



ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ (ΠΜΣ)

ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

**Συνέργεια & Συσχέτιση μεταξύ Υπολογιστικού Νέφους
& Αλυσίδας Συστοιχίας**

**(Survey on the synergy and correlation between cloud
computing and blockchain)**

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΤΩΝ

Σιδέρη Γεωργίου

&

Τσιόκανου Ανδρέα

Επιβλέπων: Αν. Καθηγητής Κρητικός Κυριάκος

Μέλη εξεταστικής επιτροπής:

Καθηγητής Κοκολάκης Σπυρίδων

Επικ. Καθηγητής Στεργιόπουλος Γεώργιος

Σάμος, Ιούνιος 2024

Η σελίδα αυτή είναι σκόπιμα λευκή.

Περίληψη

Η διπλωματική εργασία με τίτλο "Συνέργεια & Συσχέτιση μεταξύ Υπολογιστικού Νέφους & Αλυσίδας Συστοιχίας" έχει ως στόχο την διερεύνηση των τρόπων με τους οποίους μπορούν να συνδυαστούν το Υπολογιστικό Νέφος (Cloud Computing) και η Αλυσίδα Συστοιχίας (Blockchain) για την αμοιβαία υποστήριξη και ενίσχυση των δυνατοτήτων τους. Η έρευνα εστιάζει σε δύο βασικές κατευθύνσεις: πώς το Υπολογιστικό Νέφος μπορεί να ενισχύσει και να υποστηρίξει τις λειτουργίες της Αλυσίδας Συστοιχίας και πώς η Αλυσίδα Συστοιχίας μπορεί να βελτιώσει και να υποστηρίξει το Υπολογιστικό Νέφος.

Αναλύονται οι υπάρχουσες προσεγγίσεις και μέθοδοι που υλοποιούν τη συνέργεια μεταξύ των δύο τεχνολογιών, και εντοπίζονται τα ερευνητικά κενά που απαιτούν περαιτέρω διερεύνηση. Η εργασία εξετάζει τα οφέλη, τις προκλήσεις και τις εφαρμογές αυτών των τεχνολογιών σε διάφορους τομείς, όπως η αποθήκευση δεδομένων, ο έλεγχος πρόσβασης, η υγεία και οι έξυπνες πόλεις. Επιπλέον, προτείνονται κατευθύνσεις για μελλοντική έρευνα, με στόχο την αντιμετώπιση των τεχνικών προκλήσεων και την ανάπτυξη νέων εφαρμογών που θα εκμεταλλεύονται πλήρως τις δυνατότητες των δύο τεχνολογιών.

Abstract

The thesis titled "Synergy and Correlation between Cloud Computing and Blockchain" aims to explore the ways in which Cloud Computing and Blockchain technologies can be integrated to mutually support and enhance their capabilities. The research focuses on two main directions: how Cloud Computing can strengthen and support the functions of Blockchain and how Blockchain can improve and support Cloud Computing.

The thesis analyzes existing approaches and methods that implement the synergy between the two technologies and identifies research gaps that require further investigation. It examines the benefits, challenges, and applications of these technologies in various fields, such as data storage, access control, healthcare, and smart cities. Additionally, it proposes directions for future research aimed at addressing technical challenges and developing new applications that fully leverage the capabilities of both technologies.

Πρόλογος και ευχαριστίες

Θα θέλαμε να ευχαριστήσουμε θερμά όλους όσους μας βοήθησαν και μας στήριξαν στην ολοκλήρωση της διπλωματικής μας εργασίας, καθώς και στην επιτυχή περάτωση της φοίτησής μας στο Πρόγραμμα Μεταπτυχιακών Σπουδών του Πανεπιστημίου Αιγαίου. Πρώτα απ' όλα, τις οικογένειές μας για την αμέριστη ηθική και υλική τους συμπαράσταση καθ' όλη τη διάρκεια των σπουδών μας, και επίσης όλους τους φίλους και συμφοιτητές μας για την ανιδιοτελή βοήθεια που μας προσέφεραν σε όλες τις δυσκολίες που αντιμετωπίσαμε κατά τη διάρκεια της φοίτησής μας.

Θα θέλαμε να ευχαριστήσουμε θερμά τον Αν. Καθηγητή κ. Κυριάκο Κρητικό που μας έδωσε την ευκαιρία να αναπτύξουμε τη διπλωματική μας εργασία αλλά και για την υποστήριξη και την καθοδήγησή του κατά τη διάρκεια της εκπόνησης της παρούσας εργασίας. Η συνεργασία μας ήταν άψογη και οι συμβουλές του ήταν πολύτιμες σε όλα τα στάδια και τη διάρκεια της εργασίας μας, υποδεικνύοντάς μας την ορθή και επιστημονική προσέγγιση του θέματος.

© 2024

των

ΣΙΔΕΡΗ ΓΕΩΡΓΙΟΥ & ΤΣΙΟΚΑΝΟΥ ΑΝΔΡΕΑ

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

Η σελίδα αυτή είναι σκόπιμα λευκή

Πίνακας περιεχομένων

1. Εισαγωγή.....	12
2. Blockchain & Cloud Computing.....	14
2.1. Blockchain.....	14
2.1.1. Ορισμός του Blockchain	14
2.1.2. Ιστορική Αναδρομή	14
2.1.3. Λειτουργία Blockchain.....	16
2.1.4. Εφαρμογές Blockchain	17
2.1.5. Τύποι Blockchain.....	17
2.1.5.1. Δημόσια Blockchain	18
2.1.5.2. Ιδιωτικά Blockchain	18
2.1.5.3. Κοινοπρακτικά Blockchain	20
2.1.5.4. Υβριδικά Blockchain.....	21
2.1.6. Πλεονεκτήματα & Μειονεκτήματα Blockchain.....	22
2.2. Cloud Computing.....	28
2.2.1. Ορισμός Cloud Computing	28
2.2.2. Πλεονεκτήματα και μειονεκτήματα του cloud computing.....	28
2.2.3. Τύποι υπολογιστικού νέφους	33
2.2.3.1. Δημόσιο νέφος.....	33
2.2.3.2. Ιδιωτικό νέφος.....	35
2.2.3.3. Υβριδικό νέφος	36
2.2.3.4. Κοινοτικό Νέφος.....	38
2.2.3.5. Ομοσπονδιακό Νέφος.....	39
2.2.4. Υπηρεσίες του υπολογιστικού νέφους.....	40
2.2.4.1 Λογισμικό ως Υπηρεσία (Software as a Service - SaaS).....	40
2.2.4.2 Πλατφόρμα ως Υπηρεσία (Platform as a Service - PaaS).....	42
2.2.4.3 Υποδομή ως Υπηρεσία (Infrastructure as a Service - IaaS)	44
3. Μεθοδολογία & Αναζήτηση Άρθρων	46
3.1. Σχεδιασμός της Έρευνας.....	46
3.2. Συλλογή Δεδομένων	46
3.3. Αναζήτηση Άρθρων	46
3.4. Φιλτράρισμα Άρθρων	47
3.5. Ποσοτική ανάλυση.....	48
3.5.1. Ανά κατηγορία δημοσίευσης:	48
3.5.2. Ανά χρονολογία δημοσίευσης.....	49
4. Συνεισφορά του blockchain στο cloud computing.....	50
4.1. Τομείς του υπολογιστικού νέφους που επηρεάζονται από το blockchain	50

4.1.1. Κύριες περιοχές επιρροής.....	50
4.1.2. Εφαρμογές και περιπτώσεις χρήσης.....	51
4.2. Τομείς Εφαρμογών του blockchain στο υπολογιστικό νέφος	53
4.2.1. Μεταφορές.....	53
4.2.2. Υγεία.....	53
4.2.3. Γεωργία	54
4.2.4. Έξυπνες Πόλεις	55
4.2.5. Αλυσίδες Εφοδιασμού	55
4.3. Οφέλη του blockchain στο cloud computing	56
4.4. Μηχανισμός ασφαλούς αποθήκευσης δεδομένων βάσει blockchain και κώδικα	58
4.4.1. Παγκόσμιο Blockchain	58
4.4.2. Τοπικό Blockchain	58
4.4.3. Αναγεννητικοί Κώδικες.....	59
4.5. Αποδεδειγμένη Προέλευση Δεδομένων (Data Provenance) με Blockchain στο Υπολογιστικό Νέφος.....	59
4.6. Έλεγχος Πρόσβασης με Βάση το Blockchain στο Υπολογιστικό Νέφος.....	60
4.7. Ενεργοποιημένη από Blockchain αναζητήσιμη κρυπτογράφηση στα Νεφη	62
4.8. Blockchain και Data Deduplication στο Νέφος.....	64
4.8.1. Data Deduplication στο Νέφος.....	64
4.8.2. Blockchain-Enabled Cloud Data Deduplication	64
5. Συνεισφορά του cloud στο blockchain.....	66
5.1. Blockchain as a service (BaaS)	66
5.1.1. Ορισμός του blockchain as a service	66
5.1.2. Αρχιτεκτονική του blockchain as a service	67
5.1.3. Πλεονεκτήματα και μειονεκτήματα του blockchain as a service.....	68
5.1.4. BaaS πλατφόρμες	70
5.2. Εκφόρτωση Λειτουργιών Blockchain στο Νέφος.....	73
5.2.1. Εκφόρτωση βάσει Κέρδους Χρηστών	73
5.2.2. Εκφόρτωση βάσει κοινωνικής ευημερίας	74
5.2.3. Εκφόρτωση βάσει κέρδους των CSP	75
5.3. Χρήση Αποθήκευσης Νέφους στο Blockchain	76
5.3.1. Αποθήκευση Τιμών Hash στην Αλυσίδα	76
5.3.2. Αποθήκευση Μεταδεδομένων στην Αλυσίδα.....	77
5.4. Εξέλιξη Υλικού Νέφους για Blockchain Εξόρυξη.....	78
5.4.1. Εξόρυξη στο Νέφος με βάση τη CPU.....	78
5.4.2. Εξόρυξη με βάση GPU/FPGA στο cloud.....	79
5.4.3. Εξόρυξη βασισμένη σε ενοποιημένα κυκλώματα ειδικού σκοπού (ASIC).....	80
6. Ερευνητικά κενά και μελλοντικές έρευνες.....	82
6.1. Έρευνες για την βελτίωση του blockchain με τη βοήθεια του cloud.....	82
6.1.1. Επιλογή Δεδομένων για Αποθήκευση στην Αλυσίδα.....	82
6.1.2. Συνδυασμός Αποθήκευσης στο Cloud και Blockchain	83

6.1.3. Αποθήκευση Κατακερματισμένων Τιμών στην Αλυσίδα	83
6.1.4. Διαχείριση Πρόσβασης και Κλειδιών για Αποθήκευση Off-Chain	84
6.1.5. Βελτιστοποίηση Ισορροπίας Μεταξύ Αποδοτικότητας και Ασφάλειας:.....	84
6.1.6. Αντιμετώπιση του προβλήματος της κλιμακωσιμότητας:.....	84
6.1.7. Βελτίωση της διαλειτουργικότητας	84
6.1.8. Μείωση της ενεργειακής κατανάλωσης	85
6.2. Έρευνες για την βελτίωση του cloud με βάση το blockchain	85
6.2.1. Αντιμετώπιση του προβλήματος του vendor lock-in	85
6.2.2. Έλεγχος Πρόσβασης στο Νέφος βάσει Blockchain	85
6.3. Έρευνες για την βελτίωση του συνδυασμού cloud-blockchain ή/και των BaaS υπηρεσιών	86
6.3.1. Εξέταση των τεχνικών προκλήσεων της ενοποίησης	86
6.3.2. Επίδραση της ενοποίησης στη νομοθεσία και τη ρύθμιση.....	87
6.3.3. Αξιολόγηση της ωριμότητας των τεχνολογιών.....	87
6.3.4. Σχεδιασμός και υλοποίηση ασφαλών και επεκτάσιμων πλατφορμών BaaS.....	87
6.3.5. Blockchain-Enabled Cloud Data Provenance.....	87
6.3.5.1. Κίνητρα για Έντιμη Συμπεριφορά.....	88
6.3.5.2. Τιμωρίες για Κακόβουλες Ενέργειες	88
6.3.6. Κατευθύνσεις Έρευνας για την Εκφόρτωση Υπολογισμών	89
6.3.6.1. Βελτιστοποίηση Κοινωνικής Ευημερίας έναντι Μεγιστοποίησης Κέρδους Παρόχων	89
6.3.6.2. Τεχνολογίες Βαθιάς Μάθησης στην Τιμολόγηση και στις Δημοπρασίες.....	90
6.3.7. ASIC-Based Mining	90
6.3.8. Εκφόρτωση βάσει κέρδους των CSP	91
7. Συμπεράσματα	92
8. Βιβλιογραφία.....	94

Πίνακας εικόνων

Εικόνα 1. Πίτα ποσοτικής ανάλυσης.....	48
Εικόνα 2. Ποσοτική ανάλυση ανά έτος δημοσίευσης	49
Εικόνα 3. Αρχιτεκτονική υψηλού επιπέδου για την ανίχνευση προέλευσης δεδομένων σε κέντρα δεδομένων cloud με τη χρήση blockchain	60
Εικόνα 4. Αρχιτεκτονική του Blockchain as a Service	68

1. Εισαγωγή

Η ταχεία εξέλιξη της τεχνολογίας έχει φέρει στο προσκήνιο δύο καινοτόμες τεχνολογίες που έχουν τη δυνατότητα να αλλάξουν ριζικά τον τρόπο με τον οποίο διαχειριζόμαστε, επεξεργαζόμαστε και προστατεύουμε δεδομένα και υπηρεσίες: το Υπολογιστικό Νέφος (Cloud Computing) και την Αλυσίδα Συστοιχίας (Blockchain). Το Υπολογιστικό Νέφος προσφέρει ευέλικτες και αποδοτικές λύσεις για την αποθήκευση και την επεξεργασία δεδομένων μέσω διαδικτύου, επιτρέποντας στις επιχειρήσεις και τους οργανισμούς να μειώσουν τα λειτουργικά τους κόστη και να βελτιώσουν την αποδοτικότητά τους. Από την άλλη πλευρά, η Αλυσίδα Συστοιχίας, με την αποκεντρωμένη και ανθεκτική αρχιτεκτονική της, εγγυάται την ασφάλεια, τη διαφάνεια και την ακεραιότητα των συναλλαγών και των δεδομένων.

Το Υπολογιστικό Νέφος (Cloud Computing) είναι μια τεχνολογία που επιτρέπει την παροχή ευέλικτων και αποδοτικών λύσεων για την αποθήκευση και την επεξεργασία δεδομένων μέσω διαδικτύου. Επιτρέπει στις επιχειρήσεις και τους οργανισμούς να μειώσουν τα λειτουργικά τους κόστη, να βελτιώσουν την αποδοτικότητά τους και να έχουν πρόσβαση σε υπολογιστικούς πόρους κατ' απαίτηση. Ωστόσο, η τεχνολογία αυτή αντιμετωπίζει ορισμένες αδυναμίες, όπως η ευπάθεια σε κυβερνοεπιθέσεις, η πιθανή απώλεια δεδομένων λόγω παραβιάσεων ασφάλειας, και η εξάρτηση από τρίτους παρόχους υπηρεσιών για την προστασία των δεδομένων και των υπηρεσιών τους. Επίσης, η κεντροποιημένη φύση του Υπολογιστικού Νέφους μπορεί να δημιουργήσει ζητήματα σχετικά με την ιδιωτικότητα και την ασφάλεια των δεδομένων.

Η Αλυσίδα Συστοιχίας (Blockchain) είναι μια αποκεντρωμένη και ανθεκτική τεχνολογία που εγγυάται την ασφάλεια, τη διαφάνεια και την ακεραιότητα των συναλλαγών και των δεδομένων. Η τεχνολογία αυτή χρησιμοποιεί κρυπτογραφικές τεχνικές για να εξασφαλίσει ότι οι συναλλαγές είναι αμετάβλητες και διαφανείς, καθιστώντας την ιδανική για τη διαχείριση ευαίσθητων δεδομένων. Παρά τα πλεονεκτήματά της, η τεχνολογία του Blockchain αντιμετωπίζει ορισμένες προκλήσεις, όπως η χαμηλή απόδοση και επεκτασιμότητα, η υψηλή κατανάλωση ενέργειας και η δυσκολία στην υιοθέτηση από παραδοσιακά συστήματα. Επιπλέον, η πολύπλοκη φύση των αλγορίθμων συναίνεσης μπορεί να καθιστά δύσκολη την ενσωμάτωση της τεχνολογίας αυτής σε υπάρχουσες υποδομές.

Οι αδυναμίες του Υπολογιστικού Νέφους και του Blockchain μπορούν να αντιμετωπιστούν μέσω της συνέργειας των δύο τεχνολογιών. Για παράδειγμα, η αποκεντρωμένη φύση και η κρυπτογραφική ασφάλεια του Blockchain μπορούν να ενισχύσουν την ασφάλεια και την ιδιωτικότητα στο Υπολογιστικό Νέφος, ενώ οι υπολογιστικοί πόροι και η αποδοτικότητα του Υπολογιστικού Νέφους μπορούν να βελτιώσουν την επεκτασιμότητα και την απόδοση του Blockchain. Η συνεργασία αυτή μπορεί να οδηγήσει σε πιο ασφαλείς, αποδοτικές και αξιόπιστες λύσεις, εκμεταλλευόμενες τα πλεονεκτήματα και των δύο τεχνολογιών για την ανάπτυξη νέων και καινοτόμων εφαρμογών.

Για να διερευνήσει και να αναδείξει τις δυνατότητες συνέργειας και αλληλεπίδρασης μεταξύ του Υπολογιστικού Νέφους και της Αλυσίδας Συστοιχίας, η τρέχουσα διπλωματική εργασία θα πραγματοποιήσει διάφορες δραστηριότητες, συμπεριλαμβανομένης μιας βιβλιογραφικής ανασκόπησης. Αυτή η ανασκόπηση θα συγκεντρώσει και θα αναλύσει την υπάρχουσα επιστημονική και τεχνική βιβλιογραφία που αφορά την εφαρμογή και την αλληλεπίδραση των δύο τεχνολογιών. Πιο συγκεκριμένα, η έρευνα θα εστιάσει σε δύο βασικές κατευθύνσεις: αφενός, πώς το Υπολογιστικό Νέφος μπορεί να ενισχύσει και να υποστηρίξει τις λειτουργίες της Αλυσίδας Συστοιχίας, και αφετέρου, πώς η Αλυσίδα Συστοιχίας μπορεί να βελτιώσει και να υποστηρίξει το Υπολογιστικό Νέφος.

Η εξερεύνηση των δυνατοτήτων συνέργειας αυτών των τεχνολογιών αναμένεται να αποκαλύψει νέες μεθόδους και εφαρμογές που θα μπορούσαν να υλοποιηθούν, αξιοποιώντας τα πλεονεκτήματα και των δύο. Επιπλέον, θα αναλυθούν οι υπάρχουσες προσεγγίσεις και οι μέθοδοι που έχουν ήδη εφαρμοστεί σε αυτή την κατεύθυνση, ενώ θα εντοπιστούν και τα ερευνητικά κενά που απαιτούν περαιτέρω διερεύνηση. Για κάθε ερευνητικό κενό, θα προταθούν αντίστοιχες κατευθύνσεις έρευνας που θα μπορούσαν να οδηγήσουν σε λύσεις ή βελτιώσεις.

Συνοψίζοντας, η παρούσα εργασία φιλοδοξεί να αποτελέσει έναν οδηγό για τη διερεύνηση και αξιοποίηση των συνεργειών μεταξύ Υπολογιστικού Νέφους και Αλυσίδας Συστοιχίας, προσφέροντας πολύτιμα συμπεράσματα και προτάσεις για το μέλλον των τεχνολογιών αυτών.

Η αναφορά αυτή χωρίζεται σε κεφάλαια, καθένα από τα οποία εξετάζει διαφορετικές πτυχές της συνέργειας μεταξύ του Υπολογιστικού Νέφους και της Αλυσίδας Συστοιχίας. Στο Κεφάλαιο 1, παρουσιάζεται η εισαγωγή και το πλαίσιο της έρευνας. Στο Κεφάλαιο 2, αναλύονται οι βασικές έννοιες του Blockchain και του Cloud Computing, παρέχοντας μια εις βάθος κατανόηση των θεμελίων τους. Το Κεφάλαιο 3 εστιάζει στη μεθοδολογία και την αναζήτηση άρθρων, περιγράφοντας τις διαδικασίες συλλογής και ανάλυσης δεδομένων. Στο Κεφάλαιο 4, εξετάζεται η συνεισφορά του Blockchain στο Cloud Computing, αναλύοντας πώς το Blockchain μπορεί να βελτιώσει τις υπηρεσίες του Cloud. Το Κεφάλαιο 5 εξετάζει τη συνεισφορά του Cloud στο Blockchain, παρουσιάζοντας πώς το Υπολογιστικό Νέφος μπορεί να υποστηρίξει και να ενισχύσει τις λειτουργίες του Blockchain. Τέλος, στο Κεφάλαιο 6, εντοπίζονται τα ερευνητικά κενά και προτείνονται κατευθύνσεις για μελλοντική έρευνα, ενώ στο Κεφάλαιο 7 συνοψίζονται τα συμπεράσματα της έρευνας.

2. Blockchain & Cloud Computing

2.1. Blockchain

2.1.1. Ορισμός του Blockchain

Το blockchain είναι μια κατανεμημένη και αποκεντρωμένη ψηφιακή βάση δεδομένων, γνωστή και ως "κατανεμημένο καθολικό" (distributed ledger), η οποία αποθηκεύει δεδομένα (συναλλαγών) με ασφαλή και διαφανή τρόπο. Σε αντίθεση με τις συμβατικές βάσεις δεδομένων, όπου τα δεδομένα αποθηκεύονται σε έναν κεντρικό διακομιστή, το blockchain διανέμει τις εγγραφές των συναλλαγών σε ένα δίκτυο υπολογιστών (κόμβων) που βρίσκονται σε διαφορετικές τοποθεσίες παγκοσμίως. [1]

Ένα από τα βασικά χαρακτηριστικά του blockchain είναι η απουσία κεντρικού φορέα ελέγχου. Η επικύρωση και η καταγραφή των συναλλαγών πραγματοποιείται από έναν μεγάλο αριθμό κόμβων που ανήκουν στο δίκτυο. Κανένας μεμονωμένος κόμβος δεν έχει τον απόλυτο έλεγχο των δεδομένων, γεγονός που διασφαλίζει τη διαφάνεια και την ασφάλεια των συναλλαγών. Το blockchain λειτουργεί ως ένα αποκεντρωμένο δίκτυο, όπου κάθε χρήστης συμμετέχει ισότιμα στη διαδικασία, επιβεβαιώνοντας ταυτόχρονα τις συναλλαγές.

Μόλις μια συναλλαγή καταγραφεί στο blockchain, δεν μπορεί να τροποποιηθεί ή να διαγραφεί, καθώς η ακεραιότητά της επιβεβαιώνεται από όλους τους κόμβους του δικτύου. Όταν μια συναλλαγή επιβεβαιώνεται, προστίθεται σε ένα μπλοκ, το οποίο στη συνέχεια συνδέεται με προηγούμενα μπλοκ, σχηματίζοντας μια αλυσίδα συναλλαγών - τη λεγόμενη αλυσίδα μπλοκ (blockchain).

Η ασφάλεια και η ακεραιότητα του blockchain διασφαλίζονται μέσω κρυπτογραφικών τεχνικών και μηχανισμών συναίνεσης, όπως το Proof of Work (PoW) ή το Proof of Stake (PoS). Αυτοί οι μηχανισμοί διασφαλίζουν ότι όλες οι εγγραφές είναι έγκυρες και δεν μπορούν να τροποποιηθούν χωρίς την έγκριση της πλειονότητας των κόμβων.

2.1.2. Ιστορική Αναδρομή

Η ιστορία του blockchain ξεκινά τη δεκαετία του '90, όταν οι Stuart Haber και W. Scott Stornetta παρουσίασαν το 1991 ένα σύστημα για την ασφαλή χρονοσφράγιση των εγγράφων. Το σύστημα αυτό λειτουργούσε χωρίς την ανάγκη εμπιστοσύνης σε έναν κεντρικό οργανισμό. Η βασική ιδέα ήταν η δημιουργία ενός συστήματος όπου οι χρήστες θα μπορούσαν να χρονοσφραγίζουν τα έγγραφά τους, καθιστώντας τα αναλλοίωτα και καθολικά αναμφισβήτητα διότι εξασφαλίζεται η ακεραιότητα και αυθεντικότητά τους. Αυτή η ιδέα οδήγησε στην ανάπτυξη ενός συστήματος που βασίζεται σε κρυπτογραφικούς κώδικες και ένα αλυσιδωτό σύστημα μπλοκ, όπου κάθε νέο μπλοκ συνδέεται με το προηγούμενο. Οι κρυπτογραφικοί κώδικες εξασφαλίζουν την ασφάλεια και την ακεραιότητα των δεδομένων, τα οποία στη συνέχεια εγγράφονται σε μπλοκ, και κάθε μπλοκ συνδέεται με το προηγούμενο δημιουργώντας ένα αλυσιδωτό ιστορικό. Έτσι, οι χρήστες μπορούν να εμπιστευτούν την ακεραιότητα και τη σειρά των εγγραφών χωρίς την ανάγκη ενός κεντρικού οργανισμού. Αυτή η πρωτότυπη ιδέα από τους Haber και Stornetta δεν

περιλάμβανε τη δημιουργία ψηφιακών νομισμάτων, αλλά ήταν το πρώτο βήμα προς την ανάπτυξη της τεχνολογίας του blockchain.

Η τεχνολογία blockchain προέκυψε το 2008 ως πρόταση στον τομέα της επιστήμης των υπολογιστών. Ο στόχος ήταν να δημιουργηθεί ένα ασφαλές και άμεσο σύστημα διαπραγμάτευσης περιουσιακών στοιχείων μεταξύ χρηστών που δεν εμπιστεύονται απαραίτητα ο ένας τον άλλον. Ο όρος "blockchain" πρωτοεμφανίζεται σε ένα έγγραφο που δημοσιεύτηκε από τον μυστηριώδη Satoshi Nakamoto, όπου παρουσίαζε την ιδέα του Bitcoin ως ένα αποκεντρωμένο δίκτυο ηλεκτρονικών συναλλαγών. Το Bitcoin επιτρέπει άμεσες χρηματοπιστωτικές συναλλαγές χωρίς τη μεσολάβηση κάποιου χρηματοπιστωτικού ιδρύματος.

Το blockchain επιτρέπει σε δύο χρήστες να συναλλάσσονται σε ένα peer-to-peer (P2P) δίκτυο, καταγράφοντας αυτές τις συναλλαγές με κατακευκτικό τρόπο σε ολόκληρο το δίκτυο. Ο μηχανισμός συναίνεσης χρησιμοποιείται για την επαλήθευση των συναλλαγών, ενισχύοντας την εμπιστοσύνη και την ακρίβεια των δεδομένων στο σύστημα. Κάθε συναλλαγή που πραγματοποιείται μεταξύ των χρηστών καταγράφεται σε ένα μπλοκ, το οποίο αναφέρεται μαθηματικά στο προηγούμενο μπλοκ, δημιουργώντας έτσι μια αλυσίδα μπλοκ. Αυτή η αλυσίδα αποτελείται από το ιστορικό όλων των συναλλαγών που έχουν πραγματοποιηθεί στο δίκτυο, με κάθε νέο μπλοκ που προστίθεται να επιβεβαιώνει τις προηγούμενες συναλλαγές, οι οποίες έχουν ολοκληρωθεί αλλά δεν έχουν ακόμη αποθηκευτεί στο δίκτυο δεν έχουν επισημανθεί ως "ολοκληρωμένες" και δεν έχουν ενσωματωθεί στο blockchain. Αυτές οι συναλλαγές μπορεί να περιμένουν ακόμη να επιβεβαιωθούν από το δίκτυο ή να περιμένουν να περιληφθούν σε ένα νέο μπλοκ. Οι συναλλαγές πρέπει να επαληθευτούν από τους κόμβους του δικτύου προτού προστεθούν στο blockchain. Αυτή η επιβεβαίωση μπορεί να περιλαμβάνει τον έλεγχο της έγκυρης υπογραφής, του υπολογισμού του μεγέθους του κρυπτογραφικού αλγορίθμου, και άλλες διαδικασίες που εξαρτώνται από το συγκεκριμένο πρωτόκολλο του blockchain. Μέχρι να επιβεβαιωθούν και να περιληφθούν σε ένα νέο μπλοκ, αυτές οι συναλλαγές θεωρούνται ως μη επικυρωμένες ή μη επιβεβαιωμένες

Το Bitcoin, που κατασκευάστηκε το 2009, αποτέλεσε το πρώτο παράδειγμα εφαρμογής της τεχνολογίας blockchain. Το Bitcoin λειτουργεί ως αποκεντρωμένο νόμισμα, επιτρέποντας στους χρήστες να πραγματοποιούν ασφαλείς και ανώνυμες συναλλαγές χωρίς την ανάγκη ενδιάμεσων αρχών. Το Bitcoin πρόσφερε μια απλή μορφή ηλεκτρονικού νομίσματος που λειτουργούσε με βάση την τεχνολογία blockchain. Οι συναλλαγές επαληθεύονταν και καταγράφονταν σε ένα δημόσιο και ανθεκτικό βιβλίο, επιτρέποντας τις αναλήψεις αξίας χωρίς την ανάγκη μεσολάβησης τρίτων.

Ακολούθησε το Ethereum το 2015, το οποίο επέκτεινε τις δυνατότητες της τεχνολογίας blockchain. Το Ethereum δεν περιορίζεται μόνο στο να λειτουργεί ως ψηφιακό νόμισμα, αλλά επιτρέπει επίσης την εκτέλεση έξυπνων συμβολαίων. Τα έξυπνα συμβόλαια είναι προγράμματα που εφαρμόζουν αυτόματα συμφωνίες κατά τη διάρκεια της εκτέλεσής τους χωρίς την ανάγκη ενδιάμεσης εμπλοκής. Αυτό επιτρέπει τη δημιουργία ποικίλων εφαρμογών, όχι μόνο για ψηφιακά νομίσματα, αλλά και για εκτελέσιμες συμφωνίες σε διάφορους τομείς. Αυτό επιτρέπει τη δημιουργία ποικίλων εφαρμογών, όχι μόνο για ψηφιακά νομίσματα, αλλά και για εκτελέσιμες συμφωνίες σε διάφορους τομείς. Ανάμεσα σε αυτές περιλαμβάνεται η ενίσχυση της ασφάλειας σε

συναλλαγές με τη χρήση έξυπνων συμβολαίων, η αυτοματοποίηση των διαδικασιών πληρωμών σε freelance δίκτυα για τη διευκόλυνση της χρηματοδότησης, καθώς και η ανάπτυξη ποικίλων εφαρμογών όπως αποκεντρωμένες ψηφιακές αγορές και παιχνίδια. Αυτή η ευελιξία και δυνατότητα προσφέρει ένα πλούσιο οικοσύστημα για καινοτομία και ανάπτυξη σε πολλούς τομείς, ενθαρρύνοντας τη δημιουργία νέων λύσεων και την ανάπτυξη εφαρμογών που εξυπηρετούν διαφορετικές ανάγκες και χρήσεις. [2]

2.1.3. Λειτουργία Blockchain

Το blockchain είναι μια καινοτόμος τεχνολογία που λειτουργεί ως ένα αποκεντρωμένο και διανεμημένο ψηφιακό βιβλίο καταγραφής συναλλαγών. Η βασική αρχή του blockchain είναι η δημιουργία και η διατήρηση μιας αλυσίδας μπλοκ (blocks) που περιέχουν δεδομένα συναλλαγών. Κάθε μπλοκ περιλαμβάνει μια συγκεκριμένη ομάδα συναλλαγών και είναι συνδεδεμένο με το προηγούμενο μπλοκ μέσω ενός μοναδικού κρυπτογραφικού κατακερματισμού (hash). Αυτή η αλυσίδα μπλοκ δημιουργεί ένα αδιάσπαστο ιστορικό όλων των συναλλαγών που έχουν πραγματοποιηθεί στο δίκτυο, το οποίο είναι διαφανές και ασφαλές.

Το blockchain είναι ένα διανεμημένο σύστημα στο οποίο όλοι οι κόμβοι (nodes) του δικτύου διατηρούν ένα αντίγραφο του blockchain. Αυτή η αποκεντρωμένη φύση του συστήματος εξασφαλίζει ότι δεν υπάρχει κεντρικός έλεγχος, μειώνοντας τον κίνδυνο αποτυχίας λόγω ενός κεντρικού σημείου. Η αποκέντρωση αυξάνει επίσης την ανθεκτικότητα του συστήματος έναντι επιθέσεων, καθώς ένας επιτιθέμενος θα πρέπει να παραβιάσει την πλειονότητα των κόμβων για να αλλάξει τα δεδομένα.

Οι συναλλαγές στο blockchain επαληθεύονται και προστίθενται στο βιβλίο καταγραφής μέσω μηχανισμών συναίνεσης (consensus mechanisms). Αυτοί οι μηχανισμοί διασφαλίζουν ότι όλοι οι κόμβοι του δικτύου συμφωνούν για την εγκυρότητα των συναλλαγών. Ένας από τους πιο γνωστούς μηχανισμούς συναίνεσης είναι το Proof of Work (PoW). Στο PoW, οι κόμβοι που αποκαλούνται "miners" (εξορύκτες) ανταγωνίζονται για να επιλύσουν πολύπλοκα μαθηματικά προβλήματα χρησιμοποιώντας υπολογιστική ισχύ. Ο πρώτος που θα λύσει το πρόβλημα, προσθέτει το νέο μπλοκ στο blockchain και ανταμείβεται με κρυπτονομίσματα.

Το blockchain χρησιμοποιεί κρυπτογραφικές τεχνικές για να διασφαλίσει την ασφάλεια και την ακεραιότητα των δεδομένων. Κάθε μπλοκ περιέχει έναν κρυπτογραφικό κατακερματισμό του προηγούμενου μπλοκ, δημιουργώντας έτσι μια αλυσίδα ασφαλών μπλοκ. Οποιαδήποτε αλλαγή στα δεδομένα ενός μπλοκ θα αλλάξει τον κατακερματισμό του, καθιστώντας αμέσως εμφανείς οποιεσδήποτε παραποιήσεις. Αυτός ο κρυπτογραφικός κατακερματισμός εξασφαλίζει ότι τα δεδομένα στο blockchain δεν μπορούν να τροποποιηθούν ή να διαγραφούν χωρίς να ανιχνευθούν. Μάλιστα, για να γίνει τροποποίηση έστω και μιας εγγραφής δεδομένων, θα πρέπει να γίνει τροποποίηση όλων των καταγεγραμμένων μπλοκ μέχρι και το αρχικό, πράγμα που είναι αρκετά δύσκολο να επιτευχθεί, διότι οι αλλαγές θα πρέπει να γίνουν σε όλο το δίκτυο, και επιφέρει μεγάλο κόστος. Το τελευταίο ουσιαστικά προσδιορίζει πως το blockchain λίγο πολύ εξασφαλίζει την αμετάβλητη καταγραφή των συναλλαγών. Αυτή η αμετάβλητη φύση του blockchain το καθιστά

ιδανικό για την αποθήκευση κρίσιμων δεδομένων που απαιτούν υψηλή ασφάλεια και διαφάνεια, όπως είναι τα δεδομένα συναλλαγών.

Κάθε χρήστης του blockchain έχει ένα ζευγάρι κλειδιών: ένα δημόσιο και ένα ιδιωτικό. Το δημόσιο κλειδί λειτουργεί ως η διεύθυνση του χρήστη στο δίκτυο, επιτρέποντας σε άλλους χρήστες να του στείλουν συναλλαγές. Το ιδιωτικό κλειδί χρησιμοποιείται για την υπογραφή των συναλλαγών του χρήστη, εξασφαλίζοντας την ακεραιότητα και την αυθεντικότητα των δεδομένων. Η υπογραφή μιας συναλλαγής με το ιδιωτικό κλειδί δημιουργεί έναν μοναδικό κρυπτογραφικό κώδικα που μπορεί να επαληθευτεί με το δημόσιο κλειδί του χρήστη. [1] [2]

2.1.4. Εφαρμογές Blockchain

Το blockchain έχει πολλές εφαρμογές σε διάφορους τομείς. Στον χρηματοοικονομικό τομέα, χρησιμοποιείται για ασφαλείς και διαφανείς συναλλαγές χωρίς την ανάγκη μεσολαβητών, όπως τράπεζες. Το Bitcoin και το Ethereum είναι δύο από τα πιο γνωστά παραδείγματα κρυπτονομισμάτων που βασίζονται σε τεχνολογία blockchain. Στην εφοδιαστική αλυσίδα, το blockchain παρέχει διαφάνεια και ακεραιότητα στην παρακολούθηση της προέλευσης και της διακίνησης προϊόντων. Οι εταιρείες μπορούν να χρησιμοποιούν το blockchain για να παρακολουθούν κάθε στάδιο της παραγωγής και της διανομής, εξασφαλίζοντας την ποιότητα και τη γνησιότητα των προϊόντων.

Στον τομέα της ψηφιακής ταυτότητας, το blockchain διευκολύνει την ασφαλή και αδιάβλητη αποθήκευση και διαχείριση προσωπικών δεδομένων. Οι χρήστες μπορούν να δημιουργήσουν και να διαχειριστούν τις ψηφιακές ταυτότητές τους με ασφάλεια, αποφεύγοντας την ανάγκη για κεντρικούς φορείς πιστοποίησης. Στην υγειονομική περίθαλψη, το blockchain μπορεί να βελτιώσει την ασφάλεια και την ακεραιότητα των ιατρικών δεδομένων και των αρχείων ασθενών. Οι ιατρικοί πάροχοι μπορούν να μοιράζονται με ασφάλεια τα ιατρικά δεδομένα των ασθενών, εξασφαλίζοντας την ακεραιότητα και την εμπιστευτικότητα των πληροφοριών.

Η λειτουργία του blockchain και οι δυνατότητές του το καθιστούν μια επαναστατική τεχνολογία με εφαρμογές σε πολλούς τομείς. Η περαιτέρω ανάπτυξη και η ερευνητική δραστηριότητα στον τομέα αυτό μπορούν να αποκαλύψουν νέες χρήσεις και βελτιώσεις, ενισχύοντας την ασφάλεια, την αποδοτικότητα και τη διαφάνεια στις ψηφιακές συναλλαγές και τη διαχείριση δεδομένων.

2.1.5. Τύποι Blockchain

Οι τέσσερις βασικοί τύποι blockchain - δημόσιο, ιδιωτικό, κοινοπρακτικό και υβριδικό - αντιπροσωπεύουν διάφορες προσεγγίσεις στη χρήση της τεχνολογίας blockchain. Καθένας από αυτούς τους τύπους έχει τα δικά του χαρακτηριστικά και πλεονεκτήματα, προσφέροντας λύσεις σε διάφορα περιβάλλοντα και εφαρμογές.

2.1.5.1. Δημόσια Blockchain

Ένα δημόσιο (public) blockchain αποτελεί ένα αποκεντρωμένο και κατανεμημένο σύστημα, όπου ένας μη ορισμένος αριθμός συμμετεχόντων μπορεί να μοιραστεί και να επιβεβαιώσει αμοιβαία πληροφορίες σχετικά με συναλλαγές που λαμβάνουν χώρα στο σύστημα. Δεν υπάρχει ξεχωριστή οντότητα που διαχειρίζεται το σύστημα, επιτρέποντας σε οποιονδήποτε να συμμετέχει ανώνυμα, χωρίς περιορισμούς στην εξουσία. Ένα παράδειγμα εφαρμογής του δημόσιου blockchain είναι το Bitcoin, ένα διάσημο κρυπτονόμισμα που χρησιμοποιείται παγκοσμίως.

Τα δημόσια blockchains αποτελούν ενεργό αντικείμενο έρευνας στον τομέα της τεχνολογίας κατανεμημένου λογιστικού (DLT), η οποία αποτελεί τον πυρήνα τους. Τα δημόσια blockchains μπορούν να χρησιμοποιηθούν αποτελεσματικά στον χρηματοοικονομικό τομέα, μέσω συναλλαγών όπως κρυπτονομίσματα και διεθνείς μεταφορές χρημάτων, αλλά επίσης και σε άλλους τομείς, όπως το crowdfunding και οι μεταφορές. Αυτό συμβαίνει διότι επιτρέπει τη διαδικασία πιστοποίησης, γνωστή και ως συναίνεση, στην οποία όλοι οι κόμβοι φτάνουν σε συμφωνία για την ακεραιότητα και εγκυρότητα των δεδομένων που καταγράφονται στο blockchain. Επιπλέον, είναι ένα ανοικτό σύστημα το οποίο επιτρέπει σε οποιονδήποτε να δημιουργεί συναλλαγές και να συμμετέχει ως κόμβος, παρέχοντας υψηλή αξιοπιστία και ακεραιότητα μέσω της επαλήθευσης της εργασίας των συμμετεχόντων.

Παρά τα πλεονεκτήματα αυτά, υπάρχει ένα μειονέκτημα που πρέπει να ληφθεί υπόψη: η πιθανή μείωση της ταχύτητας καταγραφής και επεξεργασίας δεδομένων. Αυτό οφείλεται στο γεγονός ότι οι εγγραφές όλων των συμμετεχόντων στο δίκτυο αποθηκεύονται και μοιράζονται, ενδεχομένως επιβαρύνοντας την απόδοση του δικτύου. Παρόλο που ο αριθμός των συμμετεχόντων είναι ένας κρίσιμος παράγοντας, η ταχύτητα εξαρτάται επίσης από άλλους παράγοντες, όπως οι απαιτήσεις του δικτύου, τα χαρακτηριστικά της τεχνολογίας και ο σχεδιασμός του συστήματος επεξεργασίας και καταγραφής δεδομένων. Συνεπώς, για μια πλήρη κατανόηση, πρέπει να ληφθούν υπόψη όλοι αυτοί οι παράγοντες. [6] [9]

2.1.5.2. Ιδιωτικά Blockchain

Τα ιδιωτικά (private) blockchain αντιπροσωπεύουν έναν τύπο blockchain όπου η πρόσβαση και ο έλεγχος είναι περιορισμένοι. Σε αντίθεση με τα δημόσια blockchains που είναι ανοικτά σε οποιονδήποτε, τα ιδιωτικά blockchains λειτουργούν με περιορισμένο αριθμό συμμετεχόντων, οι οποίοι χρειάζονται άδεια για να συμμετέχουν. Τα ιδιωτικά blockchains μπορούν να είναι κεντριοποιημένα ή αποκεντρωμένα, ανάλογα με τη δομή και το μοντέλο τους. Σε πολλές περιπτώσεις, τα ιδιωτικά blockchains ελέγχονται από μια οργάνωση ή μια ομάδα οργανώσεων, και επομένως μπορεί να χαρακτηρίζονται ως κεντριοποιημένα.

Ωστόσο, υπάρχουν και ιδιωτικά blockchains που λειτουργούν με αποκεντρωμένο τρόπο, όπου ο έλεγχος και η λειτουργία τους διανέμονται μεταξύ ενός περιορισμένου αριθμού συμμετεχόντων χωρίς την κεντρική αρχή ελέγχου. Για να καθορίσουμε εάν ένα ιδιωτικό blockchain

είναι κεντριοποιημένο ή αποκεντρωμένο, πρέπει να εξετάσουμε ποιος έχει τον τελικό έλεγχο και τη διαχείριση του δικτύου. Είναι σημαντικό να αναφέρουμε ότι ένα ιδιωτικό blockchain που δεν είναι κεντριοποιημένο δεν σημαίνει απαραίτητα ότι είναι κοινοπρακτικό. Η έννοια του κοινοπρακτικού blockchain αναφέρεται σε ένα δίκτυο όπου διάφοροι συμμετέχοντες (συνήθως οργανώσεις) συνεργάζονται και διαχειρίζονται από κοινού το δίκτυο. Ένα αποκεντρωμένο ιδιωτικό blockchain μπορεί να λειτουργεί με αποκεντρωμένο τρόπο, αλλά να μην ανήκει απαραίτητα σε μια κοινοπραξία, καθώς η αποκέντρωση μπορεί να επιτευχθεί και με άλλους τρόπους.

Είναι σημαντικό να αναφέρουμε ότι ένα ιδιωτικό blockchain που δεν είναι κεντριοποιημένο δεν σημαίνει απαραίτητα ότι είναι κοινοπρακτικό. Η έννοια του κοινοπρακτικού blockchain αναφέρεται σε ένα δίκτυο όπου διάφοροι συμμετέχοντες (συνήθως οργανώσεις) συνεργάζονται και διαχειρίζονται από κοινού το δίκτυο. Ένα αποκεντρωμένο ιδιωτικό blockchain μπορεί να λειτουργεί με αποκεντρωμένο τρόπο, αλλά να μην ανήκει απαραίτητα σε μια κοινοπραξία, καθώς η αποκέντρωση μπορεί να επιτευχθεί και με άλλου

Ένα από τα κύρια χαρακτηριστικά των ιδιωτικών blockchains είναι η έμφαση στην ιδιωτικότητα. Με άλλα λόγια, μόνο όσοι έχουν εγκριθεί έχουν πρόσβαση στα δεδομένα. Αυτό καθιστά αυτούς τους τύπους blockchains κατάλληλους για χρήση σε επιχειρήσεις και οργανισμούς, διότι προσφέρουν την δυνατότητα χειρισμού των δεδομένων τους με ασφάλεια, ακρίβεια και αποτελεσματικότητα.. Ωστόσο, δεν εξασφαλίζεται πλήρως η ιδιωτικότητα. Αν όλοι οι συμμετέχοντες έχουν πρόσβαση στα δεδομένα, τότε η ιδιωτικότητα μπορεί να απειληθεί, καθώς η διαφάνεια των συναλλαγών δεν είναι εξασφαλισμένη. Συνεπώς, πέρα από την περιορισμένη πρόσβαση στα δεδομένα, είναι σημαντικό το ιδιωτικό blockchain να είναι επίσης ασφαλές.

Αυτά τα blockchains είναι συχνά πιο γρήγορα και αποδοτικά σε σύγκριση με τα δημόσια blockchains, καθώς ο περιορισμένος αριθμός συμμετεχόντων επιτρέπει γρήγορες συναλλαγές. Αυτό είναι σημαντικό, ειδικά σε περιβάλλοντα (πχ. λιανικό κατάστημα) όπου η ταχύτητα εκτέλεσης είναι ουσιώδης. Τα ιδιωτικά blockchains επίσης επιτρέπουν ευκολότερη κλιμάκωση, καθώς η προσθήκη ή η αφαίρεση συμμετεχόντων δεν επηρεάζει το σύστημα σε μεγάλο βαθμό. Αυτό τα καθιστά ευέλικτα και εύκολα προσαρμόσιμα σε αλλαγές. Αλλαγές οι οποίες αφορούν τη δυνατότητα του ιδιωτικού blockchain να προσαρμοστεί σε διάφορες αλλαγές που μπορεί να επηρεάσουν τη λειτουργία μιας επιχείρησης, όπως η επέκταση της παρουσίας της, οι οικονομικές αναδιαρθρώσεις ή οι τεχνολογικές εξελίξεις. Το ιδιωτικό blockchain πρέπει να είναι ευέλικτο και προσαρμόσιμο, ώστε να μπορεί να προσαρμοστεί στις μεταβαλλόμενες ανάγκες και απαιτήσεις της επιχείρησης.

Υπάρχουν όμως και μειονεκτήματα. Η ανάγκη για εμπιστοσύνη ανάμεσα στους συμμετέχοντες είναι υψηλή, καθώς και οι συμμετέχοντες πρέπει να εμπιστεύονται την οντότητα που ελέγχει το ιδιωτικό blockchain. Επίσης, η ασφάλεια μπορεί να διακυβευτεί εάν ένας τρίτος καταφέρει να έχει πρόσβαση στο κεντρικό σύστημα διαχείρισης. Το σύστημα διαχείρισης σε ένα ιδιωτικό blockchain μπορεί να είναι και κεντρικό ή κατακεντρωμένο, ανάλογα με τη σχεδίαση και τις απαιτήσεις του δικτύου. Συνήθως, σε επιχειρησιακά περιβάλλοντα, το σύστημα διαχείρισης έχει κεντρικό έλεγχο από μια αξιόπιστη αρχή ή οργανισμό. Ωστόσο, μπορεί να υπάρχουν και

περιπτώσεις κατανεμημένων συστημάτων διαχείρισης σε ιδιωτικά blockchains, όπου ο έλεγχος και η λειτουργία του δικτύου είναι κατανεμημένα μεταξύ των συμμετεχόντων.

Όσον αφορά την ασφάλεια, δεν μπορούμε να πούμε απαραίτητα ότι το ιδιωτικό blockchain είναι περισσότερο ή λιγότερο ασφαλές από το δημόσιο. Και τα δύο είδη blockchains έχουν τα πλεονεκτήματά τους όσον αφορά την ασφάλεια και τους κινδύνους τους. Γενικά, στο ιδιωτικό blockchain, ο έλεγχος των πρόσβασης είναι πιο εύκολος και μπορεί να υπάρχουν μηχανισμοί για τη διαχείριση της ασφάλειας που είναι πιο ευέλικτοι σε σχέση με τα δημόσια blockchains. Ωστόσο, η ασφάλεια εξαρτάται σε μεγάλο βαθμό από τον τρόπο υλοποίησης, τις πρακτικές διαχείρισης και τις αποφάσεις σχεδίασης του κάθε συστήματος. [6] [9]

2.1.5.3. Κοινοπρακτικά Blockchain

Τα κοινοπρακτικά (consortium) blockchains, εμφανίζουν πολλές ομοιότητες με τη λειτουργία των ιδιωτικών blockchains, αλλά διαφοροποιούνται στο γεγονός ότι ο έλεγχος δεν είναι συγκεντρωμένος σε μία μόνο εταιρία ή οργανισμό, αλλά ανήκει σε ένα σύμπλεγμα εταιριών. Κάθε εταιρία μπορεί να διαθέτει έναν κόμβο στο δίκτυο, και οι διαχειριστές του δικτύου είναι υπεύθυνοι για την επιλογή των κόμβων που θα συμμετέχουν στα πρωτόκολλα συναίνεσης.

Στα κοινοπρακτικά blockchains, ο έλεγχος δεν είναι συγκεντρωμένος σε μία μόνο εταιρία ή οργανισμό, αλλά ανήκει σε ένα σύμπλεγμα εταιριών. Κάθε εταιρία μπορεί να διαθέτει έναν κόμβο στο δίκτυο, και οι διαχειριστές του δικτύου είναι υπεύθυνοι για την επιλογή των κόμβων που θα συμμετέχουν στα πρωτόκολλα συναίνεσης. Αυτό σημαίνει ότι κάθε εταιρία μπορεί να έχει έναν ή περισσότερους κόμβους στο δίκτυο, ανάλογα με τον ρόλο και την συμμετοχή της στο σύνολο του συστήματος.

Το μοντέλο αυτό ενθαρρύνει τη συνεργασία και τη συμμετοχή από διάφορες εταιρίες, παρέχοντας περισσότερη διαφάνεια και αποφεύγοντας τον κεντρικό έλεγχο. Καθώς οι διαχειριστές αποφασίζουν ποιους κόμβους θα επιτρέπουν να συμμετέχουν, επιτυγχάνεται ισορροπία μεταξύ αποκεντρωμένης διαχείρισης και συνεργατικής λειτουργίας.

Από θέμα ασφάλειας, τα κοινοπρακτικά blockchains προσφέρουν συγκεκριμένα πλεονεκτήματα. Η συμμετοχή στο δίκτυο είναι περιορισμένη και ελεγχόμενη από τους διαχειριστές, μειώνοντας την πιθανότητα εισβολής από κακόβουλους χρήστες. Καθώς οι κόμβοι διαχειρίζονται από γνωστές και αξιόπιστες εταιρίες, υπάρχει καλύτερη διαχείριση των δικαιωμάτων και των προσβάσεων, γεγονός που ενισχύει την ασφάλεια. Επιπλέον, οι συμμετέχουσες εταιρίες μπορούν να συνεργαστούν για την ανάπτυξη και υλοποίηση κοινών πρωτοκόλλων ασφάλειας, καθιστώντας το δίκτυο πιο ανθεκτικό σε επιθέσεις.

Παρά τα πλεονεκτήματα, τα κοινοπρακτικά blockchains έχουν και μειονεκτήματα. Η ανάγκη για συνεργασία και εμπιστοσύνη μεταξύ των συμμετεχόντων εταιριών μπορεί να δημιουργήσει επιπλοκές, ιδιαίτερα αν υπάρξουν διαφωνίες ή συγκρούσεις συμφερόντων. Επίσης, η περιορισμένη αποκέντρωση μπορεί να θεωρηθεί μειονέκτημα σε σύγκριση με τα δημόσια blockchains, όπου ο καθένας μπορεί να συμμετέχει και να επαληθεύει τις συναλλαγές. Η δημιουργία και διαχείριση ενός κοινοπρακτικού blockchain μπορεί να απαιτεί σημαντικές δαπάνες

και συντονισμό μεταξύ των συμμετεχόντων, γεγονός που μπορεί να καθυστερήσει την ανάπτυξη και την υλοποίηση νέων εφαρμογών και υπηρεσιών. Η ανάγκη για ομοφωνία στις αποφάσεις σχετικά με την εξέλιξη του δικτύου μπορεί επίσης να είναι χρονοβόρα και να καθυστερεί την υιοθέτηση των απαραίτητων αλλαγών. Παράλληλα, η εμπιστευτικότητα των δεδομένων μπορεί να τεθεί υπό αμφισβήτηση αν δεν υπάρχει απόλυτη διαφάνεια και σαφείς κανόνες σχετικά με τη διαχείριση και την πρόσβαση στα δεδομένα από τους συμμετέχοντες. [6] [9]

2.1.5.4. Υβριδικά Blockchain

Τα υβριδικά blockchains αντιπροσωπεύουν έναν ενδιάμεσο τύπο blockchain που συνδυάζει χαρακτηριστικά τόσο από δημόσια όσο και από ιδιωτικά blockchains. Ένα από τα κύρια πλεονεκτήματά τους είναι η ασφάλεια. Το σύστημα λειτουργεί με έναν συνδυασμό κεντρικών και αποκεντρωμένων στοιχείων, που παρέχει ένα επίπεδο ελέγχου που μπορεί να προσαρμοστεί σύμφωνα με τις ανάγκες και τις προτιμήσεις του δικτύου. Αυτό επιτρέπει στις εταιρείες να διαχειρίζονται την πρόσβαση και τον έλεγχο των δεδομένων τους με πιο εξειδικευμένο τρόπο.

Η λειτουργία των υβριδικών blockchain είναι εξαιρετικά ευέλικτη. Συνδυάζονται τα πλεονεκτήματα των ιδιωτικών και δημόσιων blockchains, παρέχοντας ένα πλαίσιο όπου οι εταιρείες μπορούν να επωφεληθούν τόσο από την ιδιωτικότητα όσο και από τη διαφάνεια των δημόσιων blockchains. Αυτό τους επιτρέπει να προσαρμόζονται στις ανάγκες τους, επιτρέποντας παράλληλα τη διατήρηση της ασφάλειας και της εμπιστοσύνης στο δίκτυο.

Επιπλέον, η πρόσβαση είναι ελεγχόμενη, επιτρέποντας στους χρήστες να έχουν πρόσβαση μόνο σε επιλεγμένες πληροφορίες ή λειτουργίες, ενώ το υπόλοιπο περιεχόμενο μπορεί να παραμένει ασφαλές και προστατευμένο. Αυτό είναι σημαντικό για τη διατήρηση της απορρήτου και της εμπιστευτικότητας των δεδομένων, ενώ ταυτόχρονα επιτρέπει την εκμετάλλευση των οφελών της τεχνολογίας blockchain.

Συνολικά, τα υβριδικά blockchains αντιπροσωπεύουν έναν πολύτιμο συνδυασμό ασφάλειας, ευελιξίας και ελέγχου, παρέχοντας ένα περιβάλλον όπου οι επιχειρήσεις μπορούν να αξιοποιήσουν πλήρως τα οφέλη της τεχνολογίας blockchain με εμπιστοσύνη και ασφάλεια. [9]

Ωστόσο, όπως και κάθε τεχνολογία, έτσι και τα υβριδικά blockchains έχουν και αυτά τα μειονεκτήματά τους. Η πολυπλοκότητα της εγκατάστασης και της διαχείρισης ενός υβριδικού blockchain μπορεί να είναι σημαντική, απαιτώντας εξειδικευμένες γνώσεις και πόρους. Επίσης, η ανάγκη για συνδυασμό κεντρικών και αποκεντρωμένων στοιχείων μπορεί να επιφέρει προκλήσεις στη διαλειτουργικότητα και στη συντήρηση του δικτύου. Τέλος, η υιοθέτηση υβριδικών blockchain μπορεί να είναι πιο δαπανηρή σε σχέση με τις άλλες μορφές blockchain λόγω της πολυπλοκότητάς τους και των απαιτήσεων σε υποδομές και ασφάλεια. [6] [9]

2.1.6. Πλεονεκτήματα & Μειονεκτήματα Blockchain

Το blockchain αποτελεί μια τεχνολογία που έχει ανατρέψει τον τρόπο που αντιλαμβανόμαστε τη διαχείριση των δεδομένων και των συναλλαγών. Πρόκειται για ένα αποκεντρωμένο, κρυπτογραφικό και ασφαλές σύστημα που επιτρέπει την αξιόπιστη αποθήκευση, διαχείριση και ανταλλαγή πληροφοριών μεταξύ χρηστών, χωρίς την ανάγκη για ενδιάμεσους, όπως τράπεζες. Η ανάλυση των πλεονεκτημάτων αυτής της τεχνολογίας αποκαλύπτει τη σημαντική αλλαγή στον τρόπο που διαχειριζόμαστε τα δεδομένα και τις συναλλαγές.

- Η υψηλή ασφάλεια των δεδομένων στο blockchain αποτελεί κορυφαίο πλεονέκτημα αυτής της τεχνολογίας, διασφαλίζοντας ότι τα δεδομένα παραμένουν ακέραια και αδύνατο να υποστούν αλλοίωση ή τροποποίηση. Αυτό το χαρακτηριστικό είναι κρίσιμο σε τομείς, όπως ο χρηματοοικονομικός, όπου η αξιοπιστία και ακεραιότητα των συναλλαγών είναι αποφασιστική. Ένα από τα κύρια πλεονεκτήματα του blockchain είναι η δυνατότητα διαμοιρασμού της βάσης δεδομένων του χωρίς την ανάγκη για κεντρικό φορέα ή εξουσία. Λόγω της αποκεντρωμένης φύσης του, είναι σχεδόν αδύνατο να αλλοιωθούν τα δεδομένα, σε σύγκριση με τις παραδοσιακές βάσεις δεδομένων. Όλοι οι συμμετέχοντες στο δίκτυο έχουν πρόσβαση στην ίδια βάση δεδομένων και μπορούν να δουν όλες τις συναλλαγές, ενισχύοντας την ασφάλεια και τη διαφάνεια. Ο κατακερματισμένος μηχανισμός συναίνεσης εξασφαλίζει ότι όλοι οι χρήστες συμφωνούν στην εγκυρότητα των συναλλαγών, καθιστώντας το σύστημα υψηλά ανθεκτικό στην παραποίηση. Η αποκεντρωμένη φύση του blockchain καθιστά εξαιρετικά δύσκολο για τους επιτιθέμενους να παραβιάσουν το σύστημα. Το κατακερματισμένο βιβλίο διατηρείται σε πολλούς κόμβους, και για να πετύχει μια επίθεση, ο δράστης θα έπρεπε να καταλάβει τον έλεγχο τουλάχιστον 51% των κόμβων του δικτύου. Αυτή η απαίτηση για πλειοψηφικό έλεγχο λειτουργεί ως ισχυρός προστατευτικός μηχανισμός, καθιστώντας σχεδόν αδύνατη την επίθεση από κακόβουλους εισβολείς χωρίς υπερβολικούς υπολογιστικούς πόρους.

Η ασφάλεια στο blockchain επιτυγχάνεται κυρίως μέσω της μοναδικής ταυτοποίησης κάθε χρήστη και της χρήσης κρυπτογραφικών κατακερματισμών. Κάθε νέος χρήστης λαμβάνει μια μοναδική ταυτότητα συνδεδεμένη με τον λογαριασμό του, προσθέτοντας ένα επίπεδο ασφαλείας. Κάθε συναλλαγή και εγγραφή κρυπτογραφείται με τρόπο που δυσχεραίνει την αλλοίωση ή την υποκλοπή δεδομένων από επιτιθέμενους. Επιπλέον, κάθε νέο μπλοκ περιλαμβάνει την τιμή κατακερματισμού του προηγούμενου μπλοκ, δημιουργώντας μια αλυσίδα που είναι δύσκολο να παραβιαστεί. Οι κρυπτογραφικοί κατακερματισμοί περιέχουν στοιχεία όπως ο αριθμός ταυτότητας του μπλοκ, τον χρόνο δημιουργίας του, τον αριθμό ταυτότητας του χρήστη, και το Merkle root, που αποθηκεύει πληροφορίες για προηγούμενες συναλλαγές.

- Το blockchain παρέχει πλήρη, συνεπή και ακριβή δεδομένα ημερομηνίας, καθώς όλες οι συναλλαγές καταγράφονται πλήρως και τα δεδομένα των προηγούμενων συναλλαγών είναι άμεσα διαθέσιμα. Αυτό σημαίνει ότι ένας χρήστης μπορεί να δει το ιστορικό των συναλλαγών του από τη δημιουργία του blockchain και μετά. Κάθε συναλλαγή

καταγράφεται με τη σειρά με την οποία προστίθενται στο μπλοκ του blockchain και συνοδεύεται από μια χρονική σφραγίδα, που ακριβώς προσδιορίζει την ημερομηνία και την ώρα που η συναλλαγή εκτελέστηκε. Αυτό επιτυγχάνεται με τη χρήση timestamp, ο οποίος αποθηκεύεται στο μπλοκ του blockchain και αποτελεί αναπόσπαστο μέρος της αλυσίδας μπλοκ. [4]

- Η ταχύτητα εκτέλεσης συναλλαγών είναι ένα πλεονέκτημα του blockchain. Σε αρκετές περιπτώσεις οι συναλλαγές που πραγματοποιούνται μέσω τράπεζας ενδέχεται να απαιτούν μέρες για την επεξεργασία και υλοποίηση τους. Οι συναλλαγές που πραγματοποιούνται μεταξύ διαφορετικών χωρών συχνά αντιμετωπίζουν καθυστερήσεις λόγω διαφορετικών συστημάτων πληρωμών, νομισμάτων και διαδικασιών επεξεργασίας μεταξύ των χωρών. Ο blockchain επιτρέπει τη γρήγορη και αποτελεσματική εκτέλεση τέτοιων συναλλαγών ανεξαρτήτως χρόνου και τόπου βελτιώνοντας την αποδοτικότητα και την ταχύτητα των διασυνοριακών συναλλαγών. Το blockchain μειώνει το χρόνο υλοποίησης μια συναλλαγής σε λεπτά και επιτρέπει την επεξεργασία των συναλλαγών 24/7. [7]
- Το blockchain απλοποιεί το οικοσύστημα των ψηφιακών νομισμάτων και των κρυπτονομισμάτων, όπως το Bitcoin και άλλα κρυπτονομίσματα. με το να συγκεντρώνει όλες τις συναλλαγές σε ένα ενιαίο δημόσιο καθολικό βιβλίο, το οποίο ονομάζεται ledger. Η τεχνολογία blockchain μειώνει σε μεγάλο βαθμό τον κίνδυνο απάτης καθώς η επικύρωση μίας συναλλαγής γίνεται από πολλούς κόμβους και όχι μία κεντρική αρχή. Ο επιτιθέμενος θα πρέπει να προσπαθήσει να εξαπατήσει πολύ μεγαλύτερο αριθμό κόμβων για να εξαπατήσει το blockchain σε μία προσπάθεια αλλοίωσης. [7]
- Ανοιχτό για όλους. Το public blockchain παρέχει προσβασιμότητα σε οποιονδήποτε ενδιαφερόμενο, χωρίς τυπικές γραφειοκρατικές διαδικασίες. Κάθε άτομο έχει την ευκαιρία να συμμετέχει, να επικυρώνει συναλλαγές και να συνεισφέρει με τους υπολογιστικούς του πόρους για την ομαλή λειτουργία του συστήματος. Η διαφάνεια των διαδικασιών επιτρέπει σε κάθε χρήστη να επαληθεύει τις ενέργειές του. Ταυτόχρονα, η συνεισφορά υπολογιστικών πόρων από μέλη του δικτύου ενισχύει την απόδοση και την ασφάλεια του συστήματος. Η συνεισφορά πόρων και η ενίσχυση της απόδοσης του blockchain επιτυγχάνεται με την συμμετοχή των χρηστών στην εξόρυξη (mining) και αναλόγως την περίπτωση του blockchain, την συμμετοχή τους στους μηχανισμούς συναίνεσης. Όσον αφορά την ασφάλεια, οι συναλλαγές επαληθεύονται από πολλούς υπολογιστές (κόμβους) και δεν υπάρχει ένα μοναδικό σημείο αποτυχίας, καθιστώντας το σύστημα ανθεκτικότερο σε επιθέσεις. Με τη χρήση κρυπτογραφίας εξασφαλίζει την ακεραιότητα των δεδομένων και την ασφάλεια των συναλλαγών. Τα δεδομένα που εισέρχονται στο blockchain προστατεύονται από μη εξουσιοδοτημένη πρόσβαση και αλλοίωση. Οι συναλλαγές

επαληθεύονται από τους κόμβους του δικτύου πριν ενσωματωθούν στο blockchain, εξασφαλίζοντας την ακρίβεια και τη νομιμότητά τους.

- Το Blockchain μειώνει σημαντικά τα τέλη συναλλαγής. Στα διάφορα συστήματα, η παρουσία ενδιάμεσων οντοτήτων, όπως τράπεζες, συνεπάγεται πρόσθετες χρεώσεις και τρίτα κόστη. Με το Blockchain, αυτοί οι ενδιάμεσοι αποκλείονται ως επί το πλείστον από τη διαδικασία, καθιστώντας τις συναλλαγές πιο άμεσες και οικονομικές. Η αποκέντρωση και η αυτοματοποίηση των διαδικασιών εξαλείφουν την ανάγκη για εμπλοκή τρίτων, μειώνοντας σημαντικά τα συνολικά έξοδα.

Υπάρχουν περιπτώσεις όπου η χρήση ενδιάμεσου είναι απαραίτητη ακόμα και στο πλαίσιο των τεχνολογιών blockchain. Αν και το blockchain μπορεί να μειώσει την ανάγκη για ενδιάμεσους σε πολλές περιπτώσεις, υπάρχουν κάποιες περιπτώσεις όπου η παρουσία τους είναι ακόμα αναγκαία.: Όταν γίνεται ανταλλαγή αξίας μεταξύ διαφορετικών blockchain ή συστημάτων, ενδέχεται να απαιτείται η χρήση ενδιάμεσων για τη διευθέτηση των συναλλαγών και την εξασφάλιση της ασφάλειάς τους. Σε ορισμένες περιπτώσεις, όπως στις οικονομικές υπηρεσίες και τον τομέα των κρυπτονομισμάτων, η επαλήθευση της ταυτότητας και η συμμόρφωση με τους κανονισμούς είναι αναγκαίες για την πρόληψη της απάτης, την αντιμετώπιση της νομικής ευθύνης και τη διασφάλιση της ασφάλειας του συστήματος. Σε αυτό το πλαίσιο, η συνεργασία με ενδιάμεσους φορείς μπορεί να είναι αναγκαία για τη διασφάλιση ότι οι συναλλαγές πληρούν τις απαιτήσεις ρύθμισης και για την επαλήθευση της ταυτότητας των χρηστών. [7]

- Το blockchain λειτουργεί χωρίς την ανάγκη για κεντρικό φορέα ή εξουσία, προσφέροντας αποκέντρωση. Κανένας κόμβος δεν έχει τον απόλυτο έλεγχο των δεδομένων, γεγονός που μειώνει τον κίνδυνο αποτυχίας ή κακόβουλης επίθεσης σε έναν κεντρικό διακομιστή. Η αποκέντρωση επιτρέπει τη δημιουργία ενός συστήματος όπου οι χρήστες λειτουργούν ισότιμα και όλες οι συναλλαγές επαληθεύονται από πολλούς κόμβους ταυτόχρονα. [7]

Καθώς εξερευνούμε τον κόσμο του blockchain, είναι σημαντικό να αναγνωρίσουμε και τα προβλήματα που υπάρχουν σε αυτήν την καινοτομία. Όπως συμβαίνει με κάθε νέα τεχνολογία, έτσι και το blockchain αντιμετωπίζει ορισμένες προκλήσεις. Ας εξετάσουμε αυτά τα προβλήματα, ώστε να κατανοήσουμε καλύτερα τις προκλήσεις που προκύπτουν από τη χρήση αυτής της τεχνολογίας.

- Η κύρια πρόκληση που αντιμετωπίζει το Blockchain είναι η υψηλή κατανάλωση ενέργειας. Για να διατηρηθεί ένα ολοκληρωμένο και συνεχές αρχείο συναλλαγών σε πραγματικό

χρόνο, απαιτείται σημαντική ενεργειακή προσπάθεια. Κάθε φορά που προστίθεται ένα νέο μπλοκ στο Blockchain, έχει προηγηθεί η εκτέλεση του περίπλοκου υπολογιστικού έργου, της εξόρυξης. Η εξόρυξη έχει υψηλές απαιτήσεις σε υπολογιστική ισχύ και κατ' επέκτασιν μεγάλη κατανάλωση ενέργειας των συστημάτων. Οι υψηλές απαιτήσεις ισχύος και ενέργειας δεν αφορά όλα τα ήδη των κόμβων. Οι κόμβοι ως προς τις λειτουργίες του blockchain κατατάσσονται ως εξής:

- (1) *Κόμβοι Πλήρους Συμμετοχής (Full Nodes)*: Αυτοί οι κόμβοι αποθηκεύουν ολόκληρο το ιστορικό του blockchain και επιβεβαιώνουν τις συναλλαγές. Απαιτούν σημαντικούς πόρους και μπορούν να λειτουργήσουν σε ισχυρούς υπολογιστές ή ειδικές συσκευές.
- (2) *Κόμβοι Εξόρυξης (Mining Nodes)*: Αυτοί οι κόμβοι εκτελούν το περίπλοκο υπολογιστικό έργο που απαιτείται για την προσθήκη νέων τμημάτων στο blockchain. Χρησιμοποιούν ισχυρούς υπολογιστές και καταναλώνουν μεγάλες ποσότητες ενέργειας.
- (3) *Ελαφρύτεροι Κόμβοι*: Ορισμένες συσκευές μπορούν να λειτουργήσουν ως κόμβοι χωρίς την ανάγκη για πλήρη συμμετοχή ή εξόρυξη. Αυτοί οι κόμβοι μπορούν να παρέχουν βασική λειτουργικότητα, όπως η επαλήθευση συναλλαγών.

Επισημαίνεται ότι η υψηλή κατανάλωση ενέργειας αφορά κυρίως τους κόμβους εξόρυξης οι οποίοι είναι ένα ποσοστό του συνολικού αριθμού κόμβων του δικτύου. Σημαντικό ρόλο στην κατανάλωση συνολικά παίζει και η επιλογή του αλγορίθμου συναίνεσης καθώς η συμμετοχή των κόμβων στην συναίνεση καθορίζει και την κατανάλωση.

Στην γενικότερη υψηλή κατανάλωση της τεχνολογίας blockchain συμβάλλει και η διαδικασία επαλήθευσης της υπογραφής καθώς η διαδικασία επαναλαμβάνεται για κάθε επικοινωνία κόμβου με κόμβο (peer-to-peer βάση). Κάθε συναλλαγή πρέπει να επαληθευθεί από πολλούς κόμβους πριν να γίνει επίσημα αποδεκτή και να ενσωματωθεί στην αλυσίδα των μπλοκ. Αυτό απαιτεί τη διεξαγωγή πολύπλοκων υπολογισμών και επαλήθευσης της ψηφιακής υπογραφής για κάθε μετάδοση και επιβεβαίωση της συναλλαγής. Οι κόμβοι στο δίκτυο του blockchain πρέπει να είναι ικανοί να εκτελέσουν αυτούς τους υπολογισμούς και να διαχειριστούν τον όγκο των συναλλαγών. Συνεπώς, η πρόκληση είναι να βρεθούν τρόποι για να μειωθεί η πολυπλοκότητα των διαδικασιών επαλήθευσης ώστε να γίνει δυνατή η συμμετοχή και η συνεισφορά από μηχανήματα με περιορισμένους πόρους, ενώ παράλληλα διατηρείται η ασφάλεια και η αξιοπιστία του δικτύου. [7]

- Το υψηλό κόστος εγκατάστασης του blockchain μπορεί να αποτελεί σημαντικό εμπόδιο. Καθώς είτε εντάσσονται Mining είτε απλοί αποθηκευτικοί κόμβοι χρειάζεται σημαντική επένδυση. Οι mining κόμβοι σε ισχυρούς επεξεργαστές και συστήματα και οι αποθηκευτικοί χρειάζονται επαρκή αποθηκευτικό χώρο για την αποθήκευση του πλήρους αντιγράφου του blockchain και τη διατήρηση του συνεχούς συγχρονισμού με το δίκτυο. Επιπλέον, το κόστος λειτουργίας και συντήρησης του κόμβου επίσης πρέπει να ληφθεί

υπόψη, καθώς αυτό περιλαμβάνει την ενεργειακή κατανάλωση, τη διαχείριση του δικτύου και τη διασφάλιση της ασφάλειας του κόμβου. Παρόλο που το blockchain μας προσφέρει τη δυνατότητα να εξοικονομούμε πόρους σε άλλα σημεία, όπως το χρόνο και το χρήμα κατά τις συναλλαγές, το αρχικό κόστος είναι πολλές φορές αποθαρρυντικό. Αυτό μπορεί να αποτρέψει πολλούς ανθρώπους ή επιχειρήσεις από το να υιοθετήσουν την τεχνολογία. Το υψηλό αρχικό κόστος μπορεί να αποτελέσει σημαντικό εμπόδιο για πολλούς που ενδιαφέρονται να ενταχθούν στον χώρο του blockchain, ιδίως εκείνους που επιθυμούν να ασχοληθούν με τον τομέα του "Mining". Είναι σημαντικό να βρεθούν λύσεις για την μείωση αυτού του αρχικού κόστους προκειμένου να καταστήσουμε το blockchain προσβάσιμο και προσίτο για όλους. [7]

- Το Blockchain επεκτείνεται με την προσθήκη νέων κόμβων στην αλυσίδα, αυξάνοντας τις υπολογιστικές απαιτήσεις. Όλοι οι κόμβοι όμως δεν μπορούν να παρέχουν την απαιτούμενη χωρητικότητα, προκαλώντας δύο βασικά προβλήματα. Το πρώτο πρόβλημα είναι το ζήτημα της μειωμένης καταγραφής, καθώς οι κόμβοι δεν μπορούν να διατηρήσουν πλήρες αντίγραφο του Blockchain, παραβιάζοντας τη σταθερότητα και διαφάνεια του συστήματος. Δεύτερον, παρουσιάζεται το πρόβλημα της πιθανής κεντροποίησης του Blockchain, όπου οι λίγοι κόμβοι που διατηρούν το πλήρες αντίγραφο του Blockchain μπορεί να αποκτήσουν έλεγχο, καθιστώντας το σύστημα περισσότερο κεντρικό σε αυτά τα σημεία. Όσον αφορά το μέγεθος μνήμης η οποία απαιτείται για πλήρη αποθήκευση του Blockchain, εξαρτάται από πολλούς παράγοντες, συμπεριλαμβανομένου του μεγέθους του Blockchain, του πρωτοκόλλου και του είδους των δεδομένων που περιέχει, καθώς και του επιπέδου λειτουργικότητας που παρέχεται από κάθε κόμβο. Όσον αφορά τους ελαφρούς και μειωμένους κόμβους, αυτοί παρέχουν μια λύση στο πρόβλημα της περιορισμένης χωρητικότητας και της κεντροποίησης. Ωστόσο, ανάλογα με τις ανάγκες του δικτύου, ενδέχεται να απαιτείται περαιτέρω έρευνα και ανάπτυξη για τη βελτίωση της αποδοτικότητάς τους και την αντιμετώπιση των προκλήσεων που ενδέχεται να προκύψουν στο μέλλον. [7]
- Παρά την αύξηση της ασφάλειας που προσφέρει το blockchain στον κυβερνοχώρο, υπάρχουν ακόμα ορισμένα επιπλέον ζητήματα που πρέπει να ληφθούν υπόψη για την πλήρη εμπιστοσύνη στην τεχνολογία αυτή. Η ανθρώπινη παρέμβαση εξακολουθεί να αποτελεί πιθανό παράγοντα κινδύνου. Οι χρήστες μπορούν να γίνουν στόχοι phishing (ηλεκτρονικού ψαρέματος) ή άλλων μορφών επιθέσεων που μπορούν να θέσουν σε κίνδυνο την ασφάλεια του δικτύου. Επίσης παρά τη χρήση ισχυρής κρυπτογράφησης, υπάρχει πάντα η πιθανότητα να αναδειχθούν νέες ευπάθειες ή αδυναμίες στους αλγόριθμους κρυπτογράφησης, εισάγοντας πιθανούς κινδύνους για την ασφάλεια του συστήματος. Ακόμη υπάρχουν περιπτώσεις όπου έχουν ανακαλυφθεί κενά ασφαλείας σε συγκεκριμένες υλοποιήσεις, τα οποία πρέπει να διορθωθούν για να διατηρηθεί η εμπιστοσύνη των χρηστών. [7]

- Οι εφαρμογές του blockchain προσφέρουν λύσεις που απαιτούν σημαντικές αλλαγές ή ακόμα και την πλήρη αντικατάσταση των υπαρχόντων συστημάτων. Οι αλλαγές που απαιτούνται μπορεί να καλύπτουν πολλούς τομείς, όπως οι διαδικασίες λειτουργίας, ο τρόπος αλληλεπίδρασης με τους πελάτες, κα. Οι διαδικασίες λειτουργίας (operational processes) που σχετίζονται με το blockchain είναι οι ενέργειες και οι μηχανισμοί που διασφαλίζουν την εφαρμογή και διαχείριση της τεχνολογίας blockchain σε μια επιχείρηση και περιλαμβάνουν τη διαχείριση των κόμβων του δικτύου, τη διανομή των καθηκόντων στους συμμετέχοντες, την επίλυση των συγκρούσεων ή αντιφάσεων στα δεδομένα και τη διατήρηση της ασφάλειας του δικτύου και των συναλλαγών. Λόγω της έκτασης των αλλαγών και προκειμένου να πραγματοποιηθούν, οι εταιρείες πρέπει να εκπονήσουν σχέδια στρατηγικής μετάβασης τα οποία θα καθοδηγήσουν τη μετάβασή τους σε αυτές τις νέες τεχνολογίες. Τα σχέδια στρατηγικής μετάβασης περιλαμβάνουν ανάλυση των αναγκών, των προκλήσεων και των στόχων της εταιρείας, καθώς και τον καθορισμό των βημάτων που απαιτούνται. Επιπλέον, το budget είναι ένας σημαντικός παράγοντας για την υλοποίηση της μετάβασης, καθώς περιλαμβάνει το κόστος απόκτησης της νέας τεχνολογίας, τα έξοδα εκπαίδευσης και εγκατάστασης, καθώς και τυχόν προσαρμογές στις διαδικασίες της επιχείρησης. [7]
- Το blockchain συνιστά μια σημαντική μεταβολή προς ένα αποκεντρωμένο δίκτυο, όπου η συνεννόηση και συμφωνία των χρηστών και των φορέων είναι κρίσιμες. Στο παραδοσιακό μοντέλο, η εξουσία και ο έλεγχος συγκεντρώνονται σε κεντρικούς οργανισμούς ή φορείς. Το blockchain ανατρέπει αυτήν τη δομή, δημιουργώντας ένα δίκτυο όπου ο καθένας έχει συμμετοχή και ευθύνη. Οι αλλαγές αυτές απαιτούν από τους χρήστες και τους φορείς να αποδεχτούν και να προσαρμοστούν σε αυτήν τη νέα πραγματικότητα. Αυτή η μετάβαση μπορεί να είναι δύσκολη για διάφορους λόγους. Η αβεβαιότητα που συνοδεύει τη νέα τεχνολογία μπορεί να αποθαρρύνει τους φορείς και τους χρήστες από την υιοθέτηση του blockchain, καθώς αναρωτιούνται για την ασφάλεια, την απόδοση και την αξιοπιστία του. Επίσης η δυσκολία υλοποίησης μπορεί να αναδειχθεί ως μια πρόκληση, καθώς η μετάβαση σε ένα νέο σύστημα απαιτεί σημαντικές αλλαγές στην υποδομή, στην εκπαίδευση και στις διαδικασίες, μερικές φορές με υψηλό κόστος. Τέλος η αλλαγή στην κουλτούρα και τις πρακτικές απαιτεί από τους οργανισμούς και τους χρήστες να προσαρμοστούν σε ένα νέο περιβάλλον όπου η εξουσία δεν είναι κεντροποιημένη αλλά κατανέμεται σε όλους. [7]
- Η τεχνολογία του blockchain δεν επιτρέπει εύκολη τροποποίηση των δεδομένων αφού έχουν καταγραφεί. Για να γίνει αλλαγή, απαιτείται η επανεγγραφή των κωδικών σε όλα τα τμήματά του, μια διαδικασία αρκετά χρονοβόρα αλλά και ακριβή. Το αρνητικό αυτού του χαρακτηριστικού είναι ότι είναι δύσκολο να διορθωθούν λάθη ή να γίνουν απαραίτητες προσαρμογές. Κάτι που καθιστά το σύστημα μη ευέλικτο σε περιπτώσεις ανάγκης για

αλλαγές. Οι ατέλειες και τα λάθη στο λογισμικό μπορούν να οδηγήσουν σε αστάθεια ή μη αξιοπιστία του blockchain. Για παράδειγμα, ένα σφάλμα στον κώδικα μπορεί να επιτρέψει την ανεπιθύμητη τροποποίηση των δεδομένων ή να προκαλέσει μη έγκυρες συναλλαγές. Αυτό μπορεί να οδηγήσει σε απώλεια εμπιστοσύνης των χρηστών στο σύστημα και στην απώλεια αξιοπιστίας του blockchain ως μέσου αξιόπιστης αποθήκευσης και μετάδοσης δεδομένων. [7]

2.2. Cloud Computing

2.2.1. Ορισμός Cloud Computing

Το μοντέλο υπολογιστικής νέφους (ΥΝ) αντιπροσωπεύει ένα υπολογιστικό σύστημα που παρέχει πανταχού παρούσα πρόσβαση, κατά απαίτηση, σε μια διαμοιρασμένη δεξαμενή διαμορφώσιμων υπολογιστικών πόρων. Αυτό σημαίνει ότι οι χρήστες έχουν τη δυνατότητα να αποκτήσουν πρόσβαση σε υπολογιστικούς πόρους όποτε το χρειάζονται, χωρίς να χρειάζεται να ειδοποιήσουν εκ των προτέρων ή να διαπραγματευτούν με τον πάροχο υπηρεσιών. [38]

Αυτό το μοντέλο χαρακτηρίζεται από τη δυνατότητα γρήγορης παροχής και απελευθέρωσης πόρων. Αυτό σημαίνει ότι οι πόροι μπορούν να διατεθούν και να απελευθερωθούν με άμεσο τρόπο, ανάλογα με τις ανάγκες των χρηστών, με ελάχιστη προσπάθεια διαχείρισης από τον πάροχο υπηρεσιών.

Το μοντέλο ΥΝ αποτελείται από πέντε ουσιώδη χαρακτηριστικά, που περιλαμβάνουν χρήση κατ' απαίτηση, πανταχού παρούσα πρόσβαση, πολλαπλή μίσθωση, ελαστικότητα, μετρούμενη χρήση και ανθεκτικότητα. Επιπλέον, περιλαμβάνει τρία μοντέλα υπηρεσίας (υποδομή ως υπηρεσία, πλατφόρμα ως υπηρεσία και λογισμικό ως υπηρεσία) και τέσσερα μοντέλα ανάπτυξης (ιδιωτικό νέφος, δημόσιο νέφος, υβριδικό νέφος και κοινοτικό νέφος). [11]

2.2.2. Πλεονεκτήματα και μειονεκτήματα του cloud computing

Η εποχή της νεφο-υπολογιστικής έχει φέρει μια νέα διάσταση στον κόσμο της τεχνολογίας και των επιχειρήσεων. Αντιμετωπίζοντας τις διαρκώς εξελισσόμενες απαιτήσεις της ψηφιακής εποχής, οι επιχειρήσεις είναι σε συνεχή αναζήτηση λύσεων που θα τους επιτρέψουν να είναι ευέλικτες, αποδοτικές και ανταγωνιστικές. Σε αυτό το πλαίσιο, το η νεφο-υπολογιστική αναδεικνύεται ως μία από τις πιο καινοτόμες λύσεις. Επιτρέπει στις επιχειρήσεις να αξιοποιήσουν προηγμένες τεχνολογίες χωρίς την ανάγκη για σημαντικές επενδύσεις σε υλικό και λογισμικό. Στη συνέχεια, θα εξετάσουμε πιο αναλυτικά τα πλεονεκτήματα που προσφέρει η νεφο-υπολογιστική και τον τρόπο με τον οποίο επηρεάζει τη λειτουργία και την ανάπτυξη των επιχειρήσεων

- Το υπολογιστικό νέφος μπορεί να αναδείξει σημαντικά οικονομικά οφέλη για μικρότερες επιχειρήσεις που δεν έχουν τους πόρους να επενδύσουν σε δικές τους δομές υπολογιστικής υποδομής. Με βάση το ευέλικτο μοντέλο χρέωσης του υπολογιστικού νέφους, οι εταιρείες αυτές εξασφαλίζουν την σημαντική μείωση του λειτουργικού κόστους των εφαρμογών και υπηρεσιών τους όπου η χρέωση πραγματοποιείται με βάση την πραγματική χρήση των πόρων, οι οποίοι μπορούν να δεσμεύονται και αποδεσμεύονται όποτε προκύπτει η σχετική ανάγκη από τις εφαρμογές/υπηρεσίες. Από την άλλη μεριά, το υπολογιστικό νέφος επιτρέπει την γρήγορη ανάπτυξη, δοκιμή και εκτέλεση εφαρμογών, επιτρέποντας τις εταιρείες να λανσάρουν γρήγορα στην αγορά νεωτερικές εφαρμογές που μπορεί να τους αποδώσουν σημαντικά οικονομικά οφέλη. [10]
- Το υπολογιστικό νέφος καθιστά πιο εύκολο για τις επιχειρήσεις να αναπτύσσουν ή να συρρικνώνουν τις υπηρεσίες τους ανάλογα με τις ανάγκες των πελατών επιτρέποντας την προσαρμοστική αντιμετώπιση του φόρτου εργασίας τους. Οι υπολογιστικοί πόροι διαχειρίζονται μέσω λογισμικού και μπορούν να προσαρμοστούν γρήγορα, δηλαδή να δεσμεύονται και αποδεσμεύονται τάχιστα, σύμφωνα με τη ζήτηση. [10]
- Η εύκολη, πανταχού παρούσα πρόσβαση σε δεδομένα, υπολογιστικούς πόρους και υπηρεσίες μέσω του διαδικτύου είναι ένα σημαντικό πλεονέκτημα του υπολογιστικού νέφους. Αυτό σημαίνει ότι οι χρήστες μπορούν να έχουν πρόσβαση στα δεδομένα τους ακόμα και όταν βρίσκονται σε διαφορετικό γεωγραφικό τόπο ή ζώνη ώρας. Αυτή η ευκολία πρόσβασης επιτρέπει στις επιχειρήσεις και στους χρήστες να είναι ευέλικτοι και αποτελεσματικοί, ανεξάρτητα από τον τόπο και το χρόνο. Επιπλέον, αυτό το χαρακτηριστικό επιτρέπει τη συνεργασία και την επικοινωνία μεταξύ χρηστών που βρίσκονται σε διαφορετικές γεωγραφικές περιοχές, βελτιώνοντας έτσι την αποτελεσματικότητα και την παραγωγικότητα. Τέλος, ειδικότερα στην περίπτωση μεγάλων παρόχων νέφους, η ικανότητα διάταξης μιας εφαρμογής σε πολλές περιοχές (ουσιαστικά κέντρα δεδομένων σε διαφορετικής περιοχής) επιτρέπει την αύξηση της απόδοσης της εφαρμογής διότι επιλέγεται προς κατανάλωση εκείνο το στιγμιότυπο της που βρίσκεται πιο κοντά στον εκάστοτε πελάτη. [12]
- Η δημιουργία αντιγράφων ασφαλείας και η ανάκτηση δεδομένων είναι πιο εύκολες στο υπολογιστικό νέφος σε σύγκριση με άλλες παραδοσιακές μεθόδους αποθήκευσης δεδομένων, καθώς όλα τα δεδομένα όχι μόνο αποθηκεύονται αλλά και αναπαράγονται σε αυτό. Αυτό σημαίνει ότι δεν χρειάζεται να ανησυχούν οι χρήστες για την απώλεια δεδομένων σε περίπτωση που συμβεί κάτι σε κάποιο ξενιστή που φιλοξενεί τα δεδομένα τους ή ακόμα και σε ένα ολόκληρο κέντρο δεδομένων (εφόσον τα δεδομένα αναπαράγονται κατά μήκος των κέντρων δεδομένων ενός νέφους). Επιπλέον, το νέφος

παρέχει υπηρεσίες αυτοματοποίησης της δημιουργίας αντιγράφων ασφαλείας και ανάκτησης δεδομένων. [12]

- Η ανθεκτικότητα και η ευελιξία αποτελούν κρίσιμες πτυχές του υπολογιστικού νέφους. Αυτές οι δύο ιδιότητες είναι ουσιώδεις για τη διασφάλιση της αδιάλειπτης λειτουργίας και της ικανότητάς του να προσαρμόζεται σε διαφορετικές απαιτήσεις και συνθήκες χρήσης. Η ανθεκτικότητα στο υπολογιστικό νέφος επιτυγχάνεται μέσω μιας σειράς μέτρων ασφαλείας και ανάκαμψης. Οι πάροχοι νέφους χρησιμοποιούν συχνά αντίγραφα ασφαλείας και μηχανισμούς αυτόματης ανάκαμψης για να εξασφαλίσουν ότι οι υπηρεσίες τους θα είναι πάντα διαθέσιμες. Αυτό μπορεί να σημαίνει αυτόματη μεταφορά εργασιών σε άλλους διακομιστές κατά την περίπτωση προβλημάτων, ή ακόμα και επαναφορά δεδομένων από αντίγραφα ασφαλείας σε περίπτωση απώλειας. Από την άλλη πλευρά, η ευελιξία επιτρέπει στους χρήστες να προσαρμόζουν τις υπηρεσίες σύμφωνα με τις μεταβαλλόμενες ανάγκες τους. Μπορούν να αυξομειώνουν ή να μειώνουν τους υπολογιστικούς πόρους, να προσθέτουν ή να αφαιρούν υπηρεσίες, ανάλογα με τις αλλαγές στις απαιτήσεις τους. Τέλος, η εύκολη πρόσβαση και χρήση των υπηρεσιών μέσω του διαδικτύου επιτρέπει στους χρήστες να διαχειρίζονται και να ρυθμίζουν τις λειτουργίες τους από οπουδήποτε και οποιαδήποτε συσκευή, εξασφαλίζοντας μια ομαλή εμπειρία χρήσης. [17]
- Η ασφάλεια των υπηρεσιών στο υπολογιστικό νέφος είναι ένας κρίσιμος παράγοντας για την υιοθέτησή του. Καθώς τα (σημαντικά και πολλές φορές ιδιωτικά) δεδομένα καθώς και άλλα ψηφιακά περιουσιακά στοιχεία των πελατών αποθηκεύονται και ενσωματώνονται σε ένα περιβάλλον πολλαπλών ενοικιαστών, θα πρέπει να εξασφαλιστεί η διαθεσιμότητα, ακεραιότητα και εμπιστευτικότητά τους. Προς αυτό τον σκοπό, οι πάροχοι υπηρεσιών νέφους δεσμεύονται μέσω ενός συμβολαίου επιπέδου υπηρεσίας (SLA), το οποίο θεσπίζει τις πολιτικές ασφαλείας και αποτρέπει τυχόν συγκρούσεις μεταξύ τους και των χρηστών. Για να διασφαλίσουν την ασφάλεια των δεδομένων και άλλων ψηφιακών πόρων, οι πάροχοι υπολογιστικού νέφους χρησιμοποιούν διάφορα μέτρα, όπως η χρήση διαφορετικών κέντρων δεδομένων (geo-redundancy) για την εξασφάλιση της διαθεσιμότητας δεδομένων, η προστασία των συνδέσεων μέσω τεχνικών κρυπτογράφησης καθώς και κατάλληλη αρχιτεκτονική ασφάλειας, ενώ επίσης ακολουθούν καλές πρακτικές και διαδικασίες ασφάλειας. Ως εκ τούτου, ένα σύστημα υπολογιστικού νέφους θεωρείται πιο ασφαλές σε σύγκριση με τα παραδοσιακά πληροφοριακά συστήματα. [14]
- Η αποθήκευση πληροφοριών στο νέφος παρέχει τη δυνατότητα για σχεδόν απεριόριστη χωρητικότητα αποθήκευσης. Αυτό σημαίνει ότι οι χρήστες μπορούν να αποθηκεύουν μεγάλες ποσότητες δεδομένων χωρίς τον φόβο μη επάρκειας του χώρου. Η δυνατότητα

αυτή είναι ιδιαίτερα χρήσιμη για επιχειρήσεις και άλλους οργανισμούς που αντιμετωπίζουν αυξημένες ανάγκες αποθήκευσης δεδομένων λόγω της αυξημένης πολυπλοκότητας των πληροφοριακών τους συστημάτων ή των μεγάλων όγκων δεδομένων που παράγονται. [12]

- Στο νέφος, οι υπολογιστικοί πόροι προσφέρουν ευελιξία και κλιμακωσιμότητα (scalability). Η ευελιξία επιτρέπει στους χρήστες να προσαρμόζουν τους πόρους, όπως την επεξεργαστική ισχύ ή τη μνήμη, ανάλογα με τις ανάγκες τους και τις αλλαγές στο φορτίο εργασίας τους. Αυτό επιτρέπει στις επιχειρήσεις να προσαρμόζονται ευέλικτα σε μεταβαλλόμενες απαιτήσεις, χωρίς την ανάγκη για αγορά νέου εξοπλισμού. Από την άλλη πλευρά, η κλιμακωσιμότητα είναι σημαντική για τη διαχείριση αυξημένου φόρτου εργασίας. Όταν ο όγκος της εργασίας αυξάνεται, το νέφος μπορεί να κλιμακωθεί αυτόματα προσθέτοντας περισσότερους υπολογιστικούς πόρους. Με αυτόν τον τρόπο, διατηρείται η απόδοση χωρίς διακοπές ή απώλεια απόδοσης, ανταποκρινόμενο σε οποιεσδήποτε αλλαγές στις ανάγκες υπολογιστικής ισχύος των χρηστών. Άρα, η κλιμακωσιμότητα επιτρέπει στο νέφος να παραμένει ευέλικτο και να προσαρμόζεται στις διαφορετικές απαιτήσεις, εξασφαλίζοντας τη σταθερή λειτουργία και την αποτελεσματική χρήση των πόρων του. [12]

Παρότι το υπολογιστικό νέφος έχει πολλά πλεονεκτήματα, υπάρχουν και μειονεκτήματα που πρέπει να ληφθούν υπόψη. Οι βασικοί κίνδυνοι που συνδέονται με την υπολογιστική νέφους είναι:

- Παρά το γεγονός ότι τα δεδομένα και οι πόροι στο νέφος είναι προσβάσιμα οποιαδήποτε στιγμή και από οπουδήποτε, συχνά υπάρχουν προβλήματα που προκαλούν σοβαρές δυσλειτουργίες. Είναι σημαντικό να συνειδητοποιούν οι επιχειρήσεις ότι αυτή η τεχνολογία είναι πάντα ευάλωτη σε διακοπές και άλλα τεχνικά προβλήματα. Οι διακοπές σχετίζονται με την αποτυχία λειτουργίας ή downtime, κατά τις οποίες οι υπηρεσίες cloud δεν είναι διαθέσιμες στους χρήστες. Τα τεχνικά προβλήματα περιλαμβάνουν διακοπές των υπηρεσιών, οι οποίες συμβαίνουν όταν μια υπηρεσία στο νέφος δεν είναι προσβάσιμη εξαιτίας τεχνικών προβλημάτων, εσωτερικών σφαλμάτων ή εξωτερικών παραγόντων όπως διακοπή ισχύος. Ακόμα και οι πάροχοι υπολογιστικού νέφους με υψηλές προδιαγραφές συντήρησης μπορεί να αντιμετωπίσουν προβλήματα, όπως απώλεια σύνδεσης στο διαδίκτυο ή διακοπή ρεύματος, τα οποία προκαλούν απρόβλεπτες δυσκολίες στην ακαμψία και τη λειτουργικότητα του συστήματος νέφους. [12]
- Η αποθήκευση δεδομένων και πληροφοριών στο νέφος μπορεί να αποτελέσει έναν παράγοντα ευπάθειας για τις επιχειρήσεις, καθώς δημιουργεί δυνατότητες διείσδυσης και επιθέσεων από εξωτερικούς παράγοντες, ειδικότερα στα δημόσια νέφη, όπου η επιφάνεια

τρωτοτήτων είναι μεγάλη. Αυτό δημιουργεί ένα σοβαρό ζήτημα ασφάλειας, καθώς τα επιχειρησιακά δεδομένα μπορεί να εκτεθούν σε κίνδυνο κλοπής ή διαρροής ή εν γένει μη εξουσιοδοτημένης πρόσβασης. Οι επιχειρήσεις πρέπει να επικεντρωθούν σε προηγμένα μέτρα για μια επιπρόσθετη διασφάλιση των δεδομένων τους από τέτοιου είδους απειλών (που θα εφαρμόζονται παράλληλα με τα μέτρα ασφαλείας του νέφους), όπως η κρυπτογράφηση δεδομένων (κατά την αποθήκευση και την μεταφορά τους) και η διαχείριση πρόσβασης (access control). Επιπλέον, η συχνή επιθετικότητα των κυβερνοεγκληματιών απαιτεί συνεχή ενημέρωση και ενίσχυση των μέτρων προστασίας για την αποφυγή πιθανών παραβιάσεων ασφάλειας τόσο από την πλευρά του πελάτη όσο και του παρόχου του νέφους. [12]

- Η χρήση της υπολογιστικού νέφους καθιστά τις επιχειρήσεις εξαρτημένες από την αξιοπιστία της σύνδεσής τους στο διαδίκτυο. Οποιαδήποτε διακοπή ή πρόβλημα με τη διαδικτυακή σύνδεση μπορεί να οδηγήσει σε διακοπή της πρόσβασης στις υπηρεσίες που παρέχονται από το νέφος, προκαλώντας ανασφάλεια και πιθανές απώλειες εργασίας. Αυτό ενδέχεται να προκαλέσει σοβαρά προβλήματα λειτουργίας και να επηρεάσει την αποδοτικότητα των επιχειρήσεων, καθώς επίσης και να έχει αρνητικές επιπτώσεις στην εμπιστοσύνη των πελατών και τη φήμη της επιχείρησης. [17]
- Μπορεί να φαίνεται προφανές ότι μια εφαρμογή υπολογιστικού νέφους είναι πολύ πιο οικονομική σε σχέση με μια συγκεκριμένη λύση λογισμικού που εγκαθίσταται και λειτουργεί εντός της επιχείρησης. Ωστόσο, πρέπει να ληφθούν υπόψη τα πραγματικά κόστη. Είναι σημαντικό να εξεταστούν προσεκτικά τα σχέδια τιμολόγησης και να αναλυθούν οι λεπτομέρειες κάθε εφαρμογής. Υπάρχουν και περιπτώσεις, κυρίως σε βάθος Ζετίας και έπειτα, στις οποίες το κόστος χρήσης εφαρμογής σε υπολογιστικό νέφος, ισοσκελίζει το κόστος μιας τοπικής υποδομής. Πολλοί πάροχοι υπολογιστικού νέφους υποστηρίζουν ότι χρεώνουν μόνο για τη χρήση που κάνει ο πελάτης, αλλά στην πραγματικότητα, συνήθως η εταιρεία πρέπει να δεσμευτεί σε ένα συγκεκριμένο συμβόλαιο ανεξάρτητα από την πραγματική της χρήση. Η αγορά λογισμικού συνήθως συνοδεύεται από συγκεκριμένες δεσμεύσεις και περιορισμούς, όπως η έκδοση του λογισμικού και η διάρκεια της υποστήριξής του. Αυτά τα στοιχεία μπορούν να είναι περιοριστικά και να επιβάλλουν επιπλέον δαπάνες ή περιορισμούς στην επιχείρηση. Από την άλλη πλευρά, τα συμβόλαια με πάροχους υπολογιστικού νέφους μπορούν να παρέχουν μεγαλύτερη ευελιξία, καθώς οι συμφωνίες μπορούν να διαπραγματευτούν και να προσαρμοστούν σύμφωνα με τις ανάγκες της επιχείρησης και τις μεταβαλλόμενες συνθήκες της αγοράς. Αυτό επιτρέπει στις επιχειρήσεις να επιλέξουν το πιο κατάλληλο συμβόλαιο που ταιριάζει στις ανάγκες και τον προϋπολογισμό τους. [17]

- Επιπλέον, η αύξηση της ζήτησης για υπολογιστικούς πόρους έχει οδηγήσει στην ανάπτυξη νέων κέντρων δεδομένων και στην αυξημένη κατανάλωση ενέργειας από αυτές τις υποδομές. [14]
- Η έλλειψη υποστήριξης αποτελεί ένα σημαντικό μειονέκτημα για τις υπηρεσίες υπολογιστικού νέφους. Κατά τη χρήση τους, οι χρήστες συχνά αντιμετωπίζουν προβλήματα και απαιτούν υποστήριξη για να τα αντιμετωπίσουν. Ωστόσο, σε πολλές περιπτώσεις, η διαδικασία επικοινωνίας με τους παρόχους υπηρεσιών μπορεί να είναι δυσκολότερη από ό,τι αναμένεται. Ειδικότερα, οι χρήστες συχνά πρέπει να επικοινωνούν μέσω ηλεκτρονικών μηνυμάτων ή αιτήσεων και να αναμένουν απάντηση για μεγάλα χρονικά διαστήματα, πράγμα που μπορεί να δημιουργήσει αβεβαιότητα και δυσαρέσκεια. Αυτό επηρεάζει αρνητικά την εμπειρία του χρήστη και τη λειτουργία της επιχείρησης, καθώς η ανεπάρκεια υποστήριξης μπορεί να καθυστερήσει την αντιμετώπιση προβλημάτων και να προκαλέσει απώλεια εργασιών. Από την άλλη μεριά, όμως, καλό είναι να αναφερθεί πως υπάρχει καλή τεκμηρίωση των υπηρεσιών και προϊόντων που προσφέρονται από έναν πάροχο νέφους. [12]

2.2.3. Τύποι υπολογιστικού νέφους

Η εμφάνιση του υπολογιστικού νέφους έχει αλλάξει τον τρόπο που οι επιχειρήσεις και οργανισμοί διαχειρίζονται τις ψηφιακές υπηρεσίες τους. Μέσω αυτής της τεχνολογίας, μπορούν να αποθηκεύουν και να επεξεργάζονται τα δεδομένα τους μέσω του Διαδικτύου. Το υπολογιστικό νέφος μπορεί να αναπτύσσεται με διαφορετικά μοντέλα, όπως το δημόσιο (public), το ιδιωτικό (private), το υβριδικό (hybrid) ή το κοινοτικό (community), καθένα με μοναδικά χαρακτηριστικά και πλεονεκτήματα.

2.2.3.1. Δημόσιο νέφος

Το δημόσιο νέφος παρέχει μια ευρεία ποικιλία υπηρεσιών που καλύπτουν όλους τους τομείς της υπολογιστικής, από την αποθήκευση δεδομένων μέχρι τις εφαρμογές και τη δικτύωση. Οι εταιρείες μπορούν να προσαρμόσουν τις υπηρεσίες ανάλογα με τις ανάγκες τους και να πληρώνουν μόνο για αυτές που πραγματικά χρησιμοποιούν, αντί να επενδύουν σε ακριβό εξοπλισμό και υποδομές. Αυτό επιτρέπει στις επιχειρήσεις να εξοικονομούν σημαντικούς πόρους και να αυξάνουν την αποτελεσματικότητα και την ευελιξία τους.

Το δημόσιο νέφος ονομάζεται "δημόσιο" επειδή οι υπολογιστικοί πόροι παρέχονται από τρίτους παρόχους υπηρεσιών και είναι προσβάσιμοι από το κοινό μέσω του διαδικτύου. Αυτοί οι πάροχοι, όπως η Amazon Web Services (AWS), η Microsoft Azure και η Google Cloud Platform, διαχειρίζονται και λειτουργούν τις υποδομές και τις υπηρεσίες νέφους. Οι πάροχοι του δημόσιου νέφους βγάζουν έσοδα κυρίως μέσω της παροχής υπηρεσιών υπολογιστικού νέφους,

ακολουθώντας το μοντέλο πληρωμής ανά χρήση (pay-as-you-go). Αυτό σημαίνει ότι οι χρήστες πληρώνουν μόνο για τους πόρους και τις υπηρεσίες που καταναλώνουν.

Επιπλέον, ορισμένοι πάροχοι μπορούν να αντλούν έσοδα μέσω διαφημίσεων, ειδικά σε υπηρεσίες που απευθύνονται σε καταναλωτές, αν και αυτό δεν είναι η κανονική πρακτική για τις επιχειρηματικές λύσεις νέφους.

Η ευελιξία στις επιλογές χρέωσης είναι ένα σημαντικό πλεονέκτημα του δημόσιου νέφους. Οι εταιρείες μπορούν να επιλέξουν ανάμεσα σε διάφορα μοντέλα χρέωσης που καλύπτουν τις διαφορετικές τους ανάγκες και προτιμήσεις. Με την χρέωση βάσει την χρήση, οι επιχειρήσεις πληρώνουν μόνο για τους πόρους που πραγματικά χρησιμοποιούν, όπως η επεξεργαστική ισχύς, η αποθήκευση δεδομένων ή το εύρος ζώνης, χωρίς να αναγκάζονται να κάνουν μεγάλες αρχικές επενδύσεις. Αυτό επιτρέπει μια πιο ευέλικτη και αποτελεσματική διαχείριση του προϋπολογισμού τους, καθώς προσαρμόζουν τις δαπάνες τους ανάλογα με τη ζήτηση και τις ανάγκες τους σε κάθε χρονική στιγμή. Ωστόσο, αυτή η ευελιξία δεν ισχύει εξίσου για όλες τις υπηρεσίες. Για παράδειγμα, οι υπηρεσίες Υποδομή ως Υπηρεσία (IaaS) συνήθως χρεώνονται με βάση τη χρήση αλλά ωριαία. Το μοντέλο χρέωσης παραμένει το ίδιο, αλλά οι τιμές χρέωσης μπορεί να αλλάζουν ανάλογα με τον χρόνο δέσμευσης της υπηρεσίας. Για παράδειγμα, αν γίνει δέσμευση εικονικών μηχανών για 1 ή 2 έτη, η τιμή χρέωσης θα είναι διαφορετική σε σχέση με αυτήν που ισχύει για την κατ' απαίτηση δημιουργία εικονικής μηχανής. Αυτή η επιλογή δέσμευσης για μακροχρόνια χρήση συχνά προσφέρει σημαντικές εκπτώσεις, καθιστώντας τις μακροχρόνιες συμφωνίες πιο οικονομικές για πολλές επιχειρήσεις.

Από την άλλη πλευρά, η πληρωμή με συνδρομή προσφέρει στις επιχειρήσεις σταθερότητα και προβλεψιμότητα στις δαπάνες τους, καθώς πληρώνουν μια σταθερή μηνιαία ή ετήσια χρέωση για πρόσβαση στις υπηρεσίες του νέφους. Αυτό μπορεί να είναι ιδιαίτερα χρήσιμο για επιχειρήσεις που θέλουν να έχουν προβλέψιμα και σταθερά κόστη, χωρίς να ανησυχούν για τυχόν αυξήσεις στη χρήση πόρων.

Επιπλέον, τα αυστηρά Συμβόλαια Επιπέδου Υπηρεσιών (SLAs) που παρέχουν οι πάροχοι του δημόσιου νέφους εξασφαλίζουν υψηλή διαθεσιμότητα και αξιόπιστες υπηρεσίες. Τα SLAs καθορίζουν τις ελάχιστες απαιτήσεις απόδοσης και διαθεσιμότητας που οι πάροχοι δεσμεύονται να τηρήσουν. Συγκεκριμένα, περιλαμβάνουν εγγυήσεις για το ποσοστό διαθεσιμότητας των υπηρεσιών, που συχνά αγγίζει το 99.9% ή και περισσότερο. Αυτό σημαίνει ότι οι υπηρεσίες του νέφους θα είναι διαθέσιμες σχεδόν συνεχώς, με ελάχιστες διακοπές. Τα SLAs συχνά καθορίζουν τους χρόνους απόκρισης και αποκατάστασης σε περίπτωση προβλημάτων, εξασφαλίζοντας γρήγορη και αποτελεσματική επίλυση τυχόν τεχνικών ζητημάτων. Οι πάροχοι του νέφους συνήθως προσφέρουν και αποζημιώσεις ή εκπτώσεις στις υπηρεσίες τους αν δεν τηρήσουν τις δεσμεύσεις που περιγράφονται στα SLAs, δίνοντας έτσι ένα επιπλέον κίνητρο για την παροχή αξιόπιστων υπηρεσιών.

Η ύπαρξη αυτών των αυστηρών SLAs ενισχύει την εμπιστοσύνη των επιχειρήσεων στις υπηρεσίες του νέφους, καθώς γνωρίζουν ότι οι πάροχοι δεσμεύονται να τηρήσουν συγκεκριμένα επίπεδα απόδοσης και διαθεσιμότητας. Οι επιχειρήσεις μπορούν να αυξήσουν ή να μειώσουν τους πόρους που χρησιμοποιούν ανάλογα με τις ανάγκες τους, χωρίς τους περιορισμούς που

θέτει ο φυσικός εξοπλισμός. Αυτό επιτρέπει την άμεση ανταπόκριση σε αυξομειώσεις της ζήτησης και την αποδοτική διαχείριση των πόρων.

Αν και το δημόσιο νέφος προσφέρει αξιόλογα οφέλη, όπως ευελιξία και αποτελεσματική χρήση πόρων, υπάρχουν προκλήσεις που πρέπει να ληφθούν σοβαρά υπόψη. Η ασφάλεια δεδομένων αποτελεί έναν σημαντικό παράγοντα, καθώς οι επιχειρήσεις εκθέτουν τις ευαίσθητες πληροφορίες τους σε τρίτους παρόχους. Είναι ζωτικής σημασίας να υπάρχουν αποτελεσματικά μέτρα ασφαλείας για την προστασία των δεδομένων αυτών από διαρροές ή παραβίαση της απορρήτου τους.

Η απόδοση μπορεί να μην είναι η ίδια σε σχέση με ένα ιδιωτικό νέφος λόγω του overprovisioning των πόρων. Οι πόροι σε ένα δημόσιο νέφος μοιράζονται μεταξύ πολλών χρηστών και εφαρμογών, γεγονός που μπορεί να οδηγήσει σε μεταβολές στην απόδοση, ειδικά σε περιόδους αιχμής. Αυτό μπορεί να επηρεάσει την απόκριση και τη σταθερότητα των εφαρμογών που φιλοξενούνται στο δημόσιο νέφος. Έπειτα, οι επιχειρήσεις έχουν περιορισμένο έλεγχο πάνω στις υποδομές και τις υπηρεσίες στο δημόσιο νέφος. Αυτό μπορεί να αποτελέσει πρόβλημα για οργανισμούς που χρειάζονται εξειδικευμένες λύσεις ή θέλουν να προσαρμόσουν τις υπηρεσίες σύμφωνα με τις ακριβείς απαιτήσεις τους.

Επιπλέον, η εξάρτηση από το διαδίκτυο μπορεί να οδηγήσει σε δυσκολίες κατά την πρόσβαση στις υπηρεσίες σε περιπτώσεις που υπάρχουν προβλήματα με τη σύνδεση ή ακόμα και διακοπές στη λειτουργία τους. Η διακοπή στη λειτουργία μιας υπηρεσίας στο νέφος δεν απαραίτητα οφείλεται αποκλειστικά σε προβλήματα στη σύνδεση ή στο διαδίκτυο. Αυτό μπορεί να συμβεί για πολλούς λόγους, συμπεριλαμβανομένων τεχνικών ανωμαλιών, βλαβών στον εξοπλισμό ή ακόμα και ανθρωπίνων λαθών. Επιπλέον, η αξιοπιστία των υπηρεσιών στο νέφος επηρεάζεται από τη συνολική αρχιτεκτονική και τις διαδικασίες λειτουργίας του συστήματος. Είναι σημαντικό να υιοθετηθούν κατάλληλα μέτρα για τη διαχείριση και τη μείωση των κινδύνων που σχετίζονται με αυτές τις πιθανές προκλήσεις. [30]

2.2.3.2. Ιδιωτικό νέφος

Το ιδιωτικό νέφος αναφέρεται σε ένα εξειδικευμένο περιβάλλον υπολογιστικού νέφους που σχεδιάζεται ειδικά για την ανταπόκριση στις συγκεκριμένες ανάγκες μιας επιχείρησης ή οργανισμού. Σε αντίθεση με το δημόσιο νέφος, το ιδιωτικό νέφος δεν είναι διαθέσιμο για ευρύτερη, δημόσια χρήση, αλλά λειτουργεί αποκλειστικά για τα εσωτερικά δίκτυα και τις ανάγκες της συγκεκριμένης επιχείρησης ή οργανισμού. Οπότε, σε αυτή την περίπτωση, η επιχείρηση λειτουργεί ταυτόχρονα ως πάροχος και καταναλωτής του ιδιωτικού της νέφους όπου ένα τμήμα της επιχείρησης (πχ. το ΤΠΕ τμήμα) διοικεί και παρέχει υπηρεσίες νέφους σε άλλα τμήματα της επιχείρησης.

Το ιδιωτικό νέφος συνήθως χρησιμοποιείται από εταιρείες που λειτουργούν σε ευαίσθητους τομείς, όπως η υγεία, οι χρηματοοικονομικές υπηρεσίες, ή ο δημόσιος τομέας, όπου η απόλυτη ελεγχσιμότητα και η ασφάλεια των δεδομένων αποτελούν προτεραιότητα. Αυτό το είδος νέφους παρέχει τις ίδιες λειτουργίες με το δημόσιο νέφος, αλλά με περισσότερο έλεγχο και προσαρμογή στις ανάγκες της επιχείρησης.

Η προστασία αυτών των δεδομένων γίνεται μέσω προηγμένων μέτρων ασφαλείας, όπως εταιρικά firewalls, λογισμικά ανίχνευσης και πρόληψης εισβολών (IDS/IPS), κρυπτογράφηση δεδομένων και συστημάτων διαχείρισης ταυτότητας. Επιπλέον, η εσωτερική φιλοξενία των δεδομένων εξασφαλίζει ότι οι πληροφορίες παραμένουν στο εσωτερικό δίκτυο του οργανισμού, ελαχιστοποιώντας τον κίνδυνο διαρροής ή ανεπιθύμητης πρόσβασης. Τέλος, εφαρμόζονται καλές πρακτικές ασφάλειας καθώς και κατάλληλες αρχιτεκτονικές ασφάλειας ώστε να εξασφαλιστεί ένα υψηλό επίπεδο ασφάλειας στο ιδιωτικό νέφος.

Ωστόσο, η διαχείριση ενός ιδιωτικού νέφους απαιτεί σημαντικούς πόρους και εμπειρογνομosύνη. Οι οργανισμοί πρέπει να επενδύουν σε εξειδικευμένο προσωπικό που θα διαχειρίζεται και θα παρακολουθεί την υποδομή τους, καθώς και σε συστήματα παρακολούθησης και διαχείρισης ασφαλείας. Επιπλέον, οι εταιρείες φέρουν την πλήρη ευθύνη για τη συντήρηση και την ενημέρωση της υποδομής τους, περιλαμβανομένης της αναβάθμισης του λογισμικού και της αντιμετώπισης ενδεχόμενων ασφαλιστικών προβλημάτων. Αυτό απαιτεί συνεχείς επενδύσεις και προσοχή στη λειτουργικότητα και την ασφάλεια του ιδιωτικού νέφους.

Τα "χαλαρά" Service Level Agreements (SLAs) είναι συμφωνίες μεταξύ παρόχων υπηρεσιών νέφους και πελατών τους που ορίζουν τα επίπεδα υπηρεσίας που πρέπει να παρέχονται. Σε αντίθεση με τα "αυστηρά" SLAs που ορίζουν συγκεκριμένα πρότυπα απόδοσης και διαθεσιμότητας, τα χαλαρά SLAs είναι λιγότερο αυστηρά και μπορεί να περιλαμβάνουν ελαστικές διατάξεις. Αυτό συχνά οδηγεί σε μια μεγαλύτερη βαθμολογία ελέγχου και ευελιξίας, αλλά μπορεί επίσης να δημιουργήσει αβεβαιότητα όσον αφορά την πραγματική ποιότητα των υπηρεσιών. Η μικρή ποικιλία σε πόρους αναφέρεται στον περιορισμένο αριθμό επιλογών που διατίθενται στους χρήστες του ιδιωτικού νέφους. Αυτό μπορεί να οφείλεται στον περιορισμένο αριθμό υποδομών ή υπηρεσιών που προσφέρονται, οι οποίες μπορεί να μην καλύπτουν πλήρως τις ανάγκες ορισμένων επιχειρήσεων. Επιπλέον, οι περιορισμένες δυνατότητες επέκτασης του ιδιωτικού νέφους λόγω του περιορισμένου προϋπολογισμού μιας επιχείρησης σημαίνουν ότι η επιχείρηση ενδέχεται να μην έχει τη δυνατότητα να αναβαθμίσει ή να επεκτείνει την υποδομή του νέφους σύμφωνα με τις αυξανόμενες ανάγκες της. Αυτό μπορεί να περιορίσει την ικανότητα της επιχείρησης να ανταποκριθεί σε αιφνίδιες αλλαγές στη ζήτηση ή να παρέχει νέες υπηρεσίες και λειτουργίες στους χρήστες της. [30]

2.2.3.3. Υβριδικό νέφος

Το υβριδικό νέφος αποτελεί ένα πολύπλοκο περιβάλλον ΤΠΕ, όπου συνδυάζονται διάφορα συστατικά/υποκείμενα περιβάλλοντα σε ένα ενιαίο σύστημα. Αυτά τα περιβάλλοντα ενσωματώνονται μέσω διαφόρων δικτύων, όπως τοπικά δίκτυα (LANs), ευρυζωνικά δίκτυα (WANs), εικονικά ιδιωτικά δίκτυα (VPNs) και διεπαφές προγραμματισμού εφαρμογών (APIs).

Η συμβατότητα και η φορητότητα είναι κρίσιμες για την αποτελεσματική λειτουργία του υβριδικού νέφους. Η διασφάλιση ότι τα διάφορα περιβάλλοντα είναι σε θέση να επικοινωνούν και να συνεργάζονται μεταξύ τους, ανεξαρτήτως του ποιος τοποθετεί ή παρέχει την υποδομή, είναι κρίσιμη. Η χρήση πρότυπων τεχνολογιών και πρωτοκόλλων μπορεί να διευκολύνει την αλληλεπίδραση μεταξύ των διαφόρων στοιχείων του υβριδικού περιβάλλοντος. Τα VPN, το διαδίκτυο και τα ευρυζωνικά δίκτυα μπορούν να αποτελέσουν σημαντικά μέσα για τη δημιουργία

αυτής της φορητότητας και συμβατότητας. Επίσης, οι τεχνολογίες όπως τα software-defined δίκτυα μπορούν να προσφέρουν ευελιξία και διαχείριση του δικτύου, ενισχύοντας την απόδοση και την ασφάλεια.

Το υβριδικό νέφος μπορεί να παρέχει μια ευρεία γκάμα χαρακτηριστικών που προσαρμόζονται στις μοναδικές ανάγκες κάθε οργανισμού. Ανάλογα με τις απαιτήσεις και τις προτιμήσεις που τίθενται, ένα υβριδικό νέφος μπορεί να αποτελείται από τουλάχιστον ένα ιδιωτικό νέφος και ένα δημόσιο νέφος, επιτρέποντας σε έναν οργανισμό να αξιοποιήσει τα πλεονεκτήματα και των δύο τύπων υποδομής. Ένα υβριδικό νέφος προσφέρει στους οργανισμούς τη δυνατότητα να εκμεταλλευτούν τα πλεονεκτήματα τόσο του ιδιωτικού όσο και του δημόσιου νέφους σε συνδυασμό. Αυτό επιτρέπει σε μια επιχείρηση να ανταποκριθεί ευέλικτα στις μεταβαλλόμενες ανάγκες της, διατηρώντας ταυτόχρονα τον έλεγχο και την ασφάλεια των δεδομένων της. Για παράδειγμα, ευαίσθητες εφαρμογές και δεδομένα μπορούν να φιλοξενηθούν σε ιδιωτικό νέφος για μέγιστη ασφάλεια, ενώ η ελαστικότητα του δημόσιου νέφους μπορεί να χρησιμοποιηθεί για την αντιμετώπιση αιχμών φόρτου ή για την εκτέλεση μη- κρίσιμων εργασιών.

Μέσω αυτού του μοντέλου, οι οργανισμοί μπορούν να επιτύχουν την ιδανική ισορροπία μεταξύ ευελιξίας, ασφάλειας και αποδοτικότητας στον τομέα των υπολογιστικών υποδομών τους. Επιπλέον, μπορεί να συμπεριλαμβάνει δύο ή περισσότερα ιδιωτικά ή δημόσια νέφη, επιτρέποντας την αποτελεσματική χρήση πολλαπλών υπηρεσιών νέφους. Η διαφορά μεταξύ της προηγούμενης περίπτωσης και της περίπτωσης που περιλαμβάνει δύο ή περισσότερα ιδιωτικά ή δημόσια νέφη είναι η πολυπλοκότητα και η ευελιξία της υποδομής. Σε αυτήν την περίπτωση, ο οργανισμός μπορεί να έχει περισσότερες επιλογές σε ό,τι αφορά τη διαχείριση των φορτίων εργασίας και των δεδομένων του. Όσον αφορά τις περιπτώσεις χρήσης, ενώ στην προηγούμενη περίπτωση μπορεί να είχαμε ένα ιδιωτικό και ένα δημόσιο νέφος για την κάλυψη διαφορετικών αναγκών (ασφάλειας έναντι ευελιξίας), εδώ μπορούμε να έχουμε πολλαπλά ιδιωτικά ή δημόσια νέφη για να καλύψουμε ακόμη περισσότερες παραλλαγές αυτών των αναγκών. Αυτό μπορεί να οδηγήσει σε μεγαλύτερη πολυπλοκότητα στη διαχείριση και συντήρηση, αλλά ταυτόχρονα προσφέρει περισσότερες επιλογές και ευελιξία στον οργανισμό.

Τα πλεονεκτήματα του υβριδικού νέφους περιλαμβάνουν την ευελιξία και προσαρμοστικότητα, επιτρέποντας την επιλογή του καταλληλότερου περιβάλλοντος (δημόσιο ή ιδιωτικό νέφος) για κάθε εφαρμογή ή εργασία, ανάλογα με τις ανάγκες της επιχείρησης, καθώς και την εύκολη μεταφορά των εφαρμογών και των δεδομένων μεταξύ των διαφορετικών περιβαλλόντων. Επιπλέον, παρέχεται δυνατότητα εξοικονόμησης κόστους μέσω της χρήσης δημόσιων υπηρεσιών νέφους για μη ευαίσθητα δεδομένα ή για εργασίες με μεταβλητές ανάγκες πόρων, μειώνοντας το κόστος υποδομής.

Στο κομμάτι της ασφάλειας, τα ευαίσθητα δεδομένα μπορούν να διατηρηθούν σε ιδιωτικά νέφη, ενώ λιγότερο κρίσιμα δεδομένα μπορούν να φιλοξενηθούν σε δημόσια νέφη, με την ενίσχυση της ασφάλειας να γίνεται μέσω της χρήσης πολλαπλών επιπέδων προστασίας και ελέγχου πρόσβασης. Στην κλιμάκωση και απόδοση, δίνεται δυνατότητα δυναμικής κλιμάκωσης των πόρων ανάλογα με τις ανάγκες, επιτρέποντας την αντιμετώπιση αιχμών ζήτησης χωρίς υπερβολικές επενδύσεις σε υποδομές και βελτιωμένη απόδοση μέσω της χρήσης εξειδικευμένων πόρων από διαφορετικά περιβάλλοντα.

Παρά την πολυπλοκότητα διαχείρισης, η οποία απαιτεί προηγμένες ικανότητες και ένα ολοκληρωμένο σύστημα διαχείρισης, το υβριδικό νέφος παρουσιάζει ορισμένα μειονεκτήματα. Η διαχείριση της ασφάλειας σε πολλαπλά περιβάλλοντα μπορεί να είναι πολύπλοκη και απαιτεί εξειδικευμένη γνώση και διαδικασίες, ενώ η συμμόρφωση με κανονισμούς μπορεί να είναι δύσκολη, ειδικά όταν μεταφέρονται δεδομένα μεταξύ διαφορετικών νομικών και γεωγραφικών περιοχών.

Η αρχική επένδυση και η συνεχής διαχείριση των υβριδικών λύσεων μπορεί να είναι υψηλή, με πιθανά κρυφά κόστη από την ανάγκη για εξειδικευμένα εργαλεία και προσωπικό. Η επιχείρηση εξαρτάται από την αξιοπιστία και την απόδοση των παρόχων δημόσιων και ιδιωτικών νεφών, και η πιθανή ανάγκη αλλαγής παρόχου μπορεί να επιφέρει σημαντικές προκλήσεις και κόστος. Τέλος, η δικτύωση μεταξύ των διαφορετικών περιβαλλόντων μπορεί να προκαλέσει καθυστερήσεις και να επηρεάσει την απόδοση των εφαρμογών, απαιτώντας έναν αποτελεσματικό σχεδιασμό δικτύου που να εξασφαλίζει την σωστή λειτουργία σε όλα τα περιβάλλοντα. [30]

2.2.3.4. Κοινοτικό Νέφος

Ένα κοινοτικό νέφος βρίσκεται ανάμεσα στο δημόσιο και το ιδιωτικό cloud όσον αφορά την ομάδα των χρηστών που εξυπηρετεί. Είναι κάπως παρόμοιο με ένα ιδιωτικό cloud, αλλά η υποδομή και οι υπολογιστικοί πόροι είναι αποκλειστικά διαθέσιμοι σε δύο ή περισσότερους οργανισμούς που έχουν κοινές απαιτήσεις για την προστασία της ιδιωτικότητας, την ασφάλεια και τη συμμόρφωση με κανονισμούς, αντί για έναν μόνο οργανισμό. Το community cloud επιδιώκει να συνδυάσει την παροχή διανεμημένων πόρων από το grid computing, τον διανεμημένο έλεγχο από τα ψηφιακά οικοσυστήματα και την αειφορία από την πράσινη πληροφορική, με τις χρήσεις του cloud computing, ενώ παράλληλα κάνει μεγαλύτερη χρήση των προόδων της αυτοδιαχείρισης από την autonomic computing.

Η αντικατάσταση των vendor clouds με τη διαμόρφωση των υποχρησιμοποιούμενων πόρων των υπολογιστικών μηχανών των χρηστών για τη δημιουργία ενός community cloud, με κόμβους που ενδεχομένως εκπληρώνουν όλους τους ρόλους – καταναλωτή, παραγωγού και, πιο σημαντικά, συντονιστή – αποτελεί βασική πτυχή αυτής της προσέγγισης.

Ένα από τα βασικά πλεονεκτήματα ενός community cloud είναι ότι το κόστος δημιουργίας του μπορεί να είναι χαμηλότερο σε σύγκριση με τη δημιουργία ενός ιδιωτικού cloud για κάθε οργανισμό ξεχωριστά. Αυτό οφείλεται στην κατανομή των εξόδων μεταξύ όλων των συμμετεχόντων οργανισμών. Επιπλέον, η διαχείριση του community cloud μπορεί να ανατεθεί σε έναν πάροχο cloud, ο οποίος λειτουργεί ως αμερόληπτος τρίτος που δεσμεύεται από συμβατικές υποχρεώσεις και δεν έχει καμία προτίμηση προς κανέναν από τους πελάτες. Αυτή η εξωτερική διαχείριση μπορεί να προσφέρει υψηλά επίπεδα ασφάλειας και συμμόρφωσης με κανονισμούς, καθιστώντας την λύση ελκυστική για οργανισμούς με αυστηρές απαιτήσεις σε αυτούς τους τομείς.

Ένα άλλο πλεονέκτημα είναι η δυνατότητα χρήσης εργαλείων που βρίσκονται στο community cloud για την αξιοποίηση των αποθηκευμένων πληροφοριών, με σκοπό την εξυπηρέτηση των καταναλωτών και τη βελτιστοποίηση της αλυσίδας εφοδιασμού. Για παράδειγμα, τα δεδομένα μπορούν να χρησιμοποιηθούν για την παρακολούθηση επιστροφών

προϊόντων και τη διαχείριση της παραγωγής και διανομής με τρόπο που να ανταποκρίνεται στις πραγματικές ανάγκες σε πραγματικό χρόνο.

Ωστόσο, ένα από τα μειονεκτήματα του community cloud είναι ότι τα κόστη μπορεί να είναι υψηλότερα σε σύγκριση με ένα δημόσιο cloud. Αυτό συμβαίνει διότι οι συμμετέχοντες οργανισμοί πρέπει να επενδύσουν σε υποδομές και διαχείριση που δεν θα ήταν απαραίτητα σε ένα δημόσιο cloud. Επίσης, η ποσότητα εύρους ζώνης και αποθήκευσης δεδομένων είναι σταθερή και μοιράζεται μεταξύ όλων των μελών της κοινότητας, κάτι που μπορεί να περιορίσει την ευελιξία και την αποδοτικότητα του συστήματος σε περιόδους υψηλής ζήτησης.[30]

2.2.3.5. Ομοσπονδιακό Νέφος

Η "cloud federation" είναι μια τεχνολογία και αρχιτεκτονική που επιτρέπει σε πολλαπλούς παρόχους υπηρεσιών cloud να συνεργάζονται και να προσφέρουν ενοποιημένες υπηρεσίες στους χρήστες. Μέσω της ομοσπονδίας νεφών, οι πόροι από διαφορετικούς παρόχους cloud μπορούν να συνδυαστούν και να διατεθούν στους χρήστες ως μια ενιαία, συνεκτική υπηρεσία. Αυτή η προσέγγιση προσφέρει διάφορα πλεονεκτήματα όσον αφορά την ευελιξία, την επεκτασιμότητα, την απόδοση και την ανθεκτικότητα.

Στα ομοσπονδιακά νέφη οι υποδομές διαφορετικών παρόχων cloud μπορούν να συνεργάζονται και να διαμοιράζονται πόρους, επιτρέποντας στους χρήστες να εκμεταλλεύονται τις δυνατότητες πολλών παρόχων. Επίσης οι υπολογιστικοί πόροι μπορούν να διαμοιραστούν μεταξύ των παρόχων, επιτρέποντας την πιο αποδοτική χρήση τους. Κάθε πάροχος cloud διατηρεί την αυτονομία του, αλλά μπορεί να συμμετέχει σε ομοσπονδία με άλλους παρόχους για να προσφέρει συνδυασμένες υπηρεσίες. Παρέχεται μια ενιαία πλατφόρμα διαχείρισης που επιτρέπει στους χρήστες να διαχειρίζονται τους πόρους από διαφορετικούς παρόχους ως ένα ενιαίο σύνολο. Τέλος η ομοσπονδία νεφών μπορεί να ενσωματώσει πολιτικές ασφάλειας και συμμόρφωσης που διασφαλίζουν ότι τα δεδομένα και οι υπηρεσίες διαχειρίζονται με ασφαλή και συμμορφωμένο τρόπο.

Οι προκλήσεις της συγκεκριμένης κατηγορίας σχετίζονται με την διαλειτουργικότητα και την τυποποίηση όπου η επίτευξη διαλειτουργικότητας μεταξύ διαφορετικών παρόχων απαιτεί τη χρήση κοινών προτύπων και πρωτοκόλλων. Την ασφάλεια και την κανονιστική συμμόρφωση, καθώς η διαχείριση τους σε ένα ομοσπονδιακό περιβάλλον μπορεί να είναι περίπλοκη, ιδιαίτερα όταν οι πάροχοι έχουν διαφορετικές πολιτικές και πρακτικές. Και τέλος την διαχείριση και την συντήρηση καθώς η ενοποιημένη διαχείριση πόρων από διαφορετικούς παρόχους μπορεί να είναι δύσκολη και να απαιτεί εξειδικευμένες λύσεις και εργαλεία.

2.2.4. Υπηρεσίες του υπολογιστικού νέφους

Το υπολογιστικό νέφος έχει μετασχηματίσει τον τρόπο που οι επιχειρήσεις αντιλαμβάνονται και χρησιμοποιούν την υπολογιστική ισχύ. Αυτή η τεχνολογία διαθέτει μια πληθώρα υπηρεσιών που επιτρέπουν στις επιχειρήσεις να αποκτήσουν πρόσβαση σε πόρους υπολογιστικής ισχύος και λογισμικό χωρίς την ανάγκη να διαθέτουν και να διαχειρίζονται μια δική τους υποδομή. Οι τρεις κύριες κατηγορίες υπηρεσιών που προσφέρονται από τα συστήματα υπολογιστικού νέφους είναι: Λογισμικό ως Υπηρεσία (Software as a Service - SaaS), Πλατφόρμα ως Υπηρεσία (Platform as a Service - PaaS) και Υποδομή ως Υπηρεσία (Infrastructure as a Service - IaaS).

2.2.4.1 Λογισμικό ως Υπηρεσία (Software as a Service - SaaS)

Το Λογισμικό ως Υπηρεσία (Software as a Service - SaaS) αντιπροσωπεύει ένα μοντέλο παροχής υπηρεσιών στον τομέα του υπολογιστικού νέφους, όπου οι χρήστες έχουν πρόσβαση σε προσφερόμενο λογισμικό και εφαρμογές, που εκτελούνται στο υπολογιστικό νέφος, μέσω του Διαδικτύου χρησιμοποιώντας έναν λεπτό πελάτη όπως είναι ένας φυλλομετρητής (browser), χωρίς να απαιτείται η εγκατάσταση ή η συντήρησή των εφαρμογών αυτών στις δικές τους συσκευές, μηχανήματα ή συστήματα.

Στο επίπεδο του SaaS προσφέρεται μια ευρεία γκάμα εφαρμογών και λογισμικού, συμπεριλαμβανομένων εργαλείων παραγωγικότητας, εφαρμογών γραφείου, λογιστικών προγραμμάτων, λύσεων διαχείρισης πελατών (CRM) και πολλών άλλων. Οι χρήστες μπορούν να αποκτήσουν πρόσβαση σε αυτές τις εφαρμογές μέσω ενός φυλλομετρητή, προγραμματιστικών APIs / SDKs ή μέσω ειδικών εφαρμογών που είναι διαθέσιμες για διάφορες πλατφόρμες.

Ένα από τα βασικά πλεονεκτήματα του SaaS είναι η ευελιξία που προσφέρει στους χρήστες. Η δυνατότητα πρόσβασης από οποιαδήποτε συσκευή με σύνδεση στο Διαδίκτυο επιτρέπει στους χρήστες να εργάζονται από οπουδήποτε και οποτεδήποτε, αυξάνοντας την ευελιξία και την παραγωγικότητά τους. Αυτό σημαίνει ότι οι εργαζόμενοι μπορούν να προσαρμόσουν το περιβάλλον εργασίας τους στις δικές τους προτιμήσεις και ανάγκες, ανεξάρτητα από τον τόπο ή τη συσκευή που χρησιμοποιούν. Ακόμη το μοντέλο τιμολόγησης του SaaS προσφέρει ευελιξία και προσαρμοστικότητα στις ανάγκες του κάθε χρήστη. Αυτό επιτρέπει στις εταιρείες να επιλέξουν το πρόγραμμα συνδρομής/χρέωσης που ταιριάζει καλύτερα στις ανάγκες και τον προϋπολογισμό τους. Οι πελάτες έχουν τη δυνατότητα να επιλέξουν ανάμεσα σε διαφορετικά πακέτα υπηρεσιών που προσφέρονται, βασισμένα στην έκταση της λειτουργικότητας που χρειάζονται, τον αριθμό των χρηστών τους που θα προσπελάσουν την εκάστοτε υπηρεσία και τις απαιτήσεις τους.

Με το μοντέλο SaaS, οι εταιρείες που παρέχουν τις υπηρεσίες φέρουν το βάρος της φιλοξενίας, της συντήρησης, και της ασφάλειας του λογισμικού σε υποδομές που είναι είτε δικές τους είτε ενοικιάζονται από παρόχους νέφους. Αυτό ελαχιστοποιεί τις ανησυχίες των χρηστών σχετικά με την εγκατάσταση και τη συντήρηση λογισμικού στις δικές τους συσκευές. Οι χρήστες, αντί να αγοράζουν άδειες λογισμικού και να υποστηρίζουν το βάρος των αναβαθμίσεων,

επιλέγουν συνήθως να καταβάλλουν μηνιαία ή ετήσια συνδρομή για τη χρήση του λογισμικού αυτού. Αυτό τους παρέχει την ευελιξία να αποφύγουν αρχικά υψηλά κόστη εγκατάστασης και να εξασφαλίσουν την πρόσβαση σε συνεχείς βελτιώσεις και ενημερώσεις του λογισμικού. Επιπλέον, αυτή η δομή τιμολόγησης επιτρέπει στους χρήστες να προσαρμόσουν τις δαπάνες τους βάσει των υπηρεσιών που πραγματικά χρειάζονται, εξοικονομώντας πόρους και βελτιώνοντας την οικονομική τους αποδοτικότητα.

Το μοντέλο SaaS παρέχει προγράμματα τιμολόγησης που βασίζονται στην πραγματική χρήση, γνωστά και ως pay-as-you-go. Με αυτήν τη μέθοδο χρέωσης, οι χρήστες πληρώνουν μόνο για τους πόρους που πραγματικά χρησιμοποιούν. Αυτό σημαίνει ότι δεν υπάρχουν προκαθορισμένες πληρωμές, αλλά η χρέωση βασίζεται απευθείας στην πραγματική χρήση του λογισμικού ή των υπηρεσιών. Αυτό το μοντέλο τιμολόγησης επιτρέπει στους χρήστες να εξοικονομούν χρήματα σε περιόδους χαμηλής χρήσης, ενώ ταυτόχρονα τους παρέχει την ευελιξία να αυξομειώνουν τη χρήση τους ανάλογα με τις ανάγκες τους.

Και τα δύο μοντέλα τιμολόγησης δηλαδή η συνδρομή και το pay-as-you-go, μπορούν να εφαρμοστούν στο λογισμικό ως υπηρεσία (SaaS), αλλά εξαρτάται από την πολιτική τιμολόγησης κάθε εταιρείας ή πάροχου υπηρεσιών SaaS. Στην περίπτωση της συνδρομής, οι χρήστες πληρώνουν μια σταθερή τιμή για ένα συγκεκριμένο χρονικό διάστημα, συνήθως μηνιαία ή ετήσια, για πρόσβαση στο λογισμικό και τις υπηρεσίες του. Αυτό το μοντέλο είναι συνηθισμένο για εφαρμογές που απαιτούν σταθερή και συνεχή χρήση, όπως εφαρμογές γραφείου ή εργαλεία παραγωγικότητας. Από την άλλη πλευρά, το μοντέλο pay-as-you-go βασίζεται στην πραγματική χρήση του λογισμικού ή των υπηρεσιών και οι χρήστες πληρώνουν μόνο για τους πόρους που πραγματικά χρησιμοποιούν. Αυτό το μοντέλο είναι συχνά πιο ευέλικτο και επιτρέπει στους χρήστες να πληρώνουν μόνο για αυτό που χρειάζονται, χωρίς να πρέπει να προβλέπουν εκ των προτέρων την ακριβή χρήση τους. Δεν αποκλείεται να γίνεται χρήση ενός μοντέλου που συνδυάζει και τα 2. Συνδρομή & Pay as you go, καθώς ένας πελάτης να έχει προβλέψει τις μελλοντικές του ανάγκες και να ορίσει το κόστος της συνδρομής αναλόγως την (χρονική) περίοδο να αλλάζει και είτε να αυξομειώνεται είτε να αυξάνεται με τον χρόνο καθώς αυξάνεται η χρήση.

Ένα από τα σημαντικότερα μειονεκτήματα του SaaS είναι η ανησυχία για την ασφάλεια και το απόρρητο των δεδομένων. Όταν τα δεδομένα αποθηκεύονται και επεξεργάζονται σε απομακρυσμένα κέντρα δεδομένων από τον πάροχο SaaS, οι χρήστες είναι αναγκασμένοι να εμπιστευτούν την ασφάλεια αυτών των υποδομών. Αν και οι πάροχοι SaaS συχνά λαμβάνουν σημαντικά μέτρα ασφαλείας, όπως κρυπτογράφηση δεδομένων και εφαρμογή προηγμένων μέτρων πρόληψης, υπάρχει πάντα ο κίνδυνος για πιθανές παραβιάσεις ή διαρροές δεδομένων. Αυτό μπορεί να οδηγήσει σε μείωση της εμπιστοσύνης των χρηστών και να δημιουργήσει νομικές ή κανονιστικές επιπτώσεις για τις επιχειρήσεις που χρησιμοποιούν SaaS υπηρεσίες. Επιπλέον, οι χρήστες μπορεί να ανησυχούν για το πώς τα προσωπικά τους δεδομένα χρησιμοποιούνται από τους παρόχους των υπηρεσιών SaaS, καθώς μπορεί να υπάρχουν ζητήματα σχετικά με την ιδιωτικότητα και την εμπιστευτικότητα. Ως εκ τούτου, η ανησυχία για την ασφάλεια και το απόρρητο των δεδομένων είναι ένα σημαντικό ζήτημα που πρέπει να ληφθεί υπόψη κατά τη χρήση των υπηρεσιών SaaS.

Ένα άλλο σημαντικό πρόβλημα είναι η εξάρτηση από τη διαθεσιμότητα του δικτύου. Η λειτουργία του SaaS είναι εξ ολοκλήρου εξαρτημένη από μια σταθερή και αξιόπιστη σύνδεση στο Διαδίκτυο. Αυτό σημαίνει ότι οι χρήστες πρέπει να έχουν συνεχή πρόσβαση στο Διαδίκτυο για να μπορούν να χρησιμοποιήσουν τις εφαρμογές και να αποκτήσουν πρόσβαση στα δεδομένα τους. Εάν υπάρξουν διακοπές σύνδεσης ή προβλήματα με τον πάροχο υπηρεσιών Διαδικτύου, οι χρήστες ενδέχεται να μην έχουν πρόσβαση στα δεδομένα ή στις εφαρμογές τους. Αυτό μπορεί να προκαλέσει δυσκολίες στην εκτέλεση των εργασιών τους, καθώς εξαρτώνται από την πρόσβαση στις απαραίτητες εφαρμογές και δεδομένα για την ολοκλήρωση των καθημερινών τους καθηκόντων. Επιπλέον, η απώλεια σύνδεσης μπορεί να οδηγήσει σε απώλεια δεδομένων ή σε προβλήματα συγχρονισμού, ιδίως εάν οι αλλαγές δεδομένων δεν αποθηκεύονται τοπικά και δεν συγχρονίζονται αυτόματα με τον πάροχο SaaS. Επομένως, η εξάρτηση από τη διαθεσιμότητα του δικτύου είναι ένα σημαντικό πρόβλημα που πρέπει να ληφθεί υπόψη κατά τη χρήση των υπηρεσιών SaaS.

Η αποκεντρωμένη φύση του SaaS μπορεί να οδηγήσει σε προβλήματα απόδοσης. Καθώς οι εφαρμογές SaaS εκτελούνται σε απομακρυσμένους διακομιστές που ελέγχονται από τον πάροχο υπηρεσιών, η απόδοση του συστήματος μπορεί να επηρεαστεί από πολλούς παράγοντες. Ένας από αυτούς είναι η κίνηση στο δίκτυο. Καθώς πολλοί χρήστες συνδέονται ταυτόχρονα στον ίδιο διακομιστή, μπορεί να προκύψουν συμφόρηση και μπλοκαρίσματα στην κίνηση του δικτύου, επηρεάζοντας έτσι τους χρόνους απόκρισης και τη γενική απόδοση του συστήματος. Επιπλέον, ο φόρτος στον διακομιστή είναι ένας άλλος σημαντικός παράγοντας. Καθώς ο αριθμός των χρηστών που χρησιμοποιούν την εφαρμογή αυξάνεται, ο διακομιστής μπορεί να φτάσει στα όριά του ως προς την επεξεργαστική ισχύ και τη μνήμη, προκαλώντας αργούς χρόνους απόκρισης και πιθανά προβλήματα απόδοσης. Αυτά τα προβλήματα μπορούν να έχουν σοβαρές επιπτώσεις στην εμπειρία των χρηστών και να επηρεάσουν αρνητικά την παραγωγικότητά τους. Η αποκεντρωμένη φύση του SaaS, αν και προσφέρει πολλά πλεονεκτήματα, επιφέρει και τη δυνατότητα εμφάνισης προβλημάτων απόδοσης που πρέπει να ληφθούν υπόψη κατά τη σχεδίαση και τη διαχείριση των συστημάτων. [20]

2.2.4.2 Πλατφόρμα ως Υπηρεσία (Platform as a Service - PaaS)

Η Πλατφόρμα ως Υπηρεσία (Platform as a Service - PaaS) αποτελεί ένα είδος υπηρεσίας υπολογιστικού νέφους που παρέχει ένα ολοκληρωμένο περιβάλλον ανάπτυξης λογισμικού για τους προγραμματιστές. Αυτό το περιβάλλον περιλαμβάνει εργαλεία, βιβλιοθήκες, πλαίσια ανάπτυξης, μεσισμικό (middleware), υπηρεσίες λογισμικού και πλατφόρμες εφαρμογών που επιτρέπουν στους προγραμματιστές να αναπτύσσουν, να δοκιμάζουν και να ανακτούν εφαρμογές χωρίς την ανάγκη να διαχειρίζονται την υποκείμενη υποδομή ούτε το περιβάλλον το ίδιο. Ο όρος "ανάκτηση εφαρμογών" αναφέρεται στη διαδικασία επαναφοράς μιας εφαρμογής σε λειτουργία από το περιβάλλον ανάπτυξης ή παραγωγής μετά από μια διακοπή λειτουργίας ή ένα πρόβλημα. Κατά τη διάρκεια της διαδικασίας ανάκτησης, οι προγραμματιστές χρησιμοποιούν τις διαθέσιμες λειτουργίες της πλατφόρμας PaaS για να επαναφέρουν την εφαρμογή στην κανονική της λειτουργία.

Οι περιορισμοί στα περιβάλλοντα ανάπτυξης και στα εργαλεία που παρέχονται από τον πάροχο PaaS μπορούν να έχουν διάφορες επιπτώσεις στη διαδικασία ανάπτυξης εφαρμογών.

Οι περιορισμοί αυτοί μπορεί να επηρεάσουν την επιλογή των τεχνολογιών και την αποτελεσματικότητα της ανάπτυξης, καθώς οι προγραμματιστές πρέπει να επιλέξουν ανάμεσα στην περιορισμένη γκάμα πόρων που προσφέρονται από το PaaS. Οι προγραμματιστές θα πρέπει να προσαρμοστούν στις γλώσσες προγραμματισμού ή τα πλαίσια εφαρμογών που υποστηρίζονται από τον συγκεκριμένο πάροχο PaaS. Αυτό σημαίνει ότι ενδέχεται να μην μπορούν να χρησιμοποιήσουν τις πιο πρόσφατες τεχνολογίες ή να επιλέξουν κάποια εξειδικευμένα εργαλεία που τους είναι αναγκαία για την εργασία τους.

Επιπλέον, οι προγραμματιστές ενδέχεται να μην έχουν πρόσβαση σε ορισμένες βιβλιοθήκες που συνήθως χρησιμοποιούν για την ανάπτυξη των εφαρμογών τους. Αυτό μπορεί να τους αναγκάσει να ψάξουν για εναλλακτικές λύσεις ή να προσαρμοστούν στις διαθέσιμες επιλογές.

Ωστόσο, παρ' όλους αυτούς τους περιορισμούς, το μοντέλο παράδοσης Platform as a Service (PaaS) προσφέρει ορισμένα σημαντικά πλεονεκτήματα. Η αυτόματη κλιμακωσιμότητα είναι ένα από τα σημαντικότερα, καθώς επιτρέπει στις εφαρμογές να κλιμακώνονται αυτόματα ώστε να αντιμετωπίσουν αυξημένους φόρτους εργασίας χωρίς ανθρώπινη παρέμβαση ή διακοπή των υπηρεσιών. Επιπλέον, η διαχείριση της υποδομής, συμπεριλαμβανομένης της ανάθεσης πόρων και της ασφάλειας, αναλαμβάνεται από τον πάροχο της υπηρεσίας, απαλλάσσοντας τους προγραμματιστές από αυτές τις ευθύνες.

Αυτό σημαίνει ότι οι προγραμματιστές μπορούν να επικεντρωθούν πλήρως στην ανάπτυξη και βελτίωση των εφαρμογών τους, αντί να ασχολούνται με τις λεπτομέρειες της υποδομής και της διαχείρισης. Αυτή η αφαίρεση των φόρτων λειτουργίας επιτρέπει στους προγραμματιστές να είναι πιο παραγωγικοί και να ανταποκρίνονται πιο αποτελεσματικά στις ανάγκες των χρηστών τους. Έτσι, παρά τους περιορισμούς, το PaaS παρέχει μια ευέλικτη και αποτελεσματική λύση για την ανάπτυξη και τη διαχείριση εφαρμογών.

Επιπλέον πλεονεκτήματα του PaaS περιλαμβάνουν την υποστήριξη διαφόρων agile και συνεργατικών μεθοδολογιών ανάπτυξης λογισμικού. Οι πλατφόρμες PaaS συχνά περιλαμβάνουν ενσωματωμένα εργαλεία που διευκολύνουν την ευέλικτη ανάπτυξη και τη συνεργασία μεταξύ των ομάδων. Ορισμένες πλατφόρμες PaaS επιτρέπουν στους προγραμματιστές να δουλεύουν χωρίς σύνδεση και να συγχρονίζουν τις αλλαγές τους όταν είναι ξανά συνδεδεμένοι στο δίκτυο. Επίσης, πολλές πλατφόρμες PaaS υποστηρίζουν τη χρήση δημοφιλών ολοκληρωμένων περιβαλλόντων ανάπτυξης (IDEs), όπως το Visual Studio, το IntelliJ IDEA και άλλα, διευκολύνοντας έτσι τη μετάβαση και τη συνεχή χρήση των εργαλείων που προτιμούν οι προγραμματιστές.

Παρ' όλα αυτά, υπάρχουν ορισμένα σημαντικά μειονεκτήματα που πρέπει να ληφθούν υπόψη. Το PaaS παρουσιάζει περιορισμένη ευελιξία και έλεγχο, καθώς οι χρήστες έχουν πρόσβαση μόνο σε προκαθορισμένες πλατφόρμες, γεγονός που μπορεί να μην καλύπτει όλες τις ανάγκες τους και να προκαλεί προβλήματα συμβατότητας. Επιπλέον, υπάρχει το ζήτημα του κλειδώματος προμηθευτή (vendor lock-in), όπου η μεταφορά εφαρμογών και δεδομένων σε άλλη πλατφόρμα ή επιστροφή σε on-premises λύσεις μπορεί να είναι δύσκολη και δαπανηρή λόγω των μοναδικών APIs και προτύπων που χρησιμοποιούνται από τους παρόχους PaaS. Άλλα μειονεκτήματα περιλαμβάνουν τα ζητήματα ασφαλείας, δεδομένου ότι τα δεδομένα και οι

εφαρμογές φιλοξενούνται σε υποδομές τρίτων, αυξάνοντας την πιθανότητα παραβιάσεων και τη μη συμμόρφωση με τις κανονιστικές απαιτήσεις. Επιπλέον, η εξάρτηση από την απόδοση του δικτύου μπορεί να επηρεάσει την απόδοση των εφαρμογών, ειδικά σε περιπτώσεις χαμηλής συνδεσιμότητας ή διακοπών υπηρεσιών. [20]

2.2.4.3 Υποδομή ως Υπηρεσία (Infrastructure as a Service - IaaS)

Η υποδομή ως υπηρεσία (IaaS) προσφέρει ένα ευέλικτο περιβάλλον για την ανάπτυξη, τη διαχείριση και την παροχή υποδομής ΤΠΕ σε συστημικούς διαχειριστές και εφαρμογές. Αυτό σημαίνει ότι οι πελάτες του νέφους μπορούν να αναπτύξουν και να εκτελέσουν εφαρμογές χωρίς την ανάγκη να αγοράσουν, να στήσουν και να διαχειριστούν την υποδομή τους. Οι υπηρεσίες που παρέχονται στο πλαίσιο του IaaS περιλαμβάνουν την πρόσβαση σε επεξεργαστές, μνήμη, αποθήκευση και δίκτυο, είτε ως φυσικοί πόροι είτε ως εικονικοί πόροι που προσφέρονται από τον πάροχο υπηρεσιών. Οι χρήστες μπορούν να επιλέξουν τους απαιτούμενους πόρους ανάλογα με τις ανάγκες και προτιμήσεις τους, χωρίς την ανάγκη να αγοράσουν ή να διαχειριστούν φυσικό εξοπλισμό. Επιπλέον, οι παρόχοι IaaS συνήθως παρέχουν λειτουργικά συστήματα και άλλο λογισμικό υποδομής, όπως βάσεις δεδομένων και λύσεις ασφαλείας, που μπορούν να εκτελεστούν πάνω στην προσφερόμενη υποδομή.

Το IaaS λειτουργεί με ένα ευέλικτο μοντέλο τιμολόγησης που βασίζεται στη χρήση πόρων. Αυτό σημαίνει ότι οι χρήστες πληρώνουν μόνο για τους πόρους που χρησιμοποιούν, χωρίς να υπάρχουν προκαθορισμένα μηνιαία ή ετήσια συνδρομητικά ποσά. Αυτό τους επιτρέπει να προγραμματίσουν και να διαχειριστούν καλύτερα τον προϋπολογισμό τους, ενώ ταυτόχρονα επιτρέπει την ευελιξία να προσαρμόζουν τους πόρους τους ανάλογα με τις ανάγκες τους χωρίς περιττές δαπάνες.

Επίσης, το IaaS προσφέρει αυτόματη κλιμακωσιμότητα, δηλαδή τη δυνατότητα αυτόματης προσαρμογής των πόρων ανάλογα με τις ανάγκες του χρήστη. Αυτό σημαίνει ότι, όταν οι απαιτήσεις του χρήστη αυξάνονται, επιπλέον πόροι μπορούν να αντληθούν αυτόματα, εξασφαλίζοντας ότι η εφαρμογή λειτουργεί ομαλά χωρίς να απαιτείται ανθρώπινη παρέμβαση. Αυτό βοηθάει στη διασφάλιση της απρόσκοπτης λειτουργίας των εφαρμογών και στην αποφυγή πιθανών διακοπών λειτουργίας λόγω υπερφόρτωσης, αυξάνοντας της διαθεσιμότητα και αξιοπιστία τους.

Η πρόσβαση στην υποδομή του IaaS είναι δημόσια, επιτρέποντας στους χρήστες να αποκτήσουν πρόσβαση στους πόρους τους μέσω του Διαδικτύου. Αυτό επιτρέπει στους χρήστες να εργάζονται από οπουδήποτε, μειώνοντας την ανάγκη για φυσική παρουσία σε συγκεκριμένο χώρο εργασίας και επιτρέποντας την πρόσβαση στους πόρους από οποιαδήποτε συσκευή με σύνδεση στο διαδίκτυο. Αυτή η ευελιξία καθιστά τη διαδικασία πιο ευέλικτη και αποτελεσματική, επιτρέποντας στους χρήστες να ανταποκρίνονται στις ανάγκες τους με μεγαλύτερη άνεση και αποτελεσματικότητα.

Παρόλο που η υποδομή ως υπηρεσία (IaaS) προσφέρει πολλά πλεονεκτήματα, υπάρχουν επίσης ορισμένα μειονεκτήματα που πρέπει να ληφθούν υπόψη. Η εξάρτηση από τον πάροχο υπηρεσιών είναι ένα σημαντικό ζήτημα, καθώς οι χρήστες του IaaS εξαρτώνται από την

αξιοπιστία και την ποιότητα των υπηρεσιών του παρόχου. Οποιαδήποτε προβλήματα στη διαθεσιμότητα ή στην απόδοση της υποδομής του παρόχου μπορεί να επηρεάσουν άμεσα τις εφαρμογές και τις επιχειρηματικές διαδικασίες των χρηστών. Επιπλέον, οι χρήστες μπορεί να αντιμετωπίσουν δυσκολίες στη μετεγκατάσταση σε άλλον πάροχο ή στην επιστροφή σε φυσική υποδομή. Θέματα ασφαλείας και συμμόρφωσης είναι επίσης κρίσιμα. Παρόλο που οι πάροχοι IaaS προσφέρουν συνήθως λύσεις ασφαλείας, η ασφάλεια των δεδομένων και η συμμόρφωση με κανονισμούς μπορεί να αποτελέσουν πρόκληση. Η αποθήκευση δεδομένων σε υποδομή τρίτου μέρους μπορεί να αυξήσει τον κίνδυνο παραβίασης δεδομένων ή μη εξουσιοδοτημένης πρόσβασης. Επιπλέον, ορισμένες βιομηχανίες έχουν αυστηρές απαιτήσεις συμμόρφωσης που μπορεί να είναι δύσκολο να τηρηθούν σε ένα περιβάλλον IaaS. [20]

3. Μεθοδολογία & Αναζήτηση Άρθρων

Το τρίτο κεφάλαιο της διπλωματικής εργασίας επικεντρώνεται στην περιγραφή της μεθοδολογίας που χρησιμοποιήθηκε για την έρευνα και τη συλλογή δεδομένων, καθώς και στην αναζήτηση σχετικών άρθρων και πηγών. Αυτή η ενότητα παρέχει μια λεπτομερή εξήγηση των βημάτων και της διαδικασίας που ακολουθήθηκαν για την επίτευξη των στόχων της έρευνας.

Η μεθοδολογία που ακολουθήθηκε στην παρούσα διπλωματική εργασία περιλαμβάνει τα εξής βήματα:

3.1. Σχεδιασμός της Έρευνας

Ο σκοπός της έρευνας είναι να διερευνήσει τη συνέργεια μεταξύ του Υπολογιστικού Νέφους (Cloud Computing) και της Αλυσίδας Συστοιχίας (Blockchain). Συγκεκριμένα, η έρευνα επιδιώκει να απαντήσει σε τρία κύρια ερευνητικά ερωτήματα:

- Πρώτον, πώς το Υπολογιστικό Νέφος μπορεί να ενισχύσει τις λειτουργίες και τα χαρακτηριστικά/δυνατότητες της Αλυσίδας Συστοιχίας
- Δεύτερον, πώς η Αλυσίδα Συστοιχίας μπορεί να ενισχύσει την λειτουργία και τα χαρακτηριστικά/δυνατότητες του Υπολογιστικού Νέφους.
- Η έρευνα θα εξετάσει επίσης τις προκλήσεις και τα οφέλη από την ενσωμάτωση αυτών των δύο τεχνολογιών, προκειμένου να παρέχει ένα ολοκληρωμένο πλαίσιο για την αμοιβαία τους υποστήριξη και βελτίωση.

3.2. Συλλογή Δεδομένων

Για την έρευνα αυτή, χρησιμοποιήθηκαν κυρίως δευτερογενείς πηγές δεδομένων. Οι πηγές καλύπτουν μια εκτενή βιβλιογραφική ανασκόπηση, η οποία ενσωματώνει άρθρα, βιβλία, κεφάλαια βιβλίων, διδακτορικές/μεταπτυχιακές διατριβές που σχετίζονται με τις δύο τεχνολογίες. Για τη συλλογή των δευτερογενών δεδομένων, έγιναν αναζητήσεις σε δύο πολύ γνωστές και ευρέως διαδεδομένες βιβλιογραφικές βάσεις δεδομένων το Google Scholar & το Web of Science, προκειμένου να συγκεντρωθούν και να αναλυθούν οι πιο πρόσφατες και σχετικές πληροφορίες. Με τη χρήση αυτών των εργαλείων συλλογής δεδομένων, η έρευνα καταφέρει να προσφέρει μια σφαιρική και εμπειριστατωμένη ανάλυση της συνέργειας μεταξύ του Υπολογιστικού Νέφους και της Αλυσίδας Συστοιχίας, υποστηριζόμενη από αξιόπιστα και ποικίλα δεδομένα.

3.3. Αναζήτηση άρθρων

Η αναζήτηση άρθρων και πηγών για την παρούσα εργασία ακολούθησε συγκεκριμένα βήματα για τη διασφάλιση της ποιότητας και της σχετικότητας των πληροφοριών. Αρχικά, χρησιμοποιήθηκε ένα μοτίβο επερώτησης που εκμεταλλεύεται σχετικές λέξεις-κλειδιά για την

αναζήτηση σχετικών άρθρων. Συγκεκριμένα, το μοτίβο επερώτησης ήταν (("blockchain" OR "distributed ledger") AND cloud) OR BaaS OR "Blockchain as a Service" OR "Blockchain-as-a-Service". Με αυτό το μοτίβο, επιχειρήσαμε να καλύψουμε άρθρα που εμπεριέχουν είτε στοιχεία που σχετίζονται τόσο με το blockchain όσο και με το cloud είτε άρθρα που σχετίζονται με τη συνέργεια αυτών των τεχνολογιών, όπως είναι το μοντέλο Blockchain-as-a-Service (BaaS). Στη συνέχεια, επιλέχθηκαν κύριες βάσεις δεδομένων, όπως το Google Scholar, το IEEE Xplore και το MDPI, οι οποίες είναι γνωστές για την αξιοπιστία και την ποιότητα των δημοσιεύσεών τους. Αυτές οι βάσεις δεδομένων παρέχουν πρόσβαση σε ένα ευρύ φάσμα επιστημονικών άρθρων και τεχνικών αναφορών, εξασφαλίζοντας την αξιοπιστία και την ακρίβεια των πληροφοριών που συλλέχθηκαν για την εργασία.

3.4. Φιλτράρισμα Άρθρων

Μετά την αρχική αναζήτηση και συλλογή των άρθρων, τα άρθρα επιλέχθηκαν με βάση κριτήρια αποδοχής/αποκλεισμού και ποιότητας. Τα κριτήρια αποδοχής ήταν:

- Η συνάφειά των δημοσιεύσεων με τα ερευνητικά ερωτήματα,
- Η γλώσσα συγγραφής
- Το είδος/τύπος άρθρου (άρθρο σε συνέδριο, κεφάλαιο βιβλίου, διατριβή)
- Έτος δημοσίευσης (από 2012 και έπειτα)

Διαβάστηκαν οι περιλήψεις των άρθρων για να διασφαλιστεί η σχετικότητά τους πριν από την πλήρη ανασκόπηση. Σε δεύτερη φάση και κατά την διάρκεια της συγγραφής με βάση τις αρχικές πηγές και με την περαιτέρω ανάλυση τους, πιο εξειδικευμένες αναζητήσεις εκτελούνταν ώστε να υπάρξουν περισσότερες πηγές και μεγαλύτερη εμβάθυνση. Το αποτέλεσμα της παρούσης έρευνας προήλθε από τον συνδυασμό των νέων και των αρχικών πηγών. Με την εφαρμογή αυτών των βημάτων, διασφαλίστηκε ότι η εργασία βασίζεται σε έγκυρες και αξιόπιστες πηγές, προσφέροντας μια σφαιρική και τεκμηριωμένη ανάλυση του θέματος.

Η μεθοδολογία και η αναζήτηση άρθρων που ακολουθήθηκαν στην παρούσα διπλωματική εργασία εξασφάλισαν τη συγκέντρωση έγκυρων και αξιόπιστων δεδομένων που υποστηρίζουν τα συμπεράσματα και τις προτάσεις της έρευνας που θα αναλυθούν στο Κεφάλαιο 6.

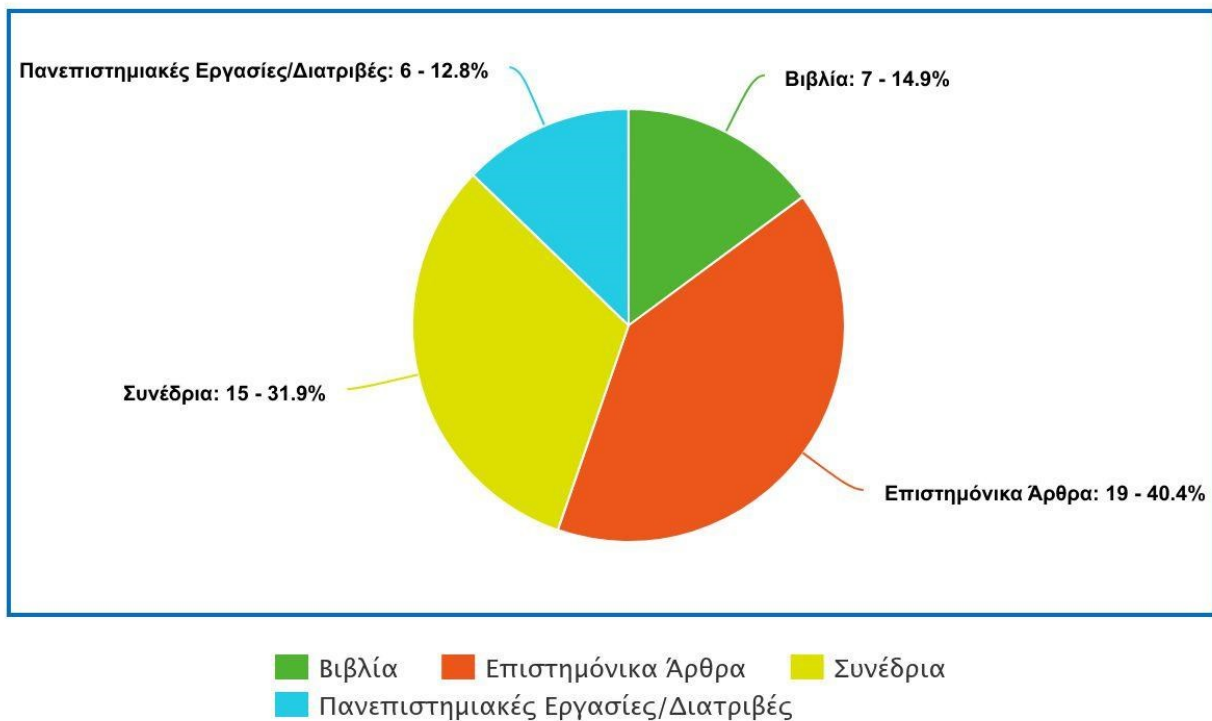
3.5. Ποσοτική ανάλυση

Αφού κατηγοριοποιήσαμε τις πηγές, ακολουθούν τα ποσοστά άρθρων/δημοσιεύσεων.

3.5.1. Ανά κατηγορία δημοσίευσης:

- **Βιβλία:** 7 πηγές (14.9%)
- **Επιστημονικά άρθρα:** 19 πηγές (40.4%)
- **Συνέδρια:** 15 πηγές (31.9%)
- **Πανεπιστημιακές εργασίες/Διατριβές:** 6 πηγές (12.8%)

Ποσοτική Ανάλυση ανά κατηγορία πηγών



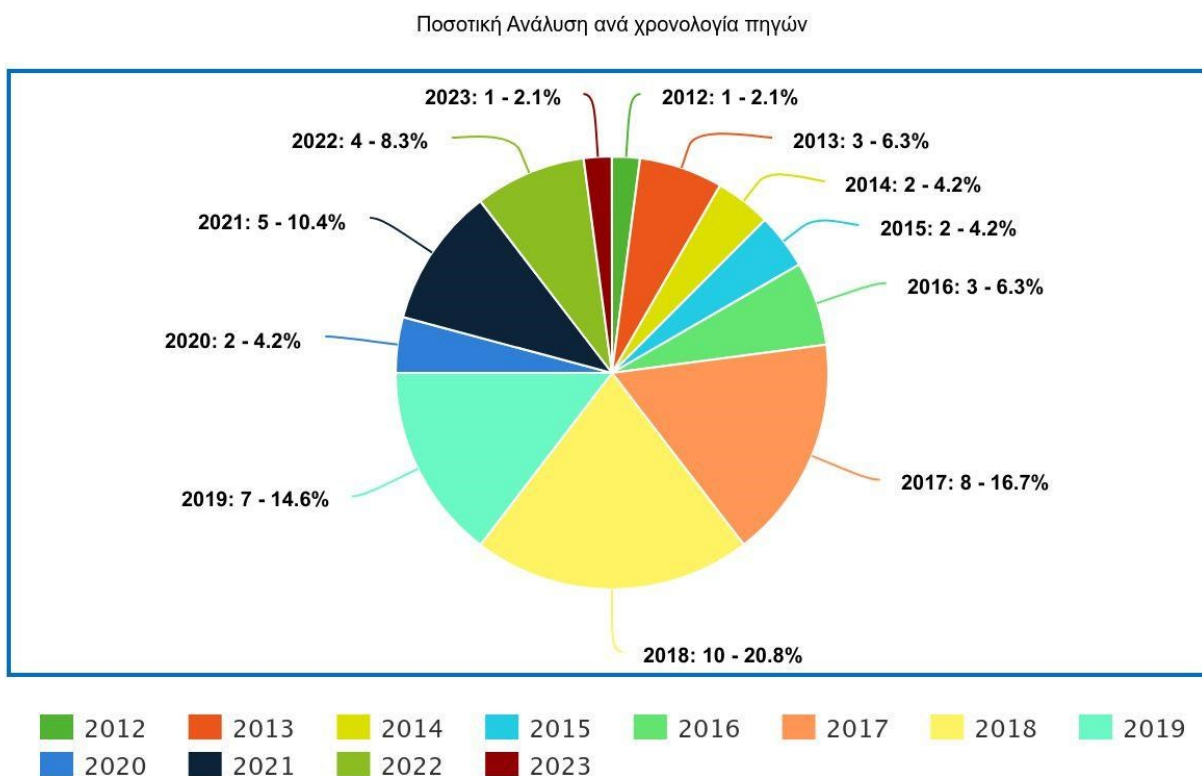
meta-chart.com

Εικόνα 1. Ποσοτική ανάλυση ανα είδος δημοσίευσης

Η πλειοψηφία των πηγών (περίπου 40.4%) είναι επιστημονικά άρθρα, γεγονός που υποδεικνύει την εκτεταμένη ακαδημαϊκή έρευνα και το ενδιαφέρον για την τεχνολογία blockchain και το cloud computing. Οι υπόλοιπες κατηγορίες πηγών προσφέρουν επίσης σημαντικές γνώσεις, αλλά σε μικρότερη έκταση.

3.5.2. Ανά χρονολογία δημοσίευσης

- **2012:** 1 πηγή (2.1%)
- **2013:** 3 πηγές (6.4%)
- **2014:** 2 πηγές (4.3%)
- **2015:** 2 πηγές (4.3%)
- **2016:** 3 πηγές (6.4%)
- **2017:** 8 πηγές (17.0%)
- **2018:** 10 πηγές (21.3%)
- **2019:** 7 πηγές (14.9%)
- **2020:** 2 πηγές (4.3%)
- **2021:** 5 πηγές (10.6%)
- **2022:** 4 πηγές (8.5%)
- **2023:** 1 πηγή (2.1%)



meta-chart.com

Εικόνα 2. Ποσοτική ανάλυση ανά έτος δημοσίευσης

Από την ανάλυση παρατηρούμε ότι το μεγαλύτερο μέρος της βιβλιογραφίας συγκεντρώνεται στα έτη 2017 και 2018, γεγονός που υποδηλώνει αυξημένο ενδιαφέρον και έρευνα στον τομέα της τεχνολογίας blockchain κατά τη διάρκεια αυτών των ετών. Η εργασία μας όμως βασίστηκε πολύ σε πηγές και δημοσιεύσεις, οι οποίες προήλθαν από το 2019 και έπειτα.

4. Συνεισφορά του blockchain στο cloud computing

4.1. Τομείς του υπολογιστικού νέφους που επηρεάζονται από το blockchain

Το υπολογιστικό νέφος αποτελεί έναν από τους κύριους συμπληρωματικούς τεχνολογικούς παράγοντες που υποστηρίζουν τη δημιουργία και λειτουργία των blockchains. Σε αυτό το σημείο θα εξετάσουμε τους βασικούς τομείς του Cloud computing που έχουν υποστεί σημαντικές μεταστροφές ως αποτέλεσμα της ένταξης σε αυτούς της τεχνολογίας του Blockchain. Ειδικότερα, η "Ασφάλεια", "Ιδιωτικότητα" και "Αποθήκευση" είναι τομείς του Cloud computing στους οποίους έχουν παρατηρηθεί πολλές προηγμένες εξελίξεις μετά την ενσωμάτωση σε αυτούς της τεχνολογίας του Blockchain.

4.1.1. Κύριες περιοχές επιρροής

Διαφάνεια και Αξιοπιστία: Η ενσωμάτωση του Blockchain στην αποθήκευση δεδομένων στο Cloud επιφέρει ουσιαστικές αλλαγές στον τρόπο που διαχειριζόμαστε την ασφάλεια και την ιδιωτικότητα των πληροφοριών. Μια σημαντική πτυχή είναι η διαφάνεια και η ακεραιότητα των δεδομένων που παρέχει το Blockchain. Συγκεκριμένα, μέσω της τεχνολογίας Blockchain, οι αλλαγές που γίνονται στα δεδομένα αποθηκεύονται σε ένα δημόσιο βιβλίο (ledger), το οποίο καταγράφει κάθε μεταβολή, από τη δημιουργία ή εισαγωγή τους έως την τροποποίηση και τη διαγραφή τους. Αυτό επιτρέπει στους χρήστες να αποκτήσουν πλήρη διαφάνεια και έλεγχο επί των δεδομένων τους, καθώς μπορούν να ανιχνεύσουν αναλυτικά τις αλλαγές που έχουν γίνει σε αυτά κάθε στιγμή. Αυτό τους δίνει τη δυνατότητα να επαληθεύουν την ακεραιότητα των δεδομένων τους και την αυθεντικότητα της προέλευσής τους. Η επιδεκτική καταγραφή των αλλαγών στα δεδομένα παρέχει ένα ισχυρό μέσο για την ανίχνευση οποιασδήποτε ανωμαλίας ή παραβίασης, καθώς οι μεταβολές που συμβαίνουν στο σύστημα αποθήκευσης δεδομένων καταγράφονται αναλυτικά και ανεπανόρθωτα. Αυτό σημαίνει ότι οι χρήστες μπορούν να ανιχνεύουν πιθανά προβλήματα ή παραβιάσεις και να λαμβάνουν άμεσα μέτρα για την αντιμετώπισή τους, προστατεύοντας έτσι την ασφάλεια και την εμπιστοσύνη στα δεδομένα που αποθηκεύονται στο Cloud.

Έλεγχος Πρόσβασης: Το Blockchain επιτρέπει τη δημιουργία ακριβών και ευέλικτων μηχανισμών ελέγχου πρόσβασης στα δεδομένα στο περιβάλλον του Cloud. Κάθε χρήστης ή οντότητα μπορεί να ορίσει λεπτομερώς ποιος έχει πρόσβαση σε ποια δεδομένα που του ανήκουν και υπό ποιες συνθήκες. Αυτό σημαίνει ότι οι πολιτικές πρόσβασης μπορούν να προσαρμοστούν σε κάθε περίπτωση, λαμβάνοντας υπόψη τις ανάγκες και τις προτεραιότητες κάθε οντότητας. Κάθε αίτημα πρόσβασης ή αλλαγής στα δεδομένα καταγράφεται στο Blockchain, δημιουργώντας ένα ισχυρό ιστορικό ελέγχου και πρόσβασης. Αυτό το ιστορικό είναι προσβάσιμο και αναγνώσιμο

από κάθε αρμόδιο χρήστη ή οντότητα, επιτρέποντάς τους να εξετάσουν ποιος είχε πρόσβαση σε ποια δεδομένα και πότε. Αυτό δημιουργεί ένα ισχυρό σύστημα ελέγχου και αναφοράς για τη διαχείριση των προσβάσεων στα δεδομένα στο περιβάλλον του Cloud, ενισχύοντας την ασφάλεια και τη διαφάνεια του συστήματος.

Η ευελιξία των μηχανισμών ελέγχου πρόσβασης στα δεδομένα μέσω του Blockchain απορρέει από τη δυνατότητα προσαρμογής των πολιτικών πρόσβασης σε κάθε περίπτωση. Κάθε χρήστης μπορεί να ορίσει λεπτομερώς ποιοι έχουν πρόσβαση σε ποια δεδομένα, υπό ποιες συνθήκες και για πόσο χρονικό διάστημα. Αυτό επιτρέπει την προσαρμογή των δικαιωμάτων πρόσβασης ανάλογα με τις ανάγκες και τις προτεραιότητες κάθε οντότητας, προσφέροντας έτσι ευελιξία στην ανταπόκριση σε διαφορετικά σενάρια πρόσβασης. Το σύστημα καταγράφει και αποθηκεύει κάθε αίτημα πρόσβασης ή αλλαγής στα δεδομένα στο Blockchain. Αυτό δημιουργεί ένα ισχυρό ιστορικό ελέγχου και πρόσβασης το οποίο είναι προσβάσιμο και αναγνώσιμο από αρμόδιους χρήστες. Μέσω αυτού του ιστορικού, είναι δυνατό να εξεταστεί ποιος είχε πρόσβαση σε ποια δεδομένα και πότε, ενισχύοντας έτσι τη διαφάνεια και την ασφάλεια του συστήματος.

Ασφάλεια Δεδομένων: Το blockchain παρέχει έναν μηχανισμό κρυπτογράφησης που εξασφαλίζει την ακεραιότητα και την αμετακλητότητα των δεδομένων. Το καθιστά δυσκολότερο για τους επιτιθέμενους να παραβιάσουν ή να αλλοιώσουν δεδομένα. Η αναλυτική καταγραφή και παρακολούθηση των προσβάσεων στα δεδομένα, σε συνδυασμό με την αδιάλειπτη επαλήθευση της αυθεντικότητας των δεδομένων, ενισχύει το επίπεδο προστασίας και ασφάλειας των πληροφοριών των χρηστών.

Αυξημένη Αποδοτικότητα και Μείωση Κόστους: Χάρη στα έξυπνα συμβόλαια (smart contracts), το blockchain μπορεί να αυτοματοποιήσει διαδικασίες και να μειώσει τις ανάγκες για μεσάζοντες, μειώνοντας τα λειτουργικά κόστη και βελτιώνοντας την ταχύτητα των υπηρεσιών.

4.1.2. Εφαρμογές και περιπτώσεις χρήσης

Η τεχνολογία blockchain βρίσκει εφαρμογή σε διάφορους τομείς του cloud computing, όπως:

Αποθήκευση Δεδομένων: Η ασφάλεια και η αμετακλητότητα του blockchain καθιστούν την τεχνολογία ιδανική για ασφαλείς και διαφανείς αποθηκευτικές λύσεις στο cloud. Τα δεδομένα αποθηκεύονται σε μπλοκ, με κάθε μπλοκ να συνδέεται κρυπτογραφημένα με το προηγούμενο, δημιουργώντας μια αλυσίδα που δύσκολα αλλοιώνεται.

Συστήματα Ταυτότητας και Πιστοποίησης: Το blockchain μπορεί να υποστηρίξει τη δημιουργία ασφαλών και επαληθεύσιμων συστημάτων ταυτότητας που χρησιμοποιούνται για τη διαχείριση ταυτοτήτων χρηστών και πιστοποιήσεων σε περιβάλλοντα cloud. Παρέχει μια αποκεντρωμένη υποδομή για τη διαχείριση ταυτοτήτων και πιστοποιήσεων με έμφαση στην ασφάλεια και την επαληθεύσιμη διαχείριση των δεδομένων. Οι ταυτότητες αποθηκεύονται κρυπτογραφημένες σε διανεμημένους κόμβους αντί για κεντρικό διακομιστή, εξασφαλίζοντας την προστασία από μη εξουσιοδοτημένη πρόσβαση και αλλοίωση.

Διαχείριση Συμβολαίων με Smart Contracts: Τα smart contracts επιτρέπουν την αυτόματη εκτέλεση συμβολαίων και τη διαχείριση συμφωνιών σε περιβάλλοντα cloud, χωρίς την ανάγκη για ενδιάμεσους, μειώνοντας το κόστος και τον χρόνο εκτέλεσης. Οι ενέργειες όπως η εγγραφή νέων ταυτοτήτων και η ανανέωση πιστοποιήσεων καταγράφονται διαφανώς και αναστρέψιμα στο blockchain, παρέχοντας αξιόπιστες αποδείξεις της αυθεντικότητας των δεδομένων και της διαδικασίας. Οι ψηφιακές υπογραφές χρησιμοποιούνται για την επαλήθευση της ταυτότητας, ενώ οι χρήστες διαχειρίζονται διακριτικά τις πληροφορίες τους, επιτρέποντας τους να μοιράζονται ή να ανανεώνουν τις πιστοποιήσεις τους με ευκολία.

Ενίσχυση της Ασφάλειας στο IoT: Με την αυξανόμενη υιοθέτηση του Internet of Things (IoT), το blockchain μπορεί να ενσωματωθεί για να εξασφαλίσει τα δεδομένα που παράγονται από διάφορες συσκευές IoT, διασφαλίζοντας την ασφάλεια και την ακεραιότητά τους μέσω αποκεντρωμένης αποθήκευσης σε edge ή fog περιβάλλοντα. Στα περιβάλλοντα edge και fog computing, ο έλεγχος πρόσβασης είναι ένα σημαντικό ζήτημα για την ασφάλεια των δεδομένων που παράγονται από συσκευές IoT και αποθηκεύονται σε αυτά τα περιβάλλοντα. Αν και το blockchain μπορεί να προσφέρει αποκεντρωμένη αποθήκευση και ασφάλεια δεδομένων, ο έλεγχος πρόσβασης στο περιβάλλον edge και fog απαιτεί προσεκτική διαχείριση.

Οι συσκευές IoT στα περιβάλλοντα edge και fog συχνά εκτελούν επεξεργασία και αποθήκευση δεδομένων τοπικά ή σε κοντινές τοποθεσίες (edge nodes, fog nodes) για να μειώσουν την καθυστέρηση και το εύρος ζώνης για την επικοινωνία με το κεντρικό νέφος (cloud). Αυτό επιφέρει την ανάγκη για μηχανισμούς ελέγχου πρόσβασης που είναι ικανοί να λειτουργούν σε αυτά τα αποκεντρωμένα περιβάλλοντα. Το blockchain μπορεί να συμβάλλει στην ενίσχυση της ασφάλειας στο IoT καταγράφοντας δεδομένα και διασφαλίζοντας την ακεραιότητά τους. Ωστόσο, ο έλεγχος πρόσβασης πρέπει να υλοποιηθεί σε κάθε σημείο του περιβάλλοντος edge και fog, χρησιμοποιώντας κατάλληλους μηχανισμούς διαχείρισης ταυτοποίησης και πρόσβασης (π.χ. κλειδιά, πιστοποιητικά). Αυτό εξασφαλίζει ότι μόνο εξουσιοδοτημένα πρόσωπα και συσκευές έχουν πρόσβαση σε ευαίσθητα δεδομένα, ενώ παράλληλα η αξιόπιστη αποθήκευση των δεδομένων στο blockchain προσφέρει επιπλέον επίπεδο ασφάλειας και εμπιστοσύνης.

Παροχή Ανθεκτικότητας σε Αποτυχίες: Η διασπορά των δεδομένων σε πολλούς κόμβους του blockchain πολλαπλών blockchain εξασφαλίζει τη συνεχή λειτουργία των υπηρεσιών, ακόμη και όταν ορισμένοι κόμβοι αντιμετωπίζουν προβλήματα ή είναι offline.

4.2. Τομείς Εφαρμογών του blockchain στο υπολογιστικό νέφος

Το Cloud computing έχει καθιερωθεί ως ένα από τα κυρίαρχα μοντέλα υπολογισμού για αρκετά χρόνια πλέον, ενώ παρατηρείται μια σημαντική αύξηση του αριθμού των επιχειρήσεων που επιλέγουν να μεταφέρουν τις λειτουργίες τους στον κόσμο του Cloud. Αυτή η μετάβαση οφείλεται σε πολλούς παράγοντες, όπως η ευκολία πρόσβασης σε πόρους, η ελκυστική

τιμολόγηση, και ο ανταγωνισμός μεταξύ των παρόχων που οδηγεί σε καλύτερες Cloud υπηρεσίες. Πέραν αυτού, το Cloud έχει εξελιχθεί σε ένα γενικότερο μοντέλο υπολογισμού που υποστηρίζει και ενισχύει άλλες νέες τεχνολογίες. Σε αυτό το πλαίσιο, η τεχνολογία Blockchain έχει κεντρίσει το ενδιαφέρον τόσο των ερευνητών όσο και των επαγγελματιών του χώρου. Η δυνατότητά της να προσφέρει ασφαλείς και αυτόματες συναλλαγές έχει ενθαρρύνει την ενσωμάτωσή της στο περιβάλλον του Cloud computing, προκειμένου να δημιουργηθούν ακόμη πιο αξιόπιστες και ευέλικτες εφαρμογές. Ακολουθούν πέντε τομείς εφαρμογών όπου η συνύπαρξη της τεχνολογίας Blockchain με το Cloud έχει ιδιαίτερο ενδιαφέρον και δυναμική: Μεταφορές, Υγεία, Γεωργία, Έξυπνες Πόλεις και Αλυσίδα Εφοδιασμού .

4.2.1. Μεταφορές

Η ενσωμάτωση της τεχνολογίας blockchain σε ένα περιβάλλον cloud στον τομέα των μεταφορών ανοίγει τον δρόμο για μια νέα εποχή ασφαλούς, αποτελεσματικής και διαφανούς διαχείρισης των δεδομένων και των διαδικασιών στον κλάδο. Η αποκεντρωμένη φύση της τεχνολογίας blockchain συνδυάζεται με την ευελιξία και την ισχύ του cloud computing για να δημιουργήσει ένα ολοκληρωμένο περιβάλλον όπου οι δεδομένες αξίες και οι εφαρμογές μπορούν να λειτουργούν αποτελεσματικά. Η χρήση της πλατφόρμας blockchain στον τομέα των μεταφορών μπορεί να οδηγήσει σε ένα ασφαλές και διαφανές σύστημα διαχείρισης δεδομένων. Αυτό θα επιτρέψει τη δημιουργία ενός κοινού αποθετηρίου πληροφοριών που μπορεί να χρησιμοποιηθεί από διάφορους φορείς μεταφορών και αρμόδιους φορείς. Στο πλαίσιο αυτό, η πλατφόρμα μπορεί να καταγράφει και να διαχειρίζεται δεδομένα σχετικά με την κυκλοφορία, τη συντήρηση οχημάτων, τις άδειες οδήγησης και άλλες πτυχές των μεταφορών. Μέσω του blockchain, αυτά τα δεδομένα είναι προστατευμένα από αλλοίωση ή απώλεια και επιτρέπουν στους ενδιαφερόμενους να έχουν πρόσβαση σε αξιόπιστες και επαληθεύσιμες πληροφορίες. Αυτό μπορεί να συμβάλλει στην αύξηση της ασφάλειας και της αποτελεσματικότητας των μεταφορικών συστημάτων, καθώς και στη βελτίωση της εμπειρίας των χρηστών. [17] [18]

4.2.2. Υγεία

Η εφαρμογή του blockchain σε συνδυασμό με το cloud computing στον τομέα της υγείας μπορεί να έχει ευρείες επιδράσεις σε πολλούς τομείς της υγείας και της ιατρικής περίθαλψης. Ένας από τους βασικούς τομείς όπου το blockchain μπορεί να διαμορφώσει τον τρόπο λειτουργίας είναι η διαχείριση των ιατρικών αρχείων. Η τεχνολογία του blockchain επιτρέπει τη δημιουργία ενός ασφαλούς και πλήρους ψηφιακού αρχείου υγείας για κάθε ασθενή, το οποίο μπορεί να περιλαμβάνει όλα τα ιατρικά του δεδομένα, ιατρικές αναφορές, αποτελέσματα εξετάσεων, και άλλες σημαντικές πληροφορίες που αφορούν την υγεία του. Αυτό το αρχείο μπορεί να μοιραστεί ασφαλώς και με ευκολία μεταξύ γιατρών, νοσοκομείων, και άλλων εμπειρογνομόνων υγείας, πάντα με τη συναίνεση του ασθενή, επιτρέποντας την άμεση πρόσβαση στις απαραίτητες πληροφορίες για την παροχή καλύτερης ιατρικής περίθαλψης. Επιπλέον, το cloud computing παρέχει την υποδομή για την αποθήκευση και τη διαχείριση των ιατρικών δεδομένων σε κλιμακούμενη βάση. Ακόμη, παρέχει υπηρεσίες αντιγράφων ασφαλείας

και αυτόματης ανάκτησης δεδομένων, βελτιώνοντας έτσι τη διαθεσιμότητα και την ασφάλεια των ιατρικών πληροφοριών.

Από την άλλη μεριά, το blockchain μπορεί να εφαρμοστεί στην επεξεργασία αξιώσεων ασφαλιστικών εταιρειών. Η τεχνολογία αυτή επιτρέπει την ασφαλή και διαφανή διαχείριση των αιτήσεων από τη συλλογή δεδομένων έως την αποζημίωση, εξοικονομώντας χρόνο και πόρους για τις ασφαλιστικές εταιρείες και τους ασφαλισμένους. Επίσης, το blockchain μπορεί να βελτιώσει τη διαχείριση της αλυσίδας εφοδιασμού στον τομέα της υγείας. Αυτό συμβάλλει στην ασφάλεια και την ποιότητα των φαρμάκων και των ιατρικών ειδών από την παραγωγή έως την παράδοση στους ασθενείς, ενισχύοντας έτσι την εμπιστοσύνη του κοινού στον τομέα της υγείας.

Συμπερασματικά, μέσω της ενσωμάτωσης του blockchain με το cloud computing, ο τομέας της υγείας μπορεί να απολαμβάνει τα οφέλη της ασφάλειας, της διαφάνειας και της αποτελεσματικότητας σε όλη την αλυσίδα της υγείας, από τη διαχείριση των δεδομένων έως την παροχή υπηρεσιών περίθαλψης και τη διαχείριση του εφοδιασμού. [17] [18]

4.2.3. Γεωργία

Στο γεωργικό τομέα η εφαρμογή της τεχνολογίας ανοίγει νέους ορίζοντες για τους αγρότες και τους επιχειρηματίες στον κλάδο της γεωργίας. Ένας από τους βασικούς τρόπους ενίσχυσης του γεωργικού τομέα είναι με την απλοποίηση της διαδικασίας εμπορίας των προϊόντων. Μέσω της τεχνολογίας blockchain, οι αγρότες μπορούν να προσφέρουν τα προϊόντα τους σε εμπορικές πλατφόρμες που λειτουργούν με έξυπνα συμβόλαια, τα οποία επιτρέπουν την απευθείας πώληση σε τελικούς καταναλωτές ή σε άλλες επιχειρήσεις.

Η διαφάνεια και η ασφάλεια που παρέχει το blockchain επίσης ενισχύουν την εμπιστοσύνη στην αλυσίδα εφοδιασμού των γεωργικών προϊόντων. Με τη χρήση blockchain, οι αγρότες μπορούν να καταγράψουν κάθε στάδιο της παραγωγής και της διανομής των προϊόντων, από τη σπορά μέχρι την παράδοση, παρέχοντας ένα ακριβές ιστορικό και προέλευση για κάθε προϊόν.

Ακόμη η εφαρμογή της τεχνολογίας blockchain μπορεί να επιτρέψει τη δημιουργία νέων μοντέλων επιχειρηματικότητας στον γεωργικό τομέα. Αυτά μπορεί να περιλαμβάνουν τη δυνατότητα για μικρούς αγρότες να συμμετέχουν σε παγκόσμιες αγορές, ή τη δυνατότητα για επενδυτές να χρηματοδοτήσουν απευθείας αγροτικά έργα μέσω του blockchain.

Από την μεριά του το cloud computing παρέχει την υποδομή για την αποθήκευση και την επεξεργασία μεγάλων όγκων δεδομένων που παράγονται από τη χρήση του blockchain. Η αποθήκευση των δεδομένων στο cloud επιτρέπει την ασφαλή και αποτελεσματική πρόσβαση σε αυτά από οποιαδήποτε θέση και οποιαδήποτε συσκευή με σύνδεση στο διαδίκτυο. Επιπλέον, το cloud computing παρέχει επεκτασιμότητα και ευελιξία, επιτρέποντας στις εφαρμογές του blockchain να αντιμετωπίσουν τις αυξανόμενες απαιτήσεις του όγκου των δεδομένων. Με αυτόν τον τρόπο, η συνδυασμένη χρήση των τεχνολογιών αυτών ενισχύει την απόδοση και την αποτελεσματικότητα στον γεωργικό τομέα. [17] [18]

4.2.4. Έξυπνες Πόλεις

Με την εμφάνιση του Cloud computing και του Διαδικτύου των Πραγμάτων (IoT), η υποδομή που υποστηρίζει τη δημιουργία έξυπνων πόλεων βρίσκεται σε ανοδική πορεία. Το Cloud computing επιτρέπει την αποθήκευση, επεξεργασία και διαχείριση δεδομένων και εφαρμογών μέσω του Διαδικτύου, παρέχοντας στις έξυπνες πόλεις τη δυνατότητα να αξιοποιήσουν την υπολογιστική ισχύ και την αποθήκευση δεδομένων με αποτελεσματικό τρόπο.

Επιπλέον, το Blockchain, ως σχετικά νέα τεχνολογία, επιδιώκει να προωθήσει εφαρμογές που εστιάζουν στον πολίτη εντός του πλαισίου μιας έξυπνης πόλης. Η συνδυασμένη χρήση του Blockchain με το IoT, την Τεχνητή Νοημοσύνη (AI) και το Cloud computing επιτρέπει την αυτόνομη λειτουργία μιας ολόκληρης έξυπνης πόλης. Μέσω του Blockchain, διευκολύνεται η αξιόπιστη και διαφανής ανταλλαγή πληροφοριών μεταξύ των συσκευών IoT, ενώ υπάρχουν πολλοί τομείς εφαρμογής για την ενσωμάτωση του Blockchain σε έξυπνες πόλεις, όπως οι πλατφόρμες εμπορίας και διανομής ενέργειας, τα συστήματα διαχείρισης κυκλοφορίας, τα έξυπνα σπίτια και οι εφαρμογές IoT.

Τέλος, το Blockchain έχει το δυναμικό να ανασχεδιάσει την ηλεκτρονική διακυβέρνηση στις έξυπνες πόλεις, ενισχύοντας τη συμμετοχή των πολιτών και τη διαμόρφωση κυβερνητικών προγραμμάτων, ενώ μέσω διαφανών και αμετάβλητων καταγραφών δημιουργεί εμπιστοσύνη μεταξύ πολιτών και κυβερνητικών οργάνων. [17] [18]

4.2.5. Αλυσίδες Εφοδιασμού

Το ουσιαστικό όφελος του blockchain και του Cloud computing στη διαχείριση αλυσίδας εφοδιασμού είναι η διαφάνεια και η ασφάλεια των δεδομένων. Με τη χρήση του blockchain, οι πληροφορίες που σχετίζονται με κάθε στάδιο της αλυσίδας εφοδιασμού μπορούν να καταγράφονται με ασφάλεια και να επιβεβαιώνονται, ενώ παράλληλα διατηρείται η ακεραιότητά τους. Αυτό είναι σημαντικό για τη διαχείριση της ποιότητας, την παρακολούθηση της παραγωγής και την αποτροπή απάτης ή ανεπιθύμητων ενεργειών στην αλυσίδα εφοδιασμού.

Επιπλέον, η αποκεντρωμένη φύση του blockchain επιτρέπει τη συνεχή ροή πληροφοριών σε ολόκληρη την αλυσίδα εφοδιασμού, βοηθώντας στην αποτελεσματική κοινοποίηση πληροφοριών μεταξύ όλων των ενδιαφερομένων μερών. Αυτό συμβάλλει στην αποτελεσματικότερη διαχείριση της αλυσίδας εφοδιασμού και στην ενίσχυση της εμπιστοσύνης μεταξύ των συνεργατών.

Το cloud computing από τη μεριά του μπορεί να συμπληρώνει την υποδομή του blockchain, προσφέροντας ευελιξία και αποθηκευτικό χώρο για τα δεδομένα που διαχειρίζεται η αλυσίδα εφοδιασμού. Η συνδυασμένη χρήση των δύο αυτών τεχνολογιών μπορεί να ενισχύσει την αποτελεσματικότητα των διαδικασιών της διαχείρισης αλυσίδας εφοδιασμού και να αποτελέσει ένα ισχυρό εργαλείο για τη μοντερνοποίηση των πρακτικών και τη διατήρηση του ανταγωνιστικού πλεονεκτήματος των επιχειρήσεων. [17] [18]

4.3. Οφέλη του blockchain στο cloud computing

Το blockchain φέρνει μια νέα διάσταση στον τομέα του υπολογιστικού νέφους, προσφέροντας πλεονεκτήματα που ενισχύουν την ασφάλεια, την ακεραιότητα και την αποτελεσματικότητα της διαχείρισης των δεδομένων. Η προσθήκη του blockchain στον τομέα του cloud computing δίνει τη δυνατότητα για μια πιο ασφαλή και αξιόπιστη διαχείριση των πληροφοριών, ενισχύοντας την εμπιστοσύνη των χρηστών στον ψηφιακό χώρο. Η ασφάλεια των δεδομένων αποτελεί ένα καίριο ζήτημα στον χώρο του υπολογιστικού νέφους όπου μεγάλος όγκος πληροφοριών μεταφέρεται και αποθηκεύεται.

- Η προσθήκη του blockchain στο cloud computing παρέχει μια επιπλέον στρώση ασφάλειας, ενισχύοντας την προστασία των δεδομένων και αντιμετωπίζοντας τις ανησυχίες σχετικά με την ιδιωτικότητα και την ακεραιότητα των πληροφοριών. Το blockchain είναι γνωστό για τη δυνατότητά του να προσφέρει ασφαλή αποθήκευση δεδομένων με τη χρήση κρυπτογραφίας και αντιμετωπίζει την πρόκληση της εμπιστευτικότητας σε περιβάλλοντα cloud. Με τη χρήση του blockchain, τα δεδομένα μπορούν να αποθηκευτούν με ασφάλεια και να προστατευτούν από ανεπιθύμητες παρεμβάσεις, παρέχοντας έτσι ένα ακόμα υψηλότερο επίπεδο ασφάλειας στα δεδομένα των χρηστών.
- Η αποκεντρωμένη δομή της τεχνολογίας blockchain αναδεικνύεται ως ένα από τα βασικά πλεονεκτήματά της σε σχέση με τον τομέα του cloud computing. Στον κόσμο του υπολογιστικού νέφους, οι χρήστες εμπιστεύονται την αποθήκευση και την επεξεργασία των δεδομένων τους σε κεντρικούς διακομιστές, πρακτική που μπορεί να αποτελέσει σημαντικό κίνδυνο για την ασφάλεια και την ακεραιότητα των δεδομένων. Η κεντρική αποθήκευση είναι επιρρεπής σε διάφορες απειλές, όπως επιθέσεις από κακόβουλους χρήστες ή κακόβουλο λογισμικό, και μπορεί να οδηγήσει σε απώλεια ή παραβίαση των δεδομένων. Η ενσωμάτωση του blockchain στο υπολογιστικό νέφος προσφέρει μια εναλλακτική λύση που αντιμετωπίζει αυτούς τους κινδύνους. Στο πλαίσιο του blockchain, τα δεδομένα αποθηκεύονται σε ένα αποκεντρωμένο δίκτυο κόμβων, όπου κάθε κόμβος διατηρεί ένα αντίγραφο των δεδομένων. Αυτό σημαίνει ότι η πληροφορία δεν αποθηκεύεται σε έναν μόνο κεντρικό διακομιστή, αλλά αντίθετα αναπαρίσταται σε ένα δίκτυο κόμβων που συνεργάζονται για την επικύρωση και τη διατήρηση των δεδομένων. Επιπλέον, η κρυπτογραφική ασφάλεια και η αποκέντρωση της επικοινωνίας μεταξύ των κόμβων ενισχύουν την εμπιστευτικότητα των δεδομένων σε ένα τέτοιο περιβάλλον. Με αυτόν τον τρόπο, η τεχνολογία blockchain συνδυάζεται αποτελεσματικά με το υπολογιστικό νέφος προσφέροντας ασφαλείς και ανθεκτικές υπηρεσίες αποθήκευσης και επεξεργασίας δεδομένων, ακόμα και σε περιβάλλοντα με υψηλές απαιτήσεις σε ασφάλεια και διαθεσιμότητα.

- Η τεχνολογία blockchain επιτρέπει τη δημιουργία ανθεκτικών συστημάτων με την αντιγραφή και αποθήκευση δεδομένων σε διάφορους κόμβους του δικτύου. Αυτό διασφαλίζει ότι η απώλεια ή η αποτυχία ενός κόμβου δεν θα οδηγήσει στην απώλεια δεδομένων ή τη διακοπή των υπηρεσιών. Η αποκεντρωμένη δομή του blockchain επίσης εξασφαλίζει την ανθεκτικότητα σε επιθέσεις και αποτυχίες, καθώς η απώλεια ή η παραβίαση των δεδομένων σε έναν μόνο κόμβο δεν επηρεάζει τη συνολική ακεραιότητα του συστήματος. Ακόμη πιο σημαντικό, η διασπορά των δεδομένων σε πολλούς κόμβους εξαλείφει τον κεντρικό σημείο αποτυχίας και εξασφαλίζει τη συνεχή λειτουργία του συστήματος ακόμα και σε περιπτώσεις προβλημάτων σε μεμονωμένους κόμβους. Με την επέκταση της τεχνολογίας blockchain, η συνδυασμένη χρήση της με το υπολογιστικό νέφος έχει ενισχύσει ακόμα περισσότερο τα πλεονεκτήματά της. Η αποθήκευση δεδομένων σε διάφορους εξυπηρετητές του νέφους επιτρέπει την επίτευξη ανθεκτικών συστημάτων, με τη δυνατότητα συνεχούς λειτουργίας ακόμα και σε περιπτώσεις αποτυχίας ενός εξυπηρετητή.
- Η συνδυασμένη χρήση της τεχνολογίας blockchain και του cloud computing προσφέρει οικονομικά οφέλη μέσω της αποθήκευσης δεδομένων στο νέφος. Αυτό επιτρέπει στις επιχειρήσεις να μειώσουν το κόστος υποδομής, καθώς δεν απαιτείται η αγορά και η συντήρηση δικών τους φυσικών υποδομών. Επιπλέον, η εκμετάλλευση των δυνατοτήτων της τεχνολογίας blockchain μπορεί να μειώσει το κόστος διαχείρισης και επεξεργασίας δεδομένων. Αυτό συμβαίνει λόγω της αυτόματης επιβεβαίωσης και της ασφαλούς αποθήκευσης δεδομένων που προσφέρει η τεχνολογία blockchain, εξοικονομώντας έτσι χρόνο και πόρους στις επιχειρήσεις.
- Τέλος, η ενσωμάτωση της τεχνολογίας blockchain με το cloud computing ανοίγει νέους ορίζοντες στον χώρο της καινοτομίας και της ανάπτυξης λύσεων. Με τη συνεχή εξέλιξη και τη συνεργασία αυτών των τεχνολογιών, επιχειρήσεις και κοινότητες μπορούν να δημιουργήσουν καινοτόμες εφαρμογές και υπηρεσίες που μπορούν να αναδιαμορφώσουν τον τρόπο λειτουργίας των κοινωνιών και των οργανισμών. Ταυτόχρονα, η συνεργασία αυτή ενισχύει την ανταγωνιστικότητα των επιχειρήσεων, προσφέροντας νέες δυνατότητες παροχής υπηρεσιών και προϊόντων. Συνολικά, η συνένωση αυτών των τεχνολογιών ανοίγει νέες προοπτικές για την ανάπτυξη καινοτόμων λύσεων που μπορούν να διαμορφώσουν τον ψηφιακό κόσμο του μέλλοντος.

4.4. Μηχανισμός ασφαλούς αποθήκευσης δεδομένων βάσει blockchain και κώδικα

Ο ρόλος του blockchain στην ασφαλή αποθήκευση δεδομένων σε περιβάλλοντα edge computing, το οποίο θεωρείται ως επέκταση του cloud computing, εξετάζεται μέσω της δημιουργίας ενός αποκεντρωμένου, ανθεκτικού στις τροποποιήσεις και διαφανούς μηχανισμού αποθήκευσης [30]. Η υλοποίηση αυτού του μηχανισμού περιλαμβάνει τη χρήση δύο επιπέδων blockchain: ένα παγκόσμιο και ένα τοπικό, καθώς και την ενσωμάτωση της τεχνολογίας αναγεννητικών κωδίκων (regenerating codes) για τη βελτίωση της αξιοπιστίας και τη μείωση της κατανάλωσης εύρους ζώνης κατά την επιδιόρθωση δεδομένων.

4.4.1. Παγκόσμιο Blockchain

Το παγκόσμιο blockchain λειτουργεί σε επίπεδο υπολογιστικού νέφους και αποθηκεύει δεδομένα με ασφαλή τρόπο, επιτρέποντας την αποθήκευση αντιγράφων των δεδομένων σε πολλαπλούς εξυπηρετητές νέφους (cloud servers). Κάθε κόμβος (εξυπηρετητής) που συμμετέχει στο blockchain διατηρεί ένα αντίγραφο των δεδομένων και χρησιμοποιεί αλγόριθμους συναίνεσης για την επικύρωση και την αποθήκευση νέων δεδομένων. Αυτό εξασφαλίζει τη διαφάνεια και την ανθεκτικότητα στις τροποποιήσεις, καθώς κανένα μέρος δεν μπορεί να τροποποιήσει τα δεδομένα μονομερώς.

4.4.2. Τοπικό Blockchain

Στο επίπεδο των τοπικών δικτύων IoT, το τοπικό blockchain εκτελείται σε συσκευές ή εξυπηρετητές edge και χρησιμοποιείται για τη διαχείριση των δεδομένων που συλλέγονται από τις IoT συσκευές. Τα δεδομένα αυτά κωδικοποιούνται και αποθηκεύονται στο τοπικό blockchain, ενώ τα αρχικά δεδομένα μπορεί να διαγραφούν από τις συσκευές για να ελευθερώσουν χώρο και να συλλέξουν νέα δεδομένα. Αυτή η διαδικασία επιτρέπει την ασφαλή και αποδοτική αποθήκευση δεδομένων σε περιορισμένους πόρους. Στο τοπικό blockchain αποθηκεύονται τα δεδομένα από τις IoT συσκευές για την υποστήριξη τοπικής ανάλυσης κοντά στις συσκευές. Εφόσον τα δεδομένα φιλτραριστούν και απαιτήσουν είτε μόνιμη αποθήκευση είτε πιο ισχυρή ανάλυση, μεταφέρονται στο παγκόσμιο blockchain. Αυτή η προσέγγιση ενισχύει την αποτελεσματικότητα και την αξιοπιστία της αποθήκευσης δεδομένων σε περιβάλλοντα edge computing, διασφαλίζοντας την ταυτόχρονη χρήση τοπικών και παγκόσμιων blockchain για την κάλυψη των αναγκών ανάλυσης και αποθήκευσης.

4.4.3. Αναγεννητικοί Κώδικες

Οι αναγεννητικοί κώδικες αποτελούν μία εξελιγμένη μέθοδο αποθήκευσης και ανάκτησης δεδομένων σε καταναμημένα συστήματα, όπως συστήματα αποθήκευσης δεδομένων σε cloud ή συστήματα αρχείων. Αναλυτικότερα, οι αναγεννητικοί κώδικες λειτουργούν ως εξής:

Τα αρχικά δεδομένα χωρίζονται σε μικρότερα τμήματα. Αυτά τα τμήματα στη συνέχεια κωδικοποιούνται χρησιμοποιώντας έναν αλγόριθμο δημιουργίας πλεονασματικών τμημάτων (parity blocks). Αυτά τα πλεονασματικά τμήματα δημιουργούνται με τέτοιο τρόπο ώστε να μπορούν να χρησιμοποιηθούν για την ανάκτηση των αρχικών δεδομένων ακόμη και αν κάποια από τα αρχικά τμήματα χαθούν ή καταστραφούν.

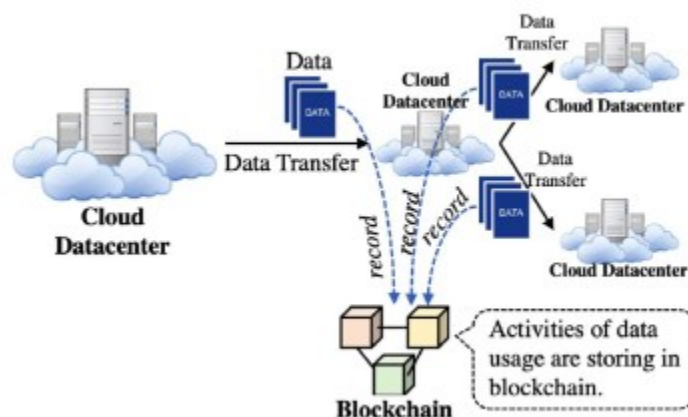
Σε περίπτωση απώλειας δεδομένων από έναν κόμβο, οι αναγεννητικοί κώδικες επιτρέπουν την ανάκτηση των χαμένων δεδομένων από άλλους κόμβους στο δίκτυο. Η ανάκτηση γίνεται χρησιμοποιώντας μόνο ένα υποσύνολο των αρχικών δεδομένων και των πλεονασματικών τμημάτων. Αυτό μειώνει δραστικά την ποσότητα των δεδομένων που πρέπει να μεταδοθούν μεταξύ των κόμβων σε σύγκριση με την κλασική πολλαπλή αποθήκευση, όπου τα ίδια δεδομένα αποθηκεύονται σε πολλαπλούς κόμβους.

Αυτή η διαδικασία όχι μόνο αυξάνει την αξιοπιστία της αποθήκευσης δεδομένων, αλλά επίσης μειώνει την κατανάλωση εύρους ζώνης κατά τις διαδικασίες επιδιόρθωσης. Σε περίπτωση που κάποιος κόμβος αποτύχει, αντί να χρειάζεται να αντιγραφεί ολόκληρος ο όγκος των δεδομένων, μόνο ένα μέρος των δεδομένων και των πλεονασματικών τμημάτων χρειάζεται να μεταδοθεί για την επαναφορά τους. Αυτό καθιστά την όλη διαδικασία πιο αποδοτική και οικονομική όσον αφορά τη χρήση πόρων του δικτύου.

Οι αναγεννητικοί κώδικες χρησιμοποιούνται ευρέως σε συστήματα που απαιτούν υψηλή διαθεσιμότητα και ανθεκτικότητα δεδομένων, όπως αποθηκευτικά συστήματα cloud, κατανεμημένα συστήματα αρχείων και συστήματα RAID. [16]

4.5. Αποδεδειγμένη Προέλευση Δεδομένων (Data Provenance) με Blockchain στο Υπολογιστικό Νέφος

Η IDC (International Data Corporation) προβλέπει ότι ο παγκόσμιος όγκος δεδομένων θα φτάσει τα 175 Ζετταμπάιτ μέχρι το 2025, με το μισό από αυτά τα δεδομένα να αποθηκεύονται σε δημόσια νέφη.[45] Η απόδειξη προέλευσης δεδομένων είναι ουσιαστική για την ιχνηλασιμότητα της χρήσης δεδομένων και συμβάλλει στη διαχείριση τέτοιου μεγάλου όγκου δεδομένων, ενισχύοντας την αποδοτικότητα και την αξιοπιστία. Η προέλευση δεδομένων περιγράφει πότε, πού και πώς τα δεδομένα αποθηκεύονται, προσπελούνται, τροποποιούνται και διαγράφονται, επιτρέποντας στους παρόχους υπηρεσιών να παρέχουν αξιόπιστη διαχείριση δεδομένων. Η εφαρμογή της προέλευσης ευνοεί και τους παρόχους και τους χρήστες, βοηθώντας στην ανακάλυψη ευπαθειών ασφάλειας, την απλοποίηση των διαδικασιών αποσφαλμάτωσης και τον εντοπισμό ασυνήθιστων διεργασιών. Παρά τα οφέλη, τα αρχεία προέλευσης μπορεί να παραβιαστούν, αυξάνοντας την ανάγκη για αξιόπιστες συλλογές προέλευσης για να εγδυθούν την ασφάλεια και την ακεραιότητα των δεδομένων.



Εικόνα 3. Αρχιτεκτονική υψηλού επιπέδου για την ανίχνευση προέλευσης δεδομένων σε κέντρα δεδομένων cloud με τη χρήση blockchain

Το blockchain, ως ανθεκτικό σε παρεμβάσεις κατακεταμμένο μητρώο, εξασφαλίζει την ασφάλεια των δεδομένων προέλευσης μέσω της ιδιότητας της ιχνηλασιμότητας, καταγράφοντας κάθε δραστηριότητα που συμβαίνει στα δεδομένα εντός των μπλοκ. Τα έξυπνα συμβόλαια ενισχύουν αυτή τη δυνατότητα, παρέχοντας ένα αυτοματοποιημένο, αξιόπιστο και λειτουργικό περιβάλλον, ανεξάρτητα από το αν τα δεδομένα αποθηκεύονται εντός ή εκτός αλυσίδας. Ειδικότερα, συστήματα όπως το ProvenChain [34] και το Smart Provenance [35] διαχειρίζονται την προέλευση των δεδομένων στο cloud, με το ProvenChain να καταγράφει δεδομένα σε ιδιωτική αλυσίδα και το Smart Provenance να εισάγει ένα αποκεντρωμένο σύστημα επαλήθευσης μέσω ψηφοφορίας. Τα έξυπνα συμβόλαια αυτοματοποιούν τη διαδικασία και ενισχύουν τη διαφάνεια, ενώ διατηρούν την ιδιωτικότητα με την αποθήκευση ευαίσθητων δεδομένων εκτός αλυσίδας. Τα συστήματα αυτά αντιμετωπίζουν προκλήσεις, όπως η έλλειψη διαλειτουργικότητας σε περιβάλλοντα ομοσπονδιακού cloud (cloud federation), αλλά προσφέρουν σημαντικά οφέλη στην ασφαλή διαχείριση δεδομένων μέσω της αξιοποίησης των δυνατοτήτων του blockchain. [25]

4.6. Έλεγχος Πρόσβασης με Βάση το Blockchain στο Υπολογιστικό Νέφος

Ο έλεγχος πρόσβασης αποτελεί θεμελιώδη μέθοδο για τη διασφάλιση της ασφάλειας και της ιδιωτικότητας των δεδομένων στο cloud, καθώς προστατεύει τα δεδομένα από την παρεμβολή μη εξουσιοδοτημένων χρηστών. Οι μέθοδοι ελέγχου πρόσβασης επηρεάζουν επίσης και άλλες λειτουργίες, όπως την πιστοποίηση, την εξουσιοδότηση και τον έλεγχο δεδομένων. Στο πλαίσιο του cloud, οι παραδοσιακές μέθοδοι ελέγχου πρόσβασης βασίζονται σε εδραιωμένες πολιτικές που χωρίζονται σε τέσσερις κατηγορίες: Διακριτικός Έλεγχος Πρόσβασης (DAC), Υποχρεωτικός Έλεγχος Πρόσβασης (MAC), Έλεγχος Πρόσβασης Βασισμένος σε Ρόλους (RBAC) και Έλεγχος

Πρόσβασης Βασισμένος σε Χαρακτηριστικά (ABAC). Κάθε μέθοδος έχει τα δικά της πλεονεκτήματα και μειονεκτήματα, με την κεντριοποίηση να αποτελεί κοινή αδυναμία που επηρεάζει τη διαφάνεια, την ιχνηλασιμότητα, την ανθεκτικότητα σε παρεμβάσεις και την πολυμερή διακυβέρνηση(multitenancy). Ο συμβιβασμός μεταξύ ασφάλειας και αποδοτικότητας είναι ένα διαρκές ζήτημα στο περιβάλλον του cloud.

Αποκλίνοντας από τις παραδοσιακές μεθόδους ελέγχου πρόσβασης, ο Έλεγχος Πρόσβασης με Βάση το Blockchain (BAC) προσφέρει κάποια οφέλη που πηγάζουν από τις ιδιότητες του blockchain. Ο Έλεγχος Πρόσβασης με Βάση το Blockchain (Blockchain-based Access Control - BAC) είναι μια τεχνολογική προσέγγιση που χρησιμοποιεί το blockchain ως βάση για τη διαχείριση και τον έλεγχο πρόσβασης σε δεδομένα ή υπηρεσίες στο περιβάλλον του cloud. Η κύρια ιδέα είναι να εκμεταλλεύεται τα χαρακτηριστικά του blockchain, όπως η αποκεντρωμένη κατανομημένη αρχιτεκτονική, η ασφάλεια μέσω κρυπτογραφίας και η ιχνηλασιμότητα των εγγραφών, για να προσφέρει ασφαλή και διαφανή διαχείριση πρόσβασης. Με το BAC, κάθε ενέργεια πρόσβασης (όπως η πρόσβαση σε δεδομένα ή η εκτέλεση ενεργειών) καταγράφεται ως μια μοναδική συναλλαγή στο blockchain. Αυτό διασφαλίζει ότι οι διαδικασίες πρόσβασης είναι αποκεντρωμένες και διαφανείς, με κάθε αλλαγή ή εξουσιοδότηση να είναι ορατή σε όλους τους συμμετέχοντες στο δίκτυο blockchain.

Το BAC επιτρέπει επίσης τη χρήση έξυπνων συμβολαίων για την αυτοματοποίηση των διαδικασιών ελέγχου πρόσβασης, ενισχύοντας την ασφάλεια με αυτόματη ανίχνευση και αποκρίνοντας σε παραβάσεις. Αυτή η τεχνολογία έχει τη δυνατότητα να αντιμετωπίσει προκλήσεις που σχετίζονται με την κεντριοποίηση και τη διαφάνεια, κάνοντας τη διαχείριση πρόσβασης στο cloud πιο ασφαλή και αξιόπιστη.

Δύο κύρια πλεονεκτήματα αναδεικνύονται από την τεχνολογία BAC [30]. Πρώτον, το BAC εισάγει την έννοια της συναίνεσης στη λειτουργία του ελέγχου πρόσβασης, επιτρέποντας τη συμμετοχή όλων των ενδιαφερομένων κατά τη διάρκεια της διαδικασίας. Δεύτερον, η ιχνηλασιμότητα που υποστηρίζεται από το blockchain προσφέρει μια ανιχνεύσιμη και αμετάβλητη δυνατότητα διακυβέρνησης για τον έλεγχο πρόσβασης, αυξάνοντας τη δυσκολία παραβίασης για τους αντιπάλους. Το blockchain βοηθά στην αποφυγή του κινδύνου αποτυχίας ενός σημείου και της κακόβουλης χρήσης δεδομένων από τρίτους, επιτρέποντας στους κατόχους δεδομένων να ελέγχουν ευέλικτα και πλήρως την πρόσβαση στα δεδομένα τους. Επιπλέον, η χρήση έξυπνων συμβολαίων προσφέρει αυτοματοποιημένη διαχείριση πρόσβασης καθώς και ανίχνευση και τιμωρία παραβάσεων, ενισχύοντας τον έλεγχο και την ασφάλεια στο cloud.Ωστόσο, η εφαρμογή του blockchain στον έλεγχο πρόσβασης των εικονικών μηχανών (VMs) απαιτεί περαιτέρω μελέτη και θα αποτελέσει μια μελλοντική τάση ερευνών.

Η εφαρμογή του blockchain στον έλεγχο πρόσβασης των εικονικών μηχανών (VMs) στο περιβάλλον του cloud επηρεάζει την ταχύτητα λήψης αποφάσεων και άλλες σημαντικές πτυχές. Η ταχύτητα λήψης αποφάσεων είναι κρίσιμη για την ασφάλεια και την αποδοτικότητα των συστημάτων, καθώς πρέπει να διασφαλίζεται η γρήγορη και αποτελεσματική αντίδραση σε κάθε είδους πρόκληση ή απειλή. Η χρήση blockchain συχνά επιφέρει υπολογιστική πολυπλοκότητα λόγω των αλγορίθμων κρυπτογράφησης και επιβεβαίωσης συναλλαγών. Αυτό μπορεί να επηρεάσει την ταχύτητα με την οποία λαμβάνονται αποφάσεις για τον έλεγχο πρόσβασης στις

εικονικές μηχανές. Η διαχείριση πόρων όπως ο χώρος αποθήκευσης και το δίκτυο επίσης παίζει σημαντικό ρόλο στην απόδοση των VMs, επηρεάζοντας την ταχύτητα λήψης αποφάσεων.

Επιπλέον, η αυτοματοποιημένη διαχείριση πρόσβασης μέσω έξυπνων συμβολαίων μπορεί να ενισχύσει την ασφάλεια και τον έλεγχο, αλλά απαιτεί συχνά πρόσθετη χρονική και υπολογιστική πόρων. Η έρευνα και η ανάπτυξη σε αυτόν τον τομέα συνεχίζονται για να βελτιωθεί η απόδοση και να ενσωματωθεί η τεχνολογία blockchain με ακόμα μεγαλύτερη αποτελεσματικότητα στον έλεγχο πρόσβασης στο cloud. [25]

4.7. Ενεργοποιημένη από Blockchain αναζητήσιμη κρυπτογράφηση στα Νεφη

Η αναζητήσιμη κρυπτογράφηση (searchable encryption) στα cloud αποτελεί μια καινοτόμο τεχνική που επιτρέπει την ασφαλή διαχείριση και αναζήτηση κρυπτογραφημένων δεδομένων, χωρίς να απαιτείται η πλήρης αποκρυπτογράφησή τους. Οι παραδοσιακές προσεγγίσεις αναζητήσιμης κρυπτογράφησης διακρίνονται σε δύο κύριες κατηγορίες: την Αναζητήσιμη Συμμετρική Κρυπτογράφηση (SSE) και την Αναζητήσιμη Κρυπτογράφηση Δημόσιου Κλειδιού (SPKE) (ή αλλιώς Αναζητήσιμη Μη Συμμετρική Κρυπτογράφηση).

Τόσο η Searchable Symmetric Encryption (SSE) όσο και η Searchable Public Key Encryption (SPKE) έχουν την κοινή λειτουργία να επιτρέπουν την αναζήτηση σε κρυπτογραφημένα δεδομένα χωρίς την ανάγκη αποκρυπτογράφησης αυτών των δεδομένων από τον διακομιστή ή το σύστημα που φιλοξενεί τα δεδομένα. Οι κοινές λειτουργίες περιλαμβάνουν:

1. *Κρυπτογράφηση Δεδομένων*: Τα δεδομένα κρυπτογραφούνται πριν αποθηκευτούν στον διακομιστή.
2. *Δημιουργία Δεικτών (Indexes)*: Δημιουργούνται κρυπτογραφημένοι δείκτες για τις λέξεις-κλειδιά που περιέχονται στα δεδομένα, οι οποίοι αποθηκεύονται μαζί με τα κρυπτογραφημένα δεδομένα.
3. *Δημιουργία Ερωτήματος (Query Generation)*: Ο χρήστης δημιουργεί ένα κρυπτογραφημένο ερώτημα με το οποίο επιθυμεί να πραγματοποιήσει αναζήτηση.
4. *Αναζήτηση*: Ο διακομιστής χρησιμοποιεί το κρυπτογραφημένο ερώτημα για να αναζητήσει τους αντίστοιχους κρυπτογραφημένους δείκτες.
5. *Αποκρυπτογράφηση Αποτελεσμάτων*: Ο χρήστης αποκρυπτογραφεί τα αποτελέσματα που επιστρέφει ο διακομιστής χρησιμοποιώντας το κατάλληλο κρυπτογραφικό κλειδί.

Η SSE βασίζεται στην αρχή της συμμετρικής κρυπτογράφησης, όπου ένας αλγόριθμος και ένα μυστικό κλειδί χρησιμοποιούνται τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση των δεδομένων. Η PKE, από την άλλη, χρησιμοποιεί ασύμμετρη κρυπτογράφηση, που σημαίνει ότι διαφορετικά κλειδιά χρησιμοποιούνται για την κρυπτογράφηση και την αποκρυπτογράφηση των δεδομένων. Διαφέρουν επίσης στην ανάγκη εμπιστοσύνης στον διακομιστή και στην αποδοτικότητα των αναζητήσεων. Η SSE είναι πιο αποδοτική υπολογιστικά

αλλά απαιτεί εμπιστοσύνη στον διακομιστή, ενώ η SPKE προσφέρει υψηλότερη ασφάλεια και προστασία της ιδιωτικότητας με το κόστος της αυξημένης υπολογιστικής πολυπλοκότητας.

Ένας από τους περιορισμούς της παραδοσιακής αναζητήσιμης κρυπτογράφησης είναι η ανάγκη για ακριβή ταύτιση, που μπορεί να μειώσει την απόδοση της διαθεσιμότητας. Η ακριβής ταύτιση στην αναζητήσιμη κρυπτογράφηση αναφέρεται στη δυνατότητα να εντοπιστούν και να επιστραφούν ακριβώς τα δεδομένα που αντιστοιχούν στο κριτήριο αναζήτησης, χωρίς να χρειαστεί να αποκρυπτογραφηθούν όλα τα δεδομένα. Η απόδοση της διαθεσιμότητας επηρεάζεται από την ακριβή ταύτιση κυρίως λόγω της αυξημένης υπολογιστικής πολυπλοκότητας που απαιτείται για την εκτέλεση των αναζητήσεων, καθώς και λόγω πιθανών συγκρούσεων αιτημάτων σε περιβάλλοντα πολλαπλών χρηστών. Για να αντιμετωπίσουν αυτό το ζήτημα, μελέτες πρότειναν τη χρήση ασαφούς αναζήτησης (fuzzy search) με λέξεις-κλειδιά, που επιστρέφει αποτελέσματα με την υψηλότερη ομοιότητα.

Η ασαφής αναζήτηση αποτελεί μια σημαντική τεχνική στον τομέα της αναζητήσιμης κρυπτογράφησης στο cloud. Αυτή η τεχνική επιτρέπει στους χρήστες να πραγματοποιούν αναζητήσεις σε κρυπτογραφημένα δεδομένα, χωρίς να απαιτείται η αποκρυπτογράφηση ολόκληρου του περιεχομένου. Αντίθετα, γίνεται δυνατή η εύρεση δεδομένων που έχουν ομοιότητα με την αναζητούμενη λέξη-κλειδί, αλλά χωρίς την ακριβή ταύτιση. Σε αντίθεση με τις παραδοσιακές μεθόδους που απαιτούν ακριβή αντιστοίχιση των δεδομένων με την αναζητούμενη λέξη-κλειδί, η ασαφής αναζήτηση επιτρέπει στους χρήστες να ανακαλύπτουν σχετικά δεδομένα με βάση τη σημασιολογική ομοιότητα. Αυτή η προσέγγιση είναι εξαιρετικά χρήσιμη στα συστήματα που διαχειρίζονται μεγάλες όγκους δεδομένων όπου η ακριβής ταύτιση μπορεί να είναι δυσχερής ή ακατάλληλη λόγω της πιθανής πολυπλοκότητας των δεδομένων. Η χρήση ασαφούς αναζήτησης μπορεί να μειώσει την ακρίβεια των αποτελεσμάτων σε σχέση με την ακριβή αντιστοίχιση, ωστόσο αποτελεί βασικό εργαλείο για τη βελτίωση της ευελιξίας και της ταχύτητας των αναζητήσεων σε κρυπτογραφημένα δεδομένα, διατηρώντας παράλληλα το επίπεδο ασφάλειας που προσφέρει η κρυπτογράφηση.

Τελευταίες έρευνες εστίασαν στη βελτίωση της αναζητήσιμης κρυπτογράφησης μέσω του blockchain, παρέχοντας λύσεις για την ανίχνευση και την αφαίρεση κακόβουλων κόμβων. Αυτές οι προσεγγίσεις βοηθούν στην προστασία από επιθέσεις, όπως οι Επιθέσεις Εκτίμησης Κλειδιών (KGAs), χρησιμοποιώντας φιλτραρισμένη κρυπτογράφηση κλειδιού, τακτική ανανέωση κλειδιού και παρακολούθηση αιτημάτων κλειδιού. Αυτές οι προσεγγίσεις συμβάλλουν στην αποτροπή επιθέσεων που στοχεύουν στην κακόβουλη εισαγωγή ή αλλοίωση κρυπτογραφημένων δεδομένων σε ένα δίκτυο blockchain, ενισχύοντας την ασφάλεια και την εμπιστοσύνη στην αποθήκευση και διαχείριση των δεδομένων.

Αυτές οι μελέτες καταδεικνύουν ότι το blockchain μπορεί να ενισχύσει την ασφάλεια και τη διαφάνεια στη διαχείριση κρυπτογραφημένων αναζητήσεων με τη χρήση τεχνολογίας διανεμημένου μητρώου, προσφέροντας βελτιωμένες λύσεις για την αξιολόγηση εγκυρότητας των αναζητήσεων και την διαχείριση δικαιωμάτων πρόσβασης. [25]

4.8. Blockchain και Data Deduplication στο Νέφος

4.8.1. Data Deduplication στο Νέφος

Σύμφωνα με την έκθεση της IDC, μέχρι το 2025, στο Νέφος θα αποθηκεύουν σχεδόν 88 Zettabyte δεδομένων, εκ των οποίων το 75% θα είναι σε μορφή διπλότυπων δεδομένων. Για να μεγιστοποιηθεί η αποδοτικότητα αποθήκευσης, η πλειονότητα των Παρόχων Υπηρεσιών Cloud (CSPs) χρησιμοποιούν τεχνολογία Data Deduplication στα προϊόντα τους Storage-as-a-Service (StaaS), όπως το Dropbox και το Google Drive. Η τεχνολογία είναι επωφελής τόσο για τους CSPs όσο και για τους χρήστες, καθώς εξοικονομεί εύρος ζώνης, αυξάνει την αποδοτικότητα αποθήκευσης και μειώνει το κόστος ισχύος και υποδομής, οδηγώντας σε χαμηλότερες τιμές υπηρεσιών για τους πελάτες.

Ωστόσο, οι μέθοδοι Data Deduplication αντιμετωπίζουν σημαντικές προκλήσεις ασφαλείας. Τα δεδομένα που αποθηκεύονται στους διακομιστές cloud μπορεί να είναι κρυπτογραφημένα για να διασφαλιστεί η εμπιστευτικότητα των εξωτερικών δεδομένων. Παρόλα αυτά, οι CSPs συνήθως δεν επιτρέπουν στους χρήστες να κρυπτογραφούν τα δεδομένα τους με συμβατικές μεθόδους κρυπτογράφησης (π.χ., AES), γεγονός που επηρεάζει την αποδοτικότητα της απαλοιφής. Αντί αυτού, χρησιμοποιείται η κρυπτογράφηση συγκλίνουσας κλειδας (convergent encryption) για την επίτευξη κρυπτογράφησης. [25]

4.8.2. Blockchain-Enabled Cloud Data Deduplication

Οι υπάρχουσες προσεγγίσεις με blockchain εστιάζουν κυρίως σε αποκεντρωμένα συστήματα απαλοιφής δεδομένων σε πολλαπλά clouds. Η τεχνολογία blockchain χρησιμοποιείται για τη διαχείριση των διαδικασιών απαλοιφής δεδομένων λόγω του υψηλού ποσοστού απαλοιφής και της ανοχής σε σφάλματα. Παραδείγματος χάρη, το CloudShare εισήγαγε το blockchain στη διαχείριση απαλοιφής δεδομένων πολλαπλών clouds. Σε αυτήν την εργασία, η κρυπτογράφηση από την πλευρά του χρήστη προστατεύει από επιθέσεις από κακόβουλους διακομιστές. Η ακεραιότητα και η κυριότητα των δεδομένων των χρηστών προστατεύονται από τις συναλλαγές στο blockchain, που είναι ανθεκτικές στην αλλοίωση.

Ορισμένες εργασίες παρουσίασαν σύστημα απαλοιφής δεδομένων βασισμένο σε έξυπνα συμβόλαια, όπως το σύστημα που παρουσίασαν οι Liu και Li. Τα Έξυπνα Συμβόλαια Επιχειρήσεων (BSC) εκτελούν περιοδικά αποδείξεις ανακτήσιμης (Proof-of-Retrievability, PoR) μέσω ενός πρωτοκόλλου πρόκλησης-απόκρισης για την επαλήθευση της ακεραιότητας και της δυνατότητας ανάκτησης αρχείων, καθώς και την αντίσταση σε επιθέσεις πλευρικών καναλιών.

Παρά τη μεγάλη σημασία της απαλοιφής δεδομένων με blockchain, μέχρι στιγμής έχουν γίνει ελάχιστες εργασίες σε αυτόν τον τομέα. Η αντίφαση μεταξύ των δεδομένων blockchain υψηλής αναπαραγωγής και του στόχου της απαλοιφής δεδομένων αποτελεί σημαντικό εμπόδιο. Μέχρι στιγμής, το blockchain χρησιμεύει ως ένα υποσύστημα για τη διασφάλιση της ασφάλειας αποθήκευσης στο cloud. Οι υπάρχουσες εργασίες αποθηκεύουν ετικέτες αρχείων on-chain, ενώ τα αρχεία παραμένουν off-chain, καταναλώνοντας έτσι μικρό χώρο αποθήκευσης και ενισχύοντας την ασφάλεια και την ακεραιότητα των δεδομένων. [25]

5. Συνεισφορά του cloud στο blockchain

Στο Κεφάλαιο 5, διερευνώνται οι διάφορες συνεισφορές της τεχνολογίας Blockchain στην τεχνολογία απαλοιφής δεδομένων στο περιβάλλον του cloud. Αυτές οι συνεισφορές περιλαμβάνουν την ενίσχυση της ασφάλειας των δεδομένων, την εξασφάλιση της ακεραιότητας των δεδομένων μέσω αποκεντρωμένων πρωτοκόλλων, και τη βελτίωση της αποδοτικότητας αποθήκευσης. Στην ενότητα αυτή, παρουσιάζονται διεξοδικά οι τρόποι με τους οποίους το Blockchain μπορεί να χρησιμοποιηθεί για την επίτευξη ασφαλούς και αποδοτικής απαλοιφής δεδομένων, καθώς και οι προκλήσεις και τα οφέλη που συνδέονται με την ενσωμάτωση αυτής της τεχνολογίας σε συστήματα cloud. Η ανάλυση θα καλύψει τις υπάρχουσες λύσεις, τα πλεονεκτήματα και τα μειονεκτήματά τους, καθώς και τις προοπτικές για μελλοντική έρευνα και ανάπτυξη.

5.1. Blockchain as a service (BaaS)

5.1.1. Ορισμός του blockchain as a service

Η διαχειρίσιμη (managed) υπηρεσία νέφους Blockchain ως Υπηρεσία (Blockchain as a Service - BaaS) αναφέρεται στον συνδυασμό της τεχνολογίας της αλυσίδας Blockchain με τον υπολογισμό στο νέφος, που επιτρέπει στους πελάτες να χρησιμοποιούν λύσεις υπολογισμού στο νέφος για τη δημιουργία, φιλοξενία και διαχείριση εφαρμογών αλυσίδας μπλοκ, όπως έξυπνες συμβάσεις, καθώς και διαχειριστικές λειτουργίες δικτύου αλυσίδας μπλοκ. Η υπηρεσία BaaS εντάσσεται στο μοντέλο Πλατφόρμας ως Υπηρεσίας (PaaS) οπότε λειτουργεί και καταναλώνεται με τον ίδιο τρόπο. Επιπλέον, η BaaS θεωρείται ως υπηρεσία που μπορεί να ελέγχεται από ένα τρίτο μέρος. Στα πλαίσια αυτής της υπηρεσίας, οι εφαρμογές blockchain των πελατών εκτελούνται σε υπάρχοντα blockchain που φιλοξενούνται στο νέφος, ενώ ο πελάτης έχει τη δυνατότητα να δημιουργήσει και το δικό του blockchain. Όλα αυτά γίνονται χωρίς να χρειάζεται ο πελάτης να γνωρίζει τις ιδιαιτερότητες της τεχνολογίας του blockchain.

Προς το παρόν, οι πάροχοι πλατφορμών BaaS επικεντρώνονται στο να κρατήσουν την υποκείμενη υποδομή ευέλικτη και εύκολα προσβάσιμη και λειτουργική, διαχειριζόμενοι τις απαραίτητες δραστηριότητες και εργασίες προς αυτό τον σκοπό. Πολλοί πάροχοι υπηρεσιών BaaS προσφέρουν τα απαραίτητα δίκτυα αλυσίδας μπλοκ και την απαιτούμενη υποδομή με αντάλλαγμα χρηματική αμοιβή. Το μοντέλο χρέωσης για τις υπηρεσίες Blockchain ως Υπηρεσία (BaaS) μπορεί να διαφέρει ανάλογα με τον πάροχο, αλλά γενικά ακολουθεί ορισμένα πρότυπα.

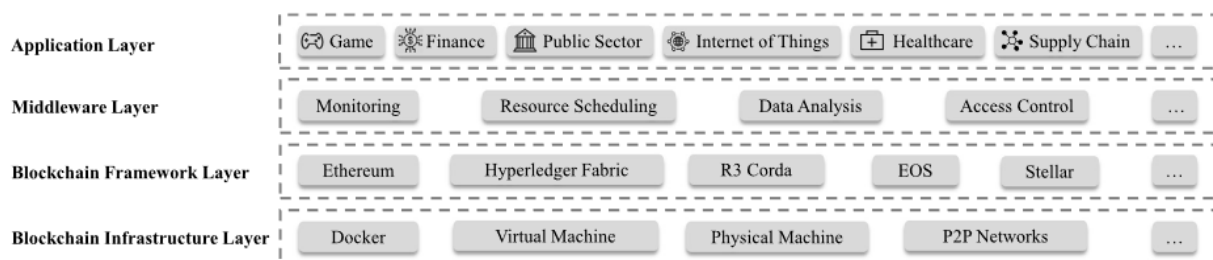
Ένα από τα πιο κοινά είναι το συνδρομητικό μοντέλο (subscription-based), όπου οι πελάτες πληρώνουν μια σταθερή μηνιαία ή ετήσια αμοιβή για τη χρήση της πλατφόρμας και των υπηρεσιών της. Το κόστος μπορεί να ποικίλει ανάλογα με το επίπεδο της υπηρεσίας και τα χαρακτηριστικά που προσφέρονται. Ένα άλλο μοντέλο είναι η πληρωμή ανά χρήση (pay-as-you-go), όπου οι πελάτες χρεώνονται ανάλογα με την πραγματική χρήση της υπηρεσίας, όπως για παράδειγμα βάσει του αριθμού των συναλλαγών, του αποθηκευτικού χώρου που χρησιμοποιείται

ή του υπολογιστικού χρόνου που καταναλώνεται. Επίσης, υπάρχει το μικτό μοντέλο (hybrid model), που συνδυάζει τα παραπάνω, όπου οι πελάτες πληρώνουν μια βασική συνδρομή και επιπλέον χρεώσεις βάσει της χρήσης. Ένα άλλο σύνθετο μοντέλο είναι η χρέωση ανά κόμβο (per-node pricing), όπου οι πελάτες χρεώνονται βάσει του αριθμού των κόμβων που χρησιμοποιούν στο δίκτυο blockchain. Αυτά τα μοντέλα επιτρέπουν στους παρόχους να προσαρμόζουν τις υπηρεσίες τους στις ανάγκες και το μέγεθος των πελατών, προσφέροντας ευελιξία και επιλογές για τη βελτιστοποίηση του κόστους.

Αφού ο πελάτης δημιουργήσει το σύστημά του, ο πάροχος υπηρεσιών διαχειρίζεται τις περίπλοκες διαδικασίες στο παρασκήνιο για λογαριασμό του πελάτη. Ο πελάτης αιτείται τη δημιουργία του blockchain δικτύου και την εκτέλεση διαχειριστικών λειτουργιών σε αυτό. Ο πάροχος υπηρεσιών BaaS αναλαμβάνει να μεταφράσει αυτές τις αιτήσεις στην εκτέλεση των κατάλληλων, περίπλοκων διαδικασιών διαχείρισης στο παρασκήνιο, παρέχοντας μια σειρά από υπηρεσίες, όπως διαχείριση της ανάθεσης πόρων, φιλοξενία εφαρμογών, χαρακτηριστικά ασφάλειας δεδομένων και διαχείριση εύρους ζώνης. Ο πάροχος υπηρεσιών BaaS παρέχει μια σειρά από υπηρεσίες, όπως διαχείριση της ανάθεσης πόρων, φιλοξενία εφαρμογών, χαρακτηριστικά ασφάλειας δεδομένων και διαχείριση εύρους ζώνης.[21]

5.1.2. Αρχιτεκτονική του blockchain as a service

Η BaaS (Blockchain as a Service) δημιουργεί ένα βολικό, επεκτάσιμο και υψηλής απόδοσης οικοσύστημα blockchain για την ανάπτυξη, κατασκευή, αναπύξιν και χειρισμό εφαρμογών blockchain. Οι τρέχουσες λύσεις BaaS συνήθως χωρίζονται σε τέσσερα επίπεδα (από το επάνω προς το κάτω): Επίπεδο Εφαρμογής, Επίπεδο Middleware, Επίπεδο Πλαίσιο Blockchain και Επίπεδο Υποδομής Blockchain, όπως φαίνεται στο Σχήμα 4. Κάθε επίπεδο μπορεί να θεωρηθεί ως ένα αρθρωτό σύστημα υπηρεσιών που περιλαμβάνει πολλαπλά απλά λειτουργικά στοιχεία.



Εικόνα 4. Αρχιτεκτονική του Blockchain as a Service

Στο επάνω μέρος της αρχιτεκτονικής BaaS βρίσκεται το επίπεδο εφαρμογής. Οι εφαρμογές βασισμένες σε blockchain αναπτύσσονται πάνω στην υποκείμενη υποδομή blockchain. Με αυτόν τον τρόπο, οι προγραμματιστές BaaS δεν χρειάζεται να κατανοήσουν πλήρως τα εσωτερικά του blockchain, αλλά μόνο τους τρόπους κλήσης υπηρεσιών BaaS για τη

δημιουργία μιας εφαρμογής blockchain. Με αυτόν τον τρόπο, οι προγραμματιστές μπορούν να επικεντρωθούν στην επιχειρηματική λογική των εφαρμογών, ενώ οι πάροχοι BaaS χρειάζεται μόνο να αναπτύξουν αποκεντρωμένες εφαρμογές πάνω σε μια υποδομή blockchain.

Το δεύτερο επίπεδο στη δομή της BaaS είναι το επίπεδο middleware, το οποίο λειτουργεί ως πράκτορας διασύνδεσης μεταξύ του επιπέδου εφαρμογής και του επιπέδου πλαισίου blockchain. Αφενός, το επίπεδο middleware αποκρύπτει την πολυπλοκότητα του υποκείμενου blockchain και προσφέρει φιλικά προς τον χρήστη διασταυρωμένα για τους προγραμματιστές εφαρμογών στο παραπάνω επίπεδο εφαρμογής. Αυτό το επίπεδο περιλαμβάνει βασικές υπηρεσίες διαχείρισης συστημάτων όπως παρακολούθηση, ανάλυση δεδομένων, προγραμματισμός πόρων και έλεγχος πρόσβασης.

Το τρίτο επίπεδο αφορά στην κατασκευή ενός πλαισίου blockchain βασισμένου στη υποδομή blockchain. Το πλαίσιο blockchain αναφέρεται γενικά στην πλατφόρμα έξυπνων συμβολαίων, όπως αναφέρθηκε στην ενότητα 2. Σε αυτό το επίπεδο, η πλατφόρμα έξυπνων συμβολαίων παρέχει προγράμματα που τεκμηριώνονται με καθορισμένες γλώσσες και εκτελούνται σε περιβάλλοντα εκτέλεσης (π.χ., εικονικές μηχανές). Από την άποψη της σταθερότητας και της ποικιλίας, το πλαίσιο BaaS υποστηρίζει δημοφιλείς πλατφόρμες έξυπνων συμβολαίων όπως το Hyperledger Fabric, το Ethereum, το Quorum (Ethereum για επιχειρήσεις), το R3 Corda, το EOS, το Stellar κ.ά. Οι προγραμματιστές blockchain μπορούν να κατασκευάσουν την επιχειρηματική λογική γραμμένη σε συγκεκριμένους κώδικες προγραμματισμού που εκτελούνται σε σταθερά περιβάλλοντα.

Επίπεδο Υποδομής Blockchain: Το επίπεδο υποδομής blockchain τοποθετείται στο κάτω μέρος της αρχιτεκτονικής BaaS. Δεδομένου ότι το blockchain είναι ουσιαστικά ένα καταναμημένο σύστημα, η υποδομή blockchain προσφέρει υπηρεσίες επικοινωνίας/δικτύωσης με αντίστοιχους υπολογιστικούς πόρους όπως φυσικές μηχανές, εικονικές μηχανές ή νεότερα docker containers για την εκτέλεση έξυπνων συμβολαίων. [43]

5.1.3. Πλεονεκτήματα και μειονεκτήματα του blockchain as a service

Το BaaS αναπτύχθηκε ως μια καινοτόμος λύση για επιχειρήσεις που επιθυμούν να εφαρμόσουν την τεχνολογία των blockchain χωρίς το βάρος της πλήρους ανάπτυξης και διαχείρισης μιας δικής τους υποδομής. Επιτρέπει στις επιχειρήσεις να αξιοποιήσουν προηγμένες τεχνολογίες χωρίς την ανάγκη για σημαντικές επενδύσεις σε υλικό και λογισμικό. Στη συνέχεια, θα εξετάσουμε πιο αναλυτικά τα πλεονεκτήματα που προσφέρει το Blockchain-as-a-Service. Έπειτα, καταλήγουμε με τα μειονεκτήματα αυτού του είδους υπηρεσίας νέφους και τον τρόπο με τον οποίο μπορούν να επηρεάσουν τη λειτουργία και ανάπτυξη των επιχειρήσεων.

- Η διαφάνεια είναι ένας σημαντικός παράγοντας για τις επιχειρήσεις στη χρήση τεχνολογίας του Blockchain. Μέσω της τεχνολογίας αυτής, οι επιχειρήσεις μπορούν να διατηρούν και

να μοιράζονται πολύτιμες πληροφορίες με υψηλό επίπεδο διαφάνειας και ανιχνευσιμότητας στις συναλλαγές, κάτι που οι καταναλωτές αρχίζουν να αναμένουν στη ψηφιακή εποχή. [21]

- Ο χρόνος και τα χρήματα αποτελούν δύο κρίσιμους παράγοντες για κάθε οργάνωση. Οι υπηρεσίες πλατφόρμας ως υπηρεσία (PaaS) που παρέχουν την υπηρεσία Blockchain-as-a-Service (BaaS), εξωτερικεύουν την υπηρεσία του Blockchain, βοηθώντας τις οργανώσεις να εξοικονομήσουν χρόνο και χρήματα από την κατασκευή των δικών τους blockchain και δίνοντάς τους ένα αξιόπιστο τρόπο χρήσης της τεχνολογίας. Επιπλέον, το BaaS εξοικονομεί κόστη στην πρόσληψη διαχειριστών για την εγκατάσταση και συντήρηση λογισμικού. Το λογισμικό ως υπηρεσία (Software-as-a-Service, SaaS), που παρέχει πρόσβαση σε προηγμένες λειτουργίες τεχνολογίας blockchain μέσω διαδικτυακής πλατφόρμας, επιτρέπει στις επιχειρήσεις να αξιοποιήσουν την τεχνολογία χωρίς την ανάγκη να αναπτύξουν ή να διαχειριστούν τη δική τους υποδομή blockchain. Κατ' αυτόν τον τρόπο, η χρήση του BaaS και του SaaS αποτελεί μια έξυπνη επένδυση για την αύξηση της αποδοτικότητας και της οικονομίας κλίμακας στον τομέα της τεχνολογίας. [21]
- Όταν μια εταιρεία αποφασίζει να χρησιμοποιήσει την τεχνολογία της αλυσίδας μπλοκ, μπορεί να επιλέξει να μην αναπτύξει την υποδομή από την αρχή. Αντί αυτού, μπορεί να χρησιμοποιήσει υπηρεσίες όπως το Blockchain-as-a-Service (BaaS), το οποίο παρέχει έτοιμες λύσεις. Αυτό σημαίνει ότι η ομάδα ανάπτυξης της εταιρείας δεν χρειάζεται να δαπανήσει χρόνο και πόρους για τη δημιουργία της υποδομής από το μηδέν. Αντίθετα, μπορεί να επικεντρωθεί στην ανάπτυξη των δικών της εφαρμογών και λειτουργιών που χρειάζονται για τις επιχειρηματικές της ανάγκες. Ταυτόχρονα, το Blockchain παρέχει την υποδομή και τις λειτουργίες που απαιτούνται, όπως διαχείριση εύρους ζώνης, φιλοξενία, ασφάλεια κ.λπ. Ο πάροχος της υπηρεσίας αναλαμβάνει τη συντήρησή της, ενώ η εταιρεία μπορεί να επικεντρωθεί μόνο στην ανάπτυξη των εφαρμογών της. Έτσι αποφεύγεται η δημιουργία μιας νέας υποδομής και επιτρέπεται η πιο αποτελεσματική χρήση των πόρων της εταιρείας. [21]

Παρότι το BaaS προσφέρει πολλά πλεονεκτήματα, πάσχει και από ορισμένα μειονεκτήματα που πρέπει να ληφθούν υπόψη πριν κάποιος υιοθετήσει αυτό το νέο είδος υπηρεσίας νέφους.

- Οι βασικοί κίνδυνοι που συνδέονται με το BaaS είναι ένας συνδυασμός μειονεκτημάτων του blockchain και του Νέφους όπως η έλλειψη επαρκούς γνώσης και εμπειρίας σχετικά με την τεχνολογία η οποία μπορεί να επηρεάσει την απόδοση των επιχειρήσεων που επιλέγουν να την υιοθετήσουν. Χωρίς την απαραίτητη κατάρτιση και κατανόηση, οι επιχειρήσεις μπορεί να καταλήξουν να καταστρέψουν αντί να βελτιώσουν τις

δραστηριότητές τους μέσω της χρήσης της τεχνολογίας blockchain [26]. Επίσης η κατανάλωση ενέργειας και οι απαιτήσεις σε υπολογιστικούς πόρους για την λειτουργία του BaaS είναι ένα μειονέκτημα [21].

- Καθώς η τεχνολογία του BaaS βασίζεται στη διάδοση πληροφοριών σε ένα παγκόσμιο δίκτυο, διεθνείς κανονισμοί μπορεί να επηρεάσουν τις πληροφορίες που κοινοποιούνται διασυνοριακά. Η ανάπτυξη του BaaS υπόκειται σε διαφορετικούς νομικούς κανονισμούς σε κάθε χώρα, και η αποκεντρωμένη φύση της τεχνολογίας μπορεί να δημιουργήσει προκλήσεις όσον αφορά τη συμμόρφωση με αυτούς τους κανονισμούς. Αυτό μπορεί να οδηγήσει σε περιορισμούς στη χρήση ή την εξαγωγή δεδομένων σε διάφορες χώρες, καθώς επίσης και σε αντιδράσεις από τους κανονιστικούς φορείς. [21]
- Ένα άλλο μειονέκτημα είναι περιορισμός δυνατοτήτων των λύσεων BaaS καθώς οι λύσεις είναι περιορισμένες στις δυνατότητες που υποστηρίζονται από την υποκείμενη πλατφόρμα. Για παράδειγμα, στο Salesforce ως πάροχος BaaS, οι δυνατότητές του περιορίζονται μόνο στη Διαχείριση Πελατειακών Σχέσεων (CRM). Δεν μπορεί να δημιουργηθεί μια εφαρμογή χρησιμοποιώντας το Salesforce BaaS και να υποστηρίξει άλλες λειτουργίες, όπως το ηλεκτρονικό εμπόριο ή ένα σύστημα διαχείρισης περιεχομένου (CMS). [21]

5.1.4. BaaS πλατφόρμες

5.1.4.1. Microsoft Azure Blockchain

Η υπηρεσία Azure Blockchain Service της Microsoft αποτελεί μια πλήρη λύση για την εφαρμογή της τεχνολογίας blockchain στο περιβάλλον του Azure Cloud. Το Azure Blockchain Service υποστηρίζει πολλές δημοφιλείς πλατφόρμες blockchain, συμπεριλαμβανομένων του Ethereum, του Hyperledger Fabric και του Corda, προσφέροντας έτσι ευελιξία στην επιλογή της κατάλληλης τεχνολογίας ανάλογα με τις ανάγκες της εφαρμογής. Επιπλέον, η συνεργασία της Microsoft με την ConsenSys επέτρεψε την ολοκλήρωση του Ethereum στην πλατφόρμα Azure, παρέχοντας έτσι πρόσβαση σε ένα εκτεταμένο οικοσύστημα εφαρμογών και λειτουργιών βασισμένων στο Ethereum.

Μια σημαντική λειτουργία της υπηρεσίας είναι η δυνατότητα αυτόματης δημιουργίας αντιγράφων ασφαλείας δεδομένων on-chain σε off-chain αποθήκευση στο cloud. Αυτό εξασφαλίζει την ασφάλεια των δεδομένων και την ευελιξία στη διαχείρισή τους. Επιπλέον, μέσω του Azure Blockchain Workbench, οι χρήστες μπορούν να δημιουργήσουν και να αναπτύξουν έξυπνα συμβόλαια, τα οποία μπορούν να προσαρμοστούν σύμφωνα με τις ανάγκες και τις προδιαγραφές τους. Αυτό προσφέρει μια πιο ευέλικτη και εύκολη διαδικασία ανάπτυξης εφαρμογών blockchain στο περιβάλλον του Azure. [22]

5.1.4.2. Amazon AWS Blockchain

Η υπηρεσία AWS Blockchain της Amazon χρησιμοποιεί πρότυπα και ένα σύστημα ανοικτού κώδικα για τη δημιουργία και την ανάπτυξη δικτύων Blockchain με αποτελεσματικό τρόπο. Οι χρήστες της AWS χρησιμοποιούν τα πρότυπα για να δημιουργήσουν διάφορες εφαρμογές Blockchain. μοντέλα Blockchain στην AWS χρησιμοποιούν τη δομή του Blockchain που εκτελείται εντός υπηρεσιών όπως το Amazon Elastic Container Service (Amazon ECS) ή εντός του Amazon Elastic Compute Cloud (Amazon EC2). Κάθε δίκτυο Blockchain χτίζεται σε ένα ιδιωτικό δίκτυο, επιτρέποντας στον χρήστη να χρησιμοποιήσει τις σχετικές λίστες ελέγχου πρόσβασης και τα υποδίκτυα του δικτύου αυτού. Επιπλέον, ο χρήστης μπορεί να καθορίσει άδειες για τον περιορισμό της πρόσβασης στους πόρους του συστήματος.

Η υπηρεσία blockchain της AWS χρησιμοποιεί δύο πλαίσια ανοικτού κώδικα, το Ethereum και το Hyperledger Fabric, για την δημιουργία των υποδομών Blockchain. Έτσι, τα πρότυπα μπορούν να εφαρμοστούν σε διάφορες υποδομές Blockchain. Τα πρότυπα που χρησιμοποιούν το Ethereum δίνουν στον χρήστη τη δυνατότητα να δημιουργήσει και να εκτελέσει εφαρμογές blockchain χωρίς διακοπές, απάτη, επίβλεψη ή παρέμβαση τρίτων. Στην AWS, οι χρήστες μπορούν να ξεκινήσουν έξυπνα συμβόλαια χρησιμοποιώντας τη γλώσσα Solidity του Ethereum. Επιπλέον, το Hyperledger Fabric επιτρέπει στους χρήστες να δημιουργήσουν εφαρμογές Blockchain παρέχοντας λίστες ελέγχου πρόσβασης και άδειες για τα δεδομένα Blockchain. Οι χρήστες μπορούν να χρησιμοποιήσουν το Hyperledger Fabric για να δημιουργήσουν ένα ιδιωτικό δίκτυο Blockchain και να περιορίσουν τις συναλλαγές που μπορούν να δουν διαφορετικά μέρη. [22]

5.1.4.3. IBM Blockchain

Η εταιρεία IBM προσφέρει μια πλατφόρμα βασισμένη σε ανοικτό κώδικα για το blockchain στο cloud computing. Η προτεινόμενη πλατφόρμα χρησιμοποιεί τα εργαλεία Hyperledger Fabric από το Linux. Με υποστήριξη ανοικτού κώδικα για τις εγκαταστάσεις και τη δυνατότητα χρήσης τρίτων παρόχων νέφους, βοηθά τους χρήστες να αποφύγουν τον περιορισμό της δέσμευσης σε έναν συγκεκριμένο προμηθευτή. Το IBM Blockchain λειτουργεί με τρία επίπεδα: το επίπεδο υπηρεσίας, το Hyperledger Fabric και το Hyperledger Composer. Επιπλέον, η πλατφόρμα της IBM επιταχύνει τη διαδικασία ανάπτυξης εφαρμογών blockchain με ένα πλαίσιο ανάπτυξης εφαρμογών. Το Hyperledger Composer προσφέρει ένα κατάλληλο επίπεδο και επιχειρηματική δομή για τη δημιουργία έξυπνων συμβολαίων και την υλοποίησή τους στο Hyperledger Fabric. [22]

5.1.4.4. Google Blockchain

Η μετάβαση της εταιρείας Blockchain στη Google Cloud Platform αντιπροσωπεύει ένα σημαντικό ορόσημο στην εξέλιξη της τεχνολογίας των Blockchain. Αυτή η μετάβαση επιτρέπει στην εταιρεία να επωφεληθεί από την υψηλή απόδοση και την αξιοπιστία των υποδομών υπολογισμού της Google Cloud. Μέσω των υπηρεσιών Compute Engine και Cloud Spanner, η εταιρεία μπορεί να διαχειριστεί με αποτελεσματικότητα την υποδομή του Blockchain και να παρέχει υψηλή διαθεσιμότητα και σταθερή συνέπεια σε παγκόσμια κλίμακα. Αυτό σημαίνει ότι η

εταιρεία θα μεταφέρει τα συστήματα και τις εφαρμογές της από την προηγούμενη υποδομή που χρησιμοποιούσε στη Google Cloud, επωφελούμενη των προηγμένων λύσεων της για την ασφαλή και αποδοτική διαχείριση των δεδομένων και των εφαρμογών της στον τομέα των Blockchain.

Επιπλέον, η συμμετοχή της Google στο Hedera Governing Council ανοίγει νέες προοπτικές για τη σταθερή ανάπτυξη και υποστήριξη των τεχνολογιών Blockchain. Η ικανότητα της Google να παρέχει τεχνολογική εμπειρογνωμοσύνη και υποστήριξη στους χρήστες της πλατφόρμας της, Google Cloud Platform, αποτελεί σημαντικό πλεονέκτημα για τους επιχειρηματίες που χρησιμοποιούν τις υπηρεσίες τους στον τομέα των Blockchain.

Τέλος, η συνεργασία με τη Theta Labs αναδεικνύει τη δυνατότητα της Google Cloud να υποστηρίζει πολύπλοκα δίκτυα Blockchain όπως το δίκτυο Theta. Η παροχή υπηρεσιών για την ανάπτυξη και λειτουργία των δικτύων Blockchain ενισχύει τη θέση της Google ως κορυφαίου παρόχου υποδομής Cloud για εφαρμογές Blockchain. [22]

5.1.4.5. Oracle Blockchain

Το 2017, η Oracle παρουσίασε την υπηρεσία τους Blockchain Cloud Service, μια πλατφόρμα-ως-υπηρεσία (PaaS) που προσφέρει ένα σύστημα κατανεμημένου λογιστικού βιβλίου που λειτουργεί στο cloud και δημιουργήθηκε βασισμένο στο Hyperledger Fabric και τις βελτιώσεις της Oracle για να προσφέρει μια διαχειριστική πλατφόρμα blockchain επιπέδου επιχείρησης. Το Oracle Blockchain επιτρέπει στον χρήστη να εγγράψει μέλη, να δημιουργήσει δίκτυα Blockchain, να καταστήσει την υλοποίηση και να εκτελέσει έξυπνα συμβόλαια.

Περιλαμβάνει τα μέλη του δικτύου επικύρωσης (ονομάζονται peers), τα οποία ενημερώνουν και επικυρώνουν το κατανεμημένο λογιστικό βιβλίο (distributed ledger) κατά την εκτέλεση οποιασδήποτε συναλλαγής και απαντούν σε ερωτήματα με την εκτέλεση του έξυπνου συμβολαίου. Αυτό το κατανεμημένο λογιστικό βιβλίο αποθηκεύει όλες τις συναλλαγές που έχουν γίνει στο δίκτυο blockchain και είναι προσβάσιμο από όλους τους κόμβους στο δίκτυο. Ο χρήστης μπορεί να επιλέξει τους επικυρωμένους κόμβους κατά τον σχεδιασμό του δικτύου. Οι εφαρμογές στην πλευρά του πελάτη μπορούν να αλληλεπιδρούν με τις συναλλαγές και τα ερωτήματα μέσω ανάπτυξης κώδικα που εκμεταλλεύεται τα παρεχόμενα SDK και το RESTful API. [22]

5.1.4.6. Alibaba Cloud

Η υπηρεσία Blockchain-as-a-Service (BaaS) της Alibaba Cloud προσφέρει ένα πλήρες οικοσύστημα λύσεων για την υλοποίηση και διαχείριση εφαρμογών Blockchain. Με βάση την ανοικτή πλατφόρμα Kubernetes, οι χρήστες μπορούν να εκτελέσουν την υπηρεσία σε διάφορα περιβάλλοντα, όπως ένα ιδιωτικό ή δημόσιο νέφος. Η υπηρεσία υποστηρίζει διάφορες ανοικτού κώδικα πλατφόρμες Blockchain, όπως την Enterprise Ethereum - Quorum και την Hyperledger Fabric, καθώς και την Blockchain τεχνολογία Ant Blockchain, η οποία είναι σχεδιασμένη για χρήση στον χώρο των οικονομικών υπηρεσιών.

Η Alibaba Cloud BaaS παρέχει ένα εύχρηστο γραφικό περιβάλλον για την εύκολη διαχείριση και λειτουργία των δικτύων Blockchain. Οι επιχειρήσεις και οι οργανισμοί μπορούν να

δημιουργήσουν και να αναπτύξουν δίκτυα Blockchain με ταχύτητα και αξιοπιστία, επωφελούμενοι από την προηγμένη υποδομή υπηρεσιών της Alibaba Cloud. Η ανάπτυξη και η εκτέλεση εφαρμογών Blockchain γίνεται άμεσα διαθέσιμη, με δυνατότητες προσαρμογής σε διαφορετικές απαιτήσεις και σενάρια χρήσης. Επιπλέον, η υπηρεσία παρέχει ευέλικτες επιλογές ασφαλείας και διαχείρισης των πόρων, επιτρέποντας στους χρήστες να αξιοποιήσουν πλήρως το δυναμικό της τεχνολογίας Blockchain για τις ανάγκες τους. [22]

5.2. Εκφόρτωση Λειτουργιών Blockchain στο Νέφος

Παρά τα πλεονεκτήματα του συστήματος blockchain σε ασφάλεια, διαφάνεια και ανοχή σε σφάλματα, οι εφαρμογές που βασίζονται σε blockchain συχνά απαιτούν ισχυρή υποστήριξη από backend υπηρεσίες. Πρώτον, τα περισσότερα συστήματα blockchain χρησιμοποιούν τον μηχανισμό συναίνεσης PoW (Proof of Work), ο οποίος δεν είναι εφικτό να εκτελεστεί σε φορητές συσκευές επικοινωνίας, όπως τα έξυπνα κινητά τηλέφωνα, λόγω του περιορισμένου υπολογιστικού τους δυναμικού. Η ανάθεση αυτού του κρυπτογραφικού παζλ σε τρίτους είναι μία λύση σε αυτό το σενάριο. Παρόμοια, η εκτέλεση σύνθετων έξυπνων συμβολαίων αποτελεί επίσης σημαντικό βάρος για συσκευές με περιορισμένους πόρους. Πρόσφατες έρευνες [52] έχουν αναλάβει να αντιμετωπίσουν τις προαναφερόμενες προκλήσεις μεταφέροντας υπολογιστικά καθήκοντα μεταξύ συσκευών και εξυπηρετών νέφους.

5.2.1. Εκφόρτωση βάσει Κέρδους Χρηστών

Σε ορισμένες προσεγγίσεις του κρυπτογραφικού παιχνιδιού Proof of Work (PoW), η στρατηγική εκτόνωσης στοχεύει στη μεγιστοποίηση του κέρδους για τους εξορύκτες και τους χρήστες της υπηρεσίας. Αυτή η προσέγγιση υποθέτει ότι η τιμή της ενέργειας είναι σταθερή και προκαθορισμένη από μια αρχή, εστιάζοντας στη βελτιστοποίηση του κέρδους μέσω της μείωσης του συνολικού κόστους, ιδίως της ενεργειακής κατανάλωσης, και της αύξησης της υπολογιστικής αποδοτικότητας.

Μια προηγμένη προσέγγιση που παρουσιάστηκε επικεντρώθηκε στο edge computing και στη χρήση κρυφής μνήμης περιεχομένου. Η ιδέα ήταν να εκτελεστούν υπολογισμοί στις ακμές του δικτύου, βελτιστοποιώντας έτσι το συνολικό καθαρό εισόδημα. Αυτή η προσέγγιση αξιολογήθηκε με βάση πειράματα που λάμβαναν υπόψη την καθυστέρηση εργασιών και την ενεργειακή κατανάλωση.

Στη συνέχεια, προτάθηκαν δύο στρατηγικές εκτόνωσης που χρησιμοποιούν τον αλγόριθμο Alternating Direction Method of Multipliers (ADMM) για την επίτευξη βέλτιστου συνολικού καθαρού εισοδήματος. Κατά τη διάρκεια των πειραμάτων, αναδείχθηκε ότι οι πιθανοτικοί περιορισμοί είχαν καλύτερη απόδοση σε σχέση με τους καθοριστικούς, καθώς επέτρεπαν μεγαλύτερη ευελιξία στην αντιμετώπιση ποικίλων συνθηκών και συνθηκών περιβάλλοντος.

Επιπλέον, η μελέτη εξέτασε τις προτιμήσεις των εξορύκτων υπό διάφορους καθοριστικούς περιορισμούς επιστροφής, επισημαίνοντας τις προκλήσεις που επηρεάζουν την πραγματική απόδοση ανάλογα με τον αριθμό των συμμετεχόντων κόμβων στο δίκτυο.

Αυτή η προσέγγιση αποτελεί σημαντικό βήμα προς την κατανόηση και τη βελτιστοποίηση της εκτόνωσης στο πλαίσιο των κρυπτογραφικών πρωτοκόλλων PoW, ενισχύοντας την απόδοση και την αποτελεσματικότητα του συστήματος. [25]

5.2.2. Εκφόρτωση βάσει κοινωνικής ευημερίας

Αυτή η ενότητα αφορά τη χρήση δημοπρασιών για την καλύτερη αξιοποίηση των πόρων cloud από τους παρόχους υπηρεσιών (CSP) στο πλαίσιο του "Blockchain as a Service" (BaaS). Οι δημοπρασίες επιτρέπουν στους CSP να προσαρμόζουν δυναμικά τις τιμές των πόρων τους με βάση τη ζήτηση από τους χρήστες του blockchain, δηλαδή τους εξορύκτες.

Η διαδικασία της δημοπρασίας περιλαμβάνει δύο φάσεις αξιολόγησης για τους εξορύκτες. Στον πρώτο γύρο, γνωστό ως αξιολόγηση ex-ante, οι εξορύκτες υποβάλλουν τις προσφορές τους χωρίς να γνωρίζουν την ακριβή ποσότητα των διαθέσιμων πόρων ή τον αριθμό των νικητών της δημοπρασίας. Σε αυτό το στάδιο, οι προσφορές τους βασίζονται στην αναμενόμενη ανταμοιβή που πιστεύουν ότι θα κερδίσουν αν αποκτήσουν τους πόρους. Στον δεύτερο γύρο, γνωστό ως αξιολόγηση ex-post, οι εξορύκτες αξιολογούν το αποτέλεσμα της δημοπρασίας με βάση την πραγματική ανταμοιβή που έλαβαν και το δικτυακό αποτέλεσμα. Το δικτυακό αποτέλεσμα καθορίζεται εμπειρικά από μια συνάρτηση S-καμπύλης, η οποία περιγράφει πώς επηρεάζεται η απόδοση του δικτύου blockchain από τον αριθμό των εξορυκτών και την ποσότητα των πόρων που διατίθενται σε κάθε εξορύκτη.

Από την πλευρά των CSP, ο στόχος είναι η μεγιστοποίηση της κοινωνικής ευημερίας, η οποία ορίζεται ως η διαφορά μεταξύ της συνολικής ικανοποίησης των εξορυκτών (μετά την αξιολόγηση ex-post) και του συνολικού κόστους των πόρων που παρέχουν οι CSP. Για να επιτύχουν αυτόν τον στόχο, οι CSP χρησιμοποιούν έναν βέλτιστο αλγόριθμο που λαμβάνει υπόψη τις προσφορές των εξορυκτών και επιλέγει τους νικητές της δημοπρασίας με έναν απληστικό (greedy) μηχανισμό. Αυτός ο μηχανισμός στοχεύει στην επίτευξη της μέγιστης κοινωνικής ευημερίας, διασφαλίζοντας ότι οι διαθέσιμοι πόροι κατανέμονται με τον πιο αποδοτικό τρόπο.

Με απλά λόγια, οι δημοπρασίες αυτές επιτρέπουν στους παρόχους υπηρεσιών cloud να αξιοποιούν καλύτερα τους πόρους τους, προσαρμόζοντας τις τιμές σύμφωνα με τη ζήτηση και διασφαλίζοντας ότι οι εξορύκτες μπορούν να αποκτήσουν τους πόρους που χρειάζονται για να μεγιστοποιήσουν την απόδοσή τους στο blockchain. [25]

5.2.3. Εκφόρτωση βάσει κέρδους των CSP

Υπάρχουν μερικές πτυχές που πρέπει να ληφθούν υπόψη από την πλευρά των CSP, όπως η εξοικονόμηση ενέργειας και κόστους. Οι Qiu et al. [51] τόνισαν ότι το blockchain δεν

μπορεί να εφαρμοστεί απευθείας σε περιβάλλοντα IoT ή άλλα δίκτυα επειδή οι περισσότεροι κόμβοι του δικτύου είναι περιορισμένοι σε πόρους. Η έρευνα πρότεινε ότι ο συνδυασμός της εξόρυξης με πράκτορες και της εξόρυξης στο cloud αποτελεί μια εφικτή μέθοδο για τη μείωση των περιορισμών. Η διαφορά μεταξύ της εξόρυξης με πράκτορες και της εξόρυξης στο cloud έγκειται κυρίως στον τρόπο και τον τόπο εκτέλεσης των υπολογιστικών εργασιών που σχετίζονται με την εξόρυξη blockchain. Η εξόρυξη με πράκτορες περιλαμβάνει τη χρήση ειδικών λογισμικών πρακτόρων που είναι εγκατεστημένοι σε τοπικές συσκευές ή κόμβους του δικτύου.

Αυτοί οι πράκτορες είναι υπεύθυνοι για την εκτέλεση συγκεκριμένων υπολογιστικών εργασιών και την αποστολή των αποτελεσμάτων τους στο κεντρικό δίκτυο για περαιτέρω επεξεργασία. Οι πράκτορες εκτελούνται τοπικά, συχνά σε συσκευές με περιορισμένους πόρους, όπως IoT συσκευές. Από την άλλη πλευρά, η εξόρυξη στο cloud μεταφέρει το μεγαλύτερο μέρος της υπολογιστικής εργασίας σε κεντρικούς servers ή πλατφόρμες cloud. Αυτό σημαίνει ότι οι βαριές υπολογιστικές διαδικασίες, όπως η λύση των puzzles του Proof of Work (PoW), εκτελούνται σε υποδομές cloud, οι οποίες διαθέτουν μεγαλύτερη υπολογιστική ισχύ και αποθηκευτικούς πόρους. Αυτό βοηθά στην ανακούφιση των τοπικών συσκευών από την έντονη υπολογιστική φόρτιση και μειώνει τους περιορισμούς των πόρων τους. Οι Chen et al. [47] επεσήμαναν ότι η εκτόνωση υπολογισμού και η εξόρυξη blockchain πρέπει να εξετάζονται ενιαία, καθώς η πολυπλοκότητα του ζητήματος αυξάνεται όταν λαμβάνονται υπόψη και οι δύο διαδικασίες (εξόρυξης με πράκτορες και εξόρυξης στο cloud) και συμμετέχουν περισσότεροι φορείς.

Η αυξημένη πολυπλοκότητα όταν λαμβάνονται υπόψη τόσο η εκτόνωση υπολογισμού όσο και η εξόρυξη blockchain μπορεί να φανεί ως μειονέκτημα. Ωστόσο, υπάρχουν σημαντικοί λόγοι για την ενιαία θεώρηση των δύο διαδικασιών, οι οποίοι υπερτερούν των μειονεκτημάτων της αυξημένης πολυπλοκότητας. Η ενιαία θεώρηση επιτρέπει την καλύτερη κατανομή των πόρων μεταξύ εκτόνωσης και εξόρυξης. Μπορεί να αξιοποιηθεί η συνολική υπολογιστική ισχύς με πιο αποδοτικό τρόπο, μειώνοντας την σπατάλη και αυξάνοντας την αποδοτικότητα του συστήματος. Επιπλέον, η ενιαία προσέγγιση επιτρέπει την ενσωμάτωση διαδικασιών και την απλοποίηση της διαχείρισης, μειώνοντας τον αριθμό των ξεχωριστών συστημάτων και εργαλείων που απαιτούνται. Η συνδυαστική προσέγγιση δίνει τη δυνατότητα για συνολική βελτιστοποίηση και αλληλεπίδραση μεταξύ των διαδικασιών, επιτρέποντας τη χρήση προχωρημένων τεχνικών, όπως η θεωρία παιγνίων, για τη βέλτιστη κατανομή πόρων και την επίτευξη του μέγιστου κέρδους για όλους τους συμμετέχοντες. Τέλος, η ενιαία θεώρηση μπορεί να οδηγήσει σε μεγαλύτερη κοινωνική ευημερία, καθώς οι διαδικασίες μπορούν να σχεδιαστούν και να εφαρμοστούν με τρόπο που μεγιστοποιεί τη συνολική ωφέλεια για το σύστημα.

Επιπλέον, κάποιες έρευνες [37] [38] χρησιμοποίησαν τη θεωρία παιγνίων για να μοντελοποιήσουν την αλληλεπίδραση μεταξύ εγωιστικών παρόχων υπηρεσιών και χρηστών. Συνοπτικά, συζητήθηκε η εκτόνωση εργασιών και η κατανομή πόρων για να βοηθηθούν οι κινητοί χρήστες να λύσουν το παζλ PoW. Οι έρευνες αυτές κατέληξαν πως τρία αντικείμενα θεωρήθηκαν σημαντικά προς βελτιστοποίηση κατά τη διάρκεια της εκτόνωσης. Από την άποψη των εξορύκτων, η στρατηγική εκτόνωσης και εξόρυξης PoW ήταν δυναμικά βελτιστοποιημένη για να επιτευχθεί το συνολικό έσοδο του εξορύκτη. Από την άποψη του παρόχου υπηρεσιών, η θεωρία

παιγνίων χρησιμοποιήθηκε για να βρεθεί το βέλτιστο σημείο ισορροπίας ώστε να διασφαλιστεί το μέγιστο κέρδος του παρόχου. Η κοινωνική ευημερία, που αντιπροσώπευε τη συνολική ωφέλεια στο σύστημα, μπορούσε να μεγιστοποιηθεί μέσω μηχανισμού δημοπρασίας. [25]

5.3. Χρήση Αποθήκευσης Νέφους στο Blockchain

Η χρήση αποθήκευσης στο cloud αποτελεί μια εναλλακτική μέθοδο για την ενίσχυση των συστημάτων blockchain, ειδικά από την προοπτική της μαζικής αποθήκευσης δεδομένων, μειώνοντας τους περιορισμούς που προκαλούνται από τον περιορισμένο χώρο αποθήκευσης των μπλοκ. Επομένως, ένα κρίσιμο ζήτημα είναι να καθοριστεί ποια δεδομένα θα αποθηκεύονται στα μπλοκ για να επιτευχθεί ισορροπία μεταξύ του μεγέθους του μπλοκ και της λειτουργικότητας του blockchain. Η αποθήκευση δεδομένων στο cloud παρέχει μια εναλλακτική λύση για την ενίσχυση των συστημάτων blockchain, ιδίως στην περίπτωση μαζικής αποθήκευσης δεδομένων. Αυτό μειώνει τους περιορισμούς που προκαλούνται από τον περιορισμένο χώρο αποθήκευσης των μπλοκ στο blockchain. Ωστόσο, ένα κρίσιμο ζήτημα είναι πώς να επιλεγούν τα δεδομένα που θα αποθηκεύονται στο blockchain για να επιτευχθεί ισορροπία μεταξύ μεγέθους μπλοκ και λειτουργικότητας. Μια συνήθης πρακτική είναι η αποθήκευση αναφοράς (hash) των δεδομένων στο blockchain, ενώ τα πλήρη δεδομένα φυλάσσονται στο cloud. Αυτό επιτρέπει γρήγορη ανάκτηση και επεξεργασία των δεδομένων από το cloud, ενώ παράλληλα διασφαλίζει την ακεραιότητα τους μέσω της blockchain τεχνολογίας. Παρ' όλα αυτά, η προσέγγιση αυτή ενδέχεται να οδηγήσει σε καθυστέρηση στην επαλήθευση των δεδομένων ή σε πιθανότητα αλλοίωσης εάν δεν ληφθούν κατάλληλα μέτρα ασφαλείας στο cloud.

Ένα άλλο σημαντικό θέμα είναι η χρήση τεχνικών blockchain για τη διευκόλυνση της ασφαλούς κοινής χρήσης δεδομένων, όπως στον τομέα της υγείας και στις έξυπνες πόλεις. Ωστόσο, οι περισσότερες πρόσφατες εργασίες εστίασαν στην εξέταση του δυναμικού συνδυασμού της αποθήκευσης στο cloud με τις υπάρχουσες τεχνικές blockchain, αντιμετωπίζοντας διάφορους περιορισμούς, όπως η συνεργασία πολλαπλών αλυσίδων. Η συνεργασία πολλαπλών αλυσίδων δεν είναι πάντοτε απαραίτητη, αλλά αποτελεί σημαντικό πλεονέκτημα σε πολλές εφαρμογές όπου η ανταλλαγή δεδομένων και η συνεργασία μεταξύ διαφορετικών blockchain είναι κρίσιμη. Σε τέτοιες περιπτώσεις, η δυνατότητα αυτή μπορεί να προσφέρει ευρύτερη διαλειτουργικότητα, ευελιξία, βελτιωμένη απόδοση και ολοκληρωμένες λύσεις, καθιστώντας την μια αξιόλογη προσθήκη στις τεχνολογικές υποδομές. [25]

5.3.1. Αποθήκευση Τιμών Hash στην Αλυσίδα

Παρόλο που το blockchain είναι ικανό να αποθηκεύσει δεδομένα ανθεκτικά σε παρεμβάσεις στην αλυσίδα, η ικανότητα αποθήκευσης του είναι περιορισμένη. Για παράδειγμα, το μέγεθος μπλοκ του Bitcoin είναι μόνο 1MB, το οποίο δεν μπορεί να χρησιμοποιηθεί για την αποθήκευση μεγάλου όγκου δεδομένων. Ταυτόχρονα, η αποθήκευση μεγάλης ποσότητας δεδομένων στην αλυσίδα θα μπορούσε να οδηγήσει σε απαγορευτικά υψηλό μέγεθος πλήρους κόμβου για χρήστες PC και κινητών. Για αυτόν τον λόγο, εισήχθη το off-chain storage (αποθήκευση εκτός αλυσίδας) ως η τεχνολογία για να αντιμετωπιστεί αυτή η πρόκληση.

Ειδικότερα, οι CSP μπορούν να προσφέρουν αποθήκευση ως υπηρεσία σε μια κλιμακούμενη λύση εκτός αλυσίδας.

Εξερευνώντας περαιτέρω, η εργασία των Shafagh et al. [50] υλοποίησε ασφαλή και αξιόπιστο έλεγχο πρόσβασης και διαχείριση κλειδιών για το σύστημα αποθήκευσης εκτός αλυσίδας με την υποστήριξη του blockchain. Η κατανεμημένη αποθήκευση cloud χρησιμοποιήθηκε για να αντιμετωπίσει τα ζητήματα κλιμάκωσης του συστήματος blockchain. Η εφαρμογή της κατανεμημένης αποθήκευσης cloud εκτός της αλυσίδας βελτιώνει την αποδοτικότητα, την ασφάλεια και τη διαλειτουργικότητα των συστημάτων blockchain, επιτρέποντας την αποτελεσματική αντιμετώπιση των προκλήσεων κλιμάκωσης. [25]

5.3.2. Αποθήκευση Μεταδεδομένων στην Αλυσίδα

Σε πολλές εργασίες οι δείκτες hash του συνόλου δεδομένων αποθηκεύονται στην αλυσίδα. Αν και αυτή η μέθοδος μπορεί να προστατεύσει τα δεδομένα από εξωτερικές παρεμβάσεις, τα δεδομένα βρίσκονται υπό την απειλή κακόβουλων εσωτερικών παραγόντων διότι υπάρχει η πιθανότητα να τροποποιηθούν από εσωτερικούς χρήστες ή παραγόντες με κακόβουλες προθέσεις. Οι επιθέσεις αυτές αφορούν τη συνεργασία πολλών εσωτερικών ή εξωτερικών παραγόντων με στόχο την επίτευξη κοινού σκοπού, συνήθως με κακόβουλο τρόπο, όπως η αλλοίωση ή η καταστροφή δεδομένων που αποθηκεύονται σε ένα σύστημα blockchain. Για να αντιμετωπιστεί αυτό το πρόβλημα, προτείνεται ένα ελεγχόμενο σχήμα ψηφοφορίας βασισμένο σε μεταδεδομένα στην αλυσίδα. Η εν λόγω προσέγγιση αντιμετώπισε τις επιθέσεις συνωμοσίας κατά τη διαδικασία τροποποίησης του αρχείου. Μέσω αυτής της τεχνικής, τα μεταδεδομένα στην αλυσίδα παρέχουν μια διαφανή και ανιχνεύσιμη ιστορία των προηγούμενων έγκυρων και μη έγκυρων αλλαγών του εγγράφου, διευκολύνοντας την ανίχνευση και αποτροπή τυχόν αλλοιώσεων ή καταστροφών δεδομένων που μπορεί να προκληθούν από κακόβουλες ενέργειες εντός του συστήματος blockchain.

Επίσης, υπάρχουν εργασίες στις οποίες εφαρμόστηκε το blockchain για να δημιουργήσει ένα αποκεντρωμένο μοντέλο PingER [47]. Το PingER (Ping End-to-End Reporting) είναι ένα σύστημα παρακολούθησης και μέτρησης της απόδοσης του Διαδικτύου που αναπτύχθηκε από το SLAC National Accelerator Laboratory. Χρησιμοποιεί το εργαλείο ping για να μετρήσει διάφορες μετρικές απόδοσης δικτύου, όπως την καθυστέρηση (latency), την απώλεια πακέτων (packet loss) και την τρέμουλα (jitter), από διαφορετικές γεωγραφικές τοποθεσίες παγκοσμίως. Σε αυτό το μοντέλο εργασίας, τα μεταδεδομένα περιελάμβαναν ρίζες Merkle με αρχεία δεδομένων ενώ οι τοποθεσίες αποθήκευσης αρχείων εκτός αλυσίδας (pointers) αποθηκεύτηκαν στην αλυσίδα. Τα αρχεία που αποθηκεύτηκαν σε εκτός αλυσίδας, χρησιμοποιήθηκαν με τα μεταδεδομένα στην αλυσίδα για να επιτρέπουν τον έλεγχο πρόσβασης και την επαλήθευση ταυτότητας ώστε να διασφαλιστεί η ασφάλεια των δεδομένων στο σύστημα αποθήκευσης εκτός αλυσίδας. [25]

5.4. Εξέλιξη Υλικού Νέφους για Blockchain Εξόρυξη

Οι αυξανόμενες προκλήσεις κατά τη διαδικασία εξόρυξης του blockchain οδήγησαν σε αυξημένο κόστος και χρήση χώρου για την εγκατάσταση εξορυκτικού εξοπλισμού σε τοπικές εγκαταστάσεις. Ωστόσο, η πρόοδος στην τεχνολογία οπτικοποίησης και παράλληλης υπολογιστικής έχει καταστήσει το cloud μια ευέλικτη επιλογή. Στο cloud, οι χρήστες πληρώνουν μόνο για τον χρόνο που χρησιμοποιούν τους υπολογιστές και απολαμβάνουν γρήγορη επεξεργασία δεδομένων.

Σε αυτό το σημείο επικεντρωνόμαστε σε δύο τεχνικές πτυχές: την καθυστέρηση και το ενεργειακό κόστος. Σε αντίθεση με την παραδοσιακή εξόρυξη blockchain, η εξόρυξη στο cloud προσφέρει πλεονέκτημα λόγω της κεντρικής ρύθμισης, που επιτρέπει βελτιστοποίηση των πόρων και εξοικονόμηση ενέργειας. Η υπολογιστική ικανότητα των μονάδων επεξεργασίας στα κέντρα δεδομένων του cloud ουσιαστικά καθορίζει την απόδοση της εκτέλεσης του μηχανισμού Proof of Work (PoW). Γι' αυτό το λόγο, πολλά προϊόντα αλλά και μελέτες στοχεύουν στη βελτίωση του ποσοστού επιτυχίας της εξόρυξης μέσω βελτιστοποίησης του (υποκείμενου) υλικού. Η βελτιστοποίηση αυτή πραγματοποιήθηκε σε τέσσερα στάδια ανάλογα με το είδος υλικού προς εστίαση την κάθε φορά: CPU, GPU, FPGA και ASIC. [21]

5.4.1. Εξόρυξη στο Νέφος με βάση τη CPU

Η διαδικασία εξόρυξης του Bitcoin βασίζεται στον αλγόριθμο SHA256. Μέσω μιας μελέτης [28], η διαδικασία αυτή περιγράφεται ως ένα πρόβλημα με περιορισμένη είσοδο και μικρή έξοδο. Στο πλαίσιο της εξόρυξης blockchain, οι εξορύκτες επιχειρούν να βρουν μια λύση που να πληροί συγκεκριμένες απαιτήσεις. Αυτές περιλαμβάνουν την εύρεση ενός αριθμού (nonce), τη ρίζας ενός δέντρου Merkle και τη χρονική στιγμή που κάνει το αποτέλεσμα των υπολογισμών να είναι μικρότερο από έναν συγκεκριμένο στόχο. Ωστόσο, η υπολογιστική ισχύς της κεντρικής μονάδας επεξεργασίας (CPU) είναι περιορισμένη για να εκτελέσει αποτελεσματικά αυτούς τους υπολογισμούς.

Για να βελτιωθεί η απόδοση της εξόρυξης, χρησιμοποιούνται διάφορες τεχνικές βελτιώσεις. Αυτές μπορεί να περιλαμβάνουν τη χρήση ειδικών μεθόδων προεπεξεργασίας των δεδομένων και την ανάπτυξη νέων αλγορίθμων όπως ο "Cuckoo Cycle" [35], που είναι πιο αποτελεσματικοί για την εξόρυξη. Αυτές οι βελτιώσεις συμβάλλουν στην αύξηση της ταχύτητας και της αποδοτικότητας της διαδικασίας εξόρυξης, καθιστώντας την πιο επικερδή και αποτελεσματική.

Παρόλα αυτά, η πρόσφατη ανάπτυξη εξοπλισμού εξόρυξης με GPU και ASIC θέτει υπό αμφισβήτηση την αρχική πρόθεση του Nakamoto για ισότιμη συμμετοχή (1 CPU = 1 ψήφος). Προκειμένου να ενθαρρυνθούν οι εξορυκτές που χρησιμοποιούν CPU, το Litecoin και άλλα κρυπτονομίσματα χρησιμοποιούν τον αλγόριθμο SCRYPT, ο οποίος απαιτεί και υπολογιστική ισχύ αλλά και αποθηκευτική χωρητικότητα. Παρόμοια, ο μηχανισμός Proof of Work (PoW) της Ethereum βασίζεται στον αλγόριθμο Ethash. Κατά τη διαδικασία εξόρυξης με τον αλγόριθμο Ethash, η ταχύτητα της μνήμης έχει σημαντική επίδραση στον ρυθμό εξόρυξης. [21]

5.4.2. Εξόρυξη με βάση GPU/FPGA στο cloud

Η κεντρική μονάδα επεξεργασίας (CPU) σχεδιάστηκε για γενική επεξεργασία. Στη διαδικασία της εξόρυξης, στοιχεία εκτός από την αριθμητική λογική μονάδα, όπως οι καταχωρητές και οι μονάδες πρόβλεψης κλάδων, ήταν περιττά. Ως εκ τούτου, η επαναλαμβανόμενη εργασία εξόρυξης για τη CPU ήταν απώλεια χρόνου και ενέργειας. Παρόλο που οι γύροι υπολογισμού SHA256 δεν μπορούν να παραλληλοποιηθούν, διαφορετικά nodes μπορούσαν να δοκιμαστούν ταυτόχρονα μεταξύ τους με παράλληλο υπολογισμό.

Το προαναφερόμενο πρόβλημα λύνεται με τη χρήση των GPUs. Σε αυτή την περίπτωση, σε ένα κέντρο εξόρυξης στο cloud που χρησιμοποιεί γραφικές κάρτες (GPU), υπάρχουν δύο βασικοί παράγοντες που πρέπει να ληφθούν υπόψη για να βελτιστοποιηθεί η υποδομή του υλικού.

Πρώτον, το κόστος του υλικού. Για να μειωθούν τα έξοδα για το υλικό, μπορεί να εξεταστεί η επιλογή οικονομικών γραφικών καρτών (GPU) αντί για τις πιο ακριβές επιλογές. Επιπλέον, οι ειδικές υποδομές, όπως οι θύρες PCIe, μπορούν να αξιοποιηθούν για να ελαχιστοποιηθούν τα κόστη. Για παράδειγμα, μια οικονομική GPU μπορεί να προσφέρει αποτελεσματική εξόρυξη χωρίς την ανάγκη για ακριβότερα εξαρτήματα. Επιπλέον, η χρήση ειδικών υποδομών, όπως οι θύρες PCIe, μπορεί να επιτρέψει τη σύνδεση περισσότερων GPU στο κέντρο εξόρυξης χωρίς την ανάγκη για ακριβότερες μητρικές πλακέτες. Με αυτόν τον τρόπο, οι δαπάνες για το υλικό μπορούν να μειωθούν σημαντικά, κάνοντας τη λειτουργία του κέντρου εξόρυξης πιο οικονομική και αποδοτική.

Δεύτερον, η σωστή σχεδίαση του συστήματος τροφοδοσίας. Για την αποτελεσματική λειτουργία του εξοπλισμού εξόρυξης στο cloud, είναι ουσιώδους σημασίας η σωστή σχεδίαση του συστήματος τροφοδοσίας και ψύξης. Μια κατάλληλη επιλογή μηχανισμών ψύξης και η σωστή διάταξη των γραφικών καρτών μπορούν να εξασφαλίσουν τη σταθερή λειτουργία τους και να αποτρέψουν την υπερθέρμανση. Η κατάλληλη ψύξη είναι απαραίτητη για να διατηρηθεί η θερμοκρασία των GPU σε ασφαλές επίπεδο, ενώ μπορεί να μειώσει επίσης την κατανάλωση ενέργειας και το κόστος λειτουργίας του εξοπλισμού. Με αυτόν τον τρόπο, η αποτελεσματικότητα και η διάρκεια ζωής του εξοπλισμού μπορούν να βελτιωθούν σημαντικά, μειώνοντας ταυτόχρονα τον κίνδυνο πιθανών βλαβών λόγω υπερθέρμανσης.

Από την άλλη μεριά, το FPGA (Field-Programmable Gate Arrays) είναι ένα ευέλικτο εργαλείο που μπορεί να προσαρμοστεί για να επιταχύνει συγκεκριμένα προβλήματα υπολογισμού, όπως η διαδικασία εξόρυξης. Ορισμένοι χάκερς ανέπτυξαν έναν εξορυκτή FPGA με προσαρμοσμένο κώδικα που ήταν ανοικτού κώδικα. Αυτός ο εξορυκτής είχε μειωμένα Input/Output operations και μνήμη RAM. Αυτή η προσέγγιση επέτρεψε την αξιοποίηση των δυνατοτήτων του FPGA για την εξόρυξη, με αποτέλεσμα μια πιο αποδοτική διαδικασία εξόρυξης χωρίς την προσθήκη περιττών στοιχείων που θα αυξομειώναν το κόστος και την πολυπλοκότητα. Η επιλογή μεταξύ FPGA και GPU εξαρτάται από τις συγκεκριμένες ανάγκες και προτεραιότητες του χρήστη, όπως η αποδοτικότητα ενέργειας, το κόστος, η ευκολία χρήσης και η απαιτούμενη υπολογιστική ισχύς. [25]

Επιλογή FPGA: Είναι κατάλληλη για όσους αναζητούν υψηλή αποδοτικότητα ενέργειας και είναι πρόθυμοι να επενδύσουν σε πιο ακριβό και περίπλοκο εξοπλισμό με δυνατότητα επαναπρογραμματισμού για εξειδικευμένους αλγόριθμους εξόρυξης.

Επιλογή GPU: Είναι ιδανική για όσους αναζητούν ευκολία στη χρήση και προγραμματισμό, καθώς και υψηλή υπολογιστική ισχύ χωρίς την ανάγκη εξειδικευμένης γνώσης. Οι GPU είναι επίσης πιο προσιτές και διαθέσιμες για ένα ευρύ φάσμα εφαρμογών. Έχουν όμως υψηλότερη κατανάλωση ενέργειας και θερμοκρασία σε σχέση με τα FPGA.

5.4.3. Εξόρυξη βασισμένη σε ενοποιημένα κυκλώματα ειδικού σκοπού (ASIC)

Η τεχνολογία ενοποιημένων κυκλωμάτων ειδικού σκοπού (Application-Specific Integrated Circuits - ASICs) μπορεί να οδηγήσει στην παραγωγή προσαρμοσμένων ολοκληρωμένων κυκλωμάτων για το συγκεκριμένο σενάριο (εφαρμογής) της εξόρυξης. Έτσι, η ανάπτυξη ενός εξορυκτής ASIC θα μπορούσε να ανταμειφθεί λόγω του βελτιστοποιημένου σχεδιασμού του για την εύρεση της κατακερματισμένης τιμής. Επιπλέον, με έναν σχετικά χαμηλό κόστος πόρων μπορούσε να επιτευχθεί μια υψηλή απόδοση στο ρυθμό κατακερματισμού.

Η εταιρεία Butterfly Labs (BFL) κυκλοφόρησε έναν εξορυκτής ASIC βασισμένο στον εξορυκτής FPGA τους το 2012. Αυτός ο εξορυκτής κατασκευάστηκε με διαδικασία 65nm έχοντας μέγιστη ταχύτητα 1,500GH/s. Το 2013, η Avalon πρότεινε έναν εξορυκτής με διαδικασία κατασκευής TSMC 110-nm. Αυτό το προϊόν μπορούσε να φτάσει τα 66Gh/s με κατανάλωση ισχύος 60W. Χάρη στην ανάπτυξη της τεχνολογίας κατασκευής τρανζίστορ, η απόδοση του εξορυκτής ASIC ουσιαστικά βελτιώθηκε εκθετικά ακολουθώντας τον νόμο του Moore. Το πιο πρόσφατο προϊόν της Avalon, το AvalonMiner 852, κατασκευάστηκε με τεχνολογία 16-nm. Μπορεί να επιτύχει 15TH/s με ενεργειακή απόδοση 100W/T. Μέχρι το 2019, το προϊόν της Bitmain καταλάμβανε το 70% των εξορυκτών στην αγορά. Διότι η εταιρεία αυτή πρότεινε πρώτη έναν εξορυκτής 7nm, ο οποίος μπορεί να επιτύχει 40TH/s με αποδεκτό κόστος ενέργειας.

Οι επεξεργαστές ASIC (Application-Specific Integrated Circuits) στον τομέα της εξόρυξης κρυπτονομισμάτων έχουν αποδειχθεί εξαιρετικά αποτελεσματικοί λόγω του εξειδικευμένου σχεδιασμού τους για συγκεκριμένους αλγόριθμους εξόρυξης. Σε αντίθεση με τους γενικούς επεξεργαστές γραφικών (GPU) και τους επαναπρογραμματίσιμους πίνακες πεδίου (FPGA), οι ASIC είναι σε θέση να επιτυγχάνουν υψηλές ταχύτητες εξόρυξης με ελάχιστη κατανάλωση ενέργειας. Αυτό οφείλεται στο γεγονός ότι κατασκευάζονται ειδικά για τον συγκεκριμένο σκοπό της εξόρυξης και υλοποιούν αλγόριθμους με υψηλή αποδοτικότητα. Το κόστος λειτουργίας είναι επίσης σημαντικό πλεονέκτημα των ASIC, καθώς η απόδοσή τους ανά μονάδα ενέργειας είναι συχνά πολύ καλύτερη σε σύγκριση με τους GPU και FPGA. Επιπλέον, το μικρότερο μέγεθος και η ολοκληρωμένη κατασκευή των ASIC τους καθιστούν ιδανικούς για χρήση σε μεγάλες εγκαταστάσεις εξόρυξης, όπου ο χώρος και η διαχείριση της θερμότητας είναι κρίσιμοι παράγοντες. [21]

6. Ερευνητικά κενά και μελλοντικές έρευνες

Η τρέχουσα μελέτη εστιάζει στην ενσωμάτωση του blockchain και του υπολογιστικού νέφους, τονίζοντας την ανάγκη να ληφθούν υπόψη και άλλες σχετικές τεχνολογίες για μελλοντικές ενημερώσεις και έρευνες. Η διερεύνηση μας υποδηλώνει ότι οι μελλοντικές προσπάθειες ενσωμάτωσης μπορεί να καλύψουν ένα ευρύτερο φάσμα, συνδυάζοντας διάφορες τεχνολογίες που σχετίζονται με τα δίκτυα και τα κατανεμημένα συστήματα.. Αυτά τα συμπεράσματα προκύπτουν από προηγούμενες μελέτες [55] [56] [57] που εξετάζουν εναλλακτικές προσεγγίσεις ολοκλήρωσης, όπως ο οριζόμενος από το λογισμικό δικτυακός προγραμματισμός (software-defined network computing), το Internet of Things (IoT), ο προγραμματισμός στην ακμή του δικτύου (edge computing), ο ομιχλώδης προγραμματισμός (fog computing) και τα δίκτυα ραδιοπρόσβασης στο νέφος.

Όσον αφορά τις ανησυχίες για την ασφάλεια, η προσέγγιση του υπολογιστικού νέφους διαφέρει σημαντικά από εκείνη των παραδοσιακών κέντρων δεδομένων. Παρόλο που το νέφος προσφέρει πολλά πλεονεκτήματα ασφάλειας σε σχέση με τα συμβατικά κέντρα δεδομένων, υπάρχουν επίσης σημαντικές προκλήσεις, όπως η διαχείριση πρόσβασης και ταυτοποίηση των χρηστών (συμπεριλαμβανομένων και των χρηστών του Παρόχου Υπηρεσιών Cloud) και η διαχείριση των πόρων. Η ασφάλεια στο υπολογιστικό νέφος μπορεί να βελτιωθεί μέσω της χρήσης της τεχνολογίας blockchain. Η τεχνολογία blockchain μπορεί να αυξήσει την ασφάλεια και την αξιοπιστία του cloud computing. Αν και θεωρείται απαιτητική τεχνολογία, το υπολογιστικό νέφος διαθέτει την απαραίτητη υπολογιστική ισχύ και χωρητικότητα αποθήκευσης ώστε να καλύψει τις απαιτήσεις χρήσης της.

6.1. Έρευνες για την βελτίωση του blockchain με τη βοήθεια του cloud

Ο συνδυασμός blockchain και cloud computing αποτελεί την καλύτερη κατεύθυνση για το μέλλον, καθώς προσφέρει μεγαλύτερη ασφάλεια και αποκέντρωση, ενώ παράλληλα βελτιώνει την εξουσιοδότηση και την προστασία της ιδιωτικότητας. Είναι απαραίτητο να συνεχίσουμε την έρευνα σε τομείς όπως η κατάλληλη αναπαραγωγή και διανομή των δεδομένων και η επιπλέον ασφάλεια, καθώς αυτές οι τεχνολογίες εξελίσσονται. Η διερεύνηση της χρήσης αυτού του συνδυασμού μπορεί να βοηθήσει τις επιχειρήσεις να αντιμετωπίσουν τις απειλές κατά των δεδομένων τους, κάτι που είναι κρίσιμο για τη λειτουργία και τη λήψη αποφάσεων στον σύγχρονο ανταγωνιστικό κόσμο. Πιο συγκεκριμένα και όσον αφορά την αποθήκευση στο νέφος (Cloud Storage) και το blockchain προκύπτουν οι εξής κατευθύνσεις για μελλοντική έρευνα:

6.1.1. Επιλογή Δεδομένων για Αποθήκευση στην Αλυσίδα

Εξερεύνηση μεθόδων για την επιλογή κατάλληλων δεδομένων που θα αποθηκεύονται στην αλυσίδα, προκειμένου να επιτευχθεί μια ισορροπία μεταξύ ασφάλειας και επεκτασιμότητας

του blockchain. Υπάρχουν λύσεις εκτός αλυσίδας για να αντιμετωπίσουμε τους περιορισμούς αποθήκευσης του blockchain. Η εφαρμογή της αποθήκευσης εκτός αλυσίδας ωφελεί το blockchain σε κλιμάκωση, αποδοτικότητα αποθήκευσης και ταχύτητα επαλήθευσης. Ο συμβιβασμός μεταξύ ασφάλειας δεδομένων και αποδοτικότητας του συστήματος blockchain είναι ένα ουσιαστικό πρόβλημα κατά τον σχεδιασμό του συστήματος επί/εκτός αλυσίδας. Η αποθήκευση πολλών τύπων μεταδεδομένων θα μπορούσε να διασφαλίσει ότι τα δεδομένα εκτός αλυσίδας είναι ασφαλή και ελεγχόμενα. Ωστόσο, η υψηλή ποσότητα δεδομένων στην αλυσίδα θα μπορούσε να μειώσει την κλιμακωσιμότητα και αποδοτικότητα του blockchain. Επομένως, ο τρόπος επιλογής κατάλληλων δεδομένων στην αλυσίδα για την αντιμετώπιση και των δύο ζητημάτων, δηλ. της ασφάλειας και κλιμακωσιμότητας, θα μπορούσε να είναι μια μελλοντική κατεύθυνση έρευνας.

6.1.2. Συνδυασμός Αποθήκευσης στο Cloud και Blockchain:

Έρευνα για τη βελτιστοποίηση της συγχώνευσης της αποθήκευσης στο cloud με τεχνικές blockchain, αντιμετωπίζοντας περιορισμούς όπως η συνεργασία πολλαπλών αλυσίδων (multi-chain collaboration). Η συνεργασία πολλαπλών αλυσίδων αποτελεί έναν σημαντικό περιορισμό κατά την ενσωμάτωση των τεχνολογιών blockchain στο περιβάλλον του cloud computing. Ο βασικός τρόπος αντιμετώπισης αυτού του προβλήματος είναι η ανάπτυξη πρωτοκόλλων και μηχανισμών που επιτρέπουν τη διαλειτουργικότητα μεταξύ διαφορετικών αλυσίδων blockchain. Αυτό μπορεί να επιτευχθεί μέσω της ανάπτυξης διακρατικών προτύπων ή μεθόδων διαλειτουργικότητας που επιτρέπουν την ασφαλή και αποδοτική μεταφορά δεδομένων και εντολών ανάμεσα σε διαφορετικά blockchain. Ένα παράδειγμα μπορεί να είναι η χρήση διαλειτουργικών γεφυρών (bridges) ή η ανάπτυξη ειδικών πρωτοκόλλων που επιτρέπουν τη συνεργασία διαφορετικών αλυσίδων για συγκεκριμένες εφαρμογές ή λειτουργίες. Η επιλογή της κατάλληλης τεχνολογικής προσέγγισης θα εξαρτηθεί από τις απαιτήσεις της συγκεκριμένης εφαρμογής και τους περιορισμούς που επιβάλλονται από το περιβάλλον του cloud. Αυτή η προσέγγιση θα επιτρέψει την αποδοτική αποθήκευση και διαχείριση δεδομένων στο cloud, ενώ ταυτόχρονα θα ενσωματώνει τα οφέλη της ασφάλειας και της διαφάνειας που προσφέρει το blockchain.

6.1.3. Αποθήκευση Κατακερματισμένων Τιμών στην Αλυσίδα

Μελετούμε τη χρήση off-chain τεχνολογίας για την αποθήκευση μεγάλου όγκου δεδομένων και τη βελτιστοποίηση της αποδοτικότητας του blockchain, αποθηκεύοντας κατακερματισμένες τιμές στην αλυσίδα. Αυτή η προσέγγιση μειώνει τον όγκο των δεδομένων στην αλυσίδα, διατηρώντας ταυτόχρονα την ασφάλεια και την ακεραιότητα των δεδομένων. Η αποθήκευση κατακερματισμένων τιμών επιτρέπει την ασφαλή κωδικοποίηση και επαλήθευση των δεδομένων χωρίς την ανάγκη για αποθήκευση πλήρους περιεχομένου στην blockchain. Έτσι, η απόδοση του blockchain βελτιώνεται καθώς μειώνεται η ποσότητα των δεδομένων που πρέπει

να διαχειριστεί κάθε κόμβος του δικτύου. Αυτή η τεχνική είναι ιδιαίτερα χρήσιμη σε εφαρμογές που απαιτούν γρήγορη απόκριση και χαμηλό κόστος αποθήκευσης στο blockchain.

6.1.4. Διαχείριση Πρόσβασης και Κλειδιών για Αποθήκευση Off-Chain

Έρευνα για την ασφαλή και αξιόπιστη διαχείριση πρόσβασης και κλειδιών για συστήματα αποθήκευσης εκτός αλυσίδας με την υποστήριξη του blockchain.

6.1.5. Βελτιστοποίηση Ισορροπίας Μεταξύ Αποδοτικότητας και Ασφάλειας

Ανάλυση των συμβιβασμών μεταξύ αποδοτικότητας αποθήκευσης και ασφάλειας δεδομένων, με σκοπό τη βελτιστοποίηση των συστημάτων on/off chain.

Η ανάπτυξη πιο αποδοτικών και ασφαλών συστημάτων blockchain σε συνδυασμό με τεχνολογίες αποθήκευσης στο νέφος είναι ένα σημαντικό ερευνητικό θέμα που αντιμετωπίζει πολλές προκλήσεις και δυνατότητες βελτίωσης. Η πρόκληση αυτή περιλαμβάνει την εύρεση της ιδανικής ισορροπίας μεταξύ αποδοτικότητας και ασφάλειας στη διαχείριση των δεδομένων και των εφαρμογών σε ένα περιβάλλον blockchain σε σύνδεση με την αποθήκευση στο νέφος.

6.1.6. Αντιμετώπιση του προβλήματος της κλιμακωσιμότητας

Τα Lightning Networks (LN) αποτελούν αποκεντρωμένη λύση δικτύου δευτέρου επιπέδου που βασίζεται στο Bitcoin και άλλα blockchain. Χρησιμοποιούν κανάλια πληρωμών εκτός αλυσίδας για να επιτρέπουν αστραπιαίες μικρές συναλλαγές μεταξύ χρηστών, χωρίς την ανάγκη επιβεβαίωσης σε κάθε συναλλαγή από το κύριο blockchain. Αυτό μειώνει το χρόνο εκτέλεσης συναλλαγών από λεπτά σε χιλιοστά του δευτερολέπτου, ενώ επίσης μειώνει τις προμήθειες για κάθε συναλλαγή. Η συνεχιζόμενη έρευνα και ανάπτυξη στον τομέα των Lightning Networks επικεντρώνεται στη βελτίωση της απόδοσης, την ασφάλεια και την ευρύτερη υιοθέτηση από την κοινότητα κρυπτονομισμάτων και τους χρήστες.

6.1.7. Βελτίωση της διαλειτουργικότητας

Τα Atomic Swaps είναι μια τεχνολογία που επιτρέπει την ασφαλή και αυτόματη ανταλλαγή διαφορετικών κρυπτονομισμάτων ανάμεσα σε διαφορετικά blockchain οικοσυστήματα, χωρίς την ανάγκη για ενδιάμεσους. Αυτή η τεχνολογία βασίζεται στη χρήση έξυπνων συμβολαίων για να εξασφαλίσει την ολοκλήρωση των συναλλαγών μόλις πληρούνται οι προϋποθέσεις, ενώ παράλληλα προσφέρει υψηλό επίπεδο ασφάλειας.

Άλλες τεχνολογίες που επιτρέπουν την ανταλλαγή δεδομένων μεταξύ διαφορετικών blockchain οικοσυστημάτων επίσης βρίσκονται σε πρώιμο στάδιο ανάπτυξης. Αυτές

συμπεριλαμβάνουν πρωτόκολλα διαλειτουργικότητας και γέφυρες ανάμεσα σε blockchain, τα οποία επιτρέπουν την ασφαλή μεταφορά και χρήση δεδομένων από ένα οικοσύστημα σε άλλο χωρίς την ανάγκη επικοινωνίας μέσω κεντρικών αρχών. Η συνεχής έρευνα σε αυτούς τους τομείς στοχεύει στη βελτίωση της απόδοσης, της ασφάλειας και της ευκολίας χρήσης των διαφορετικών blockchain τεχνολογιών.

6.1.8. Μείωση της ενεργειακής κατανάλωσης

Η αναζήτηση πιο πράσινων μεθόδων συναίνεσης παραμένει μια κρίσιμη περιοχή έρευνας, ειδικά καθώς η κατανάλωση ενέργειας από την μέθοδο/μηχανισμός Proof-of-Work εξακολουθεί να είναι ένα σημαντικό ζήτημα.

6.2. Έρευνες για την βελτίωση του cloud με βάση το blockchain

6.2.1. Αντιμετώπιση του προβλήματος του vendor lock-in

Η αντιμετώπιση του προβλήματος του vendor lock-in είναι κρίσιμη για πολλές επιχειρήσεις και οργανισμούς λόγω της έλλειψης προτύπων και της εξάρτησης από συγκεκριμένους παρόχους υπηρεσιών νέφους. Η απουσία ενός κοινού προτύπου επιτρέπει σε κάθε πάροχο να θέτει τις δικές του περιοριστικές συνθήκες και κλειδώνει τις επιχειρήσεις στη χρήση των συγκεκριμένων υπηρεσιών του. Επιπλέον, η εξάρτηση από έναν μόνο πάροχο μπορεί να αυξάνει τον κίνδυνο μείωσης της ευελιξίας και της ασφάλειας των δεδομένων, καθώς και να περιορίζει τη δυνατότητα επιλογής της καλύτερης τεχνολογικής λύσης για κάθε συγκεκριμένη ανάγκη. Συνεπώς, η ανάπτυξη κοινών προτύπων και ανοιχτών λύσεων είναι ουσιώδης για την εξάλειψη του vendor lock-in και την προώθηση της ανταγωνιστικότητας και της ασφάλειας στον τομέα των υπηρεσιών νέφους.

6.2.2. Έλεγχος Πρόσβασης στο Νέφος βάσει Blockchain

Τα εικονικά μηχανήματα (VMs) στο υπολογιστικό νέφος χρειάζονται επίσης μηχανισμούς ελέγχου πρόσβασης για την αποφυγή επιθέσεων πλευρικών καναλιών αλλά επίσης και η καταγραφή και η ανιχνευσιμότητα των κανόνων ελέγχου πρόσβασης. Ειδικότερα, τα εικονικά μηχανήματα (VMs) που φιλοξενούνται σε περιβάλλοντα cloud εκτίθενται σε επιθέσεις πλευρικών καναλιών. Αυτές οι επιθέσεις εκμεταλλεύονται τις πληροφορίες που διαρρέουν από τη χρήση κοινών πόρων, όπως η CPU, η μνήμη ή τα δίκτυα, για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητα δεδομένα. Σύμφωνα με τις γνώσεις μας, η εφαρμογή blockchain στη διαχείριση πρόσβασης VMs είναι περιορισμένη για πολλούς λόγους μεταξύ των οποίων είναι η πολυπλοκότητα υλοποίησης, το κόστος και η ταχύτητα των συναλλαγών σε σχέση με τις χρονικές απαιτήσεις για τις αποφάσεις πρόσβασης .

Στο μέλλον, η ασφάλεια των cloud VMs με την υποστήριξη του blockchain θα είναι η επόμενη τάση στην έρευνα. Ειδικότερα, για την αποφυγή τέτοιων επιθέσεων, απαιτείται ένας αποτελεσματικός μηχανισμός ελέγχου πρόσβασης για τα VMs. Η χρήση τεχνολογίας blockchain μπορεί να προσφέρει μια αξιόπιστη και ασφαλή μέθοδο, όχι μόνο για τη διαχείριση της πρόσβασης σε πόρους VMs αλλά και μέσω της αμετάβλητης καταγραφής και της διαφάνειας στην πρόσβαση διαχείριση. Ειδικότερα, οι ερευνητές θα πρέπει να εξετάσουν πώς τα αποκεντρωμένα και αμετάβλητα χαρακτηριστικά του blockchain μπορούν να εφαρμοστούν για την προστασία των VMs και πώς να αντιμετωπιστεί το ζήτημα της ταχύτητας συναλλαγών ώστε να ανταποκρίνεται στις απαιτήσεις των cloud VM περιβάλλοντων.

6.3. Έρευνες για την βελτίωση του συνδυασμού cloud-blockchain ή/και των BaaS υπηρεσιών

Το Blockchain-as-a-Service (BaaS) αναδεικνύεται ως ένας τομέας έρευνας και ανάπτυξης τόσο στον ακαδημαϊκό όσο και στον βιομηχανικό τομέα. Πέρα από τη βασική υποδομή και τα συστήματα backend, υπάρχει μεγάλη έμφαση στη διαφοροποίηση των προσφερόμενων υπηρεσιών για να καλύψουν διάφορες απαιτήσεις. Αυτό περιλαμβάνει την ενσωμάτωση υπηρεσιών που αφορούν την τεχνητή νοημοσύνη και τον έλεγχο πρόσβασης.

Από την άλλη μεριά, τρία βασικά προβλήματα των τεχνολογιών blockchain, όπως κληρονομήθηκαν από την αρχιτεκτονική τους, είναι η έλλειψη επεκτασιμότητας, η έλλειψη διαλειτουργικότητας και η αντιφατική τους στάση έναντι της έννοιας του πράσινου υπολογισμού. Επιπλέον, παρά την ευρεία υιοθέτησή του, το υπολογιστικό νέφος υποφέρει επίσης από διάφορους περιορισμούς, όπως η έλλειψη τυποποίησης που οδηγεί σε κλείδωμα του προμηθευτή, προβλήματα ασφάλειας και απορρήτου καθώς και θέματα ιδιοκτησίας δεδομένων και τοποθεσίας. Ακόμη, ενώ και οι δύο τεχνολογίες είναι σχετικά ώριμες, η ολοκλήρωσή τους μπορεί να δημιουργήσει νέες πολυπλοκότητες όσον αφορά τις τεχνικές πτυχές. Επομένως, οι παρακάτω ερευνητικές κατευθύνσεις παραμένουν σημαντικές και χρήζουν διερεύνησης ακόμη και σήμερα.

6.3.1. Εξέταση των τεχνικών προκλήσεων της ενοποίησης

Οι νέες τεχνικές προκλήσεις που προκύπτουν από την ενσωμάτωση των τεχνολογιών blockchain και cloud computing απαιτούν συνεχή έρευνα και ανάπτυξη για την αντιμετώπισή τους. Αυτές οι προκλήσεις περιλαμβάνουν την ανάγκη για επέκταση της επεκτασιμότητας του blockchain, η οποία είναι σημαντική λόγω της δυσκολίας στην επεξεργασία μεγάλου όγκου συναλλαγών. Επιπλέον, η ασφάλεια και το απόρρητο στο cloud computing απαιτούν συστηματική προστασία από κακόβουλες επιθέσεις και τη διασφάλιση της ιδιωτικότητας των δεδομένων. Η εξέλιξη αυτών των τεχνολογιών συχνά συνεπάγεται νέες πολυπλοκότητες και προκλήσεις, οι οποίες απαιτούν συνεχή προσοχή και επιμονή για την αποτελεσματική διαχείρισή τους.

6.3.2. Επίδραση της ενοποίησης στη νομοθεσία και τη ρύθμιση

Η διαρκής εξέλιξη των κανονισμών περί προστασίας δεδομένων και ιδιωτικότητας καθιστά αναγκαία την συνεχή έρευνα για το πώς αυτές οι ρυθμίσεις επηρεάζουν τις τεχνολογίες blockchain και cloud computing, ειδικά στο πλαίσιο των υπηρεσιών BaaS.

6.3.3. Αξιολόγηση της ωριμότητας των τεχνολογιών

Η ανάλυση της ωριμότητας και της αποδοχής των τεχνολογιών LN (Lightning Network) και Atomic Swaps στο πλαίσιο του blockchain είναι κρίσιμη για διάφορους λόγους. Καταρχάς, οι τεχνολογίες αυτές στοχεύουν στη βελτίωση της κλιμακωσιμότητας και της επίδοσης των δικτύων blockchain, καθώς και στη μείωση των χρόνων επιβεβαίωσης συναλλαγών. Επίσης, επιτρέπουν την απευθείας ανταλλαγή ψηφιακών περιουσιακών στοιχείων μεταξύ διαφορετικών blockchain χωρίς την ανάγκη για εμπλοκή τρίτων. Συγκεκριμένα, η Lightning Network επιτρέπει τη δημιουργία off-chain καναλιών για τις συναλλαγές, μειώνοντας έτσι τον φόρτο του κύριου blockchain. Αυτό βελτιώνει την επεξεργασία και την κλιμακωσιμότητα του δικτύου Bitcoin και άλλων blockchain που υποστηρίζουν LN. Τα Atomic Swaps από την άλλη πλευρά επιτρέπουν την άμεση και ανώνυμη ανταλλαγή κρυπτονομισμάτων μεταξύ διαφορετικών blockchain, χωρίς την ανάγκη για ενδιάμεση εμπλοκή αξιόπιστου τρίτου μέρους. Αν και αυτές οι τεχνολογίες ανήκουν στο πεδίο του blockchain, η εφαρμογή τους αντιμετωπίζει ποικίλες τεχνικές και λειτουργικές προκλήσεις που απαιτούν συνεχή έρευνα και ανάπτυξη για να βελτιωθούν και να ενσωματωθούν ευρύτερα στις πλατφόρμες blockchain.

6.3.4. Σχεδιασμός και υλοποίηση ασφαλών και επεκτάσιμων πλατφορμών BaaS

Η ανάπτυξη ασφαλών, επεκτάσιμων και αποδοτικών πλατφορμών BaaS είναι μια συνεχής διαδικασία που απαιτεί συνεχή έρευνα και καινοτομία.

6.3.5. Blockchain-Enabled Cloud Data Provenance

Η χρήση blockchain για την προέλευση δεδομένων στο υπολογιστικό νέφος έχει το δυναμικό να ενισχύσει τη διαφάνεια, την ασφάλεια και την αξιοπιστία των δεδομένων. Τα έξυπνα συμβόλαια μπορούν να επιτρέψουν την αυτόματη εκτέλεση κανόνων και πολιτικών για την πρόσβαση και τη χρήση των δεδομένων, εξασφαλίζοντας ότι οι διαδικασίες λειτουργούν με συνέπεια και ακεραιότητα.

Τα έξυπνα συμβόλαια παρέχουν κίνητρα για έντιμη συμπεριφορά διασφαλίζοντας ότι οι συμμετέχοντες στο δίκτυο συμμορφώνονται με τους κανόνες και τις πολιτικές. Επιπλέον, προβλέπουν τιμωρίες για κακόβουλες ενέργειες, όπως παραβιάσεις δεδομένων ή ανεπιθύμητες αλλαγές, ενθαρρύνοντας την ασφαλή και έντιμη χρήση των δεδομένων.

Μέσω αυτής της προσέγγισης, το blockchain μπορεί να εξαλείψει προβλήματα όπως η αλλοίωση δεδομένων και η ανεπιθύμητη παρέμβαση, ενισχύοντας την εμπιστοσύνη στον τρόπο διαχείρισης και αποθήκευσης των ευαίσθητων πληροφοριών στο νέφος υπολογιστών

Η προέλευση δεδομένων (data provenance) στο υπολογιστικό νέφος είναι η διαδικασία παρακολούθησης και καταγραφής της προέλευσης και των αλλαγών των δεδομένων. Η διαφάνεια και η ασφάλεια σε αυτή τη διαδικασία είναι κρίσιμη για την αξιοπιστία των δεδομένων. Ωστόσο, οι υπάρχουσες λύσεις ενδέχεται να μην είναι επαρκείς για να αποτρέψουν κακόβουλες ενέργειες ή να ενθαρρύνουν έντιμη συμπεριφορά λόγω της πολυπλοκότητας της τεχνολογίας και της αποκέντρωσης των δεδομένων. Η ανάγκη για προηγμένες τεχνικές που εξασφαλίζουν την ακρίβεια και την ακεραιότητα των δεδομένων είναι κρίσιμη για την αποτροπή πιθανών επιθέσεων και για την ενίσχυση της εμπιστοσύνης των χρηστών και των επιχειρήσεων στα νέφη υπολογιστών.

Η χρήση blockchain και έξυπνων συμβολαίων (smart contracts) μπορεί να παρέχει μια καινοτόμο λύση για την προέλευση δεδομένων στο cloud. Τα έξυπνα συμβόλαια είναι αυτοματοποιημένες συμφωνίες που εκτελούνται όταν πληρούνται συγκεκριμένες προϋποθέσεις, και μπορούν να προγραμματιστούν για να παρέχουν κίνητρα και τιμωρίες.

6.3.5.1. Κίνητρα για Έντιμη Συμπεριφορά

Οι χρήστες ή οι οντότητες που τηρούν τις πολιτικές και τις πρακτικές ασφαλείας θα μπορούσαν να λαμβάνουν ανταμοιβές, όπως πιστώσεις, μπόνους ή άλλες μορφές επιβράβευσης. Σε ένα σύστημα βασισμένο σε έξυπνα συμβόλαια για την προέλευση δεδομένων στο cloud, η ανταμοιβή μπορεί να προέρχεται από διάφορες πηγές, συνήθως ανάλογα με το σχεδιασμό του συστήματος και τους στόχους του. Ορισμένα πιθανά σενάρια ανταμοιβής και σχετικές αποφάσεις περιλαμβάνουν ανταμοιβές από την εταιρεία cloud, από τους χρήστες και με κρυπτονομίσματα. Η συνολική δομή και το μοντέλο ανταμοιβών προσαρμόζονται για να ευνοούν την έντιμη συμπεριφορά και να αποτρέπουν κακόβουλες ενέργειες στο πλαίσιο του cloud computing. Αυτός ο συνδυασμός ανταμοιβών και μέτρων ασφαλείας ενισχύει την ασφάλεια και την αξιοπιστία των υπηρεσιών cloud, προσφέροντας ένα πιο ασφαλές και αξιόπιστο περιβάλλον για τους χρήστες και τις επιχειρήσεις..

6.3.5.2. Τιμωρίες για Κακόβουλες Ενέργειες

Οι κακόβουλες ενέργειες θα μπορούσαν να τιμωρούνται αυτόματα, με έξυπνα συμβόλαια που επιβάλλουν ποινές, όπως πρόστιμα, περιορισμό πρόσβασης ή άλλες κυρώσεις. Οι κακόβουλες ενέργειες θα μπορούσαν να τιμωρούνται αυτόματα, με έξυπνα συμβόλαια που επιβάλλουν ποινές, όπως πρόστιμα, περιορισμό πρόσβασης ή άλλες κυρώσεις. Τα οφέλη χρήσης μιας τέτοιας λύσης είναι η ασφάλεια, καθώς η χρήση blockchain εξασφαλίζει την αμεταβλητότητα και τη διαφάνεια των εγγραφών προέλευσης δεδομένων, καθιστώντας δύσκολο για κακόβουλους χρήστες να παραποιήσουν τις πληροφορίες. Επιπλέον, προσφέρεται αξιοπιστία στα δεδομένα, καθώς οι χρήστες μπορούν να εμπιστευτούν ότι η προέλευσή τους έχει παρακολουθηθεί και καταγραφεί με ασφάλεια. Επιπλέον, η αυτοματοποίηση μέσω των έξυπνων συμβολαίων

επιτρέπει την αυτόματη επιβολή των διαδικασιών επιβράβευσης και τιμωρίας, μειώνοντας την ανάγκη για ανθρώπινη παρέμβαση και ενισχύοντας τη συνέπεια στην εφαρμογή των κανόνων.

Τα οφέλη χρήσης μιας τέτοιας λύσης είναι:

- *Ασφάλεια*: Η χρήση blockchain εξασφαλίζει την αμεταβλητότητα και τη διαφάνεια των εγγραφών προέλευσης δεδομένων, καθιστώντας δύσκολο για κακόβουλους χρήστες να παραποιήσουν τις πληροφορίες.
- *Αξιοπιστία*: Οι χρήστες μπορούν να εμπιστεύονται περισσότερο τα δεδομένα, γνωρίζοντας ότι η προέλευσή τους έχει παρακολουθηθεί και καταγραφεί με ασφάλεια.
- *Αυτοματοποίηση*: Τα έξυπνα συμβόλαια μπορούν να αυτοματοποιήσουν τις διαδικασίες επιβράβευσης και τιμωρίας, μειώνοντας την ανάγκη για ανθρώπινη παρέμβαση και ενισχύοντας τη συνέπεια στην εφαρμογή των κανόνων.

Συνοψίζοντας, η εστίαση σε ένα σύστημα βασισμένο σε έξυπνα συμβόλαια για την προέλευση δεδομένων στο cloud, που παρέχει κίνητρα για έντιμη συμπεριφορά και τιμωρίες για κακόβουλες ενέργειες, αποτελεί μια πολλά υποσχόμενη κατεύθυνση για μελλοντική έρευνα και ανάπτυξη, προσφέροντας αυξημένη ασφάλεια και αξιοπιστία στα συστήματα cloud.

6.3.6. Κατευθύνσεις Έρευνας για την Εκφόρτωση Υπολογισμών

Οι μελλοντικές έρευνες σε αυτόν τον τομέα περιλαμβάνουν την αξιολόγηση των συμβιβασμών μεταξύ της βελτιστοποίησης της κοινωνικής ευημερίας και της μεγιστοποίησης του κέρδους των παρόχων, καθώς και τη χρήση τεχνολογιών βαθιάς μάθησης στην τιμολόγηση και στις δημοπρασίες υπό την παρουσία πολλαπλών παρόχων υπηρεσιών. Η ανάγκη για μελλοντικές έρευνες στις προαναφερθείσες κατευθύνσεις είναι υπαρκτή λόγω των υφιστάμενων προκλήσεων στις αγορές υπηρεσιών, όπως η ανισορροπία μεταξύ κέρδους και κοινωνικής ευημερίας, η πολύπλοκη και αδιαφανής τιμολόγηση, η έλλειψη διαφάνειας στις δημοπρασίες και τα συγκρουόμενα συμφέροντα των παρόχων, καθιστούν απαραίτητες τις μελλοντικές έρευνες. Οι έρευνες που επικεντρώνονται στην αξιολόγηση των συμβιβασμών, στη χρήση τεχνολογιών βαθιάς μάθησης και στην ανάπτυξη δίκαιων και αποδοτικών αγορών μπορούν να προσφέρουν λύσεις που θα οδηγήσουν σε πιο ισορροπημένες και ευημερούσες αγορές υπηρεσιών.

6.3.6.1. Βελτιστοποίηση Κοινωνικής Ευημερίας έναντι Μεγιστοποίησης Κέρδους Παρόχων

Υπάρχει ένας εγγενής συμβιβασμός μεταξύ της βελτιστοποίησης της κοινωνικής ευημερίας και της μεγιστοποίησης του κέρδους των παρόχων υπηρεσιών. Η κοινωνική ευημερία αναφέρεται στο συνολικό όφελος που αποκομίζουν όλοι οι χρήστες και η κοινωνία από τις υπηρεσίες, ενώ η μεγιστοποίηση του κέρδους επικεντρώνεται στα έσοδα και την κερδοφορία των παρόχων.

Μελλοντικές έρευνες θα πρέπει να επικεντρωθούν στην ανάπτυξη μεθόδων που θα επιτρέπουν την ισορροπία μεταξύ αυτών των δύο στόχων. Αυτό μπορεί να περιλαμβάνει την ανάλυση διαφορετικών μοντέλων τιμολόγησης και στρατηγικών κατανομής πόρων που εξισορροπούν το όφελος των χρηστών με τα οικονομικά κίνητρα των παρόχων.

6.3.6.2. Τεχνολογίες Βαθιάς Μάθησης στην Τιμολόγηση και στις Δημοπρασίες

Η τιμολόγηση και οι δημοπρασίες σε περιβάλλοντα με πολλαπλούς παρόχους υπηρεσιών είναι πολύπλοκα προβλήματα που απαιτούν προηγμένες μεθόδους ανάλυσης δεδομένων και λήψης αποφάσεων.

Η χρήση τεχνολογιών βαθιάς μάθησης μπορεί να προσφέρει σημαντικές βελτιώσεις σε αυτούς τους τομείς. Τα μοντέλα βαθιάς μάθησης μπορούν να αναλύουν μεγάλα σύνολα δεδομένων για να προβλέπουν τη ζήτηση, να καθορίζουν τις βέλτιστες τιμές και να βελτιώνουν τις διαδικασίες δημοπρασίας, λαμβάνοντας υπόψη τις συμπεριφορές των χρηστών και τις στρατηγικές των ανταγωνιστών.

Η εφαρμογή αυτών των τεχνολογιών απαιτεί προσεκτική μελέτη των αλγορίθμων, της υποδομής δεδομένων και των ηθικών ζητημάτων που προκύπτουν από τη χρήση αυτόματων συστημάτων λήψης αποφάσεων.

6.3.7. ASIC-Based Mining

Οι διαφορετικές εργασίες εξόρυξης προκαλούν ετερογένεια σε ένα υπολογιστικό νέφος που χρησιμοποιεί ASICs για τις εργασίες εξόρυξης λόγω του γεγονότος πως τα κυκλώματα αυτά δεν είναι επαναπρογραμματιζόμενα. Διαφορετικοί τύποι εργασιών εξόρυξης (όπως εργασίες με διαφορετικούς αλγορίθμους συναίνεσης) χρησιμοποιούν διαφορετικά ASICs. Κάθε τύπος εργασίας εξόρυξης μπορεί να απαιτεί ένα συγκεκριμένο είδος ASIC που είναι βελτιστοποιημένο για τον συγκεκριμένο αλγόριθμο συναίνεσης που χρησιμοποιείται. Αυτό μπορεί να προκαλέσει προβλήματα στην αποδοτικότητα και τη διαχείριση των πόρων, διότι κάθε ASIC είναι σχεδιασμένο για ένα συγκεκριμένο σκοπό και δεν είναι επαναπρογραμματιζόμενο όπως τα FPGA. Η ανάγκη να υποστηρίξουν τα κέντρα δεδομένων διαφορετικούς τύπους ASIC για διαφορετικές εργασίες εξόρυξης μπορεί να αυξήσει το κόστος και την πολυπλοκότητα της υποδομής. Η ετερογένεια αυτή μπορεί να οδηγήσει σε προκλήσεις όσον αφορά την αποδοτικότητα και τη διαχείριση των πόρων.

Από την άλλη μεριά, η χρήση FPGA (Field-Programmable Gate Arrays) μπορεί να προσφέρει μια λύση για τη διατήρηση της ομοιογένειας στα κέντρα δεδομένων στο cloud. Τα FPGA είναι επαναπρογραμματιζόμενα ολοκληρωμένα κυκλώματα που μπορούν να προσαρμοστούν για διαφορετικές εργασίες (όπως αυτές της εξόρυξης), παρέχοντας μεγαλύτερη ευελιξία και διατηρώντας την ομοιογένεια των υπολογιστικών πόρων. Επιπλέον, η χρήση FPGAs μπορεί να βελτιώσει την αποδοτικότητα, καθώς οι πόροι μπορούν να επαναπρογραμματιστούν και να προσαρμοστούν στις εκάστοτε ανάγκες, αποφεύγοντας την αχρηστία ή την υποχρησιμοποίηση εξειδικευμένων ASIC.

- Οι συμβιβασμοί μεταξύ της ομοιογένειας και της αποδοτικότητας των κέντρων δεδομένων στο cloud αποτελούν ένα ενδιαφέρον πεδίο για μελλοντική έρευνα. Οι βασικοί τομείς που αξίζουν διερεύνηση περιλαμβάνουν:

- *Ανάλυση Απόδοσης*: Μελέτη της απόδοσης των κέντρων δεδομένων που χρησιμοποιούν FPGA σε σύγκριση με αυτά που χρησιμοποιούν ASIC, για διάφορες εργασίες εξόρυξης.

- *Κόστος και Οφέλη*: Εκτίμηση του κόστους υλοποίησης και συντήρησης FPGA σε σχέση με τα ASIC, λαμβάνοντας υπόψη την ευελιξία και τη δυνατότητα επαναπρογραμματισμού των FPGA.

- *Ενεργειακή Αποδοτικότητα*: Έρευνα σχετικά με την κατανάλωση ενέργειας των FPGA σε σύγκριση με τα ASIC, ειδικά σε περιβάλλοντα με ποικιλία εργασιών εξόρυξης.

Συνοψίζοντας, η χρήση FPGA για τη διατήρηση της ομοιογένειας στα κέντρα δεδομένων στο cloud μπορεί να προσφέρει σημαντικά πλεονεκτήματα όσον αφορά την ευελιξία και την αποδοτικότητα. Ωστόσο, οι συμβιβασμοί μεταξύ ομοιογένειας και αποδοτικότητας αξίζουν περαιτέρω μελέτη για να καθοριστεί η βέλτιστη προσέγγιση για τη διαχείριση των πόρων στα σύγχρονα κέντρα δεδομένων.

6.3.8. Εκφόρτωση βάσει κέρδους των CSP

Οι μελλοντικές εργασίες σε αυτό το πεδίο περιλαμβάνουν την αξιολόγηση των συμβιβασμών μεταξύ της βελτιστοποίησης της κοινωνικής ευημερίας και της μεγιστοποίησης του κέρδους του παρόχου, καθώς και τις τεχνολογίες βαθιάς μάθησης στην τιμολόγηση και δημοπρασία υπό πολλαπλούς παρόχους υπηρεσιών.

7. Συμπεράσματα

Η παρούσα διπλωματική εργασία ανέδειξε την πολυπλοκότητα και τις πολλαπλές δυνατότητες συνέργειας μεταξύ του Υπολογιστικού Νέφους (Cloud Computing) και της Αλυσίδας Συστοιχίας (Blockchain). Η ανάλυση και διερεύνηση αυτών των τεχνολογιών αποκαλύπτουν ότι η συνέργειά τους μπορεί να προσφέρει σημαντικά πλεονεκτήματα και να αντιμετωπίσει κρίσιμα ζητήματα στους τομείς της ασφάλειας, της αποδοτικότητας και της διαφάνειας των πληροφοριακών συστημάτων.

Το Υπολογιστικό Νέφος μπορεί να παρέχει τους απαραίτητους υπολογιστικούς πόρους και την υποδομή για την υποστήριξη των εφαρμογών Blockchain. Αυτό περιλαμβάνει τη δυνατότητα για αποδοτική αποθήκευση και επεξεργασία δεδομένων, μειώνοντας έτσι τα κόστη και βελτιώνοντας την απόδοση των εφαρμογών Blockchain. Επιπλέον, μέσω του Υπολογιστικού Νέφους, οι οργανισμοί μπορούν να εκμεταλλευτούν υπηρεσίες, όπως το Blockchain as a Service (BaaS), το οποίο απλοποιεί την ανάπτυξη και τη διαχείριση λύσεων Blockchain χωρίς την ανάγκη σημαντικών επενδύσεων σε υποδομές.

Αντίστοιχα, το Blockchain μπορεί να ενισχύσει το Υπολογιστικό Νέφος προσφέροντας χαρακτηριστικά που βελτιώνουν την ασφάλεια, την ακεραιότητα και τη διαφάνεια των δεδομένων. Η τεχνολογία Blockchain μπορεί να χρησιμοποιηθεί για την παροχή ασφαλούς αποθήκευσης δεδομένων, την απόδειξη της προέλευσης δεδομένων (data provenance) και τον έλεγχο πρόσβασης. Αυτές οι εφαρμογές ενισχύουν την εμπιστοσύνη και μειώνουν τους κινδύνους παραβίασης της ασφάλειας και της ακεραιότητας των δεδομένων στο Υπολογιστικό Νέφος.

Οι υπάρχουσες προσεγγίσεις δείχνουν ότι ήδη υλοποιούνται εφαρμογές που εκμεταλλεύονται αυτή τη συνέργεια, όπως οι μηχανισμοί ασφαλούς αποθήκευσης δεδομένων, η αποδεδειγμένη προέλευση δεδομένων και οι μέθοδοι ελέγχου πρόσβασης. Επίσης, το Blockchain μπορεί να προσφέρει λύσεις για την αποφυγή διπλών δεδομένων (data deduplication) και την αναζητήσιμη κρυπτογράφηση, βελτιώνοντας την αποδοτικότητα και την ασφάλεια των υπηρεσιών Cloud.

Ενώ οι παραδοσιακές λύσεις για την αποφυγή διπλών δεδομένων και την αναζητήσιμη κρυπτογράφηση είναι αποτελεσματικές, η χρήση του Blockchain προσθέτει ένα επιπλέον επίπεδο ασφάλειας, ακεραιότητας και διαφάνειας. Αυτά τα χαρακτηριστικά καθιστούν το Blockchain ιδιαίτερα χρήσιμο σε περιβάλλοντα όπου η ασφάλεια και η εμπιστοσύνη στα δεδομένα είναι κρίσιμης σημασίας, όπως στην υγειονομική περίθαλψη, τις χρηματοοικονομικές υπηρεσίες και τις έξυπνες πόλεις.

Παρά τα πλεονεκτήματα που προσφέρουν οι συνέργειες αυτές, υπάρχουν σημαντικά ερευνητικά κενά που απαιτούν περαιτέρω διερεύνηση. Αυτά περιλαμβάνουν την ανάγκη για βελτίωση της διαλειτουργικότητας μεταξύ διαφορετικών Blockchain και Cloud πλατφορμών, την ανάπτυξη λύσεων για τη μείωση της ενεργειακής κατανάλωσης, και τη βελτίωση της επεκτασιμότητας και της αποδοτικότητας των συστημάτων. Οι προτεινόμενες κατευθύνσεις για

μελλοντικές έρευνες μπορούν να συμβάλουν στην ανάπτυξη πιο ασφαλών και αποδοτικών λύσεων, ενισχύοντας την συνεργασία μεταξύ των δύο τεχνολογιών.

Η πρακτική εφαρμογή των προτεινόμενων λύσεων και η περαιτέρω διερεύνηση των συνεργειών μεταξύ Υπολογιστικού Νέφους και Αλυσίδας Συστοιχίας μπορούν να συμβάλουν στην ανάπτυξη καινοτόμων υπηρεσιών και εφαρμογών. Οι οργανισμοί μπορούν να εκμεταλλευτούν τις δυνατότητες αυτές για να βελτιώσουν την αποδοτικότητα και την ασφάλεια των πληροφοριακών τους συστημάτων, ενώ ταυτόχρονα μειώνουν τα κόστη και αυξάνουν την ευελιξία τους.

Συνοψίζοντας, η παρούσα εργασία προσφέρει σημαντικές γνώσεις και κατευθύνσεις για την ενίσχυση της συνεργασίας μεταξύ των δύο τεχνολογιών, προτείνοντας τρόπους που μπορούν να αξιοποιηθούν για τη βελτίωση της απόδοσης και της ασφάλειας των πληροφοριακών συστημάτων. Η περαιτέρω διερεύνηση και η πρακτική εφαρμογή των προτεινόμενων λύσεων μπορούν να συμβάλουν στην ανάπτυξη πιο ασφαλών, αποδοτικών και ευέλικτων υπολογιστικών περιβαλλόντων.

8. Βιβλιογραφία

1. Ντοά, Γ. (2017). "Blockchain και η εφαρμογή του στο Internet of Things (IoT)." Πανεπιστήμιο Αθηνών.
2. Sarmah, S. S. (2018). "Understanding Blockchain Technology." *Computer Science and Engineering*, 8(2), 23-29. DOI: 10.5923/j.computer.20180802.02.
3. Kim, J. (2017). "Blockchain Technology and Its Applications: Case Studies." *School of Computer Engineering*,"
4. Shrivass, M. K., & Yeboah, T. (2018). "The Disruptive Blockchain: Types, Platforms and Applications."
5. Technology.Sarmah, S. S. (2018). Understanding Blockchain Technology. *Computer Science and Engineering*, 8(2), 23-29. DOI: 10.5923/j.computer.20180802.02
6. Niranjanamurthy, M., Nithya, B. N., & Jagannatha, S. (2018). Analysis of Blockchain technology: pros, cons and SWOT. *Springer Science+Business Media, LLC, part of Springer Nature*.
7. Golosova, J., & Romanovs, A. (2018). The Advantages and Disadvantages of the Blockchain Technology. *Dept. of Modelling and Simulation, Riga Technical University, Riga, Latvia*.
8. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends.
9. Paul, P. K., Aithal, P. S., Saavedra, R., & Ghosh, S. (2021). Blockchain Technology and Its Types—A Short Review.
10. Paul, P.K., & Ghose, M.K. (2012). Cloud Computing: Possibilities, Challenges and Opportunities with Special Reference to its Emerging Need in the Academic and Working Area of Information Science.
11. Avram (Olaru), M.-G. (2013). Advantages and challenges of adopting cloud computing from an enterprise perspective. In *Proceedings of the 7th International Conference Interdisciplinarity in Engineering (INTER-ENG 2013)*.
12. Apostu, A., Puican, F., Ularu, G., Suci, G., & Todoran, G. (2013). Study on advantages and disadvantages of Cloud Computing – the advantages of Telemetry Applications in the Cloud. *Economic Informatics and Cybernetics Department, Academy of Economic Studies*, 15(17), Calea Dorobanți, Bucharest. University POLITEHNICA of Bucharest, Romania.
13. Momeni, M. R. (2015). A Survey of Mobile Cloud Computing: Advantages, Challenges and Approaches. *Department of Computer Engineering, Faculty of Electrical and Computer Engineering, Imam Reza International University of Mashhad, Mashhad, Iran*.
14. Mohabbattalab, E., von der Heidt, T., & Mohabbattalab, B. (2016). The perceived advantages of cloud computing for SMEs.
15. SUBBIAH, M., D.S.S. MUTHUKUMARAN, and D. RAMKUMAR, Enhanced Survey and Proposal to secure the data in Cloud Computing Environment. *International Journal of Engineering Science*, (2013).

16. Wang, J., Ou, W., Wang, W., Sherratt, R. S., Ren, Y., & Yu, X. (2023). Data security storage mechanism based on blockchain network.
17. Khanna, A., Sah, A., Bolshev, V., Burgio, A., Panchenko, V., & Jasiński, M. (2022). "Blockchain–Cloud Integration: A Survey."
18. Habib, G., Sharma, S., Ibrahim, S., Ahmad, I., Qureshi, S., & Ishfaq, M. (2022). "Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing."
19. Luo, C., Xu, L., Li, D., & Wu, W. (2020). "Edge Computing Integrated with Blockchain Technologies."
20. Alshinwan, M., Shdefat, A. Y., Mostafa, N., AlSokkar, A. A. M., Alsarhan, T., & Almajali, D. (2022). "Integrated cloud computing and blockchain systems: A review."
21. Shi, J. (2019). "The Application of Blockchain-as-a-Service (BaaS) and its Providers in China."
22. Alshurafa, S.M., & Eleyan, D. (2021). "A Survey Paper on Blockchain as a Service Platforms".
23. N. Courtois, M. Grajek, and R. Naik, "Optimizing SHA256 in bit-coin mining," in Proc. Int. Conf. Cryptography Security Syst., 2014, pp. 131–144.
24. Onik, M. M. H., & Miraz, M. H. (2021). Performance Analytical Comparison of Blockchain-as-a-Service (BaaS) Platforms.
25. Gai, K., Guo, J., Zhu, L., & Yu, S. (2021). Blockchain Meets Cloud Computing: A Survey.
26. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. IEEE International Congress on Big Data, 557-564.
27. Swan, M. (2015). Blockchain: Blueprint for a New Economy. O'Reilly Media.
28. Mougayar, W. (2016). The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology. Wiley.
29. Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World. Penguin.
30. Goyal, S. (2014). Public vs Private vs Hybrid vs Community - Cloud Computing: A Critical Review. I.J. Computer Network and Information Security, 2014(3), 20-29.
31. Zhang, X., Yang, L., Zhang, S., & Xu, L. (2017). "A Survey of Blockchain Consensus Algorithms."
32. Tapscott, D., Tapscott, A. (2016). "Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World."
33. Lantz L., Cawrey D. (2020). "Mastering Blockchain: Unlocking the Power of Cryptocurrencies, Smart Contracts, and Decentralized Applications."
34. Liang, X., Shetty, S., Tosh, D., Kamhoua, C., Kwiat, K., & Njilla, L. (2017). ProvChain: A Blockchain-based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability.
35. Ramachandran, A., & Kantarcioglu, M. (2018). SmartProvenance: A Distributed, Blockchain Based Data Provenance System.
36. W. Chen et al., "Cooperative and distributed computation offloading for blockchain-empowered industrial Internet of Things," IEEE Internet Things J., vol. 6, no. 5, pp. 8433–8446, Oct. 2019.

37. Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, "When mobile blockchain meets edge computing," *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 33–39, Aug. 2018
38. Z. Xiong, S. Feng, D. Niyato, P. Wang, and Z. Han, "Optimal pricing-based edge computing resource management in mobile blockchain," in *Proc. IEEE Int. Conf. Commun.*, 2018, pp. 1–6
39. H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy, "Towards blockchain-based auditable storage and sharing of IoT data," in *Proc. ACM Cloud Comput. Security Workshop*, 2017, pp. 45–50.
40. C. Qiu, H. Yao, C. Jiang, S. Guo, and F. Xu, "Cloud computing assisted blockchain-enabled Internet of Things," *IEEE Trans. Cloud Comput.*, early access, Jul. 2019, doi: 10.1109/TCC.2019.2930259.
41. K. Gai, Y. Wu, L. Zhu, L. Xu, and Y. Zhang, "Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7992–8004, Oct. 2019.
42. Liang et al., "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," in *Proc. IEEE 28th Annu. Int. Symp. PIMRC*, 2017, pp. 1–5
43. Xiaoyun Li, Zibin Zheng, Hong-Ning Dai, "When services computing meets blockchain: Challenges and opportunities," 2020
44. R. Chaudhary, A. Jindal, G. Aujla, S. Aggarwal, N. Kumar, and K. Choo, "BEST: Blockchain-based secure energy trading in SDN-enabled intelligent transportation system," *Comput. Security*, vol. 85, pp. 288–299, Aug. 2019
45. P. K. Sharma, S. Singh, Y.-S. Jeong, and J. H. Park, "DistBlockNet: A distributed blockchains-based secure SDN architecture for IoT networks," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 78–85, Sep. 2017
46. X. Ling, J. Wang, T. Bouchoucha, B. Levy, and Z. Ding, "Blockchain radio access network (B-RAN): Towards decentralized secure radio access paradigm," *IEEE Access*, vol. 7, pp. 9714–9723, 2019
47. Ali, S., Wang, G., White, B., & Cottrell, R. L. (2018). A Blockchain-Based Decentralized Data Storage and Access Framework for PingER. In 17th IEEE International Conference on Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering.