectural elements and challenges towards a global scale deployment. *Logistics*, *3*(1), 5.

[5] Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International journal of web and grid services*, *14*(4), 352-375.

[6] Bano, S., Al-Bassam, M., & Danezis, G. (2017). The road to scalable blockchain designs. *USENIX; login: magazine*, *42*(4), 31-36.

[7] Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., & Capkun, S. (2016, October). On the security and performance of proof of work blockchains. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security* (pp. 3-16).

[8] Gervais, A., Karame, G. O., Capkun, V., & Capkun, S. (2014). Is bitcoin a decentralized currency?. *IEEE security & privacy*, *12*(3), 54-60.

[9] Taskinsoy, J. (2019). Blockchain: a misunderstood digital revolution. Things you need to know about blockchain. *Things You Need to Know about Blockchain (October 8, 2019)*.

[10] Biryukov, A., Khovratovich, D., & Pustogarov, I. (2014, November). Deanonymisation of clients in Bitcoin P2P network. In *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security* (pp. 15-29).

[11] Wang, W., Hoang, D. T., Hu, P., Xiong, Z., Niyato, D., Wang, P., ... & Kim, D. I. (2019). A survey on consensus mechanisms and mining strategy management in blockchain networks. *Ieee Access*, *7*, 22328-22370.

[12] King, S., & Nadal, S. (2012). Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. *self-published paper, August*, *19*(1).

[13] Heilman, E. (2014). One weird trick to stop selfish miners: Fresh bitcoins, a solution for the honest miner. In *Financial Cryptography and Data Security: FC 2014 Workshops, BITCOIN and WAHC 2014, Christ Church, Barbados, March 7, 2014, Revised Selected Papers 18* (pp. 161-162). Springer Berlin Heidelberg.

[14] Kiviat, T. I. (2015). Beyond bitcoin: Issues in regulating blockchain tranactions. *Duke LJ*, *65*, 569.

[15] T. Lundqvist, A. de Blanche, and H. R. H. Andersson, ‘‘Thingto-thing electricity micro payments using blockchain technology,’’ in Proc. Global Internet of Things Summit (GIoTS), 2017, pp. 1–6.

[16] Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *IEEE access*, *4*, 2292-2303.

[17] Sullivan, C., & Burger, E. (2017). E-residency and blockchain. *computer law & security review*, *33*(4), 470-481.

[18] Santos, R., Bennett, K., & Lee, E. (2021). Blockchain: Understanding its uses and implications. *The Linux Foundation*.

[19] Andreas, M., & Antonopoulos, M. (2017). Mastering Bitcoin: Programming the Open Blockchain.

[20] Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Communications Surveys & Tutorials*, *18*(3), 2084-2123.

[21] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE international congress on big data (BigData congress)* (pp. 557-564). Ieee.

[22] Glaser, F. (2017). Pervasive decentralisation of digital infrastructures: a framework for blockchain enabled system and use case analysis.

[23] O'Dwyer, K. J., & Malone, D. (2014). Bitcoin mining and its energy footprint.

[24] Manimuthu, A., Rejikumar, G., & Marwaha, D. (2019). A literature review on Bitcoin: Transformation of crypto currency into a global phenomenon. *IEEE Engineering Management Review*, *47*(1), 28-35.

[25] Karame, G. O., & Androulaki, E. (2016). *Bitcoin and blockchain security*. Artech House.

[26] Y. Yuan and F.-Y. Wang, ``Blockchain and cryptocurrencies: Model, techniques, and applications,'' IEEE Trans. Syst. Man, Cybern., Syst., vol. 48, no. 9, pp. 14211428, Sep. 2018.

[27] Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016, May). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In *2016 IEEE symposium on security and privacy (SP)* (pp. 839-858). IEEE.

[28] Valdivia, L. J., Del-Valle-Soto, C., Rodriguez, J., & Alcaraz, M. (2019). Decentralization: The failed promise of cryptocurrencies. *IT Professional*, *21*(2), 33-40.

[29] Decker, C., & Wattenhofer, R. (2013, September). Information propagation in the bitcoin network. In *IEEE P2P 2013 Proceedings* (pp. 1-10). IEEE.

[30] Delgado-Segura, S., Pérez-Sola, C., Navarro-Arribas, G., & Herrera-Joancomartí, J. (2019). Analysis of the bitcoin utxo set. In *Financial Cryptography and Data Security: FC 2018 International Workshops, BITCOIN, VOTING, and WTSC, Nieuwpoort, Curaçao, March 2, 2018, Revised Selected Papers 22* (pp. 78-91). Springer Berlin Heidelberg.

[31] Schrijvers, O., Bonneau, J., Boneh, D., & Roughgarden, T. (2017). Incentive compatibility of bitcoin mining pool reward functions. In *Financial Cryptography and Data Security: 20th International Conference, FC 2016, Christ Church, Barbados, February 22–26, 2016, Revised Selected Papers 20* (pp. 477-498). Springer Berlin Heidelberg.

[32] Ahamad, S., Nair, M., & Varghese, B. (2013, December). A survey on crypto currencies. In *4th International Conference on Advances in Computer Science, AETACS* (pp. 42-48). Citeseer.

[33] Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, *151*(2014), 1-32.

[34] Vujičić, D., Jagodić, D., & Ranđić, S. (2018, March). Blockchain technology, bitcoin, and Ethereum: A brief overview. In *2018 17th international symposium infoteh-jahorina (infoteh)* (pp. 1-6). IEEE.

[35] Macrinici, D., Cartofeanu, C., & Gao, S. (2018). Smart contract applications within blockchain technology: A systematic mapping study. *Telematics and Informatics*, *35*(8), 2337-2354.

[36] Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A survey of attacks on ethereum smart contracts (sok). In *Principles of Security and Trust: 6th International Conference, POST 2017, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2017, Uppsala, Sweden, April 22-29, 2017, Proceedings 6* (pp. 164-186). Springer Berlin Heidelberg.

[37] Mohanta, B. K., Panda, S. S., & Jena, D. (2018, July). An overview of smart contract and use cases in blockchain technology. In *2018 9th international conference on computing, communication and networking technologies (ICCCNT)* (pp. 1-4). IEEE.

[38] Ritz, F., & Zugenmaier, A. (2018, April). The impact of uncle rewards on selfish mining in ethereum. In *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 50-57). IEEE.

[39] Lamport, L., Shostak, R., & Pease, M. (2019). The Byzantine generals problem. In *Concurrency: the works of leslie lamport* (pp. 203-226).

[40] Saleh, F. (2021). Blockchain without waste: Proof-of-stake. *The Review of financial studies*, *34*(3), 1156-1190.

[41] Kiayias, A., Russell, A., David, B., & Oliynykov, R. (2017, July). Ouroboros: A provably secure proof-of-stake blockchain protocol. In *Annual international cryptology conference* (pp. 357-388). Cham: Springer International Publishing.

[42] Bach, L. M., Mihaljevic, B., & Zagar, M. (2018, May). Comparative analysis of blockchain consensus algorithms. In *2018 41st international convention on information and communication technology, electronics and microelectronics (MIPRO)* (pp. 1545-1550). Ieee.

[43] Li, W., Andreina, S., Bohli, J. M., & Karame, G. (2017). Securing proof-of-stake blockchain protocols. In *Data Privacy Management, Cryptocurrencies and Blockchain Technology: ESORICS 2017 International Workshops, DPM 2017 and CBT 2017, Oslo, Norway, September 14-15, 2017, Proceedings* (pp. 297-315). Springer International Publishing.

[44] Buterin, V., & Griffith, V. (2017). Casper the friendly finality gadget. *arXiv preprint arXiv:1710.09437*.

[45] SKing, S., & Nadal, S. (2012). Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. *self-published paper, August*, *19*(1).

[46] Vasin, P. (2014). Blackcoin's proof-of-stake protocol v2. *URL: https://blackcoin. co/blackcoin-pos-protocol-v2-whitepaper. pdf*, *71*, 25.

[47] Bentov, I., Lee, C., Mizrahi, A., & Rosenfeld, M. (2014). Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract] y. *ACM SIGMETRICS Performance Evaluation Review*, *42*(3), 34-37.

[48] Bozic, N., Pujolle, G., & Secci, S. (2016). A tutorial on blockchain and applications to secure network control-planes. *2016 3rd Smart Cloud Networks & Systems (SCNS)*, 1-8.

[49] Wilkinson, S., Lowry, J., & Boshevski, T. (2014). Metadisk a blockchain-based decentralized file storage application. *Storj Labs Inc., technical report, hal*, *1*(11).

[50] Sikorski, J. J., Haughton, J., & Kraft, M. (2017). Blockchain technology in the chemical industry: Machine-to-machine electricity market. *Applied energy*, *195*, 234-246.

[51] Larimer, D. (2014). Delegated proof-of-stake (dpos). *Bitshare whitepaper*, *81*, 85.

[52] Nguyen, C. T., Hoang, D. T., Nguyen, D. N., Niyato, D., Nguyen, H. T., & Dutkiewicz, E. (2019). Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities. *IEEE access*, *7*, 85727-85745.

[53] Nguyen, G. T., & Kim, K. (2018). A survey about consensus algorithms used in blockchain. *Journal of Information processing systems*, *14*(1).

[54] Pass, R., & Shi, E. (2017). The sleepy model of consensus. In *Advances in Cryptology–ASIACRYPT 2017: 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part II 23* (pp. 380-409). Springer International Publishing.

[55] Dwork, C., Naor, M., & Sahai, A. (2004). Concurrent zero-knowledge. *Journal of the ACM (JACM)*, *51*(6), 851-898.

[56] Adam, K. (2022). Blockchain Technology for Business Processes. *Springer Books*.

[57] Lin Chen, Lei Xu, Nolan Shah, Zhimin Gao, Yang Lu, and Weidong Shi. 2017. On security analysis of proof-of-elapsedtime (PoET). In Stabilization, Safety, and Security of Distributed Systems. 282–297.

[58] Himanshu, R. (2022). An overview of blockchain technology: Architecture and consensus protocols. *Smart City Infrastructure: The Blockchain Perspective*, 293-315.

[59] Aluko, O., & Kolonin, A. (2021). Proof-of-reputation: an alternative consensus mechanism for blockchain systems. *arXiv preprint arXiv:2108.03542*.

[60] Gai, F., Wang, B., Deng, W., & Peng, W. (2018). Proof of reputation: A reputation-based consensus protocol for peer-to-peer network. In *Database Systems for Advanced Applications: 23rd International Conference, DASFAA 2018, Gold Coast, QLD, Australia, May 21-24, 2018, Proceedings, Part II 23* (pp. 666-681). Springer International Publishing.

[61] Tamang, S. (2018). Decentralized reputation model and trust framework blockchain and smart contracts.

[62] Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?—a systematic review. *PloS one*, *11*(10), e0163477.

[63] Lee, B., & Lee, J. H. (2017). Blockchain-based secure firmware update for embedded devices in an Internet of Things environment. *The Journal of Supercomputing*, *73*, 1152-1167.

[64] Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future generation computer systems*, *82*, 395-411.

[65] Ouaddah, A., Elkalam, A. A., & Ouahman, A. A. (2017). Towards a novel privacy-preserving access control model based on blockchain technology in IoT. In *Europe and MENA cooperation advances in information and communication technologies* (pp. 523-533). Springer International Publishing.

[66] Hardjono, T., & Smith, N. (2016, May). Cloud-based commissioning of constrained devices using permissioned blockchains. In *Proceedings of the 2nd ACM international workshop on IoT privacy, trust, and security* (pp. 29-36).

[67] McFarlane, C. (2019). Are smart cities the pathway to blockchain and cryptocurrency adoption. *The Forbes*, *18*.

[68] Huh, S., Cho, S., & Kim, S. (2017, February). Managing IoT devices using blockchain platform. In *2017 19th international conference on advanced communication technology (ICACT)* (pp. 464-467). IEEE.

[69] Samaniego, M., & Deters, R. (2016, November). Using blockchain to push software-defined IoT components onto edge hosts. In *Proceedings of the international conference on big data and advanced wireless technologies* (pp. 1-9).

[70] Samaniego, M., & Deters, R. (2016, December). Hosting virtual iot resources on edge-hosts with blockchain. In *2016 IEEE International conference on computer and information technology (CIT)* (pp. 116-119). IEEE.

[71] Samaniego, M., Jamsrandorj, U., & Deters, R. (2016, December). Blockchain as a Service for IoT. In *2016 IEEE international conference on internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData)* (pp. 433-436). IEEE.

[72] Boudguiga, A., Bouzerna, N., Granboulan, L., Olivereau, A., Quesnel, F., Roger, A., & Sirdey, R. (2017, April). Towards better availability and accountability for iot updates by means of a blockchain. In *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 50-58). IEEE.

[73] Liu, B., Yu, X. L., Chen, S., Xu, X., & Zhu, L. (2017, June). Blockchain based data integrity service framework for IoT data. In *2017 IEEE international conference on web services (ICWS)* (pp. 468-475). IEEE.

[74] Kang, J., Yu, R., Huang, X., Maharjan, S., Zhang, Y., & Hossain, E. (2017). Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains. *IEEE transactions on industrial informatics*, *13*(6), 3154-3164.

[75] Münsing, E., Mather, J., & Moura, S. (2017, August). Blockchains for decentralized optimization of energy resources in microgrid networks. In *2017 IEEE conference on control technology and applications (CCTA)* (pp. 2164-2171). IEEE.

[76] Mylrea, M., & Gourisetti, S. N. G. (2017, September). Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security. In *2017 Resilience Week (RWS)* (pp. 18-23). IEEE.

[77] Bergquist, J., Laszka, A., Sturm, M., & Dubey, A. (2017, December). On the design of communication and transaction anonymity in blockchain-based transactive microgrids. In *Proceedings of the 1st Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers* (pp. 1-6).

[78] Liang, G., Weller, S. R., Luo, F., Zhao, J., & Dong, Z. Y. (2018). Distributed blockchain-based data protection framework for modern power systems against cyber attacks. *IEEE Transactions on Smart Grid*, *10*(3), 3162-3173.

[79] Imbault, F., Swiatek, M., de Beaufort, R., & Plana, R. (2017, June). The green blockchain: Managing decentralized energy production and consumption. In *2017 IEEE International Conference on*

Environment and Electrical Engineering and 2017 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe) (pp. 1-5). IEEE.

[80] Sehra, A., Cohen, R., & Arulchandran, V. (2018). On cryptocurrencies, digital assets and private money. *Journal of Payments Strategy & Systems*, *12*(1), 13-32.

[81] Peters, G. W., & Panayi, E. (2016). *Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money* (pp. 239-278). Springer International Publishing.

[82] MacDonald, T. J., Allen, D. W., & Potts, J. (2016). *Blockchains and the boundaries of self-organized economies: Predictions for the future of banking* (pp. 279-296). Springer International Publishing.

[83] Nguyen, Q. K. (2016, November). Blockchain-a financial technology for future sustainable development. In *2016 3rd International conference on green technology and sustainable development (GTSD)* (pp. 51-54). IEEE.

[84] Singh, S., & Singh, N. (2016, December). Blockchain: Future of financial and cyber security. In *2016 2nd international conference on contemporary computing and informatics (IC3I)* (pp. 463-467). IEEE.

[85] Mandl, K. D., Markwell, D., MacDonald, R., Szolovits, P., & Kohane, I. S. (2001). Public standards and patients' control: how to keep electronic medical records accessible but privateMedical information: access and privacyDoctrines for developing electronic medical recordsDesirable characteristics of electronic medical recordsChallenges and limitations for electronic medical recordsConclusionsCommentary: Open approaches to electronic patient recordsCommentary: A patient's viewpoint. *Bmj*, *322*(7281), 283-287.

[86] Nugent, T., Upton, D., & Cimpoesu, M. (2016). Improving data transparency in clinical trials using blockchain smart contracts. *F1000Research*, *5*.

[87] Hou, H. (2017, July). The application of blockchain technology in E-government in China. In *2017 26th international conference on computer communication and networks (ICCCN)* (pp. 1-4). IEEE.

[88] Stanciu, A. (2017, May). Blockchain based distributed control system for edge computing. In *2017 21st international conference on control systems and computer science (CSCS)* (pp. 667-671). IEEE.

[89] Ølnes, S., & Jansen, A. (2017). Blockchain technology as s support infrastructure in e-government. In *Electronic Government: 16th IFIP WG 8.5 International Conference, EGOV 2017, St. Petersburg, Russia, September 4-7, 2017, Proceedings 16* (pp. 215-227). Springer International Publishing.

[90] Ølnes, S. (2016). Beyond bitcoin enabling smart government using blockchain technology. In *Electronic Government: 15th IFIP WG 8.5 International Conference, EGOV 2016, Guimarães, Portugal, September 5-8, 2016, Proceedings 15* (pp. 253-264). Springer International Publishing.

[91] Noizat, P. (2015). Blockchain electronic vote. In *Handbook of digital currency* (pp. 453-461). Academic Press.

[92] Melo Jr, W. S., Bessani, A., & Carmo, L. F. (2017, December). How blockchains can help legal metrology. In *Proceedings of the 1st Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers* (pp. 1-2).

[93] Melo, W., Carmo, L. F., Bessani, A., Neves, N., & Santin, A. (2018, May). How blockchains can improve measuring instruments regulation and control. In *2018 IEEE International Instrumentation and Measurement Technology Conference (I2MTC)* (pp. 1-6). IEEE.

[94] Brandon, R. M., Podhorzer, M., & Pollak, T. H. (2019). Premiums without benefits: Waste and inefficiency in the commercial health insurance industry. In *Why the United States Does Not Have a National Health Program* (pp. 73-90). Routledge.

[95] Gorman, L. (2006). The history of health care costs and health insurance. *Wisconsin Policy Research Institute Report*, *19*(10), 1-31.

[96] Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016, August). A Case Study for Blockchain in Healthcare:"MedRec" prototype for electronic health records and medical research data. In *Proceedings of IEEE open & big data conference* (Vol. 13, p. 13).

[97] Xia, Q. I., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., & Guizani, M. (2017). MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. *IEEE access*, *5*, 14757-14767.

[98] Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., & Wang, F. (2017). Secure and trustable electronic medical records sharing using blockchain. In *AMIA annual symposium proceedings* (Vol. 2017, p. 650). American Medical Informatics Association.

[99] Heston, T. F. (2017). A case study in blockchain healthcare innovation.

[100] Omar, I. A., Jayaraman, R., Salah, K., Simsekler, M. C. E., Yaqoob, I., & Ellahham, S. (2020). Ensuring protocol compliance and data transparency in clinical trials using Blockchain smart contracts. *BMC Medical Research Methodology*, *20*, 1-17.

[101] Buterin, V. (2014). A next-generation smart contract and decentralized application platform. *white paper*, *3*(37), 2-1.

[102] Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, *151*(2014), 1-32.

[103] Benchoufi, M., Porcher, R., & Ravaud, P. (2017). Blockchain protocols in clinical trials: Transparency and traceability of consent. *F1000Research*, *6*.

[104] Swan, M. (2015). Blockchain thinking: The brain as a decentralized autonomous corporation [commentary]. *IEEE Technology and Society Magazine*, *34*(4), 41-52.

[105] Shae, Z., & Tsai, J. J. (2017, June). On the design of a blockchain platform for clinical trial and precision medicine. In *2017 IEEE 37th international conference on distributed computing systems (ICDCS)* (pp. 1972-1980). IEEE.

[106] Alhadhrami, Z., Alghfeli, S., Alghfeli, M., Abedlla, J. A., & Shuaib, K. (2017, November). Introducing blockchains for healthcare. In *2017 international conference on electrical and computing technologies and applications (ICECTA)* (pp. 1-4). IEEE.

[107] Fernández-Caramés, T. M., & Fraga-Lamas, P. (2018). A Review on the Use of Blockchain for the Internet of Things. *Ieee Access*, *6*, 32979-33001.

[108] Kuo, T. T., & Ohno-Machado, L. (2018). Modelchain: Decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks. *arXiv preprint arXiv:1802.01746*.

[109] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE international congress on big data (BigData congress)* (pp. 557-564). Ieee.

[110] Cekerevac, Z., & Cekerevac, P. (2022). BLOCKCHAIN AND THE APPLICATION OF BLOCKCHAIN TECHNOLOGY. *MEST Journal*, *10*(2).

[111] Bratspies, R. M. (2018). Cryptocurrency and the Myth of the Trustless Transaction. *Mich. Tech. L. Rev.*, *25*, 1.

[112] Linn, L. A., & Koo, M. B. (2016, September). Blockchain for health data and its potential use in health it and health care related research. In *ONC/NIST use of blockchain for healthcare and research workshop. Gaithersburg, Maryland, United States: ONC/NIST* (pp. 1-10).

[113] Esposito, C., De Santis, A., Tortora, G., Chang, H., & Choo, K. K. R. (2018). Blockchain: A panacea for healthcare cloud-based data security and privacy?. *IEEE cloud computing*, *5*(1), 31-37.

[114] Bennett, B. (2017). Blockchain HIE overview: a framework for healthcare interoperability. *Telehealth and Medicine Today*, *2*(3).

[115] Pirtle, C., & Ehrenfeld, J. (2018). Blockchain for healthcare: The next generation of medical records?. *Journal of Medical Systems*, *42*(9), 172.

[116] Ma, A. (2020, December). Emerging legal issues in blockchain for construction supply chains. In *Proceedings of the 2020 4th international conference on vision, image and signal processing* (pp. 1-7).

[117] Kaushalya, K. T., Yukta, Y. P., Deepak, D. G., Suyash, S. G., Rushikesh, R. K., & Rahul, R. N. (2023). Etherswap (A crypto wallet).

[118] Gackenheimer, C. (2015). *Introduction to React*. Apress.

[119] Liu, C., Wang, D., & Wu, M. (2018). Vite: A high performance asynchronous decentralized application platform. *White Paper*.

[120] Saglio, A., Bourgeay, J., Socrate, R., Canette, A., & Cuvelier, G. (2018). Understanding the structure of ganache: Link between composition and texture. *International Journal of Gastronomy and Food Science*, *13*, 29-37.

[121] Lee, W. M., & Lee, W. M. (2019). Using the metamask chrome extension. *Beginning Ethereum Smart Contracts Programming: With Examples in Python, Solidity, and JavaScript*, 93-126.

[122] Wohrer, M., & Zdun, U. (2018, March). Smart contracts: security patterns in the ethereum ecosystem and solidity. In *2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE)* (pp. 2-8). IEEE.

[123] Shen, Z., Chen, Y., & Zhang, W. (2023, March). GSVD: Common Vulnerability Dataset for Smart Contracts on BSC and Polygon. In *CS & IT Conference Proceedings* (Vol. 13, No. 6). CS & IT Conference Proceedings.

[124] Siyal, A. A., Junejo, A. Z., Zawish, M., Ahmed, K., Khalil, A., & Soursou, G. (2019). Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives. *Cryptography*, *3*(1), 3.

[125] Monrat, A. A., Schelén, O., & Andersson, K. (2019). A survey of blockchain from the perspectives of applications, challenges, and opportunities. Ieee Access, 7, 117134-117151.

[126] Abou Jaoude, J., & Saade, R. G. (2019). Blockchain applications–usage in different domains. *Ieee Access*, *7*, 45360-45381.

[127] Guo, H., & Yu, X. (2022). A survey on blockchain technology and its security. *Blockchain: research and applications*, *3*(2), 100067.

[128] Zhang, R., Xue, R., & Liu, L. (2019). Security and privacy on blockchain. *ACM Computing Surveys (CSUR)*, *52*(3), 1-34.

[129] Khayyat, M., Alhemdi, F., & Alnunu, R. (2020). The Challenges and Benefits of Blockchain in E-government. *Int. J. Comput. Sci. Netw. Secur*, *20*, 15-20.

[130] GeeksforGeeks. (2023, March 14). *Features of blockchain*. https://www.geeksforgeeks.org/features-of-blockchain/

[131] xJinbe. (2023, July 18). Types of blockchains: public, private, and hybrid. - CoinMonks - medium. *Medium*. https://medium.com/coinmonks/types-of-blockchains-public-private-and-hybrid-ec9e46b77301

[132] Sarkar, A., & Roy, M. (2023, December). Blockchain Based Drug Supply-Chain Management System. In *2023 OITS International Conference on Information Technology (OCIT)* (pp. 950-956). IEEE.

[133] Abdallah, S., & Nizamuddin, N. (2023). Blockchain-based solution for pharma supply chain industry. *Computers & Industrial Engineering*, *177*, 108997.